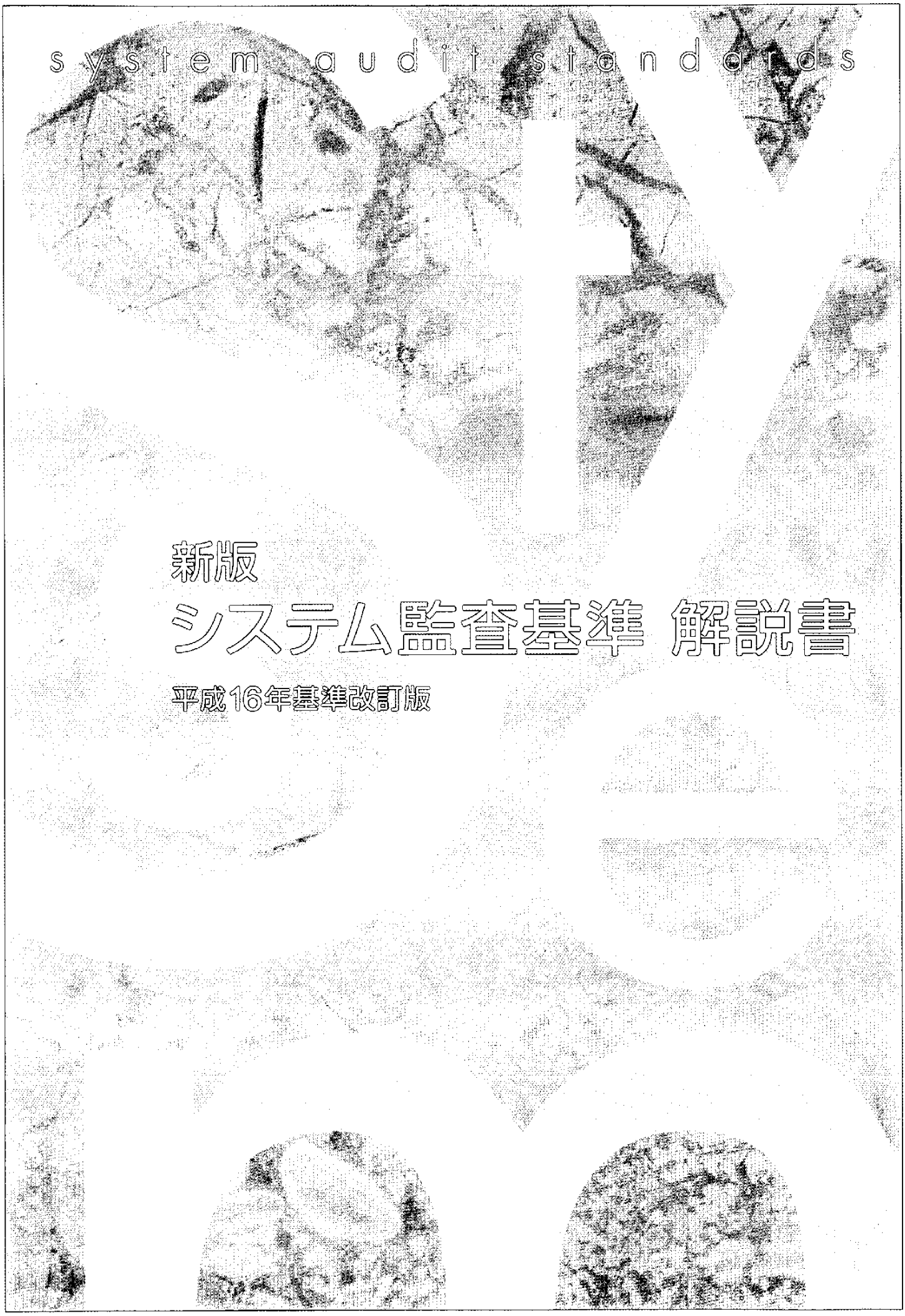
system audit standards



新版

システム監査基準 解説書

平成16年基準改訂版

新版

システム監査基準解説書

平成16年基準改訂版

監修にあたって

ITの革新とともに、情報システムはその位置付けが大きく変化し、今や企業経営、組織運営にとって欠かせない基盤となりました。即ち、かつての専用システム、大型汎用機の時代から、一人一台パソコンを持つ時代へと変遷する中で、ITが今や企業統治や企業戦略の実現手段、通信手段、外部向けサービスの提供手段に至るまで深く浸透してきています。IT は、経営の３要素と言われる「人」「モノ」「カネ」と同様に重要な要素であると言えます。

こうした変化の背景には、インターネットの急速な発展が深く関係しています。システム監査が前回 1996 年（平成８年）に改訂されてからの９年は、正にインターネットの発展の歴史そのものでもあります。この間、情報システムやインターネットは、中小企業や一般利用者に至るまで「ユーザ」の底辺を一気に拡げてきました。

ユーザの底辺が拡がり、浸透していく一方で、ユーザは情報システムを巡るリスクにも直面するようになりました。また、情報システムへの依存度の高まりとともに、そのリスクは年々高まっていると言わざるを得ません。本来、情報システムは企業・個人の利便性・効率性を大幅に向上するためのものですが、情報システムを導入・構築していく上で、その信頼性を確保していかなければ、企業の信用ある経営は成り立ちませんし、また安全性を確保しなければ、企業の継続的な製品・サービスの提供がままならないだけでなく、情報流出などがおこった場合などには法的責任や社会的責任も負いかねません。加えて、情報化投資は当然多大な費用が生じるわけですから、その目的や戦略、費用対効果やリスクに関して株主や投資家などのステークホルダーに対する説明責任も生じてきます。

そのため、経済産業省は情報システムのライフサイクル各段階におけるリスクが適切に管理されているかを監査するための必要事項を記した「システム監査基準」(1985 年策定、1996 年改訂)を、IT ガバナンスの実現に寄与することを目的に大幅に改訂し、今回新しい「システム管理基準」、「システム監査基準」として公表しました。改訂にあたっては、IT ガバナンスの観点を考慮したことに加えて、技術革新に伴う新たなリスクへの対応のための管理項目を追加し、説明責任を果たすために内部だけでなく外部への監査結果の開示も想定した手続きを記しております。また、国際的な潮流と整合性を保つため、諸外国の同様の基準や制度についても参考にして改訂を行いました。

本書は、このシステム監査基準の改訂を受けて発行するものであり、新基準の各項目を分かり易く具体的に解説したものであります。本書を参考にして、内部監査及び外部の第三者による専門的な監査が実施され、IT ガバナンスの実現により企業・組織の価値が向上していくことを期待しています。

2005 年 1 月

経済産業省商務情報政策局
情報セキュリティ政策室

目　次

システム監査基準

策定　昭和60年１月
改訂　平成８年１月30日
改訂　平成16年10月８日

Ⅰ．前文

今日、組織体の情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。さらに、それぞれの情報システムがネットワーク化されることにより、社会の重要なインフラストラクチャとなってきている。一方、情報システムはますます多様化、複雑化し、それに伴い様々なリスクが顕在化してきている。また、情報システムに係わる利害関係者も組織体内にとどまらず、社会へと広がっている。従って、このような情報システムにまつわるリスクを適切にコントロールすることが組織体における重要な経営課題となっている。システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。また、システム監査の実施は、組織体のITガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は、以下の通りである。

・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

システム監査基準は、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。本監査基準は、監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」、監査計画の立案及び監査手続の適用方法を中心に監査実施上に枠組みを規定する「実施基準」、監査報告に係わる留意事項と監査報告書の記載方式を規定する「報告基準」からなっている。

システム監査基準は、組織体の内部監査部門等が実施するシステム監査だけでなく、組織体の外部者に監査を依頼するシステム監査においても利用できる。さらに、本基準は、情報システムに保証を付与することを目的とした監査であっても、情報システムの改善のための助言を行うことを目的とした監査であっても利用できる。

システム監査の実施に当たっては、組織体における情報システムにまつわるリスクに対するコントロールの適否を判断するための尺度が必要である。システム監査は、本監査基準の姉妹編であるシステム管理基準を監査上の判断の尺度として用い、監査対象がシステム管理基準に準拠しているかどうかという視点で行われることを原則とする。しかし、システム管理基準に基づく監査に限らず、各種目的あるいは各種形態をもって実施されるシステム監査においても本監査基準を活用することができる。

システム監査基準は、昭和60年（1985年）１月に策定されたもので、その後平成８年(1996年)１月に改訂され、今回は２度目の改訂である。今回の改訂は、昨年４月に創設された情報セキュリ

ティ監査基準との整合性を図り、従来の実施基準の主要部分を抜き出し、システム管理基準として独立させ、それぞれに大幅な加筆・修正を行ったものである。

Ⅱ．システム監査の目的

システム監査の目的は、組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスの実現に寄与することにある。

Ⅲ．一般基準

１．目的、権限と責任

システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と責任は、文書化された規程、または契約書等により明確に定められていなければならない。

２．独立性、客観性と職業倫理

2.1　外観上の独立性

システム監査人は、システム監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

2.2　精神上の独立性

システム監査人は、システム監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

2.3　職業倫理と誠実性

システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

３．専門能力

システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

４．業務上の義務

4.1　注意義務

システム監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

4.2　守秘義務

システム監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、又は、自らの利益

のために利用してはならない。

5．品質管理

システム監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。

Ⅳ．実施基準

1．監査計画の立案

システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について、適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。

2．監査の手順

システム監査は、監査計画に基づき、予備調査、本調査及び評価・結論の手順により実施しなければならない。

3．監査の実施

3.1　監査証拠の入手と評価

システム監査人は適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

3.2　監査調書の作成と保存

システム監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

4．監査業務の体制

システム監査人は、システム監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導（フォローアップ）までの監査業務の全体を管理しなければならない。

5．他の専門職の利用

システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の責任において行われなければならない。

6．情報セキュリティ監査

情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。

V．報告基準

1．監査報告書の提出と開示

システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

2．監査報告の根拠

システム監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

3．監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、改善勧告、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。

4．監査報告についての責任

システム監査人は、監査報告書の記載事項について、その責任を負わなければならない。

5．監査報告に基づく改善指導（フォローアップ）

システム監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。

システム監査基準の解説

解説についての留意点

解説の構成と内容

当解説書のうち、システム監査基準の〔Ⅰ．前文〕〔Ⅱ．システム監査の目的〕に関する解説は、各項目について「主旨」と「理論的根拠／実務的配慮」の２つの区分から構成されている。また、〔Ⅲ．一般基準〕〔Ⅳ．実施基準〕〔Ⅴ．報告基準〕に関しては、上記２つの区分のほかに「関連事項」が配されている。各区分の考え方は以下のとおりである。

(1) 主旨

当該項目の主旨を記載している。

(2) 理論的根拠／実務的配慮

当該項目を設定するに当たって、理論的根拠として考えられる事項や実務上配慮すべき点を記載している。

(3) 関連事項

「理論的根拠／実務的配慮」の補足説明や、例示、引用資料等を記載している。

なお、〔Ⅲ．一般基準〕〔Ⅳ．実施基準〕〔Ⅴ．報告基準〕の各基準に該当する解説ページの目次を次ページから記す。

基準項目と解説ページ（目次）

〔Ⅲ．一般基準〕

〔Ⅳ．実施基準〕

3．監査の実施	3.1　監査証拠の入手と評価 システム監査人は適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。	47
	3.2　監査調書の作成と保存 システム監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。	49
4．監査業務の体制	システム監査人は、システム監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導（フォローアップ）までの監査業務の全体を管理しなければならない。	50
5．他の専門職の利用	システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の責任において行われなければならない。	51
6．情報セキュリティ監査	情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。	52

〔V．報告基準〕

基準項目		解説ページ
1．監査報告書の提出と開示	システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。	55
2．監査報告の根拠	システム監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。	56
3．監査報告書の記載事項	監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、改善勧告、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。	57
4．監査報告についての責任	システム監査人は、監査報告書の記載事項について、その責任を負わなければならない。	67
5．監査報告に基づく改善指導（フォローアップ）	システム監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。	68

Ⅰ．前　　文

第１パラグラフ

今日、組織体の情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。さらに、それぞれの情報システムがネットワーク化されることにより、社会の重要なインフラストラクチャとなってきている。一方、情報システムはますます多様化、複雑化し、それに伴い様々なリスクが顕在化してきている。また、情報システムに係わる利害関係者も組織体内にとどまらず、社会へと広がっている。従って、このような情報システムにまつわるリスクを適切にコントロールすることが組織体における重要な経営課題となっている。システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。また、システム監査の実施は、組織体の IT ガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。

1 主　旨

システム監査は、情報システムが組織体にとっても社会にとってもインフラストラクチャとなっている今日、情報システムにまつわるリスクが適切にコントロールされているかどうかを評価するためにますます重要になってきている。これは、IT ガバナンスに寄与することであり、また、その結果を基に説明責任を果たすことができるものである。

2 理論的根拠／実務的配慮

今日、情報システムは経営の重要な要素であり、インフラストラクチャとなっている。しかも、情報システムは、ネットワーク化によって相互接続が進展した結果、社会のインフラストラクチャとなっている。

このような客観情勢を背景として、情報システムをめぐり各種のリスクが顕在化している。このリスクにいかに対処していくかが重要な経営課題である。しかも、情報システムの拡大によって、リスクが顕在化した場合の影響を与える範囲が従来に比較して各段に広がっている。このため、リスクを適切にコントロールすることは、今日の経営における重要な要素となっている。例えば、リスクの顕在化による情報システムの停止は、リスクを適切にコントロールできなかったことの証明であり、顧客をはじめとする利害関係者に影響を与え信用を失墜させ、結果、組織体にとっては損失をもたらすことになる。

システム監査は、組織体にとって情報システムにまつわるリスクのコントロールが適切に整備・運用されていることを証明する手段として活用できる機能を果たす。このことは、IT ガバナンスに寄与するとともに、システム監査の結果を開示することによって、情報システムの管理状況について利害関係者に対する説明責任を果たすことができるものである。

第２パラグラフ

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は、以下の通りである。

・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

1 主　旨

組織体が情報リスクをコントロールしなければならないのは、情報システムが経営全般にわたって重要な役割を果たしているからであり、システム監査としてもそこが重要な監査要点又は着眼点になる。ここでは、情報リスクを適切に整備・運用しなければならない目的を、ポリシーの観点、運用の観点、情報の信頼性を保つ観点及びコンプライアンスの観点の４つの面から要約している。これらは、経営全般にわたる重要事項である。

2 理論的根拠／実務的配慮

今日、すべての業務が情報システムによって動いているといってよい。したがって、情報及び情報システムを中心とした経営が行われていると言い換えることができる。このような経営環境においては、システム監査では経営方針や戦略目標の実現に情報システムがどのように貢献しているかを監査要点又は着眼点にしなければならない。

情報システムが組織体の目的を実現するためには、情報システム自体が安全、有効かつ効率的に機能しなければならない。特に、情報システムの安全性が損なわれた場合、必ず損失が発生すると考えておくべきであろう。

報告する情報、特に外部に対する情報開示については、情報が正確であることを保証しなければならない。このためには、情報システムの信頼性を確保することが求められる。このような情報及び情報システムを監査して、その信頼性を保証できるシステム監査を実施しなければならない。

情報システムで処理しているのは業務である。その業務は、関連法規、契約又は内部規程等に準拠して実施されなければならない。業務が正確に処理されていることを保証するためには、法令等のルールを遵守しているかを監査しなければならない。

第３パラグラフ

システム監査基準は、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。本監査基準は、監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」、監査計画の立案及び監査手続の適用方法を中心に監査実施上に枠組みを規定する「実施基準」、監査報告に係わる留意事項と監査報告書の記載方式を規定する「報告基準」からなっている。

1 主　旨

システム監査基準は、システム監査人の行為規範であり、「一般基準」、「実施基準」、「報告基準」で構成されている。

2 理論的根拠／実務的配慮

システム監査は、情報システムのライフサイクルを通じて総合的に監査するものであり、そのための監査人の行為規範を規定したものがシステム監査基準である。

一般基準は、監査人の適格性や監査業務を実施する上での遵守事項等、「目的、権限と責任」、「独立性、客観性と職業倫理」、「専門能力」、「業務上の義務」、「品質管理」について規定している。

実施基準は、実際に監査を実施するための手順、手続等、「監査計画の立案」、「監査の手順」、「監査の実施」、「監査業務の体制」、「他の専門職の利用」、「情報セキュリティ監査」について規定している。

報告基準は、報告書の作成の仕方等、「監査報告書の提出と開示」、「監査報告の根拠」、「監査報告書の記載事項」、「監査報告書についての責任」、「監査報告書に基づく改善指導（フォローアップ）」について規定している。

第４パラグラフ

システム監査基準は、組織体の内部監査部門等が実施するシステム監査だけでなく、組織体の外部者に監査を依頼するシステム監査においても利用できる。さらに、本基準は、情報システムに保証を付与することを目的とした監査であっても、情報システムの改善のための助言を行うことを目的とした監査であっても利用できる。

1 主　　旨

このシステム監査基準は、内部監査であっても外部監査であっても利用できるように作成されている。内容的には、助言を与える目的のための監査でも保証を与える目的のための監査でも利用できる基準である。

2 理論的根拠／実務的配慮

システム監査基準は、従来、内部監査としてトップマネジメントにサービスすることを目的とした監査を実施するための基準として位置付けられてきた。今回の基準改訂では、この位置付けに大きな変化がある。それは、「情報システムに保証を与えることを目的とした監査」という表現に如実に現れている。新システム監査基準においては、従来の助言型監査に加えて保証型監査を導入している。

保証型監査は、「いつ、誰が、どのような判断尺度で、何を、どのように評価した」といった点が明確にされた監査実施結果でなければ説得力はない。この点について利害関係者に信頼してもらえなければ、監査結果を開示したとしても説明責任を果たしたことにはならない。

第５パラグラフ

システム監査の実施に当たっては、組織体における情報システムにまつわるリスクに対するコントロールの適否を判断するための尺度が必要である。システム監査は、本監査基準の姉妹編であるシステム管理基準を監査上の判断の尺度として用い、監査対象がシステム管理基準に準拠しているかどうかという視点で行われることを原則とする。しかし、システム管理基準に基づく監査に限らず、各種目的あるいは各種形態をもって実施されるシステム監査においても本監査基準を活用することができる。

1 主　旨

システム監査基準に基づいてシステム監査を実施する場合、判断の尺度を何に求めるかが問題となる。このため、準拠すべき基準としてシステム管理基準を設けている。しかし、すべてのシステム監査に判断基準として常にシステム管理基準を用いなければならないということではない。

2 理論的根拠／実務的配慮

システム監査基準の姉妹編としてシステム管理基準を策定しているが、これは、情報処理の現場で情報システムの管理のために活用するものである。また、システム管理基準は、システム監査の際にも判断基準として活用するものである。すなわち、情報システムの管理が、システム管理基準に準拠して行われているかどうかを確認するための尺度となる基準である。

しかし、すべてのシステム監査が、このシステム管理基準に基づいて行われなければならないということではない。システム管理基準は、基本的には情報システムのライフサイクルを対象として、情報システムの全体を総合的に管理するための１つの基準として策定したものである。

監査対象が、常に情報システムのすべてを対象とするとは限らないし、また、すべての情報システムにこのシステム管理基準がそのまま当てはまるとも考えられない。したがって、システム監査の都度、監査テーマや監査対象について、システム管理基準及びその他の基準等を勘案して、当該監査用に基準を策定することが望ましいといえる。

第６パラグラフ

システム監査基準は、昭和 60 年（1985 年）１月に策定されたもので、その後平成８年（1996 年）１月に改訂され、今回は２度目の改訂である。今回の改訂は、昨年４月に創設された情報セキュリティ監査基準との整合性を図り、従来の実施基準の主要部分を抜き出し、システム管理基準として独立させ、それぞれに大幅な加筆･修正を行ったものである。

1 主　　旨

システム監査基準は、今回が２度目の改訂であるが、今回は従来の基準の単なる延長線上で改訂したものではない。従来の基準と基本的に異なる点は、第１に、平成 15 年に告示された情報セキュリティ監査基準との整合性をとっていること、第２に、従来の実施基準を切り離し、新たにシステム管理基準を策定して二本立てとしたことである。

2 理論的根拠／実務的配慮

システム監査基準は、わが国でシステム監査が普及していく過程で、システム監査を実施したいがその方法がわからないという民間の声にこたえて、経済産業省が昭和 60 年にガイドラインとして策定したものである。

当初のシステム監査基準は、内部監査に限定され、組織体内部のシステム監査人（従業員）が最高経営者へサービスする業務として実施するものと位置付けられていた。

今回の改訂では、保証型監査を導入し、利害関係者への監査結果の報告も視野に入れている点が特徴であり、システム監査の社会的役割を強化した内容である。

システム監査と情報セキュリティ監査の違いは次のとおりである。システム監査は、情報システムのライフサイクルを通じて実施する総合的な監査であるのに対して、情報セキュリティ監査は、情報セキュリティに特化した監査である。

システム管理基準は、基本的には情報処理の現場で利用する基準として策定しているが、システム監査の際にも評価尺度として使用するものである。

Ⅱ．システム監査の目的

システム監査の目的は、組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスの実現に寄与することにある。

1 主　旨

システム監査の目的を示したものである。

2 理論的根拠／実務的配慮

システム監査は、以下の特徴をもつことを明確に示した。

(1) 情報システムにまつわるリスクに対するコントロールについて監査を実施すること。

(2) コントロールがリスクアセスメントに基づいて適切に整備・運用されているかを検証又は評価すること。

(3) 監査には、保証型又は助言型の監査があること。

(4) 最終的には IT ガバナンスの実現に寄与するものであること。

Ⅲ. 一 般 基 準

1．目的、権限と責任
2．独立性、客観性と職業倫理
3．専門能力
4．業務上の義務
5．品質管理

1．目的、権限と責任

システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と責任は、文書化された規程、または契約書等により明確に定められていなければならない。

1 主　旨

システム監査業務は組織の正式な活動であるため、目的及び対象範囲、並びにシステム監査人の権限と責任は、文書化された規程（例えば、内部監査規程、職務分掌規程、職務権限規程等）によって明確に定められている必要がある。また、外部の監査人が実施する場合は、それらは契約書や覚書等で明確に定められている必要がある。

2 理論的根拠／実務的配慮

内部監査の一環としてシステム監査を実施する場合は、内部監査規程の目的を記した条文にシステム監査の目的を含めることとなる。また、システム監査業務の範囲も、内部監査規程等に記載するとよい。システム監査人の権限と責任は、内部監査規程に定められる場合もあれば、職務分掌規程、職務権限規程に他の組織と同列に決められる場合もあるだろう。

組織の外部者がシステム監査を実施する場合は、契約書や覚書によって、その目的や対象範囲を明確にする必要がある。特に、保証型監査なのか、助言型監査なのかによって、実施する監査手続が異なることになるので、どちらであるかを明確にしておくことが重要である。

3 関連事項

・システム監査人の権限についての留意点

システム監査人の権限は、法定監査における会計監査人と異なり、法律によって当然に与えられた権限があるわけではなく、内部規定又は契約によって定められる。したがって、内部規定又は契約によって与えられた権限を越えたシステム監査を実施することはできない。例えば、子会社の内部監査の一環としてシステム監査を親会社のシステム監査人が実施する場合、親会社の内部監査規程等に子会社に対して監査を行う権限が与えられていなければ、承認を得ずに子会社のシステム監査を実施することはできない。親会社のシステム監査人によって、子会社のシステム監査を実施することが常態である場合は、あらかじめ親会社の内部監査規程等に子会社の監査を実施する権限を含めておくことが望ましい。

2．独立性、客観性と職業倫理

2．1　外観上の独立性

システム監査人は、システム監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

1 主　旨

システム監査人の独立性は、システム監査の信頼性の基礎である。第三者から見て、外観上の独立性が保たれていなければシステム監査の信頼性が担保できないため、外観上の独立性について定めたものである。

2 理論的根拠／実務的配慮

システム監査人の独立性は、監査報告書に対する信頼の基礎をなす。つまり、システム監査人の独立性はシステム監査の本質、土台、存在意義となる。システム監査人の監査結果が客観的なものであることに対し、監査報告書の結果を利用する利害関係者の信頼を得るためには、被監査主体との間に独立性が要求される。独立性は「精神上の独立性」と「外観上の独立性」に分けられる。

精神上の独立性とは、「個人が誠実性をもって行動し、客観性及び専門家としての懐疑的態度を行使できるようにしながら、専門家としての判断を損なうような影響を受けずに、意見の表明ができる精神の状態」と言い表すことができる。一方、外観上の独立性とは、「合理的かつ事情に精通し、かつ、関連するすべての情報をもつ第三者が、情報セキュリティ監査主体の構成員の誠実性、客観性又は専門家としての懐疑的態度は容認できないほど損なわれていると結論を下すほど重大な事実及び状況を回避していること」と言い表すことができる。

独立性の本質は精神上の独立性であるが、外観上の独立性が損なわれると、精神上の独立性が損なわれているとの嫌疑がもたれるため、外観上の独立性を維持することが重要である。また、精神上の独立性が保たれているかについては、第三者がうかがい知ることができないため、外部の第三者にとって、外観上の独立性が維持されているかどうかは重要な問題となる。

外観上の独立性を検討する場合の視点は幾つか考えられる。例えば、組織的に独立しているか、過去に自らが行った業務を自己レビューしていないか、システム監査人と被監査主体の責任者が親族関係にないか、等である。また、許容される独立性の程度については、システム監査の目的によって異なる。保証型監査を実施する場合は、厳密な外観上の独立性が要求されることになり、内部監査の場合、それほどの厳密性は要求されないだろう。しかし、一般的に内部監査であっても一定の独立性の保持は必要である。

内部監査として実施するシステム監査の場合は、システム監査を実施する主体である部門（例えば、内部監査部門）は経営トップ（例えば、社長）の直轄部門であるべきである。特定の部門の配下としてシステム監査部門が存在すれば、その部門のシステム監査の独立性が担保されないばかり

か、他の部門を監査する場合であっても、例えば、システム監査部門の長が課長級であるのに対し、被監査組織の長が事業部長級であれば、精神上の独立性が侵害されていると外観上判断されることになるだろう。したがって、システム監査を行う部門の部門長（例えば、内部監査部門長）は経営トップの直轄であるべきである。

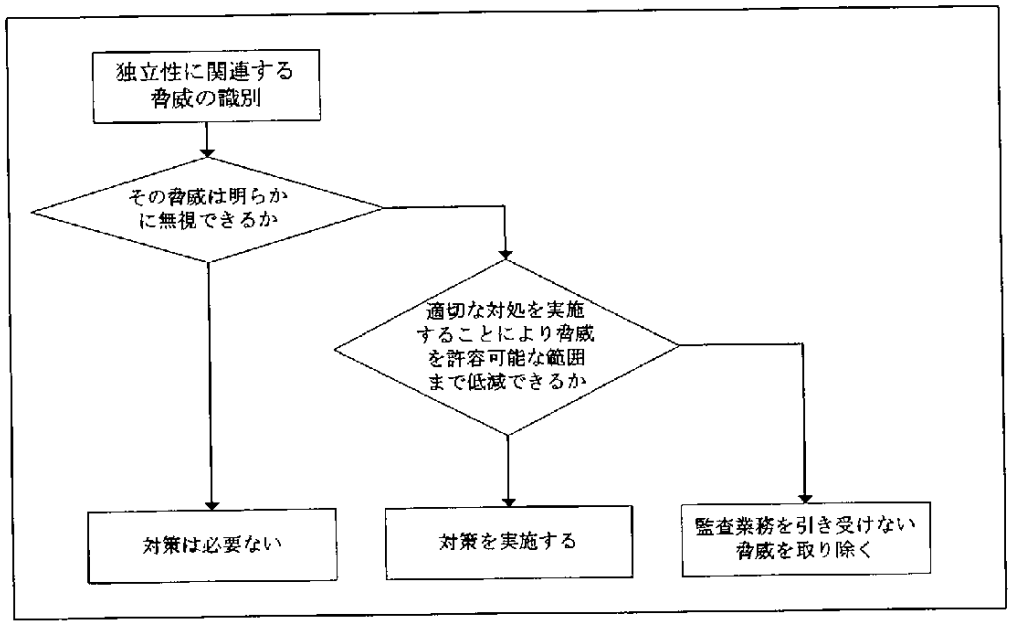
また、システム監査人がかつて在籍した部門を監査する場合は、通常１年以上のクーリングオフ期間を設けることが必要である。

外部主体による保証型監査を実施する場合は、内部監査の場合に加え、被監査主体との経済的な利害関係がないか等、よく検討する必要がある。

3 関連事項

・国際会計士連盟による外観上の独立性のフレームワーク

国際会計士連盟は、外観上の独立性を検討する際のフレームワークを公表している。会計士連盟のフレームワークでは、独立性について以下のステップで考える。



(1) Step 1 脅威の識別

監査主体の独立性に対する脅威が存在するかどうかの識別を行う。

脅威の例：

① システム監査人の所属する会社の株式を被監査主体が所有している場合、株主の権利を行使して、システム監査人の判断をゆがめるかもしれないという外観上の独立性に対する脅威が存在する。

② システム監査チームの責任者が、被監査主体の責任者の元部下である場合、元上司に遠慮して、システム監査人の判断をゆがめてしまうかもしれないという外観上の独立性に対する脅威が存在する。

(2) Step 2　脅威の影響度の検討

識別された独立性に関連する脅威が明らかに無視できるかどうかを検討する。例えば、システム監査人の親戚が、同一法人内の監査対象部門以外で、監査対象との関連がほとんどない業務を行っている場合は、独立性に関連する脅威が無視できるレベルであると通常は判断される。

(3) Step 3　対策の検討

脅威が明らかに無視できると判断できない場合は、適切な対策を実施する、監査業務を引き受けない、又は脅威自体を取り除くことになる。独立性の脅威を取り除く対策は、以下の３つに分類することができる。

	脅威を取り除く対策	対策の例示
1	法令や業界団体の規則等による対策	・独立性を規制する法令の整備 ・外部団体による独立性についてのレビュー ・業界団体による独立性についての規則や規範の整備等
2	被監査主体内で行われる対策	・被監査主体の監査委員、監査役等による承認 ・(内部監査の場合) 被監査主体の経営者、内部監査人等による承認等
3	監査主体内で行われる対策	・監査主体自身による独立性についての方針、規定、手続 ・監査主体内での独立性についてのレビュー等

2．独立性、客観性と職業倫理

2．2　精神上の独立性

システム監査人は、システム監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

1 主　旨

システム監査に本質的に求められる精神上の独立性について定めたものである。

2 理論的根拠／実務的配慮

システム監査人に本質的に求められるのは精神上の独立性である。システム監査人は、被監査主体に影響されることなく、自らが実施した監査手続に基づいて得た監査証拠によって自らの信念に従い監査意見を形成する。また、システム監査人は自らの過去の経験や思い込み等による偏向した考えに基づく監査判断を行ってはならない。システム監査人は、常に公正かつ客観的に監査判断を行うことが求められる。

精神上の独立性はシステム監査人の心の問題であり、本当のところは外からうかがい知ることができない。しかしながら、少なくとも外観上の独立性が担保されていない場合は、精神上の独立性が侵されている可能性が高いと想定できる。したがって、本質的な問題として精神上の独立性は重要であるが、第三者からの疑念を抱かれないようにするために外観上の独立性も重要となる。精神上の独立性と外観上の独立性は、それぞれが相まって信頼されるシステム監査業務の遂行に寄与することになる。

3 関連事項

独立性に関連する脅威には、次のようなものがある。

	脅威の種類	脅威の説明
1	自己利益	システム監査人が自らの利益を図る、又は損失を防ごうとすることによって生じる脅威
2	自己レビュー	システム監査人が過去において意思決定等に関与した監査対象を監査することから生じる脅威
3	擁護	システム監査人が監査目的に関連する訴訟等に関与することから生じる脅威
4	馴合い	システム監査人と監査対象との間に親密な関係が生じることによって生じる脅威
5	威嚇	監査人の交代等の条件を提示する等、システム監査人に対する監査対象からの威嚇によって生じる脅威

２．独立性、客観性と職業倫理

２．３　職業倫理と誠実性

システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

1 主　旨

職業倫理又は職務上の倫理に従い、誠実に業務を実施することを定めたものである。

2 理論的根拠／実務的配慮

監査報告書の信頼性を担保するためには、システム監査人が高い品位とともに高度な人格、すなわち、倫理観、誠実性、責任感、正義感等を有することが必要である。

職業倫理又は職務上の倫理と誠実性については、システム監査を業としない組織内部のシステム監査人にも求められるが、システム監査を業とする者にはとりわけ重要となる。システム監査を業とする者に求められるであろう職業倫理については、懇請の禁止（業務の委嘱を懇請することは、ひいては監査人の独立性を脅かすことになる）、成功報酬の禁止（問題点の多寡によって報酬が決まるとすると、監査人は監査報告書の利用者の利益ではなく、自らの利益のために業務を行うことになる）、信用失墜行為の禁止（他のシステム監査人を誹謗し、名誉を傷つける行為をすることによって、システム監査人全体の信用が失われることになる）等が考えられる。

3 関連事項

以下の団体において、倫理規定、倫理綱領等が定められている。

(1) 特定非営利活動法人　日本システム監査人協会（SAAJ）
http://www.saaj.or.jp/gaiyo/rinri.html

(2) 情報システムコントロール協会（ISACA）
http://www.isaca-osaka.org/isaca004.htm　（日本語）
http://www.isaca.org　（英語）

(3) 内部監査人協会（IIA）
http://www.iiajapan.com/ethics.htm　（日本語）
http://www.theiia.org/iia/index.cfm?doc_id=604　（英語）

(4) International Register of Certificated Auditors（IRCA）
http://www.irca.org/　（英語）

3．専門能力

システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

1 主　旨

システム監査人の能力条件を定めたものである。

2 理論的根拠／実務的配慮

IT の進歩は日進月歩である。このような変化の激しい環境において、最新の技術動向を理解し、監査を実践していく能力がシステム監査人になければシステム監査人の信頼性を担保することはできない。システム監査人は教育等を通じ、自ら研鑽を積むとともに、実務経験を通じて、専門職として期待される知識及び技能を不断の努力によって保持する必要がある。システム監査人が専門職として保持することが望まれる知識及び技能には、例えば以下のような項目がある。

(1) 監査の基礎的理論に対する知識
(2) 監査目的にあった監査手続を監査対象に適用し、必要となる監査証拠を入手する技能
(3) 実施した監査手続を監査調書としてまとめ上げる技能
(4) 監査証拠から監査意見を形成する技能
(5) 監査意見を監査報告書にまとめ上げる技能
(6) 監査計画を策定し、監査業務を管理する技能
(7) IT に関する知識
(8) 内部統制に関する知識
(9) その他、組織運営に関する一般的な知識

3 関連事項

以下の団体において、監査人のシステム継続的教育が定められている。

(1) 特定非営利活動法人　日本システム監査人協会（SAAJ）
http://www.saaj.or.jp/gaiyo/rinri.html
(2) 情報システムコントロール協会（ISACA）
http://www.isaca-osaka.org/isaca004.htm　（日本語）
http://www.isaca.org　（英語）
(3) 内部監査人協会（IIA）
http://www.iiajapan.com/ethics.htm　（日本語）
http://www.theiia.org/iia/index.cfm?doc_id=604　（英語）
(4) International Register of Certificated Auditors（IRCA）
http://www.irca.org/　（英語）

4．業務上の義務

4．1　注意義務

システム監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

1 主　旨

システム監査人が、専門職として相当な注意をもって業務を実施する旨を定めたものである。

2 理論的根拠／実務的配慮

システム監査人はシステム監査を行う専門職であり、専門職として利害関係者から期待される注意義務を果たして業務を行うことが求められる。正当な注意を怠るとシステム監査人は法的な責任を問われる可能性があるばかりでなく、システム監査全体の信用を失墜させることにもつながる。このため、システム監査人は、システム監査業務全体について正当な注意を払う必要がある。

システム監査人に求められる正当な注意義務は、民法（第644条）に規定される善良なる管理者としての注意義務（善管注意義務）に相当するものと考えられる。つまり、システム監査業務を行う地位にあるものとして当然に要求される注意義務であり、システム監査人がその技能の最善を尽くして実行しなければならないことに留意しなければならない。システム監査人は専門的な能力があることが想定されるため、システム監査人に求められる善管注意義務は一般のそれよりも高いものとなる。

システム監査人の監査によって利害関係者に何らかの損害が発生し、損害賠償を請求された場合は、正当な注意を払って業務を実施したかどうかが問われることになる。

システム監査人が正当な注意を払って業務を実施したかどうかは、監査調書によって明らかにされることになる。そのため、監査調書に記載する内容等は十分吟味しなければならない。

3 関連事項

監査調書については、「Ⅳ．実施基準　3.監査の実施　3.2　監査調書の作成と保存」を参照。

４．業務上の義務

４．２　守秘義務

システム監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、又は、自らの利益のために利用してはならない。

1 主　旨

業務上知り得た秘密を、例えば法律に基づいて開示をしなければならない場合、公益を優先する必要がある場合等の正当な理由なしに、第三者に開示することを禁止したものである。また、システム監査人は、監査の過程で知り得た秘密を自らの利益のために利用することを禁止したものである。

2 理論的根拠／実務的配慮

システム監査人が、業務上知り得た秘密を正当な理由がないのに、第三者に開示したり、システム監査人自らの利益のために利用することは、個々の監査業務においてシステム監査人に対し、被監査主体が資料の提出を拒んだりし、監査業務が成立しなくなることも考えられる。また、ひいてはシステム監査自体に対する信用の失墜にもつながる。

3 関連事項

守秘義務については、監査基準ではなく倫理規定や倫理綱領に記載すべきであるという意見もあるが、この守秘義務が重要であること、また、システム監査を実施する者が必ずしも職業団体に加入していないことを鑑み、あえてシステム監査基準に記載している。

5. 品質管理

システム監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。

1 主　旨

システム監査の有効性を担保し、監査結果の適正性を確保するために、適切な品質管理を行わなければならない旨を定めたものである。

2 理論的根拠／実務的配慮

システム監査業務の品質管理の目的は、システム監査業務の有効性を評価すること、システム監査が当該基準及びシステム監査人が所属する組織の倫理綱領等、社内規程や契約を遵守していることを保証し、システム監査人の業務の改善を促進することにある。

システム監査業務の品質管理は、システム監査業務実施前、業務実施中、業務実施後の３段階で実施するのがよい。また、品質管理のためには、監査業務の品質管理と、システム監査人の品質管理の２つの面を考慮する必要がある。システム監査人の品質管理は、一定の能力を認める技能認定等の実施、監査業務中における OJT(On-the-Job Training)、監査業務後の人事評価とその結果のフィードバック等がある。監査業務の品質管理としては、システム監査引受け前のシステム監査主体による審査、監査業務実施中の上席者や監査チーム外の品質管理担当者による監査調書のレビュー、監査実施後の品質管理専門チームによる業務レビュー（審理）等がある。

3 関連事項

システム監査人の品質管理については、公認会計士、情報セキュリティ監査をはじめ、JIS のマネジメントシステム規格（JIS Q 9001 品質マネジメントシステム規格、JIS Q 14001 環境マネジメントシステム規格）に対する適合性監査についても、JIS Q 19011 品質及び／又は環境マネジメントシステム監査のための指針」に定められている。JIS Q 19011 では次のようにガイドしているので参考にする。

5.6 監査プログラムの監視及びレビュー

監査プログラムの目的が達成できているかを評価し、また改善の機会を特定するために、監査プログラムの実施を監視し、適切な間隔でレビューすることが望ましい。その結果はトップマネジメントに報告することが望ましい。

次のような特性を監視するために、パフォーマンス指標を用いることが望ましい。

－ 監査計画を実施するための監査チームの能力

－ 監査プログラム及びスケジュールとの整合性、及び

－ 監査依頼者、被監査者及び監査員からのフィードバック

この監査プログラムのレビューでは、例えば、次のようなことに配慮することが望ましい。

a．監視の結果、及びその傾向

b．手順との適合

c．利害関係者から新たに出てきたニーズ及び期待

d．監査プログラム記録

e．代わりの、又は新規の監査方法

f．類似した状況下での監査チーム間でのパフォーマンスの一貫性

監査プログラムのレビュー結果から、監査プログラムに関する是正及び予防処置、さらには改善につなげることができる。

Ⅳ. 実施基準

1．監査計画の立案
2．監査の手順
3．監査の実施
4．監査業務の体制
5．他の専門職の利用
6．情報セキュリティ監査

1．監査計画の立案

システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について、適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。

1 主　旨

システム監査の目的は、本監査基準の冒頭に「IT ガバナンスの実現に寄与することにある」と明記され、実施される個別のシステム監査の目的もそのことに集約される。したがってシステム監査の実施に当たっては、組織体の経営目的との適合性を明確にして監査の効果をあげ、かつ監査業務の効率化を図るための監査計画を立案することが必要となる。

2 理論的根拠／実務的配慮

監査計画は、基本計画と個別計画に分けて策定する。基本計画は本来年度計画であるので、別に中長期基本計画の策定が必要となる。ただし、実務上は当該年度を中心に次年度（以降）も含めた中期の基本計画として一本化することが望ましい。内部監査では、監査の継続性の観点から複数年度を対象に基本計画を策定することが多い。一方、外部監査の場合は、監査契約によって個別計画だけとなることが多いが、総合的かつ中長期的な視野に立つ監査契約に基づく基本計画の策定が求められるところである。

監査計画の策定に当たっては、組織体の中長期・年度の経営計画及び情報システム化計画と整合性のとれた基本計画をまず立案し、それに基づいた個別計画を具体化することになる。情報システムにまつわるリスクアセスメントに基づいて、監査対象の選定、重点監査テーマの選択を行い、監査範囲と監査手続を定め、それに対応した監査実施体制、監査スケジュールを決定した計画とする。

情報システムにまつわるリスクアセスメントは、被監査部門で実施されていることが前提である。つまり、情報システムリスクの識別・評価それに基づくコントロールの整備・運用の責任は、経営及び情報システム部門を含む被監査主体にあるからである。

システム監査人は、リスクアセスメントとこれに基づくコントロールの適切性を確認して、監査計画を立案、変更することになる。リスクアセスメントが被監査部門で実施されていない場合は、必要に応じてシステム監査人が実施したり、指導することになるが、それ自体が指摘・改善勧告の対象となる問題である。

監査計画は、被監査部門の組織体の長の承認を得て発効するものであるが、監査実施過程において新しい事実を認識する、被監査主体の環境に変化があった等、監査目的の達成が阻害されるおそれが生じれば、監査手続の変更等臨機応変に修正できるように弾力的な運用が求められる点に留意する。

個別計画に基づいて実施した予備調査の結果をふまえて、「監査手続書」（監査実施計画）（「Ⅳ. 実施基準　3. 監査の実施　3.1　監査証拠の入手と評価」を参照）を作成し、本調査に備える。

以下基本計画、個別計画に分けてその記載項目について述べる。

① 基本計画

基本計画には、例えば次の事項を含めること（括弧内は留意事項）。

a．当該年度に実施する監査対象（対象となる情報システム、及び情報システムに係る業務等を明確にし、かつその範囲ー情報システムのライフサイクルプロセス、情報処理の外部委託等を明確にする）

b．重点監査テーマ（監査目的、リスクの程度、監査の着眼点等、特に重視するテーマを明確にする）

c．実施体制（監査業務の管理体制、監査担当者及び外部委託の場合の監督や監査の実施形態を明確にする）

d．スケジュール（監査対象別に日程ー開始日、終了日を明確にする）。

e．経費予算・その他（他の専門職の利用を予定する等監査に必要な経費を明確にする）

② 個別計画

個別計画には、例えば次の事項を含めること（括弧内は留意事項）

a．監査対象（基本計画に記載された対象から選ぶのが一般的であるが、緊急に変更する場合もある）

b．監査目的（監査の実施によって達成しようとする事項又は状態が監査の目的であるが、評価尺度が明確であることが必要）

c．監査範囲及び監査手続（監査範囲は監査手続を適用する範囲を意味し、監査対象の全部か一部かが明確になるように記載する。監査手続は監査範囲に対応した監査の方法を具体的に記載する。監査項目は監査範囲の中から抽出された監査手続を適用する個々の対象である）

d．監査時期及び日程（開始日、終了日、作業期間等を記載する）

e．責任者及び業務分担（個別監査業務の責任者を定め、担当者の業務分担を明確にし、氏名を記載する）

f．報告時期（関係者の出席の便をみてあらかじめ監査報告日を定めておく）

g．監査コスト（基本計画の経費予算を前提に必要経費等を記載する）

h．その他（監査報告書の開示範囲と利用目的の制限、及び、監査実施時点における制約事項、特記事項等があれば記載する）

3 関連事項

(1) IT ガバナンスについて

IT ガバナンスとは「企業が競争優位性構築を目的に、IT（情報技術）戦略の策定・実行をコントロールし、あるべき方向に導く組織能力」（経済産業省）と定義される。組織の経営戦略と IT 戦略を整合させ、IT 投資を適切に管理し、IT 要員やその体制、IT に関するリスクのコントロール等のフレームワークを確立する「IT ガバナンス」が極めて重要である。

システム監査の目的は、前述の１．主旨で述べたように「IT ガバナンスの実現に寄与すること

にある」が、組織体の内部コントロールを実現する IT のあるべき姿の実現を指向する位置付けである。言い換えれば、経営の目的である情報システムを有効かつ効率的に活用する仕組みの構築を、システム監査が支援することとなるといえる。IT ガバナンスの実現に寄与するために、適切な監査計画を立案する意義は非常に大きい。

(2) リスクアセスメントについて

リスクアセスメントとは、「情報及び情報処理施設・設備に対する脅威、影響及びぜい弱性の評価、並びにそれらが起こる可能性の評価」(JIS X 5080:2002) と定義される。システム監査では、リスクアセスメントの際、この「情報及び情報処理施設・設備」を「情報システム」に範囲を限定して取り扱う。すなわち、リスクアセスメントは情報システムにまつわる「リスクの識別と評価」あるいは「リスクの分析と評価」ということになる。

被監査部門のリスクアセスメントの適性についてのシステム監査人の判断は、リスクアセスメント手法やリスクアセスメント結果の厳密性を検証するのではなく、リスクマッピング等の工夫によって、リスクアセスメントの結果がコントロールと関連付けられており、結果 IT ガバナンスを実現するものであることを確認することが重要となる。

リスク情報の収集と評価に当たっては、関連する事業・業務部門の関係者を一堂に会した組織横断的なワークショップ形式による自由な討議又は自己評価（リスク自己評価表）が効果的で効率的とされる。なお、リスク分析手法として、(財)日本情報処理開発協会の「JRMS（平成 16 年 1 月)」や GMITS（TR X 0036）等がある。JRMS は質問票による自己点検によって、情報システムのぜい弱性を把握する定性的な方法である。一方、GMITS は、リスクを情報資産の価値、脅威、ぜい弱性の観点から定量的に把握する方法であり、ベースラインアプローチ（すべてのシステムに対しベースラインレベルの保護の達成）や組合せアプローチ（重要システムを特定し、詳細リスク分析による保護が必要か、ベースライン保護で十分かに分類）が利用されることが多い。なお、JIS や TR で利用する場合のリスクマネジメントに関連する用語については、TR Q 0008 に定義されているので参考にするとよい。

(3) システム監査基本計画書の例

平成　　年　　月　　日

殿

監査部長　　印

平成　　年度システム監査基本計画書

下記の計画に基づき本年度のシステム監査を実施いたしたくご承認願います。

記

1．本年度監査の方針

2．監査対象と重点監査テーマ

(1) 対象情報システム又は業務　　重点監査テーマ

(2) 対象情報システム又は業務　　重点監査テーマ

(3) 以下同じ

3．実施体制及びスケジュール

(1) 監査項目、所管部門、監査責任者・担当者、予定時期

(2) 監査項目、所管部門、監査責任者・担当者、予定時期

(3) 以下同じ

4．経費予算、その他

以上

(4) システム監査個別計画書の例

システム監査個別計画書

作成日　平成　年　月　日
作成者

1．監査対象、所管部門

2．重点監査テーマ、監査目的

3．監査責任者・担当者

4．監査コスト

5．監査期間、報告時期

6．監査項目ごとに
　監査手続、監査着眼点、監査範囲、担当者名、実施日の記載

以上

2．監査の手順

システム監査は、監査計画に基づき、予備調査、本調査及び評価・結論の手順により実施しなければならない。

1 主　旨

システム監査は監査計画、具体的には個別計画に基づいて、予備調査を経て本調査を実施し、それによって評価及び結論を得るという段階の手順で実施する。予備調査は事前調査とも称せられ、本調査以降の監査手続の具体化が図れる等監査精度と監査効率の向上に効果がある。

2 理論的根拠／実務的配慮

(1) 予備調査

予備調査は、監査対象の実態を明確に把握するために行う。予備調査においては、質問書の利用やインタビューの実施、資料の収集と閲覧等の実施によって、監査対象の情報システムのリスクが適切に識別されているか、リスクアセスメントに基づいたコントロールが適切に整備されているか等、監査対象の実態を可能な限り把握するように努めることとなる。

(2) 本調査

本調査は、監査目的に則して監査対象を実際に調査、分析、検証し、コントロールが適切に運用されているかを検討する。予備調査で把握できた情報システムのリスクに対するコントロールの整備状況を、更に現地調査、インタビュー、書面査閲や調査、その他の監査技法を用いて確認し、整備されたコントロールが目的どおりに実際に機能しているかの運用状況を検証することとなる。

(3) 評価・結論

a．評価・結論は、予備調査、本調査の結果をふまえて、監査対象の実態を監査目的に照らし、適切か否かを判断することとなる。

b．システム監査人は、評価・結論について、その正確性を期するために、被監査部門と意見交換をして確認することが必要である。

3 関連事項

IT 技術の革新、特にネットワーク化の進展によって、情報システムの形態、その開発・管理手法も大きく変化している。そのような監査対象の実態を、まず把握できる予備調査の重要性は高まっている。

また、個別計画に基づいて予備調査を実施し、本調査での監査手続を更に詳細にすることが可能となり、変貌する監査対象に対する効率的、効果的な監査が実現できる。

3．監査の実施

3．1　監査証拠の入手と評価

システム監査人は適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

1 主　旨

システム監査人は情報システムにまつわるリスクに対するコントロールの整備・運用状況を検証・評価し、保証又は助言を行う責任を有する。したがって、システム監査人は、適切かつ慎重に監査手続を適用して監査を行い、保証又は助言についての自らの監査意見を形成するに十分、かつ、適切な監査証拠を入手し、評価する必要がある。

2 理論的根拠／実務的配慮

(1) 監査手続

監査手続とは、予備調査及び本調査の際の調査手段として、例えば、資料（文書）の閲覧・収集、質問書・調査票の利用、現地調査、インタビュー、監査ツールの利用等各種の監査技法を選択適用する方法あるいは過程をいう。別の言い方をすれば、システム監査人が監査項目について合理的な評価・結論を得るための十分な証拠の収集を目的に、監査技法を選択し適用する手順ともいえる。実務上、予備調査の結果をふまえて、個別計画を更に詳細にした監査手続書が作成される。

監査手続書は、次のように監査手続の詳細計画（監査実施計画）として立案する。

- 監査手続の実施時期
- 監査手続の実施場所
- 監査手続の実施担当者及びその割当
- 実施すべき監査手続の概要（必要に応じて、監査要点、実施すべき監査手続の種類、監査手続実施の時期、及び試査の範囲を含む）
- 監査手続の進捗管理手段又は体制

(2) 監査証拠

監査証拠とは、システム監査人の監査意見を立証するために必要な事実のことをいう。監査証拠は、前述のように監査手続を適用して入手するが、次の４つに大別される。

a．物理的証拠（システム監査人自らが検証した現物）

b．文書的証拠（システム監査人自らが検証した文書的、電磁的記録物）

c．口頭的証拠（システム監査人が監査証拠となり得ると判断した証言、説明等、口頭での陳述。ただし第三者に証明できるように文書化されたもの）

d．状況的証拠（システム監査人自らが観察した状況。例えば、警備員が第三者の許可のない入室を防止するために入館者の社員章の確認を行っていることを観察する場

合等)

(3) 監査証拠の評価

システム監査人が入手した資料等は、すべてそのまま監査証拠となるわけではないので、監査証拠として採用するか否か、それが有する信憑性及び証明力の程度を慎重に判断し、その結果を明らかにする必要がある。

システム監査人が入手した監査証拠の評価に当たっては、リスクアセスメントの結果との関連づけが考慮されることが望ましい。被監査部門が採用しているコントロールの適否の判断は、リスクに応じたものでなければならない。リスクが相対的に高い場合にはより強力なコントロールが必要とされ、逆にリスクが低い場合にはそれに対応したコントロールとなる。

なお、監査証拠については、被監査部門とその取扱いについて定めておく必要がある。これは、保証型監査の場合でも、システム監査人の監査意見形成に関する証拠となるものであり、後日保証意見をめぐって論争が起きたときに、システム監査人にとって重要な証拠となるからである。

3 関連事項

監査手続は、次のような3つの側面をもっている。

a．情報システムに必要なコントロールを点検・評価する過程

b．監査意見を立証するために必要な監査証拠を入手する過程

c．システム監査技法を選択し適用する過程

これらそれぞれの過程で、前述した関連書類の閲覧及び査閲、担当者へのヒアリング、現場への往査及び視察、システムテストへの立会い、テストデータによる検証及び跡付け、ぜい弱性スキャン、システム侵入テスト等の監査手続の実施によって監査証拠が入手される。

3．監査の実施

3．2　監査調書の作成と保存

システム監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

1 主　旨

システム監査人は、システム監査の全過程で実施した監査手続の結果と監査手続に関連して入手した資料等は、監査の結論に至った経過が分かるように秩序整然と監査調書として作成し、情報漏えいや紛失等を考慮し、適切に保管する必要がある。

2 理論的根拠／実務的配慮

(1) 監査調書

監査調書とは、システム監査人が行った監査業務の実施記録であり、監査意見表明の根拠となるべき監査証拠、その他関連資料等をまとめたものをいう。システム監査人自身が直接に入手した資料やテスト結果だけでなく、被監査部門から提出された資料等を含み、場合によっては組織体外部の第三者から入手した資料等を含むことがある。

監査調書は、主として監査意見の根拠とするために作成されるが、それ以外にも次回以降のシステム監査を合理的に実施するための資料として、また監査の品質管理の手段としても役立つ。さらには、システム監査人が正当な注意を払って監査業務を遂行したことの証拠となることがある。

(2) 監査調書の作成上の注意

監査調書は様々な目的に役立つことから、正確かつ漏れなく必要な事項を含めて監査調書を作成しなければならず、適当な参照符号等を整備してシステム監査人が監査の結論に至った経過が秩序整然と分かるように工夫しなければならない。

(3) 監査調書の保存

監査調書は、システム監査終了後も相当の期間、整理保存しておく必要がある。監査調書には被監査部門の機密事項が含まれていることから、保管場所や保管責任者の特定等、監査調書の保管には慎重な注意が求められる。外部のシステム監査人に保証型監査を依頼した場合においては、監査調書は、システム監査人の手許に残ることに留意すること。

3 関連事項

監査報告書に添付して監査調書の提出を求める監査業務委託契約を定めている事例がある。

4．監査業務の体制

システム監査人は、システム監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導（フォローアップ）までの監査業務の全体を管理しなければならない。

1 主　旨

システム監査人は、監査計画の立案、監査手続の実施、監査証拠の入手と評価、監査報告書の作成、監査報告に基づくフォローアップからなる一連の監査業務の遂行において、監査の体制を整え監査業務を効率的に実施し、かつ重要な問題点の見落し等、監査業務上の瑕疵が生じないよう、監査業務の全体を管理し、監査業務の品質を保証する必要がある。

2 理論的根拠／実務的配慮

(1) 監査業務の管理

監査業務は、少ないコストで、最大限の効果が期待できるように実施されるべきであるが、そのためには監査業務の進捗と品質の観点から監査業務の全体を適時に管理することが最も重要な要件となる。監査業務の進捗管理は、個別計画、監査手続書の実施状況のレビュー等を通じ、品質管理は、適切な監査計画の立案と遂行、監査マニュアルの整備、及び監査調書のレビュー等を通じてなされる。

(2) 体制の整備

システム監査が監査チームによって実施される場合には、適切な職務の分担に配慮し、監査担当者間における相互チェックが機能するような体制を整えることが望ましい(要員管理の重要性)。

監査計画の立案段階において想定しなかった状況変化（リスクの変化を含む)、すなわち経営方針の変更、事業プロセスの変更、情報システムの新規開発、突発事象の発生等にも柔軟に対応できるように、必要な措置等を講じておくことが望ましい。

3 関連事項

ここでいうシステム監査人の任務は、システム監査の責任者、監査部門の責任者の任務と理解されるが、同時にシステム監査人一般の心構えと解することが重要である。

なお、「改善指導（フォローアップ）までの監査業務の全体を管理しなければならない」とあるが、内部監査の場合には改善指導（フォローアップ）はシステム監査業務の一環となるが、外部監査の場合はシステム監査に関する業務委託契約の内容によって異なることになる。

5．他の専門職の利用

システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の責任において行われなければならない。

1 主　旨

システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持（「Ⅲ．一般基準　3.専門能力」）している。しかしながら、十分かつ適切な監査証拠を入手するために、システム監査人が必要と認めた場合には、他の専門職の支援を仰ぐことを考慮すべきである。なお当該専門職からのアドバイスや監査手続の補助又は代行があっても、最終的な監査の結果についての全責任はシステム監査人にあることに留意する必要がある。

2 理論的根拠／実務的配慮

(1) 監査業務の再委託

内部監査の場合は問題とならないが、内部監査の外部委託あるいは外部監査の場合のシステム監査人にとって、他の専門職への業務委託は再委託の形となり、監査業務委託契約で再委託を禁止されている場合には問題となる。このような場合は、当該再委託先に対しても自らと同条件を課するなどで、専門職の支援が可能となるよう努力すべきである。

(2) 他の専門職の例示

システム監査人にとって必要とされる他の専門職としては、順不同であげると、ネットワークスペシャリスト、データベーススペシャリスト、システムアナリスト、ビジネスコンサルタント、システム監査コンサルタント、技術士、弁護士、公認会計士等となる。

いずれにしても、十分かつ適切な監査証拠を入手できる専門家として、高い専門性と倫理性をもった専門職でなければならない。

3 関連事項

他の専門職の利用に際し、監査業務委託契約の再委託禁止条項について留意する。

6. 情報セキュリティ監査

情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。

1 主　旨

情報セキュリティ監査制度が平成15年4月から運用・開始されている。今までシステム監査においても、情報セキュリティ確保の観点からも監査が行われていたが、情報セキュリティ監査を実施する場合には、原則として、情報セキュリティ管理基準を活用した監査を実施することが望ましい。

2 理論的根拠／実務的配慮

システム監査は、企画・開発・運用・保守という情報システムのライフサイクルに従って、特に情報システム構築・運用の全体最適化を目的とした監査であり、情報セキュリティ監査は、情報資産のライフサイクルに従って、情報システム以外の部分も対象として情報セキュリティ確保のための管理・運用を有効に行うことを目的とした監査である。

このように、システム監査と情報セキュリティ監査は、その目的が異なり並立するものである。したがって、システム監査を実施する場合に、情報セキュリティの確保に関連する項目がシステム管理基準にある場合は、それをもって完結することも可能である。

3 関連事項

情報セキュリティ監査を実施する場合には、情報セキュリティ管理基準を活用することが望ましいとされるが、必要に応じて他の基準、例えば「情報システム安全対策基準」、「コンピュータウイルス対策基準」、「コンピュータ不正アクセス対策基準」、「ソフトウェア管理ガイドライン」等を利用することもできる。また、「システム管理基準の前文　第4パラグラフ」のただし書きに、「組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の主旨及び体系に沿って、該当する関係機関等において、独自の管理基準を策定し活用することが望ましい」とある。すなわち、業界独自の管理基準がある場合には、この基準を利用することになる。

V. 報 告 基 準

1．監査報告書の提出と開示
2．監査報告の根拠
3．監査報告書の記載事項
4．監査報告についての責任
5．監査報告に基づく改善指導（フォローアップ）

1．監査報告書の提出と開示

システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

1 主　旨

システム監査人は、監査目的に応じた監査を実施した結果、システム監査人の評価を監査報告書にまとめ、依頼者に報告しなければならない。外部の利害関係者（株主等のステークホルダー）等へ信頼を得るため、開示が必要な場合は依頼者と開示方法を検討する。

2 理論的根拠／実務的配慮

監査報告書とは、監査の結果、信頼できる事実から明らかになったシステム監査人の保証又は助言に関する評価を、正式に依頼者に報告するためのものである。したがって、この段階で事実確認が不十分であったり、判断根拠が不明確なものがあってはならない。

3 関連事項

監査で把握した事実によっては、緊急な報告を要することもあり、その場合は適時に口頭報告を行い、後日、正式な監査報告書を作成し提出する。

監査報告書の開示については、システム監査人と依頼者が協議して開示方法等を定める。

2．監査報告の根拠

システム監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

1 主　旨

監査人が正しい評価を行うためには、把握している事実が信頼できるものであることが必要である。

2 理論的根拠／実務的配慮

監査結果を裏付ける監査証拠となる事実は、適切な監査手続によって収集された客観的事実、統計的な手法等で収集された合理的な根拠に基づく情報であることが必要である。そのことがシステム監査人の評価に信頼性をもたらすことになる。

3 関連事項

サンプリング等で収集した情報は、客観性をもつものであり、適切な監査証拠になる。

3．監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、改善勧告、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。

1 主　旨

個別計画ごとに、監査結果を依頼者に確実に伝えるため、監査の目的に応じた必要事項を記載する必要がある。

2 理論的根拠／実務的配慮

監査結果を依頼者に明瞭に伝達するためには、基本的には次の事項を記載する必要がある。

システム監査報告書は、内部利用であっても、外部に開示される場合であっても、基本的には、次の記載区分によって構成される。

① 導入区分（実施した監査の対象等を記載する）
② 概要区分（実施した監査の内容等を記載する）
③ 意見区分（保証意見又は助言意見を記載する）
④ 特記区分（必要に応じてその他特記すべき事項を記載する）

監査報告の明瞭性という観点から、これらの区分に従って記載するものとする。導入、概要、意見の３つの記載区分は、システム監査の目的又は実施形態を問わず、必ず設けられなければならないことに留意する。

(1) システム監査報告書記載項目の例

① 導入区分
　a．監査部門の責任者
　b．作成日
　c．監査対象
　d．監査目的
② 概要区分
　e．監査範囲及び手続
　f．実施期間
　g．担当区分及び担当者
③ 意見区分
　h．監査結果（監査意見）
　i．指摘事項
　j．改善勧告（通常改善・緊急改善）
④ 特記区分

k．関係部門との調整事項

l．その他付属事項

(2) 監査意見の種別

監査報告書は、監査の目的又は契約の内容によって、保証型の監査報告書が作成される場合と、助言型の監査報告書が作成される場合がある。

1通の監査報告書において、保証意見を記載した後で、助言意見を記載することもある。

3 関連事項

(1) 助言型報告書の雛型

システム監査人は、監査した結果、改善を要する検出事項を認めた場合には、おおむね次のように、「システム管理基準」等に照らして、検出事項を指摘し、必要に応じて当該検出事項に対する改善提言を記載した監査報告書を作成する。

システム監査報告書

平成　　年　　月　　日

宛　名

監査人署名

われわれは①、「システム管理基準」に照らして②、平成ｘ年ｘ月ｘ日から平成ｘ年ｘ月ｘ日までの期間③に係る XXX を対象として④XXX について⑤監査を実施した。われわれの任務は、監査手続を実施した結果に基づいて助言を行うことにある⑥。

われわれの監査は、「システム監査基準」に準拠して行われた。監査は、組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて⑦適切に整備・運用されているか否かを確かめ、問題点を検出し、提示するという観点から行われている⑧。

われわれは、平成ｘ年ｘ月ｘ日から平成ｘ年ｘ月ｘ日までの期間に係る XXX を対象とした XXX について、「システム管理基準」に照らして、以下の検出事項と、その改善提言を含め、ここに報告⑨する。

記⑩

1．検出事項　　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

2．改善提言　　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

（下線部①について）

システム監査人が内部監査部門であるときは「当監査部門」とする。また、システム監査人が個人事業主であるときは「私は」とする。以下の該当箇所も同様である。

（下線部②について）

システム監査の目的を十分に達成するためには、「システム管理基準」の趣旨と枠組みを尊重し、当該すべての項目について監査の対象とすることが望ましいが、「システム管理基準」のすべての項

目ではなく、一部分の項目（例えば、外部委託に係る管理項目のみ）を監査上の判断の尺度としたときは、その旨を明記する。ただし、その場合には、システム監査の対象として選択された管理項目が、監査の対象として選択されなかった他の管理項目と有機的に結びついて初めて有効に機能することもある点に留意しなければならない。また、「システム管理基準」以外の基準等を判断の尺度としたときは、該当する基準等を明記する。

（下線部③について）

雛形は、一定期間を対象としたシステム監査を実施した場合の例を示している。ある特定時点におけるシステム監査について意見を表明するときは、「平成 x 年 x 月 x 日現在における」と記載する。

（下線部④について）

システム監査の対象を記載する。監査の対象については、必要に応じて、監査対象の範囲（例えば、外部委託）、監査対象の段階（例えば、運用段階）、及び監査対象に係る監査目標（例えば、機密性）等を記載する。また、監査の対象となる組織、場所、情報システム（例えば、Web システム）等を限定する必要があるときは、当該組織、場所、情報システム等も併せて明記する。

（下線部⑤について）

システム監査の目的に応じた監査テーマを記載する。監査テーマについては、重要なリスクが情報システムのどの領域に存在するかによって実施すべきシステム監査のテーマが違ってくる。重要なリスクに応じて、監査テーマ（例えば、ネットワークシステム、個人情報保護に関するシステム等）を選択する。

（下線部⑥について）

システム監査人の任務は、助言を行うことにあることを明記する。助言はそれが実行に移されて意味をもつことから、その点を徹底するため、「当該監査の結果として提示された助言に基づいて、適切な是正措置が確実かつ速やかに実行に移されることを望む」といった文言を追加してもよい。システム監査人と被監査側の間に責任区別が存在することは当然であるが、保証意見とは異なり、責任区別についてあえて言及する必要はない。

（下線部⑦について）

リスクアセスメントが行われていないか、又はリスクアセスメントが不適切な場合には、この記載は行わない。このようなリスクアセスメントの不備は、検出事項に含めることが望ましい。また、システム監査人自らがリスクアセスメントを実施した場合には、「監査人が必要と認めて、リスクアセスメントを行った結果に基づいて」と明記する。

（下線部⑧について）

助言型のシステム監査は、情報システムにまつわるリスクのコントロールの改善を目的として、そのための問題点を検出し提示するという観点から行われるものであるから、その旨を明記する。問題点の検出は、「システム管理基準」その他適切な基準等に示された各項目に照らして行われるものであるが、マネジメント又はコントロールは、それぞれの構成要素がお互いに影響し合いながら結びついている点に着目することが肝要である。そのような観点をより明確にするためには、「問題点を検出し」の前に「体系的に」という字句を補うことが望ましい。

（下線部⑨について）

システム監査人の最終意見は、検出事項と、必要に応じてそれに対応する改善提言を示すものでなければならない。この場合、検出事項並びに改善提言の報告である旨を明記し、「以下の検出事項があるものの、当面、緊急かつ重要な影響は予想されないものと判断される」等、保証の付与と紛らわしい表現を用いてはならない。

（下線部⑩について）

検出事項及び改善提言は、意見区分の中に別途見出しを設けて記載する。検出事項及び改善提言が長文となる場合には、監査報告書別紙として取りまとめる。

検出事項及び改善提言は、それぞれ重要性が高いものから記載し、検出事項と改善提言の対応関係が明らかとなるよう工夫されることが望ましい。また、改善提言を行う場合には、緊急性のある改善提言を要緊急改善提言、その他の改善提言を分けて記載することが有益である。

(2) 保証型報告書（肯定意見）の雛型

システム監査人は、情報システムにまつわるリスクのコントロールがシステム管理基準等に照らして適切に整備され運用されている旨の監査報告書を作成する。

システム監査報告書

平成　　年　　月　　日

宛　名

監査人署名

われわれは①、「システム管理基準」に照らして②、平成ｘ年ｘ月ｘ日から平成ｘ年ｘ月ｘ日までの期間③に係るXXXを対象として④XXXについて⑤監査を実施した。われわれの責任は、監査手続を実施した結果に基づいて意見を表明することにある⑥。

われわれの監査は、「システム監査基準」に準拠して行われた。監査は、組織体の情報システムにまつわるリスクに対するコントロールが、リスクアセスメントに基づいて⑦適切に整備・運用されているか否かについて検討し評価している。採用した監査手続は、われわれが必要と認めたものを適用しており⑧、監査の結果として意見表明のための合理的な根拠を得たと確信している⑨。

われわれの意見によれば、平成ｘ年ｘ月ｘ日から平成ｘ年ｘ月ｘ日までの期間に係るXXXを対象としたシステム監査の結果について、「システム管理基準」に照らして適切であると認める⑩。

（下線部①について）

システム監査人が内部監査部門であるときは「当監査部門」とする。また、システム監査人が個

人事業主であるときは「私は」とする。以下の該当箇所も同様である。

（下線部②について）

システム監査の目的を十分に達成するためには、「システム管理基準」の趣旨と枠組みを尊重し、当該すべての項目について監査の対象とすることが望ましいが、「システム管理基準」のすべての項目ではなく、一部分の項目（例えば、外部委託に係る管理項目のみ）を監査上の判断の尺度としたときは、その旨を明記する。ただし、その場合には、システム監査の対象として選択された管理項目が、監査の対象として選択されなかった他の管理項目と有機的に結びついて初めて有効に機能することもある点に留意しなければならない。また、「システム管理基準」以外の基準等を判断の尺度としたときは、該当する基準等を明記する。

（下線部③について）

雛形は、一定期間を対象としたシステム監査を実施した場合の例を示している。ある特定時点におけるシステム監査について意見を表明するときは、「平成 x 年 x 月 x 日現在における」と記載する。

（下線部④について）

システム監査の対象を記載する。監査の対象については、必要に応じて、監査対象の範囲（例えば、外部委託）、監査対象の段階（例えば、運用段階）、及び監査対象に係る監査目標（例えば、機密性）等を記載する。また、監査の対象となる組織、場所、情報システム（例えば、Web システム）等を限定する必要があるときは、当該組織、場所、情報システム等もあわせて明記する。

（下線部⑤について）

システム監査の目的に応じた監査テーマを記載する。監査テーマについては、重要なリスクが情報システムのどの領域に存在するかによって実施すべきシステム監査のテーマが違ってくる。重要なリスクに応じて、監査テーマ（例えば、ネットワークシステム、個人情報保護に関するシステム等）を選択する。

（下線部⑥について）

情報システムにまつわるリスクに対するコントロールに直接的かつ第一次的に責任を負うのはあくまでも被監査側であって、システム監査人は自らが実施した監査の方法と結論についてのみ責任を負うという責任区別の原則を徹底するために記載される。内部監査部門によるシステム監査を前提とするときは特に記載を要しないが（記載を禁止するものではない）、外部機関による監査を前提とするときは記載することが望ましい。

（下線部⑦について）

「システム管理基準」の趣旨からすれば、情報システムにまつわるリスクに対するコントロールは、リスクアセスメントに基づくものでなければならない。リスクアセスメントが行われていないか又はリスクアセスメントが不適切な場合には、この記載は行わない。

（下線部⑧について）

システム監査報告書において、実施した監査手続のすべてを列記することは現実的でないばかりか、監査報告書読者の混乱を招く結果ともなりかねない。システム監査人が必要と認めた監査手続を実施した旨の記載で十分である。しかし、特別な追加的手続を実施したときや、実施した監査手続が特別な条件のもとで行われたときには、その旨と理由を明記しておくことが望ましい。

（下線部⑨について）

監査意見としての保証は絶対的な保証ではなく、入手した監査証拠を評価した結果得られた合理的な根拠に基づく保証である。情報システムにまつわるリスクに対するコントロールの欠陥が皆無であることを保証するものではないため、「合理的な」という字句を含めておくことが有益である。

（下線部⑩について）

システム監査人の最終意見は、簡潔明瞭でなければならない。また、助言意見と混同されるような表現は避けなければならない。「システム管理基準」に従った監査においては「『システム管理基準』に照らして、適切に」という表現を推奨しているが、これに限定されない。例えば「『システム管理基準』に準拠しているものと認める」、「『システム管理基準』の趣旨に鑑みて、有効であると認める」等の意見表明方式でもよい。これらの例は、いずれも「認める」という結語にその意味が端的にあらわれているように、積極型の保証意見である。これに対して、「『システム管理基準』に照らして、特に指摘すべき事項は見当たらなかった」、「『システム管理基準』から逸脱する重要な事実はなかった」といった意見表明方式が採用されることがある。これらの例は消極型の保証意見である。

(3) 従来型報告書の雛型

助言型監査並びに保証型監査の確立・定着に猶予期間が必要な場合は、既存システム監査報告書の雛型を併用してもよい。

ただし、当該システム監査基準及びシステム管理規準を準拠するものとする。

様　式　例

システム監査報告書

代表取締役社長　A　殿

平成ｘｘ年１２月２日

システム監査室室長　B　　印

平成　ｘｘ　年度システム監査基本計画に基づく下記項目の監査結果について、以下のとおり報告します。

監査対象	重点監査テーマ
給与計算業務	Ｚ計算センターに委託している当社の給与計算業務の信頼性確保状況を確認する。

目的	給与計算業務にかかわる機密保護対策の妥当性の評価

範囲・手続の概要

平成ｘｘ年１１月分の委託処理に対して、入力データを当社からＺ計算センターへ運搬することから、Ｚ計算センター内での処理を経て、給与明細書等の出力帳票を当社が重量するまでに至る経過を逐次、追跡調査した。

実施期間	自　平成ｘｘ年１０月２６日　　至　平成ｘｘ年１１月３０日　（　5日間）

被監査	被監査部門 人事部給与計算課 対応者 Ｃ課長、Ｄ係長	監査チーム	監査チームリーダ Ｂシステム監査室室長 監査メンバー Ｙ監査委員

総合評価

Ｚ計算センターは、「ISMS 適合性評価制度」に基づく認証を取得しており、また給与計算業務の受託経験も長く受託実績も高いので、入退館室管理の徹底、職務分担の徹底等、機密保護対策として必要最低限の要件は満たされており、総合的に当社の給与データが第三者へ漏えいする危険性は少ないと判断される。

しかしながら、「指摘事項」で示す問題発生が想定されるので、適切な対策を実施する必要がある。

概　要

リスクに対するコントロール状況

区分	概　評	評　価
情報戦略	経営方針、戦略目標への適合性を評価する。	
信頼性	情報システムの品質並びに障害の発生、影響範囲及び回復の度合いを評価する。	
安全性	情報システムの自然災害、不正アクセス及び被壊行為からの保護の度合いを評価する。	
効率性	情報システムの資源の活用及び費用対効果の度合いを評価する。	
法・規則	法・関連規則の準拠度合いを評価する。	

指摘事項（重欠点／軽欠点／アドバイス）

管理基準（項番）	指摘事項	改善勧告	区分
Ⅳ運用管理 3.入力管理	入力データは、関係者以外の者が見ても理解することが可能な状態で運搬されている。	①入力データを磁気化する。 ②入力データの運搬ケースにかぎをかける。 ③入力端末機設置し、運搬をやめる。	軽
Ⅳ運用管理 4.ﾃﾞｰﾀ管理	給与明細表を不正に持出しすることが可能である。	①給与明細出力時に立ち会う。 ②当社にプリンタを設置し、給与明細を直接出力する。	重
Ⅳ運用管理 4.ﾃﾞｰﾀ管理	給与明細の引渡し方法が不適切である。	同上	軽
Ⅳ運用管理 5.出力管理	不要出力帳票の焼却処分までの保管方法が不適切である。	①廃棄文書専用の保管箱を設置する。	軽

管理区分によって重要改善項目を明らかにする。

注意：指摘事項に対し別途の詳細改善策が必要な場合がある。

（目的について）

システム監査基本計画に基づく監査目的と個別監査目的が考慮されることが望ましい。

（リスクに対するコントロール状態について）

報告者（組織体の長）にシステム監査の結果概要を伝えるため、情報システムの情報戦略、信頼性、安全性、効率性、法・規則についての評価結果を簡潔に記載すること。

（指摘事項について）

システム管理基準に該当する項目がある場合、項番及び項目を明らかにする。

指摘事項は、何が問題であるか、理由を明確にし、事実誤認がないことを被監査部門と確認すること。

指摘事項に対する改善勧告を記述すること。改善勧告の内容は被監査部門と確認して実現可能な内容とすること。

指摘内容の重要性に応じた管理を実施するため、区分（重欠点、軽欠点、アドバイス）を設定することが望ましい。

（報告について）

システム監査報告書は、組織体の長、又は組織体の長が権限を委譲した者に提出すること。

4．監査報告についての責任

システム監査人は、監査報告書の記載事項について、その責任を負わなければならない。

1 主　旨

システム監査人は、監査依頼者に対し監査結果を記載した監査報告書の記載事項について責任を負う。

2 理論的根拠／実務的配慮

指摘事項（問題点）と判断した事項はどのような監査証拠に基づいているか等、十分な裏付けをとっておく必要がある。また、指摘事項、改善勧告の内容については、被監査部門との意見交換を行う等によって事実の誤認がないことを確認することが重要である。

3 関連事項

リスクに対するコントロールに責任を負うのはあくまでも被監査側であって、システム監査人は自らが実施した監査の方法と結論についてのみ責任を負う。

「監査報告書についての責任」の中でも保証意見が与える影響は大きいと考えられる。したがって、以下の内容を考慮する必要がある。

＜保証意見記載上の留意事項＞

・保証意見は、一定の保証を付与するものであるため、システム監査人が負うかもしれない責任に十分に留意し、あいまいな表現を避け、助言意見と混同されることがないようにしなければならない。

・システム監査の結果、無視し得ない指摘事項があることを監査意見として表明しなければならない場合、システム監査人は、監査報告書の外部開示又は非開示を考慮し、必要に応じて法律専門家に助言を求める等して、監査報告書の記載方法、表記方法、並びに取扱い方法を慎重に検討した上で監査報告書を作成し、提出しなければならない。

5．監査報告に基づく改善指導（フォローアップ）

システム監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。

1 主　旨

システム監査人は、改善勧告に基づき改善措置が被監査部門において確実に実行されていることを確認し、監査目的達成に向け、指導性を発揮する必要がある。

2 理論的根拠／実務的配慮

システム監査報告書を提出した後、改善勧告の内容に基づいて改善を促進するように改善指導（フォローアップ）するまでが監査業務（「IV．実施基準　4.監査業務の体制」）であり、監査業務の全体を管理する必要がある。

3 関連事項

(1) 改善勧告の内容、重要性、緊急性等によって改善の実現を促進させること。
(2) 改善勧告について、その後適切な措置が講じられていない場合は、改善の実現が図られるような措置をとること。
(3) 改善が図られない場合は、再度、改善勧告を出すこと。
(4) 外部監査の改善指導（フォローアップ）については、契約の締結の仕方による。

索　引

執筆及び協力者一覧

システム監査基準解説書

市村　典男	(社)情報サービス産業協会　システム監査研究会 副座長
稲垣　隆一	日本弁護士連合会　弁護士
岡崎　洋治	(財)金融情報システムセンター 監査安全部　主任研究員
橘和　尚道	NPO 法人日本システム監査人協会　副会長
鳥居　壮行	駿河台大学　文化情報学部 教授
原田　要之助	情報システム・コントロール協会　東京支部
本田　　実	システム監査学会　理事
丸山　満彦	監査法人トーマツ　エンタープライズリスクサービス部 シニアマネジャー

(五十音順，勤務先等：2005 年 1 月現在)

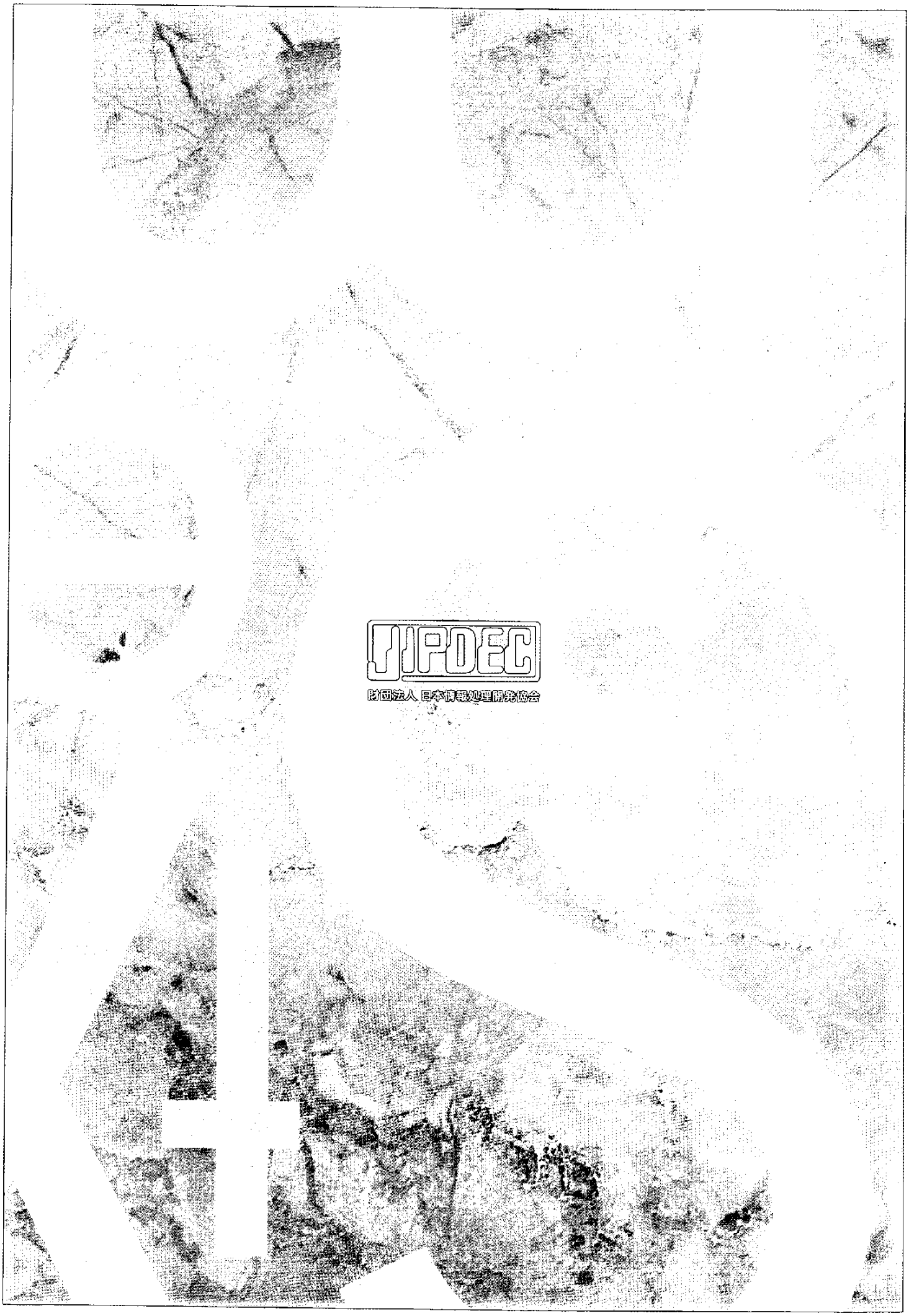
『新版　システム監査基準／システム管理基準解説書』(平成 16 年基準改訂版)

システム監査基準解説書　　2005 年 1 月 31 日　発行

編集兼
発行人　　児玉　幸治

発行所　　財団法人　日本情報処理開発協会。
〒105-0011　東京都港区芝公園 3-5-8　機械振興会館内
TEL03-3432-9381　FAX03-3432-9389
URL　http://www.jipdec.jp/

ISBN4-89078-013-0


JIPDEC
財団法人 日本情報処理開発協会

system management standards

新版

システム管理基準 解説書

平成16年基準策定版

新版

システム管理基準解説書

平成16年基準策定版

監修にあたって

ITの革新とともに、情報システムはその位置付けが大きく変化し、今や企業経営、組織運営にとって欠かせない基盤となりました。即ち、かつての専用システム、大型汎用機の時代から、一人一台パソコンを持つ時代へと変遷する中で、ITが今や企業統治や企業戦略の実現手段、通信手段、外部向けサービスの提供手段に至るまで深く浸透してきています。IT は、経営の３要素と言われる「人」「モノ」「カネ」と同様に重要な要素であると言えます。

こうした変化の背景には、インターネットの急速な発展が深く関係しています。システム監査が前回 1996 年（平成８年）に改訂されてからの９年は、正にインターネットの発展の歴史そのものでもあります。この間、情報システムやインターネットは、中小企業や一般利用者に至るまで「ユーザ」の底辺を一気に拡げてきました。

ユーザの底辺が拡がり、浸透していく一方で、ユーザは情報システムを巡るリスクにも直面するようになりました。また、情報システムへの依存度の高まりとともに、そのリスクは年々高まっていると言わざるを得ません。本来、情報システムは企業・個人の利便性・効率性を大幅に向上するためのものですが、情報システムを導入・構築していく上で、その信頼性を確保していかなければ、企業の信用ある経営は成り立ちませんし、また安全性を確保しなければ、企業の継続的な製品・サービスの提供がままならないだけでなく、情報流出などがおこった場合などには法的責任や社会的責任も負いかねません。加えて、情報化投資は当然多大な費用が生じるわけですから、その目的や戦略、費用対効果やリスクに関して株主や投資家などのステークホルダーに対する説明責任も生じてきます。

そのため、経済産業省は情報システムのライフサイクル各段階におけるリスクが適切に管理されているかを監査するための必要事項を記した「システム監査基準」(1985 年策定、1996 年改訂)を、IT ガバナンスの実現に寄与することを目的に大幅に改訂し、今回新しい「システム管理基準」、「システム監査基準」として公表しました。改訂にあたっては、IT ガバナンスの観点を考慮したことに加えて、技術革新に伴う新たなリスクへの対応のための管理項目を追加し、説明責任を果たすために内部だけでなく外部への監査結果の開示も想定した手続きを記しております。また、国際的な潮流と整合性を保つため、諸外国の同様の基準や制度についても参考にして改訂を行いました。

本書は、このシステム監査基準の改訂を受けて発行するものであり、新基準の各項目を分かり易く具体的に解説したものであります。本書を参考にして、内部監査及び外部の第三者による専門的な監査が実施され、IT ガバナンスの実現により企業・組織の価値が向上していくことを期待しています。

2005 年 1 月

経済産業省商務情報政策局
情報セキュリティ政策室

目　次

システム管理基準

策定　平成16年10月８日

前文

今日、組織体の情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。さらに、それぞれの情報システムがネットワーク化されることにより、社会の重要なインフラストラクチャとなってきている。一方、情報システムはますます多様化、複雑化し、それに伴い様々なリスクが顕在化してきている。また、情報システムに係わる利害関係者も組織体内にとどまらず、社会へと広がっている。従って、このような情報システムにまつわるリスクを適切にコントロールすることが組織体における重要な経営課題となっている。システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。また、システム監査の実施は、組織体のITガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は、以下の通りである。

・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

システム管理基準は、組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範である。

システム管理基準は、本管理基準と姉妹編をなすシステム監査基準に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。ただし、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の主旨及び体系に則って、該当する関係機関などにおいて、独自の管理基準を策定し活用することが望ましい。また、時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ましい。

なお、情報セキュリティの確保の観点から監査を実施する場合には、情報セキュリティ監査制度に基づく情報セキュリティ監査を行うことが要請される。一方で、システム管理基準においても情報セキュリティの確保に関連する項目が挙げられているが、それぞれの項目について、情報セキュリティ管理基準を活用して監査を実施することが望ましい。

システム管理基準（287 項目）

Ⅰ．情報戦略（47）

1．全体最適化（18）

1.1　全体最適化の方針・目標（6）

(1) IT ガバナンスの方針を明確にすること。
(2) 情報化投資及び情報化構想の決定における原則を定めること。
(3) 情報システム全体の最適化目標を経営戦略に基づいて設定すること。
(4) 組織体全体の情報システムのあるべき姿を明確にすること。
(5) システム化によって生ずる組織及び業務の変更の方針を明確にすること。
(6) 情報セキュリティ基本方針を明確にすること。

1.2　全体最適化計画の承認（3）

(1) 全体最適化計画の立案体制は、組織体の長の承認を得ること。
(2) 全体最適化計画は、組織体の長の承認を得ること。
(3) 全体最適化計画は、利害関係者の合意を得ること。

1.3　全体最適化計画の策定（7）

(1) 全体最適化計画は、方針及び目標に基づいていること。
(2) 全体最適化計画は、コンプライアンスを考慮すること。
(3) 全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。
(4) 全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。
(5) 全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。
(6) 全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。
(7) 全体最適化計画は、外部資源の活用を考慮すること。

1.4　全体最適化計画の運用（2）

(1) 全体最適化計画は、関係者に周知徹底すること。
(2) 全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。

2．組織体制（9）

2.1　情報システム化委員会（5）

(1) 全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。
(2) 委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。
(3) 委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。
(4) 委員会は、活動内容を組織体の長に報告すること。

(5) 委員会は、意思決定を支援するための情報を組織体の長に提供すること。

2.2 情報システム部門 (2)

(1) 情報システム部門の使命を明確にし、適切な権限及び責任を与えること。

(2) 情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。

2.3 人的資源管理の方針 (2)

(1) 情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。

(2) 人的資源の調達及び育成の方針を明確にすること。

3．情報化投資 (6)

(1) 情報化投資計画は、経営戦略との整合性を考慮して策定すること。

(2) 情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。

(3) 情報化投資に関する予算を適切に執行すること。

(4) 情報化投資に関する投資効果の算出方法を明確にすること。

(5) 情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。

(6) 投資した費用が適正に使用されたことを確認すること。

4．情報資産管理の方針 (4)

(1) 情報資産の管理方針及び体制を明確にすること。

(2) 情報資産のリスク分析を行い、その対応策を考慮すること。

(3) 情報資産の効率的で有効な活用を考慮すること。

(4) 情報資産の共有化による生産性向上を考慮すること。

5．事業継続計画 (5)

(1) 情報システムに関連した事業継続の方針を策定すること。

(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。

(3) 事業継続計画は、従業員の教育訓練の方針を明確にすること。

(4) 事業継続計画は、関係各部に周知徹底すること。

(5) 事業継続計画は、必要に応じて見直すこと。

6．コンプライアンス (5)

(1) 法令及び規範の管理体制を確立するとともに、管理責任者を定めること。

(2) 遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。

(3) 情報倫理規程を定め、関係者に教育及び周知徹底すること。

(4) 個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めること。
(5) 法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。

II．企画業務 (23)

1．開発計画 (9)

(1) 開発計画は、組織体の長が承認すること。
(2) 開発計画は、全体最適化計画との整合性を考慮して策定すること。
(3) 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。
(4) 開発計画は、関係者の教育及び訓練計画を明確にすること。
(5) 開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。
(6) 開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。
(7) 開発計画はシステムライフを設定する条件を明確にすること。
(8) 開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。
(9) 開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成し、検討すること。

2．分析 (8)

(1) 開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。
(2) ユーザニーズの調査は、対象、範囲及び方法を明確にすること。
(3) 実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。
(4) ユーザニーズは文書化し、ユーザ部門が確認すること。
(5) 情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。
(6) 情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。
(7) 情報システムの導入効果の定量的及び定性的評価を行うこと。
(8) パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。

3．調達(6)

(1) 調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。
(2) ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。
(3) 開発を遂行するために必要な要員、予算、設備、期間等を確保すること。
(4) 要員に必要なスキルを明確にすること。
(5) ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。
(6) 調達した資源は、ルールに従って管理すること。

Ⅲ．開発業務（49）

１．開発手順（4）

(1) 開発手順は、開発の責任者が承認すること。
(2) 開発手順は、開発方法に基づいて作成すること。
(3) 開発手順は、開発の規模、システム特性等を考慮して決定すること。
(4) 開発時のリスクを評価し、必要な対応策を講じること。

２．システム設計（15）

(1) システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。
(2) 運用及び保守の基本方針を定めて設計すること。
(3) 入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。
(4) データベースは、業務の内容及びシステム特性に応じて設計すること。
(5) データのインテグリティを確保すること。
(6) ネットワークは、業務の内容及びシステム特性に応じて設計すること。
(7) 情報システムの性能は、要求定義を満たすこと。
(8) 情報システムの運用性及び保守性を考慮して設計すること。
(9) 他の情報システムとの整合性を考慮して設計すること。
(10) 情報システムの障害対策を考慮して設計すること。
(11) 誤謬防止、不正防止、機密保護等を考慮して設計すること。
(12) テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。
(13) 情報システムの利用に係る教育の方針、スケジュール等を明確にすること。
(14) モニタリング機能を考慮して設計すること。
(15) システム設計書をレビューすること。

３．プログラム設計（5）

(1) プログラム設計書は、開発の責任者が承認すること。
(2) システム設計書に基づいて、プログラムを設計すること。
(3) テスト要求事項を定義し、文書化すること。
(4) プログラム設計書及びテスト要求事項をレビューすること。
(5) プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。

４．プログラミング（4）

(1) プログラム設計書に基づいてプログラミングすること。
(2) プログラムコードはコーディング標準に適合していること。
(3) プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。
(4) 重要プログラムは、プログラム作成者以外の者がテストすること。

5．システムテスト・ユーザ受入れテスト（13）

(1) システムテスト計画は、開発及びテストの責任者が承認すること。

(2) ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。

(3) システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。

(4) テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。

(5) システムテストは、本番環境と隔離された環境で行うこと。

(6) システムテストは、開発当事者以外の者が参画すること。

(7) システムテストは、適切なテスト手法及び標準を使用すること。

(8) ユーザ受入れテストは、本番同様の環境を設定すること。

(9) ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。

(10) ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。

(11) システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。

(12) システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。

(13) パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。

6．移行（8）

(1) 移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。

(2) 移行作業は文書に記録し、責任者が承認すること。

(3) 移行完了の検証方法を移行計画で明確にすること。

(4) 移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。

(5) 移行は手順書を作成し、実施すること。

(6) 移行時のリスク対策を検討すること。

(7) 運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。

(8) 移行は関係者に周知徹底すること。

Ⅳ．運用業務（73）

1．運用管理ルール（4）

(1) 運用管理ルール及び運用手順は、運用の責任者が承認すること。

(2) 運用管理ルールは、運用設計に基づいて作成すること。

(3) 運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。

(4) 運用設計及び運用管理ルールに基づいて、担当責任者を定めること。

2．運用管理（16）

(1) 年間運用計画を策定し、責任者が承認すること。

(2) 年間運用計画に基づいて、月次、日次等の運用計画を策定すること。
(3) 運用管理ルールを遵守すること。
(4) ジョブスケジュールは、業務処理の優先度を考慮して設定すること。
(5) オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。
(6) 例外処理のオペレーションは、運用管理ルールに基づいて行うこと。
(7) オペレータの交替は、運用管理ルールに基づいて行うこと。
(8) ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。
(9) オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。
(10) 事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。
(11) 事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。
(12) 事故及び障害の原因を究明し、再発防止の措置を講じること。
(13) 情報システムのユーザに対する支援体制を確立すること。
(14) 情報セキュリティに関する教育及び訓練をユーザに対して実施すること。
(15) 情報システムの稼動に関するモニタリング体制を確立すること。
(16) 情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。

3．入力管理 (5)
(1) 入力管理ルールを定め、遵守すること。
(2) データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。
(3) 入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。
(4) データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。
(5) 入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。

4．データ管理 (10)
(1) データ管理ルールを定め、遵守すること。
(2) データへのアクセスコントロール及びモニタリングは、有効に機能すること。
(3) データのインテグリティを維持すること。
(4) データの利用状況を記録し、定期的に分析すること。
(5) データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。
(6) データの授受は、データ管理ルールに基づいて行うこと。
(7) データの交換は、不正防止及び機密保護の対策を講じること。
(8) データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。
(9) データに対するコンピュータウイルス対策を講じること。
(10) データの知的財産権を管理すること。

5．出力管理 (7)

(1) 出力管理ルールを定め、遵守すること。
(2) 出力情報は、漏れなく、重複なく、正確であることを確認すること。
(3) 出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。
(4) 出力情報の引渡しは、出力管理ルールに基づいて行うこと。
(5) 出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。
(6) 出力情報のエラー状況を記録し、定期的に分析すること。
(7) 出力情報の利用状況を記録し、定期的に分析すること。

6．ソフトウェア管理（9）
(1) ソフトウェア管理ルールを定め、遵守すること。
(2) ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。
(3) ソフトウェアの利用状況を記録し、定期的に分析すること。
(4) ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。
(5) ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。
(6) ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。
(7) ソフトウェアに対するコンピュータウイルス対策を講じること。
(8) ソフトウェアの知的財産権を管理すること。
(9) フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。

7．ハードウェア管理（6）
(1) ハードウェア管理ルールを定め、遵守すること。
(2) ハードウェアは、想定されるリスクに対応できる環境に設置すること。
(3) ハードウェアは、定期的に保守を行うこと。
(4) ハードウェアは、障害対策を講じること。
(5) ハードウェアの利用状況を記録し、定期的に分析すること。
(6) ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。

8．ネットワーク管理（6）
(1) ネットワーク管理ルールを定め、遵守すること。
(2) ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。
(3) ネットワーク監視ログを定期的に分析すること。
(4) ネットワークは、障害対策を講じること。
(5) ネットワークの利用状況を記録し、定期的に分析すること。
(6) ネットワークを利用したサービスについて、組織体としての方針を明確にすること。

9．構成管理（4）
(1) 管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理するこ

と。

(2) ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。

(3) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。

(4) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。

10. 建物・関連設備管理 (6)

(1) 建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。

(2) 建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。

(3) 関連設備は、適切な運用を行うこと。

(4) 関連設備は、定期的に保守を行うこと。

(5) 関連設備は、障害対策を講じること。

(6) 建物及び室への入退の管理を記録し、定期的に分析すること。

V. 保守業務 (19)

1. 保守手順 (3)

(1) 保守ルール及び保守手順は、保守の責任者が承認すること。

(2) 保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。

(3) 保守時のリスクを評価し、必要な対応策を講じること。

2. 保守計画 (3)

(1) 保守計画はユーザ及び保守の責任者が承認すること。

(2) 変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。

(3) 保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。

3. 保守の実施 (3)

(1) システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。

(2) プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。

(3) 変更したプログラム設計書に基づいてプログラミングしていることを検証すること。

4. 保守の確認 (5)

(1) 変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。

(2) 変更したプログラムは、影響範囲を考慮してテストを行うこと。

(3) 変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。

(4) 変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。

(5) 変更したプログラムのテストの結果を記録及び保管すること。

5．移行 (3)

(1) 移行手順は、移行の条件を考慮して作成すること。

(2) 変更前のプログラム及びデータのバックアップを行うこと。

(3) 運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。

6．情報システムの廃棄 (2)

(1) 旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。

(2) 旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。

VI. 共通業務 (76)

1．ドキュメント管理 (9)

1.1 作成(5)

(1) ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。

(2) ドキュメント作成ルールを定め、遵守すること。

(3) ドキュメントの作成計画を策定すること。

(4) ドキュメントの種類、目的、作成方法等を明確にすること。

(5) ドキュメントは、作成計画に基づいて作成すること。

1.2 管理 (4)

(1) ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。

(2) ドキュメント管理ルールを定め、遵守すること。

(3) 情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。

(4) ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。

2．進捗管理 (6)

2.1 実施 (3)

(1) 進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。

(2) ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。

(3) 進捗の遅延等の対策を講じること。

2.2 評価 (3)

(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。

(2) 評価結果は、次工程の計画に反映すること。
(3) 評価結果は、進捗管理の方法、体制等の改善に反映すること。

3．品質管理 (4)

3.1 計画 (2)

(1) 品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。
(2) 品質管理計画は、方法、体制等を明確にすること。

3.2 実施 (2)

(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。
(2) 評価結果は、品質管理の基準、方法、体制等の改善に反映すること。

4．人的資源管理 (13)

4.1 責任・権限 (3)

(1) 要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。
(2) 要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。
(3) 要員の責任及び権限を周知徹底すること。

4.2 業務遂行 (4)

(1) 要員は、権限を遵守すること。
(2) 作業分担及び作業量は、要員の知識、能力等から検討すること。
(3) 要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。
(4) 不測の事態に備えた代替要員の確保を検討すること。

4.3 教育・訓練 (4)

(1) 教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。
(2) 教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。
(3) 教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。
(4) 要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。

4.4 健康管理 (2)

(1) 健康管理を考慮した作業環境を整えること。
(2) 健康診断及びメンタルヘルスケアを行うこと。

5．委託・受託（25）

5.1　計画（3）

(1) 委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。
(2) 委託又は受託の目的、対象範囲、予算、体制等を明確にすること。
(3) 委託又は受託は、具体的な効果、問題点等を評価して決定すること。

5.2　委託先選定（3）

(1) 委託先の選定基準を明確にすること。
(2) 委託候補先に必要な要求仕様を提示すること。
(3) 委託候補先が提示した提案書の比較検討を行うこと。

5.3　契約（8）

(1) 契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。
(2) コンプライアンスに関する条項を明確にすること。
(3) 再委託の可否について明確にすること。
(4) 知的財産権の帰属を明確にすること。
(5) 特約条項及び免責条項を明確にすること。
(6) 業務内容及び責任分担を明確にすること。
(7) 契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。
(8) システム監査に関する方針を明確にすること。

5.4　委託業務（7）

(1) 委託業務の実施内容は、契約内容と一致すること。
(2) 契約に基づき、必要な要求仕様、データ、資料等を提供すること。
(3) 委託業務の進捗状況を把握し、遅延対策を講じること。
(4) 委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。
(5) 成果物の検収は、委託契約に基づいて行うこと。
(6) 業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。
(7) 委託した業務の結果を分析及び評価すること。

5.5　受託業務（4）

(1) 受託業務の実施内容は、契約内容を遵守すること。
(2) 受託内容の進捗状況を把握し、リスク対策を講じること。
(3) 成果物の品質管理を行うこと。
(4) 契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。

6．変更管理（6）

6.1　管理（3）

(1) 変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。

(2) 仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。

(3) 変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。

6.2　実施（3）

(1) 変更管理案件は、変更管理ルールに従って実施すること。

(2) 変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。

(3) 変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。

7．災害対策（13）

7.1　リスク分析（3）

(1) 地震等のリスク及び情報システムに与える影響範囲を明確にすること。

(2) 情報システムの停止等により組織体が被る損失を分析すること。

(3) 業務の回復許容時間及び回復優先順位を定めること。

7.2　災害時対応計画（6）

(1) リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。

(2) 災害時対応計画は、組織体の長が承認すること。

(3) 災害時対応計画の実現可能性を確認すること。

(4) 災害時対応計画は、従業員の教育訓練の方針を明確にすること。

(5) 災害時対応計画は、関係各部に周知徹底すること。

(6) 災害時対応計画は、必要に応じて見直すこと。

7.3　バックアップ（2）

(1) 情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。

(2) 運用の責任者は、バックアップ方法及び手順を検証すること。

7.4　代替処理・復旧（2）

(1) ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。

(2) ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。

附則

1．情報セキュリティに関連する項目については、情報セキュリティ管理基準を活用することが望ましい。

2．その他、関連する基準を活用することが望ましい。

システム管理基準の解説

解説についての留意点

解説の構成と内容

1．当解説書のうち、システム管理基準の〔前文〕に関する解説は、各項目について「主旨」「理論的根拠／実務的配慮」で構成されている。

それらの区分の考え方は、以下のとおりである。

(1) 主旨

当該項目の主旨を記載している。

(2) 理論的根拠／実務的配慮

当該項目を設定するに当たって、理論的根拠として考えられる事項や実務上配慮すべき点を記載している。

2．当解説書のうち、システム管理基準の〔Ⅰ．情報戦略〕以降の全基準に関する解説は、各項目について「主旨」「着眼点」「関連事項」で構成されている。その内容は以下のとおりである。

(1) 主旨

当該項目の主旨を記載している。

(2) 着眼点

システム監査人がシステム監査を行うにあたって、情報システムの管理に関する部分について判断をする際のポイントを記載している。

(3) 関連事項

「着眼点」の補足説明や、例示、引用資料等を記載している。

なお、〔Ⅰ．情報戦略〕以降の各基準に該当する解説ページの目次を次ページから記す。

基準項目と解説ページ

〔Ⅰ．情報戦略〕

基準項目		解説ページ
1．全体最適化	1.1　全体最適化の方針・目標	
	(1) IT ガバナンスの方針を明確にすること。	41
	(2) 情報化投資及び情報化構想の決定における原則を定めること。	42
	(3) 情報システム全体の最適化目標を経営戦略に基づいて設定すること。	43
	(4) 組織体全体の情報システムのあるべき姿を明確にすること。	44
	(5) システム化によって生ずる組織及び業務の変更の方針を明確にすること。	46
	(6) 情報セキュリティ基本方針を明確にすること。	48
	1.2　全体最適化計画の承認	
	(1) 全体最適化計画の立案体制は、組織体の長の承認を得ること。	50
	(2) 全体最適化計画は、組織体の長の承認を得ること。	51
	(3) 全体最適化計画は、利害関係者の合意を得ること。	53
	1.3　全体最適化計画の策定	
	(1) 全体最適化計画は、方針及び目標に基づいていること。	54
	(2) 全体最適化計画は、コンプライアンスを考慮すること。	56
	(3) 全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。	57
	(4) 全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。	59
	(5) 全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。	60
	(6) 全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。	62
	(7) 全体最適化計画は、外部資源の活用を考慮すること。	64
	1.4　全体最適化計画の運用	
	(1) 全体最適化計画は、関係者に周知徹底すること。	65
	(2) 全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。	66
2．組織体制	2.1　情報システム化委員会	
	(1) 全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。	68
	(2) 委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。	70
	(3) 委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。	71
	(4) 委員会は、活動内容を組織体の長に報告すること。	72
	(5) 委員会は、意思決定を支援するための情報を組織体の長に提供すること。	73
	2.2　情報システム部門	
	(1) 情報システム部門の使命を明確にし、適切な権限及び責任を与えること。	74
	(2) 情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。	75
	2.3　人的資源管理の方針	
	(1) 情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。	76

〔Ⅱ．企画業務〕

	(2) ユーザニーズの調査は、対象、範囲及び方法を明確にすること。	126
	(3) 実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。	127
	(4) ユーザニーズは文書化し、ユーザ部門が確認すること。	129
	(5) 情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。	130
	(6) 情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。	132
	(7) 情報システムの導入効果の定量的及び定性的評価を行うこと。	133
	(8) パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。	134
3．調達	(1) 調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。	136
	(2) ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。	138
	(3) 開発を遂行するために必要な要因、予算、設備、期間等を確保すること。	139
	(4) 要員に必要なスキルを明確にすること。	140
	(5) ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。	142
	(6) 調達した資源は、ルールに従って管理すること。	143

〔Ⅲ．開発業務〕

基準項目		解説ページ
1．開発手順	(1) 開発手順は、開発の責任者が承認すること。	147
	(2) 開発手順は、開発方法に基づいて作成すること。	148
	(3) 開発手順は、開発の規模、システム特性等を考慮して決定すること。	149
	(4) 開発時のリスクを評価し、必要な対応策を講じること。	152
2．システム設計	(1) システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。	154
	(2) 運用及び保守の基本方針を定めて設計すること。	157
	(3) 入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。	158
	(4) データベースは、業務の内容及びシステム特性に応じて設計すること。	161
	(5) データのインテグリティを確保すること。	163
	(6) ネットワークは、業務の内容及びシステム特性に応じて設計すること。	165
	(7) 情報システムの性能は、要求定義を満たすこと。	167
	(8) 情報システムの運用性及び保守性を考慮して設計すること。	168
	(9) 他の情報システムとの整合性を考慮して設計すること。	170
	(10) 情報システムの障害対策を考慮して設計すること。	171
	(11) 誤謬防止、不正防止、機密保護等を考慮して設計すること。	173
	(12) テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。	175
	(13) 情報システムの利用に係る教育の方針、スケジュール等を明確にすること。	178
	(14) モニタリング機能を考慮して設計すること。	180
	(15) システム設計書をレビューすること。	182
3．プログラム設計	(1) プログラム設計書は、開発の責任者が承認すること。	183
	(2) システム設計書に基づいて、プログラムを設計すること。	184

	(3) テスト要求事項を定義し、文書化すること。	186
	(4) プログラム設計書及びテスト要求事項をレビューすること。	188
	(5) プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。	190
4．プログラミング	(1) プログラム設計書に基づいてプログラミングすること。	191
	(2) プログラムコードはコーディング標準に適合していること。	193
	(3) プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。	194
	(4) 重要プログラムは、プログラム作成者以外の者がテストすること。	196
5．システムテスト・ユーザ受入れテスト	(1) システムテスト計画は、開発及びテストの責任者が承認すること。	197
	(2) ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。	199
	(3) システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。	200
	(4) テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。	201
	(5) システムテストは、本番環境と隔離された環境で行うこと。	203
	(6) システムテストは、開発当事者以外の者が参画すること。	205
	(7) システムテストは、適切なテスト手法及び標準を使用すること。	206
	(8) ユーザ受入れテストは、本番同様の環境を設定すること。	208
	(9) ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。	210
	(10) ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。	211
	(11) システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。	212
	(12) システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。	213
	(13) パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。	214
6．移行	(1) 移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。	216
	(2) 移行作業は文書に記録し、責任者が承認すること。	218
	(3) 移行完了の検証方法を移行計画で明確にすること。	219
	(4) 移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。	221
	(5) 移行は手順書を作成し、実施すること。	222
	(6) 移行時のリスク対策を検討すること。	223
	(7) 運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。	224
	(8) 移行は関係者に周知徹底すること。	225

〔Ⅳ．運用業務〕

基準項目		解説ページ
1．運用管理ルール	(1) 運用管理ルール及び運用手順は、運用の責任者が承認すること。	229
	(2) 運用管理ルールは、運用設計に基づいて作成すること。	231

	(2) 出力情報は、漏れなく、重複なく、正確であることを確認すること。	292
	(3) 出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。	294
	(4) 出力情報の引渡しは、出力管理ルールに基づいて行うこと。	296
	(5) 出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。	300
	(6) 出力情報のエラー状況を記録し、定期的に分析すること。	302
	(7) 出力情報の利用状況を記録し、定期的に分析すること。	306
6．ソフトウェア管理	(1) ソフトウェア管理ルールを定め、遵守すること。	308
	(2) ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。	310
	(3) ソフトウェアの利用状況を記録し、定期的に分析すること。	312
	(4) ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。	313
	(5) ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。	314
	(6) ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。	315
	(7) ソフトウェアに対するコンピュータウイルス対策を講じること。	317
	(8) ソフトウェアの知的財産権を管理すること。	319
	(9) フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。	321
7．ハードウェア管理	(1) ハードウェア管理ルールを定め、遵守すること。	322
	(2) ハードウェアは、想定されるリスクに対応できる環境に設置すること。	324
	(3) ハードウェアは、定期的に保守を行うこと。	327
	(4) ハードウェアは、障害対策を講じること。	329
	(5) ハードウェアの利用状況を記録し、定期的に分析すること。	331
	(6) ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。	332
8．ネットワーク管理	(1) ネットワーク管理ルールを定め、遵守すること。	334
	(2) ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。	337
	(3) ネットワーク監視ログを定期的に分析すること。	341
	(4) ネットワークは、障害対策を講じること。	343
	(5) ネットワークの利用状況を記録し、定期的に分析すること。	345
	(6) ネットワークを利用したサービスについて、組織体としての方針を明確にすること。	346
9．構成管理	(1) 管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。	347
	(2) ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。	349
	(3) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。	352
	(4) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。	353
10．建物・関連設備管理	(1) 建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。	355
	(2) 建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。	357
	(3) 関連設備は、適切な運用を行うこと。	359

	(4) 関連設備は、定期的に保守を行うこと。	360
	(5) 関連設備は、障害対策を講じること。	361
	(6) 建物及び室への入退の管理を記録し、定期的に分析すること。	363

〔V. 保守業務〕

基準項目		解説ページ
1. 保守手順	(1) 保守ルール及び保守手順は、保守の責任者が承認すること。	367
	(2) 保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。	368
	(3) 保守時のリスクを評価し、必要な対応策を講じること。	369
2. 保守計画	(1) 保守計画はユーザ及び保守の責任者が承認すること。	370
	(2) 変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。	371
	(3) 保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。	372
3. 保守の実施	(1) システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。	373
	(2) プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。	374
	(3) 変更したプログラム設計書に基づいてプログラミングしていることを検証すること。	375
4. 保守の確認	(1) 変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。	376
	(2) 変更したプログラムは、影響範囲を考慮してテストを行うこと。	377
	(3) 変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。	378
	(4) 変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。	379
	(5) 変更したプログラムのテストの結果を記録及び保管すること。	380
5. 移行	(1) 移行手順は、移行の条件を考慮して作成すること。	381
	(2) 変更前のプログラム及びデータのバックアップを行うこと。	382
	(3) 運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。	383
6. 情報システムの廃棄	(1) 旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。	384
	(2) 旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。	385

〔VI. 共通業務〕

基準項目		解説ページ
1. ドキュメント管理	1.1 作成	
	(1) ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。	389
	(2) ドキュメント作成ルールを定め、遵守すること。	391
	(3) ドキュメントの作成計画を策定すること。	393

	(4) ドキュメントの種類、目的、作成方法等を明確にすること。	395
	(5) ドキュメントは、作成計画に基づいて作成すること。	397
	1.2 管理	
	(1) ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。	398
	(2) ドキュメント管理ルールを定め、遵守すること。	399
	(3) 情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。	401
	(4) ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。	403
2. 進捗管理	2.1 実施	
	(1) 進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。	405
	(2) ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。	707
	(3) 進捗の遅延等の対策を講じること。	408
	2.2 評価	
	(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。	410
	(2) 評価結果は、次工程の計画に反映すること。	412
	(3) 評価結果は、進捗管理の方法、体制等の改善に反映すること。	413
3. 品質管理	3.1 計画	
	(1) 品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。	414
	(2) 品質管理計画は、方法、体制等を明確にすること。	416
	3.2 実施	
	(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。	418
	(2) 評価結果は、品質管理の基準、方法、体制等の改善に反映すること。	420
4. 人的資源管理	4.1 責任・権限	
	(1) 要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。	422
	(2) 要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。	423
	(3) 要員の責任及び権限を周知徹底すること。	425
	4.2 業務遂行	
	(1) 要員は、権限を遵守すること。	426
	(2) 作業分担及び作業量は、要員の知識、能力等から検討すること。	427
	(3) 要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。	428
	(4) 不測の事態に備えた代替要員の確保を検討すること。	429
	4.3 教育・訓練	

	(1) 教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。	430
	(2) 教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。	432
	(3) 教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。	433
	(4) 要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。	435
	4.4 健康管理	
	(1) 健康管理を考慮した作業環境を整えること。	438
	(2) 健康診断及びメンタルヘルスケアを行うこと。	439
5. 委託・受託	5.1 計画	
	(1) 委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。	440
	(2) 委託又は受託の目的、対象範囲、予算、体制等を明確にすること。	442
	(3) 委託又は受託は、具体的な効果、問題点等を評価して決定すること。	443
	5.2 委託先選定	
	(1) 委託先の選定基準を明確にすること。	445
	(2) 委託候補先に必要な要求仕様を提示すること。	447
	(3) 委託候補先が提示した提案書の比較検討を行うこと。	448
	5.3 契約	
	(1) 契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。	450
	(2) コンプライアンスに関する条項を明確にすること。	452
	(3) 再委託の可否について明確にすること。	454
	(4) 知的財産権の帰属を明確にすること。	455
	(5) 特約条項及び免責条項を明確にすること。	457
	(6) 業務内容及び責任分担を明確にすること。	458
	(7) 契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。	460
	(8) システム監査に関する方針を明確にすること。	461
	5.4 委託業務	
	(1) 委託業務の実施内容は、契約内容と一致すること。	462
	(2) 契約に基づき、必要な要求仕様、データ、資料等を提供すること。	464
	(3) 委託業務の進捗状況を把握し、遅延対策を講じること。	465
	(4) 委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。	467
	(5) 成果物の検収は、委託契約に基づいて行うこと。	468
	(6) 業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。	469
	(7) 委託した業務の結果を分析及び評価すること。	470

	5.5 受託業務	
	(1) 受託業務の実施内容は、契約内容を遵守すること。	471
	(2) 受託内容の進捗状況を把握し、リスク対策を講じること。	473
	(3) 成果物の品質管理を行うこと。	474
	(4) 契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。	475
6．変更管理	6.1 管理	
	(1) 変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。	476
	(2) 仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。	478
	(3) 変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。	479
	6.2 実施	
	(1) 変更管理案件は、変更管理ルールに従って実施すること。	480
	(2) 変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。	482
	(3) 変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。	483
7．災害対策	7.1 リスク分析	
	(1) 地震等のリスク及び情報システムに与える影響範囲を明確にすること。	484
	(2) 情報システムの停止等により組織体が被る損失を分析すること。	486
	(3) 業務の回復許容時間及び回復優先順位を定めること。	487
	7.2 災害時対応計画	
	(1) リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。	488
	(2) 災害時対応計画は、組織体の長が承認すること。	490
	(3) 災害時対応計画の実現可能性を確認すること。	491
	(4) 災害時対応計画は、従業員の教育訓練の方針を明確にすること。	492
	(5) 災害時対応計画は、関係各部に周知徹底すること。	493
	(6) 災害時対応計画は、必要に応じて見直すこと。	494
	7.3 バックアップ	
	(1) 情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。	495
	(2) 運用の責任者は、バックアップ方法及び手順を検証すること。	497
	7.4 代替処理・復旧	
	(1) ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。	499
	(2) ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。	501
附則	1. 情報セキュリティに関連する項目については、情報セキュリティ管理基準を活用することが望ましい。	
	2. その他、関連する基準を活用することが望ましい。	

前　　文

第１パラグラフ

今日、組織体の情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。さらに、それぞれの情報システムがネットワーク化されることにより、社会の重要なインフラストラクチャとなってきている。一方、情報システムはますます多様化、複雑化し、それに伴い様々なリスクが顕在化してきている。また、情報システムに係わる利害関係者も組織体内にとどまらず、社会へと広がっている。従って、このような情報システムにまつわるリスクを適切にコントロールすることが組織体における重要な経営課題となっている。システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。また、システム監査の実施は、組織体のITガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。

1 主　旨

システム監査は、情報システムが組織体にとっても社会にとってもインフラストラクチャとなっている今日、情報システムにまつわるリスクが適切にコントロールされているかどうかを評価するためにますます重要になってきている。これは、ITガバナンスに寄与することであり、また、その結果を基に説明責任を果たすことができるものである。

2 理論的根拠／実務的配慮

今日、情報システムは経営の重要な要素であり、インフラストラクチャとなっている。しかも、情報システムは、ネットワーク化によって相互接続が進展した結果、社会のインフラストラクチャとなっている。

このような客観情勢を背景として、情報システムをめぐり各種のリスクが顕在化している。このリスクにいかに対処していくかが重要な経営課題である。また、情報システムの拡大によって、リスクが顕在化した場合の影響を与える範囲が従来に比較して各段に広がっている。このため、リスクを適切にコントロールすることは、今日の経営における重要な要素となっている。例えば、リスクの顕在化による情報システムの停止は、リスクを適切にコントロールできなかったことの証明であり、顧客をはじめとする利害関係者に影響を与え信用を失墜させ、結果、組織体にとっては損失をもたらすことになる。

システム監査は、組織体にとって情報システムにまつわるリスクのコントロールが適切に整備・運用されていることを証明する手段として活用できる機能を果たす。このことは、ITガバナンスに寄与するとともに、システム監査の結果を開示することによって、情報システムの管理状況について利害関係者に対する説明責任を果たすことができるものである。

第2パラフラフ

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は、以下の通りである。

- **情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため**
- **情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため**
- **情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため**
- **情報システムが、関連法令、契約又は内部規程等に準拠するようにするため**

1 主　旨

組織体が情報リスクをコントロールしなければならないのは、情報システムが経営全般にわたって重要な役割を果たしているからであり、システム監査としてもそこが重要な監査要点又は着眼点になる。ここでは、情報リスクを適切に整備・運用しなければならない目的を、ポリシーの観点、運用の観点、情報の信頼性を保つ観点及びコンプライアンスの観点の四つの面から要約している。これらは、経営全般にわたる重要事項である。

2 理論的根拠／実務的配慮

今日、すべての業務が情報システムによって動いているといってよい。したがって、情報及び情報システムを中心とした経営が行われていると言い換えることができる。このような経営環境においては、システム監査では経営方針や戦略目標の実現に情報システムがどのように貢献しているかを監査要点又は着眼点にしなければならない。

情報システムが組織体の目的を実現するためには、情報システム自体が安全、有効かつ効率的に機能しなければならない。特に、情報システムの安全性が損なわれた場合、必ず損失が発生すると考えておくべきであろう。

報告する情報、特に外部に対する情報開示については、情報が正確であることを保証しなければならない。このためには、情報システムの信頼性を確保することが求められる。このような情報及び情報システムを監査して、その信頼性を保証できるシステム監査を実施しなければならない。

情報システムで処理しているのは業務である。その業務は、関連法規、契約又は内部規程等に準拠して実施されなければならない。業務が正確に処理されていることを保証するためには、法令等のルールを遵守しているかを監査しなければならない。

第３パラグラフ

システム管理基準は、組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範である。

1 主　旨

システム管理基準は、情報システムのライフサイクルを通じて効果的な情報システム投資を実現するため、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範である。

2 理論的根拠／実務的配慮

システム管理基準は、従来のシステム監査基準の実施基準を切り出して独立させ、これを今日的な情報システム活用の目的及び情報環境に合致するように修正・追加等を加えて作成したものである。

システム管理基準は、第一義的には情報システムの企画・開発・運用・保守を行う情報システム関連部門で活用するためのものである。すなわち、情報処理の現場における情報システム関連業務の管理のための基準であると位置付けられている。

システム管理基準は、従来どおり情報システムのライフサイクルの流れに沿って作成しているが、企画業務フェーズの前に今日の経営環境を配慮した情報システムの位置付けを図るため、情報戦略フェーズを設定したことが大きな特徴である。

第4パラグラフ

システム管理基準は、本管理基準と姉妹編をなすシステム監査に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。ただし、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の主旨及び体系に則って、該当する関係機関などにおいて、独自の管理基準を策定し活用することが望ましい。また、時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ましい。

1 主　旨

今回のシステム監査基準の改訂では、システム監査基準とシステム管理基準の二本立てとなった。システム管理基準は、前述のように情報処理の現場での管理のために活用する基準として作成されており、それをシステム監査の際にもシステム監査人が判断の尺度として用いるべき基準と位置付けられている。

2 理論的根拠／実務的配慮

システム管理基準は、標準的に作成したものであり、あらゆる組織体に合致する形にはなっていない。すなわち、必ずこの基準に従わなければならないという性格で作成したものではない。必要に応じて修正を加えたり細分化したり、追加するなどして、この基準をベースとした業界の基準を作成して傘下の組織体に周知徹底させたり、あるいは各組織体が自己の経営環境や情報環境に合致する基準に仕立て上げたりして活用することが望ましい。

第５パラグラフ

なお、情報セキュリティの確保の観点から監査を実施する場合には、情報セキュリティ監査制度に基づく情報セキュリティ監査を行うことが要請される。一方で、システム管理基準においても情報セキュリティの確保に関連する項目が挙げられているが、それぞれの項目について、情報セキュリティ管理基準を活用して監査を実施することが望ましい。

1 主　旨

システム監査において、情報セキュリティについて監査を実施する場合は、情報セキュリティ監査基準に基づく監査を実施することが求められる。システム管理基準においても情報セキュリティに関する項目が設定されているが、それらについても情報セキュリティ管理基準を活用して監査を実施することが望ましい。

2 理論的根拠／実務的配慮

現在、システム監査基準とシステム管理基準、情報セキュリティ監査基準と情報セキュリティ管理基準といった姉妹編をもつ２組の基準が存在している。これらは、相互に関連しており、うまく活用することによって相乗効果をもたらすように作られている。

システム監査基準と情報セキュリティ監査基準は、監査という観点からは基本的な部分については同じ内容になっている。これは、システム監査は情報システムのライフサイクルに沿った総合的な監査であるのに対し、情報セキュリティ監査は情報セキュリティに特化した監査であるということに起因している。すなわち、監査の対象、目的あるいは監査業務の内容等が異なることであり、監査の理念や手続等については両者の間に相違はないからである。

システム管理基準と情報セキュリティ管理基準については、システム管理基準が情報システムのライフサイクルに沿った内容を設定しているのに対して、情報セキュリティ管理基準は、JIS X 5080 をサブコントロールに細分化した内容になっている。すなわち、監査の目的及び対象が異なるので、基準の内容もまったく別の物になっている。

システム監査は、情報セキュリティ監査よりも対象範囲が広い監査である。したがって、システム監査を実施する際にも情報セキュリティは対象になる。そこで、情報セキュリティに関しては、必要に応じて情報セキュリティ管理基準を活用したり、更に詳細な監査を必要とする場合には改めて情報セキュリティ監査を実施すること等を考慮しなければならない。

Ⅰ. 情 報 戦 略

1．全体最適化
2．組織体制
3．情報化投資
4．情報資産管理の方針
5．事業継続計画
6．コンプライアンス

1．全体最適化

1．1　全体最適化の方針・目標

(1) IT ガバナンスの方針を明確にすること。

1 主　旨

IT ガバナンスの確立に際し、その方針を明確にしておく必要がある。

2 着 眼 点

(1) 組織体としての IT ガバナンスの内容が明確に定義されていること。

(2) 情報化戦略や情報化投資の決定等について、最終的な判断を下す機関・役職が明確に定義されていること。

(3) 最高責任者直結の職務及び最高幹部会の一員として、情報システム担当の最高責任者である CIO（Chief Information Officer）が選任されていること。

(4) IT ガバナンスの重要成功要因 CSF（Critical Success Factors）が定義されていること。

(5) 組織体の長が IT ガバナンスの方針を承認していること。

3 関連事項

(1) 「IT ガバナンス」の定義の例

① 「企業が競争優位性構築を目的に、IT 戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力」－通商産業省（当時）、(財)日本情報処理開発協会

② 「主に IT 化によって新たに生じるリスクの極小化と的確な投資判断に基づく経営効率の最大化、すなわち、リスクマネジメントとパフォーマンスマネジメントであり、これらを実施するに当たっての、健全性確保のためのコンプライアンスマネジメントの確立である」－(社)日本監査役協会 IT ガバナンス委員会

③ 「IT ガバナンスは取締役会及び経営陣の責任である。それは企業ガバナンスの不可欠な部分で、リーダシップ及び組織的な構造、及び組織の IT がその組織の戦略及び目的を保持し拡張することを保証するプロセスから成る」－情報システムコントロール協会

(2) CIO 設置のポイント

① CIO の指示を、企画、開発、運用及び保守業務の責任者へ迅速かつ正確に伝えるための指揮系統を整備すること。

② 企画、開発、運用及び保守業務の現場で発生した問題が、CIO へ迅速に伝わる情報網を整備すること。

③ CIO には、経営的な観点から意思決定を行う経営者層の一員としての役割と情報システム部門の指揮者としての役割が並立する。

④ システム監査の役割が求められる場合は、被監査部門からの独立性を担保する必要がある。

1．全体最適化

1．1　全体最適化の方針・目標

(2) 情報化投資及び情報化構想の決定における原則を定めること。

1 主　旨

首尾一貫した全体最適化計画を策定するため、情報化投資及び情報化構想の決定における原則を定めておく必要がある。

2 着眼点

(1) 情報化投資及び情報化構想等にかかわる意思決定の区分が定められていること。

(2) 各意思決定区分において、誰が、いつ、どのような頻度で決定するのかが定められていること。

(3) 各決定の基準が定められていること。

3 関連事項

(1) 情報化投資及び情報化構想等にかかわる意思決定の区分の例

① 業務における情報システムの利用の大原則：どのような情報システム及び情報技術を利用するのか。

② 情報基盤戦略：ネットワーク（組織内部門間の接続、組織体外との接続）、データの共有、物的資源の利用方法、人的資源の利用方法

③ 情報システムアーキテクチャ

④ 業務ニーズの把握方法、採用の基準

⑤ 情報化投資の優先順位付けの基準

(2) 意思決定者のレベルの例

① 組織体の長、最高責任者、CIO：情報基盤戦略や情報システムアーキテクチャ等の組織体全体に影響する案件

② 情報システム部門、ユーザ部門：業務ニーズの把握、採用の判断等のスピードや業務現場の創造性が必要な案件

(3) 原則の例

① 戦略的意思決定はトップマネジメントが行うこと。

② 情報化投資は、企業戦略の一環として位置付けられること。

③ IT 投資の投資効果を考慮すること。

④ コーポレートガバナンスのリスクマネジメントを考慮すること。

⑤ ステークホルダの要請を考慮すること。

⑥ 環境変化に対応して、最適化計画を見直すこと。

⑦ 継続的な改善を目指すこと。

1．全体最適化

1．1　全体最適化の方針・目標

(3) 情報システム全体の最適化目標を経営戦略に基づいて設定すること。

1 主　旨

経営目的を実現する情報システムを企画するため、最適化計画の目標は、経営戦略との整合性を考慮して策定する必要がある。

2 着眼点

(1) 組織体のビジョン、使命、経営戦略が明文化されていること。

(2) 情報システム全体の最適化の項目及び各項目の目標が明文化されていること。

(3) 最適化目標の達成が経営戦略に貢献することが明確であること。

3 関連事項

(1) 情報システム全体の最適化目標と経営戦略との整合性の検討方法の例

① 情報システム全体の最適化目標が達成されない場合の経営的損失のシミュレーション

② 組織体全体のバランススコアカード（BSC：Balanced Scorecard）と情報システム部門のバランススコアカードとの調整

③ 組織体全体のSWOT分析と情報システム全体のSWOT分析との調整

④ 組織体の財務状態の予測と情報化投資計画の整合性の確保

⑤ 業務の新設・変更の計画と情報システム化計画の統合

（注）SWOT分析とは、組織の強み（Strength）、弱み（Weakness）、機会（Opportunity）、脅威（Threat）の４つの軸で評価する手法。

1．全体最適化

1．1　全体最適化の方針・目標

(4) 組織体全体の情報システムのあるべき姿を明確にすること。

1 主　旨

組織体全体の情報システムは、個別の情報システムが有機的に関連し、整合性が相互に保たれて効率的かつ効果的に目的を達成するものであるため、全体最適化計画は、情報システムのあるべき姿を明確にする必要がある。

2 着眼点

(1) 組織体のすべての情報システムを各ユーザ部門の業務とともに統一的にモデル化する手法を定めていること。
(2) 情報システムの現状及びあるべき姿をモデル化手法によって記述していること。
(3) 情報システムにおける現状の課題を洗い出していること。
(4) 情報システムのあるべき姿において現状の課題が解決されることを確認していること。
(5) あるべき姿を達成する具体的な手法及び工程表が明らかになっていること。

3 関連事項

(1) モデル化すべき情報システムの側面の例
　① データ構造
　② データフロー
　③ 業務フローとコントロール
　④ 組織図
　⑤ 機能構成図
　⑥ 物理的アーキテクチャ
　⑦ 論理的アーキテクチャ
　⑧ システム間インタフェース、外部とのインタフェース
(2) あるべき姿の策定におけるチェックポイントの例
　① 企業のビジョン、ミッションを実現できるか。
　② 現実的制約の段階的解消を考慮しているか。
　③ 業務改革、システム統合によって効率性、有効性を達成できるか。
　④ ユーザ部門の業務の継続性を保証しているか。
　⑤ 既存システム資産の継承と有効活用を考慮しているか。
　⑥ 段階的な移行が検討されているか。

(3) EA（Enterprize Architecture）について

EAは、業務・システム最適化計画と訳されているが、組織活動の目的を達成するための組織体の取組みであり、業務とシステムをともに最適化することを目指す手法である。米国で1980年代末ごろにその手法が提案され、米国連邦政府の業務、システム改善で実績をあげた。日本においては、政府調達改革の一環として経済産業省の「ITアソシエート協議会」が米国における事例等を調査し、EAを組織全体のIT投資戦略を記述する手法として導入することが最も適切であるとの結論によって、平成15年ごろより電子政府構築計画の一環として推進されている。EAは現状（As Is）、理想図（To Be）、移行計画（Target）の姿をユーザ部門にも分かりやすいように示すことによって、ユーザ部門自らが必要な業務と情報を明確にすることができる手法であり、以下の4つの分類体系に整理されている。

〈EAの体系〉

① 政策・業務体系

a．業務説明書……システムの目的・機能、情報システムの管理・運用体制を明らかにする。

b．機能情報関連図……システムの機能と情報の流れを明確化する。

c．業務流れ図……システム機能を利用する人、組織等の業務主体、順序並びに当該業務主体及び順序において、やり取りする情報及び成果物を明確にする。

d．情報体系整理図（UML Class Diagram）……情報の関連及び構造を明確化する。

② データ体系

a．実体関連図……論理的なデータ構造を明確にする。

b．データ定義表……物理的なデータ構造を明確にする。

③ 適用処理体系

a．情報システム関連図……情報システム間でやり取りされる情報の種類と方向を明確にする。

b．情報システム機能構成図……機能の構成を明確にする。

④ 技術体系

a．ハードウェア構成図……情報システムを構成するサーバ、クライアント等のCPU、メモリ、ハードディスク等の機器構成を明らかにする。

b．ソフトウェア構成図……情報システムを構成するサーバ、クライアント等に搭載するソフトウェアを明らかにする。

c．ネットワーク構成図……情報システムを構成するサーバ、クライアント等の機器の論理的及び物理的な接続関係を明確にする。

1．全体最適化

1．1　全体最適化の方針・目標

(5) システム化によって生ずる組織及び業務の変更の方針を明確にすること。

1 主　旨

全体最適化計画では、情報システムの（再）構築と同期して行われる組織及び業務の新設、改変及び廃止の方針を明確にする必要がある。

2 着 眼 点

(1) 組織及び業務の変更の方針は、経営の方針との整合性を検討していること。

(2) 情報システムの（再）構築と同期して行われるべき組織及び業務を明確にしていること。

(3) 組織及び業務の変更の方針を組織体の長が承認していること。

3 関連事項

(1) 情報システムの開発（新規及び再開発）、改修に伴う組織及び業務の検討事項の例

① 組織の統廃合、新設

② 業務分掌の変更

③ 業務の管理体系・管理区分の変更

④ 社内規定等の変更

(2) 組織変更の例

① 経理・会計部門の統廃合、アウトソーシング

② 発注・在庫管理部門の統廃合

③ マネジメント組織の変更

④ 情報システム運用業務体制の変更

⑤ エンドユーザ支援部門の設立

⑥ 社内機器管理部門の新設

(3) 業務変更の例

① オンライン化による報告書作成業務の廃止

② ペーパレス化に伴う台帳・帳簿作成業務の廃止

③ データ保管室の設置に伴うライブラリ管理業務の新設

④ 社内メールシステム、ワークフローシステムの構築による報告・連絡手順の変更

⑤ EUC による定型出力業務の廃止

⑥ 情報化投資にかかわる権限の改善（分散化、集中化）

(4) 業務改善との関係

全体最適化を検討する際に、その手法は種々であり、業務の改革から着手し、業務改善のツールとしてのシステム化が実行される場合と、システム統合から着手し、業務も統合される場合がある。いずれにしても、システムのみが導入されるのではなく、組織、業務も見直すことによって、有効性、効率性が達成されることに留意する。

1．全体最適化

1．1　全体最適化の方針・目標

(6) 情報セキュリティ基本方針を明確にすること。

1 主　旨

不正防止、機密保護、プライバシー保護等は、健全な経営活動推進の基盤であるため、情報セキュリティ対策の方針を全体最適化計画で明確にする必要がある。

2 着眼点

(1) 全体最適化計画では、保護すべき情報資産を明確にしていること。

(2) 情報資産に係るリスクを幅広く検討していること。

(3) 業務の重要度及びリスクに応じて、情報資産のセキュリティ対策の方針を明確にしていること。

(4) 情報資産のセキュリティ対策の方針を関係者に周知徹底し、理解させていること。

(5) 個人情報保護等法令等を検討していること。

3 関連事項

(1) 全体最適化計画のセキュリティ対策を監査するに当たっての留意事項

① 要因

ａ．自然災害……地震、火災、雷、水害等

ｂ．システム障害……機器障害、プログラムエラー、回線故障、異常輻輳等

ｃ．不正・不法行為……データの漏えい・破壊、改ざん、不正アクセス、機器の持出し等

② 対策の態様

ａ．障害の回避、未然防止

ｂ．ダメージの軽減、障害発生の影響の最小化と迅速な回復

ｃ．障害原因の追究と再発防止

ｄ．リスクの移転、保険への加入

③ 対策の内容

ａ．物理的対策（耐火構造、耐震・免震構造、消火設備設置等）

ｂ．技術的対策（アクセスコントロール機能、機器の二重化、データのバックアップ、監査証跡等）

ｃ．管理的対策（運用管理規程等の整備、管理体制の確立、意識改革と教育等）

(2) システム監査と情報セキュリティ監査の関連

① 並立する監査

経済産業省のシステム監査制度では、システム監査と情報セキュリティ監査とはその目的が

異なり、並立するものであるとしている。

② システム監査と情報セキュリティ監査の目的の違い

システム監査は、企画、開発、運用、保守という情報システムのライフサイクルに従って、特に情報システムの構築、運用の全体最適化を目的とした監査であるのに対して、情報セキュリティ監査は、情報資産のライフサイクルに従って、情報システム以外の部分も対象として情報セキュリティ確保のための管理・運用を有効に行うことを目的とした監査である。

③ システム監査と情報セキュリティ監査の背景の違い

わが国の状況を見れば、システム監査が元来内部監査による助言型監査を前提として成立してきたものであるのに対し、情報セキュリティ監査は、情報セキュリティの確保の認識・評価・可視化の必要性という社会的要請から、当初は助言型監査中心の市場になることを想定しているものの、最終的には、保証型監査を中心に行われることを前提として成立している。

④ システム監査における情報セキュリティ関連の監査項目のあり方

システム監査においても情報セキュリティ確保の観点からの監査項目を、その一環として加えていくことはあり得るが、情報セキュリティ確保の観点からの監査は、基本的には情報セキュリティ監査制度を基軸として運用を行っていくことが望ましい。なお、システム監査において情報セキュリティ確保の観点からの監査項目を加えて行う場合においては、情報セキュリティ管理基準を活用して実施することが適切である。

１．全体最適化

１．２　全体最適化計画の承認

(1) 全体最適化計画の立案体制は、組織体の長の承認を得ること。

1 主　旨

全体最適化計画は、経営戦略に基づき情報システムの中長期計画として策定する必要があるため、立案体制を組織的に確立し、組織体の長が承認する必要がある。

2 着 眼 点

(1) 情報システムに係るすべての部門が全体最適化計画の立案に参画していること。

(2) 参画者の役割を明確にしていること。

(3) 能力、経験等を考慮して参画者を選定していること。

(4) 立案体制を組織体の長が承認していること。

3 関連事項

(1) 立案体制を確立するに当たっての考慮点

① 最高経営責任者の支援を得ること。

② 立案体制の責任者として統括役員に適切な人材を得ること。

③ 適切なメンバーの選定とトップダウンの体制作りを行うこと。

④ 全体最適化計画の策定活動を、毎年行われる全社的な経営計画策定体系の一環として位置付けること。

⑤ 立案体制の形態を明確にし、立案体制の責任と権限を明らかにすること。

⑥ 立案体制は、経営方針の変更、情報環境の変化等に応じて適宜見直すこと。

(2) 立案体制への参画部門と役割の例

① 統括役員	全体最適化計画策定の最高責任者であり、立案体制の活動の承認、指示、支援者である。
② リーダー	全体最適化計画の実施・推進の責任者であり、進捗管理、メンバーのモラール維持、他部門責任者との調整を行う。
③ メンバー	ユーザ部門と情報システム部門の責任者が参加する。ユーザ部門の責任者は、業務に精通している者、情報システム部門の責任者は、企画、開発、運用、保守の各業務の情報システム環境を把握している者が望ましい。

1．全体最適化

1．2　全体最適化計画の承認

(2) 全体最適化計画は、組織体の長の承認を得ること。

1 主　旨

経営戦略に基づいて組織体全体で整合性かつ一貫性を確保した情報化を推進するため、全体最適化計画は、組織体の長が承認する必要がある。

2 着 眼 点

(1) 全体最適化計画を組織体の長が承認していること。

(2) 全体最適化計画策定のルールが定められ、その中に承認手順が含まれていること。

3 関連事項

(1) 全体最適化計画策定のルールで定めるべき事項の例

① 立案体制
② 策定時期
③ 策定手順
④ 検討範囲・検討事項
⑤ 全体最適化計画の提出先
⑥ 承認手順
⑦ 見直しの手順

(2) 全体最適化計画の記載項目の例

① 経営環境
② 業務モデルの定義
③ 現行システムの評価
④ 情報システム体系
⑤ 個別システムの構成
⑥ 個別システムの開発優先順位
⑦ 情報システム基盤の整備計画
⑧ 中期の開発計画
⑨ 費用対効果
⑩ 推進体制

(3) 全体最適化計画策定の手順の例

① 経営環境の理解	外部環境：景気の動向、業界の動向、法令の改正、新技術の動向等 内部環境：組織体の目的、経営戦略、経営目標、経営環境、経営の実態等の把握
② 業務モデルの作成	組織体の全体業務と使用される情報の調査及び業務間の関連、業務と情報との関連、情報間の関連の理解、業務の標準化、統合化
③ 情報システム体系の策定	組織体全体の情報システムを構成する個別システム体系とデータベースモデルの作成、データの標準化、システム統合
④ インタビュー	経営トップ層、各部門長に対する経営方針、経営目標、各関係部門における問題、情報化ニーズの把握等の意見聴取
⑤ 情報システム開発課題の整理	経営上、業務上の情報ニーズに対する情報システムの開発課題としての整理及び情報システム開発の必要性の明確化
⑥ 中長期計画の策定と文書化	全体最適化計画策定結果のアウトプット

(4) 全体最適化計画の承認の方法の例

① 全体最適化計画書に対する承認の印（印鑑、サイン、電子署名等）

② 経営会議等での全体最適化計画承認時の議事録

③ 経営者層及び関係者の承認の文書

④ 関係者に対する意見交換会、計画内容の確認、報告会等

1．全体最適化

1．2　全体最適化計画の承認

(3) 全体最適化計画は、利害関係者の合意を得ること。

1 主　旨

円滑に運用できる全体最適化計画とするために、利害関係者の合意を得る必要がある。

2 着 眼 点

(1) 利害関係者の範囲が明確に定義されていること。

(2) 全体最適化計画策定のルールが定められ、その中に利害関係者の合意の手順が含まれていること。

(3) 利害関係者による合意を書面として残していること。

3 関連事項

(1) 利害関係者の範囲の例

① 経営者層

② 情報システム部門の責任者

③ 各ユーザ部門の責任者

④ 財務・経理部門の責任者

⑤ 株主等の出資者

⑥ 主要顧客

(2) 利害関係者の合意の手順の例

① 全体最適化計画原案の作成

② 原案に対する利害関係者からの意見収集

③ 組織体の長及び主要利害関係者への個別説明

④ 各利害関係者からの意見の反映

⑤ 定例会等での承認

１．全体最適化

１．３　全体最適化計画の策定

(1) 全体最適化計画は、方針及び目標に基づいていること。

1 主　旨

経営戦略に基づいて組織体全体で整合性かつ一貫性を確保した情報化を推進するため、全体最適化計画は、方針及び目標に基づいて策定する必要がある。

2 着 眼 点

(1) 全体最適化計画の前文的位置に、方針及び目標が簡潔かつ明確に記されていること。

(2) 全体最適化計画の重要目標達成指標（KGI：Key Goal Indicator)、重要業績評価指標（KPI：Key Performance Indicator）が定められていること。

(3) 全体最適化計画の各事項について、方針及び目標との関連がとれていること。

(4) 目標指標のモニタリング方法が定められていること。

(5) 技術採用の方針が定められていること。

3 関連事項

(1) 重要目標達成指標と重要業績評価指標

① 重要目標達成指標：最適化計画のゴールとなる目標が最終的に達成されたかを評価する。

② 重要業績評価指標：最適化計画実施の各時点において、重要目標達成指標の達成を可能にする活動がどの程度実施されているかを評価する。

(2) 重要目標達成指標の例

① システム費用の削減

② システム部門の品質指標

③ システム資源の効率化（資源使用率等）

④ ユーザ部門の費用の削減

⑤ ユーザ部門のIT利用率向上

(3) KPIの例

① システム機能の利用頻度

② システムの可用性の状況

③ 既成パッケージソフトウェアや汎用技術の採用の割合

④ ユーザ部門からのクレーム、問合せの数

⑤ 教育講座の受講率

⑥ 担当者からの提案件数

⑦ ユーザ部門からの問合せに対するレスポンスの平均時間

(4) 技術採用方針のポイントの例

① 組織体の内外における採用実績

② 技術の発展性、主流性、標準性

③ 既採用技術との親和性、整合性、接続性

④ 非排他性、知的所有権における制約の有無

⑤ 技術の革新性とその効果

⑥ 初期費用、維持費用（バージョンアップ等の費用）

⑦ 技術提供元の経営状態

⑧ 技術者の確保の容易性等

1．全体最適化

1．3　全体最適化計画の策定

(2) 全体最適化計画は、コンプライアンスを考慮すること。

1 主　旨

関連法規、業界の自主基準等に違反しないよう、全体最適化計画は、コンプライアンスを考慮して作成する必要がある。

2 着眼点

(1) 最適化計画の策定時点で確定している考慮すべき法規等をすべて洗い出していること。

(2) 今後改定・新設等が予想される法規等への対応を講じていること。

(3) 考慮すべき法規等を定期的及び必要に応じて見直すことを定めていること。

(4) 全体最適化計画に対するコンプライアンスの面からのレビューに、法務部等法律の専門家が参画していること。

(5) コンプライアンスに関するリスクの対応方法を講じていること。

(6) 組織体の構成員に対するコンプライアンス徹底の方法を定めていること。

3 関連事項

(1) 考慮すべき法規等の洗い出しのポイント

① 組織体の事業分野に関する国内法規及びグローバルな法規の網羅性

② 事業分野に依らない国内法規及びグローバルな法規の網羅性

③ 業界内の規制

④ 株式市場等の規制

⑤ 公序良俗

⑥ 消費者団体等の動向

⑦ 組織体内における規程・ルール

(2) コンプライアンスに関するリスクの対応方法の例

① リスクアセスメントの実施

② 責任者の設置

③ 監督官庁等からのノンアクションレターの取得

④ 組織体の構成員に対するコンプライアンス違反時の処罰の設定

⑤ コンプライアンス違反が内部的又は外部からの指摘によって判明した場合の、広報等の手順の定義

1．全体最適化

1．3　全体最適化計画の策定

(3) 全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。

1 主　旨

情報化の費用対効果を高め、実効性のあるものとするために、全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にする必要がある。

2 着 眼 点

(1) 情報化投資の方針を明確にしていること。

(2) 確保すべき経営資源を明確にしていること。

(3) 方針に従った投資が行われることを確認する手順を定めていること。

(4) 経営資源に不足が生じた場合の対応手順を定めていること。

3 関連事項

(1) 情報化投資の方針として定める事項の例

① 経営戦略とのリンク付けのルール

② 経営業績とのリンク付けのルール

③ 競合他社の投資規模の考慮の方法

④ 予測される法改正等の考慮の方法

⑤ 偶発的な環境変化への対応方法

⑥ 新技術採用のルール等

(2) 確保すべき経営資源として定める事項の例

① 人的資源

a．確保すべき要員総数

b．スキル種別、スキルレベル

c．スキル種別、スキルレベルごとの要員数

d．流動性（異動の容易性、遠隔地への赴任等の容易性）

e．離職率の予測等

f．不足する場合の確保の手立て（採用、育成、外部委託等）

② 物理的資源

a．確保すべき情報システムの設備

b．災害対策設備

c．不足する場合の確保の手立て（外部委託等）　等

③　金銭的資源

a．確保すべき短期的資金、中長期的資金

b．投資回収の予測

c．金利等の予測

d．不足する場合の確保の手立て（資金調達方法、繰延支払いの方法等）　等

④　情報資産

a．顧客情報（個人・法人を特定する情報、属性、信用情報、取引履歴等）

b．マーケティング情報

c．人事情報

d．クレーム情報　等

1．全体最適化

1．3　全体最適化計画の策定

(4) 全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。

1 主　旨

全体最適化計画は、計画採択の判断の基準及び修正を検討すべき判断の基準を明確にするため、投資効果及びリスク算定の方法を示す必要がある。

2 着眼点

(1) 投資効果及びリスクの算定方法が明確に定義されていること。

(2) 計画の修正の検討が必要となる閾値（いきち）が定義されていること。

(3) 投資効果及びリスク算定が適正に行われることをモニタリングすることを定めていること。

3 関連事項

(1) 算定方法として定義すべき事項の例

① 算定のタイミング

② 対象範囲

③ 算定の根拠となる入力データ、算定の手順・方式

④ 算定実施者

⑤ 算定結果の承認者

(2) 投資効果及びリスク算定の結果の活用の例

① 計画の修正

② 組織体の責任者又はユーザ部門の責任者によるリスク受容の確認

③ リスクヘッジの方法の追加

(3) 投資効果算定に関連する手続のタイミングの例

① 全体最適化計画で投資効果を算定

② 個別計画の着手時点で再度算定

③ システム稼動後、一定期間をおいて定期的に実績値を計算

④ 当初の投資効果に満たない場合には、運用コストの削減、運用の打切り、効果を向上させるための施策の追加を検討

⑤ 結果を他の個別施策及び全体最適化計画にフィードバック

１．全体最適化

１．３　全体最適化計画の策定

(5) 全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。

1 主　旨

組織体における情報システム相互の整合性を保持し、システム構築及び運用を効率的かつ高品質・均質な品質で行うため、システム構築及び運用のための標準化の方針及び品質の方針を明確にする必要がある。

2 着 眼 点

(1) システム構築及び運用のための標準化及び品質の方針を明文化していること。

(2) 標準化及び品質の方針について周知徹底すべき関係者及び関係者の理解を確認する方法を定めていること。

(3) 標準化及び品質の方針に基づいて明文化すべき企画、開発、運用及び保守業務にかかわる標準及びその標準について周知徹底すべき範囲を定めていること。

(4) 環境の変化に対応して標準を見直すことを定めていること。

3 関連事項

(1) 標準化の目的の例

① 均質な成果物の実現

② 品質・信頼性の向上

③ 保守時の正確性、効率性の向上

④ 費用対効果の向上

⑤ 情報システム資源及びデータ等の共有化

⑥ ユーザの操作性の向上

(2) 標準化に関する関係部門と標準化が関係する業務の例

① ユーザ部門	端末管理、情報システム運用、教育等
② 企画部門	経営企画、情報システム化企画、情報システム開発、文書管理等
③ 開発部門	情報システム開発、外部委託依頼、ドキュメント管理等
④ 運用部門	情報システム運用、外部委託依頼、教育、ドキュメント管理等
⑤ 保守部門	情報システム保守、ドキュメント管理等

(3) 標準を定める事項

① ユーザ部門	媒体管理方法、端末利用マニュアル、障害報告規約等
② 企画部門	全体最適化計画作成要領、ドキュメント記述要領、プロジェクト管理手順等
③ 開発部門	システム設計マニュアル、プログラム設計マニュアル、プログラミングマニュアル、ネーミングマニュアル、テストマニュアル、画面レイアウト設計マニュアル等
④ 運用部門	出力表示メッセージ対応マニュアル、障害時対応規約等
⑤ 保守部門	プログラム変更手順マニュアル、プログラム管理手順マニュアル等

(4) 標準に影響を与える情報環境の変化の例

① 情報システム形態の変更（オープン化、分散化、集中化、ネットワークの拡大等）

② ソフトウェア(OS 等のシステムソフトウェア、DBMS 等のミドルウェア)、ハードウェア、ネットワークの変更

③ 開発手法、開発支援ツールの変更

④ 端末、ワークステーション等の形態の変更（専用端末から PC へ、等）

⑤ 組織、職務分担の変更

1．全体最適化

1．3　全体最適化計画の策定

(6) 全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。

1 主　旨

経営課題の重要性及び緊急性を反映し、開発資源を有効に活用するため、全体最適化計画は、個別計画の優先順位及び順位付けのルールを明確にする必要がある。

2 着 眼 点

(1) 個別計画の優先順位の決定方法をルールとして定めていること。

(2) 各個別計画が目的としている経営課題の重要性及び緊急性を明確にしていること。

(3) 個別計画の着手の順序、資源配分、開発の期間は、業務との整合性を考慮して検討していること。

(4) 個別計画の優先順位の決定理由を説明すべき関係者を明確にしていること。

(5) 必要に応じて個別計画の優先順位を見直すことを定めていること。

(6) 決定された優先順位に基づいて個別計画が着手されることをモニタリングするように定めていること。

3 関連事項

(1) 個別計画の優先順位の決定方法の手順の例

① 個別計画評価項目の抽出

a．経営戦略遂行に対する貢献度

・競争の優位性の確立

・経営情報の提供と経営意思決定の支援

・計画能力、予測能力の精度向上

・管理統制能力の向上

・ビジネスサイクルの短縮

・省力化、時間節約、生産性向上、品質向上

・組織間コミュニケーションの向上

b．情報基盤、資源継承、拡張性に対する貢献度

・情報の機密保持性の向上

・情報資産の保守費用の低減

・開発生産性の向上

c．情報活用能力の促進効果

・情報システムの運用性の向上
・情報加工処理能力の向上
・情報の収集能力の向上
・情報の鮮度更新能力の向上
・情報の交換能力の向上

② 定量的、定性的項目の選択と定量化

a．費用分析
b．効果分析
c．経済性分析

(2) 個別計画の優先度の検討に当たっての考慮事項

① 経営戦略、情報戦略における緊急度
② ユーザ部門のニーズ、顧客のニーズ
③ 技術的実現可能性
④ 外部の情報システムとの開発順序との整合性
⑤ 投資可能予算額との整合性
⑥ 開発体制、要員

１．全体最適化

１．３　全体最適化計画の策定

(7) 全体最適化計画は、外部資源の活用を考慮すること。

1 主　旨

全体最適化計画において資源面の制約事項を排除するためには、組織体内部の資源だけでなく、外部資源の活用を考慮する必要がある。

2 着眼点

(1) 内部資源の量及び質を正しく把握して検討を行っていること。

(2) 内部資源のコストを常に外部資源のコストと比較していること。

(3) 代替案の検討において資源の不足を制約事項とする際には、外部資源の採用を不可とする理由が明確にされていること。

3 関連事項

(1) 外部資源の活用が有効となる例

① システム設計、開発の外部委託	システム設計、開発の人的資源が組織体内に不足する場合、又は戦略的にそのような資源を組織体内にもたない場合
② 総合プロジェクトマネジメントの外部委託	複数の開発案件の設計、開発を外部に委託する際に、それらを統括管理する人的資源が組織体内に不足する場合
③ システム監査人	プロジェクトを第三者的、客観的に評価し、助言を受けることで、プロジェクトを確実に成功裏につなげたい場合
④ システムオペレーションの外部委託	システムの運用を行う人的資源が組織体内に不足する場合、又は戦略的にそのような資源を組織体内にもたない場合
⑤ ヘルプデスクの外部委託	ユーザ部門からの問合せに対応する資源が組織体内に不足する場合、又は戦略的にそのような資源を組織体内にもたない場合
⑥ 機器設置施設の外部委託	高速回線、耐震設備、電源設備等機器設置場所としての物理的資源が組織体内に不足する場合、又は戦略的にそのような資源を組織体内にもたない場合
⑦ 機器等リース	機器等を購入するための金銭的資源を繰り延べる場合
⑧ 機器とオペレーションを含むアウトソーシング	機器、機器設置場所、オペレーションに必要な資源を一括して外部に求める場合
⑨ アプリケーションサービスの外部委託	アプリケーションの開発、運用、保守を一括して外部に求める場合
⑩ ユーザ部門の機能を含む外部委託	組織体の部分的な業務機能をシステムとともに外部に求める場合（例：コールセンター、製造、セールス、マーケティング）

１．全体最適化

１．４　全体最適化計画の運用

(1) 全体最適化計画は、関係者に周知徹底すること。

1 主　旨

全体最適化計画を実行性の高いものとするため、すべての利害関係者に周知徹底し、理解させる必要がある。

2 着 眼 点

(1) 全体最適化計画を周知徹底すべき関係者のリストが作成されていること。

(2) 全関係者に全体最適化計画を周知徹底していること。

(3) 周知徹底の方法をルールとして定めていること。

(4) 全関係者に全体最適化計画を周知徹底し、理解させたことを確認していること。

3 関連事項

(1) 全体最適化計画を周知徹底すべき関係者の例

① 経営管理者層

② 情報システム部門の責任者

③ ユーザ部門の責任者

④ 株主、出資者、その他の利害関係者

(2) 周知徹底等の方法の例

① 経営会議での報告

② 関係者への回覧、部門会議

③ 組織体内のイントラネット等への掲示（必要によってアクセス制限を行う）

④ IR（Investor Relations）

1．全体最適化

1．4　全体最適化計画の運用

(2) 全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。

1 主　旨

全体最適化計画を硬直化・陳腐化させないために、定期的な見直し及び経営環境等の変化に対応した見直しを行う必要がある。

2 着眼点

(1) 全体最適化計画は定期的及び必要に応じて見直されていること。

(2) 全体最適化計画の見直しの際にはその理由を明確にしていること。

(3) 全体最適化計画の変更を組織体の長が承認していること。

(4) 全体最適化計画を定期的及び必要に応じて見直すこと、並びに見直しの手順がルールとして定められていること。

(5) ルールを遵守した見直しが行われていることをモニタリングしていること。

3 関連事項

(1) 全体最適化計画の見直し時期の例

① 経営戦略の策定時又は変更時

② 個別計画からのフィードバック時

③ 期ごとの最適化計画の妥当性の確認時

④ 情報環境の大幅な変更時

(2) 情報システムの環境に影響を与える要因の例

① 情報処理技術の進展

a．ソフトウェア（新機能、効率向上、保守性の向上等）

b．ハードウェア（新機能、性能向上機器の出現等）

c．ネットワーク（新機能、性能向上機器の出現等）

d．開発、運用環境（開発方法論、新開発手法、新運用管理手法、自動化等）等

② 経営方針の変化

a．業務の統合

b．新規業務への進出、既存業務からの撤退

c．予算の変更

d．組織改変　等

③ 経営環境の変化

a．顧客のニーズ動向
b．業界動向
c．政策動向
d．グローバルな政治・経済の動向　等

④　法制度の変化
a．法規制
b．法の規制緩和
c．法改正　等

2．組織体制

2．1　情報システム化委員会

(1) 全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。

1 主　旨

経営戦略に基づいた情報システムの全体最適化を実現するため、経営トップ（執行機関）は、情報戦略の実現を推進する情報システム化委員会を設置し、委員会の使命と権限、責任を明確にする必要がある。

2 着 眼 点

(1) 情報システムの全体最適化を推進する情報システム化委員会を設置していること。
(2) 情報システム化委員会は、必要な組織の権限者によって構成すること。
(3) 情報システム化委員会の位置付けを明確にし、関係者の合意を得ていること。
(4) 情報システム化委員会には、適切な権限及び責任を与えること。
(5) 情報システム化委員会の構成は、情報戦略、業務機能及び組織の変更に伴って見直しをすること。

3 関連事項

(1) 組織上の位置付けを確認する方法
　① 情報システム化委員会の位置付けは、組織体制図に明確に示されていること。
　② 情報システム化委員会の設置にかかわる通達、規程があること。
　③ 情報システム化委員会のメンバーは、経営トップが任命していること。
　④ 情報システム化委員会の使命と目的を組織内に周知徹底させること。
　⑤ 情報システム化委員会の名称は、企業の状況によって異なるもので、固定的なものではない。
(2) 情報システム化委員会に参画すべきメンバー
　① 経営トップ
　② 企画部門の責任者
　③ ユーザ部門の責任者
　④ 情報システム部門（開発、運用、保守等）の責任者
　⑤ 経理部門責任者　等
(3) 情報システム化委員会の設置
　① 情報システム化委員会の設置は、組織の規模、業務内容に応じて、適切に策定する必要がある。策定は、委員会の役割、責任、規模、選出組織及び名称等である。

② 大規模組織においては、全社レベルの全体最適化を実現、推進する情報システム化委員会を設置するとともに、全体最適化の下に各部門、事業所単位の最適化を実現、推進する部門の情報システム化委員会を設置することが望ましい。

小規模組織において情報システム化委員会としての編成が困難な場合は、経営トップ、情報システムの開発、運用等の責任者、及び利用者が連絡を密にできる体制を維持し、調整事項の発生に応じた検討を行うことが必要である。

２．組織体制

２．１　情報システム化委員会

(2) 委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。

1 主　旨

全体最適化計画に基づいた情報システムの企画、開発、運用、保守を実施するため、情報システム化委員会は、全社の情報化活動を総攬する権能と責任を有し、不適切な状況に対しては、是正のための適切な措置を講ずる必要がある。

2 着眼点

(1) 情報システム化委員会がモニタリング対象とする情報システムの活動を明確にすること。

(2) ビジネス環境の変化に即応できるように、適切かつ適時のモニタリングを行う仕組みを構築すること。

(3) 障害、事故、プロジェクト進捗、予算等のモニタリング項目を明確にしていること。

(4) モニタリングによって発見された不具合等に対して、適切な対応を行うこと。

(5) モニタリングによって発見され是正措置を施した施行に関して、必要な場合、全体最適化計画への対応、反映を行うこと。

3 関連事項

(1) モニタリングの方法

① 情報システム化委員会が、情報システム投資にかかわる計画の審査、決定に関与することの明確化

② 運用段階等における自動的な稼動状況ログの分析

③ 開発、運用及び保守部門等からの定期的な報告書の提出

④ 情報システムの開発、運用及び保守状況のレビュー会議の開催

⑤ 外部監査、外部コンサルタントの活用

(2) モニタリングの観点

情報システム化委員会がモニタリングを行う観点の例は、次のとおりである。

① 全体最適化計画との整合性

② 個別の開発計画との整合性（特に、進捗状況、品質の状況、予算に対する実績と見通し）

③ 経営戦略の変更、社内外環境変化への対応

(3) 是正措置の方法

① 情報システム化委員会が、トラブル発生時に備えて対策を講じ、発生時にはこれを適時に認識し、回復・修正作業を行う。

2．組織体制

2．1　情報システム化委員会

(3) 委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。

1 主　旨

変化する情報技術動向に適切かつ迅速に対応し、組織体全体としての整合性のとれた情報技術基盤を確立しリスクを低減させるため、情報システム化委員会は、技術採用指針を明確にする必要がある。

2 着眼点

(1) 組織体として関連のある情報技術分野を明確にしていること。
(2) 情報技術の最新動向等収集する範囲、部門を明確にしていること。
(3) 技術採用指針を文書化し、定期的に見直すこと。
(4) 必要に応じて、適切で客観かつ公正な外部専門家の助言を得て、これを技術採用指針に反映させること。

3 関連事項

(1) 技術採用指針を明確にする理由

組織体の情報技術基盤は企業活動の基礎であり、技術動向の判断を誤ると、組織体運営の効率性、経済性に影響する。

(2) 技術採用指針の内容
　① 情報システムのアーキテクチャ（メインフレーム、オープンシステム、Web アプリケーション等）
　② ネットワークプロトコル、伝送媒体、伝送方式の採択指針
　③ OS、ミドルウェアの採択指針
　④ データアーキテクチャ（XML、メタデータレポジトリ）の構築指針
　⑤ ビジネスコンポーネントの構築指針
(3) 諸規制の強化、緩和にかかわる情報、予測
(4) 技術標準に対する対応
　① デファクトスタンダード（事実上の業界標準）の採用
　② デジュリスタンダード（公的権威に基づく標準）の採用
(5) 制約条件の明確化
　① 既存インフラとの整合性
　② ハードウェア等のリース契約内容、条件
　③ ネットワークサービス契約内容、条件

2．組織体制

2．1　情報システム化委員会

(4) 委員会は、活動内容を組織体の長に報告すること。

1 主　旨

情報システム化委員会は、経営活動の意思決定に資するため、その活動内容を適時に組織体の長に報告する必要がある。

2 着 眼 点

(1) 情報システム化委員会の活動を組織体の長に報告する手続を定めていること。
(2) 情報システム化委員会の活動内容を報告書として作成していること。
(3) 報告書のレビュー会議を開催していること。
(4) 報告書を組織体の長に提出し、報告していること。

3 関連事項

(1) 活動報告を受けた組織体の長は、以下の対応が必要である。

情報システム化委員会からの報告を受けて、その活動をモニタリングし、必要な是正措置等を講ずる必要がある。

① 全体最適化計画の見直し
② 予算の再検討
③ 組織変更・業務分掌の変更

(2) 活動内容の報告書の内容

① 情報システム化の資源の状況
② 情報システム化の制約条件
③ 情報システム化対象業務の状況

(3) 報告のタイミング

① 定例
② 随時（環境変化）

2．組織体制

2．1　情報システム化委員会

(5) 委員会は、意思決定を支援するための情報を組織体の長に提供すること。

1 主　旨

情報システム化委員会は、全体最適化計画にかかわる環境変化、技術動向、開発、運用、保守の実施状況を適切かつ迅速に経営方針に反映させるため、経営活動の意思決定を支援する情報を組織体の長に適時提供する必要がある。

2 着眼点

(1) 情報システム化委員会は、情報化投資の是非の判断に資する情報を組織体の長に提供していること。

(2) 代替案を評価する判断根拠、基準を適切に提供していること。

(3) 全体最適化実現のための PDCA（Plan-Do-Check-Action）サイクルを確立していること。

(4) 事実と意見を区別して提供していること。

3 関連事項

(1) 提供のタイミングと方法

① タイミング：定例、随時

(2) 意思決定のための情報の例

① 外部関係

・情報システムの新しい活用事例

・自組織に関係の深い情報技術の動向

・同業他社の事例

・法制度、業界の動向　等

② 内部関係

・経営方針の見直しに伴う全体最適化への影響

・個別開発における問題・課題（スケジュール遅延、低品質、予算超過等）

2．組織体制

2．2　情報システム部門

(1) 情報システム部門の使命を明確にし、適切な権限及び責任を与えること。

1 主　旨

適時に適切な情報システム機能を遂行するために、組織体の長は情報システム部門の役割、機能を明確にするとともに、適切な権限と責任を与える必要がある。

2 着眼点

(1) 情報システム部門の使命、役割が明文化され、関係者の承認を得ていること。

(2) 情報システム部門は、ユーザ部門から独立していること。

(3) 情報システム部門は、情報化投資を集約して管理していること。

(4) IT ガバナンスを実現していること。

① 情報システム部門の使命と目的を組織内に周知徹底していること。

② 特定の IT ベンダに依存していないこと。

3 関連事項

(1) 情報システム部門の使命、機能を明確にする際の留意事項は、次のとおりである。

① ユーザ部門との使命、機能の区分を明確にする

② 業務・システムのオーナシップの方針

③ データのオーナシップの方針

④ エンドユーザコンピューティング（EUC）の方針を明確にする

(2) IT ガバナンス確立の視点は、経営戦略とそれに基づく全体最適化計画の策定の仕組みの確立と、以下の①～③に基づく。

① 情報パフォーマンスマネジメントの確立：それぞれの情報システムが経営目標に準拠し、期待される効果、効率を達成する仕組みの確立と実施、モニタリング

② 情報リスクマネジメントの確立：情報システムの障害、情報セキュリティの侵害等への対策と事業継続計画の策定、維持の仕組みの確立と実施、モニタリング

③ 情報コンプライアンスマネジメント：情報システムにかかわる法制度、業界ルール及び社内諸規程等に準拠、遵守する仕組みの確立と実施、モニタリング

2．組織体制

2．2　情報システム部門

(2) 情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。

1 主　旨

全体最適化計画を効果的に、効率的に実現するため、情報システム部門は、自社内の資源とともに外部資源も適切に活用し、組織体の情報化ニーズや投資効果に見合った体制にする必要がある。

2 着眼点

(1) 情報システム部門は、作業効率と品質の向上、及び情報セキュリティの確保の観点から適切な職務の分離、及び専門化の推進を行っていること。

(2) 情報システム部門は、迅速かつ業務実態に即した承認を実現するため、適切な権限付与を行っていること。

(3) 情報システム部門は、業務活動の状況に即した物理的セキュリティ、論理的セキュリティ、及び環境のセキュリティを適切に確保していること。

(4) 情報システム部門は、業務の活動に効果的な外部委託先を選定し、適切に管理、監督していること。

3 関連事項

(1) 職務の分離の例

① 開発と運用

② ユーザ部門と提供部門

③ データ入力部門と検証部門

(2) 職務の分離における留意点

職務の分離は、情報システムの特性、規模に応じて適切に行うことが必要である。関連する組織、要員が小規模な場合には、役割を細分化し、それぞれの役割に応じた要員を個別に確保することは困難である。このような場合には、複数の業務を特定の要員が担当することになるが、第三者によるチェック機能、あるいはシステム的なログの採取とその分析等を通して、情報システムのセキュリティの確保、品質の維持が実現することが考えられる。

(3) 情報システム部門の外部委託

情報システム部門自体を外部委託する場合は、情報システム部門の管理の方針、責任者を明確にする必要がある。(「VI. 共通業務　5. 委託・受託」を参照)

2．組織体制

2．3　人的資源管理の方針

(1) 情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。

1 主　旨

組織体は全体最適化の目標を達成するために、自組織内における情報技術に関する人的資源の現状を適切に把握し、今後必要とされる人材、能力を明らかにする必要がある。

2 着眼点

(1) 自組織内のスキルズインベントリを文書化し、定期的に更新していること。

(2) 人材のスキルズインベントリは、採択している技術指針と整合性がとれていること。

3 関連事項

(1) スキルズインベントリ作成の参考資料

① IT スキル標準

② コンピテンシーマネジメント

2．組織体制

2．3　人的資源管理の方針

(2) 人的資源の調達及び育成の方針を明確にすること。

1 主　旨

組織体の情報化に必要な人材の現状及び将来計画に従って、人的資源の採用、育成の方針を明文化し、これを周知徹底する必要がある。

2 着眼点

(1) 情報化人材の採用方針、計画を明確にしていること。

(2) 外部資源の調達の方針を明確にしていること。

3 関連事項

(1) 人的資源調達の方法

① 派遣

② 外部委託

③ 人材スカウト

(2) 人的資源育成の方法

① OJT

② 社内教育

③ 資格取得の奨励

④ 外部研修機関の利用

⑤ ｅラーニングの利用

3．情報化投資

(1) 情報化投資計画は、経営戦略との整合性を考慮して策定すること。

1 主　旨

情報化投資を経営課題の解決に役立たせるため、経営に与える利益効果、業務処理の改善等の全体最適化の観点から、経営戦略と整合性をもった情報化投資計画を策定する必要がある。

2 着眼点

(1) 情報化投資の対象範囲とその区分が定められていること。

(2) 情報化投資の有効性を評価する指標及び目標が定められ、それらが経営戦略の指標及び目標と整合がとれていること。

(3) 経営戦略の策定の責任者が情報化投資計画を承認していること。

(4) 情報化投資の優先順位付けは、全体最適化の観点を踏まえて、定量的な投資価値等に基づいて行われ、関係者の合意を得ていること。

3 関連事項

(1) 情報化投資の対象範囲と区分のポイント

① 一般設備予算の対象範囲との切分けが必要となるものの例

ａ．電話機、コピー・スキャナ機、ファクシミリ等

ｂ．電子媒体

ｃ．回線（電話回線、LAN 配線）

ｄ．電子的に購読する雑誌等

ｅ．ID カード、電子化された社員証等

② 区分

ａ．戦略的投資

ｂ．定常的な運用費、保守費

ｃ．小額の投資、消耗品

ｄ．直接投資と間接投資

ｅ．初期投資と運用費用

ｆ．全社的投資と部門投資

ｇ．全体最適化のための投資と個別案件のための投資

(2) 情報化投資の有効性を評価する指標の例

① 経営コストの削減効果

② 競争優位性を保つための情報システム開発、情報提供の効果

③　業務活動の正確性・信頼性を向上させる情報システム開発の効果

④　情報システムの利用開始可能の時期

(3) 経営戦略との整合性を考慮した予算設定方法の例

①　情報化投資コストのユーザ部門への負担配分は、情報システムや情報システム部門の人的資源等の利用度合いによって設定する。

②　個別情報システムへの投資額は、その情報システムの企業に対する貢献度に応じて設定する。

③　ハードウェア機器、ソフトウェア開発、運用要員等のコストは、市場価格と連動した基準を適用する。

④　外部からの調達単位の区分の検討

⑤　外部から調達する際に、業者間での競争入札にするか、又は、特定業者から安定的に調達するか。

３．情報化投資

(2) 情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。

1 主　旨

情報化投資計画を利害関係者の合意の上で決定するために、影響、効果、期間、実現性等の観点から複数の選択肢を挙げて検討し、最適なものを選択する必要がある。

2 着眼点

(1) 影響、効果、期間、実現性等の観点において明確な差がある複数の選択肢が挙げられていること。

(2) 選択基準が定められていること。

(3) 具体的な選択肢を選択した理由を利害関係者に説明できるようにしていること。

3 関連事項

(1) 選択肢のポイントの例

① 外部委託：アウトソースするか、直接調達するか、等

② 資源保有：所有するか、リースするか、等

③ 資源活用：新規に調達するか、既存資源を流用するか、等

④ 計画期間：短期計画か、中期計画か、等

⑤ 開発：自主開発するか、パッケージソフトウェアを採用するか、等

⑥ 業務への影響：既存の業務プロセスを前提とするか、業務プロセスの根本的な見直しも行うか、等

⑦ 組織への影響：既存の組織内だけで行うか、外部の組織を買収・統合するか、外部に委託するか、自組織の一部を切り離すか、等

3．情報化投資

(3) 情報化投資に関する予算を適切に執行すること。

1 主　旨

情報化投資計画を確実に実行するため、適切な時期、金額、契約形態等で予算を執行する必要がある。

2 着眼点

(1) 予算執行の最終決裁者が定められていること。

(2) 予算執行の時期、金額、契約形態等が計画されていること。

(3) 経営環境の変化に合わせて予算執行の時期、金額が調整されていること。

(4) 不適切であることが明白である執行を防止するための内部統制が存在していること。

(5) 予算の執行が適切であったかを事後に評価する体制が整備されていること。

3 関連事項

(1) 不適切な予算執行の弊害の例

① 時期

a．競争優位性を保つための情報システムの開発の遅れ

b．人的資源の取合い

c．社会、業界等から見ても時期尚早

d．発展途上の技術の採用　等

② 金額

a．経営環境（組織体の収入）と不釣合いな支出

b．他企業等と比較して相対的なサービスの低下　等

③ 契約形態

a．市場価格よりも高い価格での調達

b．自組織が保護されない契約内容　等

④ 内容

a．競争優位性が確保できないと判断できる投資

b．効果があまりにも長期的すぎる投資　等

3．情報化投資

(4) 情報化投資に関する投資効果の算出方法を明確にすること。

1 主　旨

情報化投資の効果を客観的に評価し、今後の情報化投資計画にフィードバックするため、投資効果の算出方法を事前に明確にしておく必要がある。

2 着 眼 点

(1) 各情報化投資案件について、その効果の算出方法を事前に定めていること。
(2) 各情報化投資案件について、その予算を個別に定めていること。
(3) 投資対効果の期待値を事前に算定していること。
(4) 投資効果の算出方法を事前に明確にすることがルールとして定められていること。
(5) 投資対効果が不明なまま情報化投資が行われることを防止する内部統制があること。

3 関連事項

(1) 投資効果の定量的算定方法の例

① 投下資本利益率（ROI：Return on Investment）

投下した資本によって生み出される利益を測る。一般的には「投資利益率＝利益÷投下資本×100%」の式で求められる。

② 単純回収期間法（Pay-back Period method）

時間価値を考慮せずに、投資額を年々の増分現金流入額によって何年間で回収できるかを計算し、その回収期間によって評価する。

③ 正味現在価値法（NPV：Net Present Value）

取得から廃棄までの全期間において、その投資による各年における金銭の流入出の増減を割引現在価値で算出する。

④ 内部利益率法（IRR：Internal Rate of Return）

投資によって発生する毎年の純現金収入の現在価値合計と、その投資に必要な現金支出額の現在価値合計額が等しくなる割引率（内部利益率）を求め、内部利益率の大小によって評価する。

3．情報化投資

(5) 情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。

1 主　旨

情報システムの全体的な業績及び個別のプロジェクトの業績の財務的な課題を早期に発見し適切な対策を講ずるために、財務的な観点からのモニタリングを行うとともに、想定される課題については事前に対応手順を準備しておく必要がある。

2 着 眼 点

(1) 情報システムの全体的な業績及び個別のプロジェクトの業績について、財務的な観点からのモニタリングを行っていること。

(2) 評価する指標及びアラームを立てる閾値（いきち）を定義していること。

(3) 投資規模等に応じて、重点的に評価すべき個別プロジェクトを明らかにしていること。

(4) 想定される財務的な課題について事前に対応手順を準備していること。

(5) 情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価して、問題点に対しては対策を講ずることがルールとして定められていること。

(6) 財務的な観点から評価が行われないままプロジェクトが推進されることを防止する内部統制があること。

3 関連事項

(1) 財務的観点からの評価の基準の例

① 業界におけるベンチマーク

② ユーザ部門等からの原価回収率

③ 情報システムへの支出が予算の範囲内に収まっているか。

④ プロジェクトへの支出が予算の範囲内に収まっているか。

⑤ プロジェクトの目標が実現されているか。

(2) 財務的観点からのプロジェクト評価手法の例

① EVM（Earned Value Management）法

② LOC（Line Of Code）法（プログラムコード行数見積り）

③ PERT（Program Evaluation and Review Technique）法（作業所要時間見積り）

④ デルファイ法（リスク識別法）

⑤ BSC（Balanced Scorecard）

(3) EVM の概要

① 特徴

a．プロジェクトの進捗状況を費用、スケジュール、作業範囲に焦点を絞って評価、費用差異及びスケジュール差異を金額として把握することができる。

② 期待される効果

a．費用とスケジュールでプロジェクトの出来高が機械的に測定可能となる。

b．将来の出来高（プロジェクトの終了見込み日、終了時の総費用等）を過去の積み重ねから推測可能となる。

③ 参考文献

a．独立行政法人　情報処理推進機構 「EVM 活用型プロジェクトマネジメント導入ガイドラインの作成　調査報告書」2003 年

b．独立行政法人　情報処理推進機構 「EVM 活用型プロジェクトマネジメント導入ガイドラインの作成　ガイドライン」2003 年

(4) 財務的観点からの業績評価を推進する施策の例

① 社外のベンチマーク用データベースと比較すること。

② プロジェクトの目標の達成を個人の業績評価に結びつけること。

(5) BSC による業績評価

① 視点

財務の視点、顧客の視点、内部プロセスの視点、学習と成長の視点

② BSC の適用のレベル

全社的レベル、事業部門レベル、部・課レベル、個人レベル

3．情報化投資

(6) 投資した費用が適正に使用されたことを確認すること。

1 主　旨

情報化投資を計画どおりに行い、また計画とのずれがあった場合にそれを適切に修正するために、投資金額、用途等を確認する必要がある。

2 着眼点

(1) 各投資案件について、投資金額、用途等を記録していること。

(2) 各投資案件について、投資金額、用途等を確認し、計画と突合していること。

(3) 計画とのずれがあった場合には、その理由を明確にしていること。

(4) 計画との大きなずれがあった場合には、元の計画に戻すための補正投資を行うか、又は投資計画自体を修正していること。

(5) 投資した費用が適正に使用されたことを確認することがルールとして定められていること。

(6) 投資した費用が適正に使用されたことの確認が行われないまま放置されることを防止する内部統制があること。

3 関連事項

(1) 投資した費用の適正使用を確認するポイントの例

① 投資時期（債務が発生した時期、実際に支払った時期）

② 金額（総額、明細）

③ 用途（ソフトウェア開発、ハードウェア購入・リース、運用委託等）

④ 支払先（契約先の選択方法、選択理由）

(2) 計画とのずれの理由の例

① 投資時期

プロジェクトの遅延、前倒し、着手順位の変更等

② 金額

a．外的要因：人件費の変動、機器費用の変動、最新技術の出現による価格低下等

b．内的要因：組織体の財務状況、情報化投資計画自体の変更、費用対効果の前提条件の変更、当該案件の規模・重要度の変更等

③ 用途

a．方式の変更：買取りからリースへ、派遣から外部委託へ、等

b．構成の変更：新規購入から既存資源の流用へ、等

④ 支払先

契約先の変更：個別契約から一括契約へ、既存業者から新規業者へ、等

(3) 補正投資の方法の例

① 当該案件への追加投資（投資が不足している場合）

② 当該案件のプロジェクト期間の変更、次期投資予算の減額（投資が過多であった場合）

③ 他案件の予算の削減、投資時期の延期（投資が過多であった場合）

4．情報資産管理の方針

(1) 情報資産の管理方針及び体制を明確にすること。

1 主　旨

組織体の経営上重要な資産である情報資産を適切に管理し、有効利用するため、管理の方針を定め、その体制を明確にする必要がある。

2 着 眼 点

(1) 情報資産の管理方針及び体制は、文書化され、組織体の長が承認していること。

(2) 情報資産の管理方針及び体制について、関係者に周知徹底していること。

(3) 管理すべき情報資産を明確にしていること。

3 関連事項

(1) 情報資産の分類の例１

① ハードウェア資産

コンピュータ、端末、周辺機器等

② ソフトウェア資産

アプリケーションソフトウェア、ソフトウェアパッケージ、OS 等

③ ネットワーク資産

ネットワーク機器、通信回線等

④ データ資産

顧客データ、商品データ、人事データ、販売管理データ等

⑤ 人的資産

運用・保守要員、開発要員、データ管理者、ユーザ等

(2) 情報資産の分類の例２

① PC や共有サーバ内に保管される電子データ

サーバ内の取引データ、サーバ内の取引先データ、サーバ内のナレッジデータベース等

② 紙、記録媒体

個人情報の入ったアンケート用紙、設計図の情報の入った CD-ROM、バックアップの磁気テープ等

③ 物理的資産、設備、サービス

ハードウェア、ソフトウェア、ネットワーク、コンピュータ室、運用・保守サービス等

(3) 情報資産の管理方針で明確にすべきこと

① 組織体の長の責任

② 情報資産の種類
③ 管理方針の適用範囲
④ 情報資産管理の目的
⑤ 法制度や契約等の要求事項への適合
⑥ 管理体制及びその役割　等

(4) 管理体制のポイント

① 情報資産は組織体全体の問題であり、組織体全体の各部門で構成される委員会形式がよい。
② それぞれの部門の役割を明確にする必要がある。
③ 管理体制での運用は、PDCA サイクルで実施する必要がある。
④ 情報資産管理の全部又は一部を外部委託しようとする場合は、費用対効果、提供されるサービス、メリット・デメリット等を考慮の上、外部委託の可否を決定する必要がある。
⑤ 管理体制が効果的に運営されるためには、定期的な監査が有効である。

4．情報資産管理の方針

(2) 情報資産のリスク分析を行い、その対応策を考慮すること。

1 主　旨

情報資産の信頼性、安全性を確保するため、情報資産がもっている顕在的なリスクや潜在的なリスクについて洗い出し、それぞれの大きさを決定し、対応策を講ずる必要がある。

2 着眼点

(1) 管理すべき情報資産の目録を作成していること。

(2) 情報資産ごとにリスクを洗い出していること。

(3) 情報資産のリスクごとに対応策を講じていること。

(4) 情報資産のリスクごとに講じた対応策について組織体の長が承認していること。

3 関連事項

(1) 情報資産の目録の例

① 情報資産名

② 責任者（管理部門、管理責任者）

③ 重要度（極秘、秘密、社外秘、公開）

④ 分類（ハードウェア資産、ソフトウェア資産、ネットワーク資産、データ資産、人的資産）

(2) 情報資産ごとのリスクの例

① 火災

建物火災、コンピュータ室火災、PC の火災、サーバ火災等

② 自然災害

地震、水害等

③ 犯罪

個人情報漏えい、破壊行為、詐取、窃取、横領、コンピュータウイルス等

④ 不正アクセス

物理的侵入、ハッカー、アクセス権濫用等

⑤ 障害

ハードウェア障害、ソフトウェア障害、ネットワーク障害、人的障害等

⑥ 動物害

鼠害、鳥害、虫害等

⑦ エラー等

操作ミス、プログラムミス等

(3) リスクごとの対応策の例

① リスクの回避

対象の情報資産を利用しないことによって、リスクそのものを取り除く対応策である。例えば、公衆回線の利用によって情報漏えいのリスクがある場合、それを専用回線の利用に置き換える。ただし、情報資産によっては、情報資産そのものの便益を享受できないことにもなる。

② リスクの予防

リスクの発生頻度を減少させる対応策である。例えば、コンピュータ室への不正アクセスの発生確率を軽減させるために、本人認証にバイオメトリックス認証を採用する。

③ リスクの軽減

リスクが発生しても損失を軽減させる対応策である。例えば、コンピュータシステムを二重化し、１台がダウンしても、全体の性能は落ちるがもう１台だけでも稼動するようなシステムにする。

④ リスクの移転

リスクが発生しても契約を通して、責任を他者に移転させる対策である。例えば、契約に免責特約条項を入れ、金銭上の責任を他者に移転させたり、保険に入ったりする。

⑤ リスクの保有

リスクに対して事前の対応策はとらず、リスクが発生した時に対処する。例えば、従業員の使用しているPCに障害が起きて使用できなくなった場合、事前に予備のPCは用意せずに、修理に出す。

4．情報資産管理の方針

(3) 情報資産の効率的で有効な活用を考慮すること。

1 主　旨

経営戦略や情報戦略の目的を達成するため、情報化投資の方針に基づき、情報資産を効率的かつ有効に活用する必要がある。

2 着眼点

(1) 情報資産の効率的かつ有効な活用方法を明確にしていること。

(2) 情報資産の効率的かつ有効な活用方法をモニタリングしていること。

3 関連事項

(1) 情報資産の効率的な活用方法

① 情報資産の利用率の向上

利用が許可されている者であれば誰でも利用できるように、情報資産の共有化、利便性向上を図る。

② 情報資産の稼動率の向上

情報資産が保有する能力を最大限発揮できるようにする。

③ 情報資産の生産性の向上

情報資産の生産性向上を図る。

(2) 情報資産の有効な活用方法

① 経営戦略や情報戦略の目的達成度の向上

戦略目的にあった情報システムを構築し、企業文化の変革、ユーザの情報リテラシー向上等を行うことによって、情報資産の活用を通して、経営戦略や情報戦略の目的達成度の向上を図る。

② 情報化投資の目的達成度の向上

情報化投資の費用対効果を明確にし、その前提条件を満たすことで、情報化投資の目的達成度の向上を図る。

③ 業務改善の目的達成度の向上

情報技術を積極的に取り入れた業務改善を推進し、企業文化の変革、ユーザの情報リテラシー向上等を行うことによって、情報資産の活用を通して、業務改善の目標達成度の向上を図る。

(3) 情報資産の効率的で有効な活用方法のモニタリング

情報資産の効率的で有効な活用方法を考慮するためには、指標を設定し、モニタリングできるようにすることである。指標を設定するためには、重要業績評価指標（KPI：Key Performance

Indicator）や重要目標達成指標（KGI：Key Goal Indicator）の考え方を導入することが効果的である。

4. 情報資産管理の方針

(4) 情報資産の共有化による生産性向上を考慮すること。

1 主　旨

経営戦略や情報戦略の目的を達成するため、情報資産の共有化による生産性向上を図る必要がある。

2 着眼点

(1) 情報資産の共有化を図っていること。

(2) 情報資産の共有化による生産性向上の指標を設定していること。

(3) 情報資産の共有化による生産性向上をモニタリングしていること。

3 関連事項

(1) 情報資産の共有化の例

① 取引データの共有化を図る。

② システム設計のノウハウの共有化を図る。

③ 稼動率の低いシステム機器の共有化を図る。

(2) 情報資産の共有化による生産性向上の例

① 取引データの共有化を図ることによって、販売戦略案の生産性を上げる。

② システム設計のノウハウの共有化を図ることによって、システム開発の生産性を上げる。

③ 稼動率の低いシステム機器の共有化を図ることによって、システム機器の稼動率を向上させ、コストパフォーマンスの観点より、生産性をあげる。

(3) 情報資産の共有化による生産性向上のモニタリング

情報資産の効率的で有効な活用方法を考慮するためには、指標を設定し、モニタリングできるようにする。指標を設定するためには、KPI や KGI の考え方を導入することが効果的である。

(4) ナレッジマネジメント

ナレッジマネジメントは知識経営、知識管理等と訳されている。組織の中にある個人の持つノウハウ（暗黙知）を読める形で（形式知）に共有することによって、組織での業務の効率化が図られる。ナレッジマネジメントは組織の手順等の標準化を促進することによって効果が上がる。専門知識を有する組織構成員の知識提供の協力を得るためには、提供に対する報酬等を考慮する必要がある。

5．事業継続計画

(1) 情報システムに関連した事業継続の方針を策定すること。

1 主　旨

組織体の事業継続性を確保するため、情報システムに関連した事業継続の方針を定める必要がある。

2 着 眼 点

(1) 情報システムに関連した事業継続の対象範囲を明確にしていること。

(2) 情報システムに関連した事業継続の方針を策定し、文書化していること。

3 関連事項

(1) 情報システムに関連した事業継続の対象範囲の例

① 対象リスク

事業継続におけるリスクは、多種多様である。

例えば、財務リスク（信用リスク、回収リスク、倒産リスク、為替リスク等）、経営リスク（製造物責任、物流リスク、生産リスク、研究開発リスク等）、法的リスク（訴訟リスク、株主代表訴訟、セクシャルハラスメント等）等が挙げられる。

これらの中で情報システムに関連したリスクが対象リスクとなる。

② 対象事業

情報システムを使用している事業、又は関連する事業すべてが対象となる。

③ 対象組織

情報システムを使用している組織、又は関連する組織すべてが対象となる。

④ 対象システム

すべての情報システムが対象となる。

⑤ 対象設備

情報システムを稼動させるのに関連するすべての設備が対象となる。

(2) 事業継続方針の内容の例

① 事業継続の方針の目的

② 事業継続の範囲

③ 事業継続のリスクアセスメント

④ 事業継続の体制及び役割

⑤ 従業員の教育訓練

⑥ 関係者への周知徹底

⑦　事業継続の方針の定期的なテスト
⑧　事業継続の方針の定期的な見直し

５．事業継続計画

(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。

1 主　旨

事業継続にかかわる事象が発生した場合にすべての利害関係者が円滑に対応できるようにするため、利害関係者を含んだ組織体制で実行性の高い事業継続計画を立案し、組織体の長が承認する必要がある。

2 着眼点

(1) 事業継続計画は、利害関係者を含んだ組織体制で立案していること。

(2) 事業継続計画を組織体の長が承認していること。

3 関連事項

(1) 事業継続計画の立案体制の例

① 委員長　CIO
② 事務局　経営企画部門
③ 委員　情報システムを利用しているユーザ部門
④ 委員　情報システムを開発・運用・保守している部門
⑤ 委員　情報通信基盤を運用・管理している部門
⑥ 委員　構内設備・工事を担当している部門
⑦ 委員　広報を担当している部門
⑧ 委員　取引先を管理する部門
⑨ 委員　海外店を担当している部門　等

(2) 事業継続計画の内容の例

事業継続の方針に基づいて作成する必要がある。

① 事業継続計画の目的
② 事業継続計画の範囲
③ 事業継続計画の実行体制
④ 事業継続計画の実行体制の役割と責任
⑤ 事業の目的及び事業の優先順位付け
⑥ 想定できる脅威とその対応策（緊急時手続を含む）
⑦ 対応策を実行するための手続
⑧ 事業継続計画の定期的な教育
⑨ 事業継続計画の定期的なテスト　等

5. 事業継続計画

(3) 事業継続計画は、従業員の教育訓練の方針を明確にすること。

1 主　旨

事業継続にかかわる脅威が発生しても、迅速かつ確実に事業継続計画に定められた手続を実行できるようにするため、事業継続計画には従業員の教育訓練の方針を明確にする必要がある。

2 着眼点

(1) 事業継続の方針と整合性がとれていること。

(2) 事業継続計画に従業員の教育訓練の方針を明確にしていること。

(3) 訓練の方針が適切であること。

3 関連事項

(1) 教育訓練の方針の内容の例

① 教育訓練の目的

② 教育訓練の範囲

③ 教育訓練の対象者

④ 教育訓練の体制

⑤ 教育訓練の時期

・定期的な実施

⑥ 教育訓練の内容

・危機管理を含め合意された緊急時手続及び過程を教育

・事件・事故後又は危機管理における役割について模擬テスト等の実施によって訓練

⑦ 教育訓練の結果のフィードバック

・教育訓練結果で問題がある場合、教育訓練の方針を見直す。

５．事業継続計画

(4) 事業継続計画は、関係各部に周知徹底すること。

1 主　旨

事業継続計画の実行性を高めるため、事業継続計画を関係者に周知徹底する必要がある。

2 着 眼 点

(1) 周知徹底の方法を明確にしていること。

(2) 周知徹底の時期が適切であること。

(3) 周知徹底されたことを確認していること。

(4) 事業継続計画が変更された場合、関連する部門に連絡すること。

3 関連事項

(1) 周知徹底の方法

① 事業継続計画を小冊子にし、関係者全員に配布

② 定期的な集合教育

③ 社内イントラへの掲載

④ ｅラーニングによる教育

(2) 周知徹底の時期

上記方法によって周知徹底を図る必要があるが、次のような時期には特に周知徹底を図る必要がある。

① 異動時

② 組織改組

③ 新規プロジェクト、新規事業の開始時

④ 企業の吸収・合併時

(3) 周知徹底の確認方法の例

① 研修の受講率の報告等

5．事業継続計画

(5) 事業継続計画は、必要に応じて見直すこと。

1 主　旨

事業継続計画の有効性を維持するため、必要に応じて見直し及び更新を行う必要がある。

2 着 眼 点

(1) 事業継続計画の見直しのルールを明文化していること。

(2) 見直しによる変更は理由を明確にしていること。

(3) 変更した計画を組織体の長が承認し、関係者に周知徹底していること。

(4) 各事業継続計画の見直しに対する責任を割り当てていること。

3 関連事項

(1) 見直しのルールの内容の例

① 見直しの目的、範囲

② 見直しの手続

③ 見直しの責任の割当て

④ 見直し結果のレビュー体制

⑤ 見直し結果の承認手続

⑥ 見直しの版管理

⑦ 見直し結果の周知徹底手続　等

(2) 見直しの必要性の例

① 経営戦略や情報戦略の変更

② 経営環境の変化

③ 情報技術の進歩

④ 新たなリスクの顕在化

⑤ 法制度の変更

⑥ 業務改革

⑦ 新規システム開発、システム改善

⑧ 社内組織改組

⑨ 分社化、吸収合併　等

6．コンプライアンス

(1) 法令及び規範の管理体制を確立するとともに、管理責任者を定めること。

1 主　旨

法令及び規範を遵守し適切に管理していくためには、組織として、法令及び規範の所管部門を明らかにし、管理体制を確立するとともに、管理責任者を定めて管理を推進する必要がある。

2 着眼点

(1) 組織体内において、法令及び規範の所管部門を定めること。

(2) 法令及び規範の所管部門において、管理責任者を定め、責任の所在を明確にすること。

(3) 該当部門の職務分掌として、法令及び規範の所管を明確に位置付けること。

(4) 法令及び規範の管理責任者は、組織体内において法令及び規範の遵守状況を確認すること。

3 関連事項

(1) 法令及び規範の所管部門、管理責任者の例

・所管部門：法務部（課）、法務室、総務部（課）、経営企画（室）、社長室等

・管理責任者：法務部（課）長、法務担当部（課）長、法務室長、総務（課）部長、経営企画部（室）長、社長室長等

法令及び規範の所管部門、管理責任者は、個人情報等の情報資産の利活用が業務運営に大きな影響を及ぼす状況を踏まえ、情報関連の法令及び規範が従来にも増して重要になっている状況を認識する必要がある。

(2) 法令及び規範所管部門の職務分掌記載の例

・遵守すべき法令及び規範の特定と社内ルールへの反映

・遵守すべき法令及び規範、社内ルールの関係者への周知徹底

・その他、法令及び規範に関する事項

6．コンプライアンス

(2) 遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。

1 主　旨

法令及び規範を遵守し適切に管理していくためには、組織として遵守すべき法令及び規範を明確に識別し特定することが必要である。その上で、特定した法令及び規範を関係者に知らせるための教育体制を確立し、関係者に周知徹底する必要がある。

2 着 眼 点

(1) 組織体内において、必要な関係法令や規範を識別し特定すること。なお、関係法令及び規範には情報関連の法規も含むものとする。

(2) 特定した関係法令や規範について、組織体内外の必要な関係者に周知徹底するために必要な教育体制を確立すること。

(3) 関係法令及び規範についての教育の実施責任者を定め、必要な教育を実施し、関係者に周知徹底すること。

(4) 特定した関係法令及び規範については、定期的に見直しを行うこと。

3 関連事項

(1) 関係法令及び規範の例

① 関係法令の例

電気通信事業法、不正アクセス禁止法、著作権法、特許法、個人情報保護法、電子署名電子認証法、特定商取引法、不正競争防止法、刑法、IT 基本法、労働者派遣法

② 規範の例（業界ガイドライン、社内規程等）

システム監査基準、情報セキュリティ監査基準、情報システム安全対策基準、コンピュータウイルス対策基準、ソフトウェア管理ガイドライン、不正アクセス対策基準、個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン、JIS Q 15001、JIS X 5070、JIS X 5080 等

6．コンプライアンス

(3) 情報倫理規程を定め、関係者に教育及び周知徹底すること。

1 主　旨

組織体として、法令及び規範を遵守し適切に管理していくためには、組織体内の遵守すべきルールとして、情報倫理規程を定めるとともに、組織体内外の関係者に教育し、周知徹底する必要がある。

2 着 眼 点

(1) 業務遂行上必要となる関係法令や規範に基づき、組織体が遵守すべきルールを情報倫理規程として定めること。

(2) 情報倫理規程を周知徹底するための教育体制を確立するとともに、必要な関係者に教育を実施すること。

(3) 情報倫理規程は、定期的に見直しを行うこと。

3 関連事項

(1) 情報倫理規程の例

① 目的

② 適用範囲と対象

③ 用語の定義　情報と種類

④ 総則　基本的な考え方

法令・規範の遵守、本規程を含む社内のポリシー・規程の遵守

罰則規定

⑤ 各論　会社が保有する情報の取扱いについての規程

セキュリティに関する規程：パスワードの管理、ウイルス対策等、社員のインターネット利用に関する規程

電子メールの利用に関する規程：利用上の注意、禁止事項等

WWW利用に関する規程：利用上の注意、禁止事項等

関連法規：知的所有権、個人情報保護法等

(2) 情報倫理教育実施の例

・教育研修部門による新入社員教育、情報システム部門による情報リテラシー教育、法務担当による個人情報保護教育、各職場によるベンダー教育

(3) 関係者、及び情報倫理規程の教育対象の例

コンピュータ犯罪、セキュリティ事故等の多くが、組織体内部要員による犯行という事実がある。したがって、情報倫理規程の周知徹底は、必要な場合、関係会社や協力会社の要員等も含め組織体内外の関係者を対象とする必要がある。

・役員、社員、契約社員、派遣社員、パート・アルバイト、請負常駐者、関係会社や協力会社要員等

6．コンプライアンス

(4) 個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めること。

1 主　旨

法令及び規範を遵守していく上で、組織体内外の各種権利保護の観点から、個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関して、組織体としての考え方を明確にした方針を定める必要がある。

2 着眼点

(1) 組織体は、個人情報保護の観点から個人情報取扱方針を定めること。

(2) 組織体は、知的財産権の保護の観点から知的財産取扱方針を定めること。

(3) 組織体は、各種権利保護とデータ取扱いの観点から、外部へのデータ提供に関する方針を定めること。

(4) 組織は、定めた方針を実行するため、業務遂行に必要な手順書、マニュアルを定め、組織体内外の関係者に周知徹底すること。

3 関連事項

(1) 個人情報取扱方針に盛り込むべき項目（「個人情報保護法」より抽出）

① 基本原則

- 利用目的による制限
- 適正な取得
- 正確性の確保
- 安全性の確保
- 透明性の確保　等

② 義務

- 利用目的の特定
- 利用目的による制限
- 適正な取得
- 取得に際しての利用目的の通知等
- データ内容の正確性の確保
- 安全管理措置
- 従業者の監督
- 委託先の監督
- 第三者提供の制限

・保有個人データに関する事項の公表等
・開示
・訂正等
・利用停止等
・理由の説明
・開示等の求めに応じる手続
・手数料
・苦情の処理　等

(2) 知的財産取扱方針の内容の項目の例

① 取扱方針の目的
② 適用範囲（従業員、外部委託要員、子会社、関連会社等）
③ 自社の特許権に関する考え方
④ 他者の著作権に関する取扱い
⑤ 秘密情報の取扱い
⑥ 自社の商標権の取扱い、他者の商標権侵害に対する留意事項　等

(3) 外部へのデータ提供に関する方針の内容の項目の例

① 取扱方針の目的
② 適用範囲
③ データ提供の基本的考え方
・対象データ
・データ提供の手続と承認プロセス
・データ提供先選定
・データ提供にかかわる契約
・データ取扱いのルール　等

(4) OECD のプライバシー８原則（括弧内は日本の個人情報保護法の対応する条項）

・収集制限の原則（第 18 条、第 23 条）
・データ内容の原則（第 19 条）
・目的明確化の原則（第 15 条、第 16 条、第 18 条）
・利用制限の原則（第 16 条、第 23 条）
・安全保護の原則（第 20 条、第 21 条、第 22 条）
・公開の原則（第 24 条）
・個人参加の原則（第 25 条、第 26 条、第 27 条）
・責任の原則（第 20 条）

6．コンプライアンス

(5) 法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講ずること。

1 主　旨

法令及び規範を遵守し適切に管理していくために、特定した法令及び規範、また社内ルールとして策定した情報倫理規程等について、組織としての遵守状況を定期的に点検・評価し、指摘事項に対し改善のために必要な方策を講ずる必要がある。

2 着 眼 点

(1) 法令及び規範及び情報倫理規程の遵守状況を定期的に点検・評価していること。

(2) 遵守状況の点検・評価によって、明らかになった指摘事項・改善事項に対して、改善計画を立案し、改善のための必要な方策を講ずること。

(3) 改善計画は、マネジメントレビューを実施し、組織体の長が承認していること。

3 関連事項

(1) 法令、規範及び情報倫理規程の遵守状況の評価の例

システム監査の実施、リスク分析、ぜい弱性評価、コンプライアンス教育の実施状況、法令・規範確認チェックシートによる定期確認、理解度テストの実施等

(2) 改善のための必要な方策の例

コンプライアンス教育の実施、情報倫理規程の周知徹底教育

(3) その他

法令、規範及び情報倫理規程の遵守状況の評価について、以下のような情報資産の適法性の観点からの評価も必要である。

・開発・運用中の情報システムの順法性

・ソフトウェアの違法コピーをしていないこと。

・リース切れのパソコン等の取扱いが適切かどうか（情報漏えいのリスクはないか）等

Ⅱ. 企 画 業 務

1．開発計画

2．分析

3．調達

1．開発計画

(1) 開発計画は、組織体の長が承認すること。

1 主　旨

開発計画が全体最適化計画に基づいていることを確認し、開発計画を実行に移すため、組織体の長が承認する必要がある。

2 理論的根拠／実務的配慮

(1) 開発計画立案ルールを策定し、関係者に周知徹底していること。

(2) 開発計画を関係者が合意していること。

(3) 開発計画を組織体の長が承認していること。

3 関連事項

(1) 開発計画書概要の内容例（組織体の長及び関係者の理解を深める開発計画書の概要を作成することが望ましい）

① 情報システム化の目的と目標

② 全体最適化計画との関連

③ 情報システム化の内容（スコープ、業務・組織改革、情報システム化の内容）

④ 開発スケジュールと体制

⑤ 費用と効果、移行時期、移行スケジュール

⑥ ・重要成功要因（CSF：Critical Success Factors）：開発を計画どおりに実行するための重要な要因・要素

・重要目標達成指標（KGI：Key Goal Indicators）：開発によって何を達成するかの指標

・重要業績評価指標（KPI：Key Performance Indicators）：開発完了時に実現した情報システムの評価の尺度

⑦ 他の情報システムとの関係

(2) 関係者とのレビューが必要な事項の例

① 情報システム化の必要性、効果

② 実現するシステムの機能、能力

③ 情報システムによる業務の変更点

④ ユーザインタフェース、操作性の概要

⑤ ユーザ部門への依頼事項

⑥ 情報システムの運用形態の変更点

1．開発計画

(2) 開発計画は、全体最適化計画との整合性を考慮して策定すること。

1 主　旨

開発する情報システムは、関連する他の情報システムと役割を分担し、組織体として最大の効果を上げる機能を実現するため、開発計画は、全体最適化計画との整合性を考慮して策定する必要がある。

2 着 眼 点

(1) 開発計画は、全体最適化計画に基づいて策定していること。

(2) 開発計画は、関連する他の情報システムとの関係を明確にしていること。

(3) 全体最適化計画と相違した事項に関しては、理由を明確にし、関係者が合意していること。

3 関連事項

(1) 全体最適化計画との整合性に当たっての考慮事項

① 対象業務、機能……他の情報システムとの整合性

② 組織全体の情報システムにおける位置付け

③ 開発費用

④ 開発スケジュール……他の情報システムとの整合性

⑤ 開発優先順位

⑥ 開発体制

⑦ 現行業務の変更事項

⑧ 他の情報システムとのインタフェース

(2) 開発計画の策定に必要な技術

① 全体最適化計画を理解し、目標とする情報システムを明確化するための必要技術を定義する要素分析技術

② 現行の業務、組織及び情報システム構造を的確に把握するための現状分析技術

③ 改善案及び情報システム化要件を明確化するためのギャップ分析技術

④ 情報システム化の目的とその範囲を明確化するための要件整理技術

⑤ 開発する情報システムの概要を作成するための情報システム概要設計技術

⑥ 開発計画を策定するための作業計画、見積技術及び効果、費用の評価技術

⑦ 開発計画に対する評価ポイントの作成技術

⑧ 開発計画をまとめ表現するためのドキュメンテーション技術

1．開発計画

(3) 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。

1 主　旨

情報システムの目的、機能等について関係者が共通認識をもち、情報システムの投資効果を確認するため、開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にする必要がある。

2 着 眼 点

(1) 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にしていること。

(2) 開発する情報システムの目的及び対象業務は、全体最適化計画との整合性を確認していること。

(3) 開発計画の投資効果の算出根拠を明確にしていること。

(4) 開発計画は、必要に応じて関係者に配布し、説明していること。

(5) 投資効果の算定は、全体最適化計画で定めた方法を使用していること。

3 関連事項

(1) 情報システム化の目的の例

① 流通システム……ｅビジネスへの対応、自動化の推進、物流時間の短縮、欠品の低減、物流費用の低減等

② 製造管理システム……製造費用の削減、人件費の低減、生産自動化の推進、適切な原材料管理等

③ 販売・マーケティングシステム……ｅビジネスへの対応、マーケット変動の迅速な把握、オーダの即時処理等

④ 金融情報システム……大量業務データの迅速な処理、エレクトロニックバンキングの実現、信頼性の確保、経営情報の即時把握、顧客管理の充実、新決済手段の拡大等

⑤ オフィスシステム……事務処理の効率化、会議の削減・効率化、文書類の削減、情報の共有化、文書管理、決裁ワークフロー等

(2) 費用対効果の要素の例

① 費用の要素

ａ．ソフトウェア開発費用（人件費、委託費、購入費用等）

ｂ．ハードウェア費用

c．通信回線使用費用
d．外部委託費用
e．教育費用
f．建物・附帯設備費用、記録媒体費用、消耗品、光熱費等

② 効果の要素
a．定量的評価……ビジネス創造性評価（新製品投入、商業圏拡大、シェア拡大等）
事業リスク評価
効率性評価
費用低減評価
品質向上評価
b．定性的評価……迅速性評価
質的評価
サービス対応評価

(3) 開発計画書の構成の例
① 情報システム化の目的
② 全体最適化計画との整合性
③ 対象業務と範囲
④ 情報システムの構想
a．主要実現機能
b．処理の概要
c．能力、効率
d．品質
⑤ 開発工数と開発体制
⑥ 開発スケジュール
⑦ 投資費用
⑧ 投資効果分析
⑨ 組織・業務改革への取組
⑩ ・重要成功要因（CSF）
・重要目標達成指標（KGI）
・重要業績評価指標（KPI）

1．開発計画

(4) 開発計画は、関係者の教育及び訓練計画を明確にすること。

1 主　旨

開発計画で策定した情報システムの品質を保ちスケジュールどおりに実現するため、開発関係者の計画に対する理解の統一と技術力を向上させる教育及び訓練計画を明確にする必要がある。

2 着眼点

(1) 情報システムの開発、運用及び保守に必要な教育及び訓練の内容を明確にしていること。

(2) 教育及び訓練の内容に準拠した実施計画が明確にしていること。

(3) 教育及び訓練に必要な資源を明確にしていること。

3 関連事項

(1) 開発、運用及び保守業務において必要な教育及び訓練の内容例

① 開発業務

a．開発計画全体の理解（機能、性能、品質、開発スケジュール、開発体制と役割、開発コスト等）

b．開発ルールの理解

c．開発方法論の理解と実践（設計から導入まで）

d．機器、利用ソフトウェアの理解（機能、使用方法、プログラマインタフェース等）

e．情報セキュリティ意識の向上（開発業務における機密保護策、個人情報保護、不正防止策）

② 運用業務

a．情報システム全体の理解（機能、性能、品質、開発スケジュール、開発体制と役割、開発コスト等）

b．運用ルールの理解

c．機器、運用関連ソフトウェアの理解（機能、使用方法、オペレータインタフェース等）

d．情報セキュリティ意識の向上（運用業務における機密保護策、個人情報保護、不正防止策）

③ 保守業務

a．情報システム全体の理解（機能、性能、品質、開発スケジュール、開発体制と役割、開発コスト等）

b．保守ルールの理解

c．機器、利用ソフトウェアの理解（機能、使用方法、プログラマインタフェース等）

d．情報セキュリティ意識の向上（保守業務における機密保護策、不正防止策）

(2) 開発、運用及び保守業務における教育及び訓練の実施形態

① 集合教育

② ｅラーニングの受講

③ OJT

④ 外部セミナーの受講

(3) 開発計画に盛り込む必要がある教育及び訓練関連の事項

① 教育及びカリキュラムの全体体系

② 教育及び訓練の内容（タイトル、教育／訓練内容、実施形態（教育方法、日程、場所）、講師スキル、評価方法）

③ スケジュール（期日又は実施時期）、コスト

1．開発計画

(5) 開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。

1 主　旨

開発、運用及び保守業務を効果的に実施するため、ユーザ部門と情報システム部門の役割分担を明確にし、相互に確認しておく必要がある。

2 着眼点

(1) 開発、運用及び保守業務におけるユーザ部門と情報システム部門の役割分担を明確にしていること。

(2) 組織及び対象業務システムの特性を考慮し、役割分担を検討していること。

(3) 役割分担をユーザ部門及び情報システム部門の責任者が承認し、周知徹底していること。

(4) 役割分担は、組織及び情報システムの変更に伴い、見直していること。

3 関連事項

(1) 役割分担の例

部門／業務	企画、開発、運用、保守部門	ユーザ部門
企画	現行システムの評価 情報システムの開発計画のとりまとめ．	現行業務処理の評価 システム化要件の明確化
開発	システム設計 プログラミング テストの実施 移行	設計仕様の確定 総合テストへの参画
運用	センターの運用 システムの評価	部門機器の運用 システムの評価
保守	保守設計 プログラミング テストの実施 移行	変更仕様の確定 テストへの参画

(2) エンドユーザコンピューティング（EUC）におけるユーザ部門と情報システム部門の役割分担の例

① ユーザ部門

a．全体最適化計画の策定への参加

b．ユーザニーズのとりまとめ

c．部門内開発計画の策定と予算要求／予算管理

d．部門内機器、部門内ネットワークの管理・運用
e．部門データ、部門ソフトウェアの開発・管理
f．部門内情報セキュリティ対策の実施
g．障害状況等の情報システム部門への報告

② 情報システム部門
a．全体最適化計画の策定への参加
b．全社統一管理規則の策定と周知徹底
c．共通ソフトウェアの開発、配布、保守
d．全社データ、全社ソフトウェアの管理
e．全社基幹システムインタフェースの構築
f．全社ネットワークの構築
g．全社セキュリティ対策の策定
h．ユーザ部門支援（ヘルプデスク）

1．開発計画

(6) 開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。

1 主　旨

情報システムのライフサイクルを通した費用を合理的に算出するために、開発計画は、開発、運用及び保守に関する費用の算出根拠を明確にする必要がある。

2 着眼点

(1) 開発、運用及び保守業務の費用項目を網羅していること。

(2) 費用の算出根拠を明確にし、関係者が承認していること。

(3) 全体最適化計画の情報化投資の方針と相違する費用項目及び費用については、相違の理由を明確にしていること。

3 関連事項

(1) 開発作業における費用項目と算出基礎項目

① CPU 能力 ……処理量、データ集中度、データの伸び率

② データベース……レコード長、レコード数、保存期間、レコードの伸び率

③ ネットワーク……回線種類、データの集中度、データの伸び率

④ 機器構成……処理量、データ量、障害対策のレベル、セキュリティ対策のレベル、目標処理時間

⑤ ソフトウェア開発……開発方法、生産性（設計、プログラミング、テスト、ドキュメンテーション）

⑥ 労務関連……人件費、残業代、外注費（請負、派遣、パッケージ購入）の方針と根拠、旅費交通費の根拠

⑦ 消耗品費……記録媒体、出力媒体、文房具類等の根拠

⑧ 設備・場所……事務経費の根拠

⑨ ソフトウェアライセンス料、保守料

(2) 運用及び保守業務における費用項目と算出基礎項目

① 機器費……レンタル費用

② 保守料……保守費

③ 回線費……回線種類、データ長、トラフィック量

④ 消耗品費……記録媒体、出力媒体

⑤ 光熱費……電気関連費用

⑥ 減価償却費

(3) 関係者（部門）の例

① 経理部門・予算管理部門
② 購買部門
③ 業務企画部門
④ 情報システム部門（企画、開発、運用及び保守）
⑤ 設備管理部門

1．開発計画

(7) 開発計画はシステムライフを設定する条件を明確にすること。

1 主　旨

情報システムのシステムライフを合理的に見積もるため、システムライフの条件を明確にする必要がある。

2 着眼点

(1) 設定条件は、業務の変化、技術的制約を考慮していること。

(2) システムライフの条件は、定量的評価及び定性的評価を考慮し、明確にしていること。

(3) システムライフの条件の設定根拠を明確にしていること。

(4) 設定したシステムライフの条件を関係者が合意していること。

3 関連事項

(1) システムライフの条件の設定に当たっての留意事項

① 定量的評価

a．処理能力の限界、拡張性の限界

b．費用（初期費用、運用費用）の増加

c．減価償却

② 定性的評価

a．全体最適化計画との乖離

b．システム構造、処理体系の陳腐化

c．エンドユーザの操作性、機能に対する不満

d．機器及びソフトウェアの陳腐化

e．情報化技術動向への遅れ

f．他の情報システムの機能向上との連携

(2) クライアントサーバシステムのシステムサイクルの検討に当たっての留意事項

① オープン環境におけるソフトウェアの多様化

② 新機能を持つソフトウェアの登場

③ オペレーティングシステムの変遷

④ ハードウェアの急速な機能向上

⑤ ネットワークの拡大等の環境変化

⑥ 社会環境・ニーズの変化

1．開発計画

(8) 開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。

1 主　旨

全体最適化計画と整合性をとり、情報システムを最も効率よく開発するため、開発計画の策定に当たっては、システム特性及び開発の規模を考慮して情報システムの形態及び開発方法を決定する必要がある。

2 着眼点

(1) 全体最適化計画における開発システムの位置付けを明確にしていること。
(2) 情報システムの目的と機能及びシステム特性と開発規模を整理していること。
(3) 開発形態及び開発方法の選定基準を明確にしていること。
(4) 開発形態及び開発方法は、開発の規模、期間及びシステム特性を考慮して決定していること。
(5) 開発形態及び開発方法は、開発要員の能力及び経験を考慮して決定していること。
(6) 開発形態及び開発方法は、保守業務を考慮して決定していること。
(7) 開発形態及び開発方法は、他の情報システムとの整合性を確認していること。

3 関連事項

(1) 情報システムの実現手段の方法
　① 自社開発……自社で新規に情報システムを開発すること。作業の一部の外部への委託、あるいはソフトウェア開発企業からの要員派遣を受ける場合がある。
　② 共同開発……同業他社、ソフトウェア会社等と共同で情報システムを開発すること。
　③ 外部委託（アウトソーシング）……情報システム関連業務を外部に委託すること。業務処理全体の外部委託をフルアウトソーシングという。
　④ システムインテグレーション……ハードウェアの選定、調達を含めて情報システムの構築をインテグレーション専門会社に委託すること。
　⑤ パッケージ購入……既に完成している業務システムのパッケージを導入すること。
　⑥ ソフトウェアの流通……協力企業、同業企業等の情報システムを移植すること。
(2) 開発ツールの例
　① 企画……要求定義のまとめ、開発計画の作成
　② 開発……システム設計、プログラミング、テスト、ドキュメンテーション及びこれらの管理ツール
　③ 運用……プログラム管理、JCL（ジョブ制御言語）・スクリプトの作成

④ 保守……変更仕様の作成、プログラミング、テスト、ドキュメンテーション及びこれらの管理ツール

(3) EUCにおける開発方法の例

① プロトタイピング……処理モデルの試作版を作成し、目標への実現度を評価しながら完成させる。

② 既存パッケージの導入……表計算、データベース管理、コミュニケーション等の既存パッケージソフトウェアを導入し、マクロ命令の使用によって目的とする情報システムを実現する。

③ モデルプログラムの提供……情報システム部門で作成したモデルプログラム、ユーティリティ等を使用し、ユーザ側で全体システムを構築する。

1．開発計画

(9) 開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成し、検討すること。

1 主　旨

情報システムに要求される機能、能力、品質等を最も効率よく実現するために、複数のシステム実現案を作成し、比較及び評価する必要がある。

2 着 眼 点

(1) 情報システムの目的を達成する複数のシステム案を作成していること。
(2) 複数のシステム案を比較する評価項目を明確にしていること。
(3) システム案の検討には、関係者が参画していること。
(4) 最終案の選定理由を明確にしていること。
(5) 最終案をユーザ、開発、運用及び保守の責任者が承認していること。
(6) 検討結果を記録していること。

3 関連事項

(1) 複数の情報システム化実現案を検討する主な理由
　① 最適な情報システム案を選択するため
　② 採用案の開発に障害が発生した場合の代替策として
　③ 情報システム稼動後の障害時のバックアップ手段として
(2) 代替案検討の視点
　① ITの活用か、人による作業か。
　② オープン環境か、メインフレームによる処理か。
　③ 基幹システムに組み込むか、部門システムとして独立させるか。
　④ 既存のシステムに組み込むか、独立したシステムとして構築するか。
　⑤ リアルタイム処理か、バッチ処理か。
　⑥ 全業務を自社で処理するか、外部委託（アウトソーシング）するか。
(3) 代替案の比較のポイント
　① 全体最適化計画との整合性
　② 各システム案の特徴及び相違点
　③ 費用対効果
　④ ユーザ評価
　⑤ 現行情報システムからの移行性

⑥ 他の情報システムとの整合性

(4) 検討結果の記録の目的

① 結果の保存と関係者の合意の記録として

② システム稼動後の評価のベースとして

③ 採用案の障害時のバックアップ用に準備する際の参考として

④ 他の情報システムの検討の参考として

2．分析

(1) 開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。

1 主　旨

要求定義の内容についてユーザ、開発、運用及び保守の各部門の理解を一致させ、確定したものとするため、要求定義は、ユーザ、開発、運用及び保守の責任者が承認する必要がある。

2 着眼点

(1) システム分析及び要求定義の手順を明確にしていること。
(2) 開発計画に基づいてシステム分析を行っていること。
(3) 要求定義を関係者が分析していること。
(4) ユーザ、開発、運用及び保守の責任者を明確にし、要求定義を承認していること。

3 関連事項

(1) 要求定義承認の主なポイント
　① ユーザ部門
　　a．要求定義項目の明確な理解
　　b．現行情報システムとの相違点、類似点の明確化
　　c．利用上の評価（操作性等）
　　d．実現時期
　② 開発部門、保守部門
　　a．要求定義項目の明確な理解
　　b．現行情報システムとの相違点、類似点の明確化
　　c．要求定義の実現可能性（技術的可能性、運用上の実現性、全体情報システムとの整合性、開発資源との整合性）
　　d．保守段階で必要とする体制（あるいは外部依存の可能性）
　③ 運用部門
　　a．要求定義項目の明確な理解
　　b．現行情報システムとの相違点、類似点の明確化
　　c．情報システム全体運用における整合性
　　d．機器・設備等の資源の利用の可能性（システムの能力・容量）
(2) 承認方法として定めるべき主な事項の例
　① 関連する承認者
　② 承認の時期

③ 確認、承認の方法、手順

④ 承認結果の記録方法

(3) 要求定義の承認方法の例

① 要求定義確認会の開催

② 開発計画書の承認

③ プロトタイプモデルによる確認

2．分析

(2) ユーザニーズの調査は、対象、範囲及び方法を明確にすること。

1 主　旨

ユーザニーズを的確に反映するため、事前にユーザニーズの調査の対象、範囲及び方法を明確にする必要がある。

2 着眼点

(1) ユーザニーズの調査の対象、範囲及び方法を事前にユーザと調整し、明確にしていること。

(2) 調査の対象、範囲及び方法は、ユーザニーズを的確に把握できるものであること。

(3) ユーザニーズの調査は、定められた調査の対象、範囲及び方法に基づいて実施すること。

3 関連事項

(1) ユーザニーズを調査するに当たっての留意事項

① 要求部門以外の関連部門まで含めた調査を実施すること。

② 要求部門には面接調査、関連部門にはアンケート調査等、調査対象に応じた方法を選択すること。

③ ユーザニーズの妥当性を確認するために、一般動向等の関連調査を実施すること。

④ 調査結果はユーザ部門にフィードバックすること。

⑤ EUC のユーザニーズの調査に当たっては、全社システムとの整合性、ユーザインタフェース等の調査を重点的に行うこと。

(2) ユーザニーズの調査方法の例

① アンケート調査……機能、操作性、処理能力、エラー対策等について質問形式で調査すること。

② 面接調査……操作性等、ユーザ部門の責任者と担当者に面接をして調査すること。

③ 実地調査……現行情報システムの操作性を実地に調査すること。

2．分析

(3) 実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。

1 主　旨

現行業務を的確かつ効率的に分析し、現行業務処理の流れ、手続、業務量等を把握するため、現状分析は、実務に精通したユーザ、開発、運用及び保守の担当者が参画する必要がある。

2 着眼点

(1) 現状分析は、調査対象業務及び情報システムに精通したユーザ、開発、運用及び保守の担当者が参画していること。

(2) 情報システムの機能、規模等を設定するために必要な情報を収集し、現状分析を行っていること。

(3) 分析結果は、将来展望を考慮して評価していること。

(4) 分析結果を記録していること。

3 関連事項

(1) 現状分析の分析項目の例

① 内部要因

a．業務処理手順……手続、業務フロー、事務処理の流れ

b．業務量……データの種類、取扱量、季節・日時変動

c．組織と要員……組織構成、業務分掌、牽制機能、要員数

d．他業務との関連……当該業務と関連する業務の範囲・接点

e．情報システム……情報システムの機能、機器構成、操作性、運用状況

② 外部要因

a．情報関連技術動向

b．業界動向

c．経済環境・動向

d．規制緩和、規制強化

(2) 現状分析に各部門が参画する目的の例

① ユーザ部門の参画

a．業務処理手順の確認、課題の抽出

b．現行、新情報システムの操作性の課題、要望の確認

c．業務部門の業務の流れに対応した手順等の伝達

② 開発部門、保守部門の参画

ａ．ユーザニーズの確認

ｂ．情報システムにおける実現妥当性の評価

ｃ．エラー時を含めた業務処理手順の確認

ｄ．他の情報システムの処理に与える影響の評価

③　運用部門の参画

ａ．運用に関するニーズの正しい把握

ｂ．要求事項の運用面における実現妥当性の評価

ｃ．他の情報システムの運用に与える影響の評価

2．分析

(4) ユーザニーズは文書化し、ユーザ部門が確認すること。

1 主　旨

ユーザニーズの調査結果を的確に開発計画の策定、開発業務に反映するため、ユーザニーズは文書化し、ユーザ部門の責任者が確認することが必要である。

2 着眼点

(1) ユーザニーズの調査結果を記録し、文書として整理していること。

(2) 調査結果には、調査の対象、範囲及び方法等を記録していること。

(3) 調査結果を記録し、ユーザの責任者が承認していること。

3 関連事項

(1) 文書化されたユーザニーズの活用方法

① ユーザ部門と開発、運用及び保守部門の認識を同一にする。

② 開発、運用及び保守段階におけるユーザニーズの再確認時に参照する。

③ 関連する他の情報システムとの整合性（インタフェース、処理機能等）を、他の情報システムの関係者が確認する。

④ 情報システムの開発完了時の評価指標とする。

(2) ユーザニーズを整理するに当たっての留意事項

① 実施した調査の調査日、場所、方法（アンケート調査、面接調査、実地調査）、対象の部門、及び関係者の職位等を記載していること。

② ユーザニーズは、要求事項の分野ごとにまとめ、同一内容のユーザニーズは整理すること。

③ ユーザニーズの文書化は、必ずしも紙媒体として作成されるものではないが、ユーザ部門の責任者が承認した内容は、そのことが分かる文書形態となっていなければならない。

2．分析

(5) 情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。

1 主　旨

情報システムの健全な運用を図るため、情報システムの導入に伴って発生する可能性のあるリスクを分析する必要がある。

2 着眼点

(1) リスク分析の対象を明確にしていること。

(2) リスクの発生頻度、影響度及び範囲を明確にしていること。

(3) リスクの種類に応じて、損害の内容及び損害額を算出していること。

(4) リスクへの対策を関係者が承認し、周知徹底していること。

3 関連事項

(1) 情報システムで発生するリスクの例

① システムの誤処理による不正データの出力

② 災害、機器障害、バグ、操作ミスによるシステムダウン、一部障害による処理停止

③ 災害による機器損害、破損

④ 不正行為によるデータ破壊、機密漏えい

⑤ コンピュータウイルスによるデータ破壊

⑥ 開発遅延、移行の誤処理による新システムへの切替失敗

⑦ 見積りミスによる費用の増加

(2) リスク分析の手順の例

① リスクの発見と確認

② 被害発生時の損害額の試算

③ リスクへの対策手段の調査と策定

④ リスクへの対策の実行

⑤ リスクへの対策結果の監視と評価

⑥ リスク対策の修正・変更

(3) リスクへの対策の手段の例

① リスク回避……損失事態が発生する可能性のある処理を避ける、あるいは他の手段で代替する対策（例：公衆回線から専用回線への変更）

② 損失予防……損失事態が発生する頻度を減少させる対策（例：火災に対する不燃材の使用）

③ 損失通報……損失事態が発生した場合、速やかに通報するための施策（例：センサー類）
④ 損失軽減……損失事態が発生しても、被害損失を減少させる施策（例：火災に対するスプリンクラ設置）
⑤ リスク分離……損失事態が発生した場合のほかの予備手段をもつ（例：システムの二重化）
⑥ リスク移転……被害損失を他のものに転移させる（例：保険）
⑦ リスク保有……被害発生時の損失を負担する（例：準備金等の対処）

2．分析

(6) 情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。

1 主　旨

情報システムの導入によって生じる業務、管理体制、諸規程等への影響を的確に把握し、情報システムの運用を円滑に行うため、業務等の新設、改変及び廃止、管理体制の変更、及び諸規程の見直しを行う必要がある。

2 着 眼 点

(1) 影響を受ける業務、管理体制、諸規程等の範囲を明確にしていること。
(2) 影響を受ける関係者が参画し、見直し等の検討を行っていること。
(3) 影響の程度及び範囲を明確にし、対応策を講じていること。
(4) 対応策を関係者が承認していること。

3 関連事項

(1) 情報システムの導入による業務、管理体制、諸規程等の見直しの例
　① 業務……組織の統合・廃止
　　・組織のスリム化（要員削減、関係会社への機能・権限の移管、組織機構の簡素化）
　　・外部への業務委託
　　・新規業務・事業
　　・ユーザ支援組織（ヘルプデスク等）の新設
　② 管理態勢……マネジメントサポート体制の強化
　　・ユーザ使用機器管理組織の新設
　　・ユーザ教育カリキュラムの推進
　③ 諸規程……業務分掌の見直し
　　・機器管理・運用規程の充実
　　・業務関連の諸手続・手順・管理ルール
(2) 見直しが必要な諸規程の例
　① 稟議規程
　② 人事・労務規程
　③ 業務分掌規程
　④ その他各種業務処理手続・規程

2．分析

(7) 情報システムの導入効果の定量的及び定性的評価を行うこと。

1 主　旨

開発計画で算出した効果に基づいて、合理的に効果を算出するため、情報システムの効果の定量的及び定性的評価を行う必要がある。

2 着眼点

(1) 情報システムの実現によって得られる効果を明確にしていること。
(2) 評価項目及び評価方法を明確にしていること。
(3) 定量的及び定性的評価を実施していること。
(4) 費用対効果を分析していること。
(5) 評価結果を関係者が合意していること。
(6) 開発計画と相違する評価結果については、理由を明確にしていること。

3 関連事項

(1) 定量的効果と定性的効果の例
　① 定量的効果……省人・省力化、在庫削減、物流費削減、欠品防止による売上増等、具体的に数値に換算できる効果
　② 定性的効果……経営管理情報の充実や顧客納期回答の迅速化、職場イメージの向上等、経営の質的向上に寄与する事項で、直接的には数値で把握できない効果
(2) 開発システムの効果算出の目的の例
　① 経営戦略、情報戦略との整合性の確認
　② 個別システムの開発の優先付け
　③ システム要件定義における機能目標設定の方向付け
　④ 情報システム稼動後における有効性評価の基準
(3) 開発システムの効果算出手順の例
　① 効果の類別化（効果の内容を的確に定義）
　② 定量的、定性的効果項目の明確化（定量的効果項目、定性的効果項目及び複合的効果項目の定義）
　③ 効果基準に対する寄与度の策定（直接的寄与度、間接的寄与度を考慮した策定）
　④ 費用対効果の算出（開発、運用費用の明確化と効果の算出）
　⑤ 効果の評価（費用対効果に基づく評価）

2．分析

(8) パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。

1 主　旨

情報システムが、期待された機能、効果を得られることを確認するため、パッケージソフトウェアの導入に際しては、機能、効果の観点からユーザニーズとパッケージソフトウェアの適合性を確認する必要がある。

2 着眼点

(1) 情報システムの処理におけるユーザニーズを整理していること。
(2) ユーザニーズに対するパッケージソフトウェアの対応状況を整理し、評価していること。
(3) 適合性の評価内容を関係者がレビューを行っていること。
(4) 適合性の評価結果は、ユーザ部門の責任者が承認していること。

3 関連事項

(1) パッケージソフトウェアの一般的な特徴
　① 特徴
　　a．既にソフトウェアとして完成しており、新たな開発の必要がない。
　　b．通常、稼動実績があり、処理の正当性が確認できている。
　　c．操作マニュアル等のドキュメントが揃っている。
　　d．導入手順が確立されている。
　② 留意事項
　　a．パッケージソフトウェアの処理内容が、現行の業務体系、処理手順に合わないことがある。
　　b．導入手順、カスタマイズ手順が確立されていないことがある。
　　c．稼動後の保守業務において、ノウハウ不足によって自組織体では対応できないことがある。
　　d．他の情報システムとの接続（業務処理面、情報システムのインタフェース等）が合わないことがある。
　　e．パッケージをカスタマイズして導入すると、パッケージのバージョンアップ時に、コストがかさむ、技術的な制約が生じる等がある。
(2) パッケージソフトウェアとユーザニーズとの整合性確認のポイント
　① 機能……ユーザ部門の業務の機能(将来機能も含めて)を満たしているか。
　② 業務処理体系、手順……ユーザ部門の現在の業務処理体系、処理手順との乖離は、許容で

きる範囲か。

ただし、BPR (Business Process Re-engineering) においては、パッケージソフトウェアの業務処理体系、処理手順に業務を合わすことも必要である。

③ 操作性、効率性……パッケージソフトウェアの操作性は、現場の実際の業務において問題がないか。またピーク時等に対する処理能力は、十分か。

3．調達

(1) 調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。

1 主　旨

構築する情報システムの機能、性能、品質等の要求を計画に従って達成するために、情報システムの構築に必要な各種の資源の調達要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認する必要がある。

2 着 眼 点

(1) 調達する資源を明確にしていること。
(2) 調達する資源は、開発計画及びユーザニーズに基づいて作成していること。
(3) 調達する資源の条件、必要事項を明確にしていること。
(4) 調達の要求事項は、ユーザ、開発、運用及び保守の責任者が承認していること。

3 関連事項

(1) 調達する項目
　① 資金……開発、運用及び保守業務を通したシステムライフサイクルに必要なコスト
　② 要員……開発業務の前段階では、開発要員を確保する。後半の段階から研修受講のため運用要員も加わる。要員は、自組織のみならず、外部からの調達も検討する。
　③ ハードウェア……開発用機器、テスト機器、本稼動用機器
　④ ソフトウェア……開発用ソフトウェア（オフィス業務用ソフトウェア、開発ツール等)、本稼動用ソフトウェア（ネットワーク、データベース処理用ソフトウェア等)
　⑤ ネットワーク……開発環境ネットワークと附帯機器・ソフトウェア、テスト用ネットワーク、本稼動用ネットワーク
　⑥ 設備……開発場所・設備、本稼動用サイト
(2) 開発計画と整合性がとれた調達の条件の例
　① 機能……開発計画における業務機能が実現できるソフトウェア、開発方法、要員のスキル
　② 性能……想定される業務量を処理できるハードウェア、ソフトウェア及びネットワーク
　③ 品質……信頼性目標を達成できるハードウェア及びネットワークの安定性、ソフトウェ

アの信頼性、品質向上に配慮された開発手法と開発支援ツール、スキルの高い要員

(3) ユーザニーズと整合性がとれた調達の条件の例

① 機能……ユーザの機能要件を満たしているパッケージソフトウェア

② 性能……満足できるレスポンスタイムを実現するハードウェア、ネットワーク及びシステム設計のスキルをもつ要員

3．調達

(2) ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。

1 主　旨

要求される機能、能力等を備えたシステム構成とするため、開発計画及びユーザニーズに基づき、ソフトウェア、ハードウェア、ネットワーク等を選択する必要がある。

2 着眼点

(1) 開発計画及びユーザニーズに基づく情報システムの実現に必要なソフトウェア、ハードウェア、ネットワーク等を明確にしていること。

(2) 機能、性能、費用、サービス、保守体制等を検討し、ソフトウェア、ハードウェア、ネットワーク等を選択していること。

(3) 他の関連する情報システムとのインタフェース及び拡張性を考慮し、ソフトウェア、ハードウェア、ネットワーク等を選択していること。

3 関連事項

(1) ソフトウェア、ハードウェア、ネットワーク等の選択に当たっての留意点

① 開発計画及びユーザニーズへの適合

a．機能の充足（業務機能、システム機能、運用機能）

b．運用の容易性（センター運用、ユーザ運用、ユーザでの操作性）

c．将来の拡張性（機器の拡張性、ソフトウェアのバージョンアップ）

d．導入時期の容易性（メーカー等のリリースと開発スケジュール）

e．相互の接続性（各機器とソフトウェアの接続、ソフトウェア間の接続）

f．効率要件の充足（処理能力、バッチ処理終了時間、サービス応答時間）

g．費用（導入費用、運用費用）

h．サポート体制の充実（導入時、稼動後の支援体制）

② 関連する他の情報システムとの整合

a．通信プロトコルの整合性

b．運用操作の統一性、整合性

c．ソフトウェアの移植性

d．開発手順・方法の統一性

e．機器の互換性

f．現行システム資産の継続性

3．調達

(3) 開発を遂行するために必要な要員、予算、設備、期間等を確保すること。

1 主　旨

情報システムの開発を着実に行うため、必要な要員、予算、設備、期間等を確保する必要がある。

2 着 眼 点

(1) システム分析に基づき、要員、予算、設備、期間等を確保し、組織体の長が承認していること。

(2) 要員、予算、設備等の投入の時期、期間、規模等を考慮していること。

(3) 能力及び経験を考慮し、要員を確保していること。

3 関連事項

(1) 開発を遂行するための資源確保のポイント

① 資金の確保

全体計画及び開発計画における予算計上と開発段階での予算の確保（ソフトウェア開発費用、ハードウェア費用、ネットワーク費用、運用費用）

② 要員の確保

開発（設計、プログラミング、テスト）要員、運用要員、間接支援（教育、ユーザ検証）要員の確保

③ 設備の確保

開発用設備、本稼動用設備、ユーザ設置環境（スペース・騒音対策等）・設備（電源等）

④ 期間の確保

開発スケジュールと他情報システムとの整合性、制度対応等の期日が定められている情報システムの対応

3．調達
(4) 要員に必要なスキルを明確にすること。

1 主　旨

開発計画で策定された機能、性能及び品質を実現するために、開発に関する組織内要員、組織外要員に必要なスキルを明確にする必要がある。

2 着眼点

(1) 開発、運用及び保守業務の各段階において、必要となる作業内容を明確にしていること。
(2) それぞれの作業内容に必要な要員のスキルを明確にしていること。
(3) 必要なスキルは、分野及びスキルの段階を設定して明確にすること。
(4) 必要なスキルは、自組織体内から調達するか、外部から調達するかを明確にしていること。

3 関連事項

(1) 要員のスキルの要素の例

開発、運用及び保守業務において関係者に求められるスキルの要素の例は、次のとおりである。1人の要員にこれらの多くのスキルを求めるのではなく、開発計画を実現するために、組織全体としてカバーする調達を行う必要がある。

① 開発業務

a．プロジェクト管理……開発段階の進捗管理、要員管理、品質管理、コスト管理等、プロジェクトマネジメントの運用ができるスキル

b．システム分析・設計……業務と情報システムのあるべき姿を明確にし、情報システムとして設計できるスキル、及びパッケージ等の特徴を把握し調達、活用できるスキル

c．プログラミング……プログラムの作成、パッケージソフトウェアの導入等で設計を実装することができるスキル

d．ドキュメンテーション…分かりやすい文書化（体系の工夫、明確な表現、可視化）ができるスキル

② 運用業務

a．運用管理……情報処理の全体の体系を理解し、障害等の異常処理に対する（対処の）判断ができるスキル

b．オペレーション……情報システムの処理状況の表示等から異常状態を認識できるスキル

c．設備管理……機器、付帯設備、場所・施設等の制約を把握し、平常時、異常時

にも的確な利活用ができるスキル

③ 保守業務

a．プロジェクト管理……保守段階の進捗管理、要員管理、品質管理、コスト管理等、プロジェクトマネジメントの運用ができるスキル

b．保守の設計……情報システムの変更要求を理解し、現行の情報システムにおける対応事項の抽出と対応方針・方法ができるスキル

c．プログラミング……テスト環境のもとで、現行情報システムのプログラム、データへの変更を行うスキル

3．調達

(5) ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。

1 主　旨

開発における必要な資源を適時に、要求事項に整合性をとり調達するために、ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って行う必要がある。

2 着 眼 点

(1) 開発に必要な資源の調達部門を定めていること。

(2) 調達のルールを定めていること。

(3) 調達のルールを、関連部門が承認していること。

(4) 調達のルールを、適宜、見直していること。

3 関連事項

(1) 調達ルールの項目の例

① 各部門の役割と責任（予算管理部門、調達した資源の利用部門、資源の管理部門、支払部門）

② RFI（Request For Information：情報提供要請）の発行

③ RFP（Request For Proposal：提案要請）の発行

④ 調達案件の起案（起案部門、申請書形式、起案内容のレビュー方法）

⑤ 見積方法（見積対象の条件、見積手順）

⑥ 評価（申請書の評価、優先度の決定方法）

⑦ 調達案件の決定（決定方法、関係者と権限）

⑧ 調達の実施（決定の通知、関連部門の役割、契約、検収方法、支払手順）

⑨ 調達のレビュー（評価項目・評価基準、評価者、次工程への反映）

(2) 調達ルールの見直しのタイミング

① 社内の組織変更、業務分掌

② 情報戦略の策定、全体最適化の観点の変更

③ 調達手段の変更、環境変化（例：関連会社の支援、海外からの調達）

3．調達

(6) 調達した資源は、ルールに従って管理すること。

1 主　旨

資源を開発計画に準拠し効果的に利活用するため、調達した資源は、ルールに従って管理する必要がある。

2 着眼点

(1) 調達する資源を明確にしていること。

(2) 調達した資源を管理するルールを制定し、ルールに従って管理していること。

(3) 調達した資源の活用状況を評価し、有効活用を図ること。

3 関連事項

(1) 調達した資源の管理ルールの項目の例

① 要員

a．氏名、所属等の個人の属性

b．経験、経歴、スキル

c．現在の担当業務、役割

d．将来の希望等

② 機器

a．調達先（ベンダー名、連絡先）

b．仕様、機能、性能

c．設置場所、あるいは利用システム名

d．管理責任部門、管理責任者、利用者

e．保守状況

f．障害記録（あるいは障害記録簿等とのリンク）

③ ソフトウェア

a．調達先（ベンダー名、連絡先）

b．仕様、機能

c．利用システム名

d．管理責任部門

Ⅲ.開 発 業 務

1．開発手順
2．システム設計
3．プログラム設計
4．プログラミング
5．システムテスト・ユーザ受入れテスト
6．移行

1．開発手順

(1) 開発手順は、開発の責任者が承認すること。

1 主　旨

開発手順が、システム分析及び要求定義で定めた要員、予算、期間等を満たしていることを確認するため、文書化された開発手順を開発の責任者が承認する必要がある。

2 理論的根拠／実務的配慮

(1) 開発の責任者を明確にしていること。

(2) 開発計画、開発方法に基づき、開発手順を定めていること。

(3) 開発手順を開発の責任者が承認し、関係者に周知徹底していること。

3 関連事項

(1) 開発の責任者

開発の責任者とは、開発手順を承認するだけではなく、その開発手順に従って実際にシステム設計、プログラム設計等を実施する要員を統括管理する責任者であり、対象となる開発システムの内容について精通し、決定権を有するものを指す。開発の責任者が複数で構成される場合には、それぞれの役割と権限を明確に定義する必要がある。

（開発が契約によって委託されている場合は、「Ⅳ．共通業務　5.委託・受託」を参照）

(2) 周知徹底すべき関係者

タイミングよく開発作業を行うには、開発手順に従って作業する要員だけでなく、各作業（例えば、入出力帳票の設計作業、入出力画面の設計作業等）ごとに、関連するユーザにも、あらかじめ作業実施に必要な内容を伝えることも必要である。特にレビュー作業が伴う工程では、レビュー時期を明確にして、進捗管理、品質管理、仕様のトレーサビリティ等を的確に行う必要がある。

1．開発手順

(2) 開発手順は、開発方法に基づいて作成すること。

1 主　旨

組織体として一貫し、効率的な開発作業を確実に遂行するため、開発手順は、組織体として標準化された開発方法に基づいて作成する必要がある。

2 着 眼 点

(1) 開発手順を明文化していること。

(2) 開発手順は、開発方法に準拠していること。

(3) 開発手順は、開発作業を遂行する上で必要な要件を満たしていること。

3 関連事項

(1) 開発方法と開発手順の関連

開発方法とは、標準化の方針に基づいて、情報システムの開発の手順、書式等のガイドラインあるいは手本のことである。開発手順とは、開発方法に基づいて個別の情報システム開発時に作成する手順書のことである。手順書には、誰が、いつ、どのような作業を、いつまでに、どの成果物を、どのような手段及び書式で作成するかを記載する。

(2) 開発方法の準拠性について確認する方法の例

ａ．第三者によるレビューの実施

ｂ．チェックリストの利用

ｃ．開発責任者によるウォークスルーの実施　等

(3) 作業遂行上必要となる要件の例

ａ．作業内容

ｂ．作業期間

ｃ．担当者

ｄ．必要とされるスキル

ｅ．成果物

ｆ．参照する文書　等

1．開発手順

(3) 開発手順は、開発の規模、システム特性等を考慮して決定すること。

1 主　旨

情報システムを効率よく開発し、かつ要求された品質を確保するため、開発手順は、情報システムの規模、期間、特性等を考慮して決定する必要がある。

2 着眼点

(1) 開発手順の決定理由を明確にしていること。

(2) 必要な作業項目を網羅していること。

(3) 作業の流れ、日程等に無理及び無駄がないこと。

(4) 開発上の重点管理項目を明確にしていること。

3 関連事項

(1) 情報システムの特性と開発手順との関連の例

次ページの表を参照。

(2) 重要な作業項目の例

各作業項目には、実施する作業内容に加え、作成する成果物や参照するマニュアル、ガイドライン等が定義されている必要がある。

① GUI（Graphical User Interface）を採用する場合の入出力画面設計の必要作業項目の例

a．画面フローの作成

b．画面レイアウト及び画面上のオブジェクトの配置

c．各オブジェクトのコントロールの定義

d．取り扱うデータの定義

e．メッセージの定義

f．プログラムとの関連性

(3) 作業の無理及び無駄排除の例

プログラミング作業の生産性の設定、期間、人数及びスキルの整合性を考慮することは、無理及び無駄を排除することにつながる。

(4) 重点管理項目の例

a．作業のクリティカルパス

b．関連する他の作業との順序

c．レビュー及びそのフィードバック

d．主要成果物

e．開発の責任者あるいはユーザによる成果物承認の方法及びタイミング

システム特性と開発手順との関連の例

システム特性の例	開発手順検討の例
・リアルタイムトランザクション処理 オーダ入力のように、単純で日常的な業務を対象とし、その時点で処理が完了するような単一のトランザクションを中心とする処理	・大量のトランザクション発生が想定されているシステムでは、ピーク時の負荷耐性、障害対応等のテスト手順が詳細に定義されていること
・バッチ処理 日次、週次、月次等のスケジュールに従って起動され、処理対象となるデータを一括して処理	・クライアントサーバシステムにおけるバッチ処理は、ジョブ制御、スケジュール管理等のツールを吟味検討し、技術的な実現方法を検討していること
・管理コントロール帳票出力処理 会計レポート、投資実績レポート等、管理者が組織をモニタし、管理するために必要な情報を提供する処理	・ユーザが必要とする情報を、タイムリーに効率的に検索、加工する方法を検討していること
・意思決定支援処理 情報検索・分析、経営戦略支援等、システムに蓄積された情報を参照・分析することによって、組織体活動の意思決定に役立てるための処理	・ユーザ要件の変化が早く、特定が困難であるため、ウォーターフォール型ではなく、スパイラル型のアプローチの適用を検討していること
・ワークグループサポート処理 電子メール、グループスケジュール、ワープロ等、組織内のユーザ間で情報の交換、蓄積、利用を行う処理	・汎用パッケージの利用を前提とするケースが多いため、パッケージの適用方法、手順を検討していること

(5) 開発方法・手順におけるソフトウェア開発プロセスの例

ソフトウェアの開発全体において、ソフトウェアの開発プロセスには、各工程の進め方について以下のような方法が存在する。

① 一方向型のプロセス

ソフトウェア開発全体において、各工程を段階的に一方向で１度だけ実施する開発方法のこと。

a．ウォーターフォール型

② 反復型のプロセス

ソフトウェア開発の工程を繰り返しながら、ソフトウェアを段階的に構築する方法のこと。

a．プロトタイプ型

b．スパイラル型　等

③ 統一プロセス（UP：Unified Process）

ユースケース駆動／アーキテクチャ中心／反復的でインクリメンタルの３つを大きな特徴とする開発プロセスのこと。

④ エクストリームプログラミング（XP：eXtreme Programming）

コーディングをソフトウェア開発の中心的存在としてとらえた、反復的でインクリメンタルな開発手法のこと。

⑤ パッケージソフトウェア利用型

汎用パッケージソフトウェアを利用し、業務とのFit & Gap分析を行い、最適なパッケージソフトウェアを導入する手法のこと。

1. 開発手順

(4) 開発時のリスクを評価し、必要な対応策を講じること。

1 主　旨

情報システムを開発計画どおりに高品質で効率よく開発するため、開発プロセス全般におけるリスクの洗い出しと評価を実施し、必要な対策を講ずる必要がある。

2 着 眼 点

(1) 開発プロセスの工程の機能を明確にしていること。
(2) 各工程単位に作業を進める上でのリスクを想定していること。
(3) リスクの評価を行い、対策を検討し、重要度の順番を付けていること。
(4) リスクの洗い出しにはユーザの代表者も参加していること。
(5) 主要なリスクが関係者の間で共通の認識になっていること。

3 関連事項

(1) 開発上想定されるリスクの例
　① 作業量の増加
　　a．作業の手戻り
　　b．設計書の理解不足、仕様の取違え
　　c．開発ツールの理解不足
　　d．コミュニケーション不足
　　e．ユーザからの追加・変更要求　等
　② 性能不足
　　a．設計書の理解不足、仕様の取違え
　　b．開発担当者のスキル不足
　　c．リソース（CPU能力、データ量等）の見積りの誤り
　　d．インタフェースの取違え　等
　③ 仕様の食違い
　　a．設計時の聞取り不足
　　b．開発担当者の思い込み
　　c．担当者の交代による引継ぎ不足
　　d．開発担当者の経験不足
　　e．未経験のツール、パッケージソフトウェアの使用　等
　④ 人的リスク

a．関係者の経験・訓練不足

b．関係者の傷病の発生

c．ユーザの責任者・担当者の交代

⑤ 調達等に関するリスク

a．予定されたハードウェア、ソフトウェアの納入遅れ

b．開発環境の構築遅延、失敗

c．ツール類の性能不足　等

(3) 開発時のリスク対応策

① 工程単位のレビューによる予定実績評価とフィードバック

② 文書・記録による確認

③ バックオフィスによるサポート体制

④ 関係者に対する教育の実施

⑤ 専門家の参加

⑥ 懸案事項のモニタリング

2．システム設計

(1) システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。

1 主　旨

システム設計書の品質を確保し、要求定義との整合性を図り、ユーザ、開発要員及び運用担当者の共有物とするため、システム設計書は、ユーザ、開発、運用及び保守の責任者が承認する必要がある。

2 着 眼 点

(1) ユーザ及び開発の責任者を明確にしていること。

(2) システム設計書をユーザ、開発、運用及び保守の責任者が承認し、関係者に周知徹底していること。

(3) システム設計書は、開発手順及びシステム設計マニュアルに基づいて作成していること。

(4) システム設計書は、必要な内容をすべて網羅していること。

(5) システム設計書と要求定義との整合性を確認していること。

3 関連事項

(1) システム設計書の内容の例

① システム概要説明

a．業務処理概要（新／旧）

b．入出力情報一覧／定義書

c．システムフロー／データフロー／会話フロー　等

② システム概要設計書

a．システム運用方式案

b．システム基本設計　等

③ ファイル設計書

a．E-R 図（Entity Relationship Diaglam）

b．ファイル一覧表

c．ファイル／データベース構造定義書

d．データベース定義書

e．トランザクションファイル定義書

f．テーブル定義書

g．コード定義書　等

④ システム詳細設計書

a．外部設計書
b．内部設計書　等

⑤　カスタマイズ設計書（パッケージソフトウェアの場合）
⑥　システム構成図
a．システム論理構成
b．ソフトウェア構成
c．ハードウェア構成
d．ネットワーク構成　等
⑦　システム性能分析
⑧　障害対策設計書
⑨　不正防止・機密保護機能設計書
a．セキュリティポリシーとの整合性
b．クローズドシステム／オープンシステムの区分
c．外部とのデータ交換時の対応　等
⑩　テスト計画書
a．システムテスト計画
b．ユーザ受入れテスト計画
⑪　ユーザ教育方針書
⑫　移行方針
⑬　システム運用管理方式概要
⑭　システム保守概要　等

(2) システム設計書の留意点

大規模なクライアントサーバシステムの場合は、システム最適化計画等で全社規模のシステム構成がグランドデザイン等として設計されていることが望ましい。

クライアントサーバシステム、Web 型システムの場合、処理やデータがサーバとクライアントに分散して配置されるため、システム概要説明書、ファイル設計書、システム構成図に関しては、サーバとクライアントへの分散配置に関して明確な記述が必要となる。業務処理の共通システム及び他の業務で関連するシステムとのインタフェースをとる場合、整合性を考慮した設計が必要になる。複雑なシステムの場合、処理データをどのように分散するかについての方針がシステム設計書に盛り込まれていることが望ましい。

外部に対してオープンなシステム（EDI (Electronic Data Interchange) や SCM (Supply Chain Management) 等）の場合は、データフォーマットやプロトコルの整合性への配慮、処理のタイミングやパフォーマンスへの配慮、更にセキュリティの確保には注意を払う必要がある。

なお、これらの設計書は承認するユーザが分かるように記述する必要がある。特に、前項「システム設計書の内容例」の②システム概要設計書、④システム詳細設計書、⑧障害対策設計書、⑨不正防止・機密保護機能設計書、⑩テスト計画書、⑪ユーザ教育方針書、⑬システム運用管理方式概要については、十分な配慮が必要である。

(3) システム設計マニュアルの内容の例

システムを設計するための開発方法に基づいたマニュアルであり、次の項目を記載する。

① 設計作業ステップと留意事項
② 成果物一覧
③ 必要スキル要件
④ システム概要説明の書き方
⑤ 入出力画面、入出力帳票、デザインガイドライン
⑥ 画面フローガイドライン
⑦ ファイル設計の方法と計画方法
⑧ システム構成図の書き方
⑨ 障害対策設計ガイドライン
⑩ 処理機能の分散化ガイドライン
⑪ データ配置の分散化ガイドライン

(4) 開発計画内容（あるいは要求定義）とシステム設計書との整合性の確認方法の例

① 設計成果物との整合性確認内容の例
  a．業務要求仕様との整合
  b．機能要求仕様との整合
  c．システムインフラストラクチャとの整合
② システム設計書完成段階でまとめて確認するのではなく、以下のように段階的に実施する。
  a．ユーザ要件確認終了後
  b．新システムを利用した業務イメージ確定後
  c．障害対策確認後
  d．不正防止・機密保護方法検討後　等

2．システム設計

(2) 運用及び保守の基本方針を定めて設計すること。

1 主　　旨

運用及び保守作業を円滑かつ効果的に推進するため、システム設計段階で運用及び保守の基本方針を定め、設計に反映しておく必要がある。

2 着 眼 点

(1) 運用の基本方針を定め、運用案を検討していること。

(2) 保守の基本方針を定め、保守手順を検討していること。

(3) 運用及び保守の基本方針を考慮したシステム設計を行っていること。

3 関連事項

(1) 運用の基本方針検討上の項目の例

① 運用の体制（管理体制、承認制度等）

② 日常運用（トランザクションスケジュール、承認スケジュール、バックアップスケジュール等）

③ 障害時運用（災害対策、エスカレーションフロー等）

④ 運用モニタリング　等

(2) 保守の基本方針検討上の項目の例

① 言語・ツール

② 保守の範囲

③ 体制

④ 手順

⑤ 保守のタイミング　等

2. システム設計

(3) 入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。

1 主　旨

データ入力時のミスの防止、作業効率の向上及び出力情報の利用効率の向上を図るため、入出力帳票、入出力画面及びコードは、ユーザが利用しやすいように設計する必要がある。

2 着 眼 点

(1) 開発方針及びシステム設計マニュアルに基づいて設計していること。

(2) ユーザの利便性に対する考慮点を明確にしていること。

(3) 入出力帳票、入出力画面及びコードをユーザがレビューしていること。

3 関連事項

(1) システム設計マニュアル

「Ⅲ. 開発業務　2. システム設計(1)の 3. 関連事項(3)」を参照。

(2) 利便性の基本的な考慮点

① 簡易性

初心者や稀にしかシステムを使用しないユーザにとっては、システムを簡単に操作でき、理解・推測しやすいことが重要である。

a．視覚的になじみやすいデザインにする。

b．アイコン、ボタン、絵等が何を意味したものか一目見て分かるようにする（ゴミ箱の絵、電話の絵等）。

c．ユーザが手順を覚えなくても操作できるデザインにする、等

② 一貫性

ユーザインタフェースが一貫していると、ユーザは既に習得した知識・技術を新しいシステムの操作に応用できる。１つのシステムに閉じた一貫性と複数のシステムにまたがる一貫性は、ともに重要である。一貫性に関する考慮点は、

a．配置の一貫性（画面の「了解」ボタンの位置等）

b．名称、表記の一貫性（英単語は、最初の文字は大文字で、それ以降は小文字等）

c．用語の一貫性　等

③ 効率性

ユーザが最も効率的に業務を遂行するための手段を提供する必要がある。

GUI を利用した入出力画面設計時の効率性に関する考慮点は、

a．マウスによる入力とキーボードからの入力を用意する等、複数の操作方法を提供する。

b．レスポンスを早くする。

c．バーコード入力、RFID（Radio Frequency ID）入力、音声入力等で省力化を図る

d．画面レイアウトの共通化を図る（一貫性と同様）。

e．期定値（Default）がある場合は自動入力を行う、等

④ 簡潔性

入出力帳票、入出力画面ともに外観は簡潔にする。一枚の帳票あるいは１つの画面の情報量を多くすると、それに比例する処理する業務の量も多くなるが、外観は複雑になる。逆に、情報量を少なくすると、帳票、画面数が多くなる。このトレードオフを適切なバランスで解決する必要がある。

(3) 入出力帳票、入出力画面、コードについての考慮点

① 入力帳票設計

a．ユーザの了承を得ているか。

b．記入しやすく設計しているか。

c．照合しやすく設計しているか。

d．重要な帳票には、連番等を付しているか。

② 出力帳票設計

a．ユーザの了承を得ているか。

b．利用しやすく設計しているか。

c．出力情報の量や保管等を勘案して設計しているか。

d．機密保護を配慮して設計しているか。

③ 入出力画面設計

a．ユーザのスキルレベルを考慮して設計しているか。

b．GUI を採用する場合、対象となる業務に合致しているか。

c．入力方式（バーコード入力、音声入力等）は効率性を考慮しているか。

d．画面上の情報量は適切で、見やすく配慮しているか。

e．ユーザの操作ミスを少なくさせる配慮をしているか、等

④ コード設計

a．体系化しているか。

b．他業務、他システムとの整合性をとっているか。

c．意味、機能、使用上の条件を明確にしているか。

(4) ユーザによるレビュー方法

レビュー対象となる設計書の例

① 入出力帳票設計書

② 入出力画面設計書

③ コード一覧表　等

特に、GUI を使用する場合、外観だけでなく操作性を含めてユーザのレビューを受ける必要があるため、入出力画面設計書のように紙ベースで仕様を決定するのは困難である。開発ツール等を用いて実際に画面を作成し、実物を見ながら検証作業を実施する方法が現実的である。

(5) パッケージソフトウェアを導入する場合の注意点

① ERP パッケージの場合

業務・システムの統合を目的として ERP（Enterprise Resource Planning）パッケージを利用する場合は、利用者の使い勝手を優先すると、かなり追加の費用が発生する場合がある。そのため一般的には ERP パッケージ仕様に合わせて業務を変えることによって、業務効率化を目指すことになる。最適化計画の中では、まず、業務の見直しを実施し、その業務改善を前提にシステムを導入するのが理想の姿である。

この場合は現状の業務ではなくターゲットとする業務との Fit & Gap 分析を実施することになる。

② パッケージソフトウェアの多くは、当初は特定のユーザ企業の業務をターゲットにしてシステム化している場合が多く、その時点・その企業での使いやすさを追求したものが多い。

パッケージソフトウェアがユーザ企業に合わない場合は、次のケースが考えられる。

a．入力方式が DUM 端末形式になっていて使いづらい。

b．業務の形態が合わない。

c．データ保持形式のテンプレートが合わない、等

パッケージソフトウェアはそのまま利用するのが原則であるが、入出力画面、入出力帳票等のユーザインタフェースに関しては、業務効率を優先する場合は、フロントエンドのシステムやカスタマイズでカバーする場合がある。

パッケージソフトウェアの品質の確認に関しては、提供しているサプライアの監査等で補う。

2．システム設計

(4) データベースは、業務の内容及びシステム特性に応じて設計すること。

1 主　旨

大量及び多種のデータを効率よく格納し、データ群の中から必要な情報を要求定義を満たす性能で検索し、更新できるようにするため、データベースは業務の内容に応じて設計する必要がある。

2 着眼点

(1) 業務の特性に基づいて、データベースの利用形態を明確にしていること。

(2) データモデルの選定理由を明確にしていること。

(3) 利用するDBMS（DataBase Management System）は、十分な機能及び性能を有していること。

(4) データベースは、データの利用形態を考慮して設計していること。

(5) データベースは、データ量の増加を考慮して設計していること。

3 関連事項

(1) データベースの利用形態

データベースの利用には、検索及び更新（削除を含む）があるが、それぞれのデータベースに対してのアクセス方法、アクセス量、頻度等を定義する必要がある。

(2) データモデルの種類と特徴

モデル	業務	データ量	アプリケーションの自由度
階層モデル	定型	大	小
ネットワークモデル	定型	大	大
リレーショナルモデル	非定型	小	大
多次元モデル	非定型	小	大

(3) データベースの機能

クライアントサーバシステムに求められるデータベース機能の例

① リモートデータベースアクセスにおいて必要な機能

a．コード変換（サーバとクライアント間）

b．２フェーズコミット（複数のコンピュータ上に格納されたデータに対する更新を同期させる機能）

c．ストアドプロシージャ（複数のデータアクセス処理を１回の呼出しで実行できるよう、サーバ上に登録しておく機能）

d．トリガ（あるデータが特定の条件を満たしたときに、あらかじめ用意しておいた処理を

起動する機能）

e．マルチスレッド（複数の処理要求をサーバプロセスで処理する機能）

f．レプリケーション（必要なタイミングでマスタデータの複製を作成する機能）

g．異なるデータベース間のアクセス　等

(4) データベースの性能

① データの格納効率

② インデックス定義／詰込み率

③ データのメンテナンス

④ 検索速度

⑤ 検索の容易性

⑥ 排他制御方式　等

(5) 設計上の配慮点

① データベースの配置方法の例

a．集中管理

b．分散管理

c．集中／分散管理　等

② データベースの分散配置の考慮点（クライアントサーバシステムの場合）

a．データの最新性

b．データボリューム

c．ネットワークの伝送容量

d．サーバの処理能力　等

③ データの複製に関する考慮点

a．マスタとスレーブの定義

b．複製のタイミング

c．データの洗替えの方法（全件ダウンロード／更新分のデータのみ）

2．システム設計
(5) データのインテグリティを確保すること。

1 主　旨

データ処理の正確性を保証し、データ入力から出力に至るすべての過程におけるデータの誤びゅう、重複、脱落等を防止し、改ざんがないことを示すため、データのインテグリティを確保する必要がある。

2 着眼点

(1) データのインテグリティを確保すべきチェックポイントを明確にしていること。
(2) データのインテグリティを確保するためのチェック機能を設計していること。
(3) チェック結果を記録する機能を組み込んでいること。

3 関連事項

(1) インテグリティ

インテグリティ（Integrity）とは、データ及び情報が正確で完全であり、かつ正確性、完全性及び正当性が維持されていること。また、ソフトウェアがそのような機能を備えていること。具体的には、データ入力から出力に至るすべての過程におけるデータの誤びゅう、重複、脱落等を防止し、アクセス権設定や履歴管理で改ざんがないことを示すことをいう。

(2) インテグリティ確保のための業務統制

インテグリティを確保するためには、業務上のコントロールを確保している必要がある。業務統制を行うには、次のような体制・ルールの策定と、実施結果の確認が必要である。

① 体制の整備（業務責任者、業務担当者の明確化等）
② 業務プロセスの明確化（業務処理への報告制度、承認制度等）
③ 業務手順書等の整備
④ データや情報の確認制度（原本保持、ダブルチェック、履歴管理等）
⑤ アクセス権の定期的確認
⑥ 定期的検査　等

(3) チェック機能、チェック結果の例

チェック機能	ポイント	チェック結果
① ハッシュトータル	処理の前後	① 入力あるいはデータ転送の際に、金額等の数値を合計し、処理の前後が一致することを確認
② ファイル間の整合性チェック	処理の前後	② ファイル数／ファイル内のレコード数等が処理前後で一致することを確認
③ DBMSがサポートする整合性維持機能	入力時／一定のタイミング	③ データの各フィールド値が指定された範囲又はパターンと一致することを確認

2．システム設計

(6) ネットワークは、業務の内容及びシステム特性に応じて設計すること。

1 主　旨

大量及び多種のデータの要求定義を満たす性能で伝送するため、ネットワークは、業務の内容及びシステム特性に応じて設計する必要がある。

2 着 眼 点

(1) 業務の内容及びシステム特性に基づいて、ネットワークの利用形態を明確にしていること。

(2) 利用するネットワークの種類及び選定理由を明確にしていること。

(3) 利用するネットワークは、適切な性能を有していること。

(4) 利用するネットワークは、適切なセキュリティを有していること。

3 関連事項

(1) ネットワーク利用形態の例

業務の特性	ネットワーク利用形態
即時性	オンラインリアルタイム通信
バッチ処理	ファイル転送通信
情報の多様性	マルチメディア通信
同報性	ブロードキャスト通信
移動性	モバイル通信
機密性	暗号化・ユーザ認証
経済性	公衆回線・専用回線、ADSL 回線等

(2) ネットワークの種類とその選定理由

ネットワークの種類	ネットワーク利用形態
イーサネット	クライアントサーバ間あるいはサーバ間
FDDI (Fiber Distributed Data Interface)	幹線 LAN として、あるいはトラフィックの集中するホスト機・サーバ等を接続
無線 LAN	クライアントサーバ間の無線形式の近距離 LAN
スイッチ	サーバ間、ルータとサーバ間、ルータ間等
専用回線	ホスト機と端末機の接続。使用率の高い LAN 間の相互接続
フレームリレー	地理的に散在した LAN を相互接続
光ファイバ	光ファイバを利用した通信サービスで、地理的に散在した LAN を相互接続
非対称型ディジタル加入者線 (ADSL)	上り通信と下り通信の通信速度が異なるメタリックケーブルを利用した加入者線形式の高速通信
加入電話網	移動先からの通信や地理的に散在する場所との通信を行う有線形式の加入電話
モバイル通信	携帯電話、PHS 等移動先からの無線形態の加入電話通信

ある業務上の要件を満たすための通信手段は、複数存在するのが一般的である。ここでのポイントは、これら複数案を、接続性、性能、経済性、運用性、将来性、セキュリティ等の観点から検討した上で選択することが重要である。

(3) 性能上の考慮点

① 物理的伝送速度
② 交換処理能力
③ 交換処理遅延
④ 実行能力（スループット）
⑤ 回線使用率
⑥ 回線エラー率、破棄率
⑦ ネットワークトポロジ
⑧ 回線接続時間
⑨ 同時接続　等

(4) セキュリティ上の考慮点

① 回線上の盗聴防止
② バックアップ回線
③ 回線接続点でのアクセス制限
④ ネットワーク監視
⑤ 認証機能
⑥ 内部アドレスの隠蔽　等

(5) 投資効率からの考慮点

① 重点システム（内部ファイアウォールの設置等）と一般システムの区分け
② モバイル接続のセキュリティと制限（RADIUS（Remote Authentication Dial-In User Service）サーバの設置等）
③ 重点利用回線（専用線等）と一般回線（公衆回線接続等）の区分け　等

2．システム設計

(7) 情報システムの性能は、要求定義を満たすこと。

1 主　旨

情報システムに期待される効果を実現するため、情報システムの性能は、要求定義を満たす必要がある。

2 着眼点

(1) 情報システムの性能分析に基づいて設計していること。

(2) 要求定義を満たす性能の確保が困難な場合、要求定義の見直しを検討していること。

(3) 要求定義の見直しは、技術的及び経済的な観点から理由を明確にしていること。

(4) 要求定義の要求から溢れた機能を明確にし、記録として残していること。

3 関連事項

(1) 性能の定義

情報システムの性能とは、情報システム全体として、一定のコストで定められた時間内に処理を完了する能力をいう。

システムが業務に対して要求仕様に基づいて性能を発揮することを確認するためには、システム自体にモニタリングする機能を組み込んでいる必要がある。モニタリングの基本方針は情報戦略の情報化投資の段階で検討され、開発計画で具体化されていなければならない。

性能評価の指標の例として、「Ⅳ．運用業務　2.運用管理(16)」を参照。

(2) 性能分析の方法と考慮点

① 方法

a．机上計算

b．ベンチマークテスト　等

特に、クライアントサーバシステムでは、複数のソフトウェア、ハードウェア及びネットワークが混在しており、システム処理やデータが複数箇所に分散していることから、システムの性能予測は困難となる。求められる性能が得られるか、システム設計段階（あるいは製品選定段階）よりベンチマーク等の手法を用い、測定する必要がある。

② 考慮点

a．CPU、メモリ、ディスクの環境設定

b．データ及び処理の分散

c．通信・コミュニケーション

d．並行・同時処理

e．セキュリティ　等

2. システム設計
(8) 情報システムの運用性及び保守性を考慮して設計すること。

1 主　旨

情報システムの円滑な運用を図り、トラブルの原因を速やかに発見し、有効な対策、改善等のための保守作業を効果的に行うため、運用業務及び保守業務で必要となる性能管理、構成管理、障害対策等の技術的な実現方法を考慮した上で設計する必要がある。

2 着 眼 点

(1) 運用の基本方式を検討していること。
(2) 運用における処理のボトルネックを検討していること。
(3) 運用性及び保守性を確保する技術的実現方法を検討していること。

3 関連事項

(1) ユーザ要件（機能要件）及び品質要件の項目の例
　① レスポンスタイム、エラップスタイム
　② バッチ処理時間
　③ オンライン稼動時間
　④ プログラムエラー率
　⑤ 平均故障間隔時間　(MTBF ： Mean Time Between Failures)　等
(2) 性能管理のための考慮点（性能管理については、「Ⅲ. 開発業務　2. システム設計(7)」を参照）
　① CPU、メモリ、ネットワークの使用率計測方式
　② オペレーティングシステムのページフォルトや、ネットワーク上のエラーパケットの発生率の計測方式等
(3) 構成管理のための考慮点（構成管理については、「Ⅳ. 運用業務　9. 構成管理」を参照）
　① ソフトウェア／データの配信方式
　② ハードウェア／ソフトウェアモジュールの構成
　③ ネットワーク構成管理の方式　等
(4) 障害対策のための考慮点
　（「Ⅳ. 運用業務　2. 運用管理(10)」を参照）
(5) 運用管理ツールの例
　① システム全体の状況を把握するための運用管理ツール
　② ネットワーク及びハードウェアの状態を監視するネットワーク管理ツール

クライアントサーバ型システムでは、一般的にプログラムとデータが分散して配置されているため、統合的な性能管理が可能な管理ツールの適用を検討すべきである。

(6) システム監視の手順の例

① 定期的にシステムの性能を監視し、記録する。

② 性能記録等を評価する。

③ 性能に関する記録及び評価結果は、定期的に運用の責任者へ報告する。

(7) サポート体制の構成

① システムの性能についての定期的な監視と記録の担当者

② 性能に関する報告を受け、今後の性能管理計画の立案を行う担当者

(8) 保守の要件項目の例

① 基本構成（OS、言語、開発ツール等）

② 機能構成

③ モジュール構成

④ コーディング方式　等

2. システム設計

(9) 他の情報システムとの整合性を考慮して設計すること。

1 主　旨

システムの設計を行う場合、当該システムだけではなく、ITインフラストラクチャや他の情報システムとの整合性を考慮して設計を行う必要がある。

2 着眼点

(1) ITインフラストラクチャとの整合性を評価していること。

(2) 基本アーキテクチャ（EA）が制定されている場合は、遵守度を評価していること。

(3) 業務間の共通システムが存在する場合は、その共通システムとの整合性と影響度を評価していること。

(4) データの授受を行う情報システムとの整合性と影響度を評価していること。

(5) ポータルに組み込まれる場合は、全体との調和をとっていること。

3 関連事項

(1) ITインフラストラクチャとの整合性の内容例

① システム構成

② ドメインと認証方式

③ トランザクション量とネットワークに流れるタイミング

④ データ授受の方式、データ量、タイミング等

⑤ マスタデータ等との整合性

⑥ 運用サイクル（モニタリング、バックアップ等）

⑦ インフラリソース（電力量、発熱量、設置スペース、管理要員数、バックアップメディアの数等）

⑧ ポータルのデザイン　等

2．システム設計

(10) 情報システムの障害対策を考慮して設計すること。

1 主　　旨

情報システムの障害発生を未然に防止し、障害の影響を最小限にとどめ、速やかに回復させるため、情報システムの障害対策を考慮して設計する必要がある。

2 着 眼 点

(1) 情報システムの信頼性指標を設定していること。

(2) 障害対策を講ずる対象を明確にしていること。

(3) 障害対策機能を設計していること。

3 関連事項

(1) 信頼性の指標の例

① 平均故障間隔時間（MTBF ： Mean Time Between Failures）

② 平均故障修復時間（MTTR ： Mean Time To Repair）

③ プログラムエラー率

(2) 障害対策を講ずる対象

① ソフトウェア

② ハードウェア

③ ネットワーク

④ データベース　等

(3) 障害の原因

① 災害

② 故障

③ エラー(プログラムエラー、操作ミス等)

④ コンピュータ犯罪　等

(4) 障害対策機能の例

障害対策機能の例	障害の原因			
	災害	故障	エラー	コンピュータ犯罪
a．障害時の代替機能	○	○	○	○
b．負荷状態の監視制御機能		○	○	
c．障害箇所の検出及び切分けの仕組み	○	○	○	○
d．障害時における縮退・再構成機能	○	○		
e．チェックポイント、リスタート機能		○	○	
f．ファイルのバックアップ・リカバリ	○	○	○	○
g．コンピュータネットワークにおける障害検知・代替機能	○	○		○
h．クライアントサーバシステムにおけるノード端末のリモートメンテナンス		○	○	

なお、クライアントサーバあるいはEUC環境における障害対策は、適用業務の重要性、緊急性を考慮し、その達成指標を設定し、対策レベルを決定することが現実的である。

(5) バックアップの対象、方法の種類

バックアップ対象	方法の種類	手　段
データベース、ファイル	ファイルバックアップ／差分バックアップ	自動バックアッププログラムの作成・実行 汎用バックアップツールの利用 予備装置の設置 バックアップセンタへのファイル転送
アプリケーションプログラム	フルバックアップ（複数世代管理）	自動バックアッププログラムの作成・実行 汎用バックアップツールの利用 ソフトウェア会社からの再調達(汎用ソフトウェアの場合) バックアップセンタへのファイル転送
各種環境定義データ	フルバックアップ	自動バックアッププログラムの作成・実行 汎用バックアップツールの利用 予備装置の設置 バックアップセンタへのファイル転送

なお、組織体内又は委託先の間でバックアップが行われている場合は、その工程及び方法が適切であるかを確認すること。特にクライアントサーバシステムの場合、複数箇所に分散されたデータのバックアップが確実に実行される必要がある。

2．システム設計

(11) 誤謬防止、不正防止、機密保護等を考慮して設計すること。

1 主　旨

情報システムの安全性を確保し、健全な運用を確保するため、誤びゅう防止、不正防止、機密保護及びプライバシー保護の機能を考慮して設計する必要がある。

2 着 眼 点

(1) 想定されるリスクを明確にしていること。

(2) リスクに対応するコントロール機能を設計していること。

(3) コントロール結果を記録する機能を設計していること。

3 関連事項

(1) リスクの例

① 責任者、権限者以外のデータベースへのアクセス

② ファイル、データ内容の破壊

③ ハードウェアの物理的破壊

④ メッセージの改ざん

⑤ 通信上のデータ盗聴

⑥ 通信ミスによるデータ漏えい

⑦ 妨害行為（なりすまし、踏み台、DoS 攻撃、デマメール等）

⑧ 機能選択ミス、入力ミス　等

(2) コントロール機能、コントロール結果の例

次ページの表を参照。

クライアントサーバシステムや Web 型システムの場合、プログラムやデータが各拠点に分散されるため、特にｄ、ｅ、ｆ、ｇ、ｊの対策は重要である。

コントロール機能、コントロール結果の例

コントロール機能	コントロール可能なリスク								
	責任者、権限者以外のデータへのアクセス	ファイル、データ内容の破壊	ハードウェアの物理的破壊	メッセージの改ざん	通信上のデータの盗聴	通信ミスによるデータの漏えい	妨害行為	選択ミス、入力ミス	コントロール結果
a．資格確認機能（識別コード、パスワード等によるユーザプロファイル管理）	○	○		○			○		資格者以外のアクセス防止
b．各資源へのアクセス制御機能	○	○		○			○	○	資格者以外のアクセス防止
c．モニタリング機能（アクセスモニタリング…違反アクセスの記録、コンソールログ、システム使用状況記録）	○	○		○	○	○	○	○	不正アクセスの発見、追跡
d．本人確認機能、相手先確認機能	○	○		○			○		不正に入手した他ユーザの識別コード、パスワード使用の防止
e．暗号化機能（回線上のデータの暗号化等も含む）	○	○		○	○	○			メッセージ、データの暗号化による不正アクセス・盗聴発生等のリスクの軽減
f．公衆回線経由のアクセスに対するコールバック、端末ID検知機能、認証サーバ設置	○	○		○	○	○	○		不正に入手した他ユーザの識別コード、パスワード使用の防止
g．外部ネットワークに対するファイアウォール	○	○		○	○	○	○		外部ネットワークからの不正侵入防止
h．コンピュータウイルス検出／修復ツール		○		○				○	過去の被害事例と同様の被害の発生防止
i．ソフトウェアライセンスの不正使用防止／監視機能	○							○	不正使用による罰則、企業イメージ低下の回避
j．ハードウェア、ネットワーク施設の入退室管理		○	○					○	物理的な破壊の防止

2．システム設計

(12) テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。

1 主　旨

情報システムが設計どおりに開発されたことを確実かつ効率的に確認するため、テスト計画の目的、範囲、方法、スケジュール等を明確にする必要がある。

2 着眼点

(1) テストの種類、目的、体制及び実施方法を明確にしていること。
(2) 信頼性、安全性、効率性及び有効性のテスト項目を定めていること。
(3) テストデータの仕様を作成していること。
(4) 性能の測定及び分析方法並びに性能のチューニングポイントを明確にしていること。
(5) テスト実施に必要な期間を設定していること。
(6) テスト結果の検証方法・体制を明確にしていること。
(7) 開発側のテストとともに、ユーザ受入れテストも考慮していること。

3 関連事項

(1) テストの種類の例
　① 単体テスト
　② プログラム結合テスト
　③ ストリングテスト
　④ サブシステムテスト
　⑤ システムテスト
　　a．機能テスト
　　b．耐久テスト
　　c．ピーク時テスト
　　d．ライブデータテスト
　　e．障害対応テスト　等
　⑥ ユーザ受入れテスト
　　a．設置確認テスト
　　b．機能確認テスト
　　c．要求仕様適合性テスト
　　d．セキュリティテスト
　　e．日常運用テスト

f．障害時運用テスト

g．ユーザの教育訓練　等

クライアントサーバシステムの場合、プログラムやデータの分散配置及びプログラムの構成要素が増えることから、ホスト集中型システムに比べて、必要となるテストの種類と検証すべき項目が増大するため、それに見合ったテストの種類の定義が必要となる。外部に公開するWeb型のシステムの場合、公開前にセキュリティ機能を十分にテストし、確認しておく必要がある。

(2) テスト項目の例

① 信頼性

a．障害検知能力

b．フェイルセーフ機能、フェイルソフト機能

c．リカバリ機能

d．ストレス耐性　等

② 安全性

a．識別・認証機能

b．アクセス管理機能

c．ファイルの保護

d．回復処理　等

③ 効率性

a．処理能力

b．レスポンスタイム計測

c．ターンアラウンドタイム計測

d．ボトルネック検出

e．ハードウェア等の資源利用度の計測

f．端末機等の操作性確認　等

④ 有効性

各種の目標値との適合等

(3) テストデータの仕様の例（単体テスト、プログラム結合テスト等の場合）

① 正常処理の検証用データ

② エラー／例外処理の検証用データ

③ プログラムのチェック機能の検証用データ

④ 共通テストデータ　等

これらのテストデータの仕様は、テストの種類及びテスト項目に対応して定義する必要がある。

(4) テストデータの仕様の例（システムテスト、ユーザ受入れテスト等の場合）

① 標準テストデータ

② マスタデータ

③ 負荷試験用データ

④ アブノーマルデータ　等

クライアントサーバシステムの場合、汎用システムのように本番環境にパーティションを区切

ったテスト環境をもつことは困難である。本番環境とは別にテスト用の擬似環境等を構築してテストを行うと、本番環境に影響を与えることなく実稼動に近いテストを行うことができる。

(5) 性能の測定及び分析方法の例

① 大量のテストデータ作成のためのテストデータ作成プログラムの用意

② WAN (Wide Area Network) 回線のシミュレートと性能測定等を行うための WAN 回線シミュレータの利用

③ プログラム処理時間、通信時間等の数値取得プログラムの用意

④ DBMS の機能によるデータアクセス時間（参照、更新に必要な時間）の取得　等

(6) テスト結果の検証方法の例

① 検証内容のチェックリストの用意

（特に、GUI の操作に関しては、検証項目が多く、チェックリストの用意に工夫をする）

② 出力画面上のフィールド、出力帳票上のデータ、ファイル／データベース内容の自動マッチング

③ テスト目標、テスト項目、テストデータとの整合性等確認・検証

(7) チューニングポイントにかかわる留意点

通常、システムのチューニングを実施するポイントは、システムテストやユーザ受入れテスト等のように、後続のテスト段階になるほど必要性が増してくることが多いが、単体テスト等の初期の段階から常にチューニングの可能性を検討しておくことが重要である。次のポイントを常に考慮する必要がある。

① 性能要件との突合

② バッチ処理の並列実行の可能性の検討　等

(8) その他

① EUC 環境でのシステムのテストには、その適用業務の特性に応じた配慮が必要である。

2．システム設計

(13) 情報システムの利用に係る教育の方針、スケジュール等を明確にすること。

1 主　旨

情報システムを円滑に導入し、期待される効果を実現するため、情報システムの利用にかかわるユーザ教育方針、スケジュール等を設計時に明確にする必要がある。

2 着 眼 点

(1) ユーザ教育の対象者、教育の種類、内容、方法等を明確にしていること。
(2) ユーザマニュアル等の作成手順及び承認手続を定めていること。
(3) ユーザ教育に必要な資源を明確にし、確保していること。
(4) ユーザ教育の方針等をユーザの責任者がレビューしていること。

3 関連事項

(1) ユーザ教育の対象者と内容の例
　① 新システムを利用する全ユーザに直接あるいは間接的に教育を実施すること。
　② システムの提供する機能によって利用するユーザが異なる場合は、教育を受講するユーザのグループ化等を考慮すること。
　③ 教育内容の例
　　a．システムの概要
　　b．現行システムとの相違
　　c．業務に与える影響
　　d．システムの操作方法
　　e．システム利用上の注意点
　　f．障害発生時の対応方法　等
(2) ユーザ教育の種類
　① 新システム運用前の研修
　② 新システム運用後の継続的な研修
(3) ユーザ教育の方法と考慮点
　① インストラクタによる講習
　② 教材テキスト・CBT（Computer Based Training）（e ラーニング）等を利用した自習
　③ OJT
(4) ユーザ教育に必要な資源の例
　① インストラクタ

② 研修の開発に要する費用と時間

③ 教材

④ デモシステム

⑤ 研修環境(研修室、研修用機器等) 等

(5) その他

① クライアントサーバシステム、EUC の環境における教育においては、ユーザ業務での利用法のみでなく、非定型型データ加工方法や、ユーザサイドのシステム運用方法、コンピュータウイルス感染防止に関する教育及びライセンスコピー遵守に関するモラル教育も必要になる。

② ユーザマニュアル等は、新システムの本稼動前のシステムテストにおいて、マニュアルの内容チェックのために使用する。システムテスト段階前にこれらのマニュアルを準備しておく必要がある。

2. システム設計
(14) モニタリング機能を考慮して設計すること。

1 主　旨

システムの稼動後に、システム開発計画の主旨に基づき、当該システムが設計どおりの性能を発揮しているかを確認するため、システム内にモニタリングの機能を組み込み、定期的に測定・解析する必要がある。

2 着 眼 点

(1) 開発計画時にモニタリング対象の指標と目標値を選定していること。
(2) 評価項目はユーザの責任者が確認をしていること。
(3) モニタリングの項目・特性値に基づき、評価指標がとれる機能をシステムの設計に組み込んでいること。
(4) モニタリング項目を継続的に測定できるようにしていること。

3 関連事項

(1) 業務システムに関するモニタリング項目の内容例
　業務システムのモニタリング項目については、「Ⅳ. 運用管理　2. 運用管理(15)の3. 関連事項」も参照。
　① 業務データ
　　a. データ登録件数推移
　　b. データ修正件数推移
　　c. データ検索件数、ヒット率の推移
　　d. 比率指標（売上高利益率、資本回転率、在庫回転率、在庫引当て率等）
　　e. データ投入完了からレポート作成までの時間
　　f. 平均レポート処理時間　等
　② 運用データ
　　a. クレーム件数、解決件数
　　b. ヘルプデスク問合せ件数、問合せ待ち時間
　　c. マニュアル改定頻度
　　d. 障害件数、平均停止時間
　　e. 保守の頻度、金額
　　f. 変更案件件数　等
(2) 情報システムの稼動条件に関するモニタリング項目の内容例

① CPU の使用率
② メモリの使用率
③ ディスク容量の使用率
④ データベース領域の容量と使用率
⑤ テーブル数、データ数、ユーザ数
⑥ データベースアクセス件数
⑦ ネットワーク負荷　等

2. システム設計

(15) システム設計書をレビューすること。

1 主　旨

システム設計書は、情報システムに対するユーザ要求を適切に反映させている必要があり、ユーザ、開発、運用及び保守の各部門の関係者も参加してレビューを行い、適切に評価する必要がある。

2 着眼点

(1) システム設計書のレビュー時期が開発計画書で明確にされ、レビュー時までにシステム設計書を適切に作成していること。
(2) レビューにはユーザ部門、開発部門、運用部門及び保守部門が参加していること。
(3) レビュー評価を適切に行っていること。
(4) レビューの終了ポイントや終了条件を明確にしていること。
(5) レビュー結果はルールに基づいて記録し、適切なフィードバックと処置を行っていること。

3 関連事項

(1) システム設計書レビュー時期設定方法の例
　① 定期的レビュー（一定期間ごとにレビューする）
　② 成果物ポイントレビュー（成果物単位にレビューする）
　③ 進捗率レビュー（進捗率に応じてレビューする） 等
(2) システム設計書のレビュー評価項目の例
　① ユーザ要求の項目の網羅の度合い
　② ユーザ要求の内容の反映度合い
　③ システム構成の適切性の度合い
　④ 業務処理方式の適切性の度合い
　⑤ 性能等の机上評価
　⑥ 既存システムへの影響度の評価
　⑦ 設計書の設計標準への遵守度合い 等
(3) レビューに対する対応の例
　① 進捗率を評価し、スケジュールを再設定する。
　② 問題点に対する解決策を策定し、修正案を関係者と協議する。
　③ 要求の修正、積残し案件の記録と実施時期・方法等の解決案を策定する。
　④ レビュー結果を記録し、関係者に周知徹底する。
　⑤ レビューの終了点をあらかじめ定め、進捗を評価して合意する、等

3．プログラム設計

(1) プログラム設計書は、開発の責任者が承認すること。

1 主　旨

プログラム設計書の品質を確保し、システム設計との整合性を図り、確実なプログラミング作業を可能にするため、プログラム設計書は、開発の責任者が承認する必要がある。

2 着 眼 点

(1) プログラム設計書を承認する開発の責任者を明確にしていること。

(2) プログラム設計書を開発の責任者が承認し、関係者に周知徹底していること。

(3) プログラム設計書は、開発手順及びプログラム設計マニュアルに基づいて作成していること。

(4) プログラム設計書は、必要な内容をすべて網羅していること。

3 関連事項

(1) プログラム設計書の内容の例

① プログラム概要

② プログラム構造

③ プログラム詳細機能説明

④ 入出力詳細記述

⑤ エラーコード、出力メッセージ一覧表

⑥ テーブル一覧表　等

(2) その他

次工程のプログラミングを外部委託する場合、プログラム設計書は原始資料として必須であり、かつ仕様変更管理上も重要である。そのためにも、開発の責任者がプログラム設計書の内容を承認する必要がある。

3．プログラム設計

(2) システム設計書に基づいて、プログラムを設計すること。

1 主　旨

システム設計で定義された機能及びシステムの構造を過不足なく正確にプログラムに反映するため、システム設計書に基づいて、プログラムを設計する必要がある。

2 着 眼 点

(1) 開発手順及びプログラム設計マニュアルに基づいて、プログラム設計書を作成していること。

(2) プログラム設計した機能は、システム設計機能に対し追跡可能であること。

(3) プログラム設計で定義された機能は、システム設計で定義された機能に対して必要十分であること。

(4) プログラム設計は、システム設計で定義されたシステムの構造を反映していること。

3 関連事項

(1) プログラム設計マニュアルの内容の例

① プログラム分割方法

② モジュール評価基準

③ プログラムパターン別標準型

④ 入出力詳細記述標準型

⑤ 共通処理機能

ａ．テーブル処理

ｂ．エラー処理

ｃ．日付処理

ｄ．データベースアクセス処理

ｅ．レポート処理

ｆ．グラフ表示処理　等

⑥ プログラム設計書作成上の留意点

⑦ プログラム設計書標準フォーム

⑧ プログラム設計書サンプル

⑨ プログラム設計マニュアル更新ルール　等

(2) プログラム設計作業の例

① システム設計書に基づいて、詳細なモジュールに分割する。

② 分割したモジュールをシステム設計書で定義された機能の充足の観点等から評価する。

③ 分割したモジュールの機能とインタフェースを決定する。

④ モジュールの共通化を図る。

(3) プログラム設計した機能のシステム設計機能に対する追跡可能性の確保

プログラム設計で詳細化した機能は、システム設計のどの機能に対応するかを明確にする。具体的には、構造図等で表現し関連を明確にする。

3．プログラム設計
(3) テスト要求事項を定義し、文書化すること。

1 主　旨

プログラム設計及びプログラミングの結果の妥当性を確認するために、テスト要求事項を定義し文書化する必要がある。

2 着 眼 点

(1) プログラム設計のためのテスト基本方針を作成していること。
(2) プログラム設計に関するテスト要求事項をすべて洗い出していること。
(3) 洗い出したテスト要求事項を文書化していること。

3 関連事項

(1) プログラム設計作業のテスト要求事項の例
　① テストの基本方針の設定
　　・トップダウンテスト／ボトムアップテスト／ビッグバンテスト
　　・ホワイトボックステスト／ブラックボックステスト
　② トップダウンテストの場合、下位モジュール（スタブ）の作成指針の設定
　③ ボトムアップテストの場合、上位モジュール（ドライバ）の作成指針の設定
　④ モジュールの機能を確認するテストケースの洗い出し
　⑤ モジュール間のインタフェースを確認するテストケースの洗い出し
(2) モジュールの分割の評価の例
　モジュールは強度（モジュール内の各機能の関連性）が高く、結合度（他のモジュールへの依存度）が低い方が良いモジュール構造となる。
　① モジュールの強度の評価
　　機能的強度が最も強度が高く、暗号的強度が最も低い。
　　・機能的強度
　　・情報的強度
　　・通信的強度
　　・手順的強度
　　・時間的強度
　　・論理的強度
　　・暗号的強度
　② モジュールの結合度

無結合が最も結合度が低く、内部結合が最も高い。

・無結合
・データ結合
・スタンプ結合
・制御結合
・共通結合
・外部結合
・内部結合

3．プログラム設計
(4) プログラム設計書及びテスト要求事項をレビューすること。

1 主　旨

プログラム設計の品質を高めるために、プログラム設計書及びテスト要求事項をレビューする必要がある。

2 着 眼 点

(1) プログラム設計の品質目標を明確にしていること。
(2) プログラム設計書及びテスト要求事項のレビューの方針を明確にしていること。
(3) プログラム設計書及びテスト要求事項をレビューする担当者を明確にしていること。
(4) プログラム設計書及びテスト要求事項のレビューでは、システム設計との整合性を確認していること。

3 関連事項

(1) プログラム設計の品質の例

ISO／IEC 9126（JIS X 0129）ソフトウェアの品質特性

① 機能性：合目的性、正確性、相互運用性、標準適合性、セキュリティ
② 信頼性：成熟性、障害許容性、回復性
③ 使用性：理解性、習得性、運用性
④ 効率性：時間効率性、資源効率性
⑤ 保守性：解析性、変更性、安定性、試験性
⑥ 移植性：環境適応性、設置性、規格適合性、置換性

(2) レビューの方針の例

① プログラム設計書及びテスト要求事項のレビューの基本方針
　ウォークスルー／インスペクション
② レビューの体制
③ レビュー結果の反映手続
④ レビューのチェックリスト

(3) プログラム設計書をレビューする担当者の例

プログラム設計書の数や難易度によってレビュー担当者を区分するのが妥当であるが、いずれの場合も当該プログラム設計書の作成者以外の者で、かつレビュー能力のある者が実行すべきである。

① プロジェクトリーダ（プログラム設計書の数が少ない場合）

② サブリーダ（開発単位がサブグループに分かれている場合で、開発単位ごとのプログラム設計書の数が少ない場合）

③ 当該プログラム設計書の作成者以外のプログラム設計書作成者（開発単位がサブグループに分かれている場合で、開発単位ごとのプログラム仕様書の数が多い場合） 等

(4) プログラム設計書のレビュー上の留意点

① 要求仕様との整合性を確認するために、レビューチームにユーザを参加させる。

② 進捗の遅れを取り戻すためにレビュー回数を減らすことのないようにする。

3．プログラム設計

(5) プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。

1 主　旨

システム設計及びプログラム設計の整合性を確保するため、プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決する必要がある。

2 着 眼 点

(1) システム設計の矛盾の報告手続を明確にしていること。
(2) 検討結果を関係者が合意していること。
(3) システム設計書の変更は、システム設計担当者自身が行っていること。
(4) システム設計との矛盾の原因を明確にし、対応策を講じていること。

3 関連事項

(1) システム設計の矛盾点
　① 技術的矛盾によって、システム設計を変更する場合
　　a．OS とアプリケーションプログラムとの整合性
　　b．周辺機器の構成とプログラム仕様の整合性
　　c．ネットワーク構成と OS との整合性
　　d．OS を含めた、使用するソフトウェアのバージョン
　② 論理的矛盾によって、システム設計を変更する場合
　　a．メインプログラム、サブプログラムとのリンケージによる調整矛盾
　　b．クライアントとサーバ間のリンケージによる調整矛盾
　　c．分散配置されたデータベースの中のデータ項目間の不整合
　　d．サブシステム間のリンケージによる調整矛盾
　③ 要求定義との不整合
　　a．要求定義とシステム設計の不一致
　　b．要求定義内の一貫性欠如
　　c．要求定義の不完全、不正確
(2) システム設計の矛盾の報告手続の例
　① 発見したシステム設計の矛盾の報告方法と報告書式
　② 再検討のための体制
　③ 再検討手順と承認方法　等

4．プログラミング

(1) プログラム設計書に基づいてプログラミングすること。

1 主　旨

プログラム設計書で定義された機能を過不足なく正確にプログラムに反映するため、プログラム設計書に基づいてプログラミングする必要がある。

2 着 眼 点

(1) 開発手順及びプログラミングマニュアルに基づいてプログラミングしていること。

(2) プログラミングの検証の手順を定めていること。

(3) プログラム仕様書に基づいたプログラミングであることを検証していること。

3 関連事項

(1) プログラミングの範囲

プログラミングとは、手続型言語によるプログラミングのことであるが、ソフトウェア部品の組合せによるプログラミング、テンプレートをベースとしたプログラムのカスタマイズ、パッケージソフトウェアのパラメータ設定等も含む。

一般にプログラム設計書に基づくコーディングと、コーディングの正しさを確認する単体テスト（プログラムデバッグ）の作業がある。

(2) 検証の手順

① 検証対応の選択

② プログラム設計書とコーディングの突合

③ 検証結果のレビュー

(3) プログラミングマニュアルの内容の例

① プログラム設計書の読み方

② 準拠すべきプログラミング標準

ａ．プログラミング標準

ｂ．コーディング標準

ｃ．エラー処理標準

ｄ．単体テスト標準

③ 共通処理プログラムの使用方法

④ 単体テストの準備

ａ．テスト範囲の基準

ｂ．テストケースの設定

ｃ．テストデータの作成
ｄ．テストツールの使用等、テスト環境の整備
ｅ．テスト結果検証体制の確立

4．プログラミング
(2) プログラムコードはコーディング標準に適合していること。

1 主　旨

プログラムの品質を確保するため、プログラムコードはコーディング標準に適合している必要がある。

2 着 眼 点

(1) コーディング標準を作成していること。
(2) プログラマに対してコーディング標準の教育を行っていること。
(3) プログラマはコーディング標準の適合の重要性を認識していること。

3 関連事項

(1) コーディング標準の例
　① コーディング標準の目的
　　生産性の向上、保守性の向上、品質向上
　② 使用すべき命令語と文法、使用すべきではない命令語と文法
　③ コメント欄の記述方法
　④ ネーミングルール
　⑤ 処理パターンごとのテンプレート
　⑥ プログラム設計書の表記とコーディングの対応付け
　⑦ コーディング標準のバージョン管理
(2) プログラマへのコーディング標準の提示、又は教育
　① プログラマにコーディング標準を提示し、必要に応じて教育する。
　② プログラミングを業務委託する場合は、業務委託契約等に基準の遵守を盛り込む。

4. プログラミング

(3) プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。

1 主　旨

プログラミングされた機能が、プログラム設計書に過不足なく正確に稼動することを検証し、プログラムテストの妥当性を確認するため、プログラムコードの評価及びプログラムテストの結果を記録及び保管する必要がある。

2 着 眼 点

(1) テスト結果に基づいて、具体的なプログラムテスト計画を作成していること。
(2) 想定したテストケースを検証するテストデータを作成していること。
(3) テスト結果の検証の責任者を明確にしていること。
(4) プログラムコードの評価及びプログラムテスト結果を記録し、保管していること。

3 関連事項

(1) プログラムテスト計画の内容の例
　① テストの目的
　② テスト範囲
　③ 必要な環境の定義
　④ テストスケジュール
　⑤ テスト担当者
　⑥ テスト結果検証方法　等
(2) 想定されるテストケース
　プログラミング段階でのテストは、単体テストとも呼び、プログラミングのすべてのロジックパス(Java 言語では、すべての分岐やテーブルサーチの通常サーチ、オーバフローサーチを含む)を一度は通し、テストされていないケースを排除することが重要である。
(3) テスト結果の記録の内容の例
　① テストされるプログラムID
　② テスト担当者（多くの場合、プログラミング担当者)
　③ テスト検証者（多くの場合、プログラム設計書作成担当者)
　④ テスト実施日
　⑤ テストケースとテストデータ
　⑥ テスト結果
　⑦ テスト実行に関する問題点

⑧ テスト結果・検証履歴（承認日、検証者）

⑨ テスト結果からの対応

(4) 保管期間の考慮点

通常、システム全体の安定稼動までを目安とするが、重要あるいは構造が複雑なプログラムの場合は、これに限らない。

(5) 検証の責任

通常は、プログラム設計者が担当するが、重要あるいは構造が複雑なプログラムについては、これに加えてプログラム設計者以外が検証する場合もある。

4．プログラミング

(4) 重要プログラムは、プログラム作成者以外の者がテストすること。

1 主　旨

プログラミングにおける誤びゅう及び不正を防止するため、重要なプログラムは、作成者以外の者がテストする必要がある。

2 着 眼 点

(1) プログラムに重要度を設定していること。

(2) 重要なプログラムは、プログラム作成者以外の者がテストしていること。

3 関連事項

(1) プログラムの重要度設定の視点の例

① 個人情報にかかわるデータ（顧客情報、人事データ等）処理

② 機密データ（戦略商品のマーケット予測データ等）処理

③ 会計データ（入金、出金データ等）処理

④ データの処理形態（オンライン処理、バッチ処理）

⑤ データの処理内容（更新又は削除処理等）

(2) テスト担当者の適格性

① プログラム仕様に精通している。

② テストの方法等を熟知している。

③ 業務内容に熟知している。

5．システムテスト・ユーザ受入れテスト

(1) システムテスト計画は、開発及びテストの責任者が承認すること。

1 主　旨

システムテスト計画の妥当性を確保するため、システム計画書は開発及びテストの責任者が承認する必要がある。

2 着 眼 点

(1) 開発及びテストの責任者を明確にしていること。

(2) 開発及びテストの責任者が承認し、関係者に周知徹底していること。

(3) システムテスト計画書は、開発手順書に基づいて作成していること。

(4) システムテスト計画書は、必要な内容をすべて網羅していること。

3 関連事項

(1) システムテスト計画書の内容の例

① システムテストの目的と範囲

② システムテストの種類

a．結合テスト

単体テストが終了したプログラムに対してプログラム間のインタフェースの適切性を確認するテストである。この場合、基本的には個々のプログラムの機能についてはテストしない。

b．総合テスト

結合テストが終了したことを前提に、システム全体の品質・性能面、運用・操作面等の総合的な観点からシステムの完全性を確認するテストである。

③ システムテストの前提条件

例：

a．結合テストの場合、すべてのプログラムの単体テストが終了し、端末等のデータ入力環境、データベースの構築等のテスト環境の整備が完了していること。

b．総合テストの場合、すべてのプログラムの結合テストが終了し、利用者マニュアルが作成済みであること。

④ システムテストの全体スケジュール

⑤ システムテストの体制

⑥ システムテストの役割分担

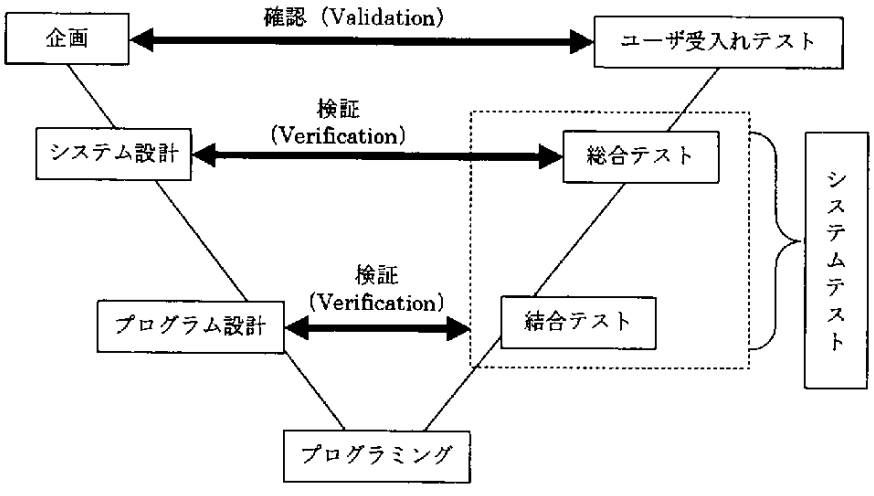
⑦ システムテスト（総合テストの段階）の種類

耐久テスト、性能テスト、効率テスト、障害テスト、リカバリテスト、外部アタックテスト等

⑧ システムテストの方法
⑨ システムテストの環境
⑩ システムテストのツール
⑪ システムテストのデータ
⑫ システムテストケース
⑬ システムテストの受入れ基準
⑭ システムテストの進捗管理方法
⑮ システムテストの問題管理方法
⑯ システムテストプログラムのバージョン管理方法

(2) システムライフサイクルにおけるシステムテストの位置付け

システムライフサイクルにおけるシステムテストの位置付けは以下のとおりである。



5．システムテスト・ユーザ受入れテスト

(2) ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。

1 主　旨

ユーザ受入れテスト計画の妥当性を確保するため、ユーザ受入れテスト計画書はユーザ及び開発の責任者が承認する必要がある。

2 着眼点

(1) ユーザ及び開発の責任者を明確にしていること。

(2) ユーザ及び開発の責任者が承認し、関係者に周知徹底していること。

(3) ユーザ受入れテスト計画書は、開発手順書に基づいて作成していること。

(4) ユーザ受入れテスト計画書は、必要な内容をすべて網羅していること。

3 関連事項

(1) ユーザ受入れテスト計画書の内容の例

① ユーザ受入れテストの目的と範囲

② ユーザ受入れテストの前提条件

総合テストの終了

ユーザ受入れテストを実施するユーザへの教育の終了　等

③ ユーザ受入れテストの全体スケジュール

④ ユーザ受入れテストの体制

ユーザ側体制、開発側体制

⑤ ユーザ受入れテストの役割分担

ユーザ側が主体となり、開発側は必要に応じてユーザ作業を支援

⑥ ユーザ受入れテストの種類

立上げ・終了テスト、通常運用テスト、障害時運用テスト、例外テスト、要件定義書によるテスト（機能、性能、品質等）、ユーザマニュアルによるテスト（操作性、運用性等）

⑦ ユーザ受入れテストの方法

⑧ ユーザ受入れテストの環境

⑨ ユーザ受入れテストのデータ

⑩ ユーザ受入れテストケース

⑪ ユーザ受入れテストの受入れ基準

⑫ ユーザ受入れテストの進捗管理方法

⑬ ユーザ受入れテストの問題管理方法

⑭ ユーザ受入れテストプログラムのバージョン管理方法

5．システムテスト・ユーザ受入れテスト

(3) システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。

1 主　旨

システム要求を満足していることを確認するため、システム要求事項を網羅してテストケースを設定し、システムテストを実施する必要がある。

2 着 眼 点

(1) システム要求事項を網羅してテストケースを設定していること。

(2) テストケースについて開発者がレビューを実施していること。

3 関連事項

(1) システム要求事項を網羅するテストケースの設定のポイント

① ユーザ要件及びシステム要求事項を確認すること。

② システム要求事項のすべてについてテスト目的やテスト要件を洗い出すこと。

③ 最少のテストケースで多くのシステム要求事項の確認ができるようなテストケースを設定すること。

④ 設定したテストケースごとにテストデータを用意するとともに、テスト結果を想定しておくこと。

(2) テストケースのレビューのポイント

① テストケースのレビューはインスペクションで行うこと。

② テストケースは例外ケース、特殊ケース、異常ケース等も考慮すること。

③ テストケースはシステム要求事項の網羅性の観点でレビューすること。

5．システムテスト・ユーザ受入れテスト

(4) テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。

1 主　旨

システムテストの目的を確実かつ効率的に達成するため、テスト計画に基づいてテストデータの作成及びシステムテストを実施する必要がある。

2 着眼点

(1) テスト計画に基づいて、具体的なシステムテストの計画を作成していること。
(2) 検証すべきテストケースを明確にし、テストデータを作成していること。
(3) 不具合が生じた場合のフォローの方法・体制を明確にしていること。
(4) システムテストの担当者にシステムテストの計画を周知徹底していること。

3 関連事項

(1) システムテストの計画の内容の例

① テストの目的
② テストの範囲
③ テストデータ作成
④ テストスケジュール
⑤ テスト担当者と役割
⑥ テスト結果検証方法
⑦ 不具合発生時のフォローの方法と体制

システムテストの計画は、システム設計時に作成したテスト計画をより具体化した内容である。

なお、予定したテスト回数で完了しない場合に備え、スケジュール、体制等に余裕をもたせること。

(2) 検証すべきテストケース

単体テストや結合テストと異なり、より実際の環境に近いテストケースを想定してシステム全体として正常かつ円滑に稼動すること。

クライアントサーバ型システムやWebアプリケーションシステムの場合、複数の拠点からのデータのアクセスやサーバ間のデータの整合性の確認等、複数の環境設定を考慮する必要がある。

(3) 不具合発生の対処

不具合は、技術的、論理的矛盾や要求定義との不整合から発生するが、いずれの場合も、プログラム（必要に応じてシステム設計書、プログラム設計書）の修正後に再テストが必要になる。再テストの内容やタイミングの決定が円滑かつ確実に実施できる配慮が必要である。

(4) システムテストへ参画する担当者

システム開発担当者だけでなく、ユーザ等も含めてそれぞれの役割分担を明確にして実行することが必要である。

5．システムテスト・ユーザ受入れテスト

(5) システムテストは、本番環境と隔離された環境で行うこと。

1 主　旨

システムテストを実施することで本番環境に悪影響を及ぼすことが考えられるため、システムテストは本番環境と隔離された環境で実施する必要がある。

2 着眼点

(1) システムテストを実施する環境は、本番環境とは物理的に隔離していること。

(2) システムテストを実施する環境は、本番環境とは論理的に隔離していること。

(3) システムテストを実施する環境は、テスト効果の観点から本番環境と相違ない環境としていること。

3 関連事項

(1) 物理的隔離の例

① システムテスト環境のコンピュータは本番環境と物理的に隔離されている。

a．システムテスト環境のコンピュータは本番環境とは別のコンピュータであること。

b．システムテストを行う際は、本番環境とネットワーク接続していないこと。

② システムテスト環境のネットワークは本番環境と物理的に隔離されている。

システムテスト環境のネットワークは本番環境のネットワークとは別のネットワークであること。

③ システムテスト環境のソフトウェアは本番環境と物理的に隔離されている。

ソフトウェアは、基本ソフトウェア、ミドルソフトウェア、アプリケーションソフトウェア等、いずれも本番用ソフトを使用しない。

④ テストデータは本番データと物理的に隔離されている。

a．テストデータは、本番データを使用しない。

b．テストデータに本番データを利用する場合は、必要に応じて編集し、秘匿が必要なデータ項目の内容を変更する。

(2) 論理的隔離の例

① システムテスト環境のコンピュータは本番環境と論理的に隔離されている。

システムテスト環境のコンピュータが本番環境と同一のコンピュータである場合、本番運用されていない時間帯にテストを実施すること。

② システムテスト環境のネットワークは本番環境と論理的に隔離されている。

システムテスト環境のネットワークが本番環境と同一のネットワークである場合、本番運

用されていない時間帯にテストを実施すること。

③ システムテスト環境のソフトウェアは本番環境と論理的に隔離されている。

ソフトウェアは、本番用ソフトウェアを使用するが、本番時はバックアップファイルからソフトウェアを再インストールすること。

④ テストデータは本番データと論理的に隔離されている。

テストデータは本番データを使用するが、本番時はバックアップファイルから再インストールすること。

5．システムテスト・ユーザ受入れテスト

(6) システムテストは、開発当事者以外の者が参画すること。

1 主　旨

開発した情報システムが全体として機能することを公正かつ客観的に検証するため、開発当事者以外の者が参画する必要がある。

2 着眼点

(1) システムテストの責任者を明確にしていること。

(2) システムテストの体制は開発当事者以外の者が参画していること。

(3) システムテストに参画する者は、システムの目的、システムテストの目的を理解していること。

3 関連事項

(1) システムテストの責任者の要件

① プログラムの作成とプログラムテストの実施に直接かかわっていないこと。

② システム全体に精通していること。

③ システムテストの遂行に当たって管理能力を有していること。

④ システムテストの経験を有していること。

(2) システムテスト体制の要件

① テスト責任者

② システム設計者

③ プログラマ

④ オペレータ、ライブラリアン等、運用部門関係者

⑤ 当該システムのユーザ

⑥ 必要に応じて企画部門、品質管理部門、教育部門の関係者

⑦ 必要に応じてパッケージベンダー、ハードウェアベンダー、ミドルソフトウェアベンダー等

(3) システムテスト体制の考慮点

① システム設計者は自己が関係したプログラムのテストには関与しないこと。

② ユーザは開発作業に参加していないユーザも含めること。

③ ERP パッケージ等を使用したシステムのテストを実施する場合は、ERP パッケージベンダーも含めること。

5. システムテスト・ユーザ受入れテスト

(7) システムテストは、適切なテスト手法及び標準を使用すること。

1 主　旨

効率的でかつ効果的にシステムテストを実施するため、適切なテスト手法及び標準を採用し、使用する必要がある。

2 着 眼 点

(1) システムテストは、システムのタイプ、システム開発の形態、アプリケーションシステムの種類等によって、適切なテスト手法を採用していること。

(2) システムテストは、システムテストの目的によって適切な標準を使用していること。

3 関連事項

(1) システムのタイプ

① クライアントサーバシステム／Web アプリケーションシステム

② オンラインシステム／バッチシステム

③ DB 更新型システム／情報系システム　等

(2) システム開発の形態

① トップダウン開発／ボトムアップ開発

② ウォータフォール型開発／スパイラルアップ型開発

③ 個別開発／パッケージ中心開発　等

(3) アプリケーションシステムの種類

① 事務処理系システム

② 生産管理系システム

③ 制御系システム

④ 経営情報系システム

⑤ 個人情報を取扱うシステム　等

(4) テスト手法の種類

結合テストで使用されるテスト手法は、次のとおりである。

① ホワイトボックステスト

主として単体テストで利用されるもので、プログラム内のすべてのコードと妥当なレベルの分岐のテストを行うテスト手法

② ブラックボックステスト

プログラムの内部構造には関係なくプログラムの仕様やインタフェースのテストを行うテ

スト手法

③ トップダウンテスト

最上位のモジュールからテストを行い、順次下位モジュールのテストを行うテスト手法。上位のテストを行う際には下位のモジュールが作成されていないため、仮のモジュール（スタブ）を作成する必要がある。

④ ボトムアップテスト

最下位のモジュールからテストを行い、順次上位モジュールのテストを行うテスト手法。下位のモジュールのテストを行う際には上位のモジュールが作成されていないため、仮の上位のモジュール（ドライバ）を作成する必要がある。

⑤ ビッグバンテスト

すべてのモジュールを一括してテストを行うテスト手法。小規模なシステムに適している。

(5) テストの目的

① 個々のプログラムの仕様のテスト

単体テスト

② プログラム又はモジュール間のインタフェースのテスト

結合テスト

③ システム要求事項のテスト

総合テスト

5. システムテスト・ユーザ受入れテスト

(8) ユーザ受入れテストは、本番同様の環境を設定すること。

1 主　旨

ユーザ要求事項の妥当性を確認するため、ユーザ受入れテストは本番同様の環境を設定する必要がある。

2 着眼点

(1) 確認すべきユーザ要求事項をすべて洗い出していること。

(2) 確認すべきユーザ要求事項をテストする環境を定義していること。

(3) 定義されたユーザ受入れテストの環境が本番環境と同様であることを確認していること。

(4) ユーザ受入れテストの実施環境は本番環境と隔離していること。

3 関連事項

(1) 確認すべきユーザ要求事項の洗い出しのポイント

① 要件定義書を基に確認すべきユーザ要求事項を洗い出す。

② 確認すべきユーザ要求事項ごとに、確認方法、確認データ及び想定確認結果を検討する。

(2) 確認すべきユーザ要求事項をテストする環境の定義のポイント

① 本番環境の範囲内で、確認すべきユーザ要求事項をテストする環境要件を定義する。

② 本番環境を新規に構築する場合は、本番環境の正常稼動確認後、論理的隔離を十分に考慮して、ユーザ受入れテストの実施環境を定義する。

③ 本番環境が現行システムの環境と同一であり、既に別アプリケーションシステムが本番稼動している場合は、別途ユーザ受入れテストの実施環境を定義する。

(3) 物理的隔離の例

① ユーザ受入れテスト環境のコンピュータが本番環境と物理的に隔離されている。

a．ユーザ受入れテスト環境のコンピュータは本番環境とは別のコンピュータであること。

b．ユーザ受入れテストを行う際は、本番環境とネットワーク接続していないこと。

② ユーザ受入れテスト環境のネットワークが本番環境と物理的に隔離されている。

ユーザ受入れテスト環境のネットワークは本番環境のネットワークとは別のネットワークであること。

③ ユーザ受入れテスト環境のソフトウェアが本番環境と物理的に隔離されている。

ソフトウェアは、基本ソフトウェア、ミドルソフトウェア、アプリケーションソフトウェア等いずれも本番用ソフトを使用していない。

④ テストデータが本番データと物理的に隔離されている。

a．テストデータは、本番データを使用していないこと。

b．テストデータに本番データを利用する場合は、必要に応じて編集し、秘匿が必要なデータ項目の内容を変更すること。

(4) 論理的隔離の例

① ユーザ受入れテスト環境のコンピュータが本番環境と論理的に隔離されている。

ユーザ受入れテスト環境のコンピュータが本番環境と同一のコンピュータである場合、本番運用されていない時間帯にテストを実施すること。

② ユーザ受入れテスト環境のネットワークが本番環境と論理的に隔離されている。

ユーザ受入れテスト環境のネットワークが本番環境と同一のネットワークである場合、本番運用されていない時間帯にテストを実施すること。

③ ユーザ受入れテスト環境のソフトウェアが本番環境と論理的に隔離されている。

ソフトウェアは、本番用ソフトウェアを使用するが、本番時はバックアップファイルから再インストールすること。

④ テストデータが本番データと論理的に隔離されている。

テストデータは本番データを使用するが、本番時はバックアップファイルから再インストールすること。

5．システムテスト・ユーザ受入れテスト

(9) ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。

1 主　旨

ユーザ受入れテストは、ユーザの視点でユーザが自ら本番運用を想定して実施する最終確認のテストであるため、要件定義書やユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施する必要がある。

2 着 眼 点

(1) ユーザ受入れテストは実務に精通したユーザが参画していること。
(2) ユーザ受入れテストは要件定義書とユーザマニュアルの内容を確認していること。
(3) ユーザ受入れテストは本番運用を想定してテストケースを設定していること。
(4) テストケースについて実務に精通したユーザがレビューしていること。

3 関連事項

(1) 本番運用を想定したテストケース設定のポイント
　① 要件定義書とユーザマニュアルを基にユーザ要求事項を確認すること。
　② ユーザ要求事項のすべてについてテスト目的やテスト要件を洗い出すこと。
　③ 最少のテストケースで多くのユーザ要求事項の確認ができるようなテストケースを設定すること。
　④ 設定したテストケースごとにテストデータを用意するとともにテスト結果を想定しておくこと。
(2) テストケースのレビューのポイント
　① テストケースのレビューは実務に精通したユーザが参画すること。
　② テストケースは本番運用時の観点を考慮すること。
　③ テストケースはユーザ要求事項の網羅性の観点でレビューすること。

5．システムテスト・ユーザ受入れテスト

(10) ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。

1 主　旨

ユーザ受入れテストは、本番運用を想定して実施する最終確認のテストであり、本番開始後のトラブルを最少化させるため、業務に精通したユーザ及び運用の担当者もテストに参画して確認する必要がある。

2 着 眼 点

(1) ユーザ受入れテストの責任者を明確にしていること。

(2) ユーザ受入れテスト体制はユーザ及び運用の担当者が参画していること。

(3) ユーザ受入れテストに参画する要員は、システムの目的、ユーザ受入れテストの目的を理解していること。

3 関連事項

(1) ユーザ受入れテストの責任者の要件

① システムテストの実施に直接かかわっていないこと。

② 業務全体に精通していること。

③ ユーザ受入れテストの遂行に当たって管理能力を有していること。

④ ユーザ受入れテストの経験を有していること。

⑤ 利害関係者に対してリーダシップを発揮できること。

(2) ユーザ受入れテスト体制の要件

以下の体制を整備すること。

① ユーザ受入れテスト責任者

② システム利用者

③ システム管理者

④ センターオペレータ

⑤ データ入力者

⑥ 支援部隊として開発者、パッケージベンダー、ハードウェアベンダー、ミドルソフトウェアベンダー　等

5．システムテスト・ユーザ受入れテスト

(11) システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。

1 主　旨

システムテスト及びユーザ受入れテストの結果に対する理解を一致させるため、ユーザ、開発、運用及び保守の責任者が承認する必要がある。

2 着 眼 点

(1) システムテスト及びユーザ受入れテストの計画で定めた目的の達成を検証していること。

(2) システムテスト及びユーザ受入れテストの結果をユーザ、開発、運用及び保守の責任者が承認していること。

3 関連事項

(1) システムテスト及びユーザ受入れテストの目的の検証方法の例

① 想定したテスト結果と実際の結果の突合

② テスト完了基準に到達しているかの確認

③ 使いやすさ等、定量化が困難な事項については、満足度調査を別途実施する。

④ システム要求事項を実現しているかの確認　等

(2) システムテスト及びユーザ受入れテスト結果報告書の内容の例

① テストの目的

② テスト責任者

③ テスト体制と役割

④ テストの範囲

⑤ テスト実施スケジュール（計画と実績）

⑥ テストケースと想定テスト結果

⑦ テストデータ

⑧ テスト結果評価

⑨ バグ分析表

⑩ 課題一覧表

⑪ 運用及び保守に関する考慮点　等

5．システムテスト・ユーザ受入れテスト

(12) システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。

1 主　旨

運用業務におけるトラブルの原因究明の基礎データとするとともに、保守業務の作業に備えるため、システムテスト及びユーザ受入れテストの結果を記録及び保管する必要がある。

2 着 眼 点

(1) テストデータ及びテスト結果の保管の責任者を明確にしていること。

(2) テストデータ、テスト結果及びテスト環境を保管していること。

(3) テストデータ、テスト結果及びテスト環境の保管期間を設定していること。

3 関連事項

(1) 保管の責任者の例

① システムテストへ参画し、今後のシステム保守に携わる者

② 特定の保管場所の管理責任者　等

(2) 一般的な保管期間

可能であれば、保管期間はシステムのライフサイクル完了までが妥当である。

(3) 保管すべきテスト環境の例

① テスト用アプリケーションソフトウェア

② テスト用基本ソフトウェア、ミドルソフトウェア

③ テスト用ハードウェア及びネットワーク

④ テスト用データベース

⑤ テスト用入力データ

⑥ テスト用出力帳票

⑦ テストツール

⑧ テスト計画

5．システムテスト・ユーザ受入れテスト

(13) パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。

1 主　旨

パッケージソフトウェアを採用して情報システムを構築する場合、情報システムの品質はパッケージソフトウェアの品質に影響されるため、パッケージソフトウェアの開発元が品質テストを実施したことを確認する必要がある。

2 着眼点

(1) パッケージソフトウェアを調達する場合、品質テストの実施とその結果を確認していること。

(2) パッケージソフトウェアを調達する場合、品質テストの実施結果の開示を調達条件に入れていること。

3 関連事項

(1) パッケージソフトウェアの品質の例

ISO／IEC 9126（JIS X 0129）ソフトウェアの品質特性

① 機能性：合目的性、正確性、相互運用性、標準適合性、セキュリティ

② 信頼性：成熟性、障害許容性、回復性

③ 使用性：理解性、習得性、運用性

④ 効率性：時間効率性、資源効率性

⑤ 保守性：解析性、変更性、安定性、試験性

⑥ 移植性：環境適応性、設置性、規格適合性、置換性

(2) パッケージソフトウェアの品質テストの要件

① 機能性のテスト要件

・マニュアルどおりの機能を実現しているか。

・処理結果は正しいか。

・標準に適合しているか。

② 信頼性のテスト要件

・誤作動及び機能停止をせず一定時間連続使用できるか。

・障害発生時には、一定時間内に修復できるか。

③ 使用性のテスト要件

・使い勝手がよいか。

・操作は覚えやすいか。

④ 効率性のテスト要件

・レスポンスタイムは許容時間内を実現しているか。

・使用する資源は一定量以内であるか。

⑤ 保守性のテスト要件

・トラブルに対してのバグフィックスは許容時間内であるか。

⑥ 移植性のテスト要件

・別の OS への移植が容易か。（例えば、Windows から Linux へ）

6. 移行

(1) 移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。

1 主　旨

移行は、開発計画に基づき開発部門がシステムを利用するユーザ部門、運用する運用部門、保守作業を行う保守部門に引き渡す作業であり、システムの開発・テスト段階から運用段階に円滑にかつ効率的に移行するため、移行計画を策定し、各部門の責任者が承認する必要がある。

2 着 眼 点

(1) 移行までに、開発、導入・テストが終了し、それぞれの作業の記録を作成し、承認され、保管していること。
(2) 移行計画の策定にはユーザ、開発、運用、保守の各部門が参加していること。
(3) 移行に必要な書類（運用、保守の引継書を含む）を整理していること。
(4) 移行計画には、移行に必要なリソースを明確にしていること。
(5) 移行全体のプロセスを各ユーザ、開発、運用、保守の責任者が承認していること。

3 関連事項

(1) 移行計画の内容の例
　① 移行の方針
　② 移行対象（データ、ソフトウェア、ハードウェア、ネットワークも含む）
　③ 旧システムの構成、新システムの構成
　④ 移行方法、移行手順（並行運用を含む）
　⑤ 移行時期、移行スケジュール
　⑥ 移行体制
　⑦ 移行リスクと対応策（旧システムへの戻しも含む）
　⑧ 移行時の並行運用計画
　⑨ 資金と設備
　⑩ 移行の検証方法と移行終了確認
　⑪ 移行データの移行方法（分散システムを含む）
　⑫ 移行時のトラブル対策
　⑬ 移行前環境の保全（対象、範囲、期限等）
　⑭ 移行の作業報告の承認
(2) 移行方法の例
　① 並行移行……一定期間、現行システムと並行に稼動させる方法

② 段階的移行……部分的に現行システムと置き換えて稼動させる方法

③ 一括移行……一時期にシステム全体を現行システムと置き換えて稼動させる方法

(3) 関係者

当該システムの直接利用のユーザ部門だけではなく、関連するユーザ部門や取引先等の組織体以外にも必要な事項を伝えることは、移行時の不必要な混乱を避け、円滑な新システムの稼動を図るために重要である。

6. 移行

(2) 移行作業は文書に記録し、責任者が承認すること。

1 主　旨

運用段階における稼動を確実なものとするため、開発業務の作業成果を本番環境に移行した作業結果を文書として記録し、責任者が承認する必要がある。

2 着眼点

(1) 移行計画書、実施記録、報告書、懸案事項等、それぞれの項目に対する記録を作成し、責任者が承認し保管していること。

(2) 作成すべき記録の種類とタイミングは、移行概要作成時に検討し、移行計画書で明確にしていること。

(3) 各作業の記録を遅滞なく作成していること。

(4) 移行作業終了後もデータの移行が継続される場合は、作業を分けて定義し、終了報告書も個別に作成していること。

3 関連事項

(1) 移行作業の記録と承認

移行は、ユーザ、開発、運用、保守等の複数の部門が共通認識の下に実施しなければならない作業で、作業内容を文書化し、作業記録を残し、移行結果を報告書として取りまとめ、結果に対してそれぞれの責任者の承認を得て内容を確定する。特に、懸案事項がある場合にはその取扱いを明確にし、関係部門の責任者の承認を得ておく。

(2) 移行時に発生する記録類

① 移行計画書
② 項目別実施記録
③ 移行報告書
④ 懸案事項報告書
⑤ 移行の作業ログ　等

6．移行

(3) 移行完了の検証方法を移行計画で明確にすること。

1 主　旨

情報システムの本番稼動環境が整ったことを確認するため、移行完了の検証方法を移行計画書で明確にする必要がある。

2 着眼点

(1) 移行計画書は、検証対象を明確にしていること。
(2) 移行計画書は、移行完了の評価基準を明確にしていること。
(3) 移行計画書は、検証方法及び体制を明確にしていること。

3 関連事項

(1) 移行の完了の検証

移行全体の完了及び各作業フェーズの完了の検証方法は、その都度その場面で検討するのではなく、計画的に実施するためにあらかじめ計画書で明確にし、個々の作業の完了、もしくは全体作業の完了について、漏れや矛盾なく推進できるよう文書化しておく。

(2) 検証対象の例

① データベース
② ソフトウェア
③ ハードウェア
④ ネットワーク
⑤ 運用・保守担当者の訓練度合い　等

(3) 完了判断基準の例

① データベースの場合は、すべての移行対象データを新データベースに転記し、確認し、かつ更新担当部門の責任者の承認を得ること。
② ソフトウェアの場合は、すべての移行対象ソフトウェアを新システム上にインストールし、新システム上での移行テストが完了していること。
③ ハードウェアの場合は、すべての移行対象ハードウェアを設置予定場所に設置し、作動確認等の一連のテストが完了していること。
④ ネットワークの場合は、新システム上のネットワークを全体のネットワークに接続し、接続通信確認等のテストが完了していること。
⑤ 運用及び保守担当者が、システムの構成や取扱い、定期的処理、緊急時処理等を理解していることを確認していること。

(4) その他

① 検証対象と完了の判断基準は、関係者の同意を得る。

② 移行完了の検証体制には、開発の責任者だけではなくユーザ、運用及び保守の責任者の参画も考慮する。

移行完了の判断基準がすべて満たされた時点で、関係者で最終報告会を開催し、確認する。並行運用を行った場合は、両者の違いの理解や移行後の運用時のリスクの最小化等を検討する。ユーザ部門に対して移行完了の報告会を開催することが望ましい。

③ 移行の前後の状況を確認できる資料の作成と保管は、トラブル発生時の原因追及に有益である。

6．移行

(4) 移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。

1 主　旨

移行計画どおりに作業を実施するため、移行に必要な要員、予算、設備等を確保する必要がある。

2 着眼点

(1) 移行作業に必要な要員、予算、設備等の見積りが正確かつ実現可能であること。

(2) 要員、予算、設備等の投入時期を移行作業の実施時期に応じて設定していること。

3 関連事項

(1) 移行に必要な各資源の検証の視点

① 予算……見積方法・支払総額、支払期限

② 要員（ユーザを含む）……資質、能力、経験、人数

③ 設備……能力、導入設備環境の整備（並行運転を含む）

④ 外部委託の場合……「VI. 共通業務　5. 委託・受託」を参照

システム分析・要求定義で見積もった工数、予算等と差がある場合、その理由を明確にし、関係者の承認を得る必要がある。

(2) 資源の投入時期

① 要員は、外部委託先も含めて、計画どおりの時期に計画どおりの資源が確保できていること。

② 設備は、ハードウェア等の納入や工事の必要性があることから、これらの作業の遅延の可能性を考慮した適切なリードタイムを見込む必要がある。

6．移行

(5) 移行は手順書を作成し、実施すること。

1 主　旨

移行計画どおりに移行作業を実施し、漏れ、重複、評価・確認不足等を防止するため、また移行作業を行う要員の教育を兼ね、移行の手順書を作成し事前確認を行う必要がある。

2 着 眼 点

(1) 移行計画書に移行の作業定義をしていること。
(2) 移行作業の内容を明確にしていること。
(3) 移行に必要な要員とそれに対する作業割当てを行っていること。
(4) 要員には事前に手順書を配布し、内容を確認していること。

3 関連事項

(1) 移行手順書の内容例
　① 移行の目的
　② 適用範囲
　③ 役割と責任
　④ 移行手順
　⑤ 問題点の管理及び解決手順
　⑥ 変更管理手順
　⑦ 移行作業の評価手順

6．移行

(6) 移行時のリスク対策を検討すること。

1 主　旨

移行時における有害事象の影響を特定し、その影響を最小限に抑えるため、移行時にもリスク対策を検討する必要がある。

2 着眼点

(1) 設計段階、導入・テスト段階で、本番移行時のリスクを想定していること。
(2) リスクの想定にはユーザ、開発、運用、保守の各部門が参加していること。
(3) リスクに対する重要度に基づく対応策が検討し、対応の優先順位付けをしていること。
(4) リスク評価には、最悪の事態も評価の対象にしていること。
(5) リスク評価・対応策の検討結果を関係者に周知徹底していること。

3 関連事項

(1) 移行時のリスク評価の内容例
　① 設計時の問題点（設計変更等）
　② 導入・テスト時の問題点（潜在的問題点等）
　③ 導入・テスト時に確認できなかった機能（本番接続後にしか確認できない項目）
　④ 初期稼動で発生しやすい障害　等
(2) リスク評価の責任者例
　① プロジェクトリーダ
　② アプリケーション責任者
　③ 運用責任者　等
(3) 移行リスクの例
　① 移行ツールの性能不足による手戻りの発生
　② 初期稼動時のリソース不足・性能不足の発生
　③ 検証不足によるバグの発現での悪影響の発生
　④ 担当者の訓練不足による手戻りの発生
　⑤ 新システム移行による情報システム全体での新たなボトルネックの発生
　⑥ 移行連絡の不徹底による手違いの発生
　⑦ 並行運用によるデータ入力負荷、管理負荷の増加
　⑧ 旧システムに戻せない　等

6. 移行

(7) 運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。

1 主　旨

移行作業終了後正式稼動前までに、システムの運用及び保守の関係者が円滑にそれぞれの作業に入れるよう設計書、テスト結果、移行結果、各種ツール類と操作マニュアル等が開発の責任者から引き継がれている必要がある。

2 着 眼 点

(1) 各文書類（設計書等）の作成を完了していること。
(2) 各種ツール類等の機能確認を行っていること。
(3) 開発の責任者から運用及び保守の関係者に資料やツール類の受渡し及び説明を行っていること。
(4) 運用及び保守の責任者は開発の責任者から受領した文書類等を元に、稼動前までに現行の文書類を適切に修正していること。
(5) 運用及び保守の責任者は、修正済み文書類を担当者に周知徹底していること。

3 関連事項

(1) 変更が必要となる手順書類の例
　① ユーザ運用マニュアル
　② 運用手順書
　③ 保守手順書
　④ ツール類操作マニュアル　等
(2) ツール類の例
　① システム構築ツール（ディレクトリ作成、ソフトウェアインストール、DB インストール、初期設定等）
　② 開発ツール（保守用）
　③ バックアップツール
　④ モニタリングツール
　⑤ クライアント設定ツール　等

6．移行

(8) 移行は関係者に周知徹底すること。

1 主　旨

当該システム及び内外の関連するシステムのそれぞれの運用に支障をきたさないため、関係者に対し、移行の概要を周知徹底する必要がある。

2 着 眼 点

(1) 移行作業と評価を完了していること。

(2) 稼動承認を行っていること。

(3) 稼動予定日を明確にしていること。

(4) 移行の概要を関係者に周知徹底していること。

3 関連事項

(1) 移行の通知内容

① 旧システムの運用を停止する理由

② 新システムの説明及び利用開始日

③ 旧システムの停止後の支援（旧システムのデータの読取り性確保等）

④ その他の支援策の説明　等

(2) 移行の周知徹底方法

① 連絡文書の配布

② 電子メールによる伝達

③ 公開しているシステム稼動情報等への掲載

④ ホームページへの掲載　等

Ⅳ.運 用 業 務

１．運用管理ルール
２．運用管理
３．入力管理
４．データ管理
５．出力管理
６．ソフトウェア管理
７．ハードウェア管理
８．ネットワーク管理
９．構成管理
１０．建物・関連設備管理

1．運用管理ルール

(1) 運用管理ルール及び運用手順は、運用の責任者が承認すること。

1 主　旨

運用管理ルール及び運用手順は、運用を円滑かつ効率的に行うために必要なものであり、運用の責任者があらかじめ内容を確認し、承認をする必要がある。

2 理論的根拠／実務的配慮

(1) 運用管理ルール及び運用手順を明文化し、組織体として承認していること。
(2) 運用管理ルールは、情報システムの運用形態を考慮していること。
(3) 運用手順は運用管理ルールに基づき作成していること。
(4) 運用管理の責任者を定めていること。
(5) 運用管理ルール及び運用手順を関係者に周知徹底していること。
(6) 定期的に運用管理ルール及び運用手順の効果を確認し、必要に応じて見直していること。

3 関連事項

(1) 運用管理ルールと運用手順

運用管理ルールは、情報システムの運用全般を安全で効率的に運用するために定める、運用関係者が遵守しなければならない基本原則をまとめたものである。

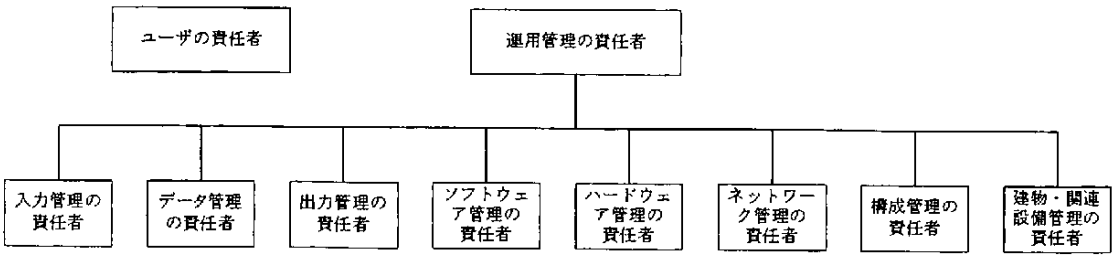
運用手順は運用管理ルールに基づき、インフラストラクチャや各運用システムが円滑かつ効率的に稼動できるよう具体的に定めた手順である。運用に携わる者は、事前に運用管理ルールと運用手順の教育を受けていなければならない。

運用を契約によって委託している場合は、「VI. 共通業務　5.委託・受託」を参照。

(2) 運用管理の責任者

運用管理の責任者は、運用管理ルールと運用手順を承認するだけではなく、その運用手順に従って実際にシステム運用、障害対応等を実施する要員を統括管理する責任者であり、対象となるインフラストラクチャや運用システムの内容について精通し、決定権を有するものを指す。運用管理の責任者が複数名から構成される場合には、それぞれの役割と権限を明確に定義する必要がある。

運用管理の責任者の例



(3) 周知徹底すべき関係者

① 情報システム部員
② 各運用担当者
③ 保守責任者、担当者
④ 開発プロジェクトの責任者
⑤ コールセンターの責任者、担当者
⑥ 外注委託先
⑦ 情報システムの利用者　等

(4) 運用コストの管理と課金等

情報システムの運用はコストが掛かるということが、ともすると利用者に忘れられがちになる場合があり、運用ルールで取決めを定めておく必要がある。

情報システムの運用コストは事前に年間運用計画の中で計画され、算定されなければならない。運用コストにはサーバ、クライアント、ソフトウェア、ネットワーク等の新規導入費、運用維持費、バージョンアップ費、情報システム部門の人件費等が含まれる。運用コストは情報システムを利用する利用部門に対して、その利用の度合い等に応じてコスト配賦という形でコスト請求を行う。

情報サービス等の形で外部の情報システムを利用する場合も、同様に情報センターが利用者に対して課金という形で利用コストの請求を行う。

昨今の情報システムはユーザ要求の多様化に伴い、新規導入、運用対象になっている情報システム数とバージョン、ネットワーク規模等が年々更新されることから、課金や配賦するコストは運用計画で毎年見直しを行い、運用管理ルールに従った配賦若しくは請求手続を行う。

1．運用管理ルール

(2) 運用管理ルールは、運用設計に基づいて作成すること。

1 主　旨

運用管理ルールは、各アプリケーション及び基本となるインフラストラクチャの設計時の運用設計に基本原則が定められているので、運用設計に基づいて作成する必要がある。大規模システムで全体最適化計画に基づく運用管理方式が定められていたり、サービスを利用する運用形態をとる場合は、それらの基本運用管理方式に基づいて作成する必要がある。

2 着 眼 点

(1) 運用設計書を作成していること。

(2) 運用設計に基づいて運用管理ルールを作成していること。

(3) 情報サービス等で基本運用管理方式が定められている場合は、それらも考慮して運用管理ルールを作成していること。

3 関連事項

(1) 運用管理ルールの項目の例

① 総則

ａ．目的

ｂ．適用範囲

ｃ．基本方針

ｄ．システム運用用務

ｅ．システム運用責任者

ｆ．システム運用責任者の任務・権限

ｇ．システム運用担当者

ｈ．システム運用担当者の任務

ｉ．機密保持

ｊ．業務効率の推進

ｋ．運用関係者の教育訓練

ｌ．運用の外部委託管理

ｍ．情報処理コストの課金

ｎ．ルールの改廃及び周知徹底

② 情報システムの管理

ａ．システム構成管理

b．システム維持・更新管理
c．システム利用者管理
d．システム操作管理
e．システム処理管理
f．システム問合せ管理
g．システムバックアップ管理
h．システム障害監視
i．エスカレーションフロー
j．システムモニタリング　等

③ 情報セキュリティ管理
a．アクセス管理
b．不正利用防止対策
c．物理的セキュリティ管理
d．情報資産のセキュリティ管理
e．バックアップ媒体管理
f．情報・電子媒体伝送のセキュリティ管理
g．ネットワーク障害対策
h．セキュリティ問題発生後の対応　等

(2) 運用管理ルールの対象の形態の例
運用管理ルールを定める上での留意点
① 集中処理
a．開発段階から運用段階への引継ぎ
b．処理依頼の具体的な手続
c．ジョブスケジュールの策定（業務の優先度の設定）
d．障害時の具体的な対策　等
② 分散処理
a．プログラムの配布手続
b．ソフトウェアのバージョン管理
c．バックアップの取得と回復手順
d．組織体全体としての管理　等

(3) 運用管理ルールの見直しの例
① 組織、制度等の変更への対応
② 技術進歩への対応
③ システム導入・改変への対応
④ 基準適合、法規制変更への対応　等

1．運用管理ルール

(3) 運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。

1 主　旨

運用業務を効率よく実施するため、運用設計及び運用管理ルールに基づき、さらに規模、期間、システム特性から運用手順を決定する必要がある。

2 着 眼 点

(1) 運用設計書及び運用管理ルールを策定していること。

(2) 運用の規模、期間、システム特性等を確認していること。

3 関連事項

(1) 運用手順の項目の例

① 運用手順の項目の例

a．運用の責任と体制……責任者の設置、目的、責任と権限、運用体制等

b．運用手続……運用時間、処理依頼、ユーザ ID 取得等

c．ジョブスケジュール……操作手順、引継ぎ、オペレータの交替、例外処理、オペレーション実施記録等

d．オペレーション……連絡体制、交替手段、リカバリ、記録等

e．入力管理……入力データの作成及び取扱い、入力者、承認、変更等

f．データ管理……データ管理者、利用状況、複写、媒体管理、保管、廃棄等

g．出力管理……出力情報の扱い、利用状況、引渡し方法、保管、廃棄等

h．パスワード及び識別コードの管理

i．ソフトウェア管理……アクセス管理、バックアップ、媒体管理、保管、廃棄等

j．ハードウェア管理……定期保守、バックアップ、利用状況、障害対策等

k．ネットワーク管理……利用状況、アクセスコントロール等

l．構成管理……管理対象、責任者、管理台帳、状況の把握、変更手続等

m．建物及び関連設備管理　等

② 運用手順は運用管理ルールに基づいて、運用業務に係る標準を明文化したものであり、文書化されたものだけでなく、端末へのメッセージの出力やファイル等の各種媒体を通して表現されるケースも考えられる。

(2) システム運用規模の例

① 大規模

a．全社基盤インフラストラクチャ（基本インフラ等）
b．全社統合アプリケーション（ERP：Enterprise Resource Planning）等
c．販売システム　等

② 中規模
a．生産システム（MRP：Material Requirements Planning）等
b．物流システム
c．会計システム
d．顧客管理システム
e．人事システム
f．構造解析システム　等

③ 小規模
a．部門システム
b．社外ホームページシステム
c．社内ホームページシステム
d．監視システム　等

(3) システム特性の例
① バッチシステム、オンラインシステム、クライアントサーバシステム、Web システム
② 資源依存システム（通信速度、CPU 能力、記録容量、クライアント数等）
③ 品質依存システム（銀行、原発、医療・医薬システム等）
④ セキュリティ依存システム（特許管理、国防システム等）
⑤ リソース集約システム（グリッドコンピューティング等）　等

(4) コスト配賦ルールあるいは情報サービス利用に基づく情報処理課金コスト業務の例
① 情報処理課金計画策定
② 課金単価管理
③ 課金の徴収・配賦管理
④ 課金実施管理
⑤ 課金結果の分析
⑥ 課金データのバックアップ管理
⑦ 課金管理のセキュリティ管理　等

1．運用管理ルール

(4) 運用設計及び運用管理ルールに基づいて、担当責任者を定めること。

1 主　旨

運用を円滑に行う上で担当責任者を明確にすることは、通常運用以外に例外処理、障害対応等で迅速な意思決定が発生する場面で特に重要であり、システム機能等の単位で担当責任者を決める必要がある。

2 着 眼 点

(1) 運用設計で運用の基本を設計していること。

(2) 運用管理ルールで運用担当別の役割と責任を決めていること。

(3) 運用の担当責任者を決めていること。

3 関連事項

(1) 担当責任者の例

① ジョブスケジュール担当責任者

② ハードウェア担当責任者（サーバ、基本 OS を含む）

③ ネットワーク担当責任者

④ クライアント担当責任者

⑤ 各アプリケーション別担当責任者　等

(2) 担当責任者の責務の例

① 運用システムの安全性、信頼性、効率性、有効性に貢献すること。

② 運用システムの定期的計画立案、報告を行うこと。

③ 担当する業務が円滑に運用できるよう、適切な処置を行うこと。

④ 運用システムに問題があるときは、運用責任者に報告し、指示を受けること。

⑤ 各担当者とのコミュニケーションを密にし、モチベーションを高めること。

2. 運用管理

(1) 年間運用計画を策定し、責任者が承認すること。

1 主　旨

情報システムの運用を円滑に行い、各情報システムのイベントをスケジュールどおりに消化推進するため、年度単位で運用計画を策定し、関係者の合意の上、責任者が承認し、関係者に周知徹底する必要がある。

2 着 眼 点

(1) 各システム予定作業項目を考慮した情報システムの年間運用計画を策定していること。
(2) 各イベントはスケジュール同士の衝突等がないよう、関係者によって調整を行っていること。
(3) 年間運用計画を運用の責任者が承認していること。
(4) 年間運用計画を関係者に周知徹底していること。

3 関連事項

(1) 年間運用計画

年間運用計画とは、一定期間（年間（月次、週次））での運用計画を指し、ジョブスケジュールとは異なる。

年間運用計画は、年間を通しての資源配分、処理のタイミング、大規模なシステムの更新や変更、責任体制等の大枠を定め、関係者に周知徹底し、円滑で効率的な運用を行うことを目的として策定される。月次、週次の運用は、年間運用計画を基に詳細を定め、実施しなければならない。

(2) 運用計画で考慮すべき項目の例

① 各システムの稼動期間
② ジョブスケジュールや障害時のシステム別処理優先順位の取決め
③ 締めの処理に対する取決め
④ 定期的大量トランザクション発生時期の確認
⑤ 新規アプリケーションの導入時期
⑥ 既存アプリケーションの更新時期
⑦ インフラストラクチャの追加・更新時期
⑧ 連休等の対応の取決め
⑨ 情報システムの目的達成の確認
⑩ 前年のモニタリング結果の反映
⑪ SLA（Service Level Agreement）の見直し　等

(3) 周知徹底すべき関係者

① 各運用担当者
② 保守責任者、担当者
③ 開発プロジェクトの責任者
④ コールセンターの責任者、担当者
⑤ 外注委託先
⑥ システム利用者　等

2. 運用管理

(2) 年間運用計画に基づいて、月次、日次等の運用計画を策定すること。

1 主　旨

情報システムの運用を円滑かつ効率的に進めるため、年間運用計画に基づいて月次、日次等の運用計画を策定する必要がある。

2 着 眼 点

(1) 年間運用計画を策定していること。
(2) 年間運用計画に基づき、月次運用計画を策定していること。
(3) 月次運用計画に基づき、日次運用計画を策定していること。
(4) 各運用計画を責任者が承認していること。
(5) 各運用計画を関係者に周知徹底していること。

3 関連事項

(1) ジョブスケジュール
ジョブスケジュールは、「Ⅳ. 運用業務　2.運用管理(4)」を参照。
(2) 月次・日次計画策定時の考慮点
① 要員スケジュール
② 委託先への確認（バックアップ、媒体保管等）
③ 月次処理・日次処理
④ データ授受のタイミング
⑤ 会議スケジュール
⑥ サプライ品の納入時期　等
(2) 周知徹底すべき関係者
① 各運用担当者
② 保守責任者及び担当者
③ 開発プロジェクトの責任者
④ コールセンターの責任者及び担当者
⑤ サプライヤ、外注委託先、取引先、共同事業相手先
⑥ システム利用者　等

2．運用管理

(3) 運用管理ルールを遵守すること。

1 主　旨

運用の標準化を図り、情報システムにかかわる誤びゅう及び不正を防止するため、管理体制、手続等、ルールとして定められた基準に従って運用管理を行う必要がある。

2 着 眼 点

(1) 運用管理ルールを明文化し、運用管理の責任者が承認していること。
(2) 運用の関係者が、運用管理ルールに関する教育訓練を受けていること。
(3) 運用の手続を運用管理ルールによって運営していること。
(4) 運用で取り扱われるデータは運用管理ルールに則り、企業として正当に承認されたデータのみを対象にしていること。
(5) 運用のモニタリングを行い、結果の分析と評価を行っていること。
(6) 運用管理及びルールに関する是正処置を行っていること。

3 関連事項

(1) 運用状況管理の内容例
　① 日常的状況管理
　　a．入退室記録の点検
　　b．運用日誌の点検
　　c．各種ログの点検
　　d．機器管理表の点検
　　e．口頭による確認　等
　② 日常的データ管理
　　a．データ登録件数の点検
　　b．サンプリングによるデータ原本との突合
　　c．業務報告等による確認
　　d．レポートによるデータ確認　等
　③ 会議体による定期的状況管理
　　a．日次打合せ
　　b．定期的運用担当者会議
　　c．ユーザ代表者との定期的運用報告会
　　d．緊急運用管理会議　等

2．運用管理

(4) ジョブスケジュールは、業務処理の優先度を考慮して設定すること。

1 主　旨

資源を有効利用し、ユーザニーズに対応した業務処理を行うため、ジョブスケジュールは、業務の優先度を考慮して設定する必要がある。

2 着 眼 点

(1) ジョブスケジュールは、処理依頼に基づき、作成していること。

(2) 優先度は、業務の重要性、緊急性、機密度等を考慮し、設定していること。

(3) ジョブスケジュールは、ユーザと調整を図り、運用の責任者が承認していること。

3 関連事項

(1) ジョブスケジュール

① ジョブの実行順序を決定するため、ジョブの優先度を設定する必要がある。

② 当該ジョブの処理形態、処理時間、出力時間、ネットワーク負荷等を考慮する。

③ 年間スケジュール、月次スケジュール、日次スケジュールと展開する。

④ ジョブスケジュールの例

次ページを参照。

(2) 処理依頼

ユーザがジョブスケジュールに反映するジョブを依頼するもので、運用の手続の中で規定される。

(3) 優先度

優先度は、当該ジョブにかかわる業務処理の組織体としての重要性、データの締めや障害時の再処理時間等を踏まえた緊急性、当該ジョブが取り扱うデータの機密度等を総合的に判断し、決定する必要がある。

(4) クライアントサーバシステムでのジョブスケジュール

クライアントサーバシステムでは、ユーザが自己の業務スケジュールに従ってオンラインでリアルタイムにデータが入力される。ERP パッケージ等の統合型システムを除き、多くのシステムが１業務につき１システムで構成されるため、システム内でのジョブスケジュールの調整は、頻繁には発生しない。

クライアントサーバシステムでジョブスケジュールの調整は、バッチ処理型のデータの場合、及びネットワークの負荷分散のため、サーバ間で処理の順番を調整する場合等で多く発生する。

ジョブスケジュールの例：

（平成　　年）

＿＿月ジョブスケジュール

作成日　　月　　日

作成者

（平成　　年）

ジョブスケジュール（日次）

月　　日（　　）

作成者

2．運用管理

(5) オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。

1 主　旨

資源を有効に活用し、操作上の誤り及び不正を防止するため、ジョブスケジュール及び指示書に基づいたオペレーションを実施する必要がある。

2 着 眼 点

(1) 指示書を運用の責任者が承認していること。

(2) オペレーションの実施結果を記録していること。

3 関連事項

(1) 指示書

① オペレータに対する作業指示書であり、実行ジョブ名、使用設備、資源等を具体的に記したものである。

a．業務名及び処理名（システム名）

b．ジョブ名称（ジョブID）

c．ジョブフロー

d．処理年月日

e．処理開始時刻及び終了時刻

f．入出力ファイル名称

g．出力帳票名

h．関係者名記入欄（作成者、オペレータ、承認者等）

② 指示書の例

次ページを参照。

(2) オペレーション実施結果

オペレーションの実施結果は、機器操作記録、オペレーション日誌、コンソールログ、ジャーナル等として記録する。

(3) その他

① エラー及び不正防止のため、センター運用の場合には、専任者によるオペレーションが望ましい。

② エンドユーザによる運用についても、計画的な処理の実行、処理結果の記録は必要である。

オペレーション指示書

（平成　年）

依頼日　　月　　日

システム名		ジョブ ID		タイミング	M・D 臨時
担当者		希望開始時刻		予定所要時間	
開始時刻		使　用 デバイス			
終了時刻					
使用時間					
メモ		出力帳票			
ジョブフロー					

2．運用管理

(6) 例外処理のオペレーションは、運用管理ルールに基づいて行うこと。

1 主　　旨

操作上の誤り及び不正を防止し、業務処理を円滑に行うため、例外処理は、運用管理ルールに基づいて的確に行う必要がある。

2 着 眼 点

(1) 例外処理を運用の責任者が承認していること。

(2) 例外処理が、他の業務に及ぼす影響を調査していること。

(3) 例外処理の頻度及び理由を分析し、ジョブスケジュールに反映していること。

(4) 例外処理の定期的見直しを行い、減らすようにしていること。

3 関連事項

(1) 例外処理

① 例外処理の例

ａ．ジョブスケジュールに未登録な処理

ｂ．プログラムエラーによる修正処理及び再処理

ｃ．オペレーションミスの修正処理

ｄ．ハードウェア障害や業務妨害による業務の再処理　等

② 例外処理はエラーの原因になる場合が多いので、原因を確かめ、減らす方向で検討すること。

③ 例外処理は指示書が不完全な場合が多いので、指示書が適切かどうかに留意すること。

(2) 他の業務に及ぼす影響

① 他の業務に及ぼす影響の例

ａ．レスポンスの悪化

ｂ．処理の遅延

ｃ．使用資源の割り当て　等

② 他の業務への影響を把握する必要性から、例外処理は、事前の承認が重要である。

(3) 他の業務に及ぼす影響

例外処理のうち、頻度が多く通常処理が可能なものをスケジュールに反映する。

2．運用管理

(7) オペレータの交替は、運用管理ルールに基づいて行うこと。

1 主　旨

業務処理を正確かつ円滑に遂行するため、オペレータの交替は、運用管理ルールに基づいて行う必要がある。

2 着眼点

(1) 引継ぎの手続を定めていること。

(2) オペレータの引継ぎの状況を運用の責任者が定期的に把握していること。

3 関連事項

(1) 引継ぎの手続

① 引継ぎの手続は、運用管理ルールのオペレーションに位置付けられる。
（「Ⅳ．運用業務　1.運用管理ルール(3)の 3.関連事項(1)」を参照）

② 引継ぎ時の確認事項

a．業務のみ処理事項

b．前任オペレータからの申し送り事項

c．引継ぎ当事者の押印　等

③ 引継ぎ手続の例
次ページを参照。

④ 外部委託によるオペレーション
オペレーションは、外部委託によって実施されるケースも多いが、外部委託については、「Ⅵ．共通業務　5.委託・受託」を参照。

⑤ その他
運用管理ルールで定めた以外の者がオペレーションしていないこと。

(2) オペレータ要員の確保

① 災害による交通手段のまひによる交替要員の欠勤、病気等による欠勤等に備えてオペレータ要員を確保しておく必要がある。

② 会議室、仮眠場所、休憩室等、オペレータの勤務環境を整えておく必要がある。

作業引継ぎ

月　　日　　時　記入

記入者		引継ぎ者	
システム／ジョブ名	特記事項／申し送り事項／対応		

2．運用管理

(8) ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。

1 主　旨

操作上の誤り及び不正を防止し、業務処理を円滑に遂行するため、ジョブスケジュールとオペレーション実施記録の差異分析を行う必要がある。

2 着 眼 点

(1) ジョブスケジュールとオペレーション実施記録の差異分析を定期的に行っていること。

(2) 差異分析は、例外処理を含めて実施していること。

(3) 差異分析の結果を運用の責任者に報告していること。

(4) 差異分析の結果をジョブスケジュールに反映していること。

3 関連事項

(1) オペレーション実施記録

機器操作記録、オペレーション日報、コンソールログ、ジャーナル等、オペレーション実施結果を記録したものである。

(2) 差異分析の内容

a．処理時刻、処理時間

b．例外処理の頻度及び理由

c．再処理の頻度及び理由

d．オペレータの特記事項　等

(3) ジョブスケジュールへの反映の例

① 処理時刻の変更

② 処理順の変更

③ 例外処理のスケジュール化　等

2．運用管理

(9) オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。

1 主　旨

操作上の誤り、不正、事故及び障害の原因を究明するため、オペレーション実施記録は、運用管理ルールに基づいて一定期間保管する必要がある。

2 着 眼 点

(1) オペレーション実施記録の保管期間を定めていること。

(2) オペレーション実施記録を定められた期間保管していること。

(3) オペレーション実施記録を廃棄した場合、廃棄の記録をとっていること。

3 関連事項

(1) オペレーション実施記録の保管

① オペレーションの実施状況を把握するため、保管対象とするオペレーション実施記録、保管期間等を定める必要がある。

② オペレーション実施記録の保管に関する事項は、通常、運用管理ルールのオペレーションの中で定められる（「Ⅳ. 運用業務　1. 運用管理ルール(3)の 3. 関連事項(1)」を参照)。

業務システムの運用が規制当局等の査察や監査の対象になる場合は、監査証跡として管理されている必要がある。

③ 保管期間は、オペレーション実施記録の内容及び媒体の種類によって異なる。

④ 保管の媒体が電子媒体の場合は、保管期間内での見読可能性を確保しておく必要がある。

(2) 事故及び障害の原因究明の例

① 当該ジョブのオペレーションが正しく実行されたか、オペレーション実施記録とジョブスケジュールによって確認する。

② 当該ジョブの処理時間の妥当性を前回の処理時間との比較によって判断する。

2．運用管理

(10) 事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。

1 主　旨

事故及び障害は、発生箇所や大きさに応じて影響度も大きくなるため、規模や影響度に応じて対応を柔軟に変えていくエスカレーションフローを明確にし、適切な処置と同時に影響の拡大を最小限に抑制する必要がある。

2 着眼点

(1) 影響度に応じたエスカレーションフロー及び体制等を定めていること。

(2) エスカレーションフローは運用責任者及び利用部門の責任者が承認していること。

(3) エスカレーションフローを関係者に周知徹底していること。

(4) エスカレーションフローは環境に応じて見直しを行っていること。

3 関連事項

(1) 障害対応組織の例

① 障害監視チーム

② 障害１次対応・２次対応チーム

③ コールセンター

④ 障害対策会議　等

(2) 障害対応手順

① エスカレーション手順書

② 障害対応手順書　等

(3) その他

① コンピュータウイルス等の場合は全社的でユーザへの影響が大きく、また、対応に協力が必要なので、ユーザも組織化しておく必要がある。

② コンピュータウイルスや踏み台攻撃の場合は他社への影響も考えられるので、対外窓口部門との連携を確立しておく必要がある。

③ 重要システムでは、情報システムの停止に備えた代替業務運用方法を検討しておく必要がある。

④ 事業継続性にかかわるような重大な障害は、「Ⅰ．情報戦略　5.事業継続計画」を参照。

2．運用管理

(11) 事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。

1 主　旨

事故及び障害の迅速な回復及び再発防止のため、事故及び障害の内容を記録し、運用の責任者に報告する必要がある。

2 着眼点

(1) 事故及び障害の発生時に報告書を作成し、運用の責任者が承認していること。
(2) 報告書は、事故及び障害の状況、原因等を記載していること。
(3) 事故及び障害発生時にあらかじめ定めた連絡体制が機能していること。

3 関連事項

(1) 事故及び障害の報告書
　① 報告書の記載内容の例
　　a．システム名
　　b．発生日時
　　c．発見部門及び発見者
　　d．対応時間及び対応者
　　e．事故及び障害の概要と対応
　　f．事故及び障害の原因
　　g．今後の対策
　　h．関係者の押印欄　等
　② 事故及び障害の報告書の例
　　次ページを参照。
(2) 事故及び障害の例
　① ハードウェアの障害
　② ソフトウェアの障害
　③ ネットワーク、電源、空調等の障害
　④ 火災、水害、停電等の事故
　⑤ 情報システム、データの破壊　等
(3) その他
　① 事故及び障害の項目に応じた回復許容時間をあらかじめ想定すること。
　② 自然災害については、「Ⅵ. 共通業務　7. 災害対策」を参照。

事故・障害報告書

<table>
<tr><td>システム名</td><td colspan="2"></td><td>システムID</td><td></td></tr>
<tr><td>発見日時</td><td colspan="2">月　日　時　分</td><td>発見部署／発見者</td><td></td></tr>
<tr><td>対応者</td><td colspan="2"></td><td>対応時間</td><td></td></tr>
<tr><td colspan="5">事故及び障害の状況</td></tr>
<tr><td colspan="5">対応内容</td></tr>
<tr><td colspan="5">原因</td></tr>
<tr><td colspan="5">再発防止策</td></tr>
<tr><td rowspan="4">事故・
障害分類</td><td rowspan="4">A．ハードウェア
B．ソフトウェア
C．ネットワーク
D．ヒューマンエラー
E．事故
F．コンピュータウイルス
G．その他</td><td rowspan="4">1．本体
2．端末
3．パソコン
4．周辺機器
5．その他</td><td>検　印</td><td></td><td></td></tr>
<tr><td>対応内容</td><td></td><td></td></tr>
<tr><td>再発防止</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

2．運用管理

(12) 事故及び障害の原因を究明し、再発防止の措置を講じること。

1 主　旨

事故及び障害の発生を防止するため、発生時に原因を明らかにし、再発を防止する処置を講ずる必要がある。

2 着 眼 点

(1) 事故及び障害の原因を分析していること。
(2) 事故及び障害の再発防止処置を講じていること。
(3) 再発防止処置を関係者に周知徹底していること。

3 関連事項

(1) 事故及び障害の原因
　① ソフトウェアの作成ミス
　② ハードウェアや関連設備の故障
　③ 回線接続断等のネットワークの障害
　④ オペレーション指示やオペレーションのミス
　⑤ コンピュータ犯罪、コンピュータウイルス　等
(2) 再発防止処置
　① 再発防止処置の例
　　a．物理的な防止措置
　　b．ソフトウェア的な対応措置
　　c．管理的な側面からの対応　等
　② 再発防止処置のための分析
　　a．発生した事故及び障害自体を徹底分析する。
　　b．事故及び障害の事例を収集し、原因を分析する。
(3) 関係者
　① 組織体の情報システムの企画、開発、運用及び保守の担当者
　② 情報システムの企画、開発、運用及び保守にかかわる外部組織体の関係者
　③ 情報システムの利用者　等
(4) その他
　事故及び障害は、その影響が組織体全体に及ぶケースもあるので、エンドユーザの故障及び障害対策は重要である。

2．運用管理

(13) 情報システムのユーザに対する支援体制を確立すること。

1 主　旨

EUC 等を中心にユーザの情報処理への利用機会が増加しており、業務への貢献と円滑な処理のため、情報システム部門が中心となってユーザ部門に対する支援体制を確立する必要がある。

2 着 眼 点

(1) ユーザ部門が利用するための基本ルールを定めていること。

(2) ユーザ部門の利用のための組織化を図っていること。

(3) 情報システム部門を中心としたユーザ利用のための支援体制を確立していること。

(4) 情報システム部門とユーザ部門で定期的に話し合う場を設けていること。

3 関連事項

(1) ユーザ部門の利用のための基本ルール項目の例

① システム利用申請基準
② 標準パソコン貸与基準
③ アプリケーション開発基準
④ 市販アプリケーション導入基準
⑤ メール利用基準
⑥ ファイルサーバ利用基準
⑦ リモートアクセス基準
⑧ 文書管理基準
⑨ ヘルプデスク利用基準
⑩ 標準外字利用基準
⑪ 情報セキュリティ基準　等

(2) ユーザ部門の組織化の例

① 情報戦略委員会
② システム委員会
③ システム定例運用会議　等

(3) ユーザ支援体制の例

① 社内 Web 上への情報システム運用情報の公開
② ユーザ教育制度（集合研修、e ラーニング、CD-ROM、外部研修等）
③ ヘルプデスク制度

④ ユーザ支援巡回サービス
⑤ 障害対応サービス
⑥ 推薦図書、見計らい図書　等

(4) ユーザと情報システム部門の話合いの場の例
① 会議形式（システム委員会、情報システム運用委員会等）
② 情報システムへの要望申請制度・依頼書制度
③ Web 上での電子掲示板、Q＆A システム　等

(5) ユーザ支援体制が不十分な場合に予想される影響
① データ入力処理の遅れ
② 情報セキュリティの破綻
③ 導入ソフトウェアのライセンス違反
④ 不明確パソコンの無断接続によるトラブル
⑤ システム利用上のコンプライアンス違反
⑥ 障害の放置　等

2．運用管理

(14) 情報セキュリティに関する教育及び訓練をユーザに対して実施すること。

1 主　旨

ユーザの情報セキュリティに関する意識を向上させるため、教育及び訓練を実施する必要がある。

2 着眼点

(1) 情報セキュリティ教育の内容を明確にしていること。

(2) 教育及び訓練を定期的に実施していること。

(3) 情報環境の変化に対応して、教育及び訓練の内容を見直していること。

3 関連事項

(1) 情報セキュリティ教育の例

① 情報セキュリティ教育の内容

a．情報セキュリティ……情報セキュリティの意義及び目的等

b．組織体におけるセキュリティの考え方……セキュリティ方針、セキュリティ規定等

c．情報資産保全……施錠管理、アクセス権管理、情報資産持出禁止、個人情報持出禁止等

d．ネットワーク接続ルールの遵守……定期的パスワード更新、パスワード長の管理、不許可パソコン接続禁止、外部媒体へのコピー制限、情報の暗号化等

e．障害時の具体的な対応策……バックアップの取得、回復方法等

f．セキュリティに関する関連法規、ガイドライン……知的財産権等

② 情報セキュリティ教育を実施するタイミング

a．新入社員研修

b．新任管理職研修

c．新任役員研修

d．その他技術研修　等

(2) その他

① バックアップの取得や障害時の回復については、具体的な方法とともに、その基本となる考え方をユーザに理解させる。また、障害回復は、実際にテストを実施し、具体的な状況を把握、確認する必要がある。

② 「Ⅵ．共通業務　4.人的資源管理　4.3 教育・訓練」を参照。

2．運用管理

(15) 情報システムの稼動に関するモニタリング体制を確立すること。

1 主　旨

情報システムの信頼性、安全性、効率性、有効性、リソース等を確認・管理するため、情報システムの稼動に関するモニタリング体制を確立する必要がある。

2 着 眼 点

(1) モニタリングを実施する社内合意を形成していること。
(2) アプリケーションのモニタリングを行う機能を組み込んでいること。
(3) インフラストラクチャのモニタリングを行う機能を組み込んでいること。
(4) モニタリング結果を評価する体制を組織化していること。
(5) 評価結果を計画的に改善に結び付けていること。

3 関連事項

(1) モニタリング項目の例（業務アプリケーションの場合）
　① リードタイム日数
　② 決裁までの期間
　③ 決算までの日数、連結の完了までの日数
　④ ｅラーニングへのアクセス回数・時間
　⑤ 販売情報へのアクセス回数
　⑥ 報告書の登録件数
　⑦ 製品歩留まり率推移
　⑧ 在庫引当率、欠品率
　⑨ アラーム件数
　⑩ スケジュール変更回数　等
(2) モニタリング項目の例（インフラストラクチャの場合）
　① CPU 使用率、ディスク使用率、DB 使用率
　② ログイン失敗件数
　③ 故障件数、故障率・故障時間
　④ システムアクセス回数・時間
　⑤ トランザクション量・パケット量
　⑥ ファイアウォールへのアタック件数
　⑦ ヘルプデスク問合わせ件数・回答率・積残し率

⑧ ウイルス駆除件数、感染件数
⑨ システム利用時間、利用ソフト種類
⑩ 消耗品の推移
⑪ TCO（Total Cost of Ownership）測定推移
⑫ 個人別 VDT（Visual Display Terminal）利用時間　等

(3) モニタリング体制の例
① 委員会（システム評価委員会、システム委員会等）
② 運用体制（運用責任者、運用担当者）
③ 検査体制（検査責任者、検査担当者）
④ 外部委託（タイガチーム等）　等

2．運用管理

(16) 情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。

1 主　旨

情報システムの費用対効果を高めるため、情報システムのモニタリング結果に基づき、稼動実績の把握と分析を行い、関係者で討議した後、性能管理及び資源の有効利用を図る必要がある。

2 着眼点

(1) 情報システムのモニタリングの仕組みと体制を有していること。
(2) 性能評価の指標を明確にしていること。
(3) モニタリング結果を把握し、分析し、評価していること。
(4) 評価結果を討議する体制を有し、問題点や対策を討議していること。
(5) 結果を関係者に報告していること。
(6) 情報システムの性能管理、リソース管理、資源の有効利用を図るための対策をとっていること。

3 関連事項

(1) 情報戦略の情報化投資との関係

情報システムのモニタリングとその結果を分析評価することは、情報化投資で計画した投資内容を検証し評価することも含まれる。戦略的投資の場合は、定量的に把握できる項目だけではなく、ライバル企業への差別化や競争優位を確保できる定性的な項目の評価も含まれる。

(2) モニタリング評価の目的
　① 戦略上の情報化投資の評価のため
　② 稼動中のシステムの改善のため
　③ インフラストラクチャを含めたシステム全体の機能改善のため
　④ リソースの適正配分のため　等

(3) 対策を組み込むタイミングの例
　① 中期計画によるローリング
　② 特別予算の申請
　③ 開発中のアプリケーションへの組込み
　④ 日常運用、定期保守での反映　等

(4) 検討する体制
　① 情報システム化委員会
　② 中期計画立案会議
　③ プロジェクト体制

④　運用会議
⑤　保守会議　等

3．入力管理

(1) 入力管理ルールを定め、遵守すること。

1 主　旨

入力データの作成、授受、検証、入力の実施、入力後の確認、保管等、情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を入力管理ルールとして明文化し、遵守する必要がある。

2 着眼点

(1) 入力管理ルールを明文化し、組織体が承認していること。

(2) 入力管理ルールには、不正、誤びゅう、漏えい等の防止、データの正確性を期すための牽制機能を明記していること。

(3) データの入力者を明確にし、入力管理の責任者が承認し、把握していること。

(4) 入力管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。

(5) 入力管理ルールを見直していること。

3 関連事項

(1) 入力管理ルールの設定項目の例

① 入力管理の責任者、担当者の設置、それぞれの職務の明記

② 入力データ作成の手続等（原始データの作成要領、エントリ指示、スケジュール依頼）

③ 授受（手続、担当者、授受の記録、授受データの形状とカウント項目、ラベル付け等）

④ 重要データ、機密データの取扱者の限定、確認のタイミング

⑤ 入力承認（入力データの承認者）

⑥ 承認時期（入力前、入力後）

⑦ データのチェック（データ内容の確認、データ原票と入力データの照合）

⑧ 入力の取消し、修正、追加

⑨ 入力記録の取得

⑩ 保管、一時保管、廃棄（データの保管状況の確認及び廃棄の方法と記録）

⑪ データの伝送、搬送（データ授受の日付、データ件数、内容、授受記録、確認）

⑫ 委託

⑬ 入力管理ルールの見直し（法制度改正、業務システムの追加・変更・廃止、事故による改善等）

(2) 入力管理の責任者、担当者の職務

① 入力データの管理者は、原則的に業務システムのユーザである。

② データ入力の承認を行う。

③ 情報システムにデータを入力する直接の担当者は、端末操作者、データエントリ担当、センターオペレータ等様々であり、それぞれの担当者を管理する責任者が存在する。

a．集中処理形態の例

入力管理の責任者……業務システムの管理者

担当者……データ作成者、業務担当者、業務システム運用者等

b．分散処理形態の例

入力管理の責任者……業務担当部門の管理責任者

(3) 関係者

入力管理の責任者、入力データの作成者等、業務処理プロセスにかかわる担当者等を指す。

(4) 入力管理ルールの見直し時期

システムの入力処理の変更、ハードウェアの変更、業務システムの追加、エラーの改善等のタイミングで行う。

(5) データ入力担当者の条件

データ入力担当者は機密保持の観点から、次の機能の者と同一にしないことが望ましい。

① システムの開発、運用、保守の担当者

② システムの管理者

3．入力管理

(2) データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。

1 主　旨

情報システムにデータを入力する際は、入力データに欠落、二重入力等の誤りが発生しないように入力管理ルールに記載されている手順に従い、正確に行う必要がある。

2 着 眼 点

(1) 入力管理の責任者が承認した担当者が入力を行っていること。
(2) 入力データの照合を行っていること。
(3) 入力データを責任者が承認していること。
(4) 入力記録及び端末操作記録を一定期間保管していること。
(5) 入力管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。
(6) 定期的に入力管理ルールの効果を確認し、必要に応じて見直していること。

3 関連事項

(1) 入力者の確認

入力者が社内関係者に限定される場合は、入力資格及び処理実施内容を確認する。
B to C 等、入力者が一般に広範囲にわたる場合にも、承認を確実に実施する。
論理チェック、物理的チェック等による検証を加える。

① 社内システムでの入力資格確認の例
　a．入力資格付与条件の設定と確認
　b．入力資格（ユーザ ID、パスワード、ID カード、生体認証等）の確認
　c．入力記録（ログ）の取得状況確認

② 電子商取引での入力資格確認の例
　a．入力資格付与条件の設定と確認
　b．入力資格（ユーザ ID、パスワード、ID カード、生体認証等）の確認
　c．電子認証局による証明
　d．入力記録（ログ）の取得状況確認

(2) データの入力操作に関するデータの照合方法の例

① 入力担当者以外の者の目視及び読上げ等による入力原票と処理結果の照合
② データの件数・金額等の合計の照合
③ 一連番号による処理の連続性・非重複等の検証

④ 打鍵データのベリファイ

⑤ 関連データとの件数、金額等の照合（乖離範囲、フォーマットによる確認等）

⑥ チェックディジットによる確認

⑦ エラーデータリストと再処理結果の検証

⑧ 取消し・修正・追加データの処理検証

(3) 入力記録及び端末操作記録の主な項目

入力内容の検証、エラー原因の追求等の目的で記録を一定期間（数か月、１年間等）保管しておく必要がある。

① 一般の情報システム

a．端末ID、業務名、処理名、処理時間、入力者名等

b．端末機別の入力件数及び合計金額

c．媒体番号、業務名、エントリ担当者名、エントリ件数、ベリファイ担当者名、ベリファイ件数等

② 電子商取引

a．利用者ID、取引内容、取引日時、取引内容の確認者等

b．利用者別の入力件数及び合計金額

3．入力管理

(3) 入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。

1 主　旨

入力データの作成、取扱い等を正確に行い、不正を防止するため、データの作成手順、取扱い等は、誤びゅう防止、不正防止及び機密保護等の対策を講ずる必要がある。

2 着 眼 点

(1) 入力データの作成手順は、誤びゅう及び不正を防止するとともに、機密保護や個人情報保護を考慮していること。

(2) 入力データの授受を記録し、データの暗号化、搬送時の保護策を講じていること。

(3) 入力データの機密度に応じて取扱者を限定していること。

(4) データ入力に係る事故・障害記録を取得し、適切な対策を講じていること。

3 関連事項

(1) 入力データの作成手順

① データを正確に作成して入力するため、作成する順序、項目数、桁数、文字等の特質に応じた入力帳票や画面を設計する。

② 業務におけるデータ発生場所、発生タイミングを明確にするとともに、作成担当者を限定する。

③ 作成データのチェック方法及び承認者を明確にする。

④ データの取消し・修正・追加の手順及び承認方法を取り決める。

(2) 入力データの作成における誤びゅう、不正防止の仕組みの例

① 画面設計

a．登録マスタからのコード選択

b．見やすさを考慮した画面レイアウト

c．チェックディジットによるチェック

d．アクセシビリティの考慮　等

② 帳票設計

a．マークシート、OCRによるデータエントリ不要帳票の利用

b．コード選択等、容易な記入への配慮

c．桁数、項目数、位置等の規定

(3) 入力データの授受

① 入力データ授受のルール化

a．データの件数票等の授受データの正当性を判断できる資料の添付
b．授受担当者及び責任者の任命
c．責任者による授受の確認
d．データの授受手段の決定（搬送又は伝送）
e．受け取った入力データの内容の確認

② 記録媒体（磁気テープ、DAT（Digital Audio Taperecorder）、CD-ROM等）の授受の記録項目と確認事項の例
a．データの名称と内容（特に個人情報の有無）の確認
b．記録媒体の形状の確認
c．記録媒体の二重化（正副の授受媒体）の有無
d．搬送方法（郵便、宅配便、専用貨物便等）の決定と信頼できる委託業者の選定
e．データの暗号化の有無と暗号化方式

③ 伝送によるデータ授受の記録項目と確認事項の例
伝送データの内容によってセキュリティについて留意する必要がある。
a．授受の時刻やタイミングの規定
b．授受担当者の指定
c．伝送路の指定（インターネット、一般加入回線、専用線等）
d．授受データの正当性チェック方式の確定
e．授受データの暗号化と暗号化方式の決定
f．確実に伝送されたことの確認

④ 個人向け電子商取引での留意事項（B to C）
a．なりすましによる不正取引の防止
b．情報漏えいの防止
c．授受データの改ざんの防止
d．授受データの否認の防止

(4) 機密度に応じた取扱者限定の例
① 顧客情報……顧客対応者、一部管理者に限定する。
② 人事情報……人事担当者に限定する。
③ 機密情報……機密情報を取り扱う担当者に限定する。
④ 個人情報……個人情報を取り扱う担当者に限定する。

(5) データの媒体変換時の留意事項
① 媒体変換作業時の原始データの厳格な管理
a．入力担当者を最小限にとどめ、データの分散を抑止する。
b．複写等を禁止する。
c．原始データが紙の場合は、原始帳票枚数を確認し、紛失や持出しがないことを確認する。
d．原始データは定められた場所に保管する。
② 媒体変換前後のデータ件数、合計等の一致確認
③ 媒体変換時のデータの暗号化実施

④ 変換後の媒体へのラベル付け（内容が類推できない表示方法）

(5) データ入力事故・障害記録の項目

① 端末ID、業務名、処理名、発生日時、入力者名等

② 事故・障害の内容、事故・障害の影響、応急・暫定措置、担当者・責任者等

③ 事故・障害の発生原因、再発防止措置、実施予定日時、担当者・責任者等

3．入力管理

(4) データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。

1 主　旨

データを正確に入力するための誤びゅう防止、不正防止、機密保護、及び個人情報保護の対策は有効に機能する必要がある。

2 着 眼 点

(1) 入力時のデータ照合が機能していること。

(2) プログラムは、誤びゅう及び不正を発見するチェック機能を有していること。

(3) 機密保護及び個人情報保護の対策を実施していること

(4) 誤びゅう防止、不正防止、機密保護及び個人情報保護の対策の効果を測定し、見直していること。

3 関連事項

(1) データ照合の実行（「Ⅳ．運用業務　3.入力管理(2)」を参照）

(2) データ入力時のプログラム処理によるチェック機能

① プログラムによるチェックの仕様

a．プログラムによる入力データのチェックは、システム開発の要求分析段階で仕様を決める。

b．パッケージプログラムの採用に当たっては、パッケージプログラムが有するデータのチェック機能又はカスタマイズによるデータチェック機能の追加が可能であることを考慮する。

② 入力ファイルの誤使用の防止

a．システム名称、ファイル名称、データ名称等の確認

b．使用するファイルの世代、バックアップデータの日付等を確認

③ プログラム処理によるチェック済の入力データも必ず責任者の承認を受けること。

(3) 機密保護と個人情報保護の対策

① 人的対策

a．データ取扱者の限定

b．非取扱者から隔離された環境での入力データの取扱い

c．取扱者への教育の実施及び教育効果の検証（確認テスト、ヒアリング等）

d．個人情報及び機密事項を取り扱うデータ取扱者からの誓約書提出　等

② システム的対策

a．資格確認機能（B to C の場合は電子認証局を含む）
b．メニュー画面へのアクセス権の設定
c．データの暗号化

(4) 入力手続、方法の見直し時期及び考慮点
① 見直し時期
a．定期的な見直し（内部監査実施後等）
b．重大なエラー、機密漏えい等の事件・事故発生時
② 見直す際の考慮点
a．発生したエラーの内容及び頻度
b．以前に発生したエラーに対する改善効果
c．発生したエラー件数及び類似エラーの有無
d．プログラムチェックの不備、入力データ照合方法の難易

(5) 入力管理の責任者の承認事項
① データ入力ルール
② データ入力担当者及び入力端末
③ データ入力処理及び処理結果
④ 入力対象データ及びファイル
⑤ 入力データ集計表
⑥ 入力データの処理予定及び処理実績
⑦ 取消し・修正・追加の実施
⑧ 入力の日時及び処理タイミング

(6) データ照合の留意点
① 照合項目、照合者についてルールどおりに行っているか。
② エラーは、責任者の承認を得て、ルールに従い、速やかに修正しているか。
③ 継続的な照合及びチェックが必要な項目、サンプリングで良い項目を明らかにしているか。
④ システムによるデータのチェックは機能しているか。
⑤ 類似したエラーの多発はないか。

3．入力管理

(5) 入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。

1 主　旨

入力データの紛失、盗難、漏えい等を防止するため、保管及び廃棄は入力管理ルールに基づいて行う必要がある。

2 着眼点

(1) 入力データの保管及び廃棄を業務の責任者が承認していること。

(2) 責任者の承認を得て、入力データを適切に保管及び廃棄していること。

(3) 重要な入力データの廃棄は、責任者が立ち会っていること。

(4) 廃棄の委託は、契約条件、廃棄方法等を調査し、決定していること。

3 関連事項

(1) 業務の責任者の承認

① 入力データ原票等の保管及び廃棄は、業務の責任者とあらかじめ保管期間、廃棄方法を取り決めておくこと。

② 外部媒体に記録された入力データ及び一時ファイルは、業務の責任者の承認のもと、入力管理の責任者が管理すること。

③ 外部媒体に記録された入力データ及び一時ファイルの破棄は、入力管理の責任者が実施すること。

(2) 適切な保管及び廃棄に当たっての考慮事項

① 保管対象を選定すること。

a．データの種類及び保管期間を確認し、保管の必要がないデータを廃棄又は業務の責任者に返却すること。

b．保管対象は一意の管理番号を割り振るなど、対象を明確にし、台帳等によって管理すること。

② 入力データの廃棄は、定めた時期に定めた方法で実施していること（外部媒体の破砕、入力データ原票の融解等）。

③ 保管場所と管理状況を確認すること。

a．データ等保管室等の保管設備の安全性（耐火、耐震、温湿度、施錠、監視設備等）

b．分散保管の実施

c．重要性の区分、施錠実施等の管理状況

d．棚卸しの実施状況

e．保管場所への立入り者の限定

④ 記録媒体の点検

a．記録媒体の定期的巻直し

b．記録媒体の定期的複写（記録媒体劣化防止）

(3) 確実な廃棄のための廃棄方法及び廃棄場所の選定に当たっての留意事項

① データの重要性及び形状（紙、外部媒体）による廃棄方法の明確化

② 確実な廃棄実施の確認

③ 搬送途中の紛失、盗難等の防止対策

④ 外部媒体の廃棄方法の確認（ダミーデータの上書き、消磁及び破砕してからの廃棄等）

(4) 廃棄記録の項目の例

① 廃棄対象媒体及び管理情報（管理番号、媒体番号等）

② 廃棄日

③ 場所

④ 廃棄方法

⑤ 搬送者、廃棄者及び確認者

⑥ 担当者及び立会者

⑦ 責任者の承認

⑧ 廃棄証明書（外部委託の場合）

(5) 保管ルールの項目例

① 保管対象データ……対象データを明確にし、保管期限も同時に定める（施錠保管の場合の対象データ等）。

② 保管責任者……定める。

③ 保管状態……保管台帳等によって、保管状態を確認すること（保管期限をチェックする仕組み、件数等管理の仕組み、貸出しのチェック等）

④ 保管場所……明確にする（データ保管庫、外部倉庫等）。

⑤ かぎ管理……かぎ管理者を定める（かぎ保管場所、スペアキーの取扱い等）。

⑥ 保管期間……業務の重要度、特性、法規制等から定める。

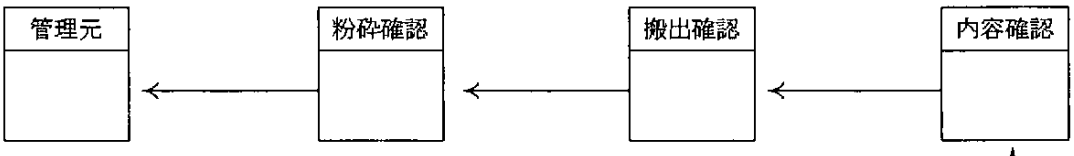
⑦ 確認、棚卸しのサイクル……期間を設定する（半期、１年等）。

(6) 廃棄管理表の例

ＭＴ廃棄管理表

廃棄箱番号					
B	O	X			

承認	予定日	. .
	実施日	. .



No.	廃棄対象ＭＴ情報			チェック	
	旧運用ナンバー	資産ナンバー	形式	消磁	梱包
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

備考	

コンピュータ出力の旧運用ナンバー、資産ナンバーＭＴについてチェックする。

4．データ管理

(1) データ管理ルールを定め、遵守すること。

1 主　旨

データの誤処理防止、機密保護及び個人情報保護のため、開発、運用及び保守業務に応じたデータの取扱い、管理の体制等をルールとして明文化し、遵守する必要がある。

2 着 眼 点

(1) データ管理ルールを明文化し、組織体として承認していること。
(2) データの管理者、検証者等の役割をあらかじめ定め、データ管理の責任者が承認していること。
(3) 管理の対象は、組織体で使用しているデータを網羅していること。
(4) 管理の体系は、組織体として一貫性をもっていること。
(5) データ管理のルールは、機密及び個人情報の取扱い方法を定めていること。
(6) データ管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。
(7) データ管理ルールを見直していること。

3 関連事項

(1) データ管理ルールの設定項目の例
　① データの種類と機密度
　② データ管理の責任者、担当者の設置、それぞれの職務の明記
　③ 授受手順（手続、担当者、授受の記録、授受データの形状とカウント項目、ラベル付け等）
　④ 重要データ、機密データの取扱者の限定（アクセスコントロール）、確認のタイミング
　⑤ データの世代管理基準
　⑥ バックアップ採取の基準と方法・保管（全バックアップ、差分バックアップ等）
　⑦ データの保管方法、保管場所及び保管期間
　⑧ データの廃棄方法、廃棄の記録
　⑨ データの複写方法
　⑩ データの利用状況の記録と確認（モニタリング）
　⑪ データ属性情報の管理方法
　⑫ データ格納媒体管理と容量及び余裕領域の管理方法
　⑬ データ管理ルールの見直し（法制度改正、業務システムの追加・変更・廃止、事故による改善等）

(2) データ管理ルールを実施する際の関連部門の役割

① 企画部門……データ管理の方針の決定、アクセス権限の設定、各関連部門との調整、データ管理ルールの遵守状況確認

② 開発部門……データバックアップ方法／世代管理の設計、アクセス管理方法の設計、テストデータの取扱い

③ 運用部門……保管場所の決定、保管ルールの実施、アクセス権限の付与（ID、パスワード等）

④ 保守部門……データを含む業務システム障害時のリカバリ

⑤ ユーザ部門……業務データの管理

⑥ その他……人事部門、経理部門等、社内サービス部門における社内データの管理

(3) データ管理の対象の例

① メインフレームシステムの例

a．データファイル、トランザクション用ファイル、システムログ

b．バッチ用データ、各種パラメータ、ワークファイル　等

② サーバシステムの例

データファイル、アプリケーションファイル、ログファイル

③ クライアントの例

データファイル、文書ファイル

④ その他テストにかかわるデータ

(4) サーバシステムにおけるデータ管理のポイント

① 各サーバシステムで管理されているデータの明確化

② すべてデータの管理者の明確化

③ 機密性の高いデータに対する不正利用及び機密保護の観点からの適切な管理

④ データに対するアクセスログの収集と確認

⑤ ウイルス対策ソフトウェアの導入とパターンファイルの最新化

4．データ管理

(2) データへのアクセスコントロール及びモニタリングは、有効に機能すること。

1 主　旨

データへの不正アクセスの防止、不正利用の防止、機密保護及び個人情報保護のため、アクセスコントロール及びモニタリングが有効に機能していることを確認する必要がある。

2 着眼点

(1) アクセスコントロールの機能を有効にしていること。
(2) アクセス状況のモニタリング機能の稼動状況を確認していること。
(3) 無資格者による情報システムの利用を定期的に調査していること。
(4) 特定のファイルへの偏った利用、異常な時刻での利用等を調査していること。
(5) 不正利用、不正アクセスの調査を行い、再発防止策を講じていること。
(6) 業務内容、組織、基本ソフトウェア等の変更に伴い、アクセスコントロール機能を見直していること。

3 関連事項

(1) アクセスコントロール機能の例
　① 資格確認機能（ユーザID、パスワード、IDカード、生体認証システム等）
　② 各資源へのアクセス権限機能（ファイル種別ごとのアクセス資格の付与等）
　③ コールバック機能
　④ ファイアウォール機能
　⑤ 電子認証局、電子署名機能
　⑥ ファイルレベルでの暗号化機能
(2) モニタリング機能の例
　① 不正アクセス警報機能
　② アクセスログ機能
　③ コンソールログ機能
　④ システムログ機能
　⑤ コミュニケーションログ機能
(3) アクセスコントロールの有効性監査の留意点
　① 使用しているアクセスコントロール機能は、対象データの保護上、有効であるか。
　② アクセスコントロールは、機能しているか。
　③ アクセスコントロールの記録は分析され、必要な措置が講じられているか。

④ システムの改変に伴い、アクセスコントロールの使用機能が見直されているか。

⑤ 最新の不正アクセス手法を調べ、対策を追加しているか。

(4) アクセスコントロールの運用に当たっての留意点

① セキュリティ管理者の設定（責任と権限）

② ログイン管理機能

③ 識別コードの割振りと管理

④ パスワード管理（パスワード規約と定期的変更の実施）

⑤ 定期的モニタ分析の方法

⑥ 機密度に応じたデータの管理

⑦ 不正行為等の発生時の対応

⑧ 人事異動、担当業務変更等のアクセス権限変更時の対応

(5) 不正アクセス防止対策の例

① 識別コード及びパスワードによる確認

a．ぜい弱なパスワード（誕生日、電話番号等）の禁止

b．パスワードの定期的変更

c．グループ共通のパスワードの禁止

d．パスワードの長さ及び文字必須使用の設定

e．個人識別カード、生体認証

② 暗号化技術の利用

a．ブラウザ、メールソフトウェアの暗号化機能の利用

b．ファイルの暗号化

c．VPN（Virtual Private Network）による回線経路の暗号化

③ 第三者による証明

電子認証局

4. データ管理

(3) データのインテグリティを維持すること。

1 主　旨

データが正確かつ完全であり、正常である状態を保つためにデータが正しく更新される必要がある。

2 着 眼 点

(1) データが正常であることを検証していること。

(2) データを登録・更新する場合は、正しく処理されたことを確認していること。

(3) データに不具合が発生した場合の回復手段を用意しておくこと。

3 関連事項

(1) データのインテグリティ（integrity）を確保するための対策の例

① 業務システム設計時に誤ったデータ処理への対策を考慮する。

② データの更新を伴うプログラムは、作動タイミング、更新内容を十分吟味する。

③ プログラムの誤作動に対する対策を講ずる。

④ プログラムの障害時のデータ矛盾が発生しないように、回復プログラム等の回避策を用意する。

⑤ プログラムでデータを生成した場合は、内容を検証する。

⑥ ホスト又はサーバとクライアントの間で、データのアップロード又はダウンロード処理が発生する場合は、そのタイミングに十分配慮する。

⑦ データの検証ツールを利用する。

⑧ 回復プログラムのテストを実施する。プログラム変更に伴う回復プログラムの変更の必要性を検討する。

⑨ 処理履歴を記録し、プログラムが正しい順序、タイミング及び時間に作動したことを確認する。

⑩ データの送受信に際しては、コントロールトータルをつけて漏れなく重複なく送受信されたことを確認する。

(2) データ障害時の復旧を考慮した対策

① ファイルの二重化（ミラーリング、RAID（Redundant Array of Independent Disks）等）

② バックアップの採取と更新ログの採取

③ 復旧手順の確立と訓練の実施

(3) インターネットにおけるインテグリティ確保の例

① 公開サーバはDMZ（De-Militarized Zone）構成とする。
② データの授受は必ず暗号化を行う。
③ なりすましを排除するために、電子署名、電子認証局等を利用する。

4．データ管理

(4) データの利用状況を記録し、定期的に分析すること。

1 主　旨

データの利用を予想し、不正利用を防止するため、データの利用状況を記録し、定期的に分析する必要がある。

2 着眼点

(1) データの利用状況を記録する機能を設けていること。

(2) データの利用状況を定期的に分析していること。

(3) 分析結果に基づき、データベース、ファイル、記録媒体等の有効利用を図り、将来のデータ量の変化への対応を考慮していること。

(4) 不正利用の調査を行い、対策を講じていること。

(5) 不正利用を検知した場合の通報先を明確にしていること。

3 関連事項

(1) データ、データファイルの利用状況の記録項目の例

① 利用者識別名

② アクセスファイル種別

③ アクセスの種類（参照、作成、追加、削除）

④ アクセス時間（開始時刻、終了時刻）

⑤ アクセス結果（通常処理、エラー処理）

⑥ ユニット利用率、ディスク使用率

⑦ データヒット率、エラー率

⑧ チャネル利用率

(2) 異常アクセスの検出の分析項目の例

① アクセス回数

② 使用時間

③ アクセス時刻

④ アクセス拒絶の記録

⑤ パスワード入力エラーの記録

(3) データファイルの利用状況の留意点

① 利用状況の把握には、独自の分析ツール、パッケージソフトウェア、システムで用意されているログ及び監査機能の使用も考慮する。

② 収集するログの範囲及びレベルは、アクセスコントロールの目的から、適切に設定する。

③ データファイルの利用状況を継続的に調査し、中・長期的な利用予測を行う。

(4) ファイルの稼動状況を把握し、将来の利用状況を予測するために、次の項目を分析する。

① データ領域の使用中領域と拡張用領域のバランス

② 新規データの伸び率

③ ピーク時間当たりのアクセス回数

④ 不要データを削除するガーベージ作業の間隔

⑤ 装置の未使用余裕領域の大きさ

(5) 不正アクセスがあった場合の対応

① 外部からの不正アクセスを検知した場合は、再度の攻撃を回避し、被害拡大の防止に努める（対策ができるまで、外部ネットワークとの接続を切断する等）。

② シャットダウン、リブート及びリストア等の回復処理はできるだけ避け、業務状況を考慮した上で、現状保持に努める（記録（ログ、ファイル等）の確保）。

③ 公的機関への連絡

・警察（各都道府県警察生活安全部）

・有限責任中間法人 JPCERT/CC

・独立行政法人情報処理推進機構　セキュリティセンター（IPA/ISEC）

4. データ管理

(5) データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。

1 主　旨

データの記録媒体の障害、誤操作、コンピュータウイルス等による影響を最小にするため、データのバックアップの範囲及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定する必要がある。

2 着 眼 点

(1) バックアップの範囲、タイミング、記録媒体、保管方法等は、業務内容、処理形態及びリカバリの方法に応じて定めていること。

(2) バックアップ方法は、情報システムの変更に伴い、見直していること。

3 関連事項

(1) バックアップの範囲の検討に当たっての考慮事項

① システムの形態（例：Web サーバシステム、クライアントサーバシステム、メインフレームシステム）

② 処理の形態（例：リアルタイム処理、バッチ処理）

③ リカバリ方法（例：即時回復、事後回復）

④ バックアップ媒体とその容量（例：CMT、DAT 等の媒体とその容量）

⑤ バックアップ時間（例：並行処理によるバックアップ時間の短縮化）

⑥ 業務の影響範囲（例：同一業務で使用するファイルの一括バックアップ）

(2) バックアップのタイミングを検討するに当たっての考慮事項

① リカバリの方法

② 回復許容時間

③ 業務の重要度

④ ファイルの特性（例：読込み専用、オンライン更新ファイル）

⑤ バックアップ採取が情報システムに与える影響度合い

⑥ リカバリ失敗時のデータロスの許容範囲、再処理の許容時間

(3) データの障害対策の検討のポイント

① データの特性を把握し、リカバリの要・不要を明確にする。

② 使用中の情報システムのリカバリ機能を理解し、適正な障害回復手段の方針を策定する。

③ 使用ソフトウェア等にリカバリ機能がない場合は、再処理に備え、データのバックアップ

を採取する。

④ 採取したバックアップファイルは、管理担当者を定め、定められた場所に保管する（耐火場所への保管、遠隔地への保管等）。

4．データ管理

(6) データの授受は、データ管理ルールに基づいて行うこと。

1 主　旨

データの誤使用、不正利用、改ざん等を防止するため、データの授受は、データ管理ルールに基づいて行う必要がある。

2 着 眼 点

(1) データの授受はデータ管理ルールで定める担当者が行っていること。

(2) データ管理ルールに基づいて、データの授受、保管、確認及び返却を行っていること。

(3) データの授受を記録し、データ管理の責任者が承認していること。

(4) データの授受記録を一定期間保管していること。

3 関連事項

(1) データの授受ルールで定める事項の例

① データ授受の責任者、担当者の設置、それぞれの職務の明記

② 授受手順（手続、授受双方の担当者、授受の記録、授受方法、授受データの形状とカウント項目、ラベル付け等）

③ 重要データ、機密データの取扱者の限定（アクセスコントロール）

④ 授受の確認方法（コンピュータウイルスチェックを含む）と責任の所在の明確化

⑤ データ授受ルールの見直し

(2) クライアントパソコンのデータ授受のポイント

① 授受データの暗号化

② メールでのデータ授受の際の送信先の確認

③ 授受データの媒体のコンピュータウイルスチェック

④ 知的財産権を侵害していないことの確認

⑤ 機密性及び重要性の観点を考慮した授受後のデータの適切な保管方法

(3) 小型大容量媒体（USB メモリ、メモリカード等）のデータ授受のポイント

① 暗号化、生体認証等の機能がある媒体の利用

② 媒体のコンピュータウイルスチェックの徹底

③ 室内からの持出厳禁等、管理ルールの策定及び徹底

④ 一時的記録データの完全消去

⑤ 紛失等、事故発生時の社内連絡先及び具体的対策の明確化

4．データ管理

(7) データの交換は、不正防止及び機密保護の対策を講じること。

1 主　旨

不正利用の防止、機密情報の漏えい及び個人情報保護のため、データの交換は、不正防止及び機密保護の対策を講ずる必要がある。

2 着 眼 点

(1) データの交換の形態に応じた不正防止、機密保護及び個人情報保護の対策を講じていること。

(2) データの交換をデータ管理の責任者が承認していること。

(3) データ管理ルールで定める機密度の高いデータの交換は、暗号化等の処置を講じていること。

(4) データの交換記録を定期的に分析していること。

3 関連事項

(1) データ交換における不正防止及び機密保護の対策の例

① データ交換の媒体には、交換対象のデータのみとし、余分なデータは含めない。

② ネットワークを介してデータ交換を行う場合は、交換元、交換先で交換手順を定め、交換データの内容を確認し、突合する。

③ データ交換を行うネットワークは専用線や VPN 等、外部からの侵入が困難なネットワークを利用する。

④ 出所不明の媒体は使用しない。

⑤ データの内容に応じた機密度を設定し、交換確認、確認後の保管、管理システムの運用を定める。

⑥ データ交換におけるデータの機密度を定め、利用可能者の限定を行う。

⑦ 複製のルールを定め、機密度の高いデータの複製を禁止する。

⑧ 不正防止及び機密保護の対策は、媒体の特性に応じた対策を策定する。

⑨ 機密性の高いデータの不正持出しを防止するため、入退管理の徹底と、入退時の携帯品の管理規定を定める。

⑩ データの交換は、責任を持つ当事者間で行う。

⑪ データの機密度に応じたデータの圧縮化、暗号化、分割及び分散した交換・管理を行う。

⑫ 機密性の高いデータの格納媒体へのラベル表示・非表示の規約を策定する。

(2) データ交換の形態の例

① 文書による交換（紙、書類に記述されたデータ）

② 電子媒体による交換（磁気テープ、CD-ROM 等に格納されたデータ）

③ ネットワークを介した交換（インターネット、EDI 等）

(3) データ交換時に確認し、記録する項目の例

① データの媒体種別、媒体番号

② 受渡し者名、受領者名

③ 保管期限、使用期限、返却日

④ 取扱区分（機密性のレベル）

⑤ 利用後の廃棄方法　等

(4) データの外部交換の例（B to B）

① 金融機関との取引決済データ

② 金融機関との給与振込みデータ

③ 部品メーカとの受発注データ

④ 製造会社との設計図データ

⑤ 情報会社から購入したデータベース

(5) データ交換の記録を分析するに当たっての留意事項

① 交換したデータの媒体種類、管理番号が明記されているか。

② 権限外の要員によるデータ交換が行われていないか。

③ データ交換は、データ交換の責任者の承認を得られているか。

④ 個人情報を交換する場合、交換先の機密性のレベルが満足できるか。

⑤ データ交換のタイミングは、処理タイミング、データ量、処理時間等から妥当か。

(6) データ交換での暗号化に当たっての留意事項

① 暗号化形式

② 暗号化の対象範囲

③ 暗号化／複合化の実施手段（ソフトウェア、ハードウェア）

④ 暗号のアルゴリズム

⑤ 暗号かぎの管理者

⑥ システムに与える負荷予測

4．データ管理

(8) データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。

1 主　旨

データの不正利用、漏えいの防止及び個人情報の侵害等を防止するため、データの保管、複写、不要データの廃棄は、不正防止及び機密保護の対策を講ずる必要がある。

2 着眼点

(1) 保管、複写、廃棄は、データの記録媒体に応じた不正防止、機密保護及び個人情報保護の対策を講じていること。

(2) 保管、複写、廃棄はデータ管理の責任者が承認していること。

(3) データは、所定の場所、期間及び方法で保管していること。

(4) データの重要度に応じて、複写を制限する対策を講じていること。

(5) 重要なデータは、複写履歴を記録していること。

(6) 重要なデータの廃棄は、データ管理の責任者が立ち会っていること。

3 関連事項

(1) データの保管及び複写における検討事項の例

① データの管理責任者の明確化

② 保管場所、保管方法のルール化

③ データの種類、重要度に応じた管理台帳の作成

④ 重要性、緊急性及び機密性のそれぞれの区分

⑤ 世代保管と分散保管

⑥ データの暗号化

⑦ データの保管、貸出及び複写の申請ルールと責任者による承認

⑧ データファイル等に対するアクセスコントロール

⑨ データのアクセスの記録と分析

⑩ 保管及び複写の記録管理（記録の保存期間等）

(2) データ保管場所の検討事項の例

① 媒体に適した保管場所

② 使用頻度と授受手順

③ 機密度と保管環境

④ 保管場所の施錠管理

⑤ 個々データの管理者（オーナー）と保管場所

(3) データの保管時における機密保護の対策例
  ① ラベル等におけるデータ内容の非表示
  ② 機密度に応じた保管時の管理体制
  ③ データの暗号化
(4) データファイルへのアクセスコントロールの例
  ① 資格確認（ユーザID、パスワード、生体認証等）
  ② 各資源へのアクセス権限制御
  ③ モニタリング（違反アクセス、システム使用状況等の記録・分析）
  ④ 相手確認（コールバック等）
  ⑤ 暗号化
(5) データの廃棄に当たっての検討事項の例
  ① 廃棄方法……消磁、破砕、裁断、焼却、融解
  ② 廃棄ルール……担当者、目的、方法、期日、場所、責任者の承認、廃棄記録等
  ③ 外部委託……委託先選定、廃棄状況の立入り確認、守秘義務契約
(6) パソコン、サーバのリースアップ、廃棄又は譲渡時の留意点
  ① 必要データのバックアップの取得
  ② ハードディスクの全データ消去
    a．全領域へのダミーデータの上書き
    b．全領域へのリフォーマット
  ③ データ消去を外部に委託する場合は、消去証明書を取得
  ④ (社)電子情報技術産業協会「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関するガイドライン」を参照。

4．データ管理

(9) データに対するコンピュータウイルス対策を講じること。

1 主　旨

データをコンピュータウイルスから保護するため、コンピュータウイルス対策を講ずる必要がある。

2 着眼点

(1) 情報システムの環境に適合したコンピュータウイルス対策を講じていること。

(2) コンピュータウイルス対策を周知徹底していること。

(3) 被害状況を報告し、コンピュータウイルス対策を実施する体制にしていること。

3 関連事項

(1) コンピュータウイルス

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を１つ以上有するもの

① 自己伝染機能……自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることによって、他のシステムに伝染する機能

② 潜伏機能……発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、条件が満たされるまで症状を出さない機能

③ 発病機能……プログラムやデータ等のファイルの破壊を行ったり、コンピュータに異常な作動をさせる等の機能

(2) コンピュータウイルスの種類

① プログラムファイル感染型（EXE ファイル、COM ファイル）

② システムプログラム感染型（SYS ファイル）

③ マクロ型（マクロ機能を持つアプリケーションのデータファイルに感染）

④ Java・ActiveX 型（ブラウザを介して感染）

⑤ ダイレクトアクション型（セキュリティホールを利用して感染）

⑥ ワーム（ネットワークを介して拡散し感染）

⑦ トロイの木馬（ファイルの破壊）

(3) コンピュータウイルス対策の主要項目

① 組織体としてのウイルス対策のルールを定めたコンピュータウイルス対策実施要綱（コンピュータウイルス検査方法、検査時期等）の策定

② 媒体、機器、プログラム、データ等の属性情報等の把握と管理

③ 媒体及び機器管理・運用手順の策定と遵守

④ ワクチンプログラムの利用

a．コンピュータ機器のコンピュータウイルス検査

b．外部交換ソフトウェア、データ等のコンピュータウイルス検査

⑤ 被害状況の把握と公的機関に対する報告

⑥ コンピュータウイルス対策支援部門の設立

⑦ 教育・啓蒙

(4) コンピュータウイルス対策の参考基準とコンピュータウイルス関連情報の収集

・「コンピュータウイルス対策基準」

・独立行政法人情報処理推進機構　セキュリティセンター　緊急対策情報

http://www.ipa.go.jp/security/index.html

・有限責任中間法人　JPCERT/CC

http://www.jpcert.or.jp/

4．データ管理

(10) データの知的財産権を管理すること。

1 主　旨

構築したデータの知的財産権の保護及び外部から導入したデータの知的財産権の侵害を防止するため、知的財産権を管理する必要がある。

2 着 眼 点

(1) 知的財産権の教育を実施し、著作物に対する認識をもっていること。

(2) 知的財産権の保護の対象とするデータを明確にしていること。

(3) 外部からのデータは、定められた手続で導入していること。

(4) 導入したデータの知的財産権を侵害していないことを定期的に調査していること。

3 関連事項

(1) データの知的財産権

データの知的財産権は、著作権法の「データベースの著作物」として保護されている。保護の対象となるデータベースは、「その情報の選択又は体系的な構成によって創作性を有するもの」と規定されている。データベースとは、「論文、数値、図形、その他の情報の集合体であって、それらの情報を電子計算機を用いて検索することができるように体系的に構成したもの」と定義されている。

(2) データの知的財産権に関連する傾向

① クライアントサーバシステムの進展、PC の普及で、エンドユーザがソフトウェア環境構築、データベースの複写等が容易に可能

② CD-ROM 等で提供される知的財産権を持つデータファイルの多種多様化

③ インターネット等でのファイル交換等、データ交換手法が多様化

④ 安価な大容量記録媒体の普及によるデータファイルの展開・蓄積が可能

⑤ LAN 等の構築によって、EUC 環境で容易にデータ交換が可能

5. 出力管理

(1) 出力管理ルールを定め、遵守すること。

1 主　旨

出力方法の誤びゅう、不正利用、漏えい等を防止し、機密保護及び個人情報保護のため、情報の出力手続、承認等のルールを定め、遵守する必要がある。

2 着眼点

(1) 出力管理ルールを明文化し、組織体として承認していること。

(2) 出力管理ルールは、誤びゅう、不正を防止し、機密保護や個人情報保護を考慮していること。

(3) 出力管理の責任者を定めていること。

(4) 出力管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。

(5) 定期的に出力管理ルールの効果を確認し、必要に応じて見直していること。

3 関連事項

(1) 出力管理ルールの策定項目の例

① 出力管理の責任者の設置、職務の明記
② 情報出力の承認
③ 管理対象
④ 情報の出力と表示（アクセス管理、アクセス権の付与、手続等）
⑤ 出力情報の複写、複製
⑥ 引渡し
⑦ 出力帳票の見直し
⑧ 後処理
⑨ 出力情報の伝送、搬送
⑩ 出力情報の保管、廃棄　等

(2) 不正防止、機密保護に当たっての考慮事項（リスク例）

① 情報の出力……漏えい、盗難（非権限者によるアクセス）、盗み見
② 後処理……紛失、盗難、誤びゅう、破損、漏えい
③ 搬送、輸送……紛失、盗難
④ 保管、廃棄……紛失、盗難、漏えい、放置（管理者の不在）
⑤ 複写、複製……紛失、漏えい
⑥ 引渡し……誤り、遅れ、受領者の相違

⑦ 形態……破損（梱包、封緘等の不適切）

(3) 出力管理の責任者の職務

① 情報システムからの出力処理にかかわる指示と承認

② 引渡し、後処理、伝送、保管等の出力情報に関する指示、承認等の実施

③ 業務システムユーザ（データ権限者）との職務範囲の明確化

④ トラブル発生時の迅速なリカバリ処理と対応指示

(4) システム形態による出力

① 集中処理形態……センターにおける処理は、ユーザの業務依頼及び業務処理スケジュールからの手続に従って行う。

② 分散処理形態……業務システムのユーザが出力管理の責任者であり、端末からの出力指示は、ユーザが直接実施する形態が多い。出力結果についても、直接ユーザの手元のプリンタ、画面又はハードディスク等に出力される。そのため、出力資格の設定には十分に配慮する。また、相互牽制機能が確実に機能するよう留意する必要がある。

(5) 出力手続

① 端末出力時の考慮事項

a．出力資格、パスワード……出力端末の正当性の確認、出力資格の確認

b．機密情報……暗号化の適用検討

c．出力確認……正常処理完了の確認方法

d．表示制限……放置による漏えい防止（スクリーンセーバの自動起動）、使用時間帯、接続時間の制限（接続時間制限による自動切断）　等

② 出力資格確認の例

a．データ、アプリケーションライブラリ、システムソフトウェア、ユーティリティソフトウェア等ごとに出力資格の設定と確認

b．出力資格及びパスワードの確認

c．出力記録の取得状況確認

(6) データ出力の関係者

① 情報システム部門

② 業務のユーザ部門

③ 外部委託先　等

(7) 出力管理ルールの見直し要因

① 定期的な見直し

② 手順又は出力形態の変更

③ 機械設備の変更、処理場所の変更　等

5. 出力管理

(2) 出力情報は、漏れなく、重複なく、正確であることを確認すること。

1 主　旨

情報システムからデータ出力を行う際は、出力情報に結果の誤り、欠落、二重出力等が発生しないように出力管理ルールに記載されている手順に従い、正確に行う必要がある。

2 着眼点

(1) 網羅性、正確性確保のための確認ルール、手順を定めていること。
(2) 出力管理の責任者が承認した担当者が出力を行っていること。
(3) 出力記録及び端末操作記録を一定期間保管していること。
(4) 出力管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。
(5) 定期的に出力管理ルールの効果を確認し、必要に応じて見直していること。

3 関連事項

(1) 出力者の確認

出力者が社内関係者に限定される場合は、出力資格及び処理実施内容を確認する。
B to C 等、出力者が一般に広範囲にわたる場合にも、承認を確実に実施する。
論理チェック、物理的チェック等による検証を加える。

① 社内システムでの出力資格確認の例
　a. 出力資格付与条件の設定と確認
　b. 出力資格（ユーザ ID、パスワード、ID カード、生体認証等）の確認
　c. 出力記録（ログ）の取得状況確認

② 電子商取引での出力資格確認の例
　a. 出力資格付与条件の設定と確認
　b. 出力資格（ユーザ ID、パスワード、ID カード、生体認証等）の確認
　c. 電子認証局による証明
　d. 出力記録（ログ）の取得状況確認

(2) 出力帳票の検証の例

① 出力管理票による検証
② 帳票枚数、ページ抜けの確認
③ 印字状況の確認
④ 二重出力のないことの確認

⑤ 梱包、発送等の正しい後処理の工程への引渡し確認

⑥ 機密度に応じた不要な出力帳票が廃棄されていることの確認

(3) 出力管理票の記述項目の例

① 出力予定日時

② 帳票種類

③ 出力プリンタ種類

④ 出力担当者

⑤ 出力プログラム名

⑥ 返却方法（発送形態、返却手段等）

⑦ 送付先

(4) 出力記録及び端末操作記録の主な項目

入力記録と同様、出力記録も出力内容の検証、エラー原因の追求等の目的で記録を一定期間（数か月、１年間等）保管しておく必要がある。特にコンテンツ提供等の商取引においては、利用者からの二重課金の問合せに対応するために記録の採取は、必須である。

① 一般の情報システム

a．端末ID、業務名、処理名、処理時間、出力依頼者名等

b．端末機別の出力依頼件数

c．出力先（帳票、端末、媒体） 等

② 電子商取引、インターネットによる情報照会等

a．利用者ID、提供内容（企業データ、映像、音楽等）、取引日時、取引内容の確認者等

b．利用者別の取引件数及び提供料の合計金額

5．出力管理

(3) 出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。

1 主　旨

出力情報の作成、取扱い等を正確に行い、改ざん、盗難、漏えい等を防止するため、誤びゅう防止、不正防止及び機密保護の対策を講ずる必要がある。

2 着 眼 点

(1) 出力情報の作成手順は、誤びゅう及び不正を防止する内容としていること。

(2) 不正な複写、複製等を防止する対策を講じていること。

(3) 出力情報の機密度に応じて取扱者を限定していること。

3 関連事項

(1) 出力情報の作成手順と取扱い

① 端末への情報出力の要件

a．情報の端末出力は、端末の操作者のアクセス資格の確認及びアクセス可能な業務の設定を行うこと。

b．社外からの情報出力は、使用ルール及び責任分担を契約によって明確にしておくこと。

c．端末からの長時間アクセスの防止及び通常と異なる大量データ出力の検知（顧客データの転売の防止）。

② センター出力における情報出力の条件

a．オペレーション指示書等によって、出力処理を行っていること。

b．複数のオペレータによるオペレーション作業を行っていること。

c．オペレーション日報等に作業結果を記録すること。

d．出力情報を確実に依頼者に引き渡すこと。

e．処理途中における機密の漏えい、紛失等を防止すること。

(2) 不正防止の仕掛け

① 端末機器への表示

a．非権限者による操作、画面ののぞき見、コピー取得の防止（端末機器の設置場所及び画面の向きの考慮、プライバシーシートの採用、ログイン時メッセージによる操作者への注意喚起等）

b．端末使用者の長時間離席時の継続表示の防止（スクリーンセーバ等）

c．通常と異なる大量照会の把握（自社又は契約先の社員による顧客名簿の流出、転売を防止）

② 出力情報のプリント

a．プリント処理者、出力権限保有者の限定

b．非権限者による出力指示の監視及び記録

c．プリンタからの印刷物の早期回収の徹底

d．社印、公印等があらかじめ印刷されている印刷用紙の管理の徹底

(3) 複写、複製等

① 重要データの複写は記録に残すこと。

② 重要機密等は、複写できないインク等で印刷すること。

(4) 出力の記録

① 情報出力に関するセンター処理の記録を取得していること。

② ネットワーク等を介する端末への情報出力の記録を取得していること。

③ 出力記録の作成段階で把握する項目

a．処理業務

b．処理日時

c．処理結果の正常、異常

d．処理担当者、依頼者

e．出力量　等

(5) 出力情報のチェック

① レコードID

② パスワードによる資格確認

③ データ件数

④ レコード項目の合計

5．出力管理

(4) 出力情報の引渡しは、出力管理ルールに基づいて行うこと。

1 主　旨

出力情報の引渡しの誤り、紛失、盗難等を防止するため、引渡し手続等のルールを定め、遵守する必要がある。

2 着 眼 点

(1) 出力情報の引渡しを記録していること。

(2) 引渡しの方法を適切に選択していること。

3 関連事項

(1) 引渡しルールとして明確にすべき項目の例

① 取扱い者（身分証の提示等）

② 引渡し確認事項（媒体、内容、数量、形態、方法等）

③ 引渡し日付（時間）

④ 引渡し場所

⑤ 記録事項

(2) データ漏えいや機密保護に配慮した引渡し、送付形態

① 梱包等送付形態の安全度

② 紛失、誤配、遅配の防止対策（媒体の正・副の別送、数量の確認）

③ 盗難対策

④ 破損、汚れ防止

⑤ 消磁防御方法

⑥ のぞき見の防止方法

⑦ 送付中の責任部門

(3) 引渡しに関するチェック項目の例

① 受領印のない引渡しを行っていないか。

② 権限者以外に引き渡されていないか。

③ 機密情報については、担当責任者に直接引き渡しているか。

④ 配布遅れはないか。ある場合は、その理由は妥当か。

⑤ 配布一覧表と受取人が適切か、定期的に見直しているか。

(4) 引渡し記録

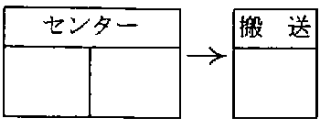
① 配布記録

a．出力情報の名称
b．作成年月日
c．媒体の種類
d．数量
e．配布先
f．配布年月日
g．受領印　等

② ユーザ自身による処理の場合
a．重要業務の処理を記録していること。
b．記録を保管していること。

(5) 重要な分散処理システムでは、出力情報に関するログを記録するシステムを整備すること（不正アクセスの防御）。

資料送付書



殿

作業名称			
依頼者TEL(内線)		作業依頼日	月 日 時
明細表	有 無	希望納期	月 日 時

資料名称	センター記入欄			ユーザ記入欄			備考
	束数	資料枚数	予定数量	束数	資料数量	出来高数量	

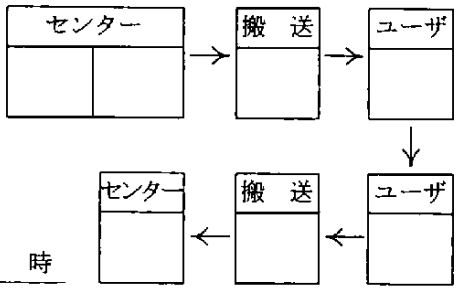
チェック後「レ」点を記す。

荷姿	送付時		送付時		備考
	ダンボール	箱	ダンボール	箱	
	ビニール袋	袋	ビニール袋	袋	
	M／T	巻	M／T	巻	
	F／D	枚	F／D	枚	
	その他( )		その他( )		

株式会社 A 情報システムセンター

①センター(控)

資料返納書



作業名称			
依頼者TEL(内線)		作業依頼日	月 日 時
明細表	有 無	希望納期	月 日 時

返却日時： 月 日 時

資料名称	センター記入欄			ユーザ記入欄			備考
	束数	資料枚数	予定数量	束数	資料数量	出来高数量	

チェック後「レ」点を記す。

荷姿	送付時		送付時		備考
	ダンボール	箱	ダンボール	箱	
	ビニール袋	袋	ビニール袋	袋	
	M／T	巻	M／T	巻	
	F／D	枚	F／D	枚	
	その他( )		その他( )		

株式会社 A 情報システムセンター 宛

③センター → ユーザ → センター

3部複写。1部目①はセンター控
2部目②はユーザ控
3部目③は受領サイン後、センター戻り

搬送指示書

月　日	時	宛先１	宛先２	宛先	担当課１	担当課２	責任者承認

搬送物荷姿	搬送番号					送付個数	受領サイン
搬送専用ケース（ジュラルミン）						ケース	
磁気媒体用トランク						個	
段ボール						箱	
その他（明細記入）						個	
備　考							

２部複写。１部目は送付先控

２部目は受領サイン後、送付先戻り

5. 出力管理

(5) 出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。

1 主　旨

出力情報の紛失、盗難、漏えい等を防止するため、保管及び廃棄は、出力管理ルールに基づいて行う必要がある。

2 着 眼 点

(1) 保管及び廃棄の責任者を定めていること。
(2) 出力情報を適切に保管していること。
(3) 出力情報の廃棄方法を定めていること。
(4) 重要な出力情報の廃棄は、責任者が立ち会っていること。
(5) 廃棄の委託は、契約条件、廃棄方法等を調査し、決定していること。
(6) 出力情報の保管及び廃棄を業務の責任者が承認していること。

3 関連事項

(1) 適切な保管場所及び保管管理に当たっての考慮事項
　① データ等保管室、保管設備の安全度と信頼度
　② 保管物品の重要性の区分
　③ 施錠の実施、管理状況（保管及び棚卸し等）
　④ 棚卸しの実施状況（管理台帳による記録、定期的な棚卸し、保管不要なデータの返却、保存期限と廃棄日との整合性確認）
　⑤ 保管場所への立入り者の限定
　⑥ 必要な保管期間（業務の重要度、法規制等を考慮）
(2) 廃棄の方法
　① 確実な廃棄を行うための廃棄方法及び廃棄場所の検討に当たっての考慮事項
　　a．方法の確実性……焼却、裁断、溶解
　　b．実施者の信頼度……自社内、社外委託
　　c．搬送の有無と方法……最終廃棄場所との関係
　　d．廃棄記録の保存
　　e．機密度に応じた適切な手続
　② 廃棄ルールと記録
　　a．対象
　　b．方法

c．時期、期日

d．担当者、立会い者

e．場所

f．搬送・輸送方法

g．責任者の承認

h．廃棄記録、廃棄証明（委託の場合）

③　廃棄方法等の監査に当たっての考慮事項

a．機密度に応じ、適切な廃棄方法が取られているか。

b．機密情報の廃棄は、再利用できない方法によって、管理者の立会いのもとに行われているか。

c．廃棄処理をその都度行わない場合、機密情報を放置していないか。

d．廃棄を外部委託する場合、モニタリングを実施すること。

(3) 廃棄の責任者

①　業務システムのユーザが、情報の廃棄の最終的な指示を行う責任者である。

②　業務システムのユーザから、情報システム部門の保管の責任者等が委託を受けて廃棄処理を行う等、情報内容や形態に合わせて実施することがある。

(4) 保管及び廃棄方法

「Ⅳ．運用業務　3.入力管理(5)」を参照。

5．出力管理

(6) 出力情報のエラー状況を記録し、定期的に分析すること。

1 主　旨

出力情報を正確に維持するため、エラー状況を記録し、定期的に分析する必要がある。

2 着 眼 点

(1) 出力情報のエラー状況を記録していること。

(2) 出力情報のエラーの原因を究明し、改善措置を図っていること。

3 関連事項

(1) エラー状況と記録項目の例

出力情報のエラー状況を記録し、システム及び運用業務の改善に役立たせる。

① エラー発生日時、エラー発見日時、エラー連絡日時

② エラー概要

③ エラー発見部門（発見者）

④ エラー責任部門

⑤ エラー原因（直接原因（原因部門、要因）、根本原因）

⑥ 業務への影響

⑦ 応急措置内容

⑧ 恒久措置方針、内容、担当部門、実施予定日、完了日

（注）ハードウェア等の出力情報以外の障害も、一括して取り扱うことが多い。

(2) エラーの発生する部分の例

① 入力データの作成ミス

② オペレーションミス

③ プログラムエラー

④ 誤った指示による処理

⑤ ハードウェア故障、通信エラー

(3) 改善措置

① 恒久的改善措置方針の検討

a．入力データのミスを防止する、チェックアウトする。

b．オペレーションミスを誘発しない。

c．プログラムエラーの修正

d．指示ミスを予防する。

② システム改善事項の一覧表化

③ 改善事項の優先順位付け

④ 計画的な改善の実施

⑤ エラーの発生頻度

a．エラーの発生頻度（現状の把握と改善目標値）

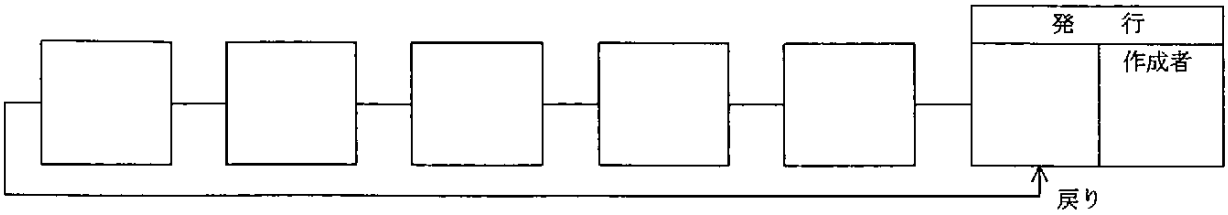
b．改善措置による改善実績の比較

(4) エラー記録表の例

次に示す「システム障害発生連絡票」と「システム障害報告書兼対策書」を参照。

システム障害発生連絡表 （第　報）

（発行No.　　）

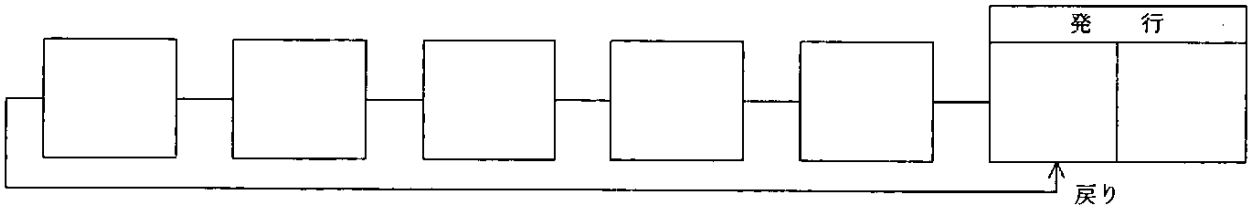


システム名称		処理名称		障害等名称	
1．発生日時	月　日（　）　時　分			報告日時	
2．発見日時	月　日（　）　時　分			(1．と異なる場合)	
3．発見・報告	当障害について(日時：　月　日　時　分) ┌より連絡を受けた。 (氏名：　所属：　) └に連絡した。				
4．現象、状況	(1)オンライン　(2)バッチ　(3)				
	(1)停止(全面；部分)　(2)結果不良　(3)システム、データ破壊　(4)その他				
	(1)システム停止時間(　)　(2)ユーザ業務停止時間(　)				
5．ユーザ業務状況、影響度	(1)確認中　(2)なし　(3)あり：				
6．原因	(1)調査中(担当：　)　(2)推定原因　(3)起因場所				
7．応急対策	(1)部署：　(2)担当者				
	(1)応援要否（要・否）　(2)応援工数　(3)応援内容				
	対策内容(システム部門)				
	(ユーザ部門)				
8．添付資料	(1)あり(内容)　(2)なし				
9．類似障害、影響、その他					

第一報は１．～５．の内容で即時報告のこと。

システム障害報告書兼対策書

No.	
発生連絡票No.	



発行元	システム名称		処理名称		障害等名称	
	発生年月日					
	障害現象		直接原因			
責任部署	根本原因		再発防止策			
	1.					
主副						
	2.					
主副						
検査部門	見解					
	類似障害		再発理由		総合的対策	

5．出力管理

(7) 出力情報の利用状況を記録し、定期的に分析すること。

1 主　旨

出力情報の有効活用を図るため、利用状況を記録し、定期的に分析する必要がある。

2 着 眼 点

(1) 出力情報の利用状況を分析及び評価していること。

(2) 分析結果に基づいて、出力情報の改善を図っていること。

3 関連事項

(1) 利用状況

① 利用状況の実態把握の例

a．ユーザの利用率が低い出力情報はないか。

b．ユーザが利用しにくい出力情報はないか。

c．利用権限に不一致はないか。

② 利用上の問題点

a．出力タイミングの遅れ

b．帳票設計の不備

c．内容の陳腐化

d．不要項目の削除、項目統合等の未実施

③ 出力情報の利用方法の限定を適切に設定していること

a．複写、複製

b．再加工

(2) 分析と評価

有効利用するための問題点の解決

① 問題点の内容は妥当か（問題点を調査する関係部門を網羅しているか）。

② 問題点を明確化（明文化）しているか。

③ 問題点の解決を図る部門を明確にしているか。

④ 問題の重要度評価、優先順位設定を行い、計画的に取組みを行っているか。

(3) 外部システムとの直接接続による利用

社外へのシステム、データの提供は、目的、提供先、提供内容又は提供範囲の妥当性を機密保護、知的財産権保護の観点から検討し、承認しているか。

① データの参照可能範囲

② プログラムの利用範囲
③ 不正アクセスに対する対処
④ 個人情報の場合、第三者提供の制限の考慮　等

6. ソフトウェア管理

(1) ソフトウェア管理ルールを定め、遵守すること。

1 主　旨

ソフトウェアの適切な利用及び不正防止のため、開発、運用及び保守業務に応じたソフトウェアの取扱い、管理の体制等をルールとして定め、遵守する必要がある。

2 着眼点

(1) ソフトウェア管理ルールを明文化し、組織体として承認していること。
(2) ソフトウェア管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証すること。
(3) 管理の対象は、組織体で使用しているソフトウェアを網羅していること。
(4) 管理の体系は、組織体として一貫性をもっていること。
(5) 定期的にソフトウェア管理ルールの効果を確認し、必要に応じて見直していること。

3 関連事項

(1) ソフトウェア管理ルールの策定項目の例
　① ソフトウェアの種類と機密度
　② ソフトウェア管理者（責任と権限）
　③ ソフトウェアの授受手順
　④ ソフトウェアの変更管理
　⑤ バックアップ採取の基準と方法・管理
　⑥ ソフトウェアの保管方法、保管場所及び保管期間
　⑦ ソフトウェアの廃棄方法
　⑧ ソフトウェアの複写方法
　⑨ 機密度に対応したアクセスコントロールの方法
　⑩ ソフトウェアの利用状況の記録
　⑪ ソフトウェアの属性情報の管理方法
　⑫ ソフトウェアの格納媒体と容量及び余裕領域の管理方法
(2) ソフトウェア管理の対象の例
　① メインフレームシステムの例
　　業務処理プログラム（オンライン用、バッチ用）、運用関連プログラム、OS、システム関連プログラム、ユーティリティプログラム、開発支援プログラム、JCL
　② クライアントサーバシステムの例

a．サーバ側……業務処理プログラム
サーバ用システム関連プログラム（OS 等）
プリントファイル管理プログラム
データファイル管理プログラム
運用関連プログラム

b．クライアント側……業務処理プログラム
クライアント用システム関連プログラム（OS 等）

③ パソコンの例
業務処理プログラム、パソコン用 OS、システム関連プログラム等

(3) クライアントサーバシステムにおけるソフトウェア管理のポイント

① 使用しているソフトウェア管理の責任者を明確にしているか。

② 各機器で使用しているソフトウェアの種類を明確にしているか。

③ ソフトウェアの保守状況の履歴を管理しているか。

④ プログラムとドキュメントを対応付けて管理しているか。

⑤ 機密性の高いソフトウェアは、不正利用及び機密保護の観点から適切な管理を行っているか。

⑥ ソフトウェアの使用許諾条件を遵守しているか。

6．ソフトウェア管理

(2) ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。

1 主　旨

ソフトウェアの不正利用を防止するため、アクセスコントロール及びモニタリングが有効に機能していることを確認する必要がある。

2 着 眼 点

(1) アクセスコントロールが有効に機能していること。

(2) アクセス状況のモニタリング機能の稼動状況を確認していること。

(3) 無資格者による情報システムの利用を定期的に調査していること。

(4) 不正利用、不正アクセスの調査を行い、再発防止策を講じていること。

(5) 業務内容、組織、基本ソフトウェア等の変更に伴い、アクセスコントロール機能を見直していること。

3 関連事項

(1) アクセスコントロール機能の例

① 資格確認機能（ユーザ ID、パスワード、生体認証等）

② 各資源へのアクセス権限機能

（ファイル種別ごとの制限、読み／書き／追加／削除の機能制限）

③ コールバック機能

④ ファイアウォール機能

(2) モニタリング機能の例

① アクセス記録

② コンソールログ

③ システム使用状況ログ

④ コミュニケーションログ

(3) アクセスコントロールの有効性監査の留意点

① 使用しているアクセスコントロールの機能は、対象データの保護に対応しているか。

② アクセスコントロールは、機能しているか。

③ アクセスコントロールの記録は、分析され必要な措置が講じられているか。

④ 情報システムの改変に伴い、アクセスコントロールの使用機能が見直されているか。

(4) アクセスコントロールの運用に当たっての留意点

① セキュリティ管理者（責任と権限）の設定

② ログイン管理機能
③ ユーザ ID の割振りと管理
④ パスワード管理（管理者と管理方法：設定・解除の状況）
⑤ 定期的モニター分析
⑥ 機密度に応じたソフトウェア管理
⑦ 不正行為等の発生時の対応（検出・検知の状況）

(5) 異常アクセスの検出の分析対象項目の例
① アクセス回数
② 使用時間
③ アクセス時刻
④ アクセス拒絶の記録
⑤ パスワード入力エラーの記録
⑥ 通常より明らかに多い情報照会及び出力依頼の記録

6. ソフトウェア管理

(3) ソフトウェアの利用状況を記録し、定期的に分析すること。

1 主　旨

ソフトウェアの稼動効率の向上を図り、不正利用を防止するため、ソフトウェアの利用状況を記録し、定期的に分析する必要がある。

2 着 眼 点

(1) ソフトウェアの利用状況を記録する機能を設けていること。

(2) ソフトウェアの利用状況を定期的に分析していること。

(3) 分析結果に基づき、情報システムの運用改善を図り、不要ソフトウェアの廃棄を行っていること。

3 関連事項

(1) ソフトウェアのファイルの利用状況の記録項目の例

① ユーザID

② アクセスファイルの種別

③ アクセスの種類（読み／書き／追加／削除）

④ アクセス時間（開始時刻、終了時刻）

⑤ ユニット利用率、ストレージ使用率

⑥ データヒット率、エラー率

⑦ チャネル利用率

(2) ソフトウェアのファイルの利用状況の留意点

① 利用状況の把握には、独自の分析ツール、システムで用意されているログ及び監査機能の使用も考慮する。

② 収集するログの範囲及びレベルは、アクセスコントロールの目的から適切に設定する。

③ ソフトウェアのファイルの利用状況を継続的に調査し、一定期間での利用予測を行う。

(3) ソフトウェアのファイルの稼動状況を把握し、将来の利用状況の予測のために、次の項目を分析する。

① ソフトウェア領域の使用中領域と拡張用領域のバランス

② 新規ソフトウェア作成の伸び率

③ ソフトウェアのファイルに対するピーク時間当たりのアクセス回数

④ 不要ソフトウェアを削除するガーベージ作業の間隔

⑤ 装置の未使用余裕領域の大きさ

6．ソフトウェア管理

(4) ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。

1 主　旨

ソフトウェアの記録媒体の障害、誤操作、コンピュータウイルス等による影響を最小にするため、ソフトウェアのバックアップの範囲及び方法は、業務内容及び処理形態を考慮して定める必要がある。

2 着 眼 点

(1) バックアップの範囲、記録媒体、保管方法等は、業務内容及び処理形態に応じて定めていること。

(2) バックアップ方法及びリカバリの方法は、情報システムの変更に伴い、見直していること。

3 関連事項

(1) バックアップの範囲の検討に当たっての考慮事項

① 障害を管理する単位（例：ディスク装置の単位）

② バックアップ媒体の容量（例：磁気テープ等の容量）

③ バックアップの時間（例：並行処理によるバックアップ時間の短縮化）

④ 業務の影響範囲（例：同一業務で使用するソフトウェアのファイルの一括バックアップ）

⑤ 情報システムの変更に伴うバックアップの範囲の変更

(2) バックアップのタイミングを検討するに当たっての考慮事項

① リカバリの方法

② 回復許容時間

③ 業務の重要度

④ ファイルの特性（例：読込み専用ファイル、オンライン用ソフトウェアのファイル等）

⑤ バックアップ採取が情報システムに与える影響度合い

⑥ リカバリ失敗時の代替手段

(3) ソフトウェアのファイルの障害対策の検討のポイント

① 使用中のソフトウェアの機能を理解し、適正な障害回復手段の方針を策定する。

② システム障害に備え、ソフトウェアのファイルのバックアップを採取する。

③ 外部より導入したソフトウェアのバックアップの採取は、使用許諾条件を遵守する。

④ 採取したバックアップファイルは、責任者を定め、安全な場所に保管する。

6．ソフトウェア管理

(5) ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。

1 主　旨

ソフトウェアの誤使用、不正利用、改ざん等を防止するため、ソフトウェアの授受は、手順、方法等を定めたソフトウェア管理ルールに基づいて行う必要がある。

2 着 眼 点

(1) ソフトウェアの授受は、ソフトウェア管理ルールで定める担当者が行っていること。

(2) ソフトウェア管理ルールに基づいて、ソフトウェアの授受、保管、確認及び返却を行っていること。

(3) ソフトウェアの授受を記録し、ソフトウェア管理の責任者が承認していること。

(4) ソフトウェアの授受記録を一定期間保管していること。

3 関連事項

(1) ソフトウェアの授受のルールで定める事項の例

① 責任者及び担当者の任命

② 取扱い及び授受の方法・手続

③ ソフトウェア管理システムの構築又はソフトウェア管理台帳の常備と記入

④ 入出庫管理システムの構築又は入出庫記録簿の常備

⑤ 授受の確認方法、障害時の連絡体制　等

(2) クライアントサーバシステム、PCのソフトウェア授受のポイント

① 授受の記録の励行

② 必要なソフトウェアのみの授受

③ 授受ソフトウェアのコンピュータウイルスチェック

④ 知的財産権を侵害していないことのチェック

⑤ 機密性及び重要性の観点を考慮した授受後の媒体の適切な保管方法

6．ソフトウェア管理

(6) ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。

1 主　旨

ソフトウェアの不正利用、漏えい等を防止するため、ソフトウェアの保管、複写及び不要ソフトウェアの廃棄は、不正防止及び機密保護の対策を講ずる必要がある。

2 着 眼 点

(1) 保管、複写及び廃棄は、ソフトウェアの機密度及び記録媒体に応じた不正防止及び機密保護の対策を講じていること。

(2) 保管、複写及び廃棄をソフトウェア管理の責任者が承認していること。

(3) ソフトウェアの複写は、使用許諾条件に基づいていること。

(4) ソフトウェアの保管、複写及び廃棄は、履歴を記録していること。

(5) 重要なソフトウェアの廃棄をソフトウェア管理の責任者が確認していること。

3 関連事項

(1) ソフトウェアの保管方法における検討事項の例

① 保管ルール（組織管理と個人管理のルール化等）

② ソフトウェアの種類・機密度に応じた管理台帳の作成

③ 重要性、緊急性及び機密性のそれぞれの区分

④ 世代管理と分散保管

⑤ ソフトウェアのライセンスの取扱い

⑥ 保管責任者

(2) ソフトウェアの保管場所における検討事項の例

① 媒体に適した保管場所

② 使用頻度と授受手順

③ 機密度と保管環境

④ 保管場所の施錠管理

⑤ 組織管理と個人管理の区分と保管場所

(3) ソフトウェアの保管時における不正防止対策の例

① 管理責任者の任命

② 管理台帳等によるデータ利用管理

③ 施錠保管、隔離保管

④ 自動入出庫装置の利用

⑤ ライセンス購入可能なソフトウェアは、ライセンスを購入し、不必要なソフトウェア格納媒体の保有を抑止

(4) ソフトウェアの保管時における機密保護の対策の例

① ラベル等におけるデータ内容の非表示

② 機密度に応じた保管時の管理体制

③ 暗号化

④ USB、PDA（携帯情報端末）等のスモールデバイスへの保管制限

(5) ソフトウェアの複写において、重要ソフトウェアの不正利用防止及び機密性の高いソフトウェアの保護の対策の例

① ソフトウェアのファイル等に対するアクセスコントロール

② ソフトウェアのファイルに対するアクセスの記録と分析

③ 複写の事前申請と責任者による許可

④ 複写先のソフトウェアの暗号化

⑤ 複写記録の管理

(6) ソフトウェアのファイルへのアクセスコントロールの例

① 資格機能管理（ユーザ ID、パスワード等）

② 各資源へのアクセス権限制限機能

③ モニタリング機能（違反アクセスの記録・分析、コンソールログ、システム使用状況記録機能等）

④ 相手確認機能（コールバック等）

⑤ 暗号化機能

(7) ソフトウェアの廃棄に当たっての検討事項

① 廃棄方法……消磁、焼却、裁断、破壊等

② 廃棄ルール……担当者、目的、方法、期日、場所、責任者の承認、廃棄記録簿等

6．ソフトウェア管理
(7) ソフトウェアに対するコンピュータウイルス対策を講じること。

1 主　旨

ソフトウェアをコンピュータウイルスから保護するため、コンピュータウイルス対策を講ずる必要がある。

2 着 眼 点

(1) 情報システムの環境に適合したコンピュータウイルス対策を講じていること。

(2) コンピュータウイルス対策を周知徹底していること。

(3) 被害状況を報告し、コンピュータウイルス対策を実施する体制になっていること。

3 関連事項

(1) ソフトウェアに対するコンピュータウイルス

コンピュータウイルスは、「第三者のプログラムやデータベースに対し、意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能のいずれか１つ以上を有するもの」である。

コンピュータウイルス自身もプログラムであるが、

① ソフトウェア、データ等、すべての情報資産が対象となり得る。

② OS及びブラウザのセキュリティホールやWebの閲覧等、ウイルス侵入の可能性が多岐にわたり、一度混入すると組織体に広く感染することから、ソフトウェアに対するコンピュータウイルス対策が必要である。

(2) コンピュータウイルス対策の主要項目

① 組織体としてのコンピュータウイルス対策実施要綱（コンピュータウイルス検査方法、検査時期等）の制定

② 機器、プログラム、データ等の属性情報等の把握と管理

③ 機器管理・運用手順の策定と遵守

④ コンピュータウイルス対策ソフトウェアの利用

ａ．コンピュータ機器のコンピュータウイルス検査

ｂ．外部交換ソフトウェア、データ等のコンピュータウイルス検査

ｃ．外部からのアタックテスト及びセキュリティホール検査

ｄ．コンピュータウイルス定義ファイル及び検索エンジンの最新化

⑤ コンピュータウイルスの万一の感染を想定

ａ．重要データのバックアップ取得

b．社外への被害拡大防止に向けた対策の立案

⑥ 被害状況の把握と公的機関に対する報告

a．独立行政法人　情報処理推進機構　セキュリティセンター（IPA/ISEC）

b．有限責任中間法人 JPCERT/CC

⑦ コンピュータウイルス対策支援部門の設立

⑧ 教育・啓蒙

a．電子メール……出所不明なメール、不審に感じたメールの添付ファイルは絶対に開かない。

b．Web……閲覧のみで感染するケースがあるため、組織体での不必要な閲覧は行わない。

c．外部記録媒体……外部記録媒体（FD、CD-ROM 等）の受領時には必ずコンピュータウイルスのチェックを行う。

(3) コンピュータウイルス対策の参考基準

経済産業省「コンピュータウイルス対策基準」（関連資料 参照）を参考にする。

6．ソフトウェア管理

(8) ソフトウェアの知的財産権を管理すること。

1 主　旨

開発したソフトウェアの知的財産権の保護及び導入したソフトウェアの知的財産権の侵害を防止するため、知的財産権を管理する必要がある。

2 着眼点

(1) 知的財産権の教育を実施し、著作物に対する認識をもっていること。
(2) 知的財産権の保護を対象とするソフトウェアを明確にしていること。
(3) 外部からのソフトウェアは、定められた手続で導入していること。
(4) 導入したソフトウェアの知的財産権を侵害していないことを定期的に調査していること。

3 関連事項

(1) ソフトウェアの知的財産権

a．プログラムの保護

保護される知的財産権は、これまでの著作権法による「プログラムの著作物」にとどまらず、特許法によりビジネスモデル特許等のアイディアやアルゴリズムも保護の対象となる。

b．同一性保持権

著作者は、著作物について同一性を保持する権利を有し、著作者の意図に反し改変・変更等をすることはできない。ただし、当該コンピュータで利用できるための改変、より効果的に利用するための改変は認められる。

c．所有者による複製

プログラムの所有者が、自己の利用のために必要と認められる限度においては、複製又は翻案することができる。ただし、著作者が複製又は翻案を許可していないプログラムについては、決して複製又は翻案をしてはならない。

(2) ソフトウェアの知的財産権の管理のポイント

① ソフトウェアの違法複製行為の禁止及び違法複製品の使用禁止の徹底
② 使用ソフトウェアを購入段階から把握及び管理するためのソフトウェア管理者の設定
③ ソフトウェアの使用手順や管理方法を定めたソフトウェアの管理規則の策定
④ ソフトウェアの違法複製等の有無の確認のためのソフトウェアの使用状況に関する監査の実施
⑤ ソフトウェアのライセンスを購入する場合の購入したライセンス数と実際の使用状況の正

確な把握

⑥ パーソナルコンピュータに添付しているリカバリ CD 等のソフトウェアの保管場所の確保と適正管理の実施

⑦ ソフトウェアの適正な使用に対するユーザ意識の向上を図るためのユーザの教育及び啓発の実施

6．ソフトウェア管理

(9) フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。

1 主　旨

フリーソフトウェアは便利に低コストで使える反面、処理結果の無保証、コンピュータウイルス混入の危険性、知的財産権侵害等のリスクもあり、利用の際は、組織体として一定の方針を定める必要がある。

2 着眼点

(1) フリーソフトウェア及びシェアウェアに対する組織体の方針を定めていること。

(2) 方針は責任者が承認するとともに、組織体のすべてに遵守されていることを検証していること。

(3) フリーソフトウェア及びシェアウェアの利用状況を管理していること。

3 関連事項

(1) フリーソフトウェア及びシェアウェアの取扱方針の項目例

フリーソフトウェア及びシェアウェアについて、組織体として、ルールを定めた上で自由な利用を認める方式や、所管部門へ登録申請を行い許可する方式等がある。

① ダウンロード時は信用できるサイトから入手する。

② ダウンロード後は、速やかにコンピュータウイルスチェックを行う。

③ フリーソフトウェア及びシェアウェアの利用は使用制限を遵守する。

④ フリーソフトウェア及びシェアウェアは作者に無断で改造しない。

⑤ シェアウェアは、使用料金を支払う。

⑥ フリーソフトウェア及びシェアウェアの利用状況を確認する。

⑦ フリーソフトウェア及びシェアウェアを組み込んだプログラムを作成する際には、権利条件等を確認する。

(2) フリーソフトウェア及びシェアウェアの留意事項

① フリーソフトウェア及びシェアウェアは、知的財産権（他のソフトウェアやアルゴリズム等）に関する確認が不十分な物が多く、無意識のうちに著作権を侵害する可能性がある。

② フリーソフトウェア及びシェアウェアの中に営利目的の利用を禁じているものがあり、作者の使用許可範囲を十分確認すること。

③ フリーソフトウェア及びシェアウェアそのものに違法性はないが、使い方によっては違法となり得るものがある。

④ フリーソフトウェア及びシェアウェアの中にバックドア、トロイの木馬等が仕込まれているケースがあり、リスクを認識しておく必要がある。

7．ハードウェア管理

(1) ハードウェア管理ルールを定め、遵守すること。

1 主　旨

ハードウェアの適切な利用を図り、障害を防止し、自然災害、不正行為等から保護するため、ハードウェア管理ルールを定め、遵守する必要がある。

2 着 眼 点

(1) ハードウェア管理ルールを明文化し、組織体として承認していること。

(2) ハードウェア管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。

(3) 組織体で使用しているハードウェアを管理の対象としていること。

(4) 定期的にハードウェア管理ルールの効果を確認し、必要に応じて見直していること。

3 関連事項

(1) ハードウェア管理ルールの策定項目の例

① ハードウェア管理の責任者と担当者の設置、職務

② 管理対象ハードウェア
（対象には移動可能な媒体、可搬型コンピュータを含む）

③ 設置及び保管場所の選定条件

④ 管理項目

⑤ 管理マニュアル

⑥ 保守の方針と実施方法

⑦ ハードウェアの監視項目、方法（ツール）

⑧ 障害発生時の対応

⑨ モバイル機器、モバイル運用の適否

(2) ハードウェア管理の責任者

運用管理の責任者は、ハードウェアの適切な利用のため、ハードウェア管理の責任者を任命する必要がある。ハードウェア管理の責任者はハードウェアの管理項目、保守状況及び障害発生時の障害内容を把握し、必要な処置を行う。

ハードウェア管理責任者は、分散処理形態のシステムでは機器の設置場所別に任命する等、システムの形態に応じて適切に任命すること。

(3) 導入と活用

① 導入や利用について技術的、経営的観点から考慮すること。

a．目的の検討と承認

b．技術的検討と承認

c．経営的検討と承認

d．既存システムに与える影響の検討

(4) 管理項目

① 利用状況のデータを把握すること。

CPU 負荷、ネットワーク負荷、チャネル負荷、ディスク容量等

② ハードウェア管理記録をとること（管理台帳、日誌・保守記録等）

③ ハードウェア管理責任者等のための説明書や手順書の整備

a．ハードウェア取扱い説明書

b．ハードウェア利用者マニュアル等

(5) ハードウェア管理ルールの見直しは、次の時点で考慮する。

① ハードウェアの導入、増設、移設、撤去

② ハードウェアの設置環境の変更

③ 業務システムの変更

④ ネットワーク環境の変更

⑤ 運用体制の変更　等

7．ハードウェア管理

(2) ハードウェアは、想定されるリスクに対応できる環境に設置すること。

1 主　旨

障害、自然災害、不正行為等が情報システムに及ぼす影響を最小にするため、ハードウェアは想定されるリスクに対応できる環境に設置する必要がある。

2 着 眼 点

(1) ハードウェアに関するリスク分析を計画的に行っていること。

(2) リスク分析の結果に基づき、リスクに対応できる環境条件を明確にしていること。

(3) リスクへの対応として設定した環境条件を維持していること。

(4) リスクに対応した管理を行うこと。

3 関連事項

(1) ハードウェアの設置環境のリスクと対策例

① 情報の漏えい、機密漏えい

ａ．無資格者のアクセス、異常時刻のアクセス、画面ののぞき見の防止等

ｂ．不特定者の自由な立入りを防止できる環境の設定

② 持出し、破壊防止

ａ．設置環境からの物品持出し、持込みの禁止
ルールの徹底、持出しの申請、入退室管理

ｂ．可搬型の媒体及び機器の管理者の明確化

ｃ．即時の棚卸し確認

ｄ．重要性の高いハードウェアの監視カメラのモニタリング

③ 使用環境の不備によるシステムの停止、稼動異常

ａ．センター等の機器の使用環境条件を満たす設置環境

ｂ．事務所環境の温度、湿度、日照、埃、震動、電源、電磁波等の制御

ｃ．保守・点検の実施

④ 設置場所の分離、施錠の不可等による物理的な管理が困難な場合
設置環境の改善、見直し

⑤ 自然災害等による機器、媒体の破壊
地震対策……機器、設備の転倒防止、フリーアクセス床の浮上り防止対策
水害対策……建物内への浸水防止防護壁の設置、想定浸水レベルより高い位置への機器の設置、ネットワークの天井部への敷設　等

(2) 環境の維持

設置環境を定常的に監視し、環境条件を的確に維持し、ハードウェアの作動に悪影響を及ぼす要因を除去することによって障害を防止する。

① 電流、電圧、温度、湿度、漏水、地震等の検知設備を設置する。

② 検知した異常に対し、警報発信、自動対策の起動等速やかな対応行動をとる。

(3) ハードウェア設置環境の防犯及び防災

分散処理システムの機器の設置環境は、ハードウェアやサービスされる情報の価値に応じて定めること。

設置に際しての考慮事項

① サーバ、主要機器の設置は、可能な範囲でコンピュータ室に準じた監視のできる環境（室）に設置する。

② 不特定多数の者が接触可能な端末からの機密情報のアクセスを不可能にする。

③ 機密情報を扱う端末は、不特定多数の者が見ることができる場所には設置しない。

④ 事務室内で不特定多数の者が接触できる端末には、かぎをつける。

⑤ 端末からの離席時に、画面に表示しない、表示させない対策を実施する。

⑥ 移動を前提としないハードウェアの移動は、許可を必要とする。

⑦ 盗難防止のために軽量機器等はチェーン等によって固定する。

⑧ 転倒防止のために機器を固定する。

(4) システム監査の実施に当たっては、経済産業省「情報システム安全対策基準」（関連資料 参照）を参考にする。

該当する基準項目を次ページの表に示す。

(5) 建物・室の入退室管理方法の違いによってハードウェアのリスクが変わる。したがって、リスクに応じた管理を行う必要がある。

管理方法の違いの例

① 受付担当者が配置されている管理方法

② カード、認証機器等による入退室管理設備が設置されている管理方法

③ 建物の設置環境（「Ⅳ. 運用業務　10. 建物・関連設備管理」を参照）

大項目	中項目	小項目
Ⅴ. 設置基準	イ. 設置環境	1. 立地・配置 7. 情報システム
	ホ. 地震対策 a. 設置環境	4. 内装 6. 什器・備品
Ⅵ. 技術基準	イ. 情報技術の適用	
	ロ. 災害・障害対策機能	1. 災害対策機能 2. 障害対策機能
	ハ. 故意・過失対策機能	2. データ処理不正防止機能 3. 情報漏えい防止機能
Ⅶ. 運用基準	イ. 計画	1. 情報システム等の運用計画 2. データ等の管理計画 3. 組織・管理規程
	ロ. 情報システムの運用	1. システム管理 2. 利用者管理 3. 操作 4. 災害発生時対応
	ハ. データ等及び記録媒体の保管及び使用	1. 管理 2. 保管 3. 使用 4. 防犯対策 5. 災害・障害対策

7．ハードウェア管理

(3) ハードウェアは、定期的に保守を行うこと。

1 主　旨

ハードウェア障害による情報システムの停止及び機能低下を未然に防止するため、定期的に保守を実施する必要がある。

2 着眼点

(1) 保守対象、保守内容及び保守サイクルを明確にしていること。

(2) 保守の実施時にデータ等の漏えいを防止していること。

(3) 保守の結果を記録し、責任者に報告していること。

3 関連事項

(1) 保守の実施に当たっての留意事項

① 各機器の定められた保守条件を満たしていること。

② 保守対象機器の漏れがないこと。

③ 保守の頻度及び方法を環境に応じて定めること。

④ 点検によって判明した障害原因を究明し、再発防止並びに問題の改善措置を講ずること。

⑤ 予防保守の必要性の検討

(2) 臨時保守の計画と実施

① 障害の内容及び頻度を考慮し、適切な臨時保守を計画、実行していること。

② 内外のハードウェアの障害に関する情報を収集し、自己の情報システムへの影響、関係を整理するとともに、適切な臨時保守を実施すること。

(3) ハードウェアの保守及び障害修理記録内容の例

① 保守実施日

② 内容（装置名、現象、原因、処置内容、作業時間）

③ 結果、特記事項

④ 保守担当者

⑤ 障害発生日時

⑥ 障害内容、影響度

⑦ 障害原因、対策内容、対策者　等

(4) 日常の点検項目

オペレーション業務における点検例

① センター機器、ネットワーク機器の作動状況の確認

② 遠隔監視装置による監視結果の確認

③ 関連設備（電源、空気調和機器、警備設備の作動）の点検を併せて行うことがある。

7．ハードウェア管理

(4) ハードウェアは、障害対策を講じること。

1 主　旨

情報システムの稼動停止及び機能低下を防止し、障害発生時の早期復旧のため、ハードウェアの障害対策を講ずる必要がある。

2 着眼点

(1) 障害時の連絡体制を整備していること。

(2) 障害対策の現状を把握し、必要に応じてレビューしていること。

(3) 障害発生のリスクを分析し、必要な障害防止策を講じていること。

(4) 障害の早期復旧措置を講じていること。

(5) 障害対策の機能を確認していること。

3 関連事項

(1) 障害時連絡網の整備

① 社内連絡（ハードウェア管理の責任者、運用管理の責任者、ユーザ部門長等）

② 社外ユーザ（ネットワーク接続先等）

③ ハードウェアベンダー（保守担当部門） 等

(2) 障害対策の把握と復旧

ハードウェア管理の責任者は、ハードウェア障害の対策内容を把握、記録し、予防、緊急対応及び早期復旧を推進する。また障害発生時対応の訓練を実施する。

① 障害防止策の実施確認

② 障害早期発見策の確認、徹底

③ 障害発生の宣言

④ 障害時の緊急連絡方法の整備

⑤ 緊急対応策（業務継続策、代替処置）

⑥ 早期復旧策推進（代替機器の利用、遠隔保守） 等

(3) 障害による情報システム機能停止等の未然防止策の例

① 保守（定期保守、臨時保守）の実施

② 代替機能の整備

③ 代替機能への切替えの定期的な訓練

④ 機器、システムの二重化

⑤ バックアップセンター等の利用の実効性の検討及びバックアップ機器等の実効性の確認

⑥ 障害復旧措置の機能の定期的確認

(4) 緊急対応策・復旧措置の明文化

① 緊急対応策・復旧措置方法の明文化と関係者への周知徹底

② 定期的な見直しの実施

(5) 代替機能、障害発生時のバックアップ措置の例

① 情報システムの二重化、ホットスタンバイ、コールドスタンバイ

② 通信回線装置、通信機器、通信回線等の二重化

③ バックアップセンターの利用

④ 業務の縮退手続の明確化

7．ハードウェア管理

(5) ハードウェアの利用状況を記録し、定期的に分析すること。

1 主　旨

ハードウェアの有効利用を図り、不正利用を防止するため、利用状況を記録し、定期的に分析する必要がある。

2 着 眼 点

(1) 利用状況の記録項目を明確にし、記録していること。

(2) 分析項目を定め、利用状況の記録を分析していること。

(3) 分析結果に基づき、ハードウェア利用の改善を図っていること。

3 関連事項

(1) 利用状況の記録・分析

① 稼動情報項目の例

a．CPU 稼動率、メモリ利用率、チャネル稼動率、ディスク利用率（容量、アクセス負荷）、プリンタ稼動率、ページング回数

b．各稼動率は単位時間当たりの最大稼動率・利用率、平均稼動率・利用率データを取得する。

② 分析事項

a．CPU 余裕率

b．CPU 及びデバイスの稼動時間、稼動率、レスポンスタイム、業務システムごとの CPU 稼動時間等

c．業務システムのレスポンスタイムとの関連で、問題の有無をチェックする（ネットワークに関する回線データと併せて判断する）。

③ 定期的な分析

稼動情報の項目を決め、定期的（１か月、３か月等）に利用状況の推移を見る。

(2) 利用状況の改善

利用状況によるシステム更新に当たっての考慮事項

① ハードウェアのネック状態の把握

CPU 負荷、ディスク容量、ネットワーク負荷の状態を把握していること。

② ピーク時処理が可能なこと。

利用状況の記録分析は、業務処理のピーク時を評価していること。

③ 情報システムの方針に沿った計画であることを責任者が承認していること。

7．ハードウェア管理

(6) ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。

1 主　旨

ハードウェアの盗難、紛失等による権限者以外のハードウェア利用の防止、及びデータ等の情報資産保護のため、ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講ずる必要がある。

2 着眼点

(1) ハードウェアの保管、移設及び廃棄に関するルールを定め、運用等の責任者が承認していること。

(2) 保管、移設及び廃棄は、ハードウェアの特性及び保有する情報資産に応じた不正防止、機密保護及び個人情報保護の対策を講じていること。

(3) ハードウェアは、所定の場所、期間及び方法で保管していること。

(4) 重要なハードウェアの移設、廃棄には、ハードウェア管理の責任者が立ち会っていること。

3 関連事項

(1) ハードウェアの保管方法における検討事項の例

① 保管ルール（組織管理と個人管理のルール化、保管状況の確認）

② 保有する情報資産（プログラム及びデータ等）の種類・区分の整理と管理台帳による管理

③ 重要性、機密性の区分による整理

④ 保管場所、保管責任者の設定と定期的な棚卸し

(2) ハードウェアの保管場所における検討事項の例

① ハードウェアの特性に適した場所

② 組織管理と個人管理の区分

③ 保管場所の環境（入退室管理手続、施錠の状況）

(3) ハードウェアの移設時における検討事項の例

① ハードウェア管理の責任者（管理責任組織）変更の手続

② 移設元、移設先のそれぞれの管理責任事項の明確化

(4) ハードウェア廃棄時の検討事項の例

① ハードウェア廃棄手続の明確化

② データ等の情報資産の消去等の対応区分の明確化

③ 廃棄業者との機密保護対策の確認と契約等による明確化

④ 廃棄作業……部門の作業状況の確認

⑤ 廃棄方法……消去、データ記録装置の除去・破壊

⑥ 廃棄ルール……ルールの目的、廃棄方法と確認方法、責任者の承認、廃棄記録簿の作成、マニフェストのチェック

(5) ハードウェアの不正利用防止策の例

① 管理責任者の役割の明確化と任命

② 管理台帳等によるハードウェア利用状況管理

③ 施錠保管、隔離保管

④ 起動時のパスワード機能

(6) ハードウェアのデータ等情報資産の機密保護対策の例

① 利用者識別とアクセス権限

② 外部記録装置・媒体の利用制限

③ データの暗号化

8. ネットワーク管理

(1) ネットワーク管理ルールを定め、遵守すること。

1 主　旨

ネットワークの正常かつ効率的な稼動のため、ネットワーク管理ルールを定め、遵守する必要がある。

2 着 眼 点

(1) ネットワーク管理の責任者を定めていること。
(2) ネットワーク管理ルールを明文化し、組織体として承認していること。
(3) ネットワーク管理の範囲を明確にしていること。
(4) ネットワークの稼動状況を常時監視できる体制を作っていること。
(5) 定期的にネットワーク管理ルールの効果を確認し、必要に応じて見直していること。

3 関連事項

(1) ネットワーク管理ルールの策定項目の例
　① ネットワーク管理の目的と範囲
　② ネットワーク管理の責任者と体制
　③ ネットワークの障害対策と障害発生時の処理手順
　④ ネットワーク構成管理の方針と手順
　⑤ ネットワーク稼動監視の方針と手順
　⑥ ネットワークセキュリティ管理の方針と手順
　⑦ ネットワークコスト管理の方針と手順
　⑧ ネットワーク機器の保守管理の方針と手順
　⑨ ネットワーク管理ツールの利用方針
　⑩ 他の組織体とのネットワーク接続方針と手順
(2) ネットワーク管理の対象の例
　① ネットワーク機器
　　ハブ、リピータ、スイッチングハブ、ルータ、ゲートウェイ、アクセスサーバ、ファイアウォール、無線 LAN アクセスポイント、通信制御装置、端末制御装置、モデム、ターミナルアダプタ等
　② 伝送路・伝送媒体
　　構内ケーブル、キャリア会社が提供する各種回線サービス等
　③ ネットワーク管理情報

ネットワーク構成図、IP アドレス設計情報、IP アドレス設定情報、ネットワーク管理台帳、ハードウェア管理台帳、ネットワーク管理用のユーザ ID 等

(3) ネットワーク管理者の責任

ネットワーク管理の責任者は、ネットワークを常に健全な状態で運用するためのネットワーク管理ルールの策定・改訂、管理手続の実施について責任を負う。また、責任者が必要に応じて複数名から構成される場合があるが、それぞれの役割と権限を明確にすること。

(4) ネットワーク管理の範囲

ネットワーク管理の責任者は、エンドユーザ、キャリア会社が提供するネットワークサービス及びベンダーが提供する IDC (インターネットデータセンター) 等との責任分界点を明確にして、ネットワーク管理の範囲と管理項目を明文化すること。

(5) ネットワーク稼動監視のポイント

① 重要なシステムに影響を及ぼすネットワーク機器や伝送路について、運転中か休止中であるかの状況が常時把握できる仕組み及び体制が機能していること。

② 重要なシステムに影響を及ぼすネットワーク機器や伝送路において、障害が発生した場合、直ちにネットワーク管理の責任者に通知する仕組みが機能していること。

③ 重要なシステムに影響を及ぼすネットワーク機器や伝送路について、使用率やエラーパケット数等の性能を定期的に計測、評価及び記録していること。

④ ネットワークに重大な過負荷・性能劣化が発見された場合、適切な対処を遅滞なく行っていること。

⑤ トラフィックの増加によってネットワークの性能劣化が予想あるいは発見された場合、ネットワークの増強等の適切な対処を遅滞なく行うことを明文化していること。

(6) ネットワーク管理ルールの見直し

① ネットワーク管理ルールは、ネットワークの規模、運用管理体制の変更、ネットワーク障害の再発防止、技術の進歩等を反映して適切に変更すること。

② ネットワーク管理の責任者が、ネットワーク管理ルールの適切性に注意を払い、結果として陳腐化したルール、非効率な手順を改める手順が明確化されていること。

③ ネットワーク管理ルールの変更は、ネットワーク管理の責任者と運用管理の責任者の承認を得た上で、各運用管理の担当者に周知徹底すること。

(7) ネットワーク管理ルールと災害復旧計画との整合性

災害時の情報システムの復旧では、通常、ネットワークを優先して復旧する。それを支援する旨をネットワーク管理ルールにおいて明確に定めていること。

(8) ネットワーク管理ツールの活用

内部、外部のネットワークを正確に効率的に管理するためにネットワーク管理ツールを活用する。導入に当たっては、自組織のネットワーク構成、運用形態、操作性等を考慮する必要がある。

(9) その他

① ネットワークのコスト管理のポイント

a. 通信料金や機器保守費用等、ネットワーク運用に係るコストを把握していること。

b. ネットワーク運用管理に係るコストの負担方法、コスト配賦を明確に定めていること。

c．ネットワークの効率的な稼動のために、キャリア会社が提供する新しいネットワークサービスを評価していること。

d．複数キャリア会社のサービス及びコストを比較していること。

② ネットワーク機器の定期保守のポイント

a．定期保守の対象機器、実施方法、実施頻度、実施者を明確に定めていること。

b．ネットワーク機器の保守は、セキュリティが確保された状態で行うことを定めていること。

c．定期保守の実施後は、結果をとりまとめ記録して評価し、保守頻度や保守項目の見直し、リプレイス等を検討すること。

d．ネットワーク管理の責任者は保守結果の評価結果について承認していること。

8．ネットワーク管理

(2) ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。

1 主　旨

ネットワークへの侵入及び不正利用を未然に防止し、早期に発見するため、ネットワークへのアクセスコントロール及びモニタリングが有効に機能していることを確認する必要がある。

2 着眼点

(1) ネットワークをセグメントに分割してアクセスコントロールを行っていること。

(2) アクセスコントロールの方法を検討し、選択していること。

(3) アクセスコントロールの有効性を確認していること。

(4) モニタリングの方法を検討し、選択していること。

(5) モニタリングによる不正アクセスの検出時のネットワーク管理責任者への通知を確実にしていること。

(6) モニタリング記録の分析結果に基づいて、必要な対策を講じていること。

(7) ネットワーク管理用のユーザ ID の管理を適切に行っていること。

(8) リモートアクセスサービスとそのユーザを適切に管理していること。

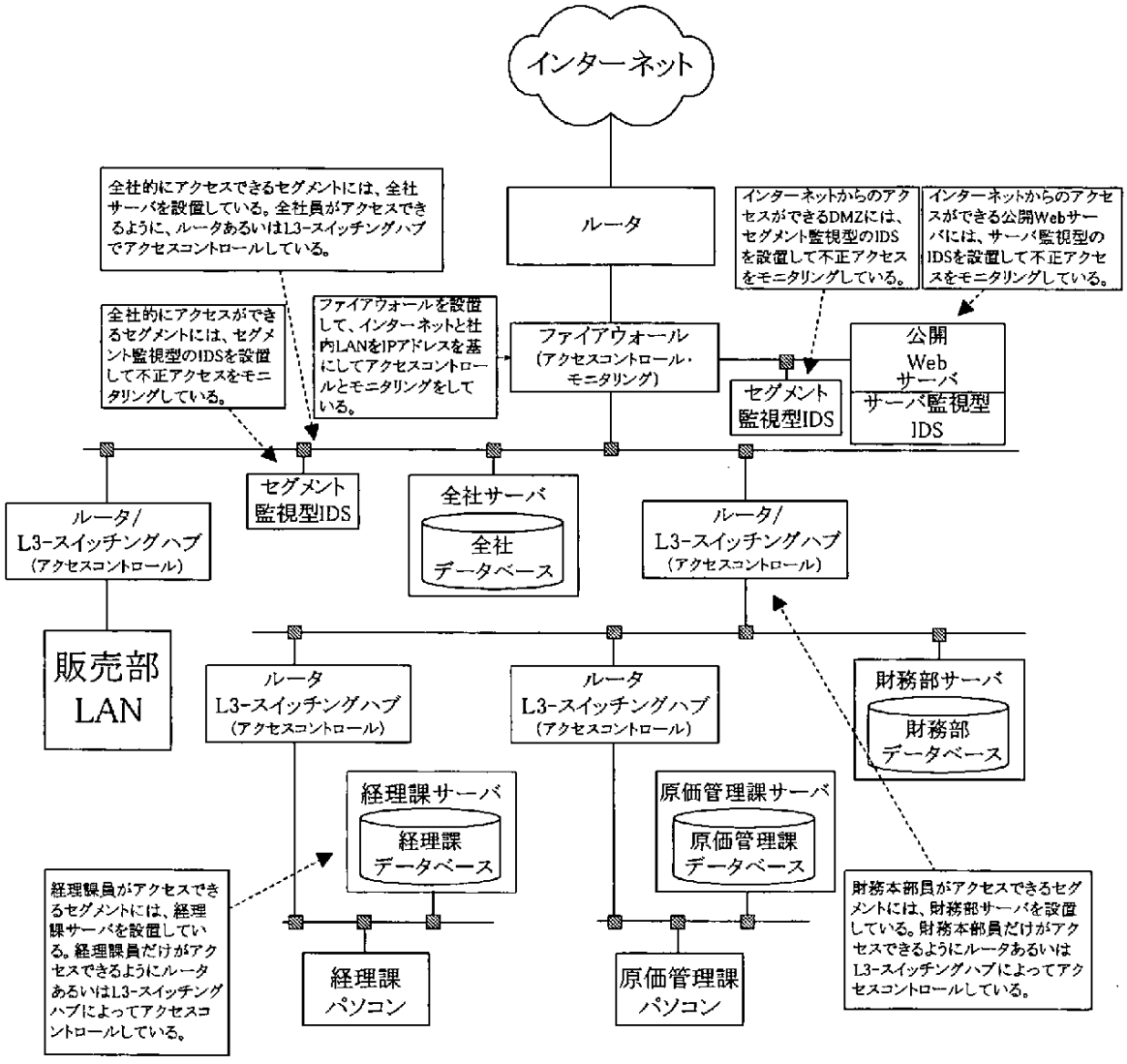
(9) 遠隔保守用のポートを適切に管理していること。

(10) ペネトレーション（侵入）テストを行い、ネットワークへのアクセスコントロール及びモニタリングが有効に機能していることを確認していること。

(11) 高いセキュリティレベルが要求されるネットワーク環境では、ネットワークの利用状況を常に収集して監視し、異常が発生した場合の原因究明手続を明確にしていること。

3 関連事項

(1) アクセスコントロール及びモニタリングの方法の例



ルータ、L3-スイッチングハブ、IDS、ファイアウォールを用いた アクセスコントロールとモニタリングの例

(2) ネットワークのセグメント化

① 組織構成、拠点、業務内容等を配慮したネットワークのアクセスコントロールの方針を明確にすること。

② ネットワークのアクセスコントロールの方針に基づいて、ネットワークをセグメントに分割して管理すること。

③ ネットワークのユーザが、共通でアクセスできるネットワークのセグメントとアクセスが制限されるネットワークのセグメントとを明確に定めていること。

(3) ネットワークのアクセスコントロール

① ファイアウォール、ルータ、スイッチングハブ等を配置して、ネットワークをセグメントに分割すること。

② 分割したセグメントに対して、ネットワーク上のパケットの IP アドレス、サービスの種類等を基にして、アクセスコントロールを行うこと。

③ ユーザの IP アドレス別にアクセスできる範囲を明確に決定していること。

④ ネットワーク管理の責任者は、ネットワークのセグメント化によるアクセスコントロールが機能していることを確実にすること。

⑤ 組織変更、組織の活動拠点の変更等によって、ネットワーク構成を変更する場合であっても、直ちにネットワークのアクセスコントロールを有効にすること。

(4) ネットワークのモニタリング

① 重要なネットワーク経路やセグメントについては、ファイアウォール、IDS（Intrusion Detection System：侵入検知システム）等を設置してモニタリングすること。

② ファイアウォール、IDS が侵入を検知したときは、直ちにネットワーク管理の責任者に通知する仕組みを確実にすること。

③ ネットワーク管理の責任者は、ファイアウォール、IDS が侵入を検知したときの対応手順について、関係者に周知徹底しておくこと。

④ ネットワーク管理の責任者は、ファイアウォール、IDS が侵入を検知した記録を文書化して、再発防止策を講ずること。

(5) ネットワーク管理用のユーザの ID 管理

① ネットワーク管理用のユーザ ID（ネットワークを管理する上で必要な ID）の付与は、ネットワーク管理の責任者が行っていること。

② ネットワーク管理用のユーザ ID とパスワードをグループ単位に付与しないこと。

③ やむを得ずネットワーク管理用のユーザ ID とパスワードをグループ単位に付与する場合は、補完的コントロールを設け、特に職務変更や離職時のコントロールを確実にすること。

④ ルータのコンフィグレーション情報を管理するためのユーザ ID を一元管理するソフトウェアツールの導入をネットワークの規模を配慮して検討すること。

(6) リモートアクセスサービスの管理

① ネットワーク管理の責任者が、ユーザからのリモートアクセスサービスの利用申請を承認すること。

② リモートアクセスサービスでは、次の設定を確実にすること。

a．複数の方法によって、ユーザ認証を行うこと。

b．コールバックを有効にすること。

c．ネットワーク管理の責任者によって承認された電話番号以外には、コールバックできない設定を有効にすること。

③ ネットワーク管理の責任者は、リモートアクセスサービスのユーザを定期的に見直すこと。

④ リモートアクセスサービスの利用履歴を、ユーザにフィードバックすること。

⑤ ネットワークに異常が発生したときは、リモートアクセスサービスを停止する手続が明確

であること。

⑥ リモートアクセスサービスのサービス時間帯を必要最小限にするように検討していること。

(7) 遠隔保守用のポートの管理

① 遠隔保守用ポートの管理の方針と手続が明確であること。

② 必要最小限の時間だけ、遠隔保守用ポートが有効になるような手続を定めていること。

(8) ペネトレーションテストによる、ネットワークへのアクセスコントロール及びモニタリングが有効に機能しているかの確認

① ペネトレーションテストの目的を明確にした上で、テストを定期的に行うこと。

② ペネトレーションテストの結果に基づいて、達成期日を明確に設定したアクションプランを定めること。

③ アクションプランの内容と結果について、ネットワーク管理の責任者が責任を負うことを明確に定めていること。

(9) ネットワークの利用状況の監視と異常が発生した場合の原因究明手続

① 高いセキュリティレベルが要求されるネットワーク環境では、ユーザの監視基準を定めて、異常なトラフィックの増加を監視する仕組みを有効にすること。

② 高いセキュリティレベルが要求されるネットワーク環境では、ユーザ端末による異常なトラフィックの増加を検知した場合の対応手続を明確に定めること。

8．ネットワーク管理

(3) ネットワーク監視ログを定期的に分析すること。

1 主　旨

ネットワークへの侵入及び不正利用を検出して必要な対策を講ずるために、ネットワーク監視ログを定期的に分析する必要がある。

2 着 眼 点

(1) ネットワーク監視を行うために、監視ログ分析の対象となるネットワーク機器を適切に識別していること。

(2) ネットワーク機器の監視ログの出力に関する設定を有効にしていること。

(3) 監視ログ分析作業の効率化に関する対策を検討し、選択していること。

(4) 監視ログへのアクセスコントロールを行っていること。

(5) 監視ログを適切に管理していること。

(6) 監視ログの分析結果についての対応を検討し、選択していること。

3 関連事項

(1) ログ分析の対象となるネットワーク機器の識別

① ネットワークへの脅威を識別した上で、ネットワーク監視ログの採取が必要最小限になるように検討していること。

② ネットワーク構成の変更に伴って、ネットワーク監視ログの採取の必要性について検討していること。

(2) ネットワーク機器のログの出力に関する設定の有効性

① ネットワーク機器のログの出力に関する設定に関して、アクセスコントロールを行っていること。

② ネットワーク管理の責任者は、必要なネットワーク監視を行うためのネットワーク機器のログに関する設定が適切であることを定期的にテストして、その結果を記録していること。

(3) 監視ログ分析作業の効率化に関する対策

① 効率的なログ分析のために、ネットワーク機器や各種サーバのシステム時刻を合わせる対策を講じていること。

② 監視ログ分析用のソフトウェアツールの利用を検討していること。その際、次の項目を検討すること。

ａ．効率的なログ分析を行うこと。

ｂ．監視ログの改ざんを発見するために、各ネットワーク機器が出力する監視ログ間の整合

性をチェックすること。

(4) 監視ログへのアクセスコントロール

① 侵入者や不正利用者によるログの改ざんに対するアクセスコントロールが有効であることを定期的にテストしていること。

② 監視ログへのアクセス履歴を採取すること。

(5) 監視ログの保管

① 監視ログの保存期間を定めること。

② 監視ログの記録媒体の保管についてセキュリティを確保すること。

③ 不正アクセス禁止法に対応できるように監視ログの保管方法を定めること。

(6) 監視ログの分析結果への対応

① ネットワーク管理の責任者は、監視ログの分析結果への対応手順を事前に定め関係者に周知徹底しておくこと。

② 監視ログの分析結果を基にして再発防止策を講ずること。

8．ネットワーク管理
(4) ネットワークは、障害対策を講じること。

1 主　旨

情報システム及び電子メールやWeb等の各種サービスの可用性を確保するため、ネットワークの障害対策を講ずる必要がある。

2 着眼点

(1) 重要なネットワーク機器や伝送路について、最長許容障害復旧時間を定めていること。

(2) 重要なネットワーク機器や伝送路について、最長許容障害復旧時間内に復旧するための措置を講じていること。

(3) 障害発生後、発生原因や対処等を記録した障害報告書を作成して、再発防止策を講じていること。

(4) ネットワーク障害の発生時の対応手順を制定していること。

(5) 必要に応じて、代替の伝送路を設定していること。

(6) ネットワークの可用性を評価して、ネットワークの障害対策を見直していること。

3 関連事項

(1) 重要な通信機器や伝送路への最長許容障害復旧時間の設定

① 業務の重要性に基づいて、関連する情報システム及び各種サービスに最長許容障害復旧時間を設定すること。

② 重要な情報システムや各種サービスに設定された最長許容障害復旧時間に基づいて、関連するネットワーク機器や伝送路に対して、最長許容障害復旧時間を定めること。

(2) ネットワーク機器や伝送路を最長許容障害復旧時間内に復旧するための措置

① 最長許容障害復旧時間が設定されたネットワーク機器や伝送路については、それを達成するための措置を講じていること。

② 伝送路については、次の項目について検討し、その結果をネットワーク設計に盛り込むこと。

a．ネットワーク障害によって不通となった経路に代わり、代替経路が自動的に選択されること。

b．ネットワーク障害によって不通となった経路に代わり、バックアップ回線が自動的に有効となり代替経路が有効になること。

③ ネットワーク機器については、次の項目について検討し、その結果をネットワーク設計やネットワーク機器の選定に盛り込むこと。

a．ネットワーク機器の冗長化を行い、ネットワーク機器の障害発生時には自動的に代替機器を作動させネットワークを復旧すること。

b．ネットワーク機器の代替機器を事前に確保しておき、ネットワーク障害の発生時に、代替機器を使ってネットワークを復旧すること。

c．保守契約を結び、障害発生時には保守業者による修理を行い、ネットワークを復旧すること。

(3) 障害報告書の作成と再発防止策

① ネットワーク障害が発生した場合には障害報告書を作成して関係者に回覧すること。

② 障害報告書にはシーケンス番号を付与して管理すること。

③ 障害報告書には、再発防止策を含むこと。

④ ネットワーク管理の責任者は、再発防止策が実施期限を設けた上で策定されていること、及び実施が期限内に完了していることに責任をもつこと。

(4) ネットワーク障害の発生時の対応手順

① ネットワーク管理の責任者は、ユーザを含めたネットワーク障害発生時の体制を明確にすること。

② ネットワーク管理の責任者は、ユーザからの障害報告の受付窓口を明確にすること。

③ ネットワーク管理の責任者は、ネットワーク障害発生時のユーザへの対処・復旧の通知の手順を制定し、ネットワーク管理者とユーザの双方に通達していること。

(5) ネットワークの可用性の評価と障害対策の見直し

① 情報システムや各種サービスの可用性に関する目標を達成する上で、ネットワークの可用性が必要十分であったかを評価すること。

② 情報システムや各種サービスの可用性に関する目標を達成するために、ネットワーク障害対策を講ずること。

8．ネットワーク管理

(5) ネットワークの利用状況を記録し、定期的に分析すること。

1 主　旨

ネットワークの効率的で安定した稼動を図るため、利用状況を記録し、定期的に分析する必要がある。

2 着眼点

(1) ネットワークの利用状況の収集、分析及び評価の手順等を明確にしていること。

(2) 分析結果に基づき、ネットワークの新設、変更等の改善措置を図っていること。

3 関連事項

(1) ネットワークの利用状況の収集、分析、評価

① 伝送路とネットワーク機器の利用状況を収集、分析、評価する手順を明確にしていること。

② 伝送路の使用率を採取し時系列に表示することによって、伝送路の利用状況の特性を把握する仕組みを有効にすること。

③ ネットワーク機器の負荷量を採取し時系列に表示することによって、ネットワーク機器の利用状況の特性を把握する仕組みを有効にすること。

④ 伝送路の変更については、伝送路の分析と評価において、新しい伝送路の確保のためのリードタイムを考慮していること。

(2) 定期的な分析及び評価の手順

① 使用率や負荷量の著しい変化があった場合、その原因分析を行うこと。

② ネットワークのボトルネックを改善するようにネットワークの評価を行うこと。

(3) 改善措置

① 伝送路の利用特性を考慮した上で、伝送容量の増減を行うこと。

② ネットワークの効率性や可用性を考慮した上で、ネットワークの分割・統合あるいは契約回線数を増減させること。

③ ネットワーク機器の負荷量を考慮した上で、ネットワーク機器のアップグレードを図ること。

8. ネットワーク管理

(6) ネットワークを利用したサービスについて、組織体としての方針を明確にすること。

1 主　旨

ネットワークを利用した情報提供等のサービスについて、組織体としての方針を明確にして、効率的にサービスを利用する必要がある。

2 着 眼 点

(1) 組織体として、ネットワークを利用した情報提供等のサービスの利用について、方針を明確にしていること。

(2) ネットワークを利用した情報提供等のサービスとそのサービスを提供する組織体を評価する手順を明確にしていること。

(3) 有料サービスの費用の支払手続を明確にしていること。

3 関連事項

(1) ネットワークを利用したサービスの利用方針

① サービスを提供する組織体から、ネットワークを利用したサービスについて説明を受ける。

② ネットワークを利用したサービスを受けるために付与されたユーザ ID とパスワードについての管理基準を明確にする。

③ ネットワーク管理の責任者は、ネットワークを利用したサービスの利用を評価して、不適切なサービスの利用を禁止する。

④ ネットワークを利用したサービスの利用を禁止できる機能をネットワークに設ける。

(2) ネットワークを利用したサービスの評価

① サービスとそのサービスを提供する組織体を評価する手順を明確にする。

② サービスの正確性や継続性について評価する。

③ サービス品目及び効率（コスト等）について評価する。

(3) 有料サービスの場合の費用の支払手続の明確化

① ネットワークを利用したサービスが有料の場合は、費用負担元、サービス利用の承認手続及びサービス利用の終了手続を明確にする。

9．構成管理

(1) 管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。

1 主　旨

ユーザ、ネットワーク管理の責任者、ベンダ間で、管理すべきソフトウェア、ハードウェア及びネットワークの二重管理の防止、及び管理の漏れが生じないように、管理の対象範囲を明確にして効率的に管理する必要がある。

2 着 眼 点

(1) 管理の対象を明確にしていること。
(2) 構成管理の責任者を定めていること。
(3) ソフトウェアのライセンス管理者を定めていること。

3 関連事項

(1) 管理対象の明確化
　① 情報システム及び電子メールや電子掲示板等の各種サービスを構成する以下の管理対象を明確に把握する。
　　a．ソフトウェア
　　b．ハードウェア
　　c．ネットワーク
　② ユーザ、ベンダー、キャリアとのネットワークの責任分界点を明確にして管理する。
　③ 管理台帳の項目と内容を整備し管理しやすくする。
　④ 現物と管理台帳との突合を行う。
(2) 構成管理の責任者の役割
　① 管理対象を効率的に管理するための構成管理の方針を制定する。
　② 構成管理の方針に基づいて構成管理の責任者を決める。
　③ ソフトウェア、ハードウェア等、管理対象をグルーピングして、グループごとに構成管理の手続を明確化する。
　④ 構成管理の手続には、情報システムを新規開発あるいは改変して運用するために必要な構成変更手続、ハードウェア構成やネットワーク構成の改変のために必要な構成変更手続を含む。
　⑤ 構成管理の責任者は、構成変更時の影響を検討して、要求されるセキュリティのレベル、性能、可用性等の劣化を予防する。

(3) ソフトウェアライセンスの管理者の役割

① ソフトウェアライセンスを一括購入してソフトウェア費用を削減する。

② ソフトウェアを記録しているCDやDVDの管理手続を定めて確実に管理する。

③ 正規のソフトウェアを使用し、違法コピー等を排除する。

④ 違法コピーのソフトウェアを使用していないことを確実にする。

9．構成管理

(2) ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。

1 主　旨

情報システムの機能維持及び障害時の早期回復を図るため、ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にする必要がある。

2 着 眼 点

(1) ソフトウェア、ハードウェア及びネットワークの管理台帳等を作成していること。

(2) 管理台帳を整備し、管理の信頼性の確保に役立たせていること。

3 関連事項

(1) ソフトウェア管理台帳

① ソフトウェアの利用に必要な管理項目を明確にして、ソフトウェア管理台帳の項目と管理手続を定める。

② ソフトウェアの利用に必要な管理項目の例は次のとおり。

a．ソフトウェアドキュメント管理者を定める。

b．使用中のソフトウェアとそのバージョンを明確にし、その利用に必要なドキュメントがすべて揃っていることを確認する。

c．ソフトウェアのライセンス契約条項を明確に把握する。

d．ソフトウェアのライセンス料をボリュームディスカウントによって削減する。

e．オープンソフトウェアの使用条件を満たす。

f．災害復旧時に必要なソフトウェアを明確にする。

g．情報セキュリティポリシーに基づく情報資産管理を行う。

③ ソフトウェア管理台帳の項目の例は次のとおり。

a．ソフトウェア名称、バージョン

b．開発元（連絡先等）、購入先、調達方法、調達費用、リース契約情報

c．保守状況、保証条件

d．管理者、管理方法、連絡先

e．使用状況、配布先、管理方法

f．ドキュメント（ユーザマニュアル、操作手順書、リリース管理情報等）

(2) ハードウェア管理台帳

① ハードウェアの利用に必要な管理項目を明確にして、ハードウェア管理台帳の項目と管理

手続を定める。

② ハードウェアの利用に必要な管理項目の例は次のとおり。

a．ハードウェア管理者を定める。

b．予算作成時に調達コストの支払先や支払額を確認する。

c．障害発生時の原因究明、障害対策、セキュリティ対策の際に、ファームウェアのバージョンを確認する。

d．定期保守計画の立案、見直し、リプレイス時期を決定する。

e．障害発生時の対応に必要な情報を提供する。

f．リースによって調達したハードウェアをリースバックする。

g．災害復旧時には業務の継続に必要なハードウェアを事前に確保する、あるいは迅速に調達する。

h．情報セキュリティポリシーに基づく情報資産管理を行う。

③ ハードウェア管理台帳の項目の例は次のとおり。(LAN 接続機器台帳の例)

a．機器名称、形式、製造元、機能性能緒元、ファームウェアのバージョン

b．管理番号、設置場所、管理責任者、連絡先

c．利用条件、保守状況、保守内容、保守条件

d．接続状況（ホスト名称、ノード情報、論理端末名称、IP アドレス等）

e．インストールソフトウェア、配布ソフトウェア情報（名称、購入先、バージョン等）

f．購入先、調達方法、調達コスト、リース契約情報

g．障害履歴、内容、対策、障害時連絡先等

h．ドキュメント（機器説明書、操作解説書、ユーザマニュアル等）

(3) ネットワーク管理台帳

① ネットワーク管理台帳はネットワーク構成図と連動して管理する。

② ネットワークの利用に必要な管理項目を明確にして、ネットワーク管理台帳の項目と管理手続を定める。

③ ネットワークの利用に必要な管理項目の例は次のとおり。

a．予算作成時にネットワーク費用の支払先や支払額を確認する。

b．ネットワークの構成変更時に構成要素の詳細を確認する。

c．ネットワークの障害対応時にネットワークの詳細情報を確認する。

d．情報セキュリティポリシーに基づいて情報資産管理を行う。

④ ネットワーク管理台帳の必要項目の例は次のとおり。

a．始点と終点の拠点名、ネットワーク種別、ネットワーク容量

b．キャリア会社名、契約条件、月額費用、DSU（Digital Service Unit：回線終端装置）契約種別

c．ネットワーク接続機器名、ホスト名、ネットワークアドレス

d．ケーブル敷設情報

e．管理責任者、障害時連絡先、監視方法

f．ネットワークの工事実施者

g．ドキュメント（障害時対応手順書、障害記録等運用記録）

(4) 管理台帳の更新

管理台帳は管理対象の変更を確実にとらえる仕組みとする。

9. 構成管理

(3) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。

1 主　旨

情報システムの停止、機能低下等を防止し、安定稼動を図るため、ソフトウェア、ハードウェア及びネットワークの導入及び変更は、影響を受ける範囲を検討して決定する必要がある。

2 着 眼 点

(1) 影響を受ける範囲を検討していること。

(2) ソフトウェア、ハードウェア及びネットワークの導入及び変更を構成管理の責任者が承認していること。

(3) 構成変更の作業中、作業後の問題発生の対処方法を確立する手続を定めていること。

3 関連事項

(1) 影響範囲の検討

① 管理対象の性能要件、信頼性要件、セキュリティ要件を明確にする。

② 管理対象の構成変更を行う場合、影響範囲の把握を行う。

③ 影響範囲の把握方法を次のとおり。

a. 変更要素の仕様による確認（マニュアル、ドキュメントの調査等）

b. 事例確認

c. メーカ、ベンダーの SE 等への確認

d. 実地テストの実施

(2) 構成管理の責任者による承認

① 性能要件、信頼性要件、セキュリティ要件を達成することを構成管理の責任者が検討する手順を構成変更手順に盛り込む。

② 構成変更の内容を構成管理者と運用管理の責任者が承認する。

(3) 構成変更時の障害対策

① 構成変更の作業中あるいは作業後に問題が発生した場合の対処方法を策定する手続を構成変更手順に盛り込む。

② 構成管理の責任者は、構成変更の内容を関係者に周知徹底する。

9．構成管理

(4) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。

1 主　旨

情報システムに与える影響を最小にするため、ソフトウェア、ハードウェア及びネットワークの導入及び変更を計画的に実施する必要がある。

2 着 眼 点

(1) ソフトウェア、ハードウェア及びネットワークの導入及び変更の計画を作成していること。

(2) 計画を運用管理の責任者が承認していること。

(3) ソフトウェア、ハードウェア及びネットワークの変更履歴を記録していること。

(4) 計画実施後に計画実施状況を評価して、評価結果を今後の計画の作成にフィードバックしていること。

3 関連事項

(1) 構成変更の計画の作成に当たっての考慮事項

① 十分な検討期間を確保する。

② 運用業務への負荷、構成変更時における障害発生の影響度、構成変更時に確保できる要員数、情報システムの特徴、費用等を基に移行方法と移行期間を検討し、適切な移行方法を選択して移行期間を確保する。

③ 構成変更の計画を関係者に周知徹底する。

④ 構成変更の計画の実施に当たって、必要なスキルを識別して要員への教育を実施する。

⑤ 構成変更の計画と全体計画との整合性を確保する。

(2) 構成管理の責任者が決定した構成要素の導入及び変更の内容に対して、運用管理の責任者が承認する。

(3) 変更履歴の管理

① 構成要素の変更履歴を管理する。

a．ソフトウェアの変更履歴管理

b．ハードウェアのリプレイス等の履歴管理

c．ハードウェアのファームウェアの変更履歴管理

d．ネットワークの変更履歴管理

② 構成変更に関するテスト結果を記録し保存する。

③ 退行テストを効率的に実施するためのテストデータを保存する。

(4) 構成変更によって、構成変更に至る課題や問題点が解消していることの確認

(5) 構成変更計画の評価と計画作成へのフィードバック

① 構成変更計画を評価する手順を定める。

② 評価の結果を今後の計画作成にフィードバックする手順を定める。

10. 建物・関連設備管理

(1) 建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。

1 主　旨

情報システムの停止、破壊等による被害を最小にするため、建物及び関連設備は、想定されるリスクを回避できる環境に設置する必要がある。

2 着眼点

(1) リスクをすべて想定していること。

(2) 自然災害の影響が最小になる場所に設置していること。

(3) 侵入を防止する設備を設置していること。

(4) 情報システムの設置場所を表示していないこと。

3 関連事項

(1) 想定されるリスク項目

① 自然災害（地震、火災等）による建物、関連設備の被害

建物及び関連設備の設置は、自然災害発生時を想定した構造にしていること。

② 建物への侵入

建物への侵入を防止する構造と、入退監視設備等による管理を適切に行っていること。

③ 関連設備、防災設備及び防犯設備が異常稼動

設備の管理は適切か、故障対策を実施しているか。

（ここでいう関連設備とは、電源設備、空気調和設備及び監視設備をいう）

(2) 入退館管理

コンピュータ室等が設置された建物を保有する場合、入退館管理を必要とする。

(3) 建物及び関連設備の管理状況の確認

① 建物及び関連設備の管理は、責任者を定め手続に従い実施していること。

② 建物は、コンピュータビルとしての目的を目立たせないこと。

③ 関連設備は、無権限者が接触しないように管理していること。

④ 問題が発見された場合、適切な解決を図っていること。

(4) コンピュータ設置場所の非表示

① 建物は、コンピュータビルであることを目立たせない（建物に看板を出さない等）。

② パンフレットや会社案内にコンピュータの設置状況を載せない。

③ 建物内でコンピュータフロアの表示をしない。

④ コンピュータ室（サーバ室、データエントリ室等）の表示をしない。

(5) 建物・関連設備のシステム監査の実施に当たっては、経済産業省の「情報セキュリティ管理基準」（関連資料 参照）及び「情報システム安全対策基準」（関連資料 参照）を参考にする。

10. 建物・関連設備管理

(2) 建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。

1 主　旨

情報システムを不正行為から保護するため、建物及び室の入退管理に不正防止及び機密保護の対策を講ずる必要がある。

2 着 眼 点

(1) 入退館、入退室にかかわるルールを明文化していること。

(2) 入退管理の責任者を定め、入退館、入退室の資格を明確にしていること。

(3) 検知した異常を責任者へ連絡する方法及び体制を確立していること。

(4) 物品の持込み及び持出しを監視していること。

(5) 入退管理の責任者は、入退管理の状況を把握していること。

3 関連事項

(1) 入退管理ルール

入退管理及び機密保護のための方針を定め、その具体的な実現ルールを定める。

入退館、入退室のルールは、資格者の対象範囲が異なる場合、別々に作成するケースが多い。

① 入退館及び入退室の管理責任者を設置すること。

② 入館又は入室資格を明確にすること。

③ 入退資格を識別できる仕組みを確立すること。

④ 重要情報資産のある室等、必要に応じて、建物の一部分を立入り制限区域とし、別途立入り資格を設定すること。

⑤ 物品、資料の持込み・持出しについて、監視設備、管理ルールを定めること。

(2) 資格の識別

入館及び入室資格者に識別証等を発行し、資格者による入館及び入室であることを確認するとともに、定期的に識別証等の発行状況を点検することによって、資格の付与状況が適切であるかを確認する必要がある。

(3) 不正防止及び機密保護対策の例

① 入館、入室の入口の限定と通過時の識別証の確認

② 識別証の常時着用、識別証と入館証の兼用化

③ 立入りエリアの限定、立入り制限区域の設定

④ 来訪者には同行者立会人を付ける

⑤ 監視装置の設置（コンピュータ室、立入り制限区域等）

⑥ 電子錠と入退記録の設備の設置

⑦ 自動化による無人化

⑧ 入退室における設備的対策の実施（パラレルロックドア、アンチパスバック方式の採用等）

(4) 入退館、入退室の監視と管理状況の例

① 無資格者の建物及び室への出入り禁止

② 来訪者の入館及び入室についての記録取得

③ 資格付与者に対する識別証の着用

④ 入退館時に必要な場合の携帯品チェックの実施

⑤ 業務上、直接関係のない者への資格付与の禁止

(5) その他、

建物・関連設備への入館及び入室の管理に当たっては、経済産業省の「情報セキュリティ管理基準」（関連資料 参照）及び「情報システム安全対策基準」（関連資料 参照）を参考にする。

10. 建物・関連設備管理

(3) 関連設備は、適切な運用を行うこと。

1 主　旨

関連設備は、管理・運用を行う上でのルールを定め、遵守することによって、継続的・安定的に運用する必要がある。

2 着眼点

(1) 関連設備を運用するためのルールを定めていること。

(2) 関連設備管理の責任者を定めていること。

(3) 関連設備について、運用担当者は、運用ルールを遵守し運用していること。

(4) 関連設備管理の管理者は、運用の状況を把握していること。

3 関連事項

(1) 関連設備の管理・運用ルールの項目の例

① 管理対象となる関連設備の一覧

② 関連設備の責任者、担当者の設定

③ 関連設備に関する作業範囲の確定

④ 関連設備の保守及び障害対応に関する手順

⑤ 関連設備の消耗品交換周期の明確化

⑥ 関連設備の保守に対する方針の決定（定期保守契約、スポット保守）

(2) 関連設備の運用状況把握上の留意点

① 関連設備は想定どおりの稼動を行っているか。

② 保守は契約どおりに実施しているか。

③ 障害発生時の対応は適切で有効に機能しているか。

④ 設備の老朽化、機能の不備、構造上の問題等、根本的な問題が発生していないか。

10. 建物・関連設備管理

(4) 関連設備は、定期的に保守を行うこと。

1 主　旨

関連設備の障害による情報システムの停止、機能低下等を未然に防止するため、定期的に保守する必要がある。

2 着 眼 点

(1) 保守の内容及び点検項目を明確にしていること。

(2) 保守を定期的に行っていること。

(3) 保守結果を記録し、責任者が承認していること。

(4) 保守結果及び障害の原因に基づき、改善措置を講じていること。

3 関連事項

(1) 保守（定期保守及び臨時保守）実施に当たっての留意事項

① 点検結果によって、必要に応じて定期保守のほかに臨時保守を行っているか。

② 臨時保守は、過去に比較して頻度が多すぎないか。

③ 保守結果を関連設備改修計画に反映させているか。

(2) 保守記録

保守には、定期保守及び臨時保守がある。これに加えて日常の点検が大切である。

定期（臨時）保守の記録項目の例

① 保守担当者

② 期日

③ 点検項目

④ 点検結果

⑤ 処置内容

⑥ 特記事項

(3) 関連設備の保守の監査に当たっては、経済産業省の「情報セキュリティ管理基準」（関連資料 参照）及び「情報システム安全対策基準」（関連資料 参照）を参考にする。

10. 建物・関連設備管理

(5) 関連設備は、障害対策を講じること。

1 主　旨

関連設備の障害を未然に防止し、あるいは早期に回復させるため、障害対策を講ずる必要がある。

2 着眼点

(1) 関連設備の稼動状況を監視していること。

(2) 瞬断及び停電対策を講じていること。

(3) 空気調和設備の能力に余力を持っていること。

(4) 監視設備は、検知状況を記録し、異常を警報する機能を有していること。

3 関連事項

(1) 関連設備の稼動監視項目の例

温度、湿度、漏水、地震、煙、雷、電圧、電流、入退室管理、出入り口

(2) 電気の瞬断、停電（電源設備）の対策の例

① 無停電電源設備の設置（CVCF、UPS 等）

② 外部電源の２系統化

③ 自家発電設備の設置

④ CVCF 蓄電池の大容量化

⑤ 自家発電及び外部電源の常時併用

(3) 空気調和設備の能力余裕

① 冷房能力の余裕設定

② 予備機の設置（水冷式空気調和設備と空冷式空気調和設備の併用等を含む）

③ 配管設備の漏水対策、耐震対策

(4) 障害対策（バックアップ）

① 障害対策の例

a．障害網の整備（社内運用部門、ユーザ、メーカへの連絡、社内報告網）

b．障害発生時の回復のための手順の明確化

c．障害発生時の回復体制の確立と、資材等の手配手順の確立

② 障害内容と記録

a．障害内容を記録すること（履歴）。

b．障害内容に応じた対策を講ずること。

③ 障害発生時のためのバックアップ措置の例

a．バックアップ体制の確立

b．バックアップ手順書（障害発生時の回復手順、体制等の対策マニュアルの整備）

c．バックアップ訓練の実施（定期的教育及び訓練の実施）

d．バックアップ訓練実施による回復許容時間の達成確認

（設備の障害発生時の措置と対策実施体制を整備し、障害回復方法を文書化し、有効に機能して回復許容時間内に復旧することをテストによって確認する）

(5) 建物・関連設備の障害のシステム監査の実施に当たっては、経済産業省の「情報セキュリティ管理基準」（関連資料 参照）及び「情報システム安全対策基準」（関連資料 参照）を参考にする。

10. 建物・関連設備管理

(6) 建物及び室への入退の管理を記録し、定期的に分析すること。

1 主　旨

建物及び室に関する入退管理の要件として、事故発生時に入館及び入室者を特定し、追跡調査を可能とする必要がある。そのため、入館及び入室の状況を記録するとともに、入退管理の責任者が定期的に分析する必要がある。

2 着 眼 点

(1) 建物及び室への入館及び入室の状況を記録していること。

(2) 入館（室）者を特定するとともに、事故発生時にトレース可能にしていること。

(3) 建物及び室の入退管理の責任者は、入退の記録を定期的に分析していること。

3 関連事項

(1) 建物及び室への入退状況の記録

入退館及び入退室の記録取得の趣旨は、必ずしも ID カードの機械設備による記録取得でなくてもよい。

(2) 建物及び室への入館及び入室の状況記録の例

① 来訪者記録

② 出張者記録

③ 開錠者・施錠者記録簿　等

(3) 入館及び入室状況の定期的分析の例

① 非権限者による入退館（室）試行記録

② 長期間入退館（室）のない権限者の記録　等

V. 保守業務

1．保守手順
2．保守計画
3．保守の実施
4．保守の確認
5．移行
6．情報システムの廃棄

1．保守手順

(1) 保守ルール及び保守手順は、保守の責任者が承認すること。

1 主　旨

保守業務の標準化を図り、円滑かつ信頼性を確保して保守業務を実施するため、保守ルール及び保守手順を定め、保守の責任者が承認する必要がある。

2 着眼点

(1) 保守のルールを定め、明文化していること。

(2) 保守の実施決定プロセス、保守業務実施のプロセスを手順としてルール化していること。

(3) 保守ルール及び保守手順を保守の責任者が承認していること。

(4) 保守ルール及び保守手順を関係者に周知徹底していること。

3 関連事項

(1) 保守のルール

① 保守のルールは、システム保守実施要領、システム保守実施基準等のように明文化すること。

② 保守のルールは、保守の実施決定プロセスも含め、ルール化すること。
（変更要求書の提出、変更作業量の検討、変更妥当性の検討と決定等）

(2) 保守のルールの例

① 保守の責任者：保守の責任者を明確にすること。

② 保守の発生理由：保守の発生理由を明確にすること。

a．ユーザの要望等による変更

b．関連法令、諸制度の変更に伴う変更

c．OS、DBMS 等のバージョンアップ対応による変更

d．内在する不整合対応による変更

③ 保守手順：変更依頼による保守の規模、期間、システム特性等を考慮して作業項目を決定すること。

④ 実施決定：保守の実施決定は保守業務管理会議において、目的、期間、効果、方法、作業量、影響範囲、優先順位等を総合的に判断して決定すること。

(3) 保守手順の例

① 保守計画

② 保守の実施

③ 保守の確認

④ 移行

⑤ 旧情報システムの廃棄

1．保守手順

(2) 保守手順は、保守の規模、期間、システムの特性等を考慮して決定すること。

1 主　旨

保守業務を効率よく実施するため、保守のルールに基づいて、保守の規模、期間、システム特性等から保守手順を決定する必要がある。

2 着眼点

(1) 保守手順は保守のルールに従っていること。

(2) 保守の規模、期間、システム特性等を確認し、決定していること。

3 関連事項

(1) 保守の規模

保守の規模を修正作業量、テスト回数、関連プログラム数等で把握する必要がある。

(2) システム特性

365日24時間運用等の稼動時間や対象ユーザ数等も重要なシステム特性のポイントとなる。

① バッチシステム、オンラインシステム、メインフレームシステム、サーバシステム

② 生命、財産、プライバシーにかかわる情報システム

③ 大量のトランザクションを処理する情報システム

1．保守手順

(3) 保守時のリスクを評価し、必要な対応策を講じること。

1 主　旨

保守の実施によって、システム障害等の各種トラブルを発生させないため、想定されるリスクを洗い出し、評価した上で必要な対応策を講ずる必要がある。

2 着眼点

(1) 保守業務の実施に当たっては、想定されるリスクを洗い出し、評価していること。

(2) 想定されるリスクに対し、必要な対策を講じていること。

3 関連事項

(1) リスクを洗い出すに当たってのポイント

① 保守計画の妥当性評価の考慮

② 保守体制への考慮

③ トラブルが及ぼす影響範囲への考慮

④ 処理タイミングへの考慮

⑤ 影響を与えるシステム、影響を受けるシステムへの考慮

(2) 想定リスクと対策の例

① スケジュール遅延が及ぼす影響への考慮

（プロジェクト管理、進捗管理の強化、要員増強、本番稼動の延期等）

② レスポンス等性能低下の観点

（仕様変更、運用方法の検討、機器性能アップ検討等）

③ 初期トラブル、バグ頻発

（テストの強化、品質管理、連絡体制の整備、バックアップ強化等）

2．保守計画

(1) 保守計画はユーザ及び保守の責任者が承認すること。

1 主　旨

保守の範囲及び作業内容を明確にするため、調査及び分析結果に基づいて保守計画を策定し、ユーザ及び保守の責任者が承認する必要がある。

2 着眼点

(1) 保守計画は、必要な内容を記載していること。

(2) 保守計画をユーザ、運用及び保守の責任者が承認していること。

3 関連事項

(1) 保守計画の内容の例

① 目的

② 保守の範囲と期間

③ 調査・分析結果
関連情報システムへの影響範囲

④ 保守内容

⑤ テスト内容

⑥ 移行内容

⑦ 作業体制

⑧ 保守日程計画

(2) 責任者の承認

ユーザ及び保守の責任者の承認が必要であるが、段階的な開発の場合には、運用の責任者の承認も必要となる。

2．保守計画

(2) 変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。

1 主　旨

変更依頼等の内容を正確に把握し、保守作業を円滑に行うため、保守の内容及び影響範囲を調査し、分析を行う必要がある。

2 着眼点

(1) 保守のルールに基づいて、変更依頼等を作成していること。

(2) 保守対象ドキュメント、プログラム、データ等の分析結果を記録していること。

(3) 変更依頼等をユーザ及び保守の責任者が承認していること。

3 関連事項

(1) 変更依頼等の例

① 保守の区分（変更依頼、修正依頼等）

② 依頼年月日

③ 依頼部門、依頼者

④ 理由

⑤ 内容

⑥ 処理希望年月日　等

(2) 保守作業が影響する範囲

① 関連する情報システム

② プログラム

③ データ

④ 利用者（社内利用者、外部接続先等）

2．保守計画

(3) 保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。

1 主　旨

保守のテストを円滑に実施するため、目的、範囲、方法、スケジュール等を設定したテスト計画を作成する必要がある。

2 着 眼 点

(1) 開発業務から引き継いだテスト環境の利用を考慮していること。

(2) テスト計画をユーザ、運用及び保守の責任者が承認していること。

3 関連事項

(1) 保守テスト計画の内容の例

① 目的
② 範囲
③ 方法
④ スケジュール
⑤ 担当者
⑥ 必要な環境
⑦ テスト項目・内容
⑧ テストの終了条件　等

3．保守の実施

(1) システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。

1 主　旨

誤びゅう、不正、機能の欠落等を防止・低減するため、保守計画に基づいてシステム設計書、プログラム設計書等を変更し、ユーザ及び保守の責任者が承認する必要がある。

2 着 眼 点

(1) 保守計画に基づいて、システム設計書、プログラム設計書等の保守対象ドキュメントを変更していること。

(2) 保守対象ドキュメントの変更をユーザ及び保守の責任者が承認していること。

3 関連事項

(1) 保守業務に必要なドキュメント等の例

① 開発マニュアル
② システム設計書
③ プログラム設計書
④ ソースプログラム
⑤ テストデータとテスト結果
⑥ システム運用マニュアル　等

(2) 責任者の承認

ユーザ及び保守の責任者の承認が必要であるが、運用に係るドキュメントの変更については運用の責任者の承認も必要である。

３．保守の実施

(2) プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。

1 主　旨

プログラムの変更等の誤びゅう及び不正防止のため、保守手順に基づき、保守の責任者が承認する必要がある。

2 着 眼 点

(1) 保守手順に基づき、プログラムの変更を行っていること。

(2) プログラムの変更を保守の責任者が承認していること。

3 関連事項

(1) プログラムの変更手順

① 変更プログラムのプログラム設計書の確認（プログラム設計書の変更内容、変更者等）

② 変更プログラムの内容の確認（プログラムの変更内容、変更者等）

③ プログラムの変更に対する保守の責任者の承認

3．保守の実施

(3) 変更したプログラム設計書に基づいてプログラミングしていることを検証すること。

1 主　旨

プログラミング時の誤びゅうを防止するため、変更したプログラム設計書に基づいてプログラミングしていることを検証する必要がある。

2 着 眼 点

(1) 変更が必要となるプログラムを明確にしていること。

(2) 変更プログラム設計書を作成していること。

(3) 変更したプログラムの検証手順を明確にしていること。

(4) 変更したプログラム設計書に基づいてプログラミングしていること。

3 関連事項

(1) 検証手順の例

① 検証方法の選択

② プログラム設計書とコーディングの突合等

③ 検証結果の確認

4．保守の確認

(1) 変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。

1 主　旨

プログラムのテストを円滑かつ確実に実施するため、変更したプログラムは保守のテスト計画に基づいて行う必要がある。

2 着 眼 点

(1) 保守のテスト計画に基づいて変更したプログラムのテストを実行していること。

(2) 保守作業が変更依頼等の要求を満たしていることを確認していること。

3 関連事項

(1) 保守テスト計画の内容の例

① 目的
② 範囲
③ 方法
④ スケジュール
⑤ 担当者
⑥ 必要な環境
⑦ テスト項目・内容
⑧ テストの終了条件　等

(2) 変更依頼等の例

① 保守の区分（変更依頼、修正依頼等）
② 依頼年月日
③ 依頼部門、依頼者
④ 理由
⑤ 内容
⑥ 処理希望年月日　等

4．保守の確認

(2) 変更したプログラムは、影響範囲を考慮してテストを行うこと。

1 主　旨

情報システムの機能及び性能の低下をもたらさないため、変更したプログラムは、影響範囲を考慮してテストを行う必要がある。

2 着 眼 点

(1) 変更プログラムが影響を及ぼす範囲を把握し、関係するソフトウェアとの結合テストを実施していること。

(2) 変更した部分以外に影響を及ぼさないことを確認していること。

(3) テストマニュアルを保守の担当者に周知徹底していること。

3 関連事項

(1) 影響範囲を把握するための資料の例

① システム構成図、プログラム一覧、プログラムとデータの関連図、ジョブネット図等

② 全体システム稼動状況、全体システム稼動スケジュール等

(2) その他

本テストの対象は、小規模な保守を対象とする。変更プログラムの及ぼす影響範囲が大きい保守の場合は、開発段階と同程度のテストが必要となる。

4．保守の確認

(3) 変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。

1 主　旨

情報システムが変更依頼等の要求を満たしていることを確認するため、プログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施する必要がある。

2 着 眼 点

(1) テストは、業務に精通したユーザが参画していること。

(2) テストに参画するユーザは、テストの目的を十分に理解していること。

(3) テストは、ユーザマニュアルに基づいて実施していること。

3 関連事項

(1) ユーザの参画

「Ⅲ．開発業務　5. システムテスト・ユーザ受入れテスト(9)」、「Ⅲ．開発業務　5. システムテスト・ユーザ受入れテスト(10)」を参照。

4．保守の確認

(4) 変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。

1 主　旨

テストの妥当性を確認し、情報システムの機能及び性能を確認するため、テストの結果をユーザ、運用及び保守の責任者が承認する必要がある。

2 着 眼 点

(1) テストの結果を検証していること。

(2) ユーザ、運用及び保守の責任者が承認していること。

3 関連事項

(1) テスト結果の内容の例

① テスト担当者

② 立会いユーザ担当者

③ テスト項目

④ テスト日時

⑤ テスト結果

⑥ 評価結果

⑦ 機能及び性能

(2) ユーザ、運用及び保守の責任者の承認

テスト結果の妥当性を承認することによって、変更プログラムの移行段階へと進むことになる。なお、段階的な稼動の場合、特に、本番稼動後の情報システムの変更については、開発の責任者の承認が必要な場合がある。

4．保守の確認
(5) 変更したプログラムのテストの結果を記録及び保管すること。

1 主　旨

テストの妥当性を確認し、障害等のトラブルの原因究明の基礎データとするため、テストデータ及びテスト結果を記録し、保管する必要がある。

2 着 眼 点

(1) テストデータ及びテスト結果の保管期間を定めていること。

(2) テスト時の環境を保管していること。

(3) 保管責任者を定めていること。

3 関連事項

(1) テスト結果の保管期間の例

① テストデータ……システムの安定稼動まで

② テスト結果……システムの更新時まで

(2) システムテスト時の環境

ソフトウェア、データベース、テストツール等は外部媒体に保存しておく。また、ハードウェア環境及びネットワーク環境について、完全保管ができない場合は、障害発生時にすぐに再現テストができるように、旧テスト環境を構築できる配慮が必要となる。

① テスト環境保管の例

a．テスト用ソフトウェア、ハードウェア、ネットワーク

b．テスト用データベース、各種マスタ

c．テストツール　等

5．移行

(1) 移行手順は、移行の条件を考慮して作成すること。

1 主　旨

移行を正確かつ円滑に行うため、期間、方法、体制等の条件を明確にし、移行手順を作成する必要がある。

2 着眼点

(1) 移行に当たっては、期間、方法、体制等の移行の条件を明確にしていること。

(2) 移行の条件を踏まえた移行手順を移行手順書としてまとめていること。

(3) 移行手順書は、ユーザ、運用及び保守の責任者が承認していること。

3 関連事項

(1) 移行に関する条件

① ユーザの条件

a．移行対象

b．移行期間、移行時期

c．移行後の確認方法

d．バックアッププログラム及びデータの保管期間及び廃棄方法

② システム運用上の条件

a．移行時の体制

b．移行時のオペレーション上の制約（タイミング等）

c．移行ツール

(2) 移行手順書

① 目的

② 移行方法（一斉移行、段階移行等）

併行運用期間を設定することがある。

③ 体制

④ 対象

⑤ 環境

⑥ ツール

⑦ 復旧のポイント

⑧ 移行日程

5．移行

(2) 変更前のプログラム及びデータのバックアップを行うこと。

1 主　旨

移行のトラブルに備えるため、変更前のプログラム及びデータのバックアップを行う必要がある。

2 着 眼 点

(1) 変更前のプログラム及びデータのバックアップを行っていること。

(2) バックアップの保管期間を定めていること。

3 関連事項

(1) バックアップ用プログラム及びデータの保管期間

保管期間……システムの安定稼動まで

5．移行

(3) 運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。

1 主　旨

他の情報システムの機能及び性能低下等を防止するため、運用及び保守の責任者は、情報システムの移行が及ぼす影響を確認する必要がある。

2 着 眼 点

(1) 移行前と移行後の情報システムの機能及び性能を明確にしていること。

(2) 移行時のほかのシステムへの影響を運用及び保守の責任者が確認していること。

3 関連事項

(1) 移行が及ぼす影響

① 保守作業が影響する範囲

「Ⅴ．保守業務　2.保守計画(2)」を参照。

② 移行作業が影響する範囲

マシン運用に関連する問題　等

6．情報システムの廃棄

(1) 旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。

1 主　旨

旧情報システムの廃棄を円滑かつ確実に実施するため、リスクを考慮した廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄する必要がある。

2 着眼点

(1) 旧情報システムを廃棄するに当たって、リスクを評価すること。
(2) (1)で評価したリスクを踏まえ、廃棄計画を策定していること。
(3) 廃棄計画は、ユーザ、運用及び保守の責任者が承認していること。
(4) 廃棄計画及び廃棄作業はあらかじめ関係者に連絡していること。

3 関連事項

(1) リスクの評価

情報資産としての観点から、旧情報システムを廃棄する場合のリスクとして、例えば、個人情報、機密情報等の漏えいがある。

(2) 廃棄計画の内容

① 廃棄目的
② 廃棄対象
③ 廃棄時期
④ 廃棄費用
⑤ 廃棄方法

(3) 関係者

① ユーザ、運用及び保守の責任者
② エンドユーザ、運用担当者及び保守担当者

(4) その他

外部のデータセンターを利用している場合は、契約満了時を廃棄時とし、ユーザ及び該当する責任者の承認が必要となる。

6．情報システムの廃棄

(2) 旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。

1 主　旨

不正防止、機密保護及びプライバシー保護のため、廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定する必要がある。

2 着 眼 点

(1) 廃棄方法及び廃棄時期を明確にしていること。

(2) 廃棄方法は、情報システムの機密度や重要度を考慮していること。

3 関連事項

(1) 廃棄方法

「Ⅳ．運用業務　6. ソフトウェア管理(6)」を参照。

Ⅵ. 共 通 業 務

1．ドキュメント管理
2．進捗管理
3．品質管理
4．人的資源管理
5．委託・受託
6．変更管理
7．災害対策

1．ドキュメント管理

1．1　作成

(1) ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。

1 主　旨

ドキュメントの品質を確認し、組織体の共有物とするため、ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認する必要がある。

2 理論的根拠／実務的配慮

(1) ドキュメントを関係者がレビューしていること。

(2) ドキュメントの内容等をユーザ部門及び情報システム部門の責任者が承認していること。

(3) ドキュメントを作成計画に基づいて配布していること。

(4) ドキュメントの作成を関係者に周知徹底していること。

3 関連事項

(1) ドキュメントのレビュー部門の例

① ドキュメント作成部門

② ドキュメント利用部門（ユーザ部門、開発部門、運用部門等）

③ ドキュメント標準化推進部門

④ ドキュメント管理部門（必要に応じて）

⑤ 情報システム企画部門

(2) ドキュメントのレビュー方法

① ウォークスルー

② インスペクション

(3) ドキュメント作成時のレビュー項目

① 必要事項の記載

② 目的に対する妥当性

③ 記述要領の遵守状況

④ 利用者側での理解の状況

⑤ 保守への対応手順

⑥ 不要な記述事項の排除

(4) ドキュメントの内容等に対する承認時の留意事項

① 内容の妥当性

② 関係者による内容のレビュー状況

③ 利用部門の利便性、理解のしやすさ

④ 配布先、配布手順

⑤ ドキュメントの版管理

⑥ 旧ドキュメントの廃棄方法

(5) 周知徹底のための方法の例

① 説明会の開催

② 内容に対する問合せ窓口の設定

③ 社内電子掲示板への掲載

1．ドキュメント管理

1．1　作成

(2) ドキュメント作成ルールを定め、遵守すること。

1 主　旨

組織体として一貫したドキュメントを作成するため、体系、記述形式、記述内容等をルールとして定め、遵守する必要がある。

2 着眼点

(1) ドキュメント作成ルールを明文化し、組織体として承認していること。

(2) ドキュメント作成ルールを情報戦略に基づいて定めていること。

(3) ドキュメント作成ルールは、ドキュメントの作成者、利用者及び管理の関係者に周知徹底していること。

(4) ドキュメント作成ルールの遵守状況をドキュメントの作成、利用及び管理の責任者が確認していること。

(5) ドキュメントの作成ルールは、情報システムの開発方法、運用形態に応じて見直していること。

(6) ディジタルファイルとして作成する場合の機密性、完全性、可用性、見読可能性の確保対策を立てていること。

3 関連事項

(1) ドキュメント作成ルールの必要性

① 必要なドキュメントの明確化と不要なドキュメントの作成防止

② 情報システムの変更に伴い保守の対象とするドキュメントの明確化

③ ドキュメントの記述項目、記述レベル、表現方法の統一化

④ ドキュメントの利用規程とドキュメントの配布対象の明確化

⑤ ドキュメント作成ソフトウェアの統一化

⑥ ドキュメントの再利用性向上

(2) ドキュメント作成ルールの項目の例

① 作成対象

② 作成方法・手段

③ 作成範囲

④ 用途分類（企画用、開発用、保守用、操作支援用等）

⑤ 作成部門の設定

⑥ 保守部門の設定

⑦ 利用部門の設定
⑧ 記述要領
⑨ ドキュメント様式、テンプレート
⑩ 管理方法（保存方法、保存期間、保存媒体等）

(3) ドキュメント作成ルールの見直しのタイミング
① 開発方法の変更：従来の開発方法・手順の変更又は新たな開発方法の採用等
② ドキュメント形式の変更：操作ガイドのメニュー化等
③ ドキュメントの管理媒体の変更：紙媒体からディジタルデータへの変更等
④ システムの処理形態の変更：集中化から分散化、分散化から集中化への変更等
⑤ ドキュメント作成支援ツールの生産性向上：CASE（Computer-Aided Software Engineering：コンピュータ支援ソフトウェア工学）ツールの高機能化・低価格化等
⑥ ドキュメントフォーマットの変更：ドキュメント編集ソフトウェアの変更、旧システムからのコンバージョン　等

1．ドキュメント管理

1．1　作成

(3) ドキュメントの作成計画を策定すること。

1 主　旨

必要なドキュメントを確実に作成するため、ドキュメント作成計画を策定する必要がある。

2 着眼点

(1) ドキュメント作成ルールに基づいて、企画、開発、運用及び保守業務にかかわるすべてのドキュメントの作成計画を策定し、関係者が承認していること。

(2) 作成するドキュメントは、企画、開発、運用及び保守業務の作業手順と整合性を図っていること。

(3) ドキュメントの作成に要する要員、予算、期間等を開発計画に反映していること。

3 関連事項

(1) ドキュメント作成計画のポイント

① 個別の情報システムごとに策定する。

② 企画、開発、運用及び保守の各業務で必要となるドキュメントを対象とする。

③ 作成対象とするドキュメントは、ドキュメント作成ルールに基づいて定める。

(2) ドキュメントの作成計画立案時の留意点

① ドキュメントの作成開始可能時期と必要時期

② ドキュメント作成要員のスキルの明確化と要員の確保

③ ドキュメント作成時の環境整備（参考資料、機器環境等）

④ 作成ドキュメントのレビュー方針（レビュー方法、レビュー回数等）と検証体制

⑤ ドキュメントの配布基準、イントラネット等への掲示基準

⑥ 作成後の保守体制

(3) ドキュメントの作成計画の記載項目の例

① ドキュメント一覧

② 目的と概要

③ ドキュメントの記載項目

④ ドキュメントの作成方法

⑤ ドキュメントのレビュー時期と参画者

⑥ ドキュメント作成者

⑦ 利用者と配布先

⑧ 作成スケジュール

⑨ 保守の対応

1．ドキュメント管理

1．1　作成

(4) ドキュメントの種類、目的、作成方法等を明確にすること。

1 主　旨

ドキュメントの種類の過不足を防ぎ、使用目的に応じ効率よく作成するため、ドキュメントの種類、目的、作成方法等をドキュメントの作成計画で明確にする必要がある。

2 着眼点

(1) ドキュメントの種類、目的、作成方法等をドキュメント作成ルールに基づいて定めていること。
(2) 作成するドキュメントの種類、作成スケジュール等は、開発計画等と整合性を図っていること。
(3) ドキュメントの目的に対応した配布先、配布形態を明確にしていること。
(4) ドキュメントの作成方法は、情報システムの形態、費用、保守等を考慮していること。
(5) ドキュメントの作成方法は、再利用を考慮していること。
(6) ドキュメント作成ルールで作成が規定されているドキュメントが作成されない場合は、理由を明確にしていること。

3 関連事項

(1) ドキュメントの作成方法の例
　① 新規に作成（独自開発の情報システム）
　② 開発支援ツールの利用（独自開発で開発支援ツールを利用した情報システム）
　③ ドキュメント作成ツールによる自動生成（独自開発の情報システム）
　④ ドキュメントの購入、修正（ソフトウェア商品、流通ソフトウェア）
(2) 開発計画とドキュメント作成計画の整合性の視点の例
　① ドキュメントの種類
　② 作業工程のインプット、アウトプットとドキュメントの関係
　③ 開発方法とドキュメントの作成方法
　④ 作成スケジュール
　⑤ 作成要員のスキルと要員数
(3) ドキュメント作成ルールで作成が規定されているドキュメントを作成しない場合の例
　① 流通マニュアルの利用
　② 市販ソフトウェアに付随の「README」、「HELP 機能」の利用
　③ 開発支援ツールの出力の利用
　④ 外部からのドキュメントの購入

(4) ドキュメントの種類に関する参考

「共通フレーム 98 ソフトウェアを中心としたシステム開発および取引のための共通フレーム」(1998 年版) を参照。

1．ドキュメント管理

1．1　作成

(5) ドキュメントは、作成計画に基づいて作成すること。

1 主　旨

ドキュメントは、必要な内容を網羅し、必要な時期までに用意するために、作成計画に基づいて作成する必要がある。

2 着眼点

(1) 作成したドキュメントの種類、内容、作成時期等は作成計画と一致していること。

(2) ドキュメントの作成計画に基づいて、ドキュメントの作成状況を管理していること。

(3) 作成の遅延、中止、追加並びに内容が変更となったドキュメントを把握し、その理由を明確にしていること。

(4) 作成の遅延に対する対策を講じていること。

(5) ドキュメントの作成に要した要員、費用、期間等の実績を把握し、作成計画と対比して次の工程もしくは次の計画立案時に反映していること。

3 関連事項

(1) ドキュメントの作成状況を作成計画に対比して監査する際のポイントの例

① 計画された種類のドキュメントの作成状況

② ドキュメント作成ルールへの遵守状況

③ 作成の仮定でのレビュー実施状況とレビュー時の検討結果の反映状況

④ 作成が遅延しているドキュメントに対する対応状況

(2) ドキュメントが作成計画と乖離している場合の例

① 作成中止（原因例：他の代替手段での対応）

② 作成方法の変更（原因例：自動作成への変更）

③ スケジュールの遅延（原因例：開発作業の遅れ、人的資源の不足）

④ 記述の不統一（原因例：記述要領の理解不足、レビューの未実施）

⑤ 記述の重複（原因例：記述範囲の不統一）

1．ドキュメント管理

1．2　管理

(1) ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。

1 主　旨

変更したドキュメントの品質を確認し、組織体の共有物とするため、ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認する必要がある。

2 着 眼 点

(1) 変更したドキュメントを関係者がレビューしていること。
(2) ドキュメントの変更内容等をユーザ部門及び情報システム部門の責任者が承認していること。
(3) 変更したドキュメントをドキュメントの作成計画に基づいて配布していること。
(4) ドキュメントの変更を関係者に周知徹底していること。

3 関連事項

(1) ドキュメントの変更内容等の承認時の留意事項
　① 内容の妥当性
　② 関係者による内容のレビュー状況
　③ 利用部門の利便性、理解のしやすさ
　④ 配布先、配布方法
　⑤ 旧版の廃棄方法
(2) 関係者への周知徹底時の留意事項
　① 変更箇所、変更理由、影響範囲の説明
　② 変更期日、変更時刻の通知
　③ 関係者への漏れのない通知
　④ 旧版の廃棄方法
(3) ドキュメント変更時の関係者の例
　① 変更したドキュメントのレビュー時の関係者
　　a．標準化推進部門
　　b．ドキュメント作成部門
　　c．ドキュメント利用部門
　② 変更したドキュメントの周知徹底時の関係者
　　a．ドキュメント利用部門
　　b．ドキュメント管理部門
　　c．ドキュメント作成部門

1．ドキュメント管理

1．2　管理

(2) ドキュメント管理ルールを定め、遵守すること。

1 主　旨

情報システムの内容と整合したドキュメントを維持し、利用を円滑にするため、原本及び配布されたドキュメントの管理ルールを定め、遵守する必要がある。

2 着眼点

(1) ドキュメント管理ルールを明文化し、組織体として承認していること。

(2) ドキュメント管理ルールを情報戦略に基づいて定めていること。

(3) ドキュメント管理ルールをドキュメントの作成者、利用者及び管理の関係者に周知徹底していること。

(4) ドキュメント管理ルールの遵守状況をドキュメントの作成、利用及び管理の責任者が確認していること。

(5) ドキュメントの管理ルールは、情報システムの開発方法、運用形態に応じて見直していること。

(6) ディジタルファイルで管理する場合の機密性、完全性、可用性、見読可能性確保の対策を立てていること。

3 関連事項

(1) ドキュメント管理ルールの必要性

ドキュメントは自部門内で作成した文書のみならず、監査報告書や顧客からの受領文書等もあり、ドキュメント管理ルールを定め、明確に管理する必要がある。これらの文書類は厳格に保管されるだけでなく、要望に応じて利用できるようになっていなければならない。

① 原本性の確保（ルールに基づかない変更を防止する）

② 最新版の明確化（どれが最新版であるか容易に判断できる）、旧版の廃棄

③ 情報システムとして統一のとれたドキュメントの保守

④ 利便性（必要な時に、簡易な方法で、最新のドキュメントが参照できる）

⑤ 情報セキュリティの確保

⑥ 知識・情報の共有化

(2) ドキュメント管理ルールの項目の例

① 管理対象

② 管理方法

③ 管理範囲

④ 管理部門
⑤ 更新手順
⑥ 廃棄の判断と方法
⑦ 保管方法・保管期限
⑧ 保管媒体

(3) ドキュメント原本の管理における留意事項
① 原本の現物（紙、ディジタルデータ）の明確化
② 原本管理者の明確化（管理責任者の任命方法、役割の明確化を含む）
③ 原本の保管場所（紙の場合はキャビネット、ディジタルデータの場合はサーバ等）、施錠状況（キャビネットのかぎ、サーバへのアクセス権等）
④ 原本の帯出状況の管理（紙の場合のみ）
⑤ 原本のバックアップの外部保管（紙、ディジタルデータ）

1．ドキュメント管理

1．2　管理

(3) 情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。

1 主　旨

情報システムの内容と整合したドキュメントを維持し、最新の状態を明確にするため、情報システムの変更時に関連ドキュメントの内容を更新し、更新履歴を記録する必要がある。

2 着眼点

(1) 情報システムの変更の影響を受けるドキュメントを明確にしていること（変更の種類とドキュメントの種類）。

(2) ドキュメントの更新を遅延なく行っていること。

(3) ドキュメントの更新は、ドキュメント管理ルールに基づいて行っていること。

(4) 作業内容を指定する位置付けにあるドキュメントは、その作業開始以前に更新されていること（例：プログラムの変更前に、当該変更を指示するプログラム設計書が変更されていること）。

(5) ドキュメントの更新作業の進捗状況を管理していること。

(6) 変更の理由、範囲等を記録し、更新履歴として管理していること。

3 関連事項

(1) ドキュメントの更新の理由の例

① 情報システムの変更（機能変更、瑕疵対応）

② ドキュメント内容の改善・充実（新規項目、内容の整理・統合・訂正）

③ 運用の変更（運用の効率化、業務変更、瑕疵対応）

④ ソフトウェアのレベルアップ（パッケージソフトウェア等のレベルアップ）

⑤ ドキュメント標準の変更への対応

(2) ドキュメントの更新手続の内容の例

① 変更手続の事務フロー

② 変更手続用文書書式

③ 変更管理方針の策定

④ 変更権限の規程

(3) ドキュメント更新時の留意事項

① 更新内容の完全性（改訂部分の抜けがないこと）

② 他のドキュメントとの連携（同期のとれた更新）

③ 更新内容の配布先（必要部門への漏れのない周知徹底）

④ 更新理由の告知（利用部門への説明）

⑤ 更新方法の明確化（全面取替え、差換え、自動更新、購入と配布（パッケージソフトウェアの場合））

⑥ 更新前内容の廃棄方法（機密保護）

(4) 更新履歴の項目の例

① 更新年月日

② バージョン情報

③ 更新内容の概要（更新理由）

④ 更新担当者

⑤ 承認者

⑥ 更新内容の配布日

⑦ 配布先

⑧ 配布手段・方法

⑨ 旧資料の廃棄方法

1．ドキュメント管理

1．2　管理

(4) ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。

1 主　旨

ドキュメントの不正利用、漏えい等を防止するため、ドキュメントの保管、複写及び不要ドキュメントの廃棄は、不正防止及び機密保護の対策を講ずる必要がある。

2 着 眼 点

(1) ドキュメントの保管、複写及び廃棄は、ドキュメントの形態及び重要度（機密度）に応じた不正防止及び機密保護の対策を講じていること。

(2) ドキュメントの管理者を定め、定期的に保管の状況を把握していること。

(3) ドキュメント管理ルールに基づいて、ドキュメントの利用状況を記録していること。

(4) 機密性の高いドキュメントの利用及び複写は、ドキュメント管理の責任者が承認していること。

(5) 機密性の高いドキュメントの廃棄は、溶解、裁断等で行い、ドキュメント管理の責任者が実施の状況を確認していること。

3 関連事項

(1) ドキュメントの保管時の留意事項

① ドキュメントの管理者を定めて管理する。

② 管理台帳を作成し、現在のドキュメントの状況を常時把握する。

③ 重要なドキュメント、機密性の高いドキュメントは、施錠できる場所に保管する。

④ 端末装置等のそばにおいて常時使用する操作解説書等には、機密事項を記載しない。

⑤ 重要なドキュメント、機密性の高いドキュメントの利用には、管理者の許可を得る。

(2) ドキュメントの複写における留意事項

① 機密性の高いドキュメントは、複写無効の特殊用紙等を用いて、複写ができないようにする。

② 不正利用の防止には、複写行為が明白となる用紙を用いる。

③ 複写禁止とするドキュメントの種類を明確にする。

④ ドキュメント上での複写禁止の表示のルールを定める。

⑤ 機密性の高いドキュメントを配布する際には、通し番号等をつける。

(3) ドキュメント廃棄時の留意事項

① 廃棄したドキュメントは、管理台帳等にその結果を記入する。

② 機密性の高いドキュメントの廃棄は、溶解、裁断等で行う。

③ 機密性の高いドキュメントの廃棄には、管理者等が立会い、廃棄状況を確認する。

④ 廃棄業者に委託する場合は、契約書に機密保持及び廃棄報告の事項を入れる。

(4) 重要なドキュメント、機密性の高いドキュメントをディジタルデータとして保管する場合の留意事項

① 保管場所（サーバ等）へのアクセスを制限するとともにアクセスのログを取り、定期的に検査する。

② ディジタルデータは暗号化する。

③ 印刷不可、内容のコピー・ペースト不可の形式で保管する。

④ ディジタル署名等による改ざん防止を行う。

2．進捗管理

2．1　実施

(1) 進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。

1 主　旨

企画、開発、運用及び保守業務を計画どおりに遂行するため、それぞれの特性に応じた進捗管理の方法、体制等を明確にし、責任者が承認する必要がある。

2 着 眼 点

(1) ユーザ、企画、開発、運用及び保守の進捗管理の責任者を明確にしていること。

(2) 進捗管理の責任者は、クリティカルパスを的確に識別して、進捗管理の方法、体制等を定めていること。

(3) ユーザ、企画、開発、運用及び保守の責任者による承認方法を明確にし、承認していること。

(4) 作業の実施に先立ち、関係者に対して、進捗管理の方法、体制等を周知徹底していること。

(5) 特に大規模な開発においては、EVM（Earned Value Management）法等を用いて投資に対する進捗度合いを管理すること。

3 関連事項

(1) クリティカルパスの識別状況を監査するに当たっての留意事項

① WBS（Work Breakdown Structure：作業分割構成図）は適切か。

② 作業項目の順序関係、作業工数見積りは妥当か。

③ クリティカルパスの決定には進捗管理の責任者が承認しているか。

④ プロジェクトの進捗に応じて変化するクリティカルパスを把握しているか。

⑤ 進捗管理の責任者は、業務の計画書等に基づいて、業務の全容を十分に把握しているか。

⑥ 進捗管理の責任者は、業務の特徴、業務の制約条件、想定されるリスク等を明確に把握しているか。

(2) 進捗管理の方法、体制として定める事項の例

① 管理項目と目標値

② 管理手法

③ 実績値収集の範囲、方法、頻度

④ 進捗報告の方法、対象者、頻度

⑤ 対策の立案方法、実施体制

⑥ 業務の工程終了時における作業実績の分析及び評価方法

⑦ 重点管理項目

(3) 開発業務における目標値の設定及び実績値収集の方法等の例

管理項目	目標値				実績値の収集		
	1週目	2週目	……	完了日	範囲	方法	頻度
システム設計書の作成本数	0本	3本	……	17本	Aサブシステム	システム設計レビュー報告書の提出	週次
プログラムのウォークスルーの消化率	7本	1.3本	……	52本	Bサブシステム	チームリーダーからの報告	日次
結合テストが完了したプログラム数	10本	15本	……	30本	Cサブシステム	結合テスト完了報告書の提出	週次

なお、目標値の設定に当たっては、実績値との差異の許容範囲をあらかじめ設定しておく必要がある。

(4) 開発業務における進捗報告の方法の例

名称	方法	対象者	頻度
チームミーティング	進捗会議の開催	チームメンバー全員	毎朝
進捗月次報告	進捗報告書の回覧	業務の責任者以上	毎月初日

(5) 外部委託の関係が複数階層にわたる場合には、見直した計画をすべての委託先に周知徹底する必要がある。

2．進捗管理

2．1　実施

(2) ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。

1 主　旨

問題点を早期に発見するため、ユーザ、企画、開発、運用及び保守の責任者は、作業の進捗状況を的確に把握する必要がある。

2 着眼点

(1) 進捗管理の責任者は、管理項目について目標値と実績値との差異を分析していること。

(2) 進捗報告は、あらかじめ定められた方法等に基づいて行っていること。

(3) ユーザ、企画、開発、運用及び保守の責任者は、進捗報告の内容の妥当性を確認していること。

(4) 作業完了の確認方法を明確にしていること。

(5) クリティカルパス上の作業の進捗状況は、重点的に把握すること。

(6) 進捗状況に応じてクリティカルパスの変化を認識すること。

3 関連事項

(1) 目標値と実績値との差異の分析状況を監査するに当たっての留意事項

　① 差異が許容範囲内のものであるか否かの判断を客観的に行っているか。

　② 潜在的な問題点の認識やその顕在化の可能性の判断を誤っていないか。

(2) 作業完了の確認方法の例

　① レビューミーティングの開催

　② 進捗報告会の開催

　③ 作業完了報告書の回覧

　④ プロジェクト統括責任者による決裁

　⑤ 成果物による確認

2．進捗管理

2．1　実施

(3) 進捗の遅延等の対策を講じること。

1 主　旨

企画、開発、運用及び保守業務を計画どおりに遂行するため、進捗の遅延等の対策を講ずる必要がある。

2 着眼点

(1) 進捗管理の責任者は、発見した問題点を関係者と直ちに協議してその原因を究明し、解決のための対策を作成していること。
(2) 進捗管理の責任者は、複数の対策案を評価し、最適な対策案を選択していること。
(3) ユーザ、企画、開発、運用及び保守の責任者は、対策を承認していること。
(4) 進捗管理の責任者は、対策の実施状況を管理していること。
(5) ユーザ、企画、開発、運用及び保守の責任者は、対策の実施結果を確認していること。
(6) 問題の発見から解決までの過程を記録していること。
(7) クリティカルパス上の作業進捗の遅延等の対策は、優先順位を上げること。

3 関連事項

(1) 対策を講ずるべき例として、作業環境や状況の変化に対応して、作業実績の把握方法等、進捗管理の方法自体を見直す場合も含まれる。
(2) 対策の立案状況を監査するに当たっての留意事項
　① 問題発生の本質的原因、発生した問題が全体の工程に与える影響度やその範囲、今後の推移状況等を的確に把握しているか。
　② 原因は、当該作業に固有のものか、又は他の作業でも発生する可能性があるかについて、客観的に評価しているか。
　③ 対策を実行することによって計画したスケジュールの中で残りの作業を完了することができるか否かについて、客観的に評価しているか。
　④ 対策を実行するために必要な要員や設備等を明確にしているか。
　⑤ 策定した対策について、関係者の合意を得ているか。
　⑥ 回復の見込めない大幅な遅延に対してはプロジェクトの打切りも代替案に挙げているか。
(3) 問題の発見からその解決までの過程を記録する目的
　① 企画、開発、運用及び保守の各業務の工程終了時に計画に対する実績を分析及び評価するため。

② 将来同様の問題が発生した際に、原因の究明、対策の立案、実施を効率的に行うため。
③ 進捗管理自体を評価するため。

2．進捗管理

2．2　評価

(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。

1 主　旨

次工程の計画の見直し及び進捗管理の方法等の改善、並行実施又は将来実施される同種の工程の計画へのフィードバックを図るため、企画、開発、運用及び保守業務の工程終了時に計画に対する作業実績を分析及び評価する必要がある。

2 着眼点

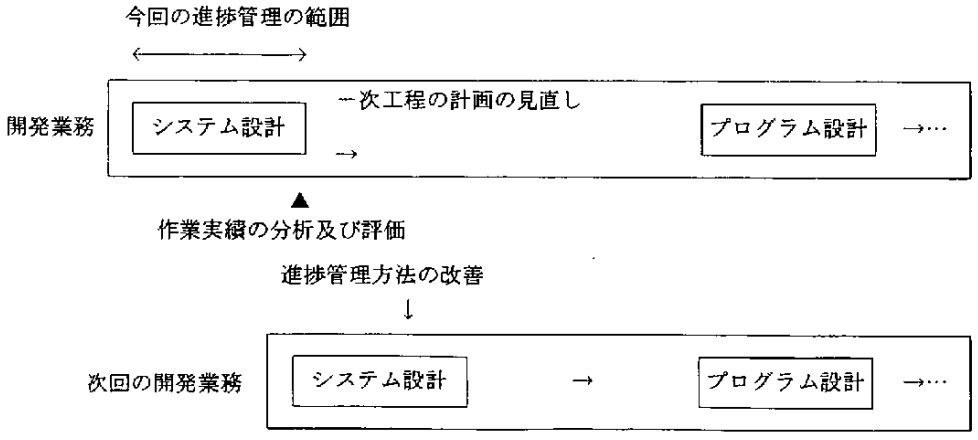
(1) 進捗管理の責任者は、目標値と実績値との差異を多面的に分析及び評価していること。

(2) 分析及び評価結果を記録し、ユーザ、企画、開発、運用及び保守の責任者が承認していること。

(3) 関係者に対して、分析及び評価結果を報告していること。

3 関連事項

企画、開発、運用及び保守業務の工程終了時に計画に対する作業実績を分析及び評価し、次工程の計画の見直し及び進捗管理の方法等の改善、並行実施又は将来実施される同種の工程の計画へのフィードバックを図ることの関係を開発業務の場合を例にあげ、図示すると次のとおりである。



(2) 分析及び評価すべき作業実績

① 業務の作業実績

a．計画に対する作業の遂行状況

b．納期に対する遅延状況

② 進捗管理の作業実施

a．実績値の収集状況

b．進捗報告の実施状況

(3) 開発業務における作業実施の分析の観点の例

① 作業の工程別、作業単位別、開発チーム別

② 要員の職種別、スキル別

③ 成果物の種類別、規模別、難易度別

(4) 目標値と実績値との差異の分析及び評価状況を監査するに当たっての留意事項

① 見積根拠及び目標値自体の妥当性を検証しているか。

② 差異の発生理由を要因別に分析及び評価しているか。

③ 実施した対策の効果を分析及び評価しているか。

2．進捗管理

2．2　評価

(2) 評価結果は、次工程の計画に反映すること。

1 主　旨

次工程の計画の実現可能性を高めるため、評価結果を次工程の計画に反映する必要がある。

2 着 眼 点

(1) 各工程の責任者は、前工程の評価結果を理解し、次工程の計画に与える影響を的確に把握していること。

(2) 企画、開発、運用及び保守業務の責任者は、見直した計画を承認していること。

(3) 見直した計画は、関係者に周知徹底していること。

3 関連事項

(1) 工程の責任者とは該当項目の計画の立案者である。なお、工程の責任者が前工程の責任者と同じ者の場合がある。

(2) 評価結果に基づいて、次工程の計画の見直しのために検討すべき課題の例

① 成果物の納期

② 作業生産性の指標

③ 要員の人選、チームの編成、委託先の選定

④ 作業を遂行するために必要な予算

(3) 外部委託の関係が複数階層にわたる場合には、見直した計画をすべての委託先に周知徹底する必要がある。

2．進捗管理

2．2　評価

(3) 評価結果は、進捗管理の方法、体制等の改善に反映すること。

1 主　旨

進捗管理の作業を効率的かつ効果的に遂行するため、評価結果を進捗管理の方法、体制等の改善に反映する必要がある。

2 着眼点

(1) 評価結果に基づいて、進捗管理の方法、体制等に関する問題点を明確にしていること。

(2) 問題点に対する改善策を作成し、有効性を検証していること。

(3) 進捗管理の方法、体制等の改善内容を組織体として承認していること。

(4) 評価結果は、当該プロジェクトに限らず、次プロジェクトに役立つように知識・ノウハウを蓄積すること。

3 関連事項

(1) 評価結果に基づいて、進捗管理の方法等の改善のために検討すべき課題の例

① 管理項目の設定方法

② 目標値の見積り方法

③ 実績値の把握方法、把握体制

④ 進捗状況の報告方法、報告体制

⑤ 対策の立案方法、実施体制

⑥ 業務の工程終了時における作業実績の分析及び評価方法

3．品質管理

3．1　計画

(1) 品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。

1 主　旨

情報システムのライフサイクルのすべてにおいて組織体の目標を達成するに足る品質を維持するための品質管理計画は、品質管理を円滑かつ効果的に行うために必要なものであり、ユーザ、企画、開発、運用及び保守の責任者が承認を行う必要がある。

2 着眼点

(1) 品質管理の責任者を定めていること。
(2) 品質管理計画を明文化し、ユーザ、企画、開発、運用及び保守の責任者が承認していること。
(3) 品質管理計画は、情報システムの企画、開発、移行、運用及び保守等の各プロセスと整合性がとられていること。
(4) 品質管理計画を結果の測定が可能な形態で作成していること。
(5) 品質管理計画は、全体最適化計画の中で策定される組織体の品質方針と整合性をとっていること。
(6) 品質管理計画を関係者に周知徹底していること。
(7) 品質管理計画を内外の環境変化に合わせて見直していること。

3 関連事項

(1) 全体最適化と品質管理計画

品質方針は全体最適化計画の中で策定される。品質方針は、組織体の全体的な最適化の方針と整合して策定され、品質目標の設定とレビューのための枠組みを与える（ISO9001. 2005.3 を参照)。品質管理は組織体がその目標を達成するための品質マネジメントシステム（PDCA サイクル）を構築することである。品質管理方針は、情報システムの構築から運用全般（システムライフサイクルの全般、保守も含まれる）に係る。

品質管理計画は品質方針に基づき、インフラストラクチャや各運用システムが構築から運用全般に至るまで、円滑かつ効率的に稼動できるよう具体的に定めた品質管理達成事項である。品質管理ルールと品質管理手順は品質管理方針及び品質管理計画に基づいて作成され、すべての関係者に周知徹底され、実行されるように教育・訓練されなければならない。

(2) 品質管理の責任者

ライフサイクル各段階での品質管理責任者を定めていること。

品質管理の最終責任者は、組織体の長であり、各業務プロセスの統括責任者である。品質管理責任者は品質を維持するためにライフサイクルの各段階で作業及び成果物の品質をレビューする。ただし、品質管理担当者は運用の責任者と同一である場合もあるが、品質のチェック機能を有効にするためには、実際の運用の責任者とは異なることが望ましい。品質管理責任者と品質管理担当者の役割と権限を明確に定義する必要がある。

(3) 品質管理計画を周知徹底すべき関係者

① 情報システム部員
② 各運用担当者
③ 保守責任者、担当者
④ 開発プロジェクトの責任者、担当者
⑤ コールセンターの責任者、担当者
⑥ 外注委託先の責任者、担当者
⑦ 品質管理担当者
⑧ 情報システムの利用者　等

(4) 品質管理の関連プロセスとの調整

品質管理はシステム開発のライフサイクル（企画・開発・検証・移行・運用・保守・見直し・廃棄等）のすべての工程で関連をもつ。また、品質の確認方法もプロセスの項目・状況によって異なる。したがって、品質管理計画・項目は各プロセスと調整を経た上で立案・実行する必要がある。

3．品質管理

3．1　計画

(2) 品質管理計画は、方法、体制等を明確にすること。

1 主　旨

品質管理計画は、組織体の品質管理マネジメントシステムを円滑に実施するために、その実施方法、体制、実施時期等を明確にする必要がある。品質管理計画は、全体最適化計画の中で定められた品質管理方針を具体化する。

2 着眼点

(1) 品質目標が達成されるように品質管理計画を作成していること。
(2) 各段階での管理が有効になるように必要な判断基準及び方法を明確にしていること。
(3) 各段階での管理の責任と権限を明確にしていること。
(4) 品質管理のプロセスを監視、測定、分析していること。
(5) 品質管理に必要な資源と情報を配分していること。

3 関連事項

(1) 品質管理計画の項目の例
　① 総則
　　a．目的
　　b．適用範囲
　　c．基本方針
　　d．品質管理体制
　　e．品質管理責任者
　　f．品質管理責任者の任務・権限
　　g．品質管理担当者
　　h．品質管理担当者の任務
　　i．機密保持
　　j．評価の基準
　　k．ルールの改廃及び周知徹底
　② 実施
　　a．実施スケジュール
　　b．実施場所
　　c．担当者

d．実施手順
e．実施の留意点
f．品質管理文書の作成

③ 報告

a．指摘する事項
b．リスク評価
c．改善点
d．改善の優先度
e．改善結果
f．次期以降の改善予定

(2) 品質管理の方法及び体制

情報システムの品質管理はドキュメント類（設計書類、記録類、ログ等）のレビュー、プログラムのデバッグ、検証（設計検証、コード検証、操作検証等）、妥当性確認、監査等を通して行われる。品質管理の体制は品質目標に従って、上記の要求を満たすような体制を構築して行わなければならない。

品質管理の方法、体制は、品質管理計画で明らかにされていなければならない。

(3) 品質管理の実施時期

品質管理はシステム開発のライフサイクル（企画・開発・検証・移行・運用・保守・見直し・廃棄等）のすべての工程で実施されるべきものであるため、それぞれの時点で責任者を定め、実施しなければならない。

プロジェクトリーダー若しくは運用管理責任者は、品質管理が適切に行われるよう資源を配分し、その実施に対して責任を負わなければならない。

3．品質管理計画

3．2　実施

(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。

1 主　旨

業務が計画どおりに実施され、品質管理目標を達成したかを評価するために、その実績を品質管理ルールに基づき、計画に対する実績を分析及び評価して、責任者が承認する必要がある。

2 着 眼 点

(1) 品質管理計画及び品質管理ルールを制定していること。
(2) 品質管理目標、評価の基準を明文化していること。
(3) 品質管理業務を実施していること。
(4) 品質管理記録を作成していること。

3 関連事項

(1) 品質管理の評価基準の例

① 開発の例

a．開発の進捗管理：計画の WBS に対する実績の進捗

b．開発仕様書の用件定義に対する適合度合い（設計検証・コード検証におけるエラー件数、実行時のバグ件数等）

c．ユーザの要求に対する適合度合い（トランザクション量、処理時間、レスポンスタイム等）

② 運用の例

以下の項目が運用上で予定されている処理時間やルールどおりの手順で実施されているか等が品質管理の目標と実績の比較、分析対象になる。運用については明確なサービスレベルの設定が品質管理上、必要である。

a．運用の責任と体制……責任者の設置の有無、責任と権限の規定、運用体制の明確化の有無等

b．運用手続……運用時間、処理依頼、ユーザ ID 取得等

c．ジョブスケジュール……操作手順、引継ぎ、オペレータの交替、例外処理、オペレーション実施記録等

d．オペレーション……連絡体制、交替手段、リカバリ、記録等

e．入力管理……入力データの作成及び取扱い、入力者、承認、変更等

f．データ管理……データ管理者、利用状況、複写、媒体管理、保管、廃棄等

g．出力管理……出力情報の取扱い、利用状況、引渡し方法、保管、廃棄等
h．パスワード及び識別コードの管理
i．ソフトウェア管理……アクセス管理、バックアップ、媒体管理、保管、廃棄等
j．ハードウェア管理……定期保守、バックアップ、利用状況、障害対策等
k．ネットワーク管理……利用状況、アクセスコントロール等
l．構成管理……管理対象、責任者、管理台帳、状況の把握、変更手続等
m．建物及び関連設備管理等

(2) 担当責任者の例

① 開発プロジェクト責任者
② ジョブスケジュール担当責任者
③ ハードウェア担当責任者（サーバ、基本 OS を含む）
④ ネットワーク担当責任者
⑤ クライアント担当責任者
⑥ 各アプリケーション別担当責任者
⑦ コールセンターの責任者、担当者
⑧ 外注委託先
⑨ 品質管理担当者
⑩ 情報システムの利用者　等

品質管理結果について、責任者の承認を得る時には、その内容への同意を得ることが重要である。記載された指摘事項、改善要求がある場合には、特にその事実についての確認が必要である。

(3) 品質管理の方法

① ドキュメント類のレビュー（品質目標との照合）
② 実行ログや監査証跡との照合（同上）
③ プログラムリスト類のトレースによる確認
④ プログラムの実行トラッキングによる確認
⑤ プログラムのデバッグによる確認
⑥ エラーの発生状況と品質目標との照合　等

3．品質管理計画

3．2　実施

(2) 評価結果は、品質管理の基準、方法、体制等の改善に反映すること。

1 主　旨

品質管理の評価結果は、組織体の品質管理目標を達成するための継続的な改善活動に役立てるため、品質管理の基準、方法、体制等の改善に反映する必要がある。

2 着 眼 点

(1) 改善は品質管理目標がよりよく達成されるように実施していること。
(2) 改善担当者の役割と責任を決めていること。
(3) 改善の担当責任者を決めていること。
(4) 改善の結果は品質管理責任者に報告していること。
(5) 品質管理の基準自体も見直していること。

3 関連事項

(1) 改善担当責任者の例

改善担当責任者が明確であることは、改善活動が実行性をもつために必要である。

① 開発プロジェクト責任者
② ジョブスケジュール担当責任者
③ ハードウェア担当責任者（サーバ、基本 OS を含む）
④ ネットワーク担当責任者
⑤ クライアント担当責任者
⑥ 各アプリケーション別担当責任者
⑦ コールセンターの責任者、担当者
⑧ 外注委託先
⑨ 品質管理担当者
⑩ 情報システムの利用者　等

(2) 評価結果の改善を反映する場

① 中期計画立案時に検討
② システム化委員会で検討
③ プロジェクト内で検討
④ 運用・保守の会議体で検討
⑤ 情報システム部門内での検討

⑥　委託の場合は委託先との会議体の中で検討　等

(3) 品質管理の基準・ルールの見直しの例

①　品質改善作業への対応

②　組織、制度等の変更への対応

③　技術進歩への対応

④　システム導入・改変への対応

⑤　基準適合、法規制変更への対応　等

4．人的資源管理

4．1　責任・権限

(1) 要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。

1 主　旨

企画、開発、運用及び保守業務を効率的に遂行し、誤びゅう及び不正を防止し、機密を保護するため、要員の責任及び権限を定める必要がある。

2 着 眼 点

(1) 企画、開発及び保守業務の遂行に必要な責任及び権限を明文化していること。

(2) 要員の責任及び権限の関係に矛盾がないこと。

(3) 要員の責任及び権限は、能力及び経験を反映していること。

(4) 責務の分離を明確にしていること。

3 関連事項

(1) 職務分析の実施

要員の責任と権限を定めるためには、職務分析が適切に行われていることが前提となる。

(2) 明文化の方法

要員の責任及び権限の明文化の例

① 職務記述書

② 組織図

③ 職務分担表

④ 要員配置表

(3) 責任と権限との整合性のチェックポイント

要員の責任と権限との間に矛盾がないかの確認に当たっての着眼点

① 要員間の整合性

② 個別要員に割り当てられた責任と権限との間の整合性

③ 部門間の整合性

④ 企業間の整合性

4．人的資源管理

4．1　責任・権限

(2) 要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。

1 主　旨

業務環境及び情報環境の変化に適応させるため、要員の責任及び権限は定期的又は適切なタイミングで見直す必要がある。

2 着 眼 点

(1) 見直しの範囲を明確にしていること。

(2) 見直しの判断基準を明確にしていること。

(3) 見直しの結果を組織体として承認していること。

(4) 見直しの手続を明確にしていること。

3 関連事項

(1) 業務環境の変化

具体的には次のような業務環境の変化によって、要員の責任及び権限の見直しが必要となる。

① 組織の統廃合

② 組織体の合併

③ 関連法令等の改正

④ 経営方針の変更

⑤ 外部委託

⑥ 要員又は組織の生産性向上

(2) 情報環境の変化

具体的には次のような情報環境の変化によって、要員の責任及び権限の見直しが必要となる。

① EUC の導入

② 分散システムから集中システムへ、集中システムから分散システムへ

③ 異組織間、異企業間のネットワーク接続

④ モバイル化

⑤ APS（Advanced Planning Scheduling）等の採用

(3) 見直しの範囲

① ユーザ部門と情報システム部門との間の責任及び権限の見直し

② 組織間の責任及び権限の明確化

③ 個人と組織との責任及び権限の分担

(4) 見直しの判断基準

組織体に次のような兆候が見られるようになってきたとき、要員の責任及び権限の見直しを検討する必要がある。

① 誰に責任及び権限があるのかが曖昧である業務の出現
② 現行の責任及び権限の枠組みでは管理できない業務の出現
③ 一部の要員への責任及び権限の集中
④ 指揮系統の上下関係が曖昧な責任及び権限の出現
⑤ 個別要員の責任及び権限の関係の矛盾
⑥ 要員の能力及び経験と責任及び権限のミスマッチ

4．人的資源管理

4．1　責任・権限

(3) 要員の責任及び権限を周知徹底すること。

1 主　旨

企画、開発、運用及び保守業務を効率的かつ確実に遂行し、要員相互の連携を図るため、責任及び権限を個々の要員に周知徹底する必要がある。

2 着 眼 点

(1) 周知徹底の方法を明確にしていること。

(2) 周知徹底の時期が適切であること。

(3) 個々の要員の理解を確認していること。

(4) 変更を関連する要員に連絡していること。

3 関連事項

(1) 周知徹底及び理解の確認の方法

① 職務記述書、組織図、職務分担表（あるいは職務分掌表）、要員配置表等による明文化

② 研修、セミナー等の開催

③ 定例会議

(2) 周知徹底の時期

要員の責任及び権限は、上記の方法によって日常的に周知徹底を図っておくことが必要であるが、次のような時期には特に周知徹底させる必要がある。

① 異動時

② 新規プロジェクト、新規事業の開始時

③ 組織体の大幅な方針の変更

④ 組織の再編成時

4．人的資源管理

4．2　業務遂行

(1) 要員は、権限を遵守すること。

1 主　旨

誤びゅう及び不正を防止し、企画、開発、運用及び保守業務を効率的かつ確実に遂行するため、要員は権限を遵守する必要がある。

2 着 眼 点

(1) 企画、開発、運用及び保守業務の責任者は、要員の職務遂行状況を把握していること。

(2) 要員間の相互牽制が機能していること。

(3) 作業報告書を作成していること。

3 関連事項

(1) 職務遂行状況の把握方法

要員の業務遂行状況は次の方法によって把握することができる。

① 作業週報、作業日報の作成

② 目標と実績との差異分析の実施

(2) 相互牽制方法

次の方法を積極的に導入することによって要員相互の牽制が可能となる。

① ジョブローテーションの実施

② 複数担当制

③ 作業日報記載の義務付け

④ ミーティングの導入

４．人的資源管理

４．２　業務遂行

(2) 作業分担及び作業量は、要員の知識、能力等から検討すること。

1 主　旨

企画、開発、運用及び保守業務を計画に基づき遂行し、目的とした成果物の品質を確保するため、作業分担及び作業量を要員の知識、能力等から検討する必要がある。

2 着 眼 点

(1) 要員の知識及び能力を反映して作業の割当てを行っていること。

(2) 企画、開発、運用及び保守業務の責任者は、要員の作業遂行能力を評価していること。

(3) 評価に基づき、作業分担及び作業量を見直していること。

3 関連事項

(1) 作業の特性

作業を要員に適切に配分するためには、まず、作業の特性が正しく把握されていなければならない。作業の特性を把握するポイントには次のものがある。

① 定型か非定型か（反復可能性）

② 複雑さ、専門性

③ 他の作業との関連性

④ 必要とされる熟練度

⑤ 肉体的、物理的要因

(2) 要員側の特性

作業を要員に適切に配分するには、個々の要員の知識及び能力も評価されなければならない。要員の知識及び能力を把握するポイントには次のものがある。

① 職種の定義、知識及び能力のレベルの定義（スキルスタンダード）

② 経験

③ 分析力、総合力

④ 協調性

⑤ モラル

⑥ コミュニケーション力　等

4．人的資源管理

4．2　業務遂行

(3) 要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。

1 主　旨

要員の交替に際しては、引継ぎミス等による誤びゅう発生の防止、担当を外れた要員による不正の防止、機密保護を考慮する必要がある。

2 着 眼 点

(1) 交替時の引継ぎルールを明確にしていること。

(2) アクセス資格を管理していること。

(3) 機密保護の方法を定めていること。

(4) 引継ぎ内容を文書で確認していること。

3 関連事項

(1) 要員交替の契機

要員の交替が発生するタイミングとしては、次のようなものが考えられる。これらに際して、誤びゅう、不正、機密漏えいが発生する余地がないか点検しておく必要がある。

① シフト勤務

② 異動・退職

③ 定期的又は不定期の休暇

④ アクシデント　等

(2) アクセスコントロール

要員交替における不正や機密漏えい対策としてアクセスコントロールを行う必要がある。

① パスワード、IDカード、生体認証等の本人認証の仕組みの導入

② コールバックシステムの導入

③ 要員ごとのデータアクセス制限

④ 引継ぎルールの制定

4．人的資源管理

4．2　業務遂行

(4) 不測の事態に備えた代替要員の確保を検討すること。

1 主　旨

企画、開発、運用及び保守業務の継続性を維持するため、不測の事態に備えた代替要員の確保を検討しておく必要がある。

2 着眼点

(1) 代替要員を必要とする作業を明確にしていること。

(2) 代替要員を確保するまでの臨時措置を検討していること。

(3) 交通経路、宿泊施設を検討していること。

3 関連事項

(1) 不測の事態発生の原因

① 事件・事故

② 病気・死亡

③ 災害・テロ

④ 突然の退職、解職

(2) 代替要員手配に当たっての緊要度の評価ポイント

① 当該業務の重要度

② 他の業務への影響度

③ 当該業務の難易度、必要とされる習熟度

(3) 臨時措置

不測の事態が発生し、代替要員を実際に確保するまでの間の対応措置を事前に考えておかなければならない。例えば次のような事項をあらかじめ決めておく必要がある。

① 業務の一時停止

② 業務の代替（システム化されていたものを手作業で行う）

③ 業務の縮小

④ 業務の中止

4. 人的資源管理

4. 3 教育・訓練

(1) 教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。

1 主　旨

組織体として一貫した教育及び訓練を行うため、人的資源管理の方針に基づいたカリキュラムを作成し、情報技術の進歩等に応じて見直す必要がある。

2 着 眼 点

(1) 教育及び訓練の方針を定めていること。
(2) 組織体の特性を考慮したスキルスタンダードを定めていること。
(3) 情報技術の多様性を反映し、キャリアパスに基づいてカリキュラムを作成していること。
(4) カリキュラムを組織体として承認していること。
(5) 情報技術の動向及び教育の実績を反映して、カリキュラムを見直していること。

3 関連事項

(1) 教育・訓練の方針

教育及び訓練のカリキュラムの作成及び見直しを行うに当たって、その基本方針は少なくとも次の3点との関連において表明されていなければならない。

① 経営戦略との関連性
② 組織戦略との関連性
③ 情報戦略との関連性

(2) 多様なスキルニーズへの対応

教育及び訓練のカリキュラムは、スキルに対する組織内の多様なニーズに対応できるものになっていなければならない。

① ユーザ部門及び情報システム部門それぞれのニーズに対応できること。
② 現在の技術動向のみならず、将来の技術動向をも見据えていること。
③ 組織の各階層のスキルニーズに応えられること。

(3) 情報技術要員の教育・研修分野

情報技術要員には様々なビジネス技能の習得が必要で、それぞれの技能分野で必要な育成を実施する必要がある。

a. システム技術（情報処理、言語、データベース、ネットワーク、セキュリティ等）
b. システムメソドロジー（コーディング技法、テスト技法、要件定義等）

c．業務知識・業務経験（財務会計、購買、営業、取引、生産、研究等）

d．ビジネススキル（状況分析、課題設定、問題解決、企画能力等）

e．ヒューマンスキル（コミュニケーション、リーダーシップ、プレゼンテーション能力等）

(4) IT要員の教育・研修方法

① 研修

a．集合研修（社内／社外）

b．電子的手段（eラーニング／CD-ROM等）

c．通信教育

d．講習会／コンファレンス

e．視察／見学ツアー　等

② メンタリング／コーチング

a．OJT（On the Job Training）

b．OFF-JT（Off the Job Training）　等

③ 経験

a．顧客の業務を通して

b．業務パッケージでの訓練

c．業務部門への出向　等

4．人的資源管理

4．3　教育・訓練

(2) 教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。

1 主　旨

要員の質的向上を図るため、教育及び訓練のカリキュラムは、技術力の向上、業務知識の習得及び情報セキュリティの確保等から検討する必要がある。

2 着 眼 点

(1) 情報技術全般及び業務アプリケーション分野について、情報処理技術者として必要な知識、能力を組織体として体系化していること。

(2) 情報セキュリティにかかわる教育を実施していること。

(3) 情報倫理にかかわる教育を実施していること。

3 関連事項

(1) 情報セキュリティ・情報倫理教育の実施方法

情報セキュリティ及び情報倫理教育は、組織におけるあらゆる教育・研修の機会を捉えて実施されなければならない。情報セキュリティ・情報倫理教育を実施する機会としては次のようなことが考えられる。

① 新人研修
② 一般研修
③ 社内講習会
④ 外部講習会
⑤ 昇格時研修　等

4．人的資源管理

4．3　教育・訓練

(3) 教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。

1 主　旨

要員が、企画、開発、運用及び保守業務の遂行に必要な知識、能力等を習得するため、教育及び訓練は、カリキュラムに基づいて定期的かつ効果的に行う必要がある。

2 着 眼 点

(1) 教育及び訓練を計画的に実施していること。

(2) 教育及び訓練の実施の効果を評価していること。

(3) カリキュラムの有効性を定期的に評価していること。

(4) 教育及び訓練の実施に必要な教材を整備していること。

(5) 教育及び訓練のインストラクタは、必要な経験及び知識を備えていること。

3 関連事項

(1) 教育・訓練計画の検討事項

教育及び訓練計画の策定に当たっての考慮事項

① 教育及び訓練の内容

② 対象者

③ 達成度

④ 評価方法

⑤ スケジュール

⑥ 運営組織及び実施体制

(2) 教育・訓練方法の例

① OJT

② OFF-JT

③ 自己啓発

④ ｅラーニング

⑤ 組織内の資格取得

⑥ 情報処理技術者試験の受験

⑦ 各種ベンダー資格の取得

(3) カリキュラムの受講者による評価方法の例

カリキュラムの評価として、以下のような項目を受講者に尋ねる方法がある。

① 全体的な評価

a．このカリキュラムの受講は有意義であったと思うか。

b．このカリキュラムは自身のスキル開発目標の達成に役立つと思うか。

c．自身の現在のスキルレベルに適したカリキュラムであったと思うか。

d．自身のスキル開発上の最適なタイミングで、このカリキュラムを受講できたと思うか。

e．このカリキュラムを開催することは、組織体にとって価値ある投資であると思うか。

f．このカリキュラムの受講を他の要員に推奨するか。

② カリキュラムについての評価

a．内容は期待を満たすものであったか。

b．内容は、事前案内に記載された目的を満たすものであったか。

c．受講した結果、自身の知識・スキルは向上したと思うか。

③ 業務への適用についての評価

この受講によって、現在担当している業務の効率性、確実性は向上すると思うか。

(4) カリキュラムの受講者の上司による評価方法の例

カリキュラムの評価として、以下のような項目を受講者の上司に尋ねる方法がある。

a．受講前と比較して受講者の受講効果は十分評価できるか。

b．このカリキュラムを開催することは、組織体にとって価値ある投資であると思うか。

(5) インストラクタの評価方法の例

インストラクタの評価として、以下のような項目を受講者に尋ねる方法がある。

① インストラクタは、対象とする領域における専門性を示したか。

② インストラクタは、キーとなる概念等について、分かりやすい説明を行ったか。

③ インストラクタは、受講者の興味を深めたか。

④ インストラクタは、質問に対して、適切かつ明快な対応をしたか。

4．人的資源管理

4．3　教育・訓練

(4) 要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。

1 主　旨

企画、開発、運用及び保守業務の遂行に必要な知識、能力等を習得させるため、キャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行う必要がある。

2 着眼点

(1) 情報戦略、業務環境及び情報環境に基づいてキャリアパスを確立していること。

(2) 情報戦略、業務環境及び情報環境の変化に対応して、キャリアパスを見直していること。

(3) キャリアパスを要員に周知徹底していること。

3 関連事項

(1) キャリアパスの意義

人材の有効活用を図る上でキャリアパスの設定は、次のような意義をもっている。

① 多能化への対応

② 個々人の動機付け

④ 組織体が必要とする人材の確実な育成

(2) 情報処理技術者試験

情報技術人材を対象とした国家試験で、知識を主体とした一定のスキルを客観的に評価する機能をもつ。スキル修得状況を確認するメルクマールとして活用できる。

また、情報処理技術者試験の区分は、システムアナリストやシステムアドミニストレータ、システム監査技術者、情報セキュリティアドミニストレータ等、組織体の情報化における役割の重要性に着目した区分となっている。

(3) 経済産業省 IT スキル標準

各種 IT 関連サービスの提供に必要とされる能力を明確化・体系化した指標であり、産学における IT サービス・プロフェッショナルの教育・訓練等に有用な共通枠組みを提供する。

IT 投資の様々な局面ごとに IT 技術者に求められる活動内容を明らかにすることで、各職種を定義している。

① スキルの専門分野・職種

a．マーケティング

市場機会の評価と選定、市場環境の分析、マーケティング戦略の立案、環境分析に基づ

く分析と洞察

b．セールス

ビジネス戦略の立案支援、顧客環境の分析、ITソリューションの提案、顧客満足度の管理、契約行為等セールス事務管理

c．コンサルタント

ビジネス戦略立案の提言・助言、顧客環境の分析、解決策の提言・助言、情報システムの評価・カウンセリング、知的資産管理

d．ITアーキテクト

アーキテクチャ設計、ソリューション構造設計、機能要件・非機能要件定義、アプリケーション及びシステム基盤設計の助言

e．プロジェクトマネジメント

プロジェクト基本計画の策定、プロジェクト全体の管理・統制、品質（納期、費用、納入物）管理、要員管理

f．ITスペシャリスト

システム基盤の分析、設計、システムの構築・導入、システムの運用・保守

g．アプリケーションスペシャリスト

アプリケーションの分析・設計、アプリケーションの開発、保守

h．ソフトウェアデベロップメント

要求分析、ソフトウェア製品の設計・開発、ソフトウェア製品のライフサイクルマネジメント

i．カスタマサービス

ソフトウェア・ハードウェアの導入、ソフトウェア・ハードウェアの保守、ソフトウェア・ハードウェアの障害回復、施設の設計・建築・管理

j．オペレーション

システムの運用・監視、サービスレベル管理、ヘルプデスク

k．エデュケーション

顧客研修ニーズの市場分析、研修カリキュラムの企画、研修コースの企画、研修コースの開発・実施、研修の効果測定

② スキルのレベル

a．レベル1～2（エントリレベル）

専門分野が確立するには至っておらず、当該職種の上位レベルの指導の下で、業務上における課題の発見・解決を行うことができるレベル。スキル開発においては、自らのキャリアパス実現に向けて積極的なスキルの研鑽が求められる。

b．レベル3～4（ミドルレベル）

専門分野が確立し、自らのスキルを駆使することによって、業務上の課題の発見・解決をリードすることができるレベル。スキル開発においても、自らのスキルの研鑽を止めることなく、また、下位レベルの育成に積極的に貢献することが求められる。

c．レベル5～7（ハイレベル）

組織体内において当該職種／専門分野に係るテクノロジやメソドロジー、ビジネスをリードするレベル。特にレベル７は、市場全体から見ても先進的なサービスの開拓や市場化をリードする。スキル開発においても、組織体のスキル開発の戦略の策定・実行に大きく貢献することが求められる。

③ キャリアパス

a．レベルアップ

b．専門分野・職種の変更

4．人的資源管理

4．4　健康管理

(1) 健康管理を考慮した作業環境を整えること。

1 主　旨

要員が身体的及び精神的に健康を保ち、企画、開発、運用及び保守業務を健全に遂行するため、健康管理を考慮した作業環境を整える必要がある。

2 着 眼 点

(1) 採光・照明、換気・空調等を適切に維持していること。
(2) VDT 作業対策を講じていること。
(3) 休憩のための施設を確保していること。
(4) 什器及び備品を適切に配置していること。
(5) オフィススペースを適切に確保していること。
(6) 受動喫煙防止の対策を立てていること。

3 関連事項

(1) 作業環境のチェックポイント
　① 採光・照明対策
　② 換気・空調（温度、湿度）対策
　③ 騒音対策
　④ 電磁波対策
　⑤ 気圧対策
　⑥ 休憩設備（リラックスルーム、休憩室等）の有無
(2) 関連法規
　① 労働安全衛生法
　② 健康増進法
　③ VCCI（Voluntary Control Council for Information Technology Equipment：情報処理装置等電波障害自主規制協議会）基準
　④ VDT 作業における労働衛生管理のためのガイドライン（厚生労働省）

4．人的資源管理

4．4　健康管理

(2) 健康診断及びメンタルヘルスケアを行うこと。

1 主　旨

要員の健康を維持するため身体面及び精神面についての健康診断及びカウンセリングを行う必要がある。

2 着眼点

(1) 要員の担当業務の特性を踏まえた健康診断を定期的に行っていること。

(2) カウンセリングを受けやすくしていること（専門カウンセラーの設置、カウンセリングの場所・予約方法の利便性、中立的なカウンセリング、相談内容の守秘等）。

(3) 健康診断又はカウンセリングの結果に基づいて必要な対策を講じていること。

(4) 必要な予防管理体制を確立していること。

3 関連事項

(1) 健康診断の種類

① 法定健康診断

a．一般健康診断

b．特殊健康診断

② 法定外健康診断

体力測定

(2) メンタルヘルスの管理方法の例

職業病、成人病、要員の物理的・肉体的健康管理のみならず、精神面又は心の側面における健康管理も重要である。

① カウンセリング

② 産業医（医師）による健康相談

③ 弁護士による悩み事相談　等

(3) 予防管理体制

重大な疾病や災害に繋がらないようにするためには、健康診断やカウンセリングの結果に基づいて、作業量の軽減、職種の変更、配置転換等、適切な予防体制がとられなければならない。

(4) その他の健康維持対策の例

① フィットネスクラブとの利用契約

② レジャー施設との利用契約

③ 指圧・マッサージの利用　等

5．委託・受託

5．1　計画

(1) 委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。

1 主　旨

委託又は受託の方針は、全体最適化計画の外部資源の活用（「Ⅰ．情報戦略　1.全体最適化　1.3 全体最適化計画の策定(7)」）の中で策定される。委託又は受託業務の内容を具体化するために委託又は受託の計画を策定し、責任者が承認する必要がある。

2 着眼点

(1) 委託又は受託計画は最適化計画に基づいて策定していること。

(2) 委託又は受託計画の立案手順を明確にしていること。

(3) 委託又は受託の責任者を明確にし、計画を責任者が承認していること。

(4) 状況の変化に応じて、委託又は受託計画を見直していること。

3 関連事項

(1) 委託又は受託計画の策定

① 委託又は受託の方針は全体最適化計画の中で組織体の情報戦略に基づいて策定する。

② 委託又は受託計画の承認に当たっては、関係者の合意が必要である。

③ 委託又は受託計画の立案手順の例

a．全体最適化の方針の確認

b．委託又は受託対象業務の把握

c．委託又は受託対象業務の状況調査

d．委託又は受託計画書の策定

e．委託又は受託による効果の算定、検討、評価

f．関係者の合意

g．委託又は受託の責任者の承認

(2) 委託又は受託の責任者

委託又は受託の責任の所在を明らかにし、委託又は受託業務を円滑に遂行するため、責任者を定める必要がある。

① 委託の責任者の例

a．情報システム部門の責任者

b．開発の責任者（プログラム開発）

c．運用の責任者

d．保守の責任者等

② 受託の責任者の例

a．プロジェクトマネージャ（プログラム開発）

b．データセンター長（運用、保守）

c．ASP 責任者、オンラインサービス責任者　等

(3) 委託又は受託計画書の例

① 目的

② 対象業務及び対象範囲

③ 業務内容

④ 期間（開発期間／運用期間）等

⑤ 委託費又は受託費の予算

⑥ 委託又は受託の効果

⑦ リスク、懸案事項と対策

⑧ 著作権等の権利関係

⑨ 機密保護対策

⑩ 委託先の選定条件

⑪ 受託の受諾基準

⑫ 委託又は受託の責任者

⑬ 委託又は受託の定期的評価

⑭ 委託又は受託の見直し時期　等

(4) 状況変化の例

① 企業戦略・情報戦略の変更

② 最適化計画の変更

③ 組織や対象業務の変更

④ 関連法規や諸制度の変更

⑤ 技術進歩、新サービスの登場

⑥ 委託又は受託先の経営環境の変化　等

(5) 合意を得る関係者の例

① 組織体の長

② 委託される業務のユーザ

③ 各運用担当者

④ 保守責任者、担当者

⑤ 開発プロジェクトの責任者

⑥ 外注委託先　等

5．委託・受託

5．1　計画

(2) 委託又は受託の目的、対象範囲、予算、体制等を明確にすること。

1 主　旨

委託又は受託業務の内容を明らかにし、業務を円滑に遂行するため、目的、対象範囲、体制、予算等を明確にする必要がある。

2 着 眼 点

(1) 委託又は受託の目的、対象範囲、予算、体制等を明確にしていること。

(2) 委託又は受託の目的、対象範囲、予算、体制等を関係者が合意していること。

3 関連事項

(1) 委託又は受託の目的の例

① 委託

a．システム開発期間の短縮

b．要員、設備の不足の解消

c．外部専門技術の活用

d．費用の削減　等

② 受託

a．宣伝効果

b．新技術の習得

c．収益の増加　等

(2) 委託又は受託の対象範囲

① 企画業務：開発計画の立案、開発計画立案のコンサルテーション等

② 開発業務：システム設計、プログラム設計、開発業務の PMO（Project Management Office）等

③ 運用業務：オペレーション、データエントリ、受注、出荷業務と関連システムのオペレーション、ネットワーク監視、ヘルプデスク等

④ 保守業務：業務システムのプログラム変更、障害時の復旧　等

(3) 体制

ハウジングやホスティングを利用する場合等、情報システム自体を組織体がまったく保有しない場合もある。また、出荷業務を倉庫業者に委託する場合等は、その業務に関するシステムは委託先のシステムに依存する場合と委託をする組織体の情報システムを利用する場合とがある。

5．委託・受託

5．1　計画

(3) 委託又は受託は、具体的な効果、問題点等を評価して決定すること。

1 主　旨

委託又は受託の目的を確実に達成するため、委託又は受託は具体的な効果、問題点、リスク等を評価した上で決定する必要がある。

2 着 眼 点

(1) 委託又は受託の効果、問題点、リスク等を全体最適の観点から検討していること。

(2) 委託にかかわる関係者が参画して評価していること。

(3) 評価結果を計画等に反映していること。

3 関連事項

(1) 委託又は受託の効果の例

① 委託

a．費用の節減（人的・物的費用節減、固定費の変動費化等）

b．期間の短縮（開発期間等）

c．専門的なサービスの享受

d．付加価値の高い業務への移行（コアコンピタンスへの集中投資）

e．投資リスクの削減　等

② 受託

a．収益の増加

b．宣伝効果

c．新技術の習得

d．優位性のあるサービスの提供によるシェアの拡大

e．ノウハウの蓄積

f．余剰設備の活用

g．新たなビジネスチャンスの獲得・提携先の獲得　等

(2) 委託又は受託の問題点とリスク

① 委託

a．委託業務についてのノウハウが蓄積されない。

b．委託先の倒産等で事業継続が困難になる。

c．品質管理が委託先に依存する。

d．情報漏えい（企業秘密、個人情報）のリスク増大
e．委託先のコンプライアンス違反によるリスク増大　等

② 受託
a．特定の得意先への依存
b．委託元の都合による予想外の作業増
c．委託元のコンプライアンス違反
d．ビジネス打切りによるリソースの余剰発生　等

(3) 全体最適の観点からの評価の視点
① 組織体の優位性の確保
② 品質面
③ 技術面
④ 費用面
⑤ コンプライアンス
⑥ 機密保持　等

5．委託・受託

5．2　委託先選定

(1) 委託先の選定基準を明確にすること。

1 主　旨

委託計画に基づいて委託先を選定するために、選定基準を明確にする必要がある。

2 着眼点

(1) 委託先の選定基準を明文化し、企画、開発、運用及び保守の責任者が承認していること。

(2) 選定基準は委託計画と整合性をとっていること。

(3) 選定基準は客観的な指標を定めていること。

(4) 選定基準は委託業務の特性を考慮していること。

(5) 選定基準は事業継続計画を考慮していること。

3 関連事項

(1) 委託先の選定基準の例

① 安定性（委託先の経営状況：売上、利益、事業内容等）

② 受託実績

③ 技術レベル（技術水準（IT スキル標準、情報処理技術者試験）、技術者の要員数等）

④ システム環境（必要な経営資源の確保）

⑤ 委託費と支払条件

⑥ セキュリティ対策状況（プライバシーマーク取得、ISMS 認定等）

⑦ 取引先、再委託先等の確認

⑧ 品質管理体制

⑨ 教育訓練体制

⑩ 委託先の第三者による監査結果の参照

⑪ 委託先の事業継続計画（バックアップ体制等）　等

(2) 委託計画との整合性

選定基準が委託計画で定めた委託先選定方針に基づいていること。委託計画には委託先の見直しの時期を含む必要がある。特に委託先の経営状況の見直しは、委託先の倒産等によって業務の遂行に支障が生じるため、定期的に検討する必要がある。

委託先の状況で事業継続に問題を及ぼすことになるのは、次のようなケースが考えられる。

① 委託先が別の企業から買収を受ける。

② 委託先が合併、事業分割等によって業務方針が変更される。

③ 委託先が倒産等によって、事業継続が困難になる。

(3) 委託業務の特性

① 企画、開発、運用、保守及び災害対策の各業務のもつ特性

② 一過性の業務か、継続的な業務かの区別

③ 委託期間（長期、短期の区別）

④ 機密度の状況　等

5．委託・受託

5．2　委託先選定

(2) 委託候補先に必要な要求仕様を提示すること。

1 主　旨

提案書を作成する際の受託条件を明確にするため、委託候補先に必要な要求仕様を提示する必要がある。

2 着 眼 点

(1) 委託方針に基づいて要求仕様を作成していること。

(2) 委託の目的を明確にしていること。

(3) 委託の範囲、要求するサービスの内容、サービスのレベルを明確にしていること。

3 関連事項

(1) 委託内容の要求仕様の例

① 委託の目的
② 委託の期間
③ 委託の対象範囲
④ 委託する業務の内容
⑤ 要求される技術
⑥ 要求される品質
⑦ 要求されるサービスレベル
⑧ 費用
⑨ 使用する機器等の所有権、保管場所
⑩ 作業場所
⑪ 知的財産権の所属
⑫ セキュリティ要件
⑬ 機密保持
⑭ 再委託の可否　等

5. 委託・受託

5. 2 委託先選定

(3) 委託候補先が提示した提案書の比較検討を行うこと。

1 主　旨

最適な委託先を公正に選定するため、選定基準に基づいて、委託先が提案した提案書を比較検討する必要がある。

2 着 眼 点

(1) 選定基準に基づいて、提案書の受託条件を比較検討していること。

(2) 委託先の決定理由を明確にしていること。

(3) 比較検討の結果をユーザ、企画、開発、運用、保守及び災害対策の責任者が承認していること。

3 関連事項

(1) 委託先の比較検討

① 複数の委託先を比較検討の対象とすることが望ましい。

② 比較検討の対象となる委託候補先は、委託先選定方針に従って選択する。

③ 比較検討結果のまとめ方の例

a. 決定した委託先

b. 決定理由

c. 受託条件比較表（資料として添付する）

委託先の提示した受託条件と選定基準による評価を一覧表にまとめたもの。

(2) 委託先評価の定期的実施

委託先の業績、業務内容等は、情報環境の影響を受け変動することが考えられる。したがって、委託実施後も委託先を定期的に調査・分析し、評価することが必要である。

(3) 代替可能性の検討

委託先の選定に当たっては、特殊な技術等が必要な場合等、代替が困難な委託先を選定する場合もあるが、継続的な業務の運用を委託する際には、委託先の倒産等、不測の事態が発生した場合等に、委託先が使用するハードウェア等について市場での調達が容易であるか等、委託先の代替可能性を検討する必要がある。

(4) 選定過程の説明責任

組織体の特性によっては、利害関係者（例えば、株主等）に対して、委託先選定の過程を説明する必要がある。

① 選択基準を遵守しているか。

② 特定の委託先に有利な要求仕様となっていないか。
③ 委託候補先をあらかじめ絞る場合には、合理的な絞込みとなっているか。
④ 選定担当者の恣意が働いていないか　等

5. 委託・受託

5. 3 契約

(1) 契約は委託契約ルール又は受託契約ルールに基づいて締結すること。

1 主　旨

委託契約を確実に行うため、委託契約ルール又は受託契約ルールに基づいて締結する必要がある。

2 着 眼 点

(1) 委託契約ルール又は受託契約ルールを定めていること。

(2) 委託契約ルール又は受託契約ルールに基づいた契約書を作成し、委託又は受託の責任者が承認していること。

(3) 契約書は法的要件を満たしていること。

(4) 契約書の内容を関係者に周知徹底していること。

3 関連事項

(1) 委託契約ルール

① 契約締結の手順

a. 契約書起案

b. 契約所管部門のチェック（総務部法務担当等）

c. 責任者の承認

d. 契約締結　等

② 標準的な契約

当該組織体の状況に応じ、標準的な契約書の様式及びその作成要領を定めておく。契約書は取引単位で取り交わすのが基本であるが、長期にわたって継続的に業務を委託する場合には、個々の取引について共通する部分について基本契約を取り交わし、個々に異なる部分について覚書を取り交わすこともある。

標準的な契約書の様式の例

a. システム開発委託契約書

b. 運用委託契約書

c. ネットワーク管理契約書

d. ソフトウェア保守契約書　等

(2) 契約書記載上の留意事項

① 委託業務内容及び範囲

② 委託方法

③ 期間又は納期
④ 成果物
⑤ 責任者
⑥ 受入れ検査
⑦ 委託費と支払条件
⑧ 権利の帰属
⑨ 瑕疵担保責任
⑩ 損害賠償
⑪ 特約条項
⑫ 免責条項
⑬ 障害対策
⑭ 再委託の可否　等

(3) 法的要件

① 契約は原則、当事者が自由に取り交わすことができるが、法律には、当事者の意思にかかわらず適用される「強行法規」と、当事者の意思によって適用しないことができる「任意法規」がある。したがって、契約締結に当たっては、「強行法規」に違反していないことを確認する。労働基準法に違反するような契約はコンプライアンス違反になる。

② 請負、派遣、準委任等の委託の契約形態に応じて、関連する法律が規定する内容を把握するとともに、委託業務の実施段階においても注意が必要である。

③ 関連する法規の例

a．民法
b．労働者派遣事業法
c．税法
d．下請代金支払遅延防止法
e．著作権法
f．不正競争防止法
g．個人情報保護法　等

④ 法的規制には、委託元の業種・業務によって異なる場合がある。インフラストラクチャ事業（電気・ガス・水道等）、金融・証券、医薬品製造、医療関係等は特殊な規制があり、遵守することが当然のように求められている。委託先に依頼する場合には、事前に法的規制を遵守できるような体制、技術・知識等を備える必要があることを伝えておかなければならない。

5. 委託・受託
5. 3 契約
(2) コンプライアンスに関する条項を明確にすること。

1 主　旨

情報の不正利用、漏えい、プライバシーの侵害等を防止するため、契約時に不正防止、機密保護等の対策を明確にする必要がある。

2 着 眼 点

(1) 不正防止、機密保護等の対策を情報セキュリティ条項として定めていること。
(2) 責任範囲を明確にしていること。
(3) 委託元の組織体の社内規程に準ずる管理が委託先でも実施されること。

3 関連事項

(1) 情報セキュリティ条項の例
　① 守秘義務及び機密保護に対する宣誓
　　例:「職務上、知り得た情報をみだりに他人に知らせ、又は不当な目的に使用してはならない。」
　② 情報の目的外の利用禁止
　　例:「委託業務に関する情報を許可なく複写、複製することを禁止する。」
　③ 事故発生時における報告義務
　④ プライバシーの保護
　⑤ 委託先におけるシステム監査の実施　等
(2) 不正防止、機密保護等の対策上必要な取決めの例
　① データの授受
　② 保管方法及び保管場所、責任者の明確化
　③ 情報の破棄方法
　④ 作業時間、作業場所
　⑤ かぎ管理、監視　等
(3) プライバシーの保護
　個人のプライバシーが侵害される危険性に対して、契約で個人情報保護のための適切な手続を定めておく必要がある。
(4) 責任範囲
　情報セキュリティ条項の違反に対する委託先の責任の範囲を明確にしておく。

(5) 社会規範と法令の新設等について

コンプライアンスの問題は、単に法令を遵守するのみではなく、社会通念上、道義的問題が生じかねない点についても配慮する必要がある。特にIT関連は社会での法的整備がITの発展より遅れている面があった。現在、法的整備が進みつつあるため、新しいIT関連の法令の新設や改訂にも注意を払っていく必要がある。

5．委託・受託

5．3　契約

(3) 再委託の可否について明確にすること。

1 主　旨

再委託にかかわるトラブルを防止するため、契約時に再委託の可否を明確にする必要がある。

2 着 眼 点

(1) 委託契約書に再委託の可否を明確にしていること。

(2) 再委託については事前に委託元の許可を得ていること。

(3) 再委託先の監督責任を明確にしていること。

(4) 再委託先の機密保持等の適用条件を明確にしていること。

3 関連事項

(1) 再委託先の監督責任

再委託先については機密漏えい防止等の観点から委託先と同等の管理をする必要がある。

① 委託先の再委託先の監督責任を明確にすること。

② 再委託先は、委託先と同等の権利、義務を有すること。

③ 再委託先の品質管理責任を明確にすること。

④ 機密保持について明確にすること。

⑤ 請負契約の場合も再委託についての機密保持等の責任を明確にすること。

⑥ 委託先による再委託先への管理状況を明確にすること。

5．委託・受託

5．3　契約

(4) 知的財産権の帰属を明確にすること。

1 主　旨

知的財産権にかかわるトラブルを防止するため、契約時に知的財産権の帰属を明確にする必要がある。

2 着 眼 点

(1) 委託先が作成したプログラム、データ及びドキュメントの知的財産権の帰属を明確にしていること。

(2) 知的財産権の管理の責任者を定めていること。

3 関連事項

(1) 知的財産権

知的財産権は、大きく著作権と工業所有権（特許権等）に分類される。

① 著作権に関する留意点

a．プログラムは著作物として保護される。

b．職務上の著作は法人著作となる。

c．原始的帰属は委託方式によって異なる。

d．権利の帰属、プログラムの改変や複製についても契約で定めておく。

② 工業所有権に関する留意点

プログラムが自然法則を利用したものと認められる場合、特許成立の可能性がある。ビジネスモデル特許について留意する。

③ 知的財産権の動向

知的財産権に関する事項は、情報環境の変化に伴って絶えず変動しており、その動向に注目する必要がある。

(2) 管理の責任者

責任の所在を明らかにするため、組織全体としての知的財産権を管理する部門及び責任者を設けておく。なお、プログラム開発時の他人の著作権侵害等についての委託先の管理責任を委託契約書に記載する。

（参考）

知的財産権には以下のものがある。

① 著作権

② 特許権
③ 実用新案権
④ 意匠権
⑤ 商標権
⑥ その他（不正競争防止法の営業秘密）

(3) 業務ノウハウと業務ソフトウェアの著作権の関係

業務ソフトウェアは、当該委託元の業務を基に設計され、プログラミング技術と創意をもって業務ソフトウェアに移植される。著作権の帰属を明確化することは、委託元の業務ノウハウを守る上では注意すべき点である。

現状の著作権法では、著作物に対して主たる創造的な創意を働かせた方に著作権があるという規定になっている。そのことは、業務ソフトウェアが委託先から市販された場合、委託元の業務ノウハウが、業務ソフトウェアとして外部に流出してしまうことを意味している。委託先は業務ノウハウを開発する何らの貢献もしていないのに、業務ノウハウの流出は、委託元の相対的競争力を弱めかねない。

そのような事態を防止し自社のノウハウを守るためには、委託元が著作権の帰属に関して、契約書上で明確な態度を示し、できれば完成・納品後の著作権が委託元に帰属するよう明記することが重要である。

(4) 委託作業のノウハウの帰属

一般的に、ソフトウェア開発企業等は、委託によるソフトウェア開発等、委託作業から得られるノウハウを基に、ナレッジの蓄積、生産性の向上、社員のスキルアップ等を行っている。そのような企業の健全な発展のためには、開発ノウハウの帰属を明記することが重要である。

(5) ソフトウェアの著作権と委託先の変更

委託先の作成したソフトウェアについて、委託元がその改変権又は第三者に開示する権利を有していない場合、ソフトウェアの改変等に際して委託先を変更することが困難になることがある。委託先の変更の自由度を確保するためには、当該ソフトウェアを利用する権利に加え、改変する権利及び守秘義務を条件に第三者に開示する権利を取得しておく必要がある。

5．委託・受託

5．3　契約

(5) 特約条項及び免責条項を明確にすること。

1 主　旨

問題の発生が想定される事項に対応するため、契約時の特約条項及び免責条項を明確にする必要がある。

2 着 眼 点

(1) 想定される問題事項を明確にしていること。

(2) 必要な特約条項及び免責条項を契約書で明確にしていること。

3 関連事項

(1) 特約条項

契約ルールで定めた標準的な契約書による対応が困難な場合に作成する。

① 特約条項の例

a．再委託の禁止又は制限

例：「本件業務を第三者に再委託することはできない。ただし、書面による承諾を得た場合はこの限りではない。」

b．プログラム等の権利帰属の条項

例：「本件プログラム及び関連資料に関する一切の権利は、～に帰属する。」

c．違約金の条項

例：「～に反した場合には、～円を違約金として支払う。」

d．検査・検収の条項　等

② 事業継続計画

災害発生時等のバックアップ体制について委託先の対応を契約書に記載する。

(2)　免責条項

トラブルを回避するため、委託先の保証と責任の範囲を明らかにし、免責については免責事由等を検討し、契約上明らかにすること。

① 免責条項の例

a．事故等の原因が委託先にある場合

b．地震等不可抗力による業務の停止　等

5. 委託・受託

5. 3 契約

(6) 業務内容及び責任分担を明確にすること。

1 主　旨

委託業務を円滑に遂行するために、契約書、仕様書に委託業務の内容、責任分担を明確にする必要がある。

2 着 眼 点

(1) 委託業務の内容、責任分担を契約書、仕様書に明記していること。

(2) 追加作業についての取扱いを明記していること。

3 関連事項

(1) 委託業務内容と責任分担の例

① システム開発

a. プロトタイプ型開発の場合、当初の開発費用に含まれるプログラム変更回数

b. データ移管の作業内容：バックアップ作業は委託元か委託先か、等

② システム運用

a. 運用業務の対象範囲

b. 運用時間

c. 修正入力の承認者

d. ジョブの起動の承認者

e. 報告する運用記録の内容　等

③ 保守

a. 報告すべき障害の対象範囲

b. 保守の記録と報告

c. 通常保守費用の範囲と追加作業の内容　等

(2) 保証・損害賠償等

事故や障害による損害が発生した場合、システム業務遂行上の責任分担を明確にすることは、双方にとって重要となる。特に、委託元が委託先に必要以上に多くを期待している場合、委託先が保証や損害賠償に応じないケースが考えられる。それを防止するためには、SLA (Service Level Agreement) 等で委託元の要求仕様を明確にして、双方の責任範囲を曖昧にせず、契約書で明確にすることが必要である。

また、委託先は自社の負荷が契約内容以上に大きくなる場合、コンティンジェンシー

（contingency）コストとして見積り金額に上乗せしてくる可能性があり、委託元が果たすべき責務を明確にしておかないと防止できなくなる可能性がある。

(3) 請負契約、準委任契約及び派遣契約

契約に際しては、請負契約であるのか、準委任契約であるのか、又は派遣契約であるのかを明確にしておく必要がある。請負契約で委託する場合には、成果物の要件を詳細に示すとともに、委託作業期間中に大きく変更しないことが肝要である。システム開発等において、成果物の要件を詳細に示せない場合には、要件確定までの業務分析コンサルティングやシステム企画策定等は準委任契約で委託し、その後の作業を請負契約で委託する等の切り分けの検討が必要である。

① 請負契約：定められた仕事を完成させることを目的とする契約

② 準委任契約：事務の遂行を目的とする契約

③ 派遣契約：労働者の派遣によって、派遣先の指揮監督の下で業務に従事する契約

5. 委託・受託

5. 3 契約

(7) 契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。

1 主　旨

委託先の委託業務内容を明確にし、円滑な業務を実施するために、契約締結後の業務の内容に追加及び変更が生じた場合、契約内容の再検討を行う必要がある。

2 着 眼 点

(1) 契約書、仕様書に委託業務の内容を明記していること。

(2) 追加される作業、変更される作業内容を明確にしていること。

(3) 当初契約外の作業は別契約で管理されていること。

3 関連事項

(1) 進捗管理、品質管理と追加作業

① 開発

特にシステム開発の局面で進捗管理、品質管理が明確で実効性のある有効なものであるためには、当初の契約書、仕様書の記載が明確である必要がある。作業範囲が不明確では追加費用発生を伴わないとの安易な発想から、本来の作業の範囲を越える追加作業が発生し、開発そのものが遅延する原因となる。また、品質管理の面からも当初の品質目標を変更するような追加変更は委託業務の品質にも支障をきたす原因となる。

② 運用、保守

運用、保守については、そのサービスレベルを明記して作業を委託することによって、その品質、作業進捗管理が有効なものになる。契約や仕様書にない追加作業、変更作業は、本来、業務上で必要とされるサービスレベルの確保を困難にする。

5．委託・受託

5．3　契約

(8) システム監査に関する方針を明確にすること。

1 主　旨

委託先の委託業務内容の信頼性、安全性、効率性の確保を担保するために、委託契約にシステム監査に関する方針を明確にする必要がある。

2 着眼点

(1) 契約でシステム監査の実施の方針を定めていること。

(2) システム監査の対象範囲、適用する基準を明確にしていること。

(3) システム監査の結果の取扱いを明確にしていること。

3 関連事項

(1) システム監査の実施の方針

① 委託側が直接にシステム監査を実施する権利を有する場合

a．委託側自らがシステム監査を実施する。

b．委託側がシステム監査人を選任する。

② 委託側の共同システム監査

各委託先が個別のシステム監査を実施する煩雑さを避けるため、いくつかの委託先が共同でシステム監査を実施する。

a．委託側自らがシステム監査を実施する。

b．委託側が共同でシステム監査人を選定する。

③ 受託側のシステム監査

a．内部監査として実施する。

b．受託側が第三者をシステム監査人に選定して実施し、その内容を公表する。

(2) システム監査の結果の取扱い

① システム監査結果の報告のルールを明確にすること。

② 基準を明確にし、一定の要求水準に到達しなかった場合の取扱いを明確にすること。

③ 受託側がシステム監査人を選定する場合のシステム監査人の選定要件を明確にすること。

5. 委託・受託

5. 4 委託業務

(1) 委託業務の実施内容は、契約内容と一致すること。

1 主　旨

委託業務の内容を過不足なく実施するため、委託業務の実施内容は、契約書に記載された内容と一致させる必要がある。

2 着 眼 点

(1) 契約で定めた委託業務の内容を実施していること。

(2) 委託業務の実施内容を委託の責任者が把握していること。

(3) 委託業務の実施内容と契約内容の相違点について、適切な措置を講じていること。

3 関連事項

(1) 実施内容の把握

① 把握内容の例

a. 実施業務の対象範囲

b. 実施業務の品質レベル

c. 実施業務に要する費用

d. 実施業務の納期　等

② 把握方法の例

a. ミーティングの開催

b. 担当者からの報告

c. 現場の視察

③ 把握のタイミング

定期的及び必要に応じて把握する（SLA レビューの実施等）

(2) 契約内容との相違

① 契約内容に比べて実施内容が十分でないケース

② 契約内容に比べて実施内容が過剰であるケース（委託先から委託元への利益供与として指摘される恐れもある。）

③ ある作業項目の費用が他の作業項目の費用として計上されるケース

(3) 適切な措置

① 適法性の観点からみた措置

② 納期面の観点からみた措置（作業の進捗については、「VI. 共通業務　2. 進捗管理」を参照）

③　費用面の観点からみた措置
④　品質面の観点からみた措置
⑤　不正防止、機密保護等の観点からみた措置

5．委託・受託

5．4　委託業務

(2) 契約に基づき、必要な要求仕様、データ、資料等を提供すること。

1 主　旨

委託業務を委託計画どおりに遂行するため、契約に基づき、必要な要求仕様、データ、資料等を委託先に提供する必要がある。

2 着眼点

(1) 委託契約書、仕様書に基づき、必要な要求仕様、データ、資料を提供していること。

(2) 資料、機材等提供の責任者、担当者を明確にしていること。

(3) 資料等提供のルールを定め、提供、変換、廃棄等の方法を明確にしていること。

3 関連事項

(1) 必要な要求仕様

要求される仕様には性能要件、セキュリティ要件等がある。

(2) データの提供

データの提供については、主に機密保護に関連する問題が生じる場合が多い。(「VI. 共通業務 5. 委託・受託　5.4 委託業務(4)」の機密保護の条項を参照) また、必要なデータが漏れなく提供されていることが必要である。

a．受渡しのルールを明確にすること。

b．データの複写の制限と廃棄のルールを明確にすること。

(3) 資料等

① 資料等の中には資材（ハードウェア等）も含まれる。

a．委託される業務に必要な資材の提供の方法

b．設置場所

c．委託業務終了後の変換の方法

d．保管責任

e．所有権　等

② 資料

資料についてはデータに準ずる取扱いになる。営業の機密保持等に留意する。

5．委託・受託

5．4　委託業務

(3) 委託業務の進捗状況を把握し、遅延対策を講じること。

1 主　旨

受託業務を受託計画どおりに遂行するため、受託業務における進捗状況を把握し、リスク対策を講ずる必要がある。

2 着眼点

(1) 受託の責任者は、進捗状況を定期的に把握していること。

(2) 遅延やその他の問題点の原因を究明し、適切な措置を講じていること。

3 関連事項

(1) 進捗状況の実施

受託の進捗管理は、受託側の組織体内での進捗管理と同様に実施する。

受託の場合は遅延の原因が必ずしも受託した側に起因せず、委託元の都合によって発生する場合があるので、委託元との定期的な会合や報告によって調整を行うことになる。大幅な仕様の変更等については、契約そのものの変更を検討する必要がある。(「VI. 共通業務　5. 委託・受託　5.3 契約(7)」を参照)

EVM (Earned Value Management) 等の管理手法の使用も有効である。(「VI. 共通業務　2. 進捗管理　2.1 実施」を参照)

(2) 受託業務で想定される進捗管理上のリスクの例

① 委託元に原因がある場合の例

a．委託元の頻繁な仕様変更

b．委託元の仕様外要求

c．委託元の受託側に対する過大な期待　等

② 受託側に原因がある場合の例

a．担当者の仕様の取違え

b．作業量の見積り間違い

c．担当者間の連携不足

d．担当者のスキル不足、交代

e．ツール類の性能不足　等

③ 委託側、受託側の双方に原因がある場合

a．受託側、委託側のコミュニケーション不足

b．受託側、委託側の責任分担の不明確　等

(3) 適切な措置

① 「Ⅵ. 共通業務　2. 進捗管理　2.2 評価」を参照。

② 適切な措置を講ずる際のポイント

a．懸案事項、責任の所在を明確化し、相互に了解すること。

b．受託側の管理下により行う。

c．受託側、委託側相互の措置の整合性を考慮すること。

d．懸案事項の具体的な対策を明確にすること。

③ 適切な措置の例

a．必要な要員の増加

b．必要な資料、資材の提供

c．委託元からの指示の文書化　等

5．委託・受託

5．4　委託業務

(4) 委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。

1 主　旨

委託契約どおりに誤びゅう防止、不正利用、漏えい、プライバシーの侵害等を防止する対策を実現するため、誤びゅう防止、不正防止、機密保護等の対策の実施状況を把握し、適切な対策を講ずる必要がある。

2 着 眼 点

(1) 誤びゅう防止、不正防止、機密保護等の対策の実現方法を明確にしていること。

(2) 誤びゅう防止、不正防止、機密保護等の対策の実現状況を把握していること。

(3) 誤びゅう防止、不正防止、機密保護等の対策の実現状況に応じて、必要な改善措置を講じていること。

(4) 不正防止、機密保護にかかわる担当者の誓約書を取り交わしていること。

3 関連事項

(1) 実現方法の例

① 入力資料の受渡簿による枚数管理等

② 作業引継ぎ時の引継書の記載

③ パスワード管理

④ 関連資料の返却、廃棄

⑤ 本番データへのアクセス禁止（ファイル分離） 等

(2) 把握方法の例

① 作業現場の視察

② 委託先からの作業報告書の提出

③ ミーティングの開催

④ アクセスログの分析　等

(3) 改善措置の例

① 入力のプルーフリストによる個別チェック

② コントロールトータルチェック機能の追加

③ チェックディジット機能の追加

④ パスワードの変更

⑤ 委託先への申入れ　等

5．委託・受託

5．4　委託業務

(5) 成果物の検収は、委託契約に基づいて行うこと。

1 主　旨

委託の目的の達成を確認するため、委託契約に基づいて成果物の検収を行う必要がある。

2 着 眼 点

(1) 成果物の検収方法を明確にしていること。

(2) 成果物の検収は、検収方法に基づいて実施していること。

(3) 検収結果を委託の責任者が承認していること。

3 関連事項

(1) 検収方法の例

① ウォークスルー

② レビュー（設計書等）

③ オペレーション日報による確認（オペレーションの場合）

④ 定期的な障害記録報告

⑤ ネットワーク監視記録、報告

⑥ 保守作業記録　等

(2) プログラム検収のポイント

① 受入れテストを行っていること。

② 受入れテストの結果を記録し、保存していること。

③ 受入れテストを関係する責任者が承認していること。

④ Fit & Gap 分析　等

５．委託・受託

５．４　委託業務

(6) 業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。

1 主　旨

業務終了後、不正競争防止、機密保持の観点から委託業務で提供したデータ、資料等の回収及び廃棄の確認を行う必要がある。

2 着眼点

(1) データ、資料等の回収、廃棄の方法を明確にしていること。

(2) 回収、廃棄の確認の方法を明確にしていること。

(3) 回収、廃棄の報告を委託の責任者が承認していること。

3 関連事項

(1) 回収の手順例

① データ、資料等の受渡簿の作成

② 回収したデータ、資料等の確認

③ 回収報告書の作成

④ 回収報告書の承認

データ、資料等の受渡簿の作成に際しては、再委託先がある場合等に当初コピーした資料の連番管理等を実施し、回収漏れがないようにする必要がある。

(2) 廃棄の手順例

① 委託作業終了後に廃棄する資料の一覧表の作成

② 委託元の廃棄への立会い、又は業者等の廃棄証明書類の入手

③ 廃棄報告書の作成

④ 廃棄報告書の承認

データの廃棄については、例えば貸与したPC等は単に初期化してもデータは完全には消去されないため、電子媒体上のデータの廃棄が完全に実施されるように留意する。再委託先がある場合等の廃棄については、回収の場合と同様に、コピーされたデータ、資料等がすべて廃棄されたことが確認できるように管理することが必要である。

5．委託・受託

5．4　委託業務

(7) 委託した業務の結果を分析及び評価すること。

1 主　　旨

今後の委託計画及び委託先選定に反映するため、委託した業務の結果を分析及び評価する必要がある。

2 着 眼 点

(1) 委託計画に基づいて、委託業務の実施結果を分析及び評価していること。

(2) 委託業務の実施結果を分析及び評価結果に記録し、委託の責任者が承認していること。

(3) 関係者に評価結果を報告していること。

3 関連事項

(1) 評価結果の例

① 委託計画の達成状況

a．計画品質（性能）の達成

b．計画納期の達成

c．計画の費用での委託業務実施

d．品質、納期、費用等の総合的評価

e．不正防止、機密保護等の対策の評価

② 委託先の評価

③ 契約書の評価　等

(2) 今後の委託業務への反映項目

① 委託計画策定段階……計画段階で考慮しなければならない項目ではないか。

② 委託先の選定段階……委託先選定基準に追加及び変更が必要な項目はないか。

③ 契約締結段階……契約書に追加及び変更が必要な条項はないか。

④ 委託業務実施段階……委託業務の実施に対して、見直しが必要な項目はないか。

５．委託・受託

５．５　受託業務

(1) 受託業務の実施内容は、契約内容を遵守すること。

1 主　旨

受託業務の内容を過不足なく実施するため、受託業務の実施内容は、契約書に記載された内容と一致させる必要がある。

2 着 眼 点

(1) 契約で定めた受託業務の内容を実施していること。

(2) 受託業務の実施内容を受託の責任者が把握していること。

(3) 受託業務の実施内容と契約内容の相違点について、適切な措置を講じていること。

3 関連事項

(1) 実施内容の把握

① 把握内容の例

a．実施業務の対象範囲

b．実施業務の品質レベル

c．実施業務に要する費用

d．実施業務の納期　等

② 把握方法の例

a．ミーティングの開催

b．担当者からの報告

c．現場の視察

d．成果物のレビュー

③ 把握のタイミング

定期的及び必要に応じて把握する。

(2) 契約内容との相違

① 契約内容に比べて実施内容が十分でないケース

② 契約内容に比べて実施内容が過剰であるケース

(3) 適切な措置

① 適法性の観点からみた措置

② 納期面の観点からみた措置（作業の進捗については、「Ⅵ．共通業務　2.進捗管理」を参照）

③ 費用面の観点からみた措置

④ 品質面の観点からみた措置

⑤ 不正防止、機密保護等の観点からみた措置

5．委託・受託

5．5　受託業務

(2) 受託内容の進捗状況を把握し、リスク対策を講じること。

1 主　旨

受託業務を受託計画どおりに遂行するため、受託業務における進捗状況を把握し、リスク対策を講ずる必要がある。

2 着眼点

(1) 受託の責任者は、進捗状況を定期的に把握していること。

(2) 遅延の原因を究明し、適切な措置を講じていること。

3 関連事項

(1) 進捗状況の実施

受託の進捗管理は、受託側の組織体内での進捗管理と同様に実施する。

受託の場合は遅延の原因が必ずしも受託した側に起因せず、委託元の都合によって発生する場合があるので、委託元との定期的な会合や報告によって調整を行うことになる。大幅な仕様の変更等については、契約そのものの変更を検討する必要がある。(「VI. 共通業務　5. 委託・受託　5.3 契約(7)」を参照)

EVM 法等の使用も有効である。(「VI. 共通業務　2. 進捗管理　2.1 実施」を参照)

(2) 適切な措置

① 「VI. 共通業務　2. 進捗管理　2.2 評価」を参照。

② 適切な措置を講ずる際のポイント

a．懸案事項、責任の所在を明確にし、相互に了解すること。

b．受託側の管理下により行うこと。

c．受託側、委託側相互の措置の整合性を考慮すること。

d．懸案事項の具体的な対策を明確にすること。

③ 適切な措置の例

a．必要な要員の増

b．必要な資料提供

c．委託側からの指示の文書化　等

5. 委託・受託
5. 5 受託業務
(3) 成果物の品質管理を行うこと。

1 主　旨

受託契約に基づく成果物の検収基準に成果物が到達するように、受託側で品質管理を行う必要がある。

2 着眼点

(1) 成果物の品質基準を明確にしていること。
(2) 受託側の品質管理方針に基づいて成果物を管理していること。
(3) 成果物の品質管理結果を改善に反映していること。

3 関連事項

(1) 受託業務の品質管理

受託業務の品質管理は、受託側の品質管理ルールに基づいて実施されるものであるが、委託元が委託元の品質管理ルールの適用を求める場合は、その品質管理ルールを適用することになる。品質管理は、基本的に委託元が検収する前に実施され、要求される品質を確保することである。

委託元での運用が特別な法規制の下で行う必要がある場合は、それに準拠することを委託元に確認しておく必要がある。

(2) 品質管理については、「VI. 共通業務　3. 品質管理」を参照。

5．委託・受託

5．5　受託業務

(4) 契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。

1 主　旨

業務終了後、不正防止、機密保持の観点から受託業務で提供されたデータ、資料等の回収及び廃棄の確認を行う必要がある。

2 着眼点

(1) データ、資料等の回収、廃棄の方法を明確にしていること。

(2) 回収、廃棄の確認の方法を明確にしていること。

(3) 回収、廃棄の報告を委託の責任者が承認していること。

3 関連事項

(1) 回収の手順例

① データ、資料等の受渡簿の作成

② 回収したデータ、資料等の確認

③ 回収報告書の作成

④ 回収報告書の承認

データ、資料等の受渡簿の作成に際しては、再委託先がある場合等に当初コピーした資料の連番管理等を実施し、回収漏れがないようにする必要がある。

(2) 廃棄の手順例

① 委託作業終了後に廃棄する資料の一覧表の作成

② 委託元の廃棄への立会い、又は業者等の廃棄証明書類の入手

③ 廃棄報告書の作成

④ 廃棄報告書の承認

データの廃棄については、例えば貸与したPC等は単に初期化してもデータは完全には消去されないため、電子媒体上のデータの廃棄が完全に実施されるように留意する。再委託先がある場合等の廃棄については、回収の場合と同様に、コピーされたデータ、資料等がすべて廃棄されたことが確認できるように管理することが必要である。

6．変更管理

6．1　管理

(1) 変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。

1 主　旨

変更管理ルール及び変更手順書は、変更を円滑かつ効果的に行うために必要なものであり、ユーザ、開発、保守の責任者が承認を行う必要がある。大規模な変更は管理基準での開発業務の管理となる。

2 着 眼 点

(1) 変更管理ルール及び変更手順を明文化し、組織体として承認していること。
(2) 変更管理ルールは、情報システムの運用形態を考慮していること。
(3) 変更手順は変更管理ルールに基づいて作成していること。
(4) 変更の責任者を定めていること。
(5) 変更管理ルール及び変更手順を関係者に周知徹底していること。
(6) 変更管理ルール及び変更用手順を見直していること。

3 関連事項

(1) 変更管理ルールの項目の例
　① 総則
　　a．目的
　　b．適用範囲
　　c．基本方針
　　d．システム変更責任者
　　e．システム変更責任者の任務・権限
　　f．システム変更担当者
　　g．システム変更担当者の任務
　　h．エスカレーションルール
　　i．機密保持
　　j．ルールの改廃及び周知徹底
　② システム変更の管理
　　a．開発時のシステム変更管理
　　b．運用時のシステム変更管理
　　c．システム更新管理

d．システムバックアップ管理
e．システム障害監視　等

③ セキュリティ管理
a．変更のアクセス管理
b．変更時のバックアップ媒体管理
c．変更に関係するネットワーク障害対策　等

(2) 変更管理ルールと変更手順

変更管理ルールは、情報システムの変更を安全で効率的に実施するために定める変更関係者が遵守しなければならない基本原則をまとめたものである。

変更手順は変更管理ルールに基づき、インフラストラクチャや各運用システムが円滑かつ効率的に変更できるよう具体的に定めた操作手順である。変更に携わる者は、事前に変更管理ルール及び変更手順の教育を受けていなければならない。

変更が契約によって委託されている場合は、「VI. 共通業務　5. 委託・受託」を参照。

(3) 変更管理の責任者

変更管理の責任者は、変更管理ルールと変更手順を承認するだけではなく、その変更手順に従って実際にシステム変更を実施する要員を統括管理する責任者であり、対象となるインフラストラクチャや変更するシステムの内容について精通し、決定権を有する者を指す。開発時点での変更は開発の責任者が変更管理の責任者であるが、既に稼動している場合は不正な変更を阻止するために、変更管理の責任者、担当者は運用責任者、担当者と原則異なることが求められる。保守責任者がいる場合は保守責任者が変更管理責任者となる。

(4) 周知徹底すべき関係者

① 情報システム部員
② 各運用担当者
③ 保守責任者、担当者
④ 開発プロジェクトの責任者
⑤ コールセンターの責任者、担当者
⑥ 委託先　等
⑦ 情報システムの利用者　等

(5) 変更管理のレビュー

変更が行われると、ユーザが本来求めていた機能や導入の効果に影響を与える可能性がある。変更管理に当たっては、本来の機能、変更点、変更後の機能、本来機能からの差異等が明確にされ、記録されている必要がある。変更に関しては、ユーザ、開発、運用、保守の担当者等にレビューが適切に行われ、管理される必要がある。

6．変更管理

6．1　管理

(2) 仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。

1 主　旨

仕様変更、問題点、ペンディング事項等の変更管理案件は、情報システムの円滑な運用を妨げないように、変更の対象となるシステムだけではなく、他のシステムへの影響も考慮して対処方法を決定する必要がある。

2 着 眼 点

(1) 他のシステムに与える影響を考慮していること。

(2) 変更管理ルールに基づいて処理していること。

3 関連事項

(1) 変更管理ルールを定める上での留意点

① 変更の依頼の管理と承認

a．変更依頼の進捗管理

b．処理依頼の内容の分類とリスク評価

c．他のシステムへの影響調査

d．ジョブスケジュールの策定（業務の優先度の設定）

e．確認テストの実施と結果の承認

f．重要な変更についての経営者層への報告　等

② 変更時の留意点

a．開発段階から運用段階への引継ぎの管理

b．ソフトウェアのバージョン管理

c．ジョブスケジュールの管理

d．バックアップの取得と回復手順

e．プログラムの配布手続

f．障害時の具体的な対策　等

6．変更管理

6．1　管理

(3) 変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。

1 主　旨

変更管理案件は、組織体の業務上、必要な変更が適時に実施されるように、提案から完了までの進捗状況を管理し、未完了案件は定期的に分析する必要がある。

2 着 眼 点

(1) 変更管理ルールを作成していること。

(2) 変更管理ルールに基づいて進捗管理を実施していること。

3 関連事項

(1) 変更管理案件の進捗管理

① 進捗管理

a．変更申請受領日を記録すること。

b．変更申請の審査を適時に実施すること。

c．一定期間以上、審査されない案件は、エスカレーション規定によって、上司に報告すること。

d．変更内容のリスク評価、レベル、種類分けの基準を明確にすること。

e．承認の手続、権限者を明確にすること。

f．審査開始日、終了日を記録すること。

g．審査結果についてはその変更の可否と理由を明確に記録すること。

h．審査結果は直ちに申請者に通知すること。

i．変更作業の開始日、終了日を記録すること。

j．緊急に必要な変更は、事後的にフォローすること。

② 定期的な未了案件の管理

a．定期的に未了案件を抽出すること。

b．一定期間以上の未了案件はその理由を確認すること。

c．一定期間以上、処理されない案件は廃案も含めて必ず処理すること。

d．予算措置等の検討が必要な案件は経営者層に報告すること。

e．要員不足等、改善を必要とする理由で未了案件が発生する場合は、改善策を検討すること。

6．変更管理

6．2　実施

(1) 変更管理案件は、変更管理ルールに従って実施すること。

1 主　旨

変更管理案件は、変更管理を円滑にかつ安全に実施するために変更管理ルールに従って実行する必要がある。

2 着 眼 点

(1) 変更管理ルールを作成していること。

(2) 変更管理の具体的なスケジュールを作成していること。

3 関連事項

(1) 変更管理案件の例

変更管理案件はいくつかの種類に分類し、そのリスクや優先順位を検討することになる。

① プログラムの基本的な変更を要請しないもの

a．画面出力を可能にする依頼

b．画面文字の大きさの変更

c．路線バス料金計算表の変更登録　等

② プログラム変更を要請するもの

a．計算ロジックの変更

b．処理手順の変更

c．セキュリティ方式の変更

d．ネットワークの変更　等

③ 他のシステムと関係する変更

a．原価計算システムと繋がる勤怠管理システムの変更

b．購買管理システムと連動する支払管理システムの変更

c．共通コードの桁数の変更

d．取引先のシステム変更に伴うシステムの変更　等

(2) 変更管理ルールのリスク評価と優先順位

① リスク評価

以下の点を考慮して評価する。

a．開発の方針を大きく変更するものか。

b．他のシステムに影響するか。

c．プログラム上いくつかの関連部分の変更も必要か。

d．システムの運用に大きな変更を及ぼさないか。

e．変更によってセキュリティのレベルに変更はないか。 等

② 優先順位

a．業務上の緊急度・重要度

b．すぐに変更可能な小規模な変更

c．予算措置が必要なものか。 等

6．変更管理

6．2　実施

(2) 変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。

1 主　旨

変更管理案件を実施する際には、変更によるシステムトラブル等を避け、変更を効率よく実施するため、関連する情報システムの環境も同時に変更する必要がある。

2 着 眼 点

(1) 変更管理ルール及び変更スケジュールを制定していること。

(2) 変更管理案件の規模、システム特性等を確認していること。

3 関連事項

(1) 変更スケジュールの項目の例

① 変更の制定項目の例

a．変更の責任と体制……責任者の設置、目的、責任と権限、変更体制等

b．変更手続……変更日時、処理依頼、ユーザ ID 取得等

c．変更スケジュール……変更日時、変更手順等

d．バックアップ体制……バックアップデータの保管等

e．変更のテスト……ユーザ、開発者、変更の責任者等

f．変更の承認……ユーザ、開発、運用、保守の責任者等

g．廃棄……「Ⅴ．保守業務　6. 情報システムの廃棄」を参照

h．変更の記録……ソフトウェアのバージョン管理等

(2) 変更の項目・内容は、前項を参照。

6．変更管理

6．2　実施

(3) 変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。

1 主　旨

変更の結果が、変更依頼どおりに実施されたことを確認し、ユーザ、開発、運用及び保守の責任者が承認する必要がある。

2 着 眼 点

(1) 変更のテストを実施していること。

(2) 変更管理ルールで変更管理の役割と責任を決めていること。

(3) 変更の担当責任者を決めていること。

3 関連事項

(1) 担当責任者の例

① 開発プロジェクト責任者

② 変更管理担当責任者

③ ハードウェア担当責任者（サーバ、基本 OS を含む）

④ 各アプリケーション別担当責任者

⑤ ネットワーク担当責任者　等

7．災害対策

7．1　リスク分析

(1) 地震等のリスク及び情報システムに与える影響範囲を明確にすること。

1 主　旨

災害時及びテロによる破壊行為発生時の情報システムの対応策を具体化するため、地震、洪水、テロ等のリスク及び情報システムに与える影響範囲を明確にする必要がある。

2 着眼点

(1) 自然災害は、すべて想定するとともに、テロ等による破壊も含めていること。
(2) 被災の規模は、最大規模を想定していること。
(3) 被災の想定は、地理的、組織的、物理的及び業務的視点から検証していること。
(4) 想定した影響範囲について、将来を考慮していること。

3 関連事項

(1) 災害の定義と想定規模

自然災害としては、地震、台風、豪雨、豪雪、暴風、竜巻、洪水、高潮等を想定し、これらを原因とする火災、水害、断水、停電、破壊、通信途絶、交通遮断、要員不足等を含むこと。また、テロ等による破壊行為も含めること。

言い換えると機器故障等によるシステム障害は、ここでいう災害には含まれない。災害の規模は、最大級（例えば、地震の場合は、震度７レベル）のものを含むことを想定している。

(2) 被災想定時の考慮点

① 地理的／組織的……社内（本店、支店、営業所、工場、研究所、バックアップセンター、海外拠点等）
　　社外（顧客、取引業者、金融機関等）
② 物理的……ハードウェア、ネットワーク、建物、マシン室及びデータ等保管室、電源室及び空気調和機械室、電源設備、空気調和設備、監視制御設備等
③ 業務的……停止又は機能縮退業務の内容

(3) リスク分析の手段

(4) 将来を考慮した影響範囲の検討の例

① 地理的／組織的……支店、営業所の新設、変更予定等
② 物理的……ネットワーク、ハードウェア及び関連設備の新設、変更予定等
③ 業務的……業務内容の新設あるいは変更に伴う情報システム機能及びデータの

変更等

なお、「将来を考慮する」という時間的幅の例としては、「次回見直しのタイミングまで」がある。

7．災害対策

7．1　リスク分析

(2) 情報システムの停止等により組織体が被る損失を分析すること。

1 主　旨

被災の程度に応じた業務の復旧の重要性及び緊急性を明確にするため、情報システムの停止等によって組織体が被る損失を分析する必要がある。

2 着 眼 点

(1) 情報システムの停止及び機能縮退によって組織体が被る損失を分析する対象範囲には、影響を受ける業務を網羅していること。

(2) 損失の分析は、組織体の損害及び社会的損害を明確にしていること。

(3) 業務の復旧の重要性及び緊急性を明確にしていること。

3 関連事項

(1) 損失の分析に当たっての留意事項

① 組織体の損害：販売機会損失、顧客サービスの低減、信用低下等

② 社会的損害　：取引先の損害（部品、材料受入れ不能、製品／サービスの未納入等）
空港、鉄道、銀行、医療機関等については、社会的混乱も考慮すること。

③ 損害額の算出：算出に当たっては、災害による直接的な損失金額だけでなく、バックアップ、代替処理、復旧に必要な費用も含める必要がある。

(2) 損失から保護する対象：情報システムの観点から

① 直接的保護対象：要員、ソフトウェア、ハードウェア、データ等

② 波及的保護対象：人命、資源、プライバシー、生活の利便性、個人及び企業の経済的利益、社会及び経済の安定的運用等

7．災害対策

7．1　リスク分析

(3) 業務の回復許容時間及び回復優先順位を定めること。

1 主　旨

被災による業務の停止及び影響を最小限にとどめ、効率的に復旧するため、業務の回復許容時間及び回復優先順位を定める必要がある。

2 着 眼 点

(1) 回復許容時間及び回復優先順位の設定は、業務の重要性、緊急性、影響範囲及び他の業務との整合性並びに実現可能性を考慮していること。

(2) 回復許容時間及び回復優先順位の設定理由を明確にしていること。

(3) 回復許容時間及び回復優先順位を関係者が合意していること。

3 関連事項

(1) 回復許容時間及び回復優先順位の設定に当たっての考慮点

① 関連する部門及び業務すべてについて、事前に内容を十分に把握しておくこと。

② 業務についての要件（例えば、回復期限として「月末」）を明確にすること。

なお、想定しているリスク及び程度、業務への影響度、あるいは組織体のおかれている経営環境、社会的立場等、設定内容は異なる。

③ 各要件だけでなく、バックアップ、復旧の実現可能性も勘案すること。

④ 要員、予算等の制約も併せて、実現可能性を検討すること。

(2) 回復許容時間及び回復優先順位の設定方法

① 業務停止期間別（１時間、半日、１日、１週間等）の損害額算定等を行い設定する。

7．災害対策

7．2　災害時対応計画

(1) リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。

1 主　旨

災害時に混乱することなく、適切な措置を迅速に確実に実行するため、事業継続計画と整合した災害時対応計画を策定する必要がある。

2 着眼点

(1) 災害時対応計画の策定ルールを明文化していること。

(2) 災害時対応計画は、事業継続計画と整合していること。

(3) 災害時対応計画は、バックアップ、代替処理対策、復旧対策等を記載していること。

(4) 将来の経営環境及び業務の変化を考慮していること。

3 関連事項

(1) 災害時対応計画の内容の例

「情報システム部門」の災害時対応計画の内容例

なお、「各ユーザ部門」においても類似の災害時対応計画が必要となる。

① 情報システム災害対策基本方針

（「全社災害対策基本方針」を受けた情報システムに関する基本方針）

② 想定被災の種類とレベル設定

（想定した被災の種類、被災の程度、影響の範囲から対応策のレベルを設定する）

③ レベル別対応策

③－1 レベル1（例えば、震度7の地震を想定し、その被災程度は本社の完全業務停止を想定）

a．基本行動指針

・災害時発生行動指針

・初期対応行動指針

・代替処理行動指針

・復旧処理時行動指針

b．連絡先・連絡手段

c．体制・役割分担

d．災害発生時行動手順

e．初期対応行動手順

f．バックアップ対象と手順

g．代替処理行動手順

h．復旧処理時行動手順　等

③－２　レベル２　等

④　定期訓練実施方法

⑤　災害時対応計画見直しルール　等

⑥　参考資料

a．想定災害の種類とリスク分析結果

b．全社災害対策基本方針

(2) 事業継続計画との整合性確保の留意点

①　災害時対応計画は、事業継続計画の方針を踏まえて策定すること。

②　災害時対応計画の訓練の実施については、事業継続計画における従業員の教育訓練の方針と整合していること。

③　事業継続計画を見直した場合、災害時対応計画の見直しも検討すること。

なお、事業継続計画の詳細については、「Ⅰ．情報戦略　5. 事業継続計画」を参照。

7．災害対策

7．2　災害時対応計画

(2) 災害時対応計画は、組織体の長が承認すること。

1 主　旨

災害発生時に混乱することなく、適切な措置が迅速に確実に実行されるため、災害時対応計画は組織体の長が承認し、関係者に周知徹底する必要がある。

2 着 眼 点

(1) 災害時対応計画を組織体の長が承認していること。

(2) 災害時対応計画を関係者に周知徹底していること。

3 関連事項

(1) 組織体の長の承認

① 計画内容は、その影響が広範多岐にわたるため、より高度な判断を要し、承認行為にはより重要な配慮が必要である。

② 投資規模あるいは影響の及ぶ範囲による承認レベルの設定（例えば、地方の工場では工場長）も考えられる。

③ 各ユーザ部門の了解を得て、最終的には組織体の長が承認する必要がある。

(2) 周知徹底すべき関係者

関係者には、組織体内のすべての担当者のみならず、関係する外部（例えば、取引先等）の担当者も含まれるので、それぞれ必要な事項を知らしめる必要がある。

7．災害対策

7．2　災害時対応計画

(3) 災害時対応計画の実現可能性を確認すること。

1 主　旨

被災の程度に応じて業務の継続性を確保し、確実に復旧するため、災害時対応計画の実現可能性を確認する必要がある。

2 着 眼 点

(1) 実現可能性を検証する計画を策定していること。

(2) 検証する計画は、被災の程度に応じた内容となっていること。

(3) 検証結果を記録し、災害時対応計画に反映していること。

3 関連事項

(1) 検証計画の要件

① （被災の程度に応じた）目的・範囲・対象

② スケジュール……期間・頻度

③ 予算……見積方法・金額

④ 体制……能力・人数

⑤ 設備……能力・代替設備　等

(2) 検証の実施

災害時対応計画の検証は、その主要構成要素である「バックアップ」、「代替処理」及び「復旧処理」の検証によって実施される。

具体的な内容は、「VI．共通業務　7.災害対策　7.3バックアップ」、「VI．共通業務　7.災害対策　7.4代替処理・復旧」を参照。

災害対策を委託契約によって行っている場合は、「IV．共通業務　5.委託・受託」を参照。

7．災害対策

7．2　災害時対応計画

(4) 災害時対応計画は、従業員の教育訓練の方針を明確にすること。

1 主　旨

災害時対応計画に定めた具体策を習熟し、確実に実行するため、従業員の教育訓練の方針を明確にし、災害時対応計画に基づいた教育訓練を定期的に行う必要がある。

2 着 眼 点

(1) 災害時対応計画に基づいて、教育訓練の方針を明確にしていること。

(2) 教育訓練の方針を踏まえた教育訓練計画を策定していること。

3 関連事項

(1) 教育訓練の方針、教育訓練計画の必要性

災害時対応計画の実践者は、組織体の従業員であるが、災害発生の特殊性から、OJT は機能しない。したがって、災害時対応計画を有効に機能させるためには、災害時を想定した教育訓練が重要であり、教育訓練の方針を明確にした計画を策定し、実施する必要がある。

(2) 教育訓練計画の内容の例

① 基本方針・目的

② 範囲

③ 対象者

④ 情報システム部門の対策と手順

⑤ 各ユーザ部門の対策と手順

⑥ 災害時連絡及び指揮命令体制　等

7．災害対策

7．2　災害時対応計画

(5) 災害時対応計画は、関係各部に周知徹底すること。

1 主　旨

災害時対応計画に定めた具体策を習熟し、確実に実行するため、災害時対応計画に基づいて、教育訓練を実施し、関係各部に周知徹底する必要がある。

2 着 眼 点

(1) 災害時対応計画に基づいて、教育訓練を定期的に実施していること。

(2) 教育訓練の結果を記録し、災害時対応計画に反映していること。

3 関連事項

(1) 教育訓練の定期的な実施

定期的な教育訓練を実施するのは、「人」の混乱を少なくし確実に活動させるためであるので、訓練のインターバルは長すぎては効果が少なく、また短すぎては、通常の業務に支障をきたす。したがって、妥当性のある期間（通常は、半年から１年）を設定する必要がある。

(2) 教育訓練結果の内容の例

原則として、教育訓練計画の内容に対応させること。

① 基本方針・目的

② 範囲

③ 対象者

④ 情報システム部門の対策と手順の問題点と改善策

⑤ 各ユーザ部門の対策と手順の問題点と改善策

⑥ 災害時連絡及び指揮命令体制の問題点と改善策　等

7．災害対策

7．2　災害時対応計画

(6) 災害時対応計画は、必要に応じて見直すこと。

1 主　旨

災害時対応計画は、経営環境及び業務の変化等に対応して、実現可能性を保持するため、適時に見直しを行う必要がある。

2 着 眼 点

(1) 見直しのルールを明文化していること。

(2) 見直しによる変更は、理由が明確であること。

(3) 変更した計画を組織体の長が承認し、関係者に周知徹底していること。

3 関連事項

(1) 計画見直しの時期

① 長期／短期計画の策定あるいは見直しの時期

② 新規システム／更改システムの稼動前

③ 定期的な訓練後

④ 検証計画の実施後　等

(2) 見直しの理由の例

① 他社事例の実例研究結果

② 経営環境の変化

a．業務のニーズ

b．業界動向

c．政策／基準の動向

③ 経営方針の変化

④ 情報処理技術の動向

⑤ 定期的訓練の結果に基づいた不具合発見

⑥ 検証計画の実施結果に基づいた不具合発見

⑦ 実際に発生した災害による教訓　等

7．災害対策

7．3　バックアップ

(1) 情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。

1 主　旨

復旧作業の効率及び経済性を考慮して、確実に回復させるため、業務の回復目標に対応して、バックアップ方法及び手順を定める必要がある。

2 着眼点

(1) 業務別にバックアップの対象を明確にし、関連業務のバックアップとの整合を図っていること。

(2) 業務の回復許容時間及び回復優先順位に対応して、バックアップ方法及び手順を定めていること。

(3) バックアップの要員及び予算を確保していること。

3 関連事項

(1)　回復目標

回復目標には、回復許容時間及び回復優先順位等があり、業務停止期間別の損害額算定等を行い設定する。

(2)　バックアップの対象

①　災害時にバックアップのための建物及び室を設置する場合は、遠隔地に設置すること。

②　災害時にバックアップのための情報システムを設置する場合は、遠隔地に設置すること。

③　記録媒体の分散保管は、集中、分散処理の形態に応じて行うこと。

④　データ等のバックアップを行うこと。

（以上、経済産業省「情報システム安全対策基準」より抜粋）

(3) バックアップ方法の例

バックアップ方法については、次の事項に関して関係各部門、回復優先順位、回復許容時間、費用対効果等を勘案し、選定することが望ましい。

①　情報システムのバックアップ方法の例

a．ミラーサイト（平常時からまったく同じシステムを同時に稼動させておく。）

b．ホットサイト（まったく同じシステムをインストールしておき、短時間の切替え、稼動を可能にしておく。）

c．コールドサイト（必要な場合に限り、設備を借りてハードウェアを搬入し、処理を継続可能にしておく。）

d．モービルユニット（ハードウェア・通信設備等一式が用意されており、トレーラ等で移動する仮設センター） 等

なお、障害等のためのバックアップの方法も、被災の程度に応じて利用することも考える必要がある。これについては、「Ⅳ. 運用業務 4.データ管理(5)」及び「Ⅳ. 運用業務 6. ソフトウェア管理(4)」を参照。

② バックアップ媒体の例

a．磁気テープ（MT、CMT、CGMT、DAT 等）

b．磁気ディスク（MO、CD-R、FD 等）

③ システム回線の例

a．回線の二重化

b．専用回線の設置 等

7．災害対策

7．3　バックアップ

(2) 運用の責任者は、バックアップ方法及び手順を検証すること。

1 主　旨

定められたバックアップ方法及び手順の実現可能性を確認するため、運用の責任者は、バックアップ方法及び手順を検証する必要がある。

2 着 眼 点

(1) 実現可能性を検証する計画を策定していること。

(2) 検証結果を記録し、バックアップ方法及び手順に反映していること。

3 関連事項

(1) 検証計画の内容の例

災害発生時にあらかじめ定めたバックアップ方法及び手順が有効に機能するかを確認するための計画であり、環境変化等によってバックアップ方法及び手順を見直した場合等にも実施する。

① 目的

② 対象範囲

③ 実施時期と頻度

④ 実施体制と役割分担

⑤ バックアップ対象と手順　等

(2) 検証方法の例

① 計画に対する検証の場合

a．バックアップ目標時間と実績値の比較

b．計画した要員体制と実績値の比較

c．計画した予算額と実績値の比較　等

② データの検証の場合

a．バックアップデータと元データの突合

b．復元されたデータと元データの突合

c．一定期間保管されたデータの復元テスト　等

(3) 検証結果の内容の例

原則として、検証計画の項目に対応した内容となる。

① 目的

② 対象範囲と反省点

③ 実施時期と反省点
④ 実施体制と役割分担の問題点と改善点
⑤ バックアップ対象及び手順の問題点と改善点　等

(4) 検証の実施上の留意点
① 検証においても、時間・予算・要員を確保し、組織体の長の承認を得る必要がある。
② 検証の実施に当たっては、必要に応じて関連部門のユーザも加えること。
③ 検証の実施によって、運用担当者の訓練もできるように配慮すること。

7．災害対策

7．4　代替処理・復旧

(1) ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。

1 主　旨

停止した情報システムを復旧するまでの間、業務を継続するため、代替処理手続及び体制を定める必要がある。また、その実現可能性を確認するため、ユーザ及び運用の責任者が検証する必要がある。

2 着 眼 点

(1) 業務の回復許容時間及び回復優先順位に対応して、代替処理手続及び体制の必要な業務を明確にしていること。

(2) 代替処理の要員及び予算を確保していること。

(3) 代替処理の責任者及び指揮命令系統を明確にしていること。

(4) 実現可能性を検証する計画を策定していること。

(5) 検証結果を記録し、代替処理手続及び体制に反映していること。

3 関連事項

(1) 代替処理手続の必要性

すべての業務に代替処理手続を設定する必要はなく、業務の特性を見て判断する必要がある。例えば、1両日中に日次の受注処理が復旧できずに代替処理手続の必要性があるとした場合でも、月末締めの処理は、月末までに復旧すれば締め処理自体の代替処理手続は必要ない。

(2) 代替処理手続及び体制に当たっての留意点

① 被災の程度によって異なるが、マニュアル処理手続が基本であるが、データ量や利便性等によっては、代替処理システムとしてPCによるシステムを構築すること等も考慮する。

② 外部委託やバックアップセンターが可能な場合は、マニュアル処理手続は、適用する必要はない。

③ 被災地域以外の情報システムの利用や、応援要員の確保も考慮する。

④ ソフトウェア、ハードウェア、ネットワーク及び関連設備等の開発・製造、あるいは納入業者との連携をとっていること。

(3) 検証計画の内容の例

災害発生時にあらかじめ定めた復旧までの代替処理手続及び体制が有効に機能するかを確認するための計画であり、環境変化等によって復旧までの代替処理手続及び体制を見直した場合等にも実施する必要がある。

① 目的
② 対象範囲
③ 実施時期と頻度
④ 実施体制と役割分担
⑤ 代替処理手続　等

(4) 検証結果の内容の例

原則として、検証計画の項目に対応した内容となる。

① 目的
② 対象範囲と反省点
③ 実施時期と反省点
④ 実施体制と役割分担の問題点と改善点
⑤ 代替処理手続の問題点と改善点　等

(5) 検証の実施上の留意点

① 検証においても、時間・予算・要員を確保し、組織体の長の承認を得る必要がある。
② 検証の実施に当たっては、関連部門のユーザも参画することが重要である。

7．災害対策

7．4　代替処理・復旧

(2) ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。

1 主　旨

停止した情報システムを円滑かつ確実に復旧するため、復旧までの手続及び体制を定める必要がある。また、その実現可能性を確認するため、ユーザ及び運用の責任者が検証する必要がある。

2 着 眼 点

(1) 業務の回復許容時間及び回復優先順位に対応して、復旧処理手続及び体制を定めていること。

(2) 復旧の進捗状況を関係者に周知徹底する体制を定めていること。

(3) 復旧の要員及び予算を確保していること。

(4) 実現可能性を検証する計画を策定していること。

(5) 検証結果を記録し、復旧手続及び体制に反映していること。

3 関連事項

(1) 復旧手続及び体制

① 代替処理要員、復旧要員及び移行要員の連絡体制を確立する必要がある。

② 復旧後の各システム間のデータの整合性を確保するため、システムの相互関連性を考慮しながら、復旧順序を検討する必要がある。

③ 代替処理したデータを復旧後の情報システムへ取り込む方法を定めていること。

④ 全体復旧後、システム間の整合性を検証することが重要である。

(2) 検証計画の内容の例

災害発生時にあらかじめ定めた復旧処理手続及び体制が有効に機能するかを確認するための計画であり、環境変化等によって、復旧処理手続及び体制を見直した場合等にも実施する必要がある。

① 目的

② 対象範囲

③ 実施時期と頻度

④ 実施体制と役割分担

⑤ 復旧手続

⑥ 整合性の確認方法　等

(3) 検証結果の内容の例

原則として、検証計画の項目に対応した内容となる。

① 目的
② 対象範囲と反省点
③ 実施時期と反省点
④ 実施体制と役割分担の問題点と改善点
⑤ 復旧手続の問題点と改善点
⑥ 整合性の確認方法の問題点と改善点　等

(4) 実施上の留意点
① 検証においても、時間・予算・要員を確保し、組織体の長の承認を得る必要がある。
② 検証の実施に当たっては、関連部門のユーザも参画することが重要である。

参　　考

1. システム管理基準とCOBIT-Ⅲとの比較表
2. システム管理基準と他基準との比較表

1. システム管理基準とCOBIT-Ⅲとの比較表

大項目	中項目	小項目	管理項目	PO1 戦略的IT計画の定義	PO2 情報アーキテクチャの定義	PO3 技術指針の決定	PO4 ITの組織とそのかかわりの定義	PO5 IT投資の管理	PO6 マネジメントの意図と指針の周知	PO7 人的資源の管理	PO8 外部要求事項の遵守の保証	PO9 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI1 コンピュータ化対応策の明確化	AI2 アプリケーションソフトウエアの調達と保守	AI3 技術インフラの調達と保守	AI4 機作、運用手続の作成と維持	AI5 システムの導入と受入信認	AI6 変更管理	DS1 サービスレベルの定義と管理	DS2 サードパーティのサービスの管理	DS3 成果と能力（キャパシティ）の管理	DS4 継続的なサービスの保証	DS5 システムセキュリティの保証	DS6 コストの捕捉と配賦	DS7 利用者の教育と研修	DS8 利用者に対する支援と助言	DS9 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M1 プロセスのモニタリング	M2 内部統制の十分性の評価	M3 独立した第三者の保証の獲得	M4 独立監査の実施
1. 情報戦略	01. 全体最適化	1.1 全体最適化の方針・目標	(01)ITガバナンスの方針を明確にすること。	1																															
			(02)情報化投資及び情報化構想の決定における原則を定めること。	1																															
			(03)情報システム全体の最適化目標を経営戦略に基づいて設定すること。	1																															
			(04)組織体全体の情報システムのあるべき姿を明確にすること。		1		1																													
			(05)システム化によって生ずる組織及び業務の変更の方針を明確にすること。				1																													
			(06)情報セキュリティ基本方針を明確にすること。						1																											
		1.2 全体最適化計画の承認	(01)全体最適化計画の立案体制は、組織体の長の承認を得ること。				1																													
			(02)全体最適化計画は、組織体の長の承認を得ること。				1																													
			(03)全体最適化計画は、利害関係者の合意を得ること。				1																													
		1.3 全体最適化計画の策定	(01)全体最適化計画は、方針及び目標に基づいていること。	1	1																														
			(02)全体最適化計画は、コンプライアンスを考慮すること。								1																								1	1
			(03)全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。					1																												
			(04)全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。					1																												
			(05)全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。											1																						
			(06)全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。	1																															
			(07)全体最適化計画は、外部資源の活用を考慮すること。				1																													
		1.4 全体最適化計画の運用	(01)全体最適化計画は、関係者に周知徹底すること。						1																											
			(02)全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。	1																															
	02. 組織体制	2.1 情報システム化委員会	(01)全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。				1																													

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
I．情報戦略	02. 組織体制	2.1 情報システム化委員会	(02)委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。				1																										1		
			(03)委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。			1																													
			(04)委員会は、活動内容を組織体の長に報告すること。				1																												
			(05)委員会は、意思決定を支援するための情報を組織体の長に提供すること。				1																												
		2.2 情報システム部門	(01)情報システム部門の使命を明確にし、適切な権限及び責任を与えること。				1																												
			(02)情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。				1																												
		2.3 人的資源管理の方針	(01)情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。				1																												
			(02)人的資源の調達及び育成の方針を明確にすること。				1																												
	03. 情報化投資	(空白)	(01)情報化投資計画は、経営戦略との整合性を考慮して策定すること。					1																												
			(02)情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。					1																												
			(03)情報化投資に関する予算を適切に執行すること。					1																												
			(04)情報化投資に関する投資効果の算出方法を明確にすること。					1																												
			(05)情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。					1																												
			(06)投資した費用が適正に使用されたことを確認すること。					1																			1									
	04. 情報資産管理の	(空白)	(01)情報資産の管理方針及び体制を明確にすること。				1																												
			(02)情報資産のリスク分析を行い、その対応策を考慮すること。									1																								
			(03)情報資産の効率的で有効な活用を考慮すること。						1																											

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作・運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
I. 情報戦略	04. 情報資産管理の	(空白)	(04)情報資産の共有化による生産性向上を考慮すること。						1																										
	05. 事業継続計画	(空白)	(01)情報システムに関連した事業継続の方針を策定すること。																				1											
			(02)事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。																				1											
			(03)事業継続計画は、従業員の教育訓練の方針を明確にすること。																				1											
			(04)事業継続計画は、関係各部に周知徹底すること。																					1										
			(05)事業継続計画は、必要に応じて見直すこと。																					1										
	06. コンプライアンス	(空白)	(01)法令及び規範の管理体制を確立するとともに、管理責任者を定めること。								1																								
			(02)遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。								1																								
			(03)情報倫理規程を定め、関係者に教育及び周知徹底すること。								1																								
			(04)個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めること。								1																								
			(05)法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。								1																								
II. 企画業務	01. 開発計画	(空白)	(01)開発計画は、組織体の長が承認すること。	1																														
			(02)開発計画は、全体最適化計画との整合性を考慮して策定すること。	1																														
			(03)開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。	1																														
			(04)開発計画は、関係者の教育及び訓練計画を明確にすること。							1																								
			(05)開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。				1																											
			(06)開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。					1																			1								

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
Ⅱ. 企画業務	01. 開発計画	(空白)	(07)開発計画はシステムライフを設定する条件を明確にすること。										1																						
			(08)開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。												1																				
			(09)開発計画の策定に当たっては、情報システムの目的を遂成する実現可能な代替案を作成し、検討すること。												1																				
	02. 分析	(空白)	(01)開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。												1																				
			(02)ユーザニーズの調査は、対象、範囲及び方法を明確にすること。												1																				
			(03)実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。												1																				
			(04)ユーザニーズは文書化し、ユーザ部門が確認すること。													1																				
			(05)情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。												1																				
			(06)情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。												1																				
			(07)情報システムの導入効果の定量的及び定性的評価を行うこと。												1																				
			(08)パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。													1																				
	03. 調達	(空白)	(01)調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。													1																				
			(02)ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。														1																				
			(03)開発を遂行するために必要な要員、予算、設備、期間等を確保すること。			1																														
			(04)要員に必要なスキルを明確にすること。			1																														
			(05)ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。														1																				

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
Ⅱ. 企画業務	03. 調達	(空白)	(06)調達した資源は、ルールに従って管理すること。														1																			
Ⅲ. 開発業務	01. 開発手順	(空白)	(01)開発手順は、開発の責任者が承認すること。													1																			
			(02)開発手順は、開発方法に基づいて作成すること。											1																					
			(03)開発手順は、開発の規模、システム特性等を考慮して決定すること。											1																					
			(04)開発時のリスクを評価し、必要な対応策を講じること。												1																				
	02. システム設計	(空白)	(01)システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。													1																			
			(02)運用及び保守の基本方針を定めて設計すること。													1																			
			(03)入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。													1																			
			(04)データベースは、業務の内容及びシステム特性に応じて設計すること。		1											1																			
			(05)データのインテグリティを確保すること。																												1				
			(06)ネットワークは、業務の内容及びシステム特性に応じて設計すること。														1																		
			(07)情報システムの性能は、要求定義を満たすこと。											1																					
			(08)情報システムの運用性及び保守性を考慮して設計すること。												1									1											
			(09)他の情報システムとの整合性を考慮して設計すること。													1																			
			(10)情報システムの障害対策を考慮して設計すること。																						1										
			(11)誤謬防止、不正防止、機密保護等を考慮して設計すること。																						1										
			(12)テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。																1																
			(13)情報システムの利用に係る教育の方針、スケジュール等を明確にすること。																1																
			(14)モニタリング機能を考慮して設計すること。																					1											
			(15)システム設計書をレビューすること。											1																					
	03. プログラム設計	(空白)	(01)プログラム設計書は、開発の責任者が承認すること。													1																			
			(02)システム設計書に基づいて、プログラムを設計すること。													1																			

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入認証	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
III. 開発業務	03. プログラム設計	(空白)	(03)テスト要求事項を定義し、文書化すること。													1																				
			(04)プログラム設計書及びテスト要求事項をレビューすること。											1																						
			(05)プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。													1																				
	04. プログラミング	(空白)	(01)プログラム設計書に基づいてプログラミングすること。													1																				
			(02)プログラムコードはコーディング標準に適合していること。											1																						
			(03)プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。											1																						
			(04)重要プログラムは、プログラム作成者以外の者がテストすること。											1																						
	05. システムテスト・ユーザ受入れテスト	(空白)	(01)システムテスト計画は、開発及びテストの責任者が承認すること。											1																						
			(02)ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。											1																						
			(03)システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。											1																						
			(04)テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。											1																						
			(05)システムテストは、本番環境と隔離された環境で行うこと。											1																						
			(06)システムテストは、開発当事者以外の者が参画すること。											1																						
			(07)システムテストは、適切なテスト手法及び標準を使用すること。											1																						
			(08)ユーザ受入れテストは、本番同様の環境を設定すること。																	1																
			(09)ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。																	1																
			(10)ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。																	1																

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入慣認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
Ⅲ. 開発業務	05. システムテスト・ユーザ受入れテスト	(空白)	(11)システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。																1																	
			(12)システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。																1																	
			(13)パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。													1																			
	06. 移行	(空白)	(01)移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。																1																	
			(02)移行作業は文書に記録し、責任者が承認すること。																1																	
			(03)移行完了の検証方法を移行計画で明確にすること。																1																	
			(04)移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。																1																	
			(05)移行は手順書を作成し、実施すること。																1																	
			(06)移行時のリスク対策を検討すること。																1																	
			(07)運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。																1																	
			(08)移行は関係者に周知徹底すること。																1																	
Ⅳ. 運用業務	01. 運用管理ルール	(空白)	(01)運用管理ルール及び運用手順は、運用の責任者が承認すること。															1																		
			(02)運用管理ルールは、運用設計に基づいて作成すること。															1																		
			(03)運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。															1																		
			(04)運用設計及び運用管理ルールに基づいて、担当責任者を定めること。															1																		
	02. 運用管理	(空白)	(01)年間運用計画を策定し、責任者が承認すること。	1																															
			(02)年間運用計画に基づいて、月次、日次等の運用計画を策定すること。																													1				
			(03)運用管理ルールを遵守すること。				1																													
			(04)ジョブスケジュールは、業務処理の優先度を考慮して設定すること。																												1					

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入情認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
Ⅳ. 運用業務	02. 運用管理	(空白)	(05)オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。																												1					
			(06)例外処理のオペレーションは、運用管理ルールに基づいて行うこと。																												1					
			(07)オペレータの交替は、運用管理ルールに基づいて行うこと。																												1					
			(08)ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。																												1					
			(09)オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。																												1					
			(10)事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。																											1						
			(11)事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。																											1						
			(12)事故及び障害の原因を究明し、再発防止の措置を講じること。																											1						
			(13)情報システムのユーザに対する支援体制を確立すること。																										1							
			(14)情報セキュリティに関する教育及び訓練をユーザに対して実施すること。																									1								
			(15)情報システムの稼動に関するモニタリング体制を確立すること。																													1				
			(16)情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。																					1												
	03. 入力管理	(空白)	(01)入力管理ルールを定め、遵守すること。																												1					
			(02)データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。																												1					
			(03)入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。																												1					
			(04)データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。																												1					

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
Ⅳ. 運用業務	03. 入力管理	(空白)	(05)入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。																											1						
	04. データ管理	(空白)	(01)データ管理ルールを定め、遵守すること。																											1						
			(02)データへのアクセスコントロール及びモニタリングは、有効に機能すること。																											1						
			(03)データのインテグリティを維持すること。																											1						
			(04)データの利用状況を記録し、定期的に分析すること。																											1						
			(05)データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。																											1						
			(06)データの授受は、データ管理ルールに基づいて行うこと。																											1						
			(07)データの交換は、不正防止及び機密保護の対策を講じること。																											1						
			(08)データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。																											1						
			(09)データに対するコンピュータウイルス対策を講じること。																											1						
			(10)データの知的財産権を管理すること。																						1												
	05. 出力管理	(空白)	(01)出力管理ルールを定め、遵守すること。																											1						
			(02)出力情報は、漏れなく、重複なく、正確であることを確認すること。																											1						
			(03)出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。																											1						
			(04)出力情報の引渡しは、出力管理ルールに基づいて行うこと。																											1						
			(05)出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。																											1						
			(06)出力情報のエラー状況を記録し、定期的に分析すること。																											1						
			(07)出力情報の利用状況を記録し、定期的に分析すること。																											1						
	06. ソフトウェア管理	(空白)	(01)ソフトウェア管理ルールを定め、遵守すること。																									1								
			(02)ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。																									1								

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	D4 独立監査の実施
IV. 運用業務	06. ソフトウェア管理	(空白)	(03)ソフトウェアの利用状況を記録し、定期的に分析すること。																						1											
			(04)ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。																				1												
			(05)ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。																						1										
			(06)ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。																						1										
			(07)ソフトウェアに対するコンピュータウイルス対策を講じること。																						1										
			(08)ソフトウェアの知的財産権を管理すること。																						1										
			(09)フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。																										1						
	07. ハードウェア管理	(空白)	(01)ハードウェア管理ルールを定め、遵守すること。																				1												
			(02)ハードウェアは、想定されるリスクに対応できる環境に設置すること。																													1			
			(03)ハードウェアは、定期的に保守を行うこと。														1																		
			(04)ハードウェアは、障害対策を講じること。																					1											
			(05)ハードウェアの利用状況を記録し、定期的に分析すること。																				1												
			(06)ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。																							1									
	08. ネットワーク管理	(空白)	(01)ネットワーク管理ルールを定め、遵守すること。																							1									
			(02)ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。																							1									
			(03)ネットワーク監視ログを定期的に分析すること。																								1								
			(04)ネットワークは、障害対策を講じること。																					1											
			(05)ネットワークの利用状況を記録し、定期的に分析すること。																				1												
			(06)ネットワークを利用したサービスについて、組織体としての方針を明確にすること。						1																										

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
Ⅳ. 運用業務	09. 構成管理	(空白)	(01)管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。																										1						
			(02)ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。																	1														
			(03)ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。																						1									
			(04)ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。																						1									
	10. 建物・関連設備管理	(空白)	(01)建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。																												1				
			(02)建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。																												1				
			(03)関連設備は、適切な運用を行うこと。																												1				
			(04)関連設備は、定期的に保守を行うこと。																												1				
			(05)関連設備は、障害対策を講じること。																												1				
			(06)建物及び室への入退の管理を記録し、定期的に分析すること。																												1				
Ⅴ. 保守業務	01. 保守手順	(空白)	(01)保守ルール及び保守手順は、保守の責任者が承認すること。																	1															
			(02)保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。																	1															
			(03)保守時のリスクを評価し、必要な対応策を講じること。																	1															
	02. 保守計画	(空白)	(01)保守計画はユーザ及び保守の責任者が承認すること。																	1															
			(02)変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。																	1															
			(03)保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。																	1															
	03. 保守の実施	(空白)	(01)システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。																	1															
			(02)プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。																	1															

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
V. 保守業務	03. 保守の実施	(空白)	(03)変更したプログラム設計書に基づいてプログラミングしていることを検証すること。																	1															
	04. 保守の確認	(空白)	(01)変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。																	1															
			(02)変更したプログラムは、影響範囲を考慮してテストを行うこと。																	1															
			(03)変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。																	1															
			(04)変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。																	1															
			(05)変更したプログラムのテストの結果を記録及び保管すること。																	1															
	05. 移行	(空白)	(01)移行手順は、移行の条件を考慮して作成すること。																	1															
			(02)変更前のプログラム及びデータのバックアップを行うこと。																	1															
			(03)運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。																	1															
	06. 情報システムの廃棄	(空白)	(01)旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。											1																					
			(02)旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。											1																					
VI. 共通業務	01. ドキュメント管理	1.1 作成	(01)ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。											1																					
			(02)ドキュメント作成ルールを定め、遵守すること。											1																					
			(03)ドキュメントの作成計画を策定すること。											1																					
			(04)ドキュメントの種類、目的、作成方法等を明確にすること。											1																					
			(05)ドキュメントは、作成計画に基づいて作成すること。											1																					
		1.2 管理	(01)ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。											1																					
			(02)ドキュメント管理ルールを定め、遵守すること。											1																					
			(03)情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。											1																					

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入借認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
VI. 共通業務	01. ドキュメント管理	1.2 管理	(04)ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。											1																						
	02. 進捗管理	2.1 実施	(01)進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。										1																						
			(02)ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。										1																						
			(03)進捗の遅延等の対策を講じること。										1																						
		2.2 評価	(01)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。										1																						
			(02)評価結果は、次工程の計画に反映すること。										1																						
			(03)評価結果は、進捗管理の方法、体制等の改善に反映すること。										1																						
	03. 品質管理	3.1 計画	(01)品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。											1																					
			(02)品質管理計画は、方法、体制等を明確にすること。											1																					
		3.2 実施	(01)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。											1																					
			(02)評価結果は、品質管理の基準、方法、体制等の改善に反映すること。											1																					
	04. 人的資源管理	4.1 責任・権限	(01)要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。							1																									
			(02)要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。							1																									
			(03)要員の責任及び権限を周知徹底すること。							1																									
		4.2 業務遂行	(01)要員は、権限を遵守すること。							1																									
			(02)作業分担及び作業量は、要員の知識、能力等から検討すること。							1																									
			(03)要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。							1																									
			(04)不測の事態に備えた代替要員の確保を検討すること。							1																									

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入確認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
VI. 共通業務	04. 人的資源管理	4.3 教育・訓練	(01)教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。							1																									
			(02)教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。							1																									
			(03)教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。							1																									
			(04)要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。							1																									
		4.4 健康管理	(01)健康管理を考慮した作業環境を整えること。							1																									
			(02)健康診断及びメンタルヘルスケアを行うこと。							1																									
	05. 委託・受託	5.1 計画	(01)委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。																			1													
			(02)委託又は受託の目的、対象範囲、予算、体制等を明確にすること。																			1													
			(03)委託又は受託は、具体的な効果、問題点等を評価して決定すること。																			1													
		5.2 委託先選定	(01)委託先の選定基準を明確にすること。																				1												
			(02)委託候補先に必要な要求仕様を提示すること。																				1												
			(03)委託候補先が提示した提案書の比較検討を行うこと。																				1												
		5.3 契約	(01)契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。																				1												
			(02)コンプライアンスに関する条項を明確にすること。																					1											
			(03)再委託の可否について明確にすること。																					1											
			(04)知的財産権の帰属を明確にすること。																					1											
			(05)特約条項及び免責条項を明確にすること。																					1											
			(06)業務内容及び責任分担を明確にすること。																					1											
			(07)契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。																					1											
			(08)システム監査に関する方針を明確にすること。																						1										
		5.4 委託業務	(01)委託業務の実施内容は、契約内容と一致すること。																						1										

大項目	中項目	小項目	管理項目	PO1 戦略的IT計画の定義	PO2 情報アーキテクチャの定義	PO3 技術指針の決定	PO4 ITの組織とそのかかわりの定義	PO5 IT投資の管理	PO6 マネジメントの意図と指針の周知	PO7 人的資源の管理	PO8 外部要求事項の遵守の保証	PO9 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入認証	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
VI. 共通業務	05. 委託・受託	5.4 委託業務	(02)契約に基づき、必要な要求仕様、データ、資料等を提供すること。																			1														
			(03)委託業務の進捗状況を把握し、遅延対策を講じること。																			1														
			(04)委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。																			1														
			(05)成果物の検収は、委託契約に基づいて行うこと。																			1														
			(06)業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。																			1														
			(07)委託した業務の結果を分析及び評価すること。																			1														
		5.5 受託業務	(01)受託業務の実施内容は、契約内容を遵守すること。																			1														
			(02)受託内容の進捗状況を把握し、リスク対策を講じること。																			1														
			(03)成果物の品質管理を行うこと。																			1														
			(04)契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。																			1														
	06. 変更管理	6.1 管理	(01)変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。																	1																
			(02)仕様変更、問題点、ベンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。																	1																
			(03)変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。																	1																
		6.2 実施	(01)変更管理案件は、変更管理ルールに従って実施すること。																	1																
			(02)変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。																	1																
			(03)変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。																	1																
	07. 災害対策	7.1 リスク分析	(01)地震等のリスク及び情報システムに与える影響範囲を明確にすること。									1																								
			(02)情報システムの停止等により組織体が被る損失を分析すること。									1																								
			(03)業務の回復許容時間及び回復優先順位を定めること。									1																								

大項目	中項目	小項目	管理項目	PO01 戦略的IT計画の定義	PO02 情報アーキテクチャの定義	PO03 技術指針の決定	PO04 ITの組織とそのかかわりの定義	PO05 IT投資の管理	PO06 マネジメントの意図と指針の周知	PO07 人的資源の管理	PO08 外部要求事項の遵守の保証	PO09 リスク評価	PO10 プロジェクト管理	PO11 品質管理	AI01 コンピュータ化対応策の明確化	AI02 アプリケーションソフトウエアの調達と保守	AI03 技術インフラの調達と保守	AI04 操作、運用手続の作成と維持	AI05 システムの導入と受入信認	AI06 変更管理	DS01 サービスレベルの定義と管理	DS02 サードパーティのサービスの管理	DS03 成果と能力（キャパシティ）の管理	DS04 継続的なサービスの保証	DS05 システムセキュリティの保証	DS06 コストの捕捉と配賦	DS07 利用者の教育と研修	DS08 利用者に対する支援と助言	DS09 構成管理	DS10 問題と事故の管理	DS11 データ管理	DS12 設備管理	DS13 オペレーション管理	M01 プロセスのモニタリング	M02 内部統制の十分性の評価	M03 独立した第三者の保証の獲得	M04 独立監査の実施
VI. 共通業務	07. 災害対策	7.2 災害時対応計画	(01)リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。																					1												
			(02)災害時対応計画は、組織体の長が承認すること。																					1												
			(03)災害時対応計画の実現可能性を確認すること。																					1												
			(04)災害時対応計画は、従業員の教育訓練の方針を明確にすること。																					1												
			(05)災害時対応計画は、関係各部に周知徹底すること。																					1												
			(06)災害時対応計画は、必要に応じて見直すこと。																					1												
		7.3 バックアップ	(01)情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。																					1												
			(02)運用の責任者は、バックアップ方法及び手順を検証すること。																					1												
		7.4 代替処理・復旧	(01)ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。																					1												
			(02)ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。																					1												
附則1	(空白)	(空白)	情報セキュリティに関連する項目については、情報セキュリティ管理基準を活用することが望ましい。																						1											
附則2	(空白)	(空白)	その他、関連する基準を活用することが望ましい。								1																									

2. システム管理基準と他基準との比較表

システム管理基準と国際標準化(ISO／IEC15288、ISO／IEC12207)との対応付け

システム管理基準			ISO/IEC 15288:2002(JIS X 0170-2004)		ISO/IEC 12207:1995(JIS X 0160-1996)		
プロセス			プロセス		プロセス		
情報戦略	全体最適化	全体最適化の方針・目的	事業ﾌﾟﾛｾｽ	事業環境ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ(5.3.2)			
情報戦略	全体最適化	全体最適化計画の承認					
情報戦略	全体最適化	全体最適化計画の策定	事業ﾌﾟﾛｾｽ	ｼｽﾃﾑﾗｲﾌｻｲｸﾙﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ(5.3.4)			
情報戦略	全体最適化	全体最適化計画の運用					
情報戦略	組織体制	情報システム化委員会					
情報戦略	組織体制	情報システム部門					
情報戦略	組織体制	人的資源管理の方針	事業ﾌﾟﾛｾｽ	資源ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ			
情報戦略	情報化投資		事業ﾌﾟﾛｾｽ	投資ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ(5.3.3)			
情報戦略	情報資産管理の方針						
情報戦略	事業継続計画						
情報戦略	コンプライアンス						
			事業ﾌﾟﾛｾｽ	品質ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ			
			ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	ﾌﾟﾛｼﾞｪｸﾄ評価ﾌﾟﾛｾｽ			
			ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	ﾘｽｸﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ			
			ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	構成ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ			
			ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	情報ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽ			
企画業務	開発計画		ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	ﾌﾟﾛｼﾞｪｸﾄ計画ﾌﾟﾛｾｽ			
企画業務	分析		技術ﾌﾟﾛｾｽ	利害関係者要求事項明確化ﾌﾟﾛｾｽ	開発ﾌﾟﾛｾｽ	ｼｽﾃﾑ要求分析	
			技術ﾌﾟﾛｾｽ	要求事項分析ﾌﾟﾛｾｽ	開発ﾌﾟﾛｾｽ	ｼｽﾃﾑ方式設計	
					開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ要求分析	
企画業務	調達		ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	意思決定ﾌﾟﾛｾｽ			
開発業務	開発手順		ﾌﾟﾛｼﾞｪｸﾄﾌﾟﾛｾｽ	ﾌﾟﾛｼﾞｪｸﾄ管理ﾌﾟﾛｾｽ			
開発業務	システム設計		技術ﾌﾟﾛｾｽ	ｱｰｷﾃｸﾁｬﾗﾙ設計ﾌﾟﾛｾｽ	開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ方式設計	
開発業務	プログラム設計		技術ﾌﾟﾛｾｽ	ｱｰｷﾃｸﾁｬﾗﾙ設計ﾌﾟﾛｾｽ	開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ詳細設計	
開発業務	プログラミング		技術ﾌﾟﾛｾｽ	実行ﾌﾟﾛｾｽ	開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱｺｰﾄﾞ作成及びﾃｽﾄ	
			技術ﾌﾟﾛｾｽ	統合ﾌﾟﾛｾｽ			
開発業務	システムテスト・ユーザ受入れテスト		技術ﾌﾟﾛｾｽ	検定ﾌﾟﾛｾｽ	開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ結合ﾃｽﾄ	
					開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ適格性確認ﾃｽﾄ	
					開発ﾌﾟﾛｾｽ	ｼｽﾃﾑ結合ﾃｽﾄ	
					開発ﾌﾟﾛｾｽ	ｼｽﾃﾑ適格性確認ﾃｽﾄ	
					運用ﾌﾟﾛｾｽ	運用ﾃｽﾄ	

システム管理基準			ISO/IEC 15288:2002(JIS X 0170-2004)		ISO/IEC 12207:1995(JIS X 0160-1996)		
					開発ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ導入	
開発業務	移行		技術ﾌﾟﾛｾｽ	移行ﾌﾟﾛｾｽ			
			技術ﾌﾟﾛｾｽ	検証ﾌﾟﾛｾｽ			
運用業務	運用管理ルール		技術ﾌﾟﾛｾｽ	運転ﾌﾟﾛｾｽ			
運用業務	運用管理		技術ﾌﾟﾛｾｽ	運転ﾌﾟﾛｾｽ	運用ﾌﾟﾛｾｽ	ｼｽﾃﾑ運用	
運用業務	入力管理						
運用業務	データ管理						
運用業務	出力管理						
運用業務	ソフトウェア管理						
運用業務	ハードウェア管理						
運用業務	ネットワーク管理						
運用業務	構成管理				支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	構成管理ﾌﾟﾛｾｽ	構成識別
					支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	構成管理ﾌﾟﾛｾｽ	構成状況の記録
					支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	構成管理ﾌﾟﾛｾｽ	構成評価
運用業務	建物･関連設備管理						
保守業務	保守手順						
保守業務	保守計画		技術ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	問題把握及び修正分析	
保守業務	保守の実施		技術ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	修正の実施	
保守業務	保守の確認		技術ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	保守ﾚﾋﾞｭｰ及び受入れ	
保守業務	移行				保守ﾌﾟﾛｾｽ	移行	
保守業務	情報システムの廃棄		技術ﾌﾟﾛｾｽ	処分ﾌﾟﾛｾｽ	保守ﾌﾟﾛｾｽ	ｿﾌﾄｳｪｱ廃棄	
共通業務	ドキュメント管理	作成			支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	文書化ﾌﾟﾛｾｽ	設計及び作成
共通業務	ドキュメント管理	管理			支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	文書化ﾌﾟﾛｾｽ	文書発行
					支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	文書化ﾌﾟﾛｾｽ	保守
共通業務	進捗管理	実施					
共通業務	進捗管理	評価			組織に関するﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	管理ﾌﾟﾛｾｽ	実行及び管理
共通業務	品質管理	計画					
共通業務	品質管理	実施					
					支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	品質保証ﾌﾟﾛｾｽ	製品の保証
					支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	品質保証ﾌﾟﾛｾｽ	ﾌﾟﾛｾｽの保証
					支援ﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	品質保証ﾌﾟﾛｾｽ	品質ｼｽﾃﾑの保証
共通業務	人的資源管理	責任･権限			組織に関するﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	管理ﾌﾟﾛｾｽ	ﾚﾋﾞｭｰ及び評価
共通業務	人的資源管理	業務遂行					
共通業務	人的資源管理	教育･訓練			組織に関するﾗｲﾌｻｲｸﾙﾌﾟﾛｾｽ	教育訓練ﾌﾟﾛｾｽ	教材の開発

システム管理基準			ISO/IEC 15288:2002(JIS X 0170-2004)		ISO/IEC 12207:1995(JIS X 0160-1996)		
					組織に関するライフサイクルプロセス	教育訓練プロセス	教育訓練計画の実施
共通業務	人的資源管理	健康管理					
共通業務	委託・受託	計画	協定プロセス	取得プロセス	取得プロセス		
共通業務	委託・受託	委託先選定	協定プロセス	取得プロセス	取得プロセス		
共通業務	委託・受託	契約	協定プロセス	取得プロセス、供給プロセス	取得プロセス		
共通業務	委託・受託	委託業務	協定プロセス	取得プロセス	取得プロセス		
共通業務	委託・受託	受託業務	協定プロセス	供給プロセス	供給プロセス		
共通業務	変更管理	管理					
共通業務	変更管理	実施					
共通業務	災害対策	リスク分析					
共通業務	災害対策	災害時対応計画					
共通業務	災害対策	バックアップ					
共通業務	災害対策	代替処理・復旧					
					支援ライフサイクルプロセス	検証プロセス	検証
					支援ライフサイクルプロセス	妥当性確認プロセス	妥当性確認
					支援ライフサイクルプロセス	共同レビュープロセス	プロジェクト管理レビュー
					支援ライフサイクルプロセス	共同レビュープロセス	技術レビュー
					支援ライフサイクルプロセス	監査プロセス	監査
					支援ライフサイクルプロセス	問題解決プロセス	問題解決
					組織に関するライフサイクルプロセス	管理プロセス	計画立案
					組織に関するライフサイクルプロセス	管理プロセス	終了
					組織に関するライフサイクルプロセス	環境整備プロセス	環境の構築
					組織に関するライフサイクルプロセス	環境整備プロセス	環境の維持
					組織に関するライフサイクルプロセス	改善プロセス	プロセスの確立
					組織に関するライフサイクルプロセス	改善プロセス	プロセスの確立
					組織に関するライフサイクルプロセス	改善プロセス	プロセスの改善

索　引

【さ】

【た】

【な】

【は】

【ま】

【や】

【ら】

【英字】

執筆及び協力者一覧

システム管理基準解説書

江藤　友保	(株)シーイーシー 管理本部
小田　浩史	富士通エフ・アイ・ピー(株)　アウトソーシング事業部オンサイトサービス部
川辺　良和	(有)インターギデオン　代表取締役
喜入　　博	KPMG ビジネスアシュアランス(株)　常勤顧問
清水　惠子	日本公認会計士協会 監査対応 IT 委員会　専門委員
千枝　和行	(社)日本情報システム・ユーザー協会 ビジネスシステム定義研究プロジェクト 委員
鳥居　壮行	駿河台大学　文化情報学部 教授
新田　　稔	IBM ビジネスコンサルティング サービス(株) 公共事業本部 IS リスクマネジメント　マネージング・コンサルタント
本田　　実	システム監査学会　理事

(五十音順，勤務先等：2005 年 1 月現在)

『新版　システム監査基準／システム管理基準解説書』(平成 16 年基準改訂版)

システム管理基準解説書　　2005 年 1 月 31 日　発行

編 集 兼
発 行 人　　児玉　幸治

発 行 所　　財団法人　日本情報処理開発協会
〒105-0011　東京都港区芝公園 3-5-8　機械振興会館内
TEL03-3432-9381　FAX03-3432-9389
URL　http://www.jipdec.jp/

ISBN4-89078-013-0

財団法人 日本情報処理開発協会

related material

関連資料

関連資料

目　次

情報システム安全対策基準

平成７年８月29日（通商産業省告示第５１８号）（制定）

平成９年９月24日（通商産業省告示第５３６号）（最終改正）

情報システム安全対策基準を次のように定め、平成７年８月29日から施行する。

なお、平成３年通商産業省告示第１７５号は、平成７年８月28日限り、廃止する。

平成７年８月29日

I　主旨

本基準は、情報システムの機密性、保全性及び可用性を確保することを目的として、自然災害、機器の障害、故意・過失等のリスクを未然に防止し、また、発生したときの影響の最小化及び回復の迅速化を図るため、情報システムの利用者が実施する対策項目を列挙したものである。

II　用語の定義

本基準に用いられる主な用語の定義は、以下のとおりである。

(1) 情報システム関連

①コンピュータ……演算、記憶、制御及び入出力の各機能を有する装置

②ホストコンピュータ……利用者に計算又はデータベースサービスを提供し、ネットワーク制御機能を実行できるサーバを含むコンピュータ

③端末機……データ等の入出力のために、コンピュータに通信回線等で接続された機器（ワークステーション、パーソナルコンピュータ、ATM、CD、各種発券機等）

④通信関係装置……通信回線、交換機、多重化装置、ネットワーク機器、MDF、IDF 等

⑤情報システム……ホストコンピュータ、端末機、通信関係装置、プログラム等の全部又は一部により構成されるデータを処理するためのシステム

⑥情報システム等……情報システム及び関連設備

⑦データ……情報システムの入出力情報

⑧プログラム……プログラム言語により記述された命令の組合せ

⑨ドキュメント……システム設計、プログラム作成、情報システムの運用等に関する記録

⑩データ等……データ、プログラム及びドキュメント

⑪記録媒体……データ等を記録した機器、ディスク、磁気テープ、フィルム、カード、用紙（有印帳票を含む）等

⑫ファイル……記憶装置又は記録媒体に、電子的又は光学的に記録されているデータ等

(2) 設備関連

①電源設備……情報システム等を作動させるための受電設備、定電圧定周波数電源装置、分電盤、配線等の設備

②空気調和設備……コンピュータ室等の空気調和をする機器、冷却塔及びその附属設備

③監視設備……情報システム、電源設備、空気調和設備等の運転の状態を監視し、必要な措置（異常警報を発して記録し、操作を行う等）を行う設備

④関連設備……電源設備、空気調和設備及び監視設備

⑤防災設備……火災報知設備、消火設備、漏水検知設備、感震器、超高感度煙監視器、耐火金庫等

⑥防犯設備……入退管理設備、侵入監視設備、保管設備等

(3) 建物及び室関係

①建物……情報システム等を収容する建物

②コンピュータ室……ホストコンピュータを設置するための専用の室

③事務室……端末機、サーバ、ワークステーション、パーソナルコンピュータ等を設置している室、店舗、配送センタ等

④データ等保管室……データ、プログラム等を含んだ記録媒体及びドキュメントを保管する室

⑤端末スペース……特定サービスを目的として、一般の利用者に開放する端末機を設置した場所

Ⅲ　基準の構成

本基準は、設置基準、技術基準及び運用基準から構成されており、その内容は以下のとおりである。

(1) 設置基準（100項目）

情報システム、関連設備、防災設備及び防犯設備を火災、地震等の自然災害、構成要素の障害、不法侵入者による破壊行為等の危険から物理的に保護するための設備及び機器の設置環境面の対策

(2) 技術基準（26項目）

情報システムの具備すべき機能を、円滑かつ安全に発揮するためのハードウェア及びソフトウェアによる技術面の対策

(3) 運用基準（66項目）

設置基準、技術基準で示すそれぞれの対策の適切な適用を図り、情報システム等の安全性及び信頼性の確保を図るための運用面の対策

Ⅳ　適用区分

(1) 設置基準

設置基準は、建物、コンピュータ室、事務室、データ等保管室、端末スペース及び関連設備の合計６項目に区分し、運用する情報システムの重要度等を考慮して、各対策項目の適用区分を明記している。

関連設備は、その基準項目が建物又は室と一体となって対策する必要のある場合は、建物及び室にも適用区分を明記している。

(2) 技術基準及び運用基準

技術基準及び運用基準は、情報システムの利用形態、情報システム利用者の特定性の程度等による障害の影響又は対策の適合性から、それぞれの情報システムの重要度を考慮して、各対策項目の適用区分を明記している。

(3) 技術基準及び運用基準における適用区分の考え方は以下のとおりである。

利用者区分	不特定利用者	特定企業内利用者	特定部門内利用者
情報システムの利用者	・不特定の一般の者	・情報システムを保有する企業に属する者	・情報システムを保有する企業及び外部企業の特定部門に所属する者
情報システムの例	・銀行オンラインシステム ・パソコン通信システム ・受発注オンラインシステム（VAN）	・販売、在庫管理システム ・住民情報システム	・人事情報システム ・経理システム ・航空管制システム ・ダム水量制御システム ・CAD、CAM、CIM ・企業間資金移動システム
端末、クライアントの範囲	・情報システムに接続する他社のホスト、サーバにつながる端末、クライアントを含む。 （自社でシステム的、物理的管理不可能）	・企業内の端末等 （自社で管理可能）	・部門内端末（自部門で管理可能）
端末、クライアントの管理者	・自社の他部門（自社でシステム的、物理的管理可能） ・他社（自社でシステム的管理可能、物理的管理不可能）	・自社の他部門（自社でシステム的、物理的管理可能）	・自部門（自部門でシステム的、物理的管理可能）
ホスト、サーバの管理者	・システム管理部門 ・情報システムを保有する部門	・システム管理部門 ・情報システムを保有する部門	・情報システムを保有する特定部門

(4) 本基準を利用する場合は、以下を考慮して利用すること。

①情報システムは、重要度により以下の３グループに分けている。

A　人命、他人の財産、プライバシー等社会に影響を与える情報システム

B　企業への影響の大きい情報システム

C　企業への影響の小さい情報システム

②本基準では、①のA、B、Cに対して、個別対策項目のコスト、効果、難易度等を評価して、室区分又は利用者区分に対して、適用の範囲を以下のマークで表示し適用区分としている。

☆……①のAに限定して必要な対策

○……①のA、Bに必要な対策

◎……①のA、B、C全てに必要な対策

－……適用除外

V　設置基準

項目	対策項目	適用区分 1 建物	2 コンピュータ室	3 事務室	4 データ等保管室	5 端末スペース	6 関連設備
イ．設置環境							
1．立地・配置	(1) 建物及び室は、火災の被害を受ける恐れのない場所に設けること。	☆	◎	☆	◎	☆	－
	(2) 建物及び室は、水の被害を受ける恐れのない場所に設けること。	☆	○	☆	○	☆	－
	(3) 建物は、落雷の被害を受ける恐れのない場所に設けること。	☆	－	－	－	－	－
	(4) 建物及び室は、電界及び磁界の被害を受ける恐れのない場所に設けること。	☆	◎	☆	◎	☆	－
	(5) 建物及び室は、空気汚染の被害を受ける恐れのない場所に設けること。	☆	☆	☆	☆	－	－
	(6) 室は、専用とすること。	－	○	－	○	☆	－
	(7) 情報システムを事務室に設置する場合は、設置位置等に配慮すること。	－	－	○	－	－	－
	(8) 建物の内外及び室は、情報システム及び記録媒体の所在を明示しないこと。	◎	◎	☆	◎	－	－
	(9) 建物及び室は、避難のために必要な空間を確保すること。	◎	◎	◎	◎	－	－
2．開口部	(1) 外部及び共用部分に面する窓は、防災措置を講ずること。	☆	◎	☆	◎	－	－
	(2) 外部より容易に接近しうる窓は、防犯措置を講ずること。	○	◎	☆	◎	－	－
	(3) 室は、外光による影響を受けない措置を講ずること。	－	◎	◎	◎	－	－
	(4) 出入口は、不特定多数の人が利用する場所を避けて設置すること。	☆	◎	☆	◎	－	－
	(5) 出入口は、できるだけ少なくし、入退管理設備を設けること。	☆	◎	☆	◎	－	－
	(6) 建物及び室の適切な位置に非常口を設けること。	◎	◎	☆	◎	－	－
3．構造	(1) 建物は、建築基準法に規定する耐火性能を有すること。	◎	－	－	－	－	－
	(2) 情報システムの専用の室は、独立した防火区画とすること。	－	○	☆	○	－	－
	(3) 建物及び室は、水の被害を防止する措置を講ずること。	◎	◎	☆	◎	☆	－
4．内装	(1) 建物及び室の内装は、不燃材料を使用すること。	☆	◎	○	◎	☆	－
	(2) 室の壁及び天井材料は、防音性能を有すること。	－	◎	○	－	－	－
	(3) 室の照明器具は、防眩措置を講ずること。	－	◎	◎	－	－	－
	(4) 室のフリーアクセス床の主要部分は、不燃材料を使用すること。	－	◎	○	◎	－	－
	(5) 室の床表面材料は、静電気による影響を防止する措置を講ずること。	－	◎	◎	◎	☆	－
	(6) 建物及び室のカーテン、ブラインド、じゅうたん等は、防炎性能を有するものを使用すること。	☆	◎	◎	◎	☆	－
5．建築設備	(1) 建物は、避雷設備を設置すること。	◎	－	－	－	－	－
	(2) 建物及び室は、自動火災報知設備を設置すること。	◎	◎	◎	◎	◎	－
	(3) 建物及び室は、非常放送設備を設置すること。	◎	◎	◎	◎	－	－
	(4) 建物及び室は、消火設備を設置すること。	◎	◎	◎	◎	☆	－
	(5) 建物及び室は、排煙設備を設置すること。	☆	◎	○	◎	－	－
	(6) 建物及び室は、非常照明設備を設置すること。	☆	◎	◎	◎	－	－
	(7) 建物及び室は、誘導灯又は誘導標識を設置すること。	☆	◎	◎	◎	－	－
	(8) 建物及び室は、避難器具を設置すること。	◎	◎	◎	－	－	－

項目	対策項目	適用区分 1 建物	2 コンピュータ室	3 事務室	4 データ等保管室	5 端末スペース	6 関連設備
	(9) 室内は、情報システムの運転に必要な水使用設備以外設置しないこと。	—	◎	☆	◎	—	—
	(10) 室内、天井裏等は、水配管を通さないこと。	—	◎	☆	◎	—	—
	(11) 建物及び室は、小動物等による被害防止の措置を講ずること。	○	◎	○	◎	◎	—
	(12) 情報システムを設置した室は、保守用コンセントを設けること。	—	◎	◎	—	◎	—
6．什器・備品	(1) 什器、備品等は不燃性のものを使用すること。	—	◎	○	◎	☆	—
	(2) 情報システムの運用に関連する機器のための防水カバーを常備すること。	—	◎	◎	◎	☆	—
	(3) 衣服、履き物、什器、備品等は、静電気防止の措置を講ずること。	—	◎	☆	◎	—	—
7．情報システム	(1) 情報システムの保守に必要な空間を確保すること。	—	◎	◎	—	◎	—
	(2) コンピュータ、端末機及び通信関係装置からの電波放射による情報漏えいを防止する措置を講ずること。	☆	☆	☆	—	☆	—
	(3) 水冷式コンピュータを設置する場合は、水漏れ防止の措置を講ずるとともに、漏水の恐れのある場所に漏水検知器等を設置すること。	—	◎	—	—	—	◎
	(4) 通信関係装置を設置する場合は、防災及び防犯措置を講ずること。	—	◎	◎	—	◎	—
	(5) 通信関係装置を設置する場合は、避雷措置を講ずること。	◎	—	—	—	◎	—
	(6) 外部からの通信回線の引込口は、多重化し、専用とすること。	☆	—	—	—	—	—
	(7) 通信回線は、専用の配線スペースに設けること。	—	◎	☆	—	—	—
	(8) 記録媒体は、盗難防止措置を講ずること。	☆	◎	◎	◎	◎	—
ロ．電源設備							
1．設置	(1) 電源設備は、停電に対する措置を講ずること。	—	—	—	—	—	○
	(2) 情報システムの電源設備は、電圧及び周波数の変動に対する措置を講ずること。	—	—	—	—	—	○
	(3) 情報システムの電源設備の電気容量は、機器の負荷を考慮して余裕を持たせること。	—	—	—	—	—	◎
	(4) 情報システムの変圧器は、専用とすること。	—	—	—	—	—	○
	(5) 情報システムの電源設備は、ラインフィルタの交流透過電流の還流値が、一定の値を超えない措置を講ずること。	—	—	—	—	—	◎
	(6) 情報システムの三相電源に単相機器を接続する場合は、設備不平衡による障害の防止措置を講ずること。	—	—	—	—	—	◎
	(7) 情報システムの配線にノイズが誘導しないよう、電磁遮蔽の措置を講ずること。	—	—	—	—	—	◎
	(8) 情報システム専用の電源配線スペースを設けること。	—	—	—	—	—	☆
	(9) 情報システムの分電盤は、専用とし、それぞれ当該室内に設置すること。	—	—	—	—	—	◎
	(10) 情報システムのアースは、専用とすること。	—	—	—	—	—	◎
	(11) 監視設備、防災設備及び防犯設備の予備電源設備を設置すること。	—	—	—	—	—	◎
2．防災・防犯措置	(1) 電源設備は、防災及び防犯措置を講ずること。	—	—	—	—	—	◎
	(2) 電源設備は、避雷措置を講ずること。	—	—	—	—	—	◎

項目	対策項目	適用区分 1 建物	2 コンピュータ室	3 事務室	4 データ等保管室	5 端末スペース	6 関連設備
	(3) 電源設備を設置した室から情報システムの分電盤までの配線は、防火、防犯、ノイズ防止等の措置を講ずること。	—	—	—	—	—	◎
	(4) 電源配線が防火壁等を貫通する部分及びこれに近接する部分は、延焼防止及び防煙の措置を講ずること。	—	—	—	—	—	◎
	(5) 分電盤の通電部分は、感電防止の措置を講ずること。	—	—	—	—	—	◎
	(6) 分電盤の主回路は、地絡を検知し、警報を発する装置又は自動遮断する装置を設けること。	—	—	—	—	—	◎
ハ．空気調和設備 1．設置	(1) 空気調和設備は、情報システムの適正な稼動及びその運用に携わる者の健康に配慮し、適切な室内環境を維持するための措置を講ずること。	—	—	—	—	—	◎
	(2) コンピュータ室の空気調和設備は、専用とすること。	—	—	—	—	—	○
	(3) コンピュータ室の空気調和設備は、能力に余裕を持たせること。	—	—	—	—	—	○
	(4) コンピュータ室の空気調和設備は、負荷変動に対して的確に作動する自動制御装置を設置すること。	—	—	—	—	—	○
	(5) コンピュータ室の空気調和設備は、凍結防止の措置を講ずること。	—	—	—	—	—	○
	(6) コンピュータ室の空気調和設備は、水質を管理する措置を講ずること。	—	—	—	—	—	○
2．防災・防犯措置	(1) 空気調和設備は、防災及び防犯措置を講ずること。	—	—	—	—	—	◎
	(2) 空気調和設備は、水漏れ防止の措置を講ずるとともに、漏水の恐れのある場所に漏水検知器等を設置すること。	—	—	—	—	—	◎
	(3) 空気調和設備の外気取入口及び排気口は、雨が浸入しない構造とすること。	—	—	—	—	—	◎
	(4) 空気調和設備の配管、ダクト類は、耐火性に優れた材料を使用すること。	—	—	—	—	—	◎
	(5) 空気調和設備等のダクトが室内を貫通する部分は、防火及び防煙措置を講ずること。	—	—	—	—	—	◎
	(6) 空気調和設備の断熱材料は、不燃材料とすること。	—	—	—	—	—	◎
ニ．監視設備	(1) 情報システム等を設置した建物及び室の人の出入りを遠隔監視する設備を設置すること。	—	—	—	—	—	○
	(2) 情報システム等を設置した建物及び室の防災設備及び防犯設備の作動を遠隔監視する設備を設置すること。	—	—	—	—	—	○
	(3) 電源設備及び空気調和設備の稼動状況を遠隔監視する設備を設置すること。	—	—	—	—	—	○
	(4) 通信回線の利用状況、障害等を監視する設備を設置すること。	—	—	—	—	—	○
ホ．地震対策 a．設置環境 1．立地・配置	(1) 建物は、活断層等による地震の被害の恐れのある場所を避けて設置すること。	☆	—	—	—	—	—
	(2) 室は、地震の被害の少ない位置に設置すること。	—	◎	☆	◎	☆	—
	(3) 災害時にバックアップするための建物及び室を設置する場合は、遠隔地に設置すること。	☆	☆	☆	☆	—	—
2．構造	(1) 建物は、建築基準法に規定する耐震構造とすること。	◎	—	—	—	—	—

項　　目	対　策　項　目	適用区分					
		1 建物	2 コンピュータ室	3 事務室	4 データ等保管室	5 端末スペース	6 関連設備
3．開口部	(1) 建物及び室の出入り口の扉は、十分な強度を持った防火戸等とすること。	◎	◎	☆	◎	☆	－
	(2) 建物及び室の窓ガラスは、破損、飛散及び落下防止の措置を講ずること。	☆	◎	◎	◎	◎	－
4．内装	(1) 建物及び室の内装及び照明器具は、地震時に落下及び損傷しない措置を講ずること。	◎	◎	◎	◎	◎	－
	(2) 室のフリーアクセス床は、耐震構造又は免震構造とすること。	－	◎	◎	◎	☆	－
5．設備	(1) 地震を感知し、情報システム等の運転を制御する設備を設置すること。	－	－	－	－	－	☆
	(2) 室は、災害時の緊急通信用設備を設置すること。	－	◎	☆	☆	◎	－
	(3) 災害時の断水対策として、補給水用設備を設置すること。	☆	－	－	－	－	－
6．什器・備品	(1) 什器、備品等は、設置位置に応じた移動及び転倒防止の措置を講ずること。	－	◎	◎	◎	－	－
	(2) 什器、備品等のガラスは、破損、飛散及び落下防止の措置を講ずること。	－	○	○	○	－	－
	(3) 記録媒体、ドキュメント等は、収納位置に応じた移動及び落下防止の措置を講ずること。	－	◎	◎	◎	－	－
7．情報システム	(1) 情報システムは、設置位置に応じた移動、転倒及び振動防止の措置を講ずること。	－	◎	◎	－	◎	－
	(2) 災害時にバックアップするための情報システムを設置する場合は、遠隔地に設置すること。	－	☆	☆	－	－	－
b．電源設備	(1) 電源設備は設置位置に応じた移動、転倒及び振動防止の措置を講ずること。	－	－	－	－	－	◎
	(2) 災害時の停電対策として、自家発電設備を設置すること。	－	－	－	－	－	☆
c．空気調和設備	(1) 空気調和設備は、設置位置に応じた移動、転倒及び振動防止の措置を講ずること。	－	－	－	－	－	◎
d．監視設備	(1) 監視設備は、設置位置に応じた移動、転倒及び振動防止の措置を講ずること。	－	－	－	－	－	◎

VI　技術基準

項　目	対　策　項　目	利用者区分による適用		
		1 不特定	2 特定企業内	3 特定部門内
イ．情報技術の適用	(1) 情報技術による安全機能は、情報システムの集中、分散処理の形態に応じて採用すること。	◎	◎	◎
	(2) 情報技術製品は、安全機能を評価及び確認し、適切に利用すること。	◎	◎	◎
ロ．災害・障害対策機能				
1．災害対策機能	(1) 情報システムは、代替運転する機能を設けること。	◎	○	☆
	(2) データ及びプログラムを復旧する機能を設けること。	◎	○	☆
	(3) 回復許容時間に対応したバックアップ機能を設けること。	◎	○	☆
	(4) 情報システムを遠隔地でバックアップする機能を設けること。	☆	☆	☆
2．障害対策機能	(1) データのエラー検出機能を設けること。	◎	◎	○
	(2) 集中、分散処理の形態に応じて、情報システムの障害箇所を検出し、切り離して処理を継続する機能を設けること。	◎	◎	○
	(3) 集中、分散処理の形態に応じて、障害による情報システムの停止の後、処理を回復する機能を設けること。	◎	◎	○
3．保守機能	(1) 障害内容を解析し障害箇所を特定化する機能を設けること。	◎	◎	○
	(2) 情報システムを停止しないで保守する機能を設けること。	○	○	☆
	(3) 遠隔操作により保守する機能を設けること。	○	○	☆
4．運用支援機能	(1) 情報システムの稼動及び障害を監視し、運転を制御する機能を設けること。	○	○	☆
	(2) 情報システムを自動的に運転する機能を設けること。	○	○	☆
ハ．故意・過失対策機能				
1．アクセス制御機能	(1) 集中、分散処理の形態に応じて、情報システムの資源の機密度を区別する機能を設けること。	◎	◎	○
	(2) 集中、分散処理の形態に応じて、情報システムの利用者の登録と管理機能を設けること。	◎	◎	◎
	(3) 集中、分散処理の形態に応じて、情報システム及びその資源にアクセスするユーザ等の正当性を識別し、認証する機能を設けること。	◎	◎	○
	(4) 集中、分散処理の形態に応じて、情報システム及びその資源に対するアクセス権限を制御する機能を設けること。	◎	◎	○
	(5) アクセスを監視する機能を設けること。	◎	◎	☆
2．データ処理不正防止機能	(1) 集中、分散処理の形態に応じて、データの不正な変更を発見する機能を設けること。	◎	◎	☆
	(2) 集中、分散処理の形態に応じて、プログラムの不正な変更及び実行を発見する機能を設けること。	○	○	☆
	(3) データの変更等及びプログラムの実行に異常を発見した場合に、集中、分散処理の形態に応じて、処理を迂回又は停止する機能を設けること。	○	○	☆
	(4) 共用資源の保護機能を設けること。	◎	◎	◎
3．情報漏えい防止機能	(1) コンピュータ、端末機及び通信関係装置からの電波放射による情報漏えいを防止する機能を設けること。	☆	☆	☆
	(2) ファイル、伝送情報等を暗号化する機能を設けること。	○	○	○
ニ．監査機能	(1) 情報システムは、監査機能を設けること。	○	○	☆

Ⅶ　運用基準

項　　目	対　策　項　目	利用者区分による適用		
		1 不特定	2 特定企業内	3 特定部門内
イ．計画				
1．情報システム等の運用計画	(1) 情報システム等の運用計画は、集中、分散処理の形態に応じて策定すること。	◎	◎	○
	(2) 集中、分散処理の形態に応じ、情報システムの構成機器の変更及びソフトウェアの修正、変更等の管理計画を策定すること。	◎	◎	◎
	(3) 運用計画は、リスク評価に基づく災害、障害、故意及び過失の安全対策を盛り込むこと。	◎	◎	◎
2．データ等の管理計画	(1) データ等は、機密度及び重要度に応じた区分を設け、保有、利用、配布、持出し、持込み、保管、消去、廃棄等の管理計画を策定すること。	◎	◎	◎
	(2) データ等の作成、更新、複写、移動、伝送等に当たっては、集中、分散処理の形態に応じた管理計画を策定すること。	◎	◎	◎
3．組織・管理規程	(1) 情報システム等の円滑な運用を行う組織及び災害等への対応組織を整備すること。	◎	◎	◎
	(2) 情報システム等の運用に当たっては、責任分担及び責任分界点を明確にすること。	◎	◎	◎
	(3) 情報システムの集中、分散処理の形態に応じた運用に関する管理規程を整備するとともに、管理責任者を定めること。	◎	◎	○
	(4) データ等及び記録媒体の使用及び保管に関する管理規程を整備するとともに、管理責任者を定めること。	◎	◎	○
	(5) 入退館及び入退室に関する管理規程を整備するとともに、管理責任者を定めること。	◎	◎	☆
	(6) 防災及び防犯に関する管理規程を整備するとともに、管理責任者を定めること。	◎	◎	○
	(7) 関連設備、防災設備及び防犯設備に関する管理規程を整備するとともに、管理責任者を定めること。	◎	◎	○
4．災害時対応計画	(1) 情報システムの代替処理及び復旧措置を定めた災害時運用マニュアルを整備すること。	○	○	○
	(2) 業務は、回復許容時間を設定し、再開順位を定めること。	○	○	○
	(3) 要員確保計画を策定すること。	◎	◎	☆
ロ．情報システムの運用				
1．システム管理	(1) 集中、分散処理の形態に応じた、情報システム、データ等の運用に関する細則を定めること。	○	○	○
	(2) 構成機器の変更及びソフトウェアの修正、変更等に当たっては、集中、分散処理の形態に応じた、情報システムの正常な動作に影響を与えない措置を講ずること。	◎	○	○
	(3) 集中、分散処理の形態に応じて、運転の監視、制御及び記録を行い、毎日の運転状況を分析すること。	◎	◎	☆
	(4) アクセスモニタリングの結果を分析し、集中、分散処理の形態に応じた不正防止のための措置を講ずること。	◎	○	☆
	(5) 情報システムの構成機器の鍵は、特定者が管理すること。	◎	◎	○
	(6) 情報システムの障害を分析し、再発防止の措置を講ずること。	◎	◎	◎
	(7) 情報システムの保守の内容及び結果を調査及び分析すること。	◎	◎	◎
	(8) 情報システムの保守に当たっては、集中、分散処理の形態に応じたデー	◎	◎	◎

項　　目	対　策　項　目	利用者区分による適用		
		1 不特定	2 特定企業内	3 特定部門内
	タ保護のための措置を講ずること。			
	(9) 端末機は用途及び設置環境に応じた、適切な管理を行うこと。	◎	◎	◎
2．利用者管理	(1) 集中、分散処理の形態に応じた、情報システムの利用マニュアルを整備し、利用者に徹底すること。	◎	◎	◎
	(2) 利用者の情報システムへのアクセス権限は、集中、分散処理の形態に応じて定めること。	◎	○	☆
	(3) 情報システム利用者のパスワード、識別コード等は、集中、分散処理の形態に応じて管理すること。	◎	○	☆
	(4) 情報システム利用者の操作資格は、集中、分散処理の形態に応じて定めること。	☆	☆	☆
3．操作	(1) 業務処理スケジュールに基づく情報システムの運転マニュアルを常備すること。	◎	◎	○
	(2) 集中、分散処理の形態に応じた、端末機の操作マニュアル、操作ガイドを常備すること。	◎	◎	◎
	(3) 集中、分散処理の形態に応じた、障害時の措置及び回復手順を定めたマニュアルを常備すること。	◎	○	☆
4．災害発生時対応	(1) 災害発生時は、災害時対応計画に沿って速やかに情報システム等の被災程度を調査及び分析すること。	◎	◎	○
	(2) 被災程度に応じて、予め定められた災害時運用マニュアルに沿い、業務再開方式を決定すること。	◎	◎	○
ハ．データ等及び記録媒体の保管及び使用 1．管理	(1) データ等及び記録媒体は、集中、分散処理の形態に応じて、保管、使用等に関する細則を定めること。	◎	◎	◎
2．保管	(1) データ等及び記録媒体は、集中、分散処理の形態に応じて、定められた場所に保管すること。	◎	◎	◎
	(2) 記録媒体の保管設備の鍵は、特定者が管理すること。	○	○	○
	(3) 記録媒体の保管状況は、特定者が定期的に点検すること。	◎	○	○
3．使用	(1) データ等及び記録媒体の取扱い及び受渡しは、集中、分散処理の形態に応じて、定められた方法によって行うこと。	◎	◎	○
	(2) データ等及び記録媒体の作成、追加、更新、複写、廃棄等について管理記録を整備すること。	◎	◎	○
4．防犯対策	(1) データ等及び記録媒体の不正持出し及び不正使用を防止するため、管理責任者は使用状況を点検すること。	◎	◎	◎
	(2) データ等の暗号鍵の管理は特定者が行うこと。	○	○	○
5．災害・障害対策	(1) 記録媒体の分散保管は、集中、分散処理の形態に応じて行うこと。	○	○	○
	(2) データ等のバックアップを行うこと。	○	○	○
ニ．入退館及び入退室 1．入退者	(1) 情報システムの集中、分散処理の形態に応じ、情報システム等を設置した建物及び室の入退館及び入退室の資格付与細則を定めること。	◎	◎	◎

項　　目	対　策　項　目	利用者区分による適用		
		1 不特定	2 特定企業内	3 特定部門内
	(2) 建物及び室の入退者に対しては、資格審査を行い資格識別証を発行し、入退館及び入退室を管理すること。	◎	○	○
	(3) 一時的に入退館及び入退室の資格を与えた者は、必要に応じ立会人を付け、立入場所の抑制を行うこと。	◎	○	○
	(4) 建物又は室の重要度に応じ、入退の記録をとること。	◎	◎	○
	(5) 出入口の施錠及び解錠、鍵の保管及び受渡し等の記録をとり、鍵管理を行うこと。	◎	◎	○
2．搬出入物	(1) 情報システム等の運用に関連する各室の搬出入物は、必要な物に限定すること。	◎	◎	◎
	(2) 搬出入物は内容を確認し、記録をとること。	○	○	☆
ホ．関連設備・防災設備及び防犯設備				
1．管理	(1) 関連設備、防災設備及び防犯設備の変更、増設等に当たっては、情報システムの正常な動作に影響を与えない措置を講ずること。	◎	○	☆
	(2) 関連設備、防災設備及び防犯設備の定期点検を実施し、結果を調査及び分析すること。	◎	○	☆
	(3) 関連設備、防災設備及び防犯設備の障害を調査及び分析し、再発防止の措置を講ずること。	◎	◎	○
2．操作	(1) 関連設備、防災設備及び防犯設備の操作及び保守管理は、特定者が行うこと。	◎	◎	☆
	(2) 定常時及び災害、障害時の措置を定めた関連設備、防災設備及び防犯設備の取扱いマニュアルを常備すること。	◎	○	☆
3．監視	(1) 情報システムの運転状況の変化に対し、監視設備により、電源設備及び空気調和設備の作動を制御すること。	◎	◎	○
	(2) 電源設備及び空気調和設備の監視データを記録し、分析すること。	◎	◎	○
	(3) 防災及び防犯のため、館内及び室内を定期的に巡回すること。	○	○	☆
ヘ．要員	(1) 要員の配置、交替等の管理は、集中、分散処理の形態に応じ適正に行うこと。	◎	◎	◎
	(2) 安全対策に係る規程、マニュアル等を習熟させるための教育及び訓練を実施すること。	◎	◎	◎
	(3) 災害時対応計画に沿った教育及び訓練を実施すること。	◎	◎	◎
ト．外部委託	(1) 情報システム等の運用管理作業を外部に委託する場合は、安全対策に関する項目を盛り込んだ作業契約を締結すること。	◎	◎	◎
	(2) 委託先における安全対策の実施状況を確認すること。	◎	◎	◎
	(3) 情報システムのバックアップを外部に委託する場合は、定期的に切替、起動、戻し等のテストを行うこと。	○	○	○
チ．システム監査	(1) 安全対策に関するシステム監査の報告を受け、必要な措置を講ずること。	◎	○	○
	(2) 災害時対応計画に関するシステム監査の報告を受け、必要な措置を講ずること。	◎	○	○

Ⅷ　留意事項

(1) 基準の活用に当たっては，リスク評価に基づき対策項目の組合せを考慮するとともに，対策の実施によって生じる制約と情報システムの利便性又は可用性の調和に配慮すること。

(2) 本基準の地震対策の項目については，最大規模の地震災害を想定して，対策を講ずること。

なお，地震対策項目のうち災害時とした項目は，水害，火災，爆破等の他の大規模な災害にも適用できる。

(3) 技術基準は機能を中心に記述しているため，各対策項目の実施に当たっては機能の実現に必要なハードウェア，ソフトウェア等を整備するとともに，適切な運用を図ること。

(4) システム監査の実施については，「システム監査基準」を活用すること。

(5) コンピュータウイルス対策の実施については，「コンピュータウイルス対策基準」を活用すること。

コンピュータウイルス対策基準

平成７年７月７日（通商産業省告示第４２９号）（制定）
平成９年９月24日（通商産業省告示第５３５号）（改定）
平成12年12月28日（通商産業省告示第９５２号）（最終改定）

コンピュータウイルス対策基準を次のように定め、平成７年７月１日から施行する。
なお、平成２年通商産業省告示第１３９号は、平成７年６月30日限り、廃止する。

1．主旨

本基準は、コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたものである。

2．用語の定義

本基準に用いられる主な用語の定義は、以下のとおりである。

（1） コンピュータウイルス（以下「ウイルス」とする。）

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

①自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

②潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

③発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

（2） ソフトウェア

システムプログラム、アプリケーションプログラム、ユーティリティプログラム等のプログラム

（3） システム

ハードウェア、ソフトウェア若しくはネットワーク又はこれらの複合体

（4） ワクチン

ウイルスの検査、予防又は修復のいずれかの機能を含むソフトウェア

（5） バックアップ

プログラム、データ等と同一の内容を別の媒体に記録すること。

（6） ファイル

記憶装置又は記録媒体上に、電子的又は光学的に記録されているプログラム、データ等

（7） 保守機能

システムを正常な状態に維持するための機能

（8） セキュリティ機能

プログラム、データ等の機密性、保全性及び可用性を確保するための機能

3．構成

本基準は、システムユーザ基準、システム管理者基準、ソフトウェア供給者基準、ネットワーク事業者基準及びシステムサービス事業者基準から成り、その構成及び内容は、以下のとおりである。

（1） システムユーザ基準（18項目）

システムを利用する者（以下「システムユーザ」とする。）のための対策をまとめたもの。

①ソフトウェア管理（2項目）

システムユーザが導入するソフトウェアに対する対策についてまとめたもの。

②運用管理（12項目）

システムユーザがシステムを利用する上での対策についてまとめたもの。

③事後対応（3項目）

システムユーザがウイルスを発見した場合の対策についてまとめたもの。

④監査（1項目）

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

（2） システム管理者基準（31項目）

システムを導入、維持及び管理する者（以下「システム管理者」とする。）のための対策についてまとめたもの。

①コンピュータ管理（8項目）

システム管理者がハードウェア及びソフトウェアを導入及び更新する場合の対策についてまとめたもの。

②ネットワーク管理（5項目）

システム管理者がネットワークを導入及び更新する上での対策についてまとめたもの。

③運用管理（9項目）

システム管理者がシステムを維持及び管理する上での対策についてまとめたもの。

④事後対応（6項目）

システム管理者がウイルスを発見した場合及びシステムユーザから発見の連絡を受けた場合の対策についてまとめたもの。

⑤教育・啓蒙（2項目）

システム管理者及びシステムユーザに対して行うウイルス対策の教育・啓蒙についてまとめたもの。

⑥監査（1項目）

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

（3） ソフトウェア供給者基準（21項目）

ソフトウェアの開発並びにソフトウェア製品の開発、製造及び出荷を行う者（以下「ソフトウェア供給者」とする。）のための対策をまとめたもの。

①開発管理（9項目）

ソフトウェア及びソフトウェア製品の開発並びに開発環境の導入、更新及び管理に関する対策についてまとめたもの。

②製品管理（3項目）

ソフトウェア製品の製造及び出荷をする場合の対策についてまとめたもの。

③事後対応（7項目）

ソフトウェア供給者がウイルスを発見した場合及び製品のユーザから発見の連絡を受けた場

合の対策についてまとめたもの。

④教育・啓蒙（１項目）

ソフトウェア供給者に対して行うウイルス対策の教育・啓蒙についてまとめたもの。

⑤監査（１項目）

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

（４） ネットワーク事業者基準（15 項目）

パソコン通信等のネットワークを介して情報を提供する事業者（以下「ネットワーク事業者」とする。）のための対策をまとめたもの。

①システム管理（２項目）

ネットワーク事業に用いるシステムを導入及び更新する上での対策についてまとめたもの。

②運用管理（４項目）

ネットワーク事業に用いるシステムを維持及び管理する上での対策についてまとめたもの。

③事後対応（６項目）

ネットワーク事業者がウイルスを発見した場合及びネットワークのユーザから発見の連絡を受けた場合の対策についてまとめたもの。

④教育・啓蒙（２項目）

ネットワーク事業者及びネットワークのユーザに対して行うウイルス対策の教育・啓蒙についてまとめたもの。

⑤監査（１項目）

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

（５） システムサービス事業者基準（19 項目）

システムの管理、保守、レンタル等のサービスを行う事業者（以下「システムサービス事業者」とする。）のための対策をまとめたもの。

①システム管理（５項目）

サービスに用いるシステムを導入及び更新する上での対策についてまとめたもの。

②運用管理（６項目）

サービスに用いるシステムを維持及び管理する上での対策についてまとめたもの。

③事後対応（６項目）

システムサービス事業者がウイルスを発見した場合及びサービスを受けているユーザから発見の連絡を受けた場合の対策についてまとめたもの。

④教育・啓蒙（１項目）

システムサービス事業者に対して行うウイルス対策の教育・啓蒙についてまとめたもの。

⑤監査（１項目）

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

4．システムユーザ基準

項　　目	対　策　項　目
a．ソフトウェア管理	(1) ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。 (2) オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。
b．運用管理	(1) 外部より入手したファイル及び共用するファイル媒体は、ウイルス検査後に利用すること。 (2) ウイルス感染の被害が最小となるよう、システムの利用は、いったん初期状態にしてから行うこと。 (3) ウイルス感染を早期に発見するため、システムの動作の変化に注意すること。 (4) ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。 (5) 不正アクセスによるウイルス被害を防止するため、パスワードは容易に推測されないように設定し、その秘密を保つこと。 (6) 不正アクセスによるウイルス被害を防止するため、パスワードは随時変更すること。 (7) 不正アクセスによるウイルス被害を防止するため、システムのユーザＩＤを共用しないこと。 (8) 不正アクセスによるウイルス被害を防止するため、アクセス履歴を確認すること。 (9) 不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。 (10) システムを悪用されないため、入力待ちの状態で放置しないこと。 (11) ウイルス感染を防止するため、出所不明のソフトウェアは利用しないこと。 (12) ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管すること。
c．事後対応	(1) ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。 (2) ウイルス被害の拡大を防止するため、システムの復旧は、システム管理者の指示に従うこと。 (3) ウイルス被害の拡大を防止するため、感染したプログラムを含むフロッピーディスク等は破棄すること。
d．監査	(1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

5．システム管理者基準

項　　目	対　策　項　目
a．コンピュータ管理	(1) ウイルス対策を円滑に行うため、コンピュータの管理体制を明確にすること。 (2) ウイルス感染を防止するため、機器を導入する場合は、ウイルス検査を行うこと。 (3) ウイルス感染を防止するため、コンピュータにソフトウェアを導入する場合は、ウイルス検査を行うこと。 (4) ウイルス被害に備えるため、システムにインストールした全ソフトウェアの構成情報を保存すること。 (5) オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。 (6) 不正アクセスによるウイルス被害を防止するため、システムのユーザ数及びユーザのアクセス権限を必要最小限に設定すること。 (7) ウイルス被害を防止するため、共用プログラムが格納されているディレクトリに対するシステムのユーザの書き込みを禁止すること。 (8) ウイルス被害を防止するため、システム運営に必要のないプログラムは削除すること。
b．ネットワーク管理	(1) ウイルス対策を円滑に行うため、ネットワークの管理体制を明確にすること。 (2) ウイルスに感染した場合の被害範囲を特定するため、ネットワーク接続機器の設置状況をあらかじめ記録し、管理すること。 (3) ウイルス被害に備えるため、緊急時の連絡体制を定め、周知・徹底すること。 (4) 不正アクセスによるウイルス被害を防止するため、ネットワーク管理情報のセキュリティを確保すること。 (5) 不正アクセスによるウイルス被害を防止するため、外部ネットワークと接続する機器の

項　　目	対　策　項　目
	セキュリティを確保すること。
c．運用管理	（1）　システムの重要情報の管理体制を明確にすること。 （2）　不正アクセスからシステムの重要情報を保護するため、システムが有するセキュリティ機能を活用すること。 （3）　パスワードを容易に推測されないようにするため、安易なパスワード設定を排除すること。 （4）　ウイルスの被害に備えるため、運用システムのバックアップを定期的に行い、一定期間保管すること。 （5）　ウイルスの被害を防止するため、匿名で利用できるサービスは限定すること。 （6）　不正アクセスを発見するため、アクセス履歴を定期的に分析すること。 （7）　ウイルス感染を早期に発見するため、システムの動作を監視すること。 （8）　ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。 （9）　システムの異常が発見された場合は、速やかに原因を究明すること。
d．事後対応	（1）　ウイルス感染の拡大を防止するため、感染したシステムの使用を中止すること。 （2）　ウイルス感染の拡大を防止するため、必要な情報をシステムユーザに、速やかに通知すること。 （3）　ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。 （4）　安全な復旧手順を確立して、システムの復旧作業にあたること。 （5）　ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。 （6）　ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
e．教育・啓蒙	（1）　ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。 （2）　セキュリティ対策及びウイルス対策について、システムユーザの教育・啓蒙を行うこと。
f．監査	（1）　ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

6．ソフトウェア供給者基準

項　　目	対　策　項　目
a．開発管理	（1）　開発ツールからウイルスが開発システムに感染するのを防ぐため、開発ツールの管理体制を明確にすること。 （2）　パスワードの漏えいを防ぐため、パスワードを厳重に管理すること。 （3）　不正利用によるウイルス被害を防止するため、開発システムを厳重に管理すること。 （4）　不正アクセスによるウイルス被害を防止するため、ネットワーク等を利用した開発システムへのアクセスに対しては、セキュリティを強化すること。 （5）　不正アクセスによるウイルス被害を防止するため、開発者のアクセス権限を必要最小限に設定すること。 （6）　開発段階のプログラムに対して開発者、修正者及び責任者を明確にし、厳重に管理すること。 （7）　ウイルス被害に備えるため、開発段階のプログラムのバックアップを行い保存すること。 （8）　不正利用を防止するため、開発終了時にプログラム内のデバッグ機能を確実に取り除くこと。 （9）　ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。
b．製品管理	（1）　製品の製造段階でのウイルス感染を防止するため、専用のシステム又は機器を用いて複製を行うこと。 （2）　ウイルス感染を防止するため、製品の原本は、厳重に管理すること。 （3）　製品の流通段階でのウイルス感染を防止するため、ライトプロテクト、密封包装等の対策を施すこと。
c．事後対応	（1）　製品のウイルス感染を発見した場合は、流通を停止し、製品のユーザに情報を通知するとともに製品の回収を行うこと。 （2）　ウイルス感染の拡大を防止するため。感染した開発システムの使用を中止すること。 （3）　ウイルス感染の拡大を防止するため、必要な情報を関連する全てのソフトウェア供給者に、速やかに通知すること。

項　　目	対　策　項　目
	(4) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。 (5) 安全な復旧手順を確立して、開発システムの復旧作業にあてること。 (6) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。 (7) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
d．教育・啓蒙	(1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。
e．監査	(1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

7．ネットワーク事業者基準

項　　目	対　策　項　目
a．システム管理	(1) ウイルスに感染した場合の被害範囲を特定するため、ネットワーク事業に用いるシステムの設定状況をあらかじめ記録し、管理すること。 (2) ウイルス被害に備えるため、緊急時の連絡体制を定め、周知・徹底すること。
b．運用管理	(1) 不正アクセスによるウイルス被害を防止するため、ネットワークのユーザのアクセス権限を必要最小限に設定すること。 (2) ウイルス被害を防止するため、ファイルを公開する前に、最新のワクチンの利用等によりウイルス検査を行うこと。 (3) 不正アクセスによるウイルス被害を防止するため、パスワード等のネットワーク管理情報を厳重に管理すること。 (4) ウイルス被害に備えるため、利用状況の履歴を常に記録し、一定期間保存すること。
c．事後対応	(1) ウイルス被害の拡大を防止するため、ウイルスを含むファイルの公開を停止すること。 (2) ウイルス感染の拡大を防止するため、必要な情報をネットワークのユーザ及び他のネットワーク事業者に、速やかに通知すること。 (3) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。 (4) 安全な復旧手順を確立して、その情報をネットワークのユーザに通知すること。 (5) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。 (6) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
d．教育・啓蒙	(1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。 (2) セキュリティ対策及びウイルス対策について、ネットワークのユーザの教育・啓蒙を行うこと。
e．監査	(1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

8．システムサービス事業者基準

項　　目	対　策　項　目
a．システム管理	(1) ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。 (2) 不正利用を防止するため、保守機能を含むソフトウェア及びその情報は厳重に管理すること。 (3) オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。 (4) サービスに用いるディスクは、初期化したディスクを用いて、オリジナルプログラムから作成すること。 (5) ウイルス被害に備えるため、サービスに用いるディスクの構成情報を保存すること。
b．運用管理	(1) ウイルス被害に備えるため、サービスに用いるシステムの管理体制を明確にすること。 (2) ウイルス感染を防止するため、サービスに用いるシステムは、最新のワクチンの利用等により事前にウイルス検査を行うこと。 (3) ウイルス被害に備えるため、ウイルス検査履歴等を一定期間保管すること。 (4) ウイルス感染を防止するため、一度サービスに用いたシステムは、続けて他のサービスに利用しないこと。 (5) ウイルス被害を防止するため、サービスに必要としない機器は切り離すこと。

項　　目	対　策　項　目
	(6) サービスに用いるディスクへのウイルス感染を防止するため、ライトプロテクト措置を行うこと。
c．事後対応	(1) ウイルス感染の拡大を防止するため、サービスに用いている感染したシステムの使用を中止すること。 (2) ウイルス感染の拡大を防止するため、必要な情報をサービスを受けているユーザに、速やかに通知すること。 (3) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。 (4) 安全な復旧手順を確立して、サービスに用いているシステムの復旧作業にあたること。 (5) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。 (6) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
d．教育・啓蒙	(1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。
e．監査	(1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

9．留意事項

(1) 本基準は、コンピュータの種類、システムの形態又はソフトウェアの相違等の実態に則して活用すること。

(2) ソフトウェア供給者基準、ネットワーク事業者基準及びシステムサービス事業者基準は、各事業者特有の観点からまとめた基準であることから、各事業に用いるシステムの導入に当たっては、システム管理者基準を活用すること。

(3) システム自体の安全対策については、「情報システム安全対策基準」（平成７年通商産業省告示第５１８号）を活用すること。

(4) システム監査の実施については、「システム監査基準」（平成８年１月３０日通産省公報）を活用すること。

(5) 本基準は、原則として、企業等の組織を対象としているが、個人ユーザも活用することができる。

(6) コンピュータ不正アクセス対策については、「コンピュータ不正アクセス対策基準」（平成８年通商産業省告示第３６２号）を活用すること。

(7) コンピュータウイルス、不正アクセス、災害等の対策としては、警察庁からも「情報システム安全対策指針」（平成９年国家公安委員会告示第９号）が発表されており、本基準と併せて活用することにより、情報システムのセキュリティを高めることができる。

○通商産業省告示第９５１号

平成７年通商産業省告示第４２９号（コンピュータウイルス対策基準）に基づき、経済産業大臣が別に指定する者を次のように定め、平成１３年１月６日から施行する。

なお、平成７年通商産業省告示第４３０号（コンピュータウイルス対策基準に基づく通商産業大臣が別に指定する者）は、平成１３年１月５日限り、廃止する。

平成１２年１２月２８日

１．名称　　情報処理振興事業協会

２．主たる所在地　　東京都文京区本駒込二丁目二十八番八号

ソフトウェア管理ガイドライン

平成７年11月15日策定

1．主旨

本ガイドラインは、ソフトウェアの違法複製等を防止するため、法人、団体等（以下「法人等」という。）を対象として、ソフトウェアを使用するに当たって実行されるべき事項をとりまとめたものである。

2．用語の定義

本ガイドラインに用いられる主な用語の定義は、以下のとおりである。

(1) ソフトウェア

パーソナルコンピュータで稼動し、一般に市販・流通しているシステムプログラム、アプリケーションプログラム、ユーティリティプログラム等のパッケージソフトウェアをいう。

(2) 違法複製等

ソフトウェアは、著作物として著作権法で保護されており、著作権者に無断で複製することは禁止されている。この場合、著作権法及び使用許諾契約書（約款）に違反して複製する行為を示す。

(3) 使用許諾契約（約款）

ソフトウェアメーカ（著作権者）が、ソフトウェアの使用権をユーザに許諾するための契約（約款）で、ソフトウェアの利用範囲、使用条件が記載されている。

3．構成

本ガイドラインは、法人等が実施すべき基本的事項、ソフトウェア管理責任者が実施すべき事項、ソフトウェアユーザが実施すべき事項から成り、その構成及び内容は以下のとおりである。

(1) 法人等が実施すべき基本的事項

法人等が、自己の組織内においてソフトウェアの違法複製等が行われることを防止するために行うべき最も基本的な事項についてまとめたもの。

(2) ソフトウェア管理責任者が実施すべき事項

法人等におけるソフトウェアの使用等について責任を負う者（以下「ソフトウェア管理責任者」という。）が行うべき事項についてまとめたもの。

(3) ソフトウェアユーザが実施すべき事項

法人等の事業所においてソフトウェアを使用する法人等の構成員（以下「ソフトウェアユーザ」という。）が行うべき事項についてまとめたもの。

4．法人等が実施すべき基本的事項

(1) ソフトウェアの使用等を的確に管理し、ソフトウェアの違法複製等の行為を効果的に防止するため、法人等におけるソフトウェアの使用等について責任を負うソフトウェア管理責任者を任命し、ソフトウェアの適切な管理体制を整備すること。

(2) ソフトウェアの適正な使用等を確立するため、ソフトウェアの使用手順や管理方法等を定めたソフトウェア管理規則を策定すること。

(3) ソフトウェアの違法複製等の有無を確認するため、すべてのソフトウェアを対象として、ソ

フトウェアの使用状況についての監査（以下「ソフトウェア監査」という。）を実施すること。

(4) ソフトウェアの適正な使用等に対するソフトウェアユーザ意識の向上を図るため、関係法令や使用許諾契約等について、ソフトウェアユーザの教育、啓蒙を行うこと。

5．ソフトウェア管理責任者が実施すべき事項

(1) 法人等におけるソフトウェアの使用状況を常時把握するため、すべてのソフトウェアの使用状況を記録したソフトウェア管理台帳を整備すること。

(2) ソフトウェア監査等によりソフトウェアの違法複製等を発見した場合は、事情を調査した上で、違法複製されたソフトウェアを消去する等、適切な措置を速やかに講じること。

(3) すべてのソフトウェアユーザを対象として、関係法令、ソフトウェア管理規則、使用許諾契約に規定された使用条件等の周知徹底を図ること。

6．ソフトウェアユーザが実施すべき事項

(1) 関係法令、ソフトウェア管理規則及び使用許諾契約に規定された使用条件並びにソフトウェア管理責任者の指示を遵守すること。

(2) 法人等が保有するソフトウェアと個人が保有するソフトウェアとの区分が不明確になることを防ぐため、個人が保有するソフトウェアを法人等の事業所において使用する場合、予めソフトウェア管理責任者の承諾を得ること。

7．留意事項

本ガイドラインは、法人等におけるソフトウェアの使用数、組織の規模等の実態に則して運用すること。

コンピュータ不正アクセス対策基準

平成８年８月８日（通商産業省告示第３６２号）（制定）
平成９年９月24日（通商産業省告示第５３４号）（改定）
平成12年12月28日（通商産業省告示第９５０号）（最終改定）

コンピュータ不正アクセス対策基準を次のように定め、平成８年８月８日から施行する。

Ⅰ．主旨

本基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。

Ⅱ．用語の定義

本基準で用いられる用語の定義は、以下のとおりである。

1．コンピュータ不正アクセス（以下「不正アクセス」とする。）

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。

2．ソフトウェア

システムプログラム、アプリケーションプログラム、ユーティリティプログラム等のプログラム及びそれに付随するデータ

3．コンピュータ

ネットワークに接続され得るコンピュータであり、ルータ、交換機等の通信用コンピュータ及びその他専用コンピュータを含むもの。

4．ネットワーク

通信回線及び通信機器の複合体

5．システム

コンピュータ及びネットワークの複合体

6．ファイル

記憶装置又は記録媒体上に記録されているプログラム、データ等

7．機器

ハードウェア、通信回線又は通信機器

8．バックアップ

プログラム、データ等と同一の内容を別の媒体に記録すること。

9．保守機能

システムを正常な状態に維持するための機能

Ⅲ．構成

本基準は、システムユーザ基準、システム管理者基準、ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準からなり、その構成及び内容は以下のとおりである。

1．システムユーザ基準

システムを利用する者（以下「システムユーザ」とする。）が実施すべき対策についてまとめたもの。

（1） パスワード及びユーザＩＤ管理（９項目）

システムユーザ自身が使用するパスワード及びユーザＩＤを管理する際に実施すべき対策についてまとめたもの。

（2） 情報管理（７項目）

システムユーザ自身が利用する情報を管理する際に実施すべき対策についてまとめたもの。

（3） コンピュータ管理（6項目）

システムユーザ自身が利用するコンピュータを利用及び管理する際に実施すべき対策についてまとめたもの。

（4） 事後対応（2項目）

システムの異常及び不正アクセスをシステムユーザが発見した場合の対応についてまとめたもの。

（5） 教育及び情報収集（2項目）

セキュリティ対策に関する教育及び情報の収集についてまとめたもの。

（6） 監査（1項目）

不正アクセス対策を適切に実施するための監査についてまとめたもの。

2．システム管理者基準

システムユーザの管理並びにシステム及びその構成要素の導入、維持、保守等の管理を行う者(以下「システム管理者」とする。）が、実施すべき対策についてまとめたもの。

（1） 管理体制の整備（7項目）

システム及びその構成要素を管理するための体制を整備する際に実施すべき対策についてまとめたもの。

（2） システムユーザ管理（10項目）

システムユーザをシステム管理者が管理する際に実施すべき対策についてまとめたもの。

（3） 情報管理（8項目）

システム全体の情報をシステム管理者が管理する際に実施すべき対策についてまとめたもの。

（4） 設備管理（18項目）

ハードウェア、ソフトウェア、通信回線及び通信機器並びにそれらの複合体をシステム管理者が管理する際に実施すべき対策についてまとめたもの。

（5） 履歴管理（4項目）

システムの動作履歴、使用記録等をシステム管理者が記録、分析及び保存する際に実施すべき対策についてまとめたもの。

（6） 事後対応（6項目）

システム全体の異常及び不正アクセスをシステム管理者が発見した場合並びにシステムユーザからの発見の連絡を受けた場合の対応についてまとめたもの。

（7） 情報収集及び教育（4項目）

セキュリティ対策に関する情報の収集及びその活用方法並びにシステムユーザへの教育についてまとめたもの。

（8） 監査（1項目）

不正アクセス対策を適切に実施するための監査についてまとめたもの。

3．ネットワークサービス事業者基準

ネットワークを利用して、情報サービス及びネットワーク接続サービスを提供する事業者（以下「ネットワークサービス事業者」とする。）が実施すべき対策についてまとめたもの。

（1） 管理体制の整備（２項目）

ネットワークサービスを行うための体制を整備する際に実施すべき対策についてまとめたもの。

（2） ネットワークサービスユーザ管理（７項目）

ネットワークサービスユーザをネットワークサービス事業者が管理する際に実施すべき対策についてまとめたもの。

（3） 情報管理（３項目）

ネットワークサービスユーザ及び事業者自身の情報を管理する際に実施すべき対策についてまとめたもの。

（4） 設備管理（５項目）

ネットワークサービスに係る機器をネットワークサービス事業者が管理する際に実施すべき対策についてまとめたもの。

（5） 事後対応（６項目）

ネットワークサービスに係るシステムの異常及び不正アクセスをネットワークサービス事業者が発見した場合並びに発見の連絡を受けた場合の対応についてまとめたもの。

（6） 情報収集及び教育（３項目）

セキュリティ対策に関する情報の収集及びその活用方法並びにネットワークサービスユーザへの教育についてまとめたもの。

（7） 監査（１項目）

不正アクセス対策を適切に実施するための監査についてまとめたもの。

4．ハードウェア・ソフトウェア供給者基準

ハードウェア及びソフトウェア製品の開発、製造、販売等を行う者（以下「ハードウェア・ソフトウェア供給者」とする。）が、実施すべき対策についてまとめたもの。

（1） 管理体制の整備（２項目）

ハードウェア及びソフトウェアを供給するための体制について実施すべき対策をまとめたもの。

（2） 設備管理（２項目）

ハードウェア及びソフトウェア製品の開発及び製造に係る機器をハードウェア・ソフトウェア供給者が管理する際に実施すべき対策についてまとめたもの。

（3） 開発管理（７項目）

ハードウェア及びソフトウェア製品をハードウェア・ソフトウェア供給者が開発及び製造する際に実施すべき対策についてまとめたもの。

（4） 販売管理（４項目）

ハードウェア及びソフトウェア製品をハードウェア・ソフトウェア供給者が販売等を行う場合に実施すべき対策についてまとめたもの。

（5） 事後対応（6項目）

開発システムの異常及び不正アクセスをハードウェア・ソフトウェア供給者が発見した場合の対応についてまとめたもの。

（6） 情報収集及び教育（2項目）

セキュリティ対策に関する情報の収集及びその活用方法並びに製品のユーザに対する教育についてまとめたもの。

（7） 監査（1項目）

不正アクセス対策を適切に実施するための監査についてまとめたもの。

Ⅳ. 個人ユーザが留意する点

本基準は、企業等の組織及び個人を対象としているが、構成の便宜上、組織を対象とした記述となっているため、個人ユーザは以下の項目について留意することにより、不正アクセスからの被害を防止することができる。

1．不正アクセスによる被害の予防について

「Ｖ1．システムユーザ基準」の「(1) パスワード及びユーザＩＤ管理」、「(2) 情報管理」、「(3) コンピュータ管理」の中の必要な項目

2．不正アクセスによる被害の発見、復旧、拡大及び再発防止について

「Ｖ2．システム管理者基準」の「(6) 事後対応」

Ⅴ. 基準項目

1．システムユーザ基準

項　　目	対　策　項　目
（1） パスワード及びユーザID管理	1. ユーザIDは、複数のシステムユーザで利用しないこと。 2. ユーザIDは、パスワードを必ず設定すること。 3. 複数のユーザIDを持っている場合は、それぞれ異なるパスワードを設定すること。 4. 悪いパスワードは、設定しないこと。 5. パスワードは随時変更すること。 6. パスワードは、紙媒体等に記述しておかないこと。 7. パスワードを入力する場合は、他人に見られないようにすること。 8. 他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。 9. ユーザIDを利用しなくなった場合は、速やかにシステム管理者に届け出ること。
（2） 情報管理	1. 重要な情報は、パスワード、暗号化等の対策を図ること。 2. 重要な情報を送信する場合は相手先を限定し、宛先を十分に確認すること。 3. ファイルの属性は、内容の重要度に応じたアクセス権限を必ず設定すること。 4. コンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。 5. 重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。 6. 重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。 7. ファイルのバックアップを随時行い、その磁気媒体等を安全な場所に保管すること。
（3） コンピュータ管理	1. コンピュータ、通信機器及びソフトウェアの導入、更新、撤去等を行う場合は、システム管理者の指導の下で行うこと。 2. コンピュータを管理するために与えられた最上位の権限（以下「特権」とする。）によるコンピュータの利用は、必要最小限にすること。 3. 特権によりコンピュータを利用する場合は、コンピュータ、場所、期間等を限定すること。 4. コンピュータが無断で利用された形跡がないか、利用履歴等を随時確認すること。

項　　目	対　策　項　目
	5. コンピュータを入力待ち状態で放置しないこと。 6. パスワードの入力を省略する機能は、システム管理者の指導の下で使用すること。
（4）　事後対応	1. システムの異常を発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。 2. 不正アクセスを発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。
（5）　教育及び情報収集	1. システム管理者からセキュリティ対策に関する教育を随時受けること。 2. セキュリティ対策に関する情報を入手した場合は、システム管理者に随時提供すること。
（6）　監査	1. システムユーザが行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

2．システム管理者基準

項　　目	対　策　項　目
（1）　管理体制の整備	1. システムのセキュリティ方針を確立し、周知・徹底すること。 2. システムの管理体制、管理手順を確立し、周知・徹底すること。 3. 緊急時の連絡体制及び復旧手順を確立し、周知・徹底すること。 4. システム管理の業務上知り得た情報の秘密を守ること。 5. システム管理者の権限は、業務を遂行する上で必要最小限にすること。 6. システム管理者は２人以上かつ必要最小限の管理者で、その業務は定期的に交代すること。 7. システム管理者の資格を喪失した者の権限は、速やかに停止すること。
（2）　システムユーザ管理	1. システムユーザの登録は、必要な機器に限定し、システムユーザの権限を必要最小限に設定すること。 2. ネットワークを介して外部からアクセスできるユーザ ID は、必要最小限にすること。 3. ユーザ ID は、個人単位に割り当て、パスワードを必ず設定すること。 4. 長期間利用していないユーザ ID は、速やかに停止すること。 5. ユーザ ID の廃止等の届出があった場合は、速やかに登録を抹消すること。 6. パスワードは、当該システムユーザ以外に知らせないこと。 7. パスワードのチェックを随時行い、悪いパスワードは、速やかに変更させること。 8. パスワードが当該システムユーザ以外に知られた場合又はその疑いのある場合は、速やかに変更させること。 9. 特権を付与する場合は、当該システムユーザの技術的能力等を考慮すること。 10. 必要としなくなったシステムユーザの特権は、速やかに停止すること。
（3）　情報管理	1. 通信経路上の情報は、漏えいを防止する仕組みを確立すること。 2. 通信経路上で情報の盗聴及び漏えいが行われても、内容が解析できない機密保持機能を用いること。 3. 通信経路上で情報の改ざんが行われても、検出できるような改ざん検知機能を用いること。 4. システム関連のファイルは、システムユーザがアクセスできないように管理すること。 5. 重要な情報は、削除、改ざん、漏えい等による被害が少なくなるように分散化すること。 6. 重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。 7. 重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。 8. ファイルのバックアップを随時行い、その磁気媒体等を安全な方法で保管すること。
（4）　設備管理	1. すべての機器及びソフトウェアの管理者を明確にすること。 2. 重要な情報が格納されているか又は重要な処理を行う機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。 3. 移動可能な機器は、盗難防止策を行うこと。 4. システム構成を常に把握しておくこと。 5. 機器及びソフトウェアを導入する場合は、セキュリティ機能がセキュリティ方針に適合していることをあらかじめ確認してから行うこと。 6. 機器及びソフトウェアの設定情報がシステムに適合していることを随時確認すること。 7. 機器及びソフトウェアは、供給者の連絡先及び更新情報が明確なものを利用すること。 8. セキュリティ上の問題点が解決済みの機器及びソフトウェアを利用すること。 9. 外部と接続する機器は、十分なアクセス制御機能を有したものを利用すること。 10. システム構成の変更を行う前に、セキュリティ上の問題が生じないことを確認すること。 11. ネットワークを介して外部からアクセスできる通信経路及びコンピュータは、必要最小限にすること。

項　目	対　策　項　目
	12. ネットワークを介して外部からシステム管理を行う場合は、認証機能、暗号機能及びアクセス制御機能を設定すること。 13. 長期間利用しない機器は、システムに接続しないこと。 14. 機器及びソフトウェアの廃棄、返却、譲渡等を行う場合は、情報の漏えいを防ぐ対策を行うこと。 15. ソフトウェア及びシステムファイルの改ざんが生じていないことを随時確認すること。 16. システムが提供するパスワード強化機能は最大限に活用すること。 17. ネットワークの負荷状況を監視すること。 18. システムの利用形態等に応じて、ネットワークを分離すること。
(5)　履歴管理	1. システムのセキュリティ方針に基づいたシステムの動作履歴、使用記録等を記録すること。 2. システムの動作履歴、使用記録等を記録する場合は、改ざん、削除、破壊及び漏えいの防止措置を施すこと。 3. 記録したシステムの動作履歴、使用記録等を随時分析すること。 4. 記録したシステムの動作履歴、使用記録等は、安全な方法で一定期間保管すること。
(6)　事後対応	1. 異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。 2. 不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。 3. 関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。 4. 事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。 5. 不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。 6. 不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
(7)　情報収集及び教育	1. セキュリティ対策に関する情報を随時収集すること。 2. 収集した情報を分析し、重要な情報については速やかに対応すること。 3. システムユーザがセキュリティ対策を行う場合に必要な情報を提供すること。 4. システムユーザに、セキュリティ教育を随時実施すること。
(8)　監査	1. システム管理者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

3．ネットワークサービス事業者基準

項　目	対　策　項　目
(1)　管理体制の整備	1. ネットワークサービス事業者の要員の業務範囲を明確にすること。 2. 不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知・徹底すること。
(2)　ネットワークサービスユーザ管理	1. ネットワークサービス事業者及びネットワークサービスユーザの責任範囲を明確にすること。 2. ネットワークサービス事業者が提供できるセキュリティサービスを明示すること。 3. ネットワークサービスユーザとの連絡体制を複数確立し、周知・徹底すること。 4. 不正アクセスを行ったネットワークサービスユーザに対するサービスを制限できる仕組みを確立すること。 5. ネットワークサービスユーザから要求があった場合、本人の利用情報等を開示すること。 6. ネットワークサービスユーザへの不正アクセスを監視できる仕組みを確立すること。 7. ネットワークサービスユーザの利用情報等を記録できる仕組みを確立すること。
(3)　情報管理	1. ネットワークサービスユーザの情報は、厳重に管理すること。 2. ネットワークサービスユーザの情報を公開する場合は、本人の了解を得ること。 3. ネットワーク構成等の重要な情報は、公開しないこと。
(4)　設備管理	1. ネットワークサービスに係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。 2. ネットワークサービスに係る機器の管理が常に可能な仕組みを確立すること。 3. ネットワークサービスに係る機器を遠隔管理する通信回線は、複数確保すること。 4. ネットワークサービスユーザにサービスを提供するネットワークは、他の業務のネットワークと分離すること。 5. 特定のサービスに関する情報は、そのサービスに関連した機器に限定して流すこと。
(5)　事後対応	1. 異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。 2. 不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。 3. 関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。

項　目	対　策　項　目
	4. 事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。 5. 不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。 6. 不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
(6) 情報収集及び教育	1. セキュリティ対策に関する情報を随時収集すること。 2. ネットワークサービスユーザがセキュリティ対策を行う場合に必要な情報を提供すること。 3. ネットワークのセキュリティ上の問題及びその対策に関する十分な情報を提供し、必要に応じてその情報を活用するための教育をすること。
(7) 監査	1. ネットワークサービス事業者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

4．ハードウェア・ソフトウェア供給者基準

項　目	対　策　項　目
(1) 管理体制の整備	1. ハードウェア・ソフトウェア供給者の要員の業務範囲を明確にすること。 2. 不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知・徹底すること。
(2) 設備管理	1. 開発業務に係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。 2. 開発業務に係るネットワークは、他の業務のネットワークと分離すること。
(3) 開発管理	1. 製品のセキュリティ機能の実装に関する方針を明確にすること。 2. 製品は、機密保持機能、認証機能、改ざん検知機能等のセキュリティ機能を設けること。 3. 製品のネットワークに係る機能は、セキュリティ上の重要な情報の解析を防ぐ機能を組み込むこと。 4. 製品の保守に係る機能は、利用する者を限定する機能を組み込むこと。 5. セキュリティの設定を行わないと製品が利用できない機能を設けること。 6. 製品の開発に使用したデバッグ機能等は、出荷前に削除しておくこと。 7. 製品のセキュリティ機能が仕様どおり動作するか検査すること。
(4) 販売管理	1. 製品は、流通段階における改ざん等を防止するための措置を施すこと。 2. 製品は、利用上の制限事項及び推奨事項を明示の上、販売等を行うこと。 3. 製品は、供給者の連絡先を明示しておくこと。 4. 製品にセキュリティ上の問題が発見された場合は、製品のユーザ及び関係者に情報を通知するとともに、問題を解決するための適切な処置を行うこと。
(5) 事後対応	1. 製品開発システムにおける異常を発見した場合は、速やかに原因を追究すること。 2. 不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。 3. 関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。 4. 事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。 5. 不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。 6. 不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。
(6) 情報収集及び教育	1. 製品のセキュリティ対策に関する情報を随時収集し、その情報を製品の開発に生かすこと。 2. 製品の販売を通じてセキュリティ対策の情報を提供し、必要に応じて教育を行うこと。
(7) 監査	1. ハードウェア・ソフトウェア供給者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

VI. 留意事項

1．本基準は、システムの構成及び利用形態、取り扱う情報等に則して活用すること。

2．ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準は、各事業者特有の観点からまとめた基準であることから、各事業の機器の導入等にあたっては、システム管理者基準も併せて活用すること。

3．コンピュータウイルス対策の実施については、「コンピュータウイルス対策基準」（平成７年７月７日付　通産省告示第４２９号）を活用すること。

4．システム自体の安全対策の実施については、「情報システム安全対策基準」（平成７年８月２９日付　通産省告示第５１８号）を活用すること。
5．システム監査の実施については、「システム監査基準」（平成８年１月３０日付　通産省公報）を活用すること。
6．ソフトウェア管理の実施については、「ソフトウェア管理ガイドライン」（平成７年１１月１５日付　通産省公報）を活用すること。
7．コンピュータウイルス、不正アクセス、災害等の対策としては、警察庁からも「情報システム安全対策指針」（平成９年国家公安委員会告示第９号）が発表されており、本基準と併せて活用することにより、情報システムのセキュリティを高めることができる。

通商産業省告示第９４９号

平成８年通商産業省告示第３６２号（コンピュータ不正アクセス対策基準）に基づき、経済産業大臣が別に指定する者を次のように定め、平成１３年１月６日から施行する。

なお、平成８年通商産業省告示第３６３号（コンピュータ不正アクセス対策基準に基づく通商産業大臣が別に指定する者）は、平成１３年１月５日限り、廃止する。

平成１２年１２月２８日

１．名称　　情報処理振興事業協会
２．主たる所在地　　東京都文京区本駒込二丁目二十八番八号

情報セキュリティ監査基準

平成15年４月１日策定

前文

情報セキュリティを脅かすリスクが多様化し複雑化している現状に鑑みるとき、情報セキュリティ監査は、情報セキュリティに係るリスクのマネジメントが効果的に実施されていることを担保するための有効な手段となる。情報セキュリティ監査は、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を与えるものだからである。

情報セキュリティ対策は、本来的には、企業、団体、自治体等の組織体の責任において遂行されるべきものであるが、情報セキュリティをマネジメントプロセスに組み込んで構築し運用するためには、管理サイクルの見直しにとって情報セキュリティ監査は不可欠な要素となる。さらに、外部利害関係者との影響関係を視野に入れた IT ガバナンスという観点からも、情報セキュリティ監査のモニタリング機能としての重要性は益々高まってきている。

情報セキュリティ監査基準とは、情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。本監査基準は、監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」、監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」、監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」からなっている。

情報セキュリティ監査基準は、組織体の内部監査部門等が実施する情報セキュリティ監査だけでなく、組織体の外部者に監査を依頼する情報セキュリティ監査においても利用できる。さらに、本監査基準は、情報セキュリティに保証を付与することを目的とした監査であっても、情報セキュリティの欠陥に対して助言を行うことを目的とした監査であっても利用できる。

情報セキュリティ監査の実施に当たっては、組織体における情報セキュリティの適否を判断するための尺度が必要である。情報セキュリティ監査は、本監査基準の姉妹編である情報セキュリティ管理基準を監査上の判断の尺度として用い、監査対象が情報セキュリティ管理基準に準拠しているかどうかという視点で行われることを原則とする。情報セキュリティ管理基準は、国際規格をもとに作成されており、組織体が情報セキュリティを構築し運用するための標準的な対策を提供している。しかし、情報セキュリティ管理基準に基づく監査に限らず、各種目的あるいは各種形態をもって実施される情報セキュリティ監査においても本監査基準を活用することができる。

情報セキュリティ監査の目的

情報セキュリティ監査の目的は、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにある。

情報セキュリティのマネジメントは第一義的には組織体の責任において行われるべきものであり、情報セキュリティ監査は組織体のマネジメントが有効に行われることを保証又は助言を通じて支援するものである。

情報セキュリティ監査は、情報セキュリティに係るリスクのマネジメント又はコントロールを対象として行われるものであるが、具体的に設定される監査の目的と監査の対象は監査依頼者の要請に応じたものでなければならない。

一般基準

1．目的、権限と責任

情報セキュリティ監査を実施する目的及び対象範囲、並びに情報セキュリティ監査人の権限と責任は、文書化された規程又は契約書等により明確に定められていなければならない。

2．独立性、客観性と職業倫理

2.1　外観上の独立性

情報セキュリティ監査人は、情報セキュリティ監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

2.2　精神上の独立性

情報セキュリティ監査人は、情報セキュリティ監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

2.3　職業倫理と誠実性

情報セキュリティ監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

3．専門能力

情報セキュリティ監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

4．業務上の義務

4.1　注意義務

情報セキュリティ監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

4.2　守秘義務

情報セキュリティ監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。

5．品質管理

情報セキュリティ監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。

実施基準

1．監査計画の立案

情報セキュリティ監査人は、実施する情報セキュリティ監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。

2．監査の実施

2.1　監査証拠の入手と評価

情報セキュリティ監査人は、監査計画に基づいて、適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

2.2　監査調書の作成と保存

情報セキュリティ監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

3．監査業務の体制

情報セキュリティ監査人は、情報セキュリティ監査の目的が有効かつ効率的に達成されるように、

適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導までの監査業務の全体を管理しなければならない。

4．他の専門職の利用

情報セキュリティ監査人は、情報セキュリティ監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、情報セキュリティ監査人の責任において行われなければならない。

報告基準

1．監査報告書の提出と開示

情報セキュリティ監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、情報セキュリティ監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

2．監査報告の根拠

情報セキュリティ監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

3．監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、その他特記すべき事項について、情報セキュリティ監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。

4．監査報告についての責任

監査報告書の記載事項については、情報セキュリティ監査人がその責任を負わなければならない。

5．監査報告に基づく改善指導

情報セキュリティ監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。

情報セキュリティ管理基準

平成15年４月１日策定

前文

インターネットを中核とする情報技術が組織体の活動や社会生活に深く浸透することに伴い、情報セキュリティの確保は、組織体が有効かつ効率的に事業活動を遂行するための前提条件となり、また安全な社会生活を支える基盤条件となっている。国際社会においても情報セキュリティ確保の要請は喫緊の課題とされている。

情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備、運用するための実践規範である。情報セキュリティマネジメントは、第一義的には、組織体における必要性と組織体の責任において果たされるべきものである。本管理基準は、情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定することによって、組織体が情報セキュリティマネジメント体制の構築と、適切なコントロールの整備と運用を効果的に導入できるように支援することを目的としている。

情報セキュリティ管理基準は、情報セキュリティに係るマネジメントサイクル確立のための国際標準規格である ISO/IEC 17799:2000（JIS X 5080:2002）をもとにしており、情報資産を保護するための最適な実践慣行を帰納要約し、情報セキュリティに関する、マネジメント及びコントロールの項目を規定したものである。本管理基準は、組織体の業種及び規模等を問わず適用できるよう汎用的なものとなっている。組織体においては、本管理基準を基礎として、リスクアセスメントの結果等に基づき、独自に必要とする項目を追加、あるいは削除して活用することができる。ただし、情報セキュリティは、個々のマネジメント及びコントロールの項目が相互に結びつき合ってはじめて有効に機能するものであり、また、計画、実施、評価、是正を通じたマネジメントサイクルとして機能するように留意しなければならない。

情報セキュリティ管理基準は、主要な管理項目ごとにその目的を示し、次いで管理の目的を達成するために必要とされるコントロール目標と具体的なコントロール手続を規定している。本管理基準は、管理項目ごとにその目的から具体的なコントロール手続に至るまでを関連づけて、末広がりとなる体系性をもたせている。効果的な情報セキュリティ管理を実現するためには、マネジメントサイクル構築の出発点となるべき管理の目的を明確にした上で、リスクアセスメントに基づいた最適な管理資源の配分が行えるよう、必要とされるコントロールを対応づけてゆくことが重要となるからである。

情報セキュリティ管理基準は、本管理基準と姉妹編をなす情報セキュリティ監査基準に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。また、本管理基準は、ISMS 適合性評価制度において用いられる適合性評価の尺度と整合するように配慮している。

なお、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の趣旨及び体系に則って、該当する関係機関において独自の管理基準を策定し活用することが望ましい。

注

○コントロールについて

本管理基準中、各目的の下位に存在し、「O.O.O　……」と記述される部分を「コントロール」と呼ぶ。

例）1.1.1　経営人は、組織にまたがる情報セキュリティ基本方針の発行及び維持を通じて、明確な基本方針の方向性を定めること

○サブコントロールについて

本管理基準中、コントロールの下位に存在し、「O.O.O.O　……」と記述される部分を「サブコントロール」と呼ぶ。

例）1.1.1.1 基本方針文書には、情報セキュリティの管理に対する組織の取組み方法を明示すること

目次

1 セキュリティ基本方針

1.1 情報セキュリティ基本方針

目的：情報セキュリティのための経営陣の指針及び支持を規定するため

1.1.1 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること

1.1.1.1 基本方針文書には、経営陣の責任を明記すること

1.1.1.2 基本方針文書には、情報セキュリティの管理に対する組織の取組み方法を明示すること

1.1.1.3 基本方針文書には、情報セキュリティの定義を含めること

1.1.1.4 基本方針文書には、その目的を含めること

1.1.1.5 基本方針文書には、適用範囲を含めること

1.1.1.6 基本方針文書には、情報共有を可能にするための機構としてのセキュリティの重要性を含めること

1.1.1.7 基本方針文書には、情報セキュリティの目標を支持する経営陣の意向声明書を含めること

1.1.1.8 基本方針文書には、原則を支持する経営陣の意向声明書を含めること

1.1.1.9 基本方針文書には、法律上及び契約上の要求事項への適合を含めること

1.1.1.10 基本方針文書には、セキュリティ教育の要求事項を含めること

1.1.1.11 基本方針文書には、ウイルス及び他の悪意のあるソフトウェアの予防及び検出を含めること

1.1.1.12 基本方針文書には、事業継続管理を含めること

1.1.1.13 基本方針文書には、セキュリティ基本方針違反に対する措置を含めること

1.1.1.14 基本方針文書には、セキュリティの事件・事故を報告することを含めること

1.1.1.15 基本方針文書には、情報セキュリティマネジメントの一般的責任の定義を含めること

1.1.1.16 基本方針文書には、特定責任の定義を含めること

1.1.1.17 基本方針文書には、基本方針を支持する文書（例えば、特定の情報システムについてのより詳細なセキュリティ個別方針及び手順又は利用者が従うことが望ましいセキュリティ規則）の参照情報を含めること

1.1.1.18 基本方針文書には、この基本方針が、想定した読者にとって、適切で、利用可能で、かつ理解し易い形で、組織全体にわたって利用者に知らせること

1.1.2 基本方針には、定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が存在すること

1.1.2.1 見直し手続によって、当初のリスクアセスメントの基礎事項に影響を及ぼす変化（例えば、重大なセキュリティの事件・事故、新しいぜい（脆）弱性、又は組織基盤若しくは技術基盤の変化）に対応して確実に見直しを実施すること

1.1.2.2 記録されたセキュリティの事件・事故の性質、回数及び影響によって示される、

基本方針の有効性について、日程を定め、定期的に見直しを実施すること

1.1.2.3 事業効率における管理策の費用及び影響について、日程を定め、定期的に見直しを実施すること

1.1.2.4 技術変更による効果について、日程を定め、定期的に見直しを実施すること

2 組織のセキュリティ

2.1 情報セキュリティ基盤

目的：組織内の情報セキュリティを管理するため

2.1.1 セキュリティを主導するための明りょうな方向付け及び経営者による目に見える形での支持を確実にするために、運営委員会を設置すること

2.1.2 運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること

2.1.2.1 運営委員会は、適切な責任及び資源配分によって、組織内におけるセキュリティを促進すること

2.1.2.2 運営委員会は、情報セキュリティ基本方針並びに全体的な責任の見直し及び承認をすること

2.1.2.3 運営委員会は、情報資産が重大な脅威にさらされていることを示す変化を監視すること

2.1.2.4 運営委員会は、情報セキュリティの事件・事故の見直し及び監視をすること

2.1.2.5 運営委員会は、情報セキュリティを強化するための主要な発議の承認をすること

2.1.2.6 運営委員会は、一人の管理者が、すべてのセキュリティ関連活動に責任をもつこと

2.1.3 大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を設置すること

2.1.3.1 管理者の代表を集めた委員会では、組織全体の情報セキュリティのそれぞれの役割及び責任への同意を得ること

2.1.3.2 管理者の代表を集めた委員会では、情報セキュリティのための個別の方法及び手順（例えば、リスクアセスメント、セキュリティの分類体系）への同意を得ること

2.1.3.3 管理者の代表を集めた委員会では、組織全体の情報セキュリティの発議（例えば、セキュリティの意識向上プログラム）への同意及び支持を得ること

2.1.3.4 管理者の代表を集めた委員会では、セキュリティを、情報化計画の作成過程の一部にすることを確実にすること

2.1.3.5 管理者の代表を集めた委員会では、新しいシステム又は新しいサービスのため

のそれぞれの情報セキュリティの管理策の妥当性の評価及びその実施の調整をすること

2.1.3.6 管理者の代表を集めた委員会では、情報セキュリティの事件・事故の見直しをすること

2.1.3.7 管理者の代表を集めた委員会では、組織全体への情報セキュリティに対する目に見える形での業務上の支援の促進をすること

2.1.4 個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を、明確に定めること

2.1.4.1 情報セキュリティ基本方針には、組織内のセキュリティの役割及び責任の割当てに関する全般的な手引を規定すること

2.1.4.2 情報セキュリティ基本方針に、個別のサイト、システム又はサービスに関するより詳細な手引を追加すること

2.1.4.3 個々の物理的資産及び情報資産に限定した責任、並びに事業継続計画のようなセキュリティ手順を、明確に定義すること

2.1.4.4 一人の情報セキュリティ管理者を任命すること

2.1.4.5 情報資産の責任者は、その資産のセキュリティに対して最終的な責任をもつこと

2.1.4.6 情報資産の責任者は、委任された責任が正しく果たされたかを判断できること

2.1.4.7 各管理者が責任を負う範囲は明確に規定すること

2.1.4.8 個々のシステムに関連したいろいろな資産及びセキュリティ手順は、識別され、及び明確に定義されること

2.1.4.9 各資産又はセキュリティ手順に対する管理者の責任は、協議の下で決め、その責任の詳細は、文書化されること

2.1.4.10 承認の権限の範囲は、明確に定義され、文書化されること

2.1.5 新しい情報処理設備に対する経営者による認可手続を確立すること

2.1.5.1 新しい設備は、その目的及び用途について、適切な利用部門の経営陣の承認を得ること

2.1.5.2 情報システムセキュリティ環境の維持に責任をもつ管理者からも承認を得ること

2.1.5.3 ハードウェア及びソフトウェアは、他のシステム構成要素と両立できることを、確実にするために検査すること

2.1.5.4 個人が所有する情報処理設備を業務情報の処理に用いる場合、その使用及びそれに伴って必要となる管理策は、認可を得ること

2.1.5.5 職場での個人用情報処理設備の使用は、評価を受け、認可を得ること

2.1.6 専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること

2.1.6.1 専門家によるセキュリティの助言は、経験を積んだ社内の情報セキュリティ助言者が行うこと

2.1.6.2 専門家を雇わないならば、特定の個人を指名して、社内の知識及び経験を一貫性を保つように調整させ、セキュリティの方針決定を支援させること

2.1.6.3 このような任に当たる者は、自分自身の経験を超えた専門的な助言を与えるためには、適切な社外の助言者との接触をもつこと

2.1.6.4 情報セキュリティ助言者又は同等の担当者は、自らの経験又は外部の助言を用いて、情報セキュリティのあらゆる面について助言を与えることを業務とすること

2.1.6.5 助言者は、組織内のあらゆる経営陣と直接接触できること

2.1.6.6 情報セキュリティ助言者又は同等の担当者は、セキュリティの事件・事故又は違反の疑いがあるときに速やかに相談を受け付けること

2.1.6.7 情報セキュリティ助言者又は同等の担当者は、セキュリティの事件・事故又は違反の疑いがあるときに専門家の指導に関する情報又は調査手段を提供すること

2.1.7 行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること

2.1.7.1 セキュリティのグループ及び業界の委員会の一員となることも考慮すること

2.1.7.2 組織の機密情報が認可されていない人々に絶対に渡らないように、セキュリティ情報の交換を制限すること

2.1.8 情報セキュリティ基本方針の実施を、他者が見直すこと

2.1.8.1 情報セキュリティ基本方針文書には、情報セキュリティの基本方針及び責任を記述すること

2.2 第三者によるアクセスのセキュリティ

目的：第三者によってアクセスされる組織の情報処理設備及び情報資産のセキュリティを維持するため

2.2.1 組織の情報処理施設への第三者のアクセスに関連づけてリスクを評価し、適切な管理策を実施すること

2.2.1.1 物理的アクセス、例えば、事務所、コンピュータ室及びファイルキャビネットへのアクセスを考慮すること

2.2.1.2 論理的アクセス、例えば、組織のデータベース、情報システムへのアクセスを考慮すること

2.2.1.3 第三者に接続する業務上の必要がある場合には、その管理策の要求事項を明らかにするために、リスクアセスメントを実施すること

2.2.1.4 リスクアセスメントにおいては、要求されるアクセスの種類、情報の価値、第

三者が採用する管理策、及び組織の情報のセキュリティに対するこのアクセスの影響を考慮すること

2.2.1.5 第三者アクセスにかかわるすべてのセキュリティ要求事項又は内部管理策は、第三者との契約書に反映させること

2.2.1.6 情報及び情報処理施設への第三者によるアクセスは、適切な管理策を実施すること

2.2.1.7 第三者によるアクセスは、接続又はアクセスについての条件を明示した契約書を締結するまで、開始させないこと

2.2.2 組織の情報処理施設への第三者アクセスにかかわる取決めは、正式な契約に基づくこと

2.2.2.1 第三者アクセスに関する契約には、組織のセキュリティ基本方針及び標準類に適合することを確実にするために、すべてのセキュリティ要求事項を含めるか又は引用すること

2.2.2.2 第三者アクセスに関する契約書は、組織と第三者との間に誤解が全くないことを確実にするものであること

2.2.2.3 組織は、その供給業者の損失補償について納得していること

2.2.2.4 契約書には、情報セキュリティに関する一般方針を含めることを考慮すること

2.2.2.5 契約書には、情報及びソフトウェアを含む、組織の資産を保護する手順を含むことを考慮すること

2.2.2.6 契約書には、資産が危険にさらされているか、例えば、データの喪失又は変更が生じているかどうかを判定するための手順を含めることを考慮すること

2.2.2.7 契約書には、契約の終了時又は契約期間中の合意時点における情報及び資産を確実に返還又は破棄するための管理策を含めることを考慮すること

2.2.2.8 契約書には、完全性及び可用性を含めることを考慮すること

2.2.2.9 契約書には、情報の複製及び開示の制限を含めることを考慮すること

2.2.2.10 契約書には、利用できる各サービスの記述を含めることを考慮すること

2.2.2.11 契約書には、サービスの目標となるレベル及びサービスの受け入れられないレベルを含めることを考慮すること

2.2.2.12 契約書には、必要ならば、要員の異動に関する規定を含めることを考慮すること

2.2.2.13 契約書には、契約当事者それぞれの義務を含めることを考慮すること

2.2.2.14 契約書には、法律関連事項を含めることを考慮すること（例えば、データ保護に関連して制定された法律における責任。特に、契約が他国の組織との協力にかかわるものである場合、その国の法制度を考慮する）

2.2.2.15 契約書には、知的所有権（IPR）及び著作権の取扱い、並びに共同作業に伴う保護の条項を含めることを考慮すること

2.2.2.16 契約書には、承認されたアクセス方法、並びに固有の識別子（例えば、利用

者 ID 及びパスワード）の管理及び使用を含むアクセス制御の合意事項を含めることを考慮すること

2.2.2.17 契約書には、利用者によるアクセス及び利用者特権の認可手続を含むアクセス制御の合意事項を含めることを考慮すること

2.2.2.18 契約書には、利用可能サービスを認可されている個人、並びにその利用者が持っている権限及び特権の内容の一覧表を維持管理するための要求事項を含むアクセス制御の合意事項を含めることを考慮すること

2.2.2.19 契約書には、検証可能な性能基準、それらの監視及び報告の定義を含めることを考慮すること

2.2.2.20 契約書には、利用者の活動を監視し、無効にする権利を含めることを考慮すること

2.2.2.21 契約上の責任を監査する権利又はそのような監査を第三者に実施させる権利を含めることを考慮すること

2.2.2.22 契約書には、問題解決のための段階的処理手順の確立を含めることを考慮すること

2.2.2.23 契約書には、障害対策の取決めを含めることを考慮すること

2.2.2.24 契約書には、ハードウェア及びソフトウェアの導入及び保守に関する責任を含めることを考慮すること

2.2.2.25 契約書には、明確な報告の構成及び合意された報告の形式を含めることを考慮すること

2.2.2.26 契約書には、変更管理の明確な、設定された手続を含めることを考慮すること

2.2.2.27 契約書には、要求される物理的保護の管理策、及びそれらの管理策の実施を確実にするための仕組みを含めることを考慮すること

2.2.2.28 契約書には、利用者及び管理者に対する、方法、手順及びセキュリティについての訓練を含めることを考慮すること

2.2.2.29 契約書には、悪意のあるソフトウェアからの保護を確実にするための管理策を含めることを考慮すること

2.2.2.30 契約書には、セキュリティ事件・事故及びセキュリティ違反についての報告、通知及び調査に関する取決めを含めることを考慮すること

2.2.2.31 契約書には、第三者と下請け業者とのかかわりを含めることを考慮すること

2.3 外部委託

目的：情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため

2.3.1 情報システム、ネットワーク及び／又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間

で合意される契約書に記述すること

2.3.1.1 外部委託契約書には、法的な要求事項（例えば、データ保護に関連して制定された法律）をどのように満たすかを取り扱うこと

2.3.1.2 外部委託契約書には、請負業者を含め、外部委託にかかわるすべての当事者がそれぞれのセキュリティの責任についての認識を確実にするためにどのような取決めが適切であるかを取り扱うこと

2.3.1.3 外部委託契約書には、組織の事業資産の完全性及び機密性をどのように維持し、それを検証するかを取り扱うこと

2.3.1.4 外部委託契約書には、慎重な取扱いを要する組織の業務情報への認可された利用者によるアクセスを制約及び制限するために、どのような物理的及び論理的管理策を用いるかを取り扱うこと

2.3.1.5 外部委託契約書には、災害の際に、サービスの可用性をどのように維持するかを取り扱うこと

2.3.1.6 外部委託契約書には、外部委託した装置については、どのようなレベルの物理的セキュリティを施すかを取り扱うこと

2.3.1.7 外部委託契約書には、監査する権利を取り扱うこと

2.3.1.8 2.2.2 に列挙した事項も、この契約の一部として考慮すること

2.3.1.9 契約では、両当事者間の合意によるセキュリティマネジメント計画において、追加されたセキュリティ要求事項及び手順を認めること

3 資産の分類及び管理

3.1 資産に対する責任

目的：組織の資産の適切な保護を維持するため

3.1.1 情報システムそれぞれに関連づけて重要な資産について目録を作成し、維持すること

3.1.1.1 組織は、その資産並びにそれらの相対価値及び重要度を明確に把握できるようにすること

3.1.1.2 情報システムそれぞれに関連づけて重要な資産について目録を作成すること

3.1.1.3 各資産を、その現在の所在とともに、明確に識別すること

3.1.1.4 各資産を、その現在の所在とともに、セキュリティの分類について合意すること

3.1.1.5 各資産を、その現在の所在とともに、文書化すること

3.1.1.6 各資産を、その現在の所在とともに、その管理責任及びセキュリティの分類について合意すること

3.2 情報の分類

目的：情報資産の適切なレベルでの保護を確実にするため

3.2.1 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響（例えば、情報への認可されていないアクセス又は情報の損傷）を考慮に入れること

3.2.1.1 情報及び重要なデータを取り扱うシステムからの出力は、それが組織に対してもつ価値及び取扱い慎重度によってラベル付けすること

3.2.1.2 過度の分類によって無駄な出費を生じないようにすること

3.2.1.3 分類の指針には、前もって決められた個別方針に従って変わることもある、という事実を予期し考慮しておくこと

3.2.1.4 分類区分の数及びそれらの区分を用いる効用を考慮すること

3.2.1.5 他の組織からの文書に付いている分類ラベルは、同じか又は類似した名称のラベルでも、定義が異なることがあるので、その解釈には注意すること

3.2.1.6 情報（例えば、文書、データ記録、データファイル又はディスケット）の分類を定める責任、及びその分類を定期的に見直す責任は、その情報の作成者又は指定された管理者にあること

3.2.2 組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること

3.2.2.1 各分類について、複製に適用する取扱い手順を定めること

3.2.2.2 各分類について、保存に適用する取扱い手順を定めること

3.2.2.3 各分類について、郵便による伝達に適用する取扱い手順を定めること

3.2.2.4 各分類について、ファクシミリによる伝達に適用する取扱い手順を定めること

3.2.2.5 各分類について、電子メールによる伝達に適用する取扱い手順を定めること

3.2.2.6 各分類について、移動電話による伝達に適用する取扱い手順を定めること

3.2.2.7 各分類について、音声メールによる伝達に適用する取扱い手順を定めること

3.2.2.8 各分類について、留守番電話による伝達に適用する取扱い手順を定めること

3.2.2.9 各分類について、言葉による伝達に適用する取扱い手順を定めること

3.2.2.10 各分類について、破棄に適用する取扱い手順を定めること

3.2.2.11 取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを（出力に）付けること

3.2.2.12 ラベル付けは、分類の指針に定める規則に従った分類を反映すること

4 人的セキュリティ

4.1 職務定義及び雇用におけるセキュリティ

目的：人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため

4.1.1 セキュリティの役割及び責任は、組織の情報セキュリティ基本方針で定められたとおりに、適切に文書化すること

4.1.1.1 セキュリティの役割及び責任を文書化したものには、セキュリティ基本方針を実行又は維持するための一般的な責任のすべてを含めること

4.1.1.2 セキュリティの役割及び責任を文書化したものには、特定の資産を保護するための具体的な責任を含めること

4.1.1.3 セキュリティの役割及び責任を文書化したものには、特定のセキュリティの手続を含めること

4.1.1.4 セキュリティの役割及び責任を文書化したものには、特定のセキュリティ活動を進めるための具体的な責任を含めること

4.1.2 常勤職員を採用するときは、提出された応募資料の内容を検査すること

4.1.2.1 かなりの権限をもつ地位に就く職員については、この調査を定期的に繰り返すこと

4.1.2.2 経営者は新入職員及び経験の浅い職員に取扱いに慎重を要するシステムにアクセスすることを認めたときは、それらに対する管理監督についての評価を行うこと

4.1.2.3 すべての職員の仕事は、上級の職員による定期的見直し及び承認手順のもとに置くこと

4.1.2.4 職員の個人的事情がその仕事に影響を及ぼす可能性を、管理者は認識していること

4.1.2.5 不正行為、盗難、誤り又はその他のセキュリティにかかわる問題は、当該裁判管轄で施行されている適切な法令に従って取り扱うこと

4.1.2.6 常勤職員を採用するときは、提出された応募資料の内容を検査すること

4.1.2.7 応募資料の検査において、提出された人物推薦状は役にたつかを考慮すること

4.1.2.8 応募資料の検査において、履歴書の検査をすること

4.1.2.9 応募資料の検査において、提示された学術上及び職業上の資格の確認をすること

4.1.2.10 応募資料の検査において、公的証明書（パスポート又は同種の文書）の検査をすること

4.1.2.11 組織は、その者に対して信用調査を行うこと

4.1.2.12 請負業者及び臨時職員に対しても同様の審査手続を実施すること

4.1.2.13 派遣会社が従う必要のある審査の責任及び通知の手順を、派遣会社との契約に明記すること

4.1.3 従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること

4.1.3.1 既存の契約（機密保持条項を含むもの）の効力が及ばない臨時職員及び外部利用者に対しては、情報処理設備へのアクセスを認める前に、機密保持契約書へ

の署名を要求すること

4.1.3.2 機密保持契約は、雇用条件又は請負契約に変更がある場合、特に従業員がその組織を離れることになるとき又は請負契約が終了するときには、見直しを行うこと

4.1.4 雇用条件には、情報セキュリティに対する従業員の責任について記述してあること

4.1.4.1 適切ならば、これらの責任を、雇用終了後の定められた期間継続すること

4.1.4.2 従業員がセキュリティ要求事項を無視した場合に採る措置についても雇用条件に含めること

4.1.4.3 著作権法又はデータ保護に関連して制定された法律といったものに基づく、従業員の責任及び権利を明確にすること

4.1.4.4 著作権法又はデータ保護に関連して制定された法律といったものに基づく、従業員の責任及び権利を雇用条件に含めること

4.1.4.5 雇用条件には、雇用者側データについての重要度の分類及びその管理に対しての義務を含めること

4.1.4.6 雇用条件には、通常の勤務場所及び勤務時間からは外れた状況においても、これらの責任が適用されることの記述があること

4.2 利用者の訓練

目的：情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティ基本方針を維持していくことを確実にするため

4.2.1 組織の基本方針及び手順について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと

4.2.1.1 教育には、セキュリティ要求事項、法律上の責任及び業務上の管理策とともに、情報又はサービスへのアクセスを許可する前に実施する、情報処理設備の正しい使用方法（例えば、ログオン手順、パッケージソフトウェアの使用方法）に関する訓練を含むこと

4.3 セキュリティ事件・事故及び誤動作への対処

目的：セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため

4.3.1 セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること

4.3.1.1 事件・事故の正式な報告手順を、事件・事故への対処手順とともに確立すること

4.3.1.2 事件・事故の正式な報告を受けたならば直ちに取るべき措置に着手できるようにすること

4.3.1.3 すべての従業員及び請負業者に、セキュリティ事件・事故の報告手順を認識させておくこと

4.3.1.4 すべての従業員及び請負業者に、セキュリティ事件・事故をできるだけ速やかに報告するよう要求すること

4.3.1.5 適切なフィードバックの手続を構築していること

4.3.2 情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求すること

4.3.2.1 利用者は、全ての従業員及び請負業者に、事件・事故の発生を知った場合又はその疑いを持った場合は、できるだけ速やかに、自分の管理者又はサービス提供者に対し直接報告すること

4.3.2.2 利用者には、弱点ではないかと疑われる事柄の証明を、いかなる場合でも自ら試みるべきでないと知らせておくこと

4.3.3 ソフトウェアの誤動作を報告する手順を確立すること

4.3.3.1 ソフトウェア誤動作を報告する手順の確立において、問題の兆候及び画面に現れるメッセージへの注意を考慮すること

4.3.3.2 ソフトウェア誤動作を報告する手順の確立において、コンピュータの隔離を考慮すること

4.3.3.3 ソフトウェア誤動作を報告する手順の確立において、コンピュータの使用停止を考慮すること

4.3.3.4 ソフトウェア誤動作を報告する手順の確立において、適切な関係先に対する警報を考慮すること

4.3.3.5 ソフトウェア誤動作を報告する手順の確立において、装置の検査の前に組織のすべてのネットワークを切断することを考慮すること

4.3.3.6 ソフトウェア誤動作を報告する手順の確立において、ディスケットを別のコンピュータに移さないことを考慮すること

4.3.3.7 ソフトウェア誤動作を報告する手順の確立において、情報セキュリティ管理者への速やかな報告を考慮すること

4.3.3.8 利用者は、疑いのあるソフトウェアの除去を認可なしに試みないこと

4.3.3.9 回復処置は、適切に訓練されること

4.3.3.10 回復処置は、経験を積んだ職員が実施すること

4.3.4 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを備えていること

4.3.4.1 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする

仕組みから得られる情報を、事件・事故の再発若しくは影響の大きい事件・事故又は誤動作を識別するために用いること

4.3.5 組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備えていること

4.3.5.1 違反した従業員に対する、正式な懲戒手続は、重大な又は度重なるセキュリティ違反を犯した疑いのある従業員に対して、正しく、かつ、公平な取扱いを確実にするものであること

5 物理的及び環境的セキュリティ

5.1 セキュリティが保たれた領域

目的：業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため

5.1.1 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること

5.1.1.1 セキュリティ境界を明確に定義すること

5.1.1.2 情報処理設備を収容した建物又は敷地の境界は、物理的に頑丈であること

5.1.1.3 敷地の外周壁を堅固な構造物とすること、及びすべての外部扉を認可されていないアクセスから開閉制御の仕組み（かんぬき、警報装置、錠など）で適切に保護すること

5.1.1.4 敷地又は建物への物理的アクセスを管理するために、有人の受付又はその他の手段を設けること

5.1.1.5 敷地及び建物へのアクセスは、認可された職員だけに制限すること

5.1.1.6 物理的な壁は、床から天井にわたる構造で設けること

5.1.1.7 セキュリティ境界上にあるすべての防火扉は、警報装置付き及び密閉式であること

5.1.2 認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によってセキュリティの保たれた領域を保護すること

5.1.2.1 セキュリティが保たれた領域への訪問者を監視すること

5.1.2.2 セキュリティが保たれた領域への訪問者に立ち入り許可を求めさせること

5.1.2.3 セキュリティが保たれた領域への入退の日付・時間を記録すること

5.1.2.4 セキュリティが保たれた領域への訪問者には、認可された特定の目的に限ってのアクセスを認めること

5.1.2.5 セキュリティが保たれた領域への訪問者には、その領域のセキュリティ要求事項及び非常時の手順を説明した文書を渡すこと

5.1.2.6 取扱いに慎重を要する情報及び情報処理設備へのアクセスを管理すること

5.1.2.7 取扱いに慎重を要する情報及び情報処理設備へのアクセスは認可された者だけに制限すること

5.1.2.8 アクセスをすべて認可して妥当性を確認するために、暗証番号付きの磁気カードといった認証管理策を用いること

5.1.2.9 すべてのアクセスの監査証跡は、安全に保管しておくこと

5.1.2.10 すべての要員に、目に見える何らかの形状をした身分証明の着用を要求すること

5.1.2.11 付添いを伴わない見知らぬ人及び目に見える身分証明を着用していない人に対しては、誰であるか問い掛けるよう奨励すること

5.1.2.12 セキュリティが保たれた領域へのアクセス権は、定期的に見直し及び更新すること

5.1.3 セキュリティが保たれた領域の選択及び設計においては、火災、洪水、爆発、騒擾、その他の自然又は人為的災害による損害の可能性を考慮すること

5.1.3.1 関連する健康及び安全に関する規制並びに標準類も考慮に入れること

5.1.3.2 隣接場所から及んでくるセキュリティ上のいかなる脅威についても考慮すること

5.1.3.3 主要な設備は、一般の人のアクセスが避けられる場所に設置すること

5.1.3.4 建物は目立たせず、その用途を示す表示は最小限とすること

5.1.3.5 情報処理作業の存在を示すものは建物の内外を問わず一切表示しないこと

5.1.3.6 複写機、ファクシミリといった支援機能及び装置は、セキュリティの保たれた領域内の適切な場所に設置すること

5.1.3.7 要員が不在のときは扉及び窓に施錠すること

5.1.3.8 一階の窓については、外部に対する防御を考慮すること

5.1.3.9 すべての外部扉及びアクセス可能な窓には、適切な侵入者の検知システムを設置すること

5.1.3.10 侵入者の検知システムは、専門の標準類に従って取り付けられること

5.1.3.11 侵入者の検知システムは、定期的に点検すること

5.1.3.12 無人の領域には常に警報装置を稼働させること

5.1.3.13 コンピュータ室又は通信室といった他の領域においても、警報装置を設置すること

5.1.3.14 組織自ら管理する情報処理設備は、第三者が管理するものから物理的に分離しておくこと

5.1.3.15 取扱いに慎重を要する情報処理設備の所在を掲げた職員録及び社内電話帳は、一般の人に容易に見られないようにすること

5.1.3.16 危険物又は可燃物は、セキュリティが保たれた領域から十分に離れた場所に、安全に保管すること

5.1.3.17 セキュリティが保たれた領域には、事務用品などを、必要もないのに大量に

保管しないこと

5.1.3.18 緊急時に用いる代替装置及びバックアップされた媒体は、主事業所から十分に離れた場所に置くこと

5.1.4 セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加すること

5.1.4.1 セキュリティが保たれた領域の存在又はそこでの作業は、その必要がある要員だけが知っていること

5.1.4.2 セキュリティが保たれた領域において監視もなく作業することは、避けること

5.1.4.3 セキュリティが保たれた領域を無人にするときは、物理的な施錠を行うこと

5.1.4.4 セキュリティが保たれた領域を無人にするときは、定期的に検査すること

5.1.4.5 セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスを許可するときは、アクセスができる範囲を限定し、アクセスが必要な場合に限ること

5.1.4.6 セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは認可のもとにおくこと

5.1.4.7 セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは監視下におくこと

5.1.4.8 あるセキュリティ境界の中にセキュリティ要求事項の異なる領域が存在するときは、その領域の間に、物理的アクセスを管理するための障壁及び境界を追加すること

5.1.4.9 認可なしの、写真機、ビデオカメラ、録音機、又はその他の記録装置の使用は、許さないこと

5.1.5 品物を受け渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること

5.1.5.1 品物を受け渡しする場所についてのセキュリティ要求事項は、リスクアセスメントに基づいて決定すること

5.1.5.2 建物の外から一時保管場所へのアクセスは、本人の確認及び認可を受けた要員に限定すること

5.1.5.3 一時保管場所については、建物内の他の場所にアクセスすることなく受渡しの要員が荷おろしできるように、設計を行うこと

5.1.5.4 一時保管場所の内部扉を開いているときは、外部扉を締めること

5.1.5.5 一時保管場所から使用場所に搬入品を移送する前に、危険の可能性がないかどうか、その品物を検査すること

5.1.5.6 敷地内に搬入するときには、搬入品の登録を行うこと

5.2 装置のセキュリティ

目的：資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため

5.2.1 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること

5.2.1.1 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること

5.2.1.2 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること

5.2.1.3 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること

5.2.1.4 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の策定を考慮すること

5.2.1.5 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること

5.2.1.6 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること

5.2.1.7 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること

5.2.2 装置は、停電、その他の電源異常から保護すること

5.2.2.1 装置は、装置製造者の仕様に適合した適切な電力の供給を確保すること

5.2.2.2 電源の多重化をすること

5.2.2.3 無停電電源装置（UPS）を設置すること

5.2.2.4 非常用発電機の設置をすること

5.2.2.5 障害対策計画では、UPS が故障した場合に取るべき措置についても計画しておくこと

5.2.2.6 UPS は、容量が十分であることを定期的に確認すること

5.2.2.7 UPS は、製造者の推奨に従って点検すること

5.2.2.8 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること

5.2.2.9 発電機を使用する場合、製造者の推奨に従って定期的に点検すること

5.2.2.10 発電機を長時間運転できるように、燃料の十分な供給を確保すること

5.2.2.11 電源の緊急スイッチは、機械室の非常口近くに設置すること

5.2.2.12 主電源の停電時用として非常用照明を備えること

5.2.2.13 落雷防護はすべての建物に備えること

5.2.2.14 すべての外部通信回線に落雷防護フィルタを付けること

5.2.3 データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること

5.2.3.1 情報処理設備に接続する電源ケーブル及び通信回線は、可能ならば地下に埋設

するか、又はそれに代わる十分な保護手段を施すこと

5.2.3.2 ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること

5.2.3.3 干渉を防止するために、電源ケーブルは通信ケーブルから隔離すること

5.2.3.4 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること

5.2.3.5 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること

5.2.3.6 取扱いに慎重を要するシステム又は重要なシステムに対しては、データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、代替経路又は伝送媒体を使用すること

5.2.3.7 取扱いに慎重を要するシステム又は重要なシステムに対しては、データ伝送又は情報サービスに使用する通信ケーブルの配線は光ファイバケーブルを使用すること

5.2.3.8 取扱いに慎重を要するシステム又は重要なシステムに対しては、認可されていない装置がケーブルに取り付けられているかどうかについての調査すること

5.2.4 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること

5.2.4.1 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること

5.2.4.2 認可された保守担当者だけが装置の修理及び手入れを実施すること

5.2.4.3 すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること

5.2.4.4 すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること

5.2.4.5 装置を保守するために搬出する場合、適切な管理策を施すこと

5.2.4.6 保険約款によって定められたすべての要求事項に従うこと

5.2.5 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること

5.2.5.1 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること

5.2.5.2 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと

5.2.5.3 ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること

5.2.5.4 装置の保護に関しては、製造者の指示に常に従うこと

5.2.5.5 在宅作業についての管理策は、リスクアセスメントによって決定すること

5.2.5.6 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること

5.2.5.7 事業所外の装置を保護するために、十分な保険が付保されていること

5.2.5.8 セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること

5.2.6 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること

5.2.6.1 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること

5.2.6.2 取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアが、消去又は上書きされているか確認すること

5.3 その他の管理策

目的：情報及び情報処理設備の損傷又は盗難を防止するため

5.3.1 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮すること

5.3.1.1 クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること

5.3.1.2 クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること

5.3.1.3 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管すること

5.3.1.4 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと

5.3.1.5 パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと

5.3.1.6 パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること

5.3.1.7 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること

5.3.1.8 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと

5.3.1.9 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと

5.3.2 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできないこと

5.3.2.1 持出し時及び返却時に記録を残すこと

5.3.2.2 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること

5.3.2.3 現場検査があることを各人が認識していること

6 通信及び運用管理

6.1 運用手順及び責任

目的：情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため

6.1.1 セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと

6.1.1.1 操作手順は、正式な文書として取り扱うこと

6.1.1.2 操作手順が変更の場合は管理者によって認可されること

6.1.1.3 操作手順には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.4 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.5 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.6 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.7 操作手順には、特別な出力の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.8 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.9 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること

6.1.2 情報処理設備及びシステムの変更について管理すること

6.1.2.1 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること

6.1.2.2 運用プログラムは、厳重な変更管理の下に置くこと

6.1.2.3 プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること

6.1.2.4 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合すること

6.1.2.5 重要な変更を識別及び記録すること

6.1.2.6 重要な変更の潜在的な影響の評価をすること

6.1.2.7 変更の申出を正式に承認する手順を確立すること

6.1.2.8 変更の詳細の、全関係者への通知をすること

6.1.2.9 うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること

6.1.3 セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立すること

6.1.3.1 情報システムの故障及びサービスの停止に対処できるように、手順を定めること

6.1.3.2 サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること

6.1.3.3 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること

6.1.3.4 機密性に対する違反に対処できるように、手順を定めること

6.1.3.5 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を含めること

6.1.3.6 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること

6.1.3.7 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること

6.1.3.8 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること

6.1.3.9 通常の障害対策計画手順には、監督機関に対する措置の報告を含めること

6.1.3.10 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること

6.1.3.11 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での証拠として使用するために、監査証跡及びこれに類する証拠を収集し、安全に保管すること

6.1.3.12 ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること

6.1.3.13 セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理されること

6.1.3.14 事件・事故管理手順では、身分が明らかで、認可された要員だけに、作動中のシステム及びデータに対するアクセスを、許すことを考慮すること

6.1.3.15 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること

6.1.3.16 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること

6.1.3.17 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認

することを考慮すること

6.1.4 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又は実行の分離を考慮すること

6.1.4.1 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による監督といった他の管理策を考慮すること

6.1.4.2 セキュリティ監査は、独立性を維持すること

6.1.4.3 どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること

6.1.4.4 ある作業を始めることと、その作業を認可することとを分離すること

6.1.4.5 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること

6.1.4.6 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること

6.1.5 開発施設、試験施設及び運用施設を分離するため、ソフトウェアの開発から運用の段階への移行についての規則を明確に定め、文書化すること

6.1.5.1 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること

6.1.5.2 同様な分離は、開発と試験との機能間でも実行すること

6.1.5.3 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持すること

6.1.5.4 開発施設、試験施設及び運用施設を分離すること

6.1.5.5 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること

6.1.5.6 開発作業と試験作業とは、可能な限り分離すること

6.1.5.7 コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと

6.1.5.8 運用システム及び試験システムに対しては、異なるログオン手順を用いること

6.1.5.9 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること

6.1.5.10 メニューには、適切な識別メッセージを表示すること

6.1.5.11 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得すること

6.1.5.12 管理用パスワードは、使用後には変更されることを確実にすること

6.1.6 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること

6.1.6.1 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること

6.1.6.2 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること

6.1.6.3 外部委託による施設管理においては、事業継続計画との関連性を考慮すること

6.1.6.4 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮すること

6.1.6.5 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当てを考慮すること

6.1.6.6 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順を考慮すること

6.2 システムの計画作成及び受入れ

目的：システム故障のリスクを最小限に抑えるため

6.2.1 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること

6.2.1.1 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること

6.2.1.2 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資源の使用を監視すること

6.2.1.3 管理者は、使用傾向、特に業務用ソフトウェア又は情報システムの管理ツールと関連した傾向を識別すること

6.2.1.4 システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を用いること

6.2.2 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること

6.2.2.1 管理者は、新しいシステムを受け入れるための要求事項及び基準を、明確に定義すること

6.2.2.2 管理者は、新しいシステムを受け入れるための要求事項及び基準を、文書化すること

6.2.2.3 管理者は、新しいシステムを受け入れるための要求事項及び基準を、合意すること

6.2.2.4 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること

6.2.2.5 管理者は、新しいシステムを受け入れるための要求事項及び基準を、試験することを確実にすること

6.2.2.6 システムの受け入れにおいて、性能及びコンピュータの容量・能力の要求事項を考慮すること

6.2.2.7 システムの受け入れにおいて、誤りからの回復及び再起動の手順並びに障害対策計画を考慮すること

6.2.2.8 システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮すること

6.2.2.9 システムの受け入れにおいて、合意された適切なセキュリティ管理策を考慮すること

6.2.2.10 システムの受け入れにおいて、手動による有効な手順を考慮すること

6.2.2.11 システムの受け入れにおいて、事業継続の取決めを考慮すること

6.2.2.12 システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること

6.2.2.13 システムの受け入れにおいて、新しいシステムが組織のセキュリティ全般に及ぼす影響について、検討したという証拠について考慮すること

6.2.2.14 システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと

6.2.2.15 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと

6.2.2.16 主要な新しいシステム開発においては、適切な試験を実施し、すべての受入れ基準が完全に満たされていることを確認すること

6.3 悪意のあるソフトウェアからの保護

目的：ソフトウェア及び情報の完全性を保護するため

6.3.1 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること

6.3.1.1 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと

6.3.1.2 ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること

6.3.1.3 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクから保護し、どのような保護対策を行うことが望ましいかを示す組織としての個別方針を考慮すること

6.3.1.4 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期更新を考慮すること

6.3.1.5 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること

6.3.1.6 未承認のファイル又は無認可の変更の存在に対しては、正式に調査すること

6.3.1.7 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること

6.3.1.8 電子メールの添付ファイル及びダウンロードしたファイルのすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること

6.3.1.9 システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること

6.3.1.10 ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考慮すること

6.3.1.11 ウイルス感染からの回復のための適切な事業継続計画を考慮すること

6.3.1.12 悪意のあるソフトウェアに関するすべての情報を確認すること

6.3.1.13 警告情報が正確、かつ、役立つことを確実にするための手順を考慮すること

6.3.1.14 管理者は、単なるいたずらと真のウイルスとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること

6.3.1.15 職員は、単なるいたずらの問題及びそれらを受け取ったときの対応について認識していること

6.4 システムの維持管理（Housekeeping）

目的：情報処理及び通信サービスの完全性及び可用性を維持するため

6.4.1 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること

6.4.1.1 災害又は媒体故障が発生した後、極めて重要なすべての業務情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備えること

6.4.1.2 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた場所に保管すること

6.4.1.3 重要な業務用ソフトウェアについては、少なくとも 3 世代又は 3 サイクル分のバックアップのための情報を保持すること

6.4.1.4 バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施すこと

6.4.1.5 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること

6.4.1.6 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのい

かなる要求事項も決定しておくこと

6.4.1.7 バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること

6.4.1.8 復元手順は、定期的に検査及び試験すること

6.4.2 運用担当者は、自分の作業の記録を継続すること

6.4.2.1 記録には、システムの起動及び終了の時刻を含めること

6.4.2.2 記録には、システム誤り及び実施した是正処置を含めること

6.4.2.3 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること

6.4.2.4 記録には、記録の作成者の名前を含めること

6.4.3 運用担当者の記録は、定期的に独立した検査を受けること

6.4.4 障害については報告を行い、是正処置をとること

6.4.4.1 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること

6.4.4.2 報告された障害の取扱いについては、明確な規定があること

6.4.4.3 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと

6.4.4.4 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを含むこと

6.5 ネットワークの管理

目的：ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため

6.5.1 ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること

6.5.1.1 ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること

6.5.1.2 ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること

6.5.1.3 ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること

6.5.1.4 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立すること

6.5.1.5 公衆ネットワークを通過するデータの機密性及び完全性を保護するため、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理

策を確立すること

6.5.1.6 サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整すること

6.6 媒体の取扱い及びセキュリティ

目的：財産に対する損害及び事業活動に対する妨害を回避するため

6.6.1 コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること

6.6.1.1 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること

6.6.1.2 組織の管理外となる媒体のすべてについて、認可を必要とすること

6.6.1.3 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること

6.6.1.4 すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること

6.6.1.5 コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書化すること

6.6.2 媒体が不要となった場合は、安全、かつ、確実に処分すること

6.6.2.1 媒体の安全な処分のための、正式な手順を確立すること

6.6.2.2 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること

6.6.2.3 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること

6.6.2.4 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと

6.6.2.5 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること

6.6.2.6 処分しようとする媒体を集める場合、集積することによる影響に配慮すること

6.6.3 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること

6.6.3.1 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎

重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類に対応させて策定すること

6.6.3.2 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること

6.6.3.3 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮すること

6.6.3.4 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持について考慮すること

6.6.3.5 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを確実にすること

6.6.3.6 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること

6.6.3.7 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮すること

6.6.3.8 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること

6.6.3.9 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて考慮すること

6.6.3.10 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること

6.6.4 認可されていないアクセスからシステムに関する文書を保護すること

6.6.4.1 システムに関する文書は、安全に保管すること

6.6.4.2 システムに関する文書にアクセスできる者は、人数を最小限に抑えること

6.6.4.3 システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること

6.6.4.4 システムに関する文書で、 公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること

6.7 情報及びソフトウェアの交換

目的：組織間で交換される情報の紛失、改ざん又は誤用を防止するため

6.7.1 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと

6.7.1.1 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること

6.7.1.2 セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること

6.7.1.3 セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること

6.7.1.4 セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術標準を考慮すること

6.7.1.5 セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること

6.7.1.6 セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること

6.7.1.7 セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考慮すること

6.7.1.8 セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考慮すること

6.7.1.9 セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考慮すること

6.7.1.10 セキュリティ条件にかかわる合意では、取扱いに慎重を要するもの(例えば、暗号かぎ) を保護するために必要とされる特別な管理策を考慮すること

6.7.2 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること

6.7.2.1 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること

6.7.2.2 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いること

6.7.2.3 媒体の配送においては、宅配業者の身分を確認する手順を導入すること

6.7.2.4 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること

6.7.2.5 媒体の配送においては、施錠されたコンテナの使用を考慮すること

6.7.2.6 媒体の配送においては、手渡しを考慮すること

6.7.2.7 媒体の配送においては、開封防止包装の利用を考慮すること

6.7.2.8 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること

6.7.2.9 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること

6.7.3 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること

6.7.3.1 電子商取引のセキュリティにおいては、認証 (買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求すべきか) について考慮すること

6.7.3.2 電子商取引のセキュリティにおいては、認可 (価格を決める権限、重要な取引

文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか。取引相手はこれらをどうやって知るか）について考慮すること

6.7.3.3 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること

6.7.3.4 電子商取引のセキュリティにおいては、価格情報について考慮すること

6.7.3.5 電子商取引のセキュリティにおいては、注文取引について考慮すること

6.7.3.6 電子商取引のセキュリティにおいては、審査について考慮すること

6.7.3.7 電子商取引のセキュリティにおいては、決済について考慮すること

6.7.3.8 電子商取引のセキュリティにおいては、注文について考慮すること

6.7.3.9 電子商取引のセキュリティにおいては、責任について考慮すること

6.7.3.10 電子商取引に関する当事者間の合意は、権限の詳細も含め、合意した取引条件を両当事者に義務付ける契約書によって裏付けること

6.7.3.11 情報サービス事業者と付加価値ネットワーク事業者との間にも、合意を交わすこと

6.7.3.12 公開している取引システムでは、その取引条件を顧客に公表すること

6.7.3.13 電子商取引に用いる基幹コンピュータのもつ攻撃に対する耐性について、及び電子商取引の実施に必要なネットワーク相互接続のセキュリティ上のかかわりについて、考慮すること

6.7.4 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること

6.7.4.1 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること

6.7.4.2 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること

6.7.4.3 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること

6.7.4.4 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の責任を含めること

6.7.4.5 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること

6.7.4.6 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること

6.7.4.7 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること

6.7.5 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること

6.7.5.1 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける

情報のぜい（脆）弱性を考慮すること

6.7.5.2 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること

6.7.5.3 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること

6.7.5.4 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること

6.7.5.5 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについて考慮すること

6.7.5.6 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮すること

6.7.5.7 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること

6.7.5.8 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること

6.7.5.9 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること

6.7.5.10 電子オフィスシステムのセキュリティにおいては、緊急時に用いる代替手段についての要求事項及び取決めについて考慮すること

6.7.6 電子的に公開した情報の完全性を保護するように注意すること

6.7.6.1 公開されたシステム（例えば、インターネット経由でアクセスできるウェブサーバ）に掲載している情報は、システムが設置された地域又は取引が行われている地域に適用される、法律、規則及び規制に適合することを確実にすること

6.7.6.2 情報を公開する前に、正式な認可の手続がとられること

6.7.6.3 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって保護すること

6.7.6.4 公開している電子システムは、それが情報のフィードバック及び直接入力を許すものである場合には、情報は、あらゆるデータ保護に関連して制定された法律に従って収集すること

6.7.6.5 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること

6.7.6.6 取扱いに慎重を要する情報は、収集の過程及び保管時に保護すること

6.7.6.7 公開のシステムにアクセスができても、アクセス権限がないと先のネットワー

クへのアクセスは、許さないこと

6.7.7 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な手順及び管理策をもつこと

6.7.7.1 音声・画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること

6.7.7.2 電話を使うときには、適切な注意を払うことの必要を、職員に意識させること

6.7.7.3 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせること

6.7.7.4 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残さないようにさせること

6.7.7.5 職員に、ファクシミリを用いる上での問題点を意識させること

7 アクセス制御

7.1 アクセス制御に関する業務上の要求事項

目的：情報へのアクセス制御をするため

7.1.1 アクセス制御についての業務上の要求事項を定義し、文書化すること

7.1.1.1 利用者ごと、または利用者からなるグループごとに対するアクセス制御規則を、アクセス方針宣言書に明確に記述すること

7.1.1.2 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること

7.1.1.3 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること

7.1.1.4 アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること

7.1.1.5 アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること

7.1.1.6 アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮すること

7.1.1.7 アクセス制御に関する個別方針には、異なるシステム及びネットワークにおける、アクセス制御と情報分類の方針との整合性を考慮すること

7.1.1.8 アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること

7.1.1.9 アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用

者のアクセス権限情報を考慮すること

7.1.1.10 アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること

7.1.1.11 アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別すること

7.1.1.12 アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定すること

7.1.1.13 アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をすること

7.1.1.14 アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス許可の変更をすること

7.1.1.15 アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をすること

7.2 利用者のアクセス管理

目的：情報システムへの認可されていないアクセスを防止するため

7.2.1 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること

7.2.1.1 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること

7.2.1.2 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者 ID を用いること

7.2.1.3 利用者登録手続において、グループ ID の使用は、実施される作業に適切な場合にだけ許可すること

7.2.1.4 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査すること

7.2.1.5 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査すること

7.2.1.6 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査すること

7.2.1.7 利用者登録手続において、重複する利用者 ID が別の利用者に発行されないことを確実にすること

7.2.1.8 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めるこ

とを考慮すること

7.2.1.9 利用者登録手続において、アクセス権の宣言書を利用者に発行すること

7.2.1.10 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること

7.2.1.11 利用者登録手続において、認可手続が完了するまでサービス提供者が利用者にアクセスさせないようにすること

7.2.1.12 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること

7.2.1.13 利用者登録手続において、職務を変更した利用者、又は組織から離れた利用者のアクセス権を直ちに取り消すこと

7.2.1.14 利用者登録手続において、もはや必要のない利用者 ID 及びアカウントがないか定期的に検査し、あれば削除すること

7.2.2 特権の割り当て及び使用は、制限し、管理すること

7.2.2.1 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割り当てを管理すること

7.2.2.2 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別すること

7.2.2.3 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること

7.2.2.4 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと

7.2.2.5 特権の割り当てにおいて、利用者に対する特権の許可が必要ないように、システムルーチンの開発及び使用を促進すること

7.2.2.6 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者 ID とは別の利用者 ID に、割り当てること

7.2.3 パスワードの割当ては、正規の管理手続によって統制すること

7.2.3.1 パスワード管理手続の取組において、個人のパスワードを秘密に保つこと

7.2.3.2 パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に求めること

7.2.3.3 パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること

7.2.3.4 パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること

7.2.3.5 パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること

7.2.3.6 パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避けること

7.2.3.7 パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること

7.2.3.8 パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと

7.2.3.9 パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びＩＣカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮すること

7.2.4 データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること

7.2.4.1 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと

7.2.4.2 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと

7.2.4.3 利用者アクセス権の見直しにおいて、特権の割り当てを定期的に検査して、認可されていない特権が取得されてないことを確実にすること

7.3 利用者の責任

目的：認可されていない利用者のアクセスを防止するため

7.3.1 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと

7.3.1.1 すべての利用者に、パスワードを秘密にしておくように助言すること

7.3.1.2 すべての利用者に、パスワードを紙に記録して保管しないように助言すること

7.3.1.3 すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合は、パスワードを変更するように助言すること

7.3.1.4 すべての利用者に、最短６文字の質の良いパスワードを選択すること

7.3.1.5 すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること

7.3.1.6 すべての利用者に、特権アカウントのパスワードは、通常のパスワードより頻繁に変更するように助言すること

7.3.1.7 すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること

7.3.1.8 すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること

7.3.1.9 すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること

7.3.1.10 すべての利用者に、個人用のパスワードを共有しないように助言すること

7.3.1.11 すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言すること

7.3.2 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること

7.3.2.1 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護をすること

7.3.2.2 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること

7.3.2.3 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言すること

7.3.2.4 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること

7.3.2.5 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること

7.4 ネットワークのアクセス制御

目的：ネットワークを介したサービスの保護のため

7.4.1 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること

7.4.1.1 ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること

7.4.1.2 ネットワーク及びネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること

7.4.1.3 ネットワーク及びネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決

めるための認可手順を対象にすること

7.4.1.4 ネットワーク及びネットワークサービスの使用についての個別方針には、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること

7.4.1.5 ネットワーク及びネットワークサービスの使用についての個別方針は、業務上のアクセス制御方針と整合していること

7.4.2 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること

7.4.2.1 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること

7.4.2.2 指定された接続経路には、専用線又は専用電話番号を割り当てること

7.4.2.3 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること

7.4.2.4 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること

7.4.2.5 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること

7.4.2.6 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び／又はセキュリティゲートウェイを使用させること

7.4.2.7 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること

7.4.2.8 組織内の利用者グループのために別々の論理領域（例えば、仮想私設網（Virtual Private Network : VPN））を設定することによって、ネットワークアクセスを制限すること

7.4.2.9 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと

7.4.3 遠隔地からの利用者のアクセスには、認証を行うこと

7.4.3.1 コールバックの手順及び制御を用いるとき、組織は、転送機能をもつネットワークサービスを用いないこと

7.4.3.2 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること

7.4.3.3 コールバックの手順及び制御を徹底的に試験すること

7.4.4 遠隔コンピュータシステムへの接続は、認証されること

7.4.5 診断ポートへのアクセスは、セキュリティを保つように制御されること

7.4.5.1 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピ

ュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること

7.4.5.2 ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にすること

7.4.6 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること

7.4.6.1 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること

7.4.6.2 ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと

7.4.6.3 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮すること

7.4.7 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと

7.4.7.1 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること

7.4.7.2 電子メールには制限を適用すること

7.4.7.3 一方向のファイル転送には制限を適用すること

7.4.7.4 双方向のファイル転送には制限を適用すること

7.4.7.5 対話型アクセスには制限を適用すること

7.4.7.6 時間帯又は日付に対応したネットワークアクセスには制限を適用すること

7.4.8 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと

7.4.8.1 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること

7.4.8.2 ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと

7.4.9 ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にすること

7.4.9.1 ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にすること

7.5 オペレーティングシステムのアクセス制御

目的：認可されていないコンピュータアクセスを防止するため

7.5.1 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること

7.5.2 情報サービスへのアクセスは、安全なログオン手続を経て達成されること

7.5.2.1 コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること

7.5.2.2 システムについての情報の開示は最小限にすること

7.5.2.3 ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しないこと

7.5.2.4 ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示すること

7.5.2.5 ログオン手順中に、認可されていない利用者の助けとなる表示をしないこと

7.5.2.6 誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しないこと

7.5.2.7 許容されるログオンの試みの失敗回数を制限すること

7.5.2.8 ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと

7.5.2.9 ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること

7.5.2.10 ログオンの失敗時には、データリンク接続を切ること

7.5.2.11 ログオン手順のために許容される最長時間及び最短時間を制限すること

7.5.2.12 許容される最長時間及び最短時間の制限から外れる場合、システムはログオンを終了すること

7.5.2.13 ログオンの失敗時には、失敗した試みを記録すること

7.5.2.14 ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること

7.5.2.15 ログオンが無事できた時点で、前回のログオン以降、失敗したログオンの試みがある場合は、その詳細を表示すること

7.5.3 すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者 ID）を保有すること

7.5.3.1 利用者 ID には、利用者の特権レベル（例えば、管理者（マネージャ）、監督者（スーパーバイザ））を表示しないこと

7.5.3.2 明らかに業務上の利点がある例外的状況において、利用者のグループ又は特定の業務に対して、共有利用者 ID を用いる場合、管理者の承認を文書で得ること

7.5.4 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること

7.5.4.1 パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること

7.5.4.2 パスワードの管理システムでは、適切ならば、利用者に自分のパスワードの選択及び変更を許可し、入力誤りを考慮した確認手順を組み入れること

7.5.4.3 パスワードの管理システムでは、質の良いパスワードを選択させるようにすること

7.5.4.4 パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること

7.5.4.5 パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること

7.5.4.6 パスワードの管理システムでは、以前の利用者パスワードの記録を、一定期間、維持し再使用を防止すること

7.5.4.7 パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにすること

7.5.4.8 パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること

7.5.4.9 パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存すること

7.5.4.10 パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること

7.5.5 システムユーティリティのために認証手順を使用すること

7.5.5.1 業務用ソフトウェアからシステムユーティリティを分離すること

7.5.5.2 システムユーティリティの使用を、可能な限り少人数の信頼できる認可された利用者だけに制限すること

7.5.5.3 システムユーティリティを臨時に使用する際には認可をすること

7.5.5.4 システムユーティリティの使用の制限をすること

7.5.5.5 システムユーティリティのすべての使用を記録すること

7.5.5.6 システムユーティリティの認可レベルの明確化及び文書化をすること

7.5.5.7 すべての不要なユーティリティソフトウェア及びシステムソフトウェアの除去をすること

7.5.6 脅迫の標的となり得る利用者のために、脅迫に対する警報（duress alarm）を備えることを考慮すること

7.5.6.1 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと

7.5.6.2 脅迫に対する警報に対応する責任及び手順を明確に定めること

7.5.7 リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末は遮断されること

7.5.7.1 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること

7.5.7.2 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであること

7.5.8 リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供すること

7.5.8.1 既定の時間枠（例えば、バッチファイル伝送のための時間枠）を使うか、又は短時間の通常の対話型処理（session）を用いること

7.5.8.2 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること

7.6 業務用ソフトウェアのアクセス制御

目的：認可されていないコンピュータアクセスを防止するため

7.6.1 ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限すること

7.6.1.1 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること

7.6.1.2 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮すること

7.6.1.3 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮すること

7.6.1.4 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること

7.6.1.5 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にすること

7.6.1.6 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること

7.6.2 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること

7.6.2.1 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること

7.6.2.2 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること

7.7 システムアクセス及びシステム使用状況の監視
目的：認可されていない活動を検出するため

7.7.1 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること
7.7.1.1 監査記録には、利用者 ID を含めること
7.7.1.2 監査記録には、ログオン及びログオフの日時を含めること
7.7.1.3 監査記録には、可能ならば、端末の ID 又は所在地を含めること
7.7.1.4 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること
7.7.1.5 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること

7.7.2 情報処理設備の使用状況を監視する手順を確立すること
7.7.2.1 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること
7.7.2.2 監視項目には、認可されているアクセスについて、利用者 ID を含むこと
7.7.2.3 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと
7.7.2.4 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと
7.7.2.5 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと
7.7.2.6 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと
7.7.2.7 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること
7.7.2.8 監視項目には、すべての特権操作について、システムの起動及び停止を含めること
7.7.2.9 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること
7.7.2.10 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること
7.7.2.11 監視項目には、認可されていないアクセスの試みについて、ネットワークの

ゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること

7.7.2.12 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること

7.7.2.13 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること

7.7.2.14 監視項目には、システム警告又は故障について、システム記録例外事項を含めること

7.7.2.15 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること

7.7.3 監視の結果は、定期的に見直すこと

7.7.3.1 監視結果の見直しの頻度は、関係するリスクによって決めること

7.7.3.2 考慮すべきリスク要因には、業務手続に与える重要性の度合を含めること

7.7.3.3 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること

7.7.3.4 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること

7.7.3.5 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること

7.7.4 システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること

7.7.4.1 セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製すること

7.7.4.2 ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮すること

7.7.4.3 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮すること

7.7.4.4 記録機能のセキュリティに対して注意すること

7.7.4.5 管理策は、認可されていない変更及び運用上の問題から保護することを目標とすること

7.7.5 コンピュータの時計は正しく設定すること

7.7.5.1 コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時（例えば、万国標準時に（UCT）又は現地の標準時）に合わせること

7.7.5.2 コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること

7.8 移動型計算処理及び遠隔作業

目的：移動型計算処理及び遠隔作業の設備を用いるときの情報セキュリティを確実にするため

7.8.1 ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特別な注意を払うこと

7.8.1.1 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること

7.8.1.2 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること

7.8.1.3 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること

7.8.1.4 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと

7.8.1.5 悪意のあるソフトウェアに対抗する手順を整えること

7.8.1.6 悪意のあるソフトウェアに対抗する手順は最新のものであること

7.8.1.7 移動型計算処理を用いる要員に対する訓練を計画すること

7.8.1.8 情報を素早く、容易にバックアップできる装置が利用可能となっていること

7.8.1.9 これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること

7.8.1.10 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと

7.8.1.11 ネットワークに接続された移動型設備の使用に対して適切な保護がなされること

7.8.1.12 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること

7.8.1.13 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること

7.8.1.14 大切な、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないこと（可能ならば、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いること）

7.8.2 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手配されていることを確実にすること

7.8.2.1 遠隔作業の場所に適切な保護が整っていること

7.8.2.2 遠隔作業は、経営陣によって認可され、管理されること

7.8.2.3 遠隔作業は、この作業形態のため適切に手配されていること

7.8.2.4 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること

7.8.2.5 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可すること

7.8.2.6 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮すること

7.8.2.7 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮すること

7.8.2.8 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること

7.8.2.9 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること

7.8.2.10 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報の取扱いに慎重を要する度合を考慮すること

7.8.2.11 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮すること

7.8.2.12 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの情報又は資源への認可されていないアクセスの脅威を考慮すること

7.8.2.13 遠隔作業活動のための適切な装置を準備すること

7.8.2.14 遠隔作業活動のための適切な保管棚・庫の準備をすること

7.8.2.15 遠隔作業活動のための許可される作業を明確にすること

7.8.2.16 遠隔作業活動のための作業時間を明確にすること

7.8.2.17 遠隔作業活動のための保持してもよい情報の分類を明確にすること

7.8.2.18 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること

7.8.2.19 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること

7.8.2.20 遠隔作業を行う場所の物理的なセキュリティを確保すること

7.8.2.21 家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引を明確にすること

7.8.2.22 ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること

7.8.2.23 バックアップ及び事業継続のための手順を明確にすること

7.8.2.24 監査及びセキュリティの監視を行うこと

7.8.2.25 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること

8 システムの開発及び保守

8.1 システムのセキュリティ要求事項

目的：情報システムへのセキュリティの組み込みを確実にするため

8.1.1 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には、管理策についての要求事項を明確にすること

8.1.1.1 セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること

8.1.1.2 セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること

8.1.1.3 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考慮すること

8.1.1.4 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること

8.1.1.5 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること

8.1.1.6 セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること

8.1.1.7 セキュリティが確保できなかった場合又はセキュリティが確保されていない場合に起こると思われる業務上の損害の可能性もセキュリティ要求事項及び管理策に反映されること

8.2 業務用システムのセキュリティ

目的：業務用システムにおける利用者データの消失、変更又は誤用を防止するため

8.2.1 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること

8.2.1.1 業務取引処理（transaction）、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること

8.2.1.2 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること

8.2.1.3 データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること

8.2.1.4 入力漏れデータ又は不完全なデータを検出するための二重入力又はその他の入力検査を実施すること

8.2.1.5 データ量の上限及び下限からの超過を検出するための二重入力又はその他の入力検査を実施すること

8.2.1.6 認可されていない又は一貫しない制御データを検出するための二重入力又は

その他の入力検査を実施すること

8.2.1.7 入力データの妥当性及び完全性を確認するために重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること

8.2.1.8 入力データに認可されていない変更があるかどうかについての紙に印刷した入力文書の点検を考慮すること

8.2.1.9 妥当性確認の誤りに対応する手順について考慮すること

8.2.1.10 入力データのもっともらしさを試験する手順について考慮すること

8.2.1.11 データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること

8.2.2 処理したデータの改変を検出するために、システムに妥当性の検査を組み込むこと

8.2.2.1 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること

8.2.2.2 データ変更を行う追加・削除の機能を持つプログラムの使用及びその位置について考慮すること

8.2.2.3 プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること

8.2.2.4 データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮すること

8.2.2.5 取引処理の更新後のデータファイルのバランスを取るための処理又はバッチの制御を考慮すること

8.2.2.6 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること

8.2.2.7 システム生成データの妥当性確認を考慮すること

8.2.2.8 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること

8.2.2.9 レコード及びファイルの全体のハッシュ合計の検査を考慮すること

8.2.2.10 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること

8.2.2.11 プログラムが正しい順序で実行されることの検査を考慮すること

8.2.2.12 プログラムが正しい順序で実行されない場合は終了され、問題が解決するまでは処理が停止することを確実に実施しているかの検査を考慮すること

8.2.3 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮すること

8.2.3.1 メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと

8.2.4 業務用システムからの出力データについては、保存された情報の処理がシステム環

境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること

8.2.4.1 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと

8.2.4.2 出力データの妥当性確認には、すべてのデータの処理を確実にするための調整制御の回数を含むこと

8.2.4.3 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、読取り装置又はその後の処理システムにとっての十分な情報の供給を含むこと

8.2.4.4 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと

8.2.4.5 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと

8.3 暗号による管理策

目的：情報の機密性、真正性又は完全性を保護するため

8.3.1 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること

8.3.1.1 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること

8.3.1.2 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を含めた取組みを考慮すること

8.3.1.3 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを考慮すること

8.3.1.4 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について考慮すること

8.3.1.5 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について考慮すること

8.3.1.6 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを考慮すること

8.3.1.7 暗号による管理策の使用に関する個別方針を定めるとき、組織全体にわたって効果的に実施するために採用すべき標準類を考慮すること

8.3.2 取扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化（Encryption）すること

8.3.2.1 リスクアセスメントに基づき、要求される保護レベルを、使用される暗号アルゴリズムの形式及び品質、並びに使用すべき暗号かぎの長さを考慮して明確にすること

8.3.2.2 組織における暗号利用の個別方針を実施するとき、世界の異なる地域における暗号技術の使用、及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること

8.3.2.3 暗号技術の輸出入に適用される規制も考慮すること

8.3.2.4 適切な保護レベルを明らかにするため、及び要求される保護レベルを提供し、かぎ管理機能をもつ安全な製品を選択するために、専門家の助言を求めること

8.3.2.5 組織が意図した暗号使用に適用される法令及び規制に関して、必要に応じて法律家の助言を求めること

8.3.3 電子文書の真正性及び完全性を保護するために、ディジタル署名を用いること

8.3.3.1 秘密かぎの機密性を保護するために注意を払うこと

8.3.3.2 秘密かぎにアクセスした者は、文書に署名でき、その結果かぎの所有者の署名を盗用することがあり得るため、このかぎを秘密に保管すること

8.3.3.3 公開かぎの完全性を保護すること

8.3.3.4 ディジタル署名に使用される暗号かぎは、暗号化に使用されるものとは異なること

8.3.3.5 ディジタル署名を用いるときは、ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること

8.3.3.6 電子商取引の場合、ディジタル署名の法的位置付けを知ること

8.3.3.7 法的枠組みが不十分である場合、ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること

8.3.3.8 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては、法律家による助言を求めること

8.3.4 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には、否認防止サービスを用いること

8.3.5 一連の合意された標準類、手順及び方法に基づくかぎ管理システムを、暗号技術の利用を支援するために用いること

8.3.5.1 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること

8.3.5.2 すべてのかぎは、変更及び破壊から保護し、共通かぎ及び秘密かぎは、認可されていない露呈から保護すること

8.3.5.3 かぎを生成し、保存し、記録保管するために用いられる装置を保護するためには、物理的保護策を用いること

8.3.5.4 かぎ管理システムでは、種々の暗号システム及び種々の業務用ソフトウェアの

ためのかぎを生成する方法を定めること

8.3.5.5 かぎ管理システムでは、公開かぎ証明書を生成し入手する方法を定めること

8.3.5.6 かぎ管理システムでは、予定している利用者にかぎを配付する方法を定めること

8.3.5.7 かぎ管理システムでは、かぎを保存する方法を定めること

8.3.5.8 かぎ管理システムでは、かぎを変更又は更新する方法を定めること

8.3.5.9 かぎ管理システムでは、セキュリティが損なわれたかぎを処理する方法について定めること

8.3.5.10 かぎ管理システムでは、かぎを無効にする方法について定めること

8.3.5.11 かぎ管理システムでは、事業継続管理の一部として、例えば、暗号化された情報の回復のために、消失したかぎ又は損傷したかぎを回復する方法を定めること

8.3.5.12 かぎ管理システムでは、かぎを、例えば、記録保管された情報又はバックアップされた情報などのために、記録保管する方法について定めること

8.3.5.13 かぎ管理システムでは、かぎを破壊する方法を定めること

8.3.5.14 かぎ管理システムでは、かぎ管理に関連する活動を記録し監査する方法を定めること

8.3.5.15 かぎ管理システムでは、セキュリティが損なわれる可能性を軽減するために、かぎは一定期間だけ用いることができるように、かぎの活性化及び非活性化の期日を定めること

8.3.5.16 かぎの活性化及び非活性化の期間は、暗号による管理策が使用される環境及び認識されているリスクによって決めること

8.3.5.17 安全に管理された共通かぎ及び秘密かぎの問題に加え、公開かぎの保護についても考慮すること

8.3.5.18 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に関する問題を扱うこと

8.4 システムファイルのセキュリティ

目的：ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため

8.4.1 運用システムでのソフトウェアの実行を管理すること

8.4.1.1 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること

8.4.1.2 運用システムは、実行可能なコードだけを保持すること

8.4.1.3 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れ

の確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しないこと

8.4.1.4 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること

8.4.1.5 古い版のソフトウェアは、事故対策用として保持すること

8.4.1.6 運用システムに使用されるベンダー供給ソフトウェアは、供給者によって支援されるレベルで、維持管理されること

8.4.1.7 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること

8.4.1.8 セキュリティ上の欠陥を除去するか又は軽減するのに役立つ場合には、ソフトウェアパッチを適用すること

8.4.1.9 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること

8.4.1.10 供給者の活動は監視されることが望ましい

8.4.2 試験データを保護し、管理すること

8.4.2.1 システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと

8.4.2.2 個人情報が入っている運用データベースは、使用しないようにすること

8.4.2.3 個人情報が入っている情報を使用する場合は、使用する前に、個人的要素を消去すること

8.4.2.4 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用すること

8.4.2.5 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けること

8.4.2.6 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること

8.4.2.7 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること

8.4.3 プログラムソースライブラリへのアクセスに対しては、厳しい管理を維持すること

8.4.3.1 可能な限り、プログラムソースライブラリは、運用システムに含めないこと

8.4.3.2 各アプリケーションごとに、プログラムライブラリ管理責任者を任命すること

8.4.3.3 IT 支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと

8.4.3.4 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと

8.4.3.5 IT 支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プロ

グラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること

8.4.3.6 プログラムリストは、セキュリティの保たれた環境に保持されること

8.4.3.7 プログラムソースライブラリへのすべてのアクセスについて、監査記録を維持管理すること

8.4.3.8 ソースプログラムの旧版は、記録保管しておくこと

8.4.3.9 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと

8.4.3.10 プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従うこと

8.4.3.11 各アプリケーションごとに、プログラムライブラリ管理責任者を任命すること

8.5 開発及び支援過程におけるセキュリティ

目的：業務用システム及び情報のセキュリティを維持するため

8.5.1 情報システムの変更の実施を厳しく管理すること

8.5.1.1 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないように考慮すること

8.5.1.2 支援プログラマによるシステムへのアクセスはその作業に必要な部分に限定されること

8.5.1.3 変更に対する正式な合意及び承認が得られていることを確実にすること

8.5.1.4 業務用ソフトウェア及び運用の変更管理手順は統合されること

8.5.1.5 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること

8.5.1.6 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確実にすること

8.5.1.7 業務用ソフトウェア及び運用の変更過程では、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするためにこの手順をレビューすること

8.5.1.8 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識別すること

8.5.1.9 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を得ること

8.5.1.10 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること

8.5.1.11 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること

8.5.1.12 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新されること

8.5.1.13 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実にすること

8.5.1.14 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェアの更新について版数の管理を行うこと

8.5.1.15 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること

8.5.1.16 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること

8.5.1.17 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること

8.5.2 オペレーティングシステムを変更した場合は、業務用システムをレビューし、試験すること

8.5.2.1 オペレーティングシステムの変更によって業務用ソフトウェアの管理及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること

8.5.2.2 年間支援計画及び予算には、オペレーティングシステムの変更の結果として必要となるレビュー及びシステム試験を必ず含めるようにすること

8.5.2.3 実施前に行う適切なレビューに間に合うように、オペレーティングシステムの変更を通知することを確実にすること

8.5.2.4 事業継続計画に対して適切な変更がなされることを確実にすること

8.5.3 パッケージソフトウェアの変更は極力行わないようにし、絶対に必要な変更を厳しく管理すること

8.5.3.1 ベンダー供給のパッケージソフトウェアは、変更しないで使用すること

8.5.3.2 パッケージソフトウェアの変更が絶対必要であると判断された場合は、組み込まれている管理策及び完全性の処理が損なわれるリスクを考慮すること

8.5.3.3 パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること

8.5.3.4 パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる可能性を考慮すること

8.5.3.5 パッケージソフトウェアの変更が絶対必要であると判断された場合は、変更の結果として、将来のソフトウェア保守に対して組織が責任を負うようになるかどうかの影響を考慮すること

8.5.3.6 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと

8.5.3.7 変更はすべて、完全に試験すること

8.5.3.8 変更はすべて、文書化すること

8.5.3.9 将来更新されたソフトウェアに再び適用できるようにすること

8.5.4 隠れチャネル（Covert channels）及びトロイの木馬（Trojan code）の危険性から保護するために、ソフトウェアの購入、使用及び修正を管理し、検査すること

8.5.4.1 プログラムは定評のある開発元のものだけを購入すること

8.5.4.2 コードの確認ができるようにソースコードでプログラムを購入すること

8.5.4.3 評価された製品を用いること

8.5.4.4 使用前にすべてのソースコードを検査すること

8.5.4.5 一旦導入したコードへのアクセス及びそのコードへの変更を管理すること

8.5.4.6 重要なシステムでの作業には確実に信頼できる要員を用いること

8.5.5 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために、管理策を用いること

8.5.5.1 ソフトウェア開発を外部委託する場合、使用許諾に関する取決め、コードの所有権及び知的所有権について考慮すること

8.5.5.2 ソフトウェア開発を外部委託する場合、実施される作業の質及び正確さの認証を考慮すること

8.5.5.3 ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託（escrow）契約に関する取決めについて考慮すること

8.5.5.4 ソフトウェア開発を外部委託する場合、なされた作業の質及び正確さの監査のためのアクセス権について考慮すること

8.5.5.5 ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること

8.5.5.6 ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること

9 事業継続管理

9.1 事業継続管理の種々の面

目的：事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため

9.1.1 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること

9.1.1.1 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること

9.1.1.2 業務手続の中断が事業に及ぼすと思われる影響を理解し(組織の存続性を脅かす可能性のある重大な事件・事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である)、情報処理施設の事業目的を確立すること

9.1.1.3 事業継続の手続の一部をなすこともある適切な保険への加入を考慮すること

9.1.1.4 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること

9.1.1.5 合意された戦略に従って事業継続計画を明確にし、文書化すること

9.1.1.6 実行されている計画及び手続を定期的に試験し、更新すること

9.1.1.7 事業継続管理が組織の手続及び機構に確実に組み込まれるようにすること

9.1.1.8 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること

9.1.2 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること

9.1.2.1 それらの障害の影響(損害規模及び回復期間の両面から)を判断するために、リスクアセスメントを行うこと

9.1.2.2 これら両活動の実施には、事業資源及び手続の管理者が全面的に関与すること

9.1.3 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てること

9.1.3.1 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること

9.1.4 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること

9.1.4.1 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること

9.1.4.2 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施すること

9.1.4.3 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に注意すること

9.1.4.4 事業継続計画の作成過程では、合意された手順及び過程を文書化すること

9.1.4.5 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと

9.1.4.6 事業継続計画の作成過程では、計画の試験及び更新を行うこと

9.1.4.7 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと

9.1.4.8 これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること

9.1.5 すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること

9.1.5.1 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること

9.1.5.2 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正すること

9.1.5.3 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件を考慮すること

9.1.5.4 事業継続計画作成の枠組みでは、事業運営及び／又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること

9.1.5.5 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決めを含むこと

9.1.5.6 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の手順について考慮すること

9.1.5.7 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること

9.1.5.8 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表について考慮すること

9.1.5.9 事業継続計画作成の枠組みでは、事業継続手続を理解させ、手続が継続して有効であることを確保するために計画される認識及び教育活動について考慮すること

9.1.5.10 事業継続計画作成の枠組みでは、個人の責任について考慮すること

9.1.5.11 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するのに誰が責任をもつかを記述すること

9.1.5.12 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること

9.1.5.13 事業継続計画作成の枠組みでは、各計画には特定の責任者がいること

9.1.5.14 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること

9.1.5.15 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者の責任とすること

9.1.6 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること

9.1.6.1 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職

員がそれらの計画を確実に認識するものであること

9.1.6.2 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと

9.1.6.3 計画の個々の構成要素を、頻繁に試験すること

9.1.6.4 計画が実際に役立つことを保証するために、様々な手法を使用すること

9.1.6.5 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画の検討）

9.1.6.6 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）

9.1.6.7 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）

9.1.6.8 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施する）

9.1.6.9 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）

9.1.6.10 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験する）

9.1.6.11 いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反映させること

9.1.7 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること

9.1.7.1 事業継続上の問題を適切に対処することを確実にするための手順を、組織の変更管理プログラムの中に含めること

9.1.7.2 各事業継続計画の定期的見直しに対する責任を割り当てること

9.1.7.3 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に更新すること

9.1.7.4 この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること

10 適合性

10.1 法的要求事項への適合

目的：刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため

10.1.1 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること

10.1.1.1 各情報システムについて、すべての関連する法令、規制及び契約上の要求事

項に適合する特定の管理策、及び個々の責任も同様に明確に定め、文書化すること

10.1.2 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は、法的制限事項に適合するように、適切な手続を実行すること

10.1.2.1 ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること

10.1.2.2 ソフトウェア製品の取得手続に関する標準類を発行すること

10.1.2.3 ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること

10.1.2.4 適切な財産登録簿を維持管理すること

10.1.2.5 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること

10.1.2.6 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること

10.1.2.7 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確認すること

10.1.2.8 適切な使用許諾条件を維持管理するための個別方針を定めること

10.1.2.9 ソフトウェアの処分又は他人への譲渡についての個別方針を定めること

10.1.2.10 適切な監査ツールを用いること

10.1.2.11 公衆ネットワークから入手するソフトウェア及び情報の使用条件に従うこと

10.1.3 組織の重要な記録は、消失、破壊及び改ざんから保護されること

10.1.3.1 組織の重要な記録は、消失、破壊及び改ざんから保護されること

10.1.3.2 記録類は、記録の種類（例えば、会計記録、データベース記録、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について保持期間及び記録媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光学媒体）の詳細も定めておくこと

10.1.3.3 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること

10.1.3.4 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、必要なときに、認可されている者が使用できるようにすること

10.1.3.5 記録の保管に用いられる媒体が劣化する可能性を考慮すること

10.1.3.6 保管及び取扱いの手順は、製造業者の推奨に従って実行すること

10.1.3.7 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確保する手順を含めること

10.1.3.8 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式

で取り出すことができるように、データ保管システムを選択すること

10.1.3.9 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にすること

10.1.3.10 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること

10.1.3.11 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行すること

10.1.3.12 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること

10.1.3.13 主要な情報の出典一覧を維持管理すること

10.1.3.14 重要な記録及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実行すること

10.1.4 関連する法令に従って個人情報を保護するために、管理策を用いること

10.1.4.1 データ保護の担当役員を任命すること

10.1.4.2 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当役員に報告することは、データ所有者の責任であること

10.1.4.3 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任であること

10.1.5 情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐための管理策を用いること

10.1.5.1 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされること

10.1.5.2 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること

10.1.5.3 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること

10.1.5.4 すべての利用者は、その許可されたアクセスの正確な範囲を認識していること

10.1.5.5 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを通知すること

10.1.5.6 ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告メッセージをコンピュータの画面上に表示すること

10.1.5.7 利用者は、引き続きログオン処理を行うために画面上のメッセージに同意し、それに適切に対応すること

10.1.6 暗号による管理策の規制においては、国の法律への適合を確実なものにするために、

法的な助言を求めること

10.1.6.1 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること

10.1.7 人又は組織に対する措置を支援するには、十分な証拠をもつこと

10.1.7.1 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること

10.1.7.2 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとること

10.1.7.3 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること

10.1.7.4 コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっておくこと

10.1.7.5 コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること

10.1.7.6 コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること

10.1.7.7 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得ること

10.2 セキュリティ基本方針及び技術適合のレビュー

目的：組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため

10.2.1 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること

10.2.1.1 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること

10.2.1.2 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること

10.2.2 情報システムは、セキュリティ実行標準と適合していることを定期的に検査すること

10.2.2.1 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行うこと

10.2.2.2 技術適合の検査では、専門家の技術援助を得ること

10.2.2.3 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアに

よって実施されること

10.2.2.4 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること

10.2.2.5 いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施されること

10.3 システム監査の考慮事項

目的：システム監査手続の有効性を最大限にすること、及びシステム監査手続へのからの干渉を最小限にするため

10.3.1 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意されること

10.3.1.1 監査要求事項は、担当経営陣の同意を得ること

10.3.1.2 検査の範囲は、合意され、管理されること

10.3.1.3 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定すること

10.3.1.4 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること

10.3.1.5 複製ファイルは、監査が完了した時点で消去すること

10.3.1.6 検査を実施するための情報資源は、明確に識別され、利用可能であること

10.3.1.7 特別又は追加処理の要求事項は、識別され、合意されること

10.3.1.8 すべてのアクセスは、照合用の証跡を残すために、監視され、記録されること

10.3.1.9 すべての手順、要求事項及び責任について、文書化すること

10.3.2 システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること

10.3.2.1 システム監査ツールは、開発及び運用システムから分離しておくこと

10.3.2.2 システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと

『新版　システム監査基準／システム管理基準解説書』（平成16年基準改訂版）

関連資料　　2005年1月31日　発行

編集兼
発行人　　児玉　幸治

発行所　　財団法人　日本情報処理開発協会
〒105-0011　東京都港区芝公園3-5-8　機械振興会館内
TEL03-3432-9381　FAX03-3432-9389
URL　http://www.jipdec.jp/

ISBN4-89078-013-0

財団法人 日本情報処理開発協会