法規適合性に関するＩＳＭＳユーザーズガイド

-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-

ISMS：Information Security Management System
情報セキュリティマネジメントシステム

平成 21 年 4 月

財団法人　日本情報処理開発協会

はじめに

我が国における情報セキュリティマネジメントシステム（ISMS）適合性評価制度は、2002年 4 月より本格運用を開始しました。本制度は、我が国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られるレベルの情報セキュリティを達成、維持することを目的としています。

本制度に適用される ISMS 認証基準である JIS Q 27001:2006（ISO/IEC 27001：2005)は、多くの企業が情報セキュリティマネジメントの構築に活用し、これにより認証を取得している事業者も増えています。

財団法人日本情報処理開発協会及び ISMS 適合性評価制度技術専門部会においても、ISMS 認証取得を目指す組織の理解を深めるために、2007 年 1 月に ISMS ユーザーズガイド（JIS Q 27001：2006 対応）を、2007 年 11 月に ISMS ユーザーズガイドーリスクマネジメント編ーを公表してきました。企業がリスクマネジメントを実施する上で、企業の法的リスクを考慮することは重要であり、とりわけ 2005 年 4 月の個人情報保護法の完全施行に伴う法規順守については重要な課題となっております。個人情報保護に対応する手段として ISMS の枠組みは極めて有効であり、ISMS の枠組みが法令及び規制の要求事項に適合させる仕組みであることを理解して頂くため、「法規適合性に関する ISMS ユーザーズガイド」（以下、本ガイド）を作成することとなりました。

本ガイドの主な読者は、企業の経営層のほか、ISMS の構築または ISMS 認証取得を検討している組織において、実際に ISMS に携っている担当者あるいはその責任者を想定しています。本ガイドが個人情報保護に関する法規適合性を理解する上での一助となり、ISMS を構築・運用する上で参考になることを期待しています。

本ガイドの作成にあたり、ご協力頂いた ISMS 適合性評価制度技術専門部会、個人情報保護 WG の皆様、ISMS 適合性評価制度運営委員会の皆様をはじめご協力頂いた関係各位に対し厚く御礼申し上げます。

2009 年 4 月

ISMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会

目次

１．序文

１．１　本ガイドの位置付け

本ガイドは、効果的な情報セキュリティマネジメントシステム（Information Security Management System：ISMS）（以下、「ISMS」という。）を構築しようとするユーザを対象に、特に法規(1)適合性の観点からリスクアセスメントを実施し、その結果に基づき法的リスクについての対応策を検討するためのガイドとして作成したものです。

本ガイドでは、法的リスクアセスメント全般についての考え方、とりわけ個人情報保護の対応についての理解を深めるために必要な事項について、できるだけわかりやすい例示により解説を試みていますが、認証基準の全てを網羅している訳ではありません。本ガイドのほか、ISMS 認証基準、ISMS ユーザーズガイド、及び ISMS ユーザーズガイド-リスクマネジメント編-を併せてご利用下さい。

１．２　法規適合性の重要性

昨今、企業における不祥事事件が多発しており、企業の社会的責任（CSR：Corporate Social Responsibility）を求める圧力は強くなりつつあります。とりわけ法規順守を確実にすることは、企業経営にとって重要な課題であり、社会的責任の基礎となるものです。システムセキュリティ技術に長けていたとしても法規違反を犯していては本末転倒なことであり、ISMS を構築する上で法規順守は大前提となるものです。法規違反をすれば、顧客や株主、取引先等の利害関係者から信頼を失うだけでなく、金融機関からの資金調達の困難、取引停止や顧客離れ、損害賠償など経営問題に発展しかねません。法規順守を組織のマネジメントとして取り組むことは経営課題であり、企業の経営理念として法規への適合を定め、企業全体で法規を遵守するという企業風土を確立させる必要があります。そのためには、各従業員が法規を遵守して業務を行う意識を向上させ、日常業務の中で法規適合性の浸透を徹底させなければなりません。

そのための方法として、法規順守に関する企業の法務リスクを管理するリスクマネジメントの確立が重要といえます。

JIS Q 27002:2006 規格は、法的な要求事項を満たす情報セキュリティを実施するための有効な出発点であり、法的な観点から組織にとって不可欠であると考えられる管理策について、次のように記載しています。

---

(1) 本ガイドでの法規とは、法令（強行法規を含む）及び規制要求事項のことをいいます。「強行法規」については、1.2 節末尾の「強行法規の解説」を参照して下さい。

a)個人データ及び個人情報の保護（15.1.4　参照）

b)組織の記録の保護（15.1.3　参照）

c)知的所有権（15.1.2　参照）

これらの管理策の妥当性は，組織が直面している固有のリスクに照らして決まることに留意することが望ましい。したがって，一般的な取組方法は有効な出発点と考えられるが，リスクアセスメントに基づく管理策の選択に取って代わることはない。

（JIS Q 27002:2006　より引用）

また、ISMS 認証基準では、リスクアセスメント手順や判断基準を明確にすることを要求しています。組織は特定された事業上の情報セキュリティ要求事項に対して適切なリスクアセスメントの方法を特定するのみならず、特定された法令及び規制の要求事項に対しても適切なリスクアセスメントの方法を特定しなければなりません。すなわち、リスク全般を考慮したリスクマネジメントを実施するためには、法規適合性の観点から企業の法的リスクを評価することが求められます。

この認証基準は、企業が適切なリスク管理体制を構築するのに役立ちます。
例えば、大和銀行代表訴訟事件判決（大阪地方裁判所平成１２年９月２０日判決）は、取締役等の善管義務の内容として適切なリスク管理体制を構築する義務があることを明らかにした上で、どのような内容のリスク管理体制を構築するかは経営判断の問題であり、取締役に広い裁量が与えられることを明らかにしました。また、日本長期信用銀行プロジェクト融資事件判決（平成１４年４月２５日東京地裁判決）は、この裁量の範囲を超えたかどうかの判断にあたっては、「判断の前提となった事実の認識に不注意な誤りがあったか否か、又は判断の過程・内容が取締役として著しく不合理なものであったか否か、すなわち、当該判断をするために当時の状況に照らして合理的と考えられる情報収集・分析、検討がなされたか否か、これらを前提とする判断の推論過程及び内容が明らかに不合理なものであったか否かが問われなければならない。」として、判断に供される情報が適切に収集されること、分析・検討・判断の過程と内容に不合理がないことを求めています。ISMS 認証基準に準拠してリスクアセスメント手順や判断基準を明確にすること、すなわち、事業上の情報セキュリティ要求事項や、適切なリスクアセスメントの方法を特定すること、特定された法令及び規制の要求事項に対して適切なリスクアセスメントの方法を特定することは、情報に関するリスクに関する資料収集や、判断の過程、内容を合理的なものにし、適切な裁量の範囲で情報リスクの管理体制を構築することに役立つでしょう。

★「強行法規」の解説

強行法規とはその規定が適用される人の意思によってその内容を左右することが許されない規定をいいます。例えば刑法の殺人罪の規定は、人の意思によって内容を左右することは許されませんから強行法規です。また、安全対策を求める個人情報保護法２０条は、個人情報取扱事業者が安全対策を行うか否かについての意思の自由を許さない強行法規です。強行法規に対するのが任意規定で、適用を受ける人の意思によってその内容に優先する内容を定めることができます。その例は、私法に多く見られ、例えば、業務の委託に関する民法の委任契約は、対価の支払いを要しない無償契約ですが、当事者の意思によって対価の支払いを要する有償委任契約とすることができます。強行規定が人の意思によってその内容を左右できないのは、強行規定が秩序や人の保護を目的とするからです。

１．３　個人情報保護の対応

「情報」は、「人」、「物」、「金」に続く第４の経営資源としての価値が高まっています。最近では個人情報漏洩事件が相次いで発生しており、個人情報は、その価値の高さゆえ、漏洩事故が経営的な問題として大きな影響を与えています。

そもそも、個人情報保護法や新会社法の施行によって、個人情報のみならず、これを取り扱うシステムのセキュリティを確保し、そのための内部統制を適切に構築・維持することは、以下に述べるように、個人情報保護法・会社法を遵守する遵法経営の要件となっています。

すなわち、個人情報を取り扱う企業においては、個人情報保護法やこれによる個人情報保護ガイドライン、JIS Q 15001 を含む企業の自主規範に準拠した、個人データの CIA の確保、本人からの開示請求、利用停止や削除要求などへの対応が求められます。

また、会社法は、「取締役の職務の執行が法令・・に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」（362 条 4 項 6 号）を求め、会社法施行規則は、「業務の適正を確保する体制」の内容として、「情報の保存及び管理」「損失の危険の管理」「職務執行の効率性確保」「使用人の職務執行の適法性確保」を企業集団全体で行う体制を整備すべきことを求めています（会社法施行規則 100 条 1 項）。そして、この体制を適切に構築・監査することは役員の善管注意義務（362 条 5 項）の内容をなしています。

このように、個人情報を保有している企業にとっては、個人情報保護法、業務所管省庁の定める個人情報保護ガイドライン、JIS Q 15001 を含む企業の自主規範に従って個人情報を適正に取扱うためのマネジメントシステムを構築することが喫緊の経営課題であるだけでなく、その企業が採択した個人情報保護への対策が法律上の義務や JIS Q 15001 を含む自主規範を遵守したことを主張できるだけの記録などの証拠を収集できる枠組みを確立し

ておくことが企業や役職員の責任を明らかにするためにも重要です。

これらの要求に応える個人情報保護対策には、技術的なセキュリティのほか、人的セキュリティを含む組織全体のセキュリティ対策を、的確なリスクマネジメントを通じて合理的に取り組むことが重要です。

情報セキュリティマネジメントシステム（ISMS）の構築は、JIS Q 15001 にはない詳細なリスクマネジメントと、これにもとづく情報セキュリティのためのマネジメントシステムの枠組みと運用を提供し、個人情報保護のためのコンプライアンス経営と内部統制の構築維持のための有効な手段となります。　また、的確なリスクアセスメントにもとづく ISMS の構築・維持と記録の整備は、個人情報取扱に伴うリスクの把握と個人情報保護のための経営の効率化に役立つだけでなく、個人情報の漏洩事故などに際しても、個人情報保護対策の合理性を立証するのに役立ちます。

１．４　ISMS 認証基準

ISMS 認証基準は、ISMS 制度において第三者である認証機関が本制度の認証を希望する事業者の適合性を評価するための基準です。現在、最新版として ISMS 認証基準は、JIS Q 27001:2006 が適用されています。JIS Q 27001:2006 は、「0　序文」、「1　適用範囲」、「2 引用規格」、「3　用語及び定義」、「4　情報セキュリティマネジメントシステム」、「5　経営陣の責任」、「6　ISMS 内部監査」「7　ISMS のマネジメントレビュー」、「8　ISMS の改善」及び附属書 A（規定）「管理目的及び管理策」、附属書 B（参考）「OECD 原則及びこの規格」、附属書 C（参考）「JIS Q 9001:2000、JIS Q 14001:2004、及びこの規格の比較」から構成されています。認証基準では、PDCA モデルに基づいたプロセスアプローチを採用し、リスクマネジメントを明確化するとともに、組織の ISMS を確立、導入、運用、監視、レビュー、維持、かつ継続的に改善することを要求しています。また、リスクアセスメントの結果に基づいて附属書 A「管理目的及び管理策」から管理目的及び管理策を選択し、選択した管理目的及び管理策の実施や運用に関する手順、記録などを文書化することを要求しています。選択された管理目的及び管理策は、定期的にもしくは必要に応じて見直すことが重要です。また、企業がリスクアセスメントの結果、必要と判断した管理目的及び管理策は追加することもできます。

２．適用範囲

ISMS とは、企業や組織の目標を達成するために、特定の事業領域のリスクマネジメントを効率的、効果的に行うための仕組みです。このことを ISMS 認証基準では以下のように説明しています。

> 3.7 情報セキュリティマネジメントシステム，ISMS（information security management system）
> マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分。
> 注記　マネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

また、ISMS を導入することにより、以下のような効果が期待されます。

■組織の目標を明確にし、確実に伝達し実施されるようにする
■実施の状況を継続的に管理し、適正な水準に保つ
■定期的な見直しを実施し、対策や実施の体制等を柔軟に改善する
■社会環境や要請を認識し、組織の目標に反映する

ISMS は、情報セキュリティの分野にかかるマネジメントが対象です。情報セキュリティに関するマネジメントシステムの構築とは、企業や組織が所有し、管理、運用する資産の価値に見合う対策の実施や、コンプライアンスの観点から法令等を順守し、それを維持するための枠組みを構築することを意味します。

ISMS 認証基準の「1.　適用範囲」では、組織における ISMS の位置付けと、ISMS 認証基準の適用について述べています。

（注記）本ガイドにおける資産とは、情報に関連した資産のことをいいます。ISMS 認証基準（Ver.2.0）対応のユーザーズガイドでは情報資産と呼んでいましたが、JIS Q 27002:2006 で用語が「資産」に変更されたため本ガイドでは、一部の箇所を除き以下、資産と呼びます。

> この ISMS は，情報資産を保護し，また，利害関係者に信頼を与える，十分で，かつ，均整のとれたセキュリティ管理策の選択を確実にするために設計される。
>
> （JIS Q 27001:2006　1 適用範囲　1.1 一般　より引用）

従って、ISMS 認証基準の要求事項を適切に実施することは、利害関係者からの信頼を確保するために十分なバランスのとれた情報セキュリティを構築し、維持していくことにつながるのです。

２．１ 利害関係者

利害関係者とは、JIS Q 9000:2000 の定義によると、「組織のパフォーマンス及び成功に利害関係をもつ人又はグループ」となります。顧客や投資家等といった組織外部の人々のみならず、組織内の人々等を含みその対象は広範囲に及びます。

3.3.1　組織(organization)
責任，権限及び相互関係が取り決められている人々及び施設の集まり。
例　会社，法人，事業所，企業，団体，慈善団体，個人業者(sole trader)，協会，若しくはこれらの一部又は組合せ
注記 1　この取決めは，一般に秩序だっている。
注記 2　組織は，公的又は私的のいずれでもあり得る。
注記 3　この定義は，品質マネジメントシステム(3.2.3)規格の目的に対して有効なものである。ISO/IEC Guide2 での用語“組織”の定義はこれとは異なる。

3.3.5　顧客(customer)
製品(3.4.2)を受け取る組織(3.3.1)又は人。
例　消費者，依頼人，エンドユーザ，小売り業者，受益者及び購入者
注記　顧客は，組織の内部又は外部のいずれでもあり得る。

3.3.6　供給者(supplier)
製品(3.4.2)を提供する組織(3.3.1)又は人。
例　製品の生産者，卸売業者，小売り業者，納入業者，サービス提供者又は情報提供者
注記 1　供給者は，組織の内部又は外部のいずれでもあり得る。
注記 2　契約関係においては，供給者は“契約者”と呼ばれる。

3.3.7　利害関係者(interested party)
組織(3.3.1)のパフォーマンス及び成功に利害関係をもつ人又はグループ
例　顧客(3.3.5)，所有者，組織内の人々，供給者(3.3.6)，銀行家，組合，パートナ又は社会
注記　グループは，一つの組織，その一部又は複数の組織のこともある。
(JIS Q 9000:2006　3 用語及び定義　3.3 組織に関する用語　より引用)

２．２ 適用

ISMS 認証基準は、どのような組織であっても必ず適用させる事が必要な要求事項と、事業の特性により適用除外が可能である要求事項で構成されており、広く利用可能な基準としてあらゆる組織に適合できるよう配慮されています。

表２-１　要求事項の適用について

JIS Q 27001:2006	要求事項の取扱い
JIS Q 27001:2006 の箇条 4,5,6,7 及び 8	必ず適用させる事が必要な要求事項
JIS Q 27001:2006 の附属書 A「管理目的及び管理策」	適用除外が可能となっている要求事項

ISMS 認証基準の附属書 A「管理目的及び管理策」に規定された要求事項の適用を除外する場合は、除外する理由を合理的に説明しなければなりません。組織の都合で一方的に除外することは認められていないからです。このことを ISMS 認証基準では以下のように説明しています。

> 組織がこの規格への適合を宣言する場合には，箇条 4，5，6，7 及び 8 に規定するいかなる要求事項の除外も認められない。
>
> （JIS Q 27001:2006　1 適用範囲　1.2 適用　より引用）

また、ISMS 認証基準及び附属書 A「管理目的及び管理策」に規定された要求事項の適用を除外する場合は、原則的に組織の実施するリスクアセスメントの結果に基づき、経営陣や責任者の判断により正式にリスクの受容が決定されたことを示す証拠を、適用宣言書に合理的な理由と併せて明記する必要があります。このことを ISMS 認証基準では以下の様に説明しています。

> リスクの受容基準を満たすために必要とみられる管理策の適用を除外する場合は，それがいかなるものであっても，適用除外を正当とする理由と，責任ある者が関連するリスクを受容したことを示す証拠とが必要である。何らかの管理策を適用除外とするとき，その除外が，セキュリティ要求事項（リスクアセスメント及び該当する法令又は規制の要求事項から決定されたもの）を満たす情報セキュリティを提供するその組織の能力及び/又は責任を損なう場合には，この規格への適合の主張は，受け入れられない。
>
> （JIS Q 27001:2006　1 適用範囲　1.2 適用　より引用）

リスクを内包した資産を保護するには、その資産が持つ価値や脅威、ぜい弱性を明らか

にし、リスクの大小を判別して適切な対策を講じなければなりません。安易な適用除外は、マネジメントシステムの一貫性に大きな影響を与えます。
以下に例示するような「除外の原則」を定め、ある要求事項について条件が全て満たされる場合にのみ適用を除外するなど公正な判断が求められます。

■ISMS の能力、責任に影響を及ぼさないこと
■ISMS の目標と相反しないこと
■関連法規や規制に関する要求事項でないこと

２．３ 適用宣言書

ISMS 認証基準では、適用宣言書について次のように定義しています。

> 3.16 適用宣言書（statement of applicability）
> その組織の ISMS に関連して適用する管理目的及び管理策を記述した文書。
> 注記　管理目的及び管理策は，組織の情報セキュリティに対する，次のものに基づく
> － リスクアセスメント及びリスク対応のプロセスの結果及び結論
> － 法令又は規制の要求事項
> － 契約上の義務
> － 事業上の要求事項
> （JIS Q 27001:2006　3 用語及び定義　より引用）

リスクアセスメント及びリスク対応の作業結果を踏まえ、ISMS 認証基準の附属書 A「管理目的及び管理策」の管理目的及び管理策を選択します。適用宣言書には、選択結果と、適用しない場合にはその理由も明記します。また、組織で必要と判断した管理策が、詳細管理策の項目には無く独自に追加した場合は、その内容と理由についても記述します。
上記のプロセスを経て、全ての管理策は適用宣言書に記載されます。

３．引用規格

ISMS 認証基準では、次の規格を引用規格として挙げています。ここでは、下記以外の規格も含めて情報セキュリティ及びマネジメントシステムについての規格を紹介します。

> 次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。これらの引用規格のうちで，西暦年を付記してあるものは，記載の年の版を適用し，その後の改正版（追補を含む。）には適用しない。
>
> JIS Q 27002:2006　情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範
>
> 注記　対応国際規格：ISO/IEC 17799:2005, Information technology－Security techniques－Code of practice for information security management（IDT）
>
> （JIS Q 27001:2006　2 引用規格　より引用）

３．１　JIS Q 27002

ISO/IEC 27002（ISO/IEC 17799）の制定発行に伴って、日本工業標準調査会(JISC)により日本工業標準(JIS)として制定された国内規格です。内容は、ISO/IEC 27002（ISO/IEC 17799）（※１）を忠実に日本語に翻訳し、国際規格との整合性が厳密に保たれたものとなっています。

※１　ISO/IEC 27002（ISO/IEC 17799）

情報セキュリティに対するマネジメントシステムの国際規格として、2000 年に ISO/IEC 17799 として制定発行されました。この規格は英国規格 BS 7799-1:1999（※２）を基にしており、実践のための規範をまとめたものです。現在使用されているのは、2005 年に改訂された版です。2007 年 7 月に規格番号が変更され、ISO/IEC 27002 となりました。

＜参考＞

ISO/IEC 27002 は、審査登録制度における認証基準ではありません。認証基準は、JIS Q 27001 です。

※２　BS 7799

1995 年に英国で制定発行された情報セキュリティに関する英国規格（British Standard）で、情報セキュリティの技術的対策だけではなく、人及び組織の管理を含めたマネジメントに関する実践のための規範をまとめたものです。その後、1998 年に認証の基準となる第 2 部が制定されて 2 部構成になり、2006 年 3 月に第 3 部（Guidelines for information

security risk management）が制定されました。なお、第 1 部と第 2 部は、BS ISO/IEC 17799:2005 及び BS ISO/IEC 27001:2005 に置き換わりました。

３．２　JIS Q 9001

品質に関するマネジメントシステムの要求事項に関する規格で、第 1 版は 1994 年に制定されました。現在使用されているのは、2000 年に改訂された第 2 版です。なお、認証基準は、第 2 版と整合性がとられています。
JIS Q 9000 シリーズには、JIS Q 9001 以外に品質マネジメントの基本及び用語をまとめた JIS Q 9000 と、パフォーマンス改善のための指針をまとめた JIS Q 9004 等があります。

３．３　TR Q 0008

2002 年に ISO/IEC Guide73 として制定されたリスクマネジメントの用語を日本語に翻訳した標準情報(TR)です。規格ではありませんが、リスクマネジメントの活動及び用語の使い方の標準として ISMS 認証基準でも採用しています。

> この標準情報は，リスクマネジメントの側面を含む規格の準備，又は改定の際に使用される上位の一般文書です。
> この標準情報の意図は，リスクマネジメント活動の記述及びリスクマネジメント用語の使い方に対する，統一的な取組を促進することである。この標準情報は，リスクマネジメント実施のための手引書としてではなく，ISO 及び IEC のメンバー間の相互理解に貢献することを目的としている。
>
> （TR Q 0008:2003　1.適用範囲　より引用）

＜参考＞
国家規格（National Standards）について審議する日本工業標準調査会では、標準情報(TR)を以下のように説明しています。TR Q 0008 は「タイプ II」です。

ＴＳ／ＴＲ制度について

本制度は、先端技術分野等の技術進歩の早い分野において、日本工業規格（ＪＩＳ）として制定するには熟度の低いものについて、迅速かつ適切に標準情報（ＴＳ及びＴＲ)として開示することにより、オープンな議論を推進し、コンセンサスの形成を促し、ＪＩＳ化の促進を図るためのものです。 この制度は、ＩＳＯ(国際標準化機構）のＴＳ制度及びＴＲ制度と同じ趣旨の制度です。

１．標準仕様書(ＴＳ)及び標準報告書(ＴＲ)の分類

① 標準仕様書(ＴＳ)

日本工業標準調査会の審議において、市場適合性が確認できない、又は技術的に開発途上にあるなど、ＪＩＳ制定へのコンセンサスが得られなかったが、将来ＪＩＳ制定の可能性があると判断され、公表される標準文書。標準仕様書(ＴＳ)は、次のとおり細分されます。

a) 標準仕様書(ＴＳ／タイプⅠ)

ＪＩＳ制定への必要なコンセンサスが得られなかったが､将来､ＪＩＳ制定への可能性がある標準文書。

b) 標準仕様書（ＴＳ／タイプⅡ)

技術的に開発途上にあるなど、現時点ではＪＩＳ制定が困難であるが、将来、ＪＩＳ制定への可能性がある標準文書。

なお、標準仕様書（ＴＳ)は、発行後３年以内に見直しを行い、ＪＩＳとするか、更に３年延長するか、又は廃止します。延長は、原則として１回限りとします。

② 標準報告書(ＴＲ)

ＪＩＳとは異なる種類の標準に関連する情報類(標準化関連情報、データ集など）として、これ自体はＪＩＳにはならないものの、標準化の推進に資するものとして公表される標準文書。 なお、標準報告書(ＴＲ)は、原則として発行後５年をもって廃止します。

２．標準仕様書(ＴＳ)及び標準報告書(ＴＲ)は、団体、企業等だれでも提案することができます。

提案する場合は、原案とともに必要な書類を主務大臣に提出する必要があります。詳しくは「標準仕様書（ＴＳ）／標準報告書（ＴＲ）原案の提案について」をご覧ください。 なお、提案者は、提案した標準仕様書(ＴＳ)及び標準報告書(ＴＲ)に対する意見・質問に対応する責務を負います。

３．標準仕様書(ＴＳ)及び標準報告書(ＴＲ)の公表

標準仕様書（ＴＳ）及び標準報告書（ＴＲ）は、JISC ﾎｰﾑﾍﾟｰｼﾞにおいて閲覧に供します。

（日本工業標準調査会 Web ページより引用

http://www.jisc.go.jp/jis-act/ts-tr.html　2009.3.19 現在）

３．４　その他の参考規格

①　TR X 0036 -1～5(GMITS)

「IT セキュリティマネジメントのガイドライン（Guidelines for the management of IT security)」と称し、ISO/IEC TR 13335 として国際化された標準情報です。このガイドラインでは、IT セキュリティの管理をどのように構築していくかをリスクマネジメントを含め

て記述した解説書です。
1996 年から順次制定発行されて、以下の 5 部で構成されています。

■第 1 部：IT セキュリティの概念およびモデル
■第 2 部：IT セキュリティのマネジメント及び計画
■第 3 部：IT セキュリティマネジメントのための手法
■第 4 部：セーフガードの選択
■第 5 部：ネットワークセキュリティに関するマネジメントの手引

これらの規格は 2006 年に有効期限が切れ、現在、別の規格として発行されていますが、この旧標準情報にも、本ガイドにおいて有益な情報が含まれていますので、旧標準情報からの内容を多く引用しています。
なお、これらの標準情報は改訂によって、次のような規格に一部が引き継がれています。

TR X 0036-1（ISO/IEC TR 13335-1）
TR X 0036-2（ISO/IEC TR 13335-2）　→　JIS Q 13335-1 （ISO/IEC 13335-1）

TR X 0036-3（ISO/IEC TR 13335-3）
TR X 0036-4（ISO/IEC TR 13335-4）　→　ISO/IEC 27005（2008.06.15 発行）

TR X 0036-5（ISO/IEC TR 13335-5）　→　ISO/IEC 18028-1

② JIS Q 13335-1
上記 GMITS の第 1 部と第 2 部を統合し国際標準化した規格 ISO/IEC 13335-1(Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management）の国内規格です。用語の定義の多くは、この規格から引用しました。

４．用語及び定義

ISMS 認証基準では、新たに情報セキュリティやリスクマネジメントに関する用語の定義が追加されました。

ISMS 認証基準の用語及び定義の表記順序は、英語表記のアルファベット順に掲載されています。そのため一見すると脈絡無く用語が並んでいるように見えますが、内容により以下の４つに大別して整理すると理解し易いと思います。

表４-１　用語の分類

基本となる用語の定義	3.1 資産（asset）	
	3.5 情報セキュリティ事象（information security event）	
	3.6 情報セキュリティインシデント（information security incident）	
情報セキュリティに関する用語の定義	3.4 情報セキュリティ（information security）	
	3.3 機密性（confidentiality）	
	3.8 完全性（integrity）	
	3.2 可用性（availability）	
リスクマネジメントに関する用語の定義	3.14 リスクマネジメント（risk management）	
	3.12 リスクアセスメント（risk assessment）	3.11 リスク分析（risk analysis）
		参考　リスク因子（risk source）
		3.13 リスク評価（risk evaluation）
	3.15 リスク対応（risk treatment）	
	3.10 リスクの受容（risk acceptance）	
	3.9 残留リスク（residual risk）	
マネジメントシステムに関する用語の定義	3.7 情報セキュリティマネジメントシステム, ISMS（information security management system）	
	3.16 適用宣言書（statement of applicability）	

４．１　情報セキュリティとは

組織経営に不可欠である情報は、適切に保護されなければなりません。情報が適切に保

護されていないと、漏洩したり、内容が不正確であったり、必要な時に使えない等、業務の遂行に支障をきたすといったリスクがあります。「情報セキュリティ」とは、重要な情報をこうしたリスクから守ることです。

ISMS 認証基準では、情報セキュリティを以下のように定義しています。

> 3.4 情報セキュリティ(information security)
> 情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい（JIS Q 27002:2006）。
> (JIS Q 27001:2006　3 用語及び定義　より引用)

情報セキュリティに関わるリスクを明確にするために、情報セキュリティの主たる 3 要素である「機密性」、「完全性」、「可用性」のそれぞれの観点から分析を行います。その他の 4 つの特性は、通常上記 3 つの要素から導くことができると考えられます。

> 3.1 資産（asset）
> 組織にとって価値をもつもの（JIS Q 13335-1:2006）。
> （JIS Q 27001:2006　3 用語及び定義　より引用）

なお、「資産」の詳細については、JIS Q 27002 の箇条 7 に説明されており、情報は資産の一部として扱われることになります。本ガイドでは情報に関わる資産として 7.2.4 (1)②に例示をしていますので、参照して下さい。

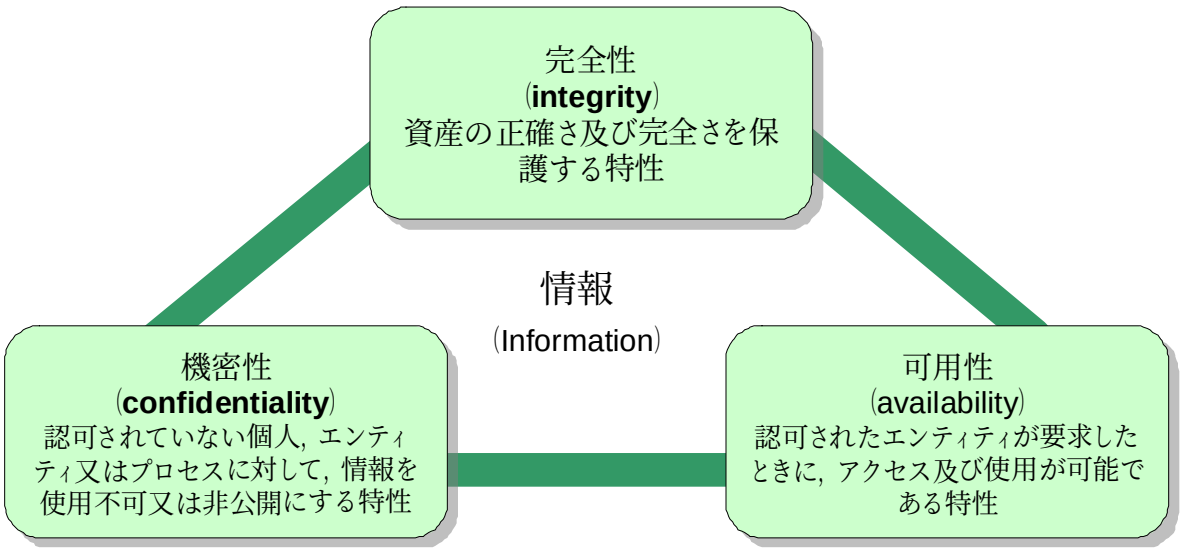


図 4 - 1　情報セキュリティの主な要素

「機密性」、「完全性」、「可用性」は、1992 年に発行された「OECD 情報セキュリティガイ

ドラインに関する委員会勧告」[2]の附属文書「情報システムのセキュリティガイドライン」[3]（以下、「OECD ガイドライン」という。）において定義されて以来使われてきました。

> 情報システムの機密性、完全性及び可用性を阻害する危害（harm）から情報システムを保護すること
>
> （OECD ガイドライン:1992　より引用）

この 3 つの「～性」は、その頭文字をとって「情報セキュリティの C.I.A」と言われることがあります。

ISMS 認証基準では、機密性、完全性、可用性を以下のように定義しています。

> 3.3 機密性(confidentiality)
> 認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性（JIS Q 13335-1:2006）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

情報の機密性は、「情報が漏洩しないようにする」ことにより確保されます。

> 3.8 完全性(integrity)
> 資産の正確さ及び完全さを保護する特性（JIS Q 13335-1:2006）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

完全性には二つの意味があります。一つは情報そのものの完全性を確保することです。これは「情報が改ざんされないようにする」ことに関連します。

もう一つは情報処理の方法の完全性です。これは、「情報システムが勝手に変更されないようにする」ことや「情報の取扱いが手順化されていて、その手順が確実に順守されるようにする」ことに関連します。

> 3.2 可用性(availability)
> 認可されたエンティティが要求したときに，アクセス及び使用が可能である特性（JIS Q 13335-1:2006）。
> (JIS Q 27001:2006　3 用語及び定義　より引用)

---

[2] Recommendation of the Council concerning Guidelines for the Security of Information Systems(adopted by the Council at its 793rd Session of 26-27 November 1992)

[3] Guidelines for the Security of Information Systems,26 November 1992

可用性は、「自然災害やシステムダウンなどにより、情報が使えなくなること」に関連します。

なお、その他の 4 つの特性については、JIS Q 13335-1:2006 に定義があり、以下のようになっています。

真正性（authenticity）
ある主体又は資源が，主張どおりであることを確実にする特性。真正性は，利用者，プロセス，システム，情報などのエンティティに対して適用する。

責任追跡性（accountability）
あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性（**JIS X 5004**）

否認防止（non-repudiation）
ある活動又は事象が起きたことを，後になって否認されないように証明する能力。

信頼性（reliability）
意図した動作及び結果に一致する特性。

（JIS Q 13335-1　2 用語及び定義　より引用）

４．２　リスクマネジメントとは

ISMS 認証基準では、リスクマネジメントについては以下のように定義しています。

3.14　リスクマネジメント（risk management）
リスクに関して組織を指揮し管理する調整された活動（TR Q 0008:2003）。

（JIS Q 27001:2006　3 用語及び定義　より引用）

リスクは、「組織の活動の遂行を阻害する事象の発生の可能性」と定義しますが、標準情報(TR Q 0008:2003)「リスクマネジメント－用語－規格において使用するための指針」には以下のように定義しています。

3.1.1 リスク（risk）
事象（3.1.4）の発生確率（3.1.3）と事象の結果（3.1.2）の組合せ。
備考 1.　用語“リスク”は，一般に少なくとも好ましくない結果を得る可能性がある場合にだけ使われる。

2. ある場合には，リスクは期待した成果，又は事象からの偏差の可能性から生じる。
3. 安全に関する事項に対しては，ISO/IEC Guide51:1999 を参照のこと。

（TR Q 0008:2003　3.用語及び定義　より引用）

3.4.10 リスクの受容（risk acceptance）
リスク（3.1.1）を受容する意思決定。
備考 1.“受容する（accept）”という動詞は，名詞“受容（acceptance）”のもつ基礎的な辞書の意味を引き継いで選ばれている。
2.リスクの受容は，リスク基準に依存する。

（TR Q 0008:2003　3.用語及び定義　より引用）

3.4.11 残留リスク（residual risk）
リスク対応（3.4.1）の後に残っているリスク（3.1.1）。
備考　安全に関する適用の場合は，ISO/IEC Guide51:1999 参照。

（TR Q 0008:2003　3.用語及び定義　より引用）

リスクの特性は、上記「備考　2.」にあるように、結果そのものの「良い」、「悪い」により規定されるものではなく、その期待値に対してどのような分布を持つかにより規定されます。また、リスクとはあくまで「可能性」のことを指します。

４．３　マネジメントシステムとは

ISMS 認証基準では、情報セキュリティマネジメントシステム（ISMS）については以下のように定義しています。

3.7　情報セキュリティマネジメントシステム，ISMS（information security management system）
マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分。
注記　マネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる。

（JIS Q 27001:2006　3 用語及び定義　より引用）

ISMS 認証基準では、適用宣言書については以下のように定義しています。

> 3.16　適用宣言書（statement of applicability）
> その組織の ISMS に関連して適用する管理目的及び管理策を記述した文書。
> 注記　管理目的及び管理策は，組織の情報セキュリティに対する，次のものに基づく。
> ― リスクアセスメント及びリスク対応のプロセスの結果及び結論
> ― 法令又は規制の要求事項
> ― 契約上の義務
> ― 事業上の要求事項
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

４．４　情報セキュリティ事象・情報セキュリティインシデントについて

JIS Q 27002:2006 への改正にともなって、「13　情報セキュリティインシデントの管理」がひとつの箇条としてまとめられました。これに伴って、表 3-1 のように関連した用語の定義が追加されました。

> **3.5 情報セキュリティ事象**（information security event）
> システム，サービス又はネットワークにおける特定の状態の発生。特定の状態とは，情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関連するかもしれない未知の状況を示しているものをいう（ISO/IEC TR 18044:2004）。
>
> **3.6 情報セキュリティインシデント**（information security incident）
> 望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（ISO/IEC TR 18044:2004）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

詳細は、「JIS Q 27002:2006　13　情報セキュリティインシデントの管理」や「ISO/IEC TR 18044:2004 Information Security Incident Management」を参照して下さい。

参考：「ISO/IEC TR 18044 Information Security Incident Management（情報セキュリティインシデントの管理）」の概要

JTC1/SC27 では、情報セキュリティインシデントの管理に関して ISO/IEC TR 18044 という技術報告書（Technical Report）を発表しています。

この技術報告書は、以下のような点から助言及び指針を与えています。

組織は、情報セキュリティインシデントへの対応手順や迅速に対応できる体制を整備しなければなりません。しかしながら、たとえ体制を確立したとしても、現場の当事者が多くの情報セキュリティ事象の中から情報セキュリティインシデントを検出するのが遅れると、結果的に対応が遅れてしまいます。したがって、情報セキュリティインシデントと認識された以後のことばかりではなく、それ以前の情報セキュリティ事象にも広く注意をする必要があります。つまり、情報セキュリティインシデントとなる可能性や未知の状況を示す「情報セキュリティ事象」が、事業運営を危うくしたり情報セキュリティを脅かしたりする確率を高め、結果として情報セキュリティインシデントに変遷する可能性に留意する必要があります。そのため、情報セキュリティインシデントの管理では、情報セキュリティインシデントとして検出される前の情報セキュリティ事象を対象とする管理策も講じなければなりません。

それらについて以下の流れで示しています。

・情報セキュリティインシデントの検出、報告及び査定
・影響の予防及び低減、並びに、影響からの回復のための適切な管理策の活性化（activation）を含んだ、情報セキュリティインシデントへの対応
・情報セキュリティインシデントからの学習及び予防的管理策の探求、情報セキュリティインシデントマネジメントの総合的な取り組みに対する四六時中の改善

また、これらを確立するために PDCA モデルに似た以下のようなプロセスモデルを適用しています。

・計画準備段階
・利用段階
・レビュー段階
・改善段階

このようなプロセスモデルを適用し、計画準備段階において事前計画に基づく対応手順を充実させた上で、実際の情報セキュリティインシデント発生時に、手順に従って対応することを基本にしています。しかし、その一方で、計画準備段階に用意した手順が情報セキュリティインシデントの実情に沿わないときには、定められた手順以外の対応をするための手続きが必要であることも指摘しています。なぜなら、情報セキュリティインシデントにおいては、予測不可能な状況となることもあり、その場合には、事前計画で想定した

範囲内だけで事後対応を実施することは、むしろ想定外の状況に柔軟に対応できなくなる場合があります。そのため、想定外の状況に遭遇した場合には、担当者の判断で、事前に定められた処置とは異なる例外処置をとれるようにすることも必要です。この技術報告書は、そのような例外処置に関する管理策を講じることについても述べています。

５．ISMS における法規適合性

ISMS における法規適合性とは、組織として対処すべき法的リスクを特定し、リスクアセスメント[4]に基づいた合理的なリスク対策を実施することです。ISMS プロセスでは、リスクマネジメントの枠組みの中に、法令及び規制の要求事項に対応することが組み込まれています。個人情報保護を例にとると、個人情報の保護についてどの程度の保護レベルまで担保しなければならないかについては、最終的には組織の合理的な価値判断と資源配分の中で実現されるものです。しかしながら、個人情報保護法の完全施行に伴い、個人情報に関するシステムを適用範囲とした ISMS は､最低限個人情報保護法に準拠せざるを得ません。その結果、リスクアセスメントに際しては、「個人情報の保護に関する法律」の第四章の第一節第 15 条から第 31 条、個人情報保護ガイドラインや、JIS Q 15001 など企業が自主的に採用する規範や契約にもとづく義務への準拠も含めたリスクマネジメントを行うことになります。）

５．１　マネジメントシステムの要求事項

法規を遵守すること（以下「法規遵守」又は「法規順守性」と言います）については、組織あるいは企業にとって不可欠な要求事項であり、ISMS を構築するための有効な出発点となります。

ISMS では、マネジメントシステムの要求事項として、「4.2 ISMS の確立及び運営管理」があります。その要求事項の中で「4.2.1 ISMS の確立 b) ISMS の基本方針を定義する」では、「事業上の要求事項及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮する」と規定しています。また、「c) リスクアセスメントに対する取組方を定義する」では、「ISMS, 特定された事業上の情報セキュリティ要求事項, 並びに特定された法令及び規制の要求事項（legal and regulatory requirements）に適したリスクアセスメントの方法を特定する」と規定しています（表５-１を参照)。

このことから、組織として法的リスク、経営リスクについて対処する基本方針を策定する必要があり、対処すべきリスクを経営に対する影響、重要度に応じてリスクアセスメントし、経営上の観点からリスク対策を実施しなければなりません。しかしながら、リスクアセスメントのプロセスの過程で、著しいコンプライアンス（法規順守）違反が判明した際は、分析を一時中断し、管理策の検討、導入の工程に速やかに入る必要があります。このような法規順守違反を判断するためには、順守すべき要求事項をベースラインとするベースラインアプローチ的手法を取ることも有効です。

---

[4] 法令（強行法規を含む）及び規制要求事項を識別し、その適合性を評価することは、リスクアセスメントの内容に含まれます。

すなわち、情報資産を洗い出す際に、管理すべき個人情報、関係する法令を特定し、システムに自社の立場、業務を折り込み、法令も反映した実効性のあるマネジメントシステムを構築する必要があります。

表５-１　ISMS 認証基準の 4. 情報セキュリティマネジメントシステム（抜粋）

4 情報セキュリティマネジメントシステム

4.1 一般要求事項

組織は，その組織の事業活動全般及び直面するリスクに対する考慮のもとで，文書化した ISMS を確立，導入，運用，監視，レビュー，維持及び改善しなければならない。

4.2 ISMS の確立及び運営管理

4.2.1 ISMS の確立

組織は，次の事項を実行しなければならない。

a) 事業・組織・所在地・資産・技術の特徴の見地から，ISMS の適用範囲及び境界を定義する。この定義には，適用範囲からの除外について，その詳細及びそれが正当である理由も含めるものとする（1.2 参照)。

b) ISMS 基本方針を，事業・組織・所在地・資産・技術の特徴の見地から，次を満たすように定義する。

1) 目的を設定するための枠組みを含め，また，情報セキュリティに関係する活動の方向性の全般的認識及び原則を確立する。

2) 事業上及び法令又は規制の要求事項，並びに契約上のセキュリティ義務を考慮する。

注記 この規格の目的のために，ISMS 基本方針は，情報セキュリティ基本方針を包含する上位概念とする。これらの方針は，一つの文書に記載することができる。

c) リスクアセスメントに対する組織の取組み方を，次を満たすように定義する。

1) ISMS，特定された事業上の情報セキュリティの要求事項，並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法を特定する。

2) リスク受容基準を設定し，また，リスクの受容可能レベルを特定する［5.1 f) 参照］。

選択するリスクアセスメントの方法は，それを用いたリスクアセスメントが，比較可能で，かつ，再現可能な結果を生み出すことを確実にしなければならない。

注記 リスクアセスメントの方法には，幾つか異なるものがある。

参考 リスクアセスメントの方法の例については，TR X 0036-3 による。

d) リスクを，特定する。

e) それらのリスクを分析し，評価する。

f) リスク対応のための選択肢を特定し，評価する。

g) リスク対応のための，管理目的及び管理策を選択する。

h) その結果としての残留リスクについて経営陣の承認を得る。

i) その ISMS を導入し，運用することについて経営陣の許可を得る。

j) 適用宣言書を作成する。

５．２　法規適合性の要求項目

ISMS 認証基準附属書 A「管理目的及び管理策」A.15.1 法的要求事項の順守における「A.15.1.4 個人データ及び個人情報の保護」では、「個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にしなければならない。」と規定しています。「A.13.2.3 証拠の収集」では、「情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には，関係する法域で定めている証拠に関する規則に従うために，証拠を収集，保全及び提出しなければならない。」と規定しています。さらに、「A.15.1.3 組織の記録の保護」では、「重要な記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊及び改ざんから保護しなければならない。」と規定しています（表５-２を参照）。

ISMS では 133 の管理策が規定されており、管理策の中から個人情報保護対応として適切なものを選択しなければならず、個人情報を扱っている事業者は、法的要求事項への適合を合理的な理由なしに不採用にすることはできません。もっとも、133 項目の管理策に個人情報保護対応のすべての管理策が網羅されているわけではないので、組織は個人情報保護ガイドライン、契約上の義務なども考慮して必要に応じて別途追加の管理策を採択しなければなりません。ISMS における具体的な管理策の選択は、法律上の責任判断に影響を与える可能性があります。そのため、リスクアセスメントを実施した上で管理策を決定することにより、より合理的なシステムを構築することができるのです。なお、リスクアセスメント結果に基づく組織の適切な対応とそれに基づいた運用の記録は、適切なリスク対策を行ったことの証拠として役立てることができます。

表５-２　ISMS 認証基準の附属書 A「管理目的及び管理策」（抜粋）

A.15　順守		
A.15.1　法的要求事項の順守 目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 注記　法的順守は，しばしば，コンプライアンスといわれることがある。		
A.15.1.1	適用法令の識別	管理策 各情報システム及び組織について，すべての関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組み方を，明確に定め，文書化し，また，最新に保たなければならない。
A.15.1.2	知的財産権（IPR）	管理策： 知的財産権が存在する可能性があるものを利用するとき，及び権利関係のあるソフトウェア製品を利用するときは，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を導入しなければならない。

A.15.1.3	組織の記録の保護	管理策 重要な記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊及び改ざんから保護しなければならない。
A.15.1.4	個人データ及び個人情報の保護	管理策 個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にしなければならない。
A.15.1.5	情報処理施設の不正使用防止	管理策 認可されていない目的のための情報処理施設の利用は，阻止しなければならない。
A.15.1.6	暗号化機能に対する規制	管理策 暗号化機能は，関連するすべての協定，法令及び規制を順守して用いなければならない。

なお、「BS 7799-2　PD3005：2002（BS 7799　第２部　管理策の選択）」における法的要求事項の「データ保護及び個人情報の機密保持」に関する詳細管理策については、次のように記載されています。

BS7799-2 第２部の管理策の A.12.1.1 に記述されているように、組織又は検討した ISMS に適用する法的要求事項を特定して、それを文書化することが望ましい。この要求事項の根拠となるのは、BS7799 第２部の管理策である。次の表は、どの BS7799 第２部の管理目的及び管理策が ISO/IEC 17799 の第 12 節に示した法的要求事項の根拠となるのか、又は、その法的要求事項と併せてどの管理目的及び管理策を検討したらよいかについて記述したものである。これが、法的要求事項の完全なリストではないことに注意が必要である。
この手引きでは、次の法的要求事項を扱っている。

要求事項	手引きの参照項
知的財産権（IPR）及びソフトウェアの著作権	3.1.1 (48 項目)
組織の記録の保護	3.1.2 (64 項目)
データ保護及び個人情報の機密保持	3.1.3 (68 項目)
情報処理設備の誤用の防止	3.1.4 (61 項目)
暗号による管理策の規制	3.1.5 (20 項目)
証拠	3.1.6 (27 項目)

これは、要求事項の確定したリストではなく、組織がその固有の事業環境に基づいて要求事項の独自のリストを開発するための基礎としてだけ使用することが望ましい。各組織は、端緒として上記のリストを使用して、適用できる法的、法令上又は規制上の要求事項を識別し、これを受けて、さらに満たすべきすべての追加の要求事項を識別することが望ましい。この要求事項のなかには、取引先との契約上の義務の一部を構成するものがある。これ以外にも、外部委託又は第三

> 者サービスの供与の場合のように、検討すべき契約上の要求事項が発生することがある。こうした要求事項も支えるような管理策が、実施されることを確実にすることが望ましい。
>
> 【PD 3005　BS 7799 第 2 部の管理策の選択の手引き　邦訳版　3.1 抜粋】

ここでは、旧英国基準と当時のガイドである PD 3005 を用いて、法的要求事項の管理目的、管理策が他の複数の管理策と密接に関係があることを示しているに過ぎません。文中の A.12.1.1 等の記載は旧基準のものであり、現基準である JIS Q 27001 では、A.15.1.1 として読み替える必要があります。PD 3005 に記載されていたこれらの法的要求事項に対する追加の管理目的と管理策については、JIPDEC が認証基準移行時に発行したマッピング表などを参照の上、現認証基準との整合をとっていただく必要があります。

６．法的リスクアセスメント

法的リスクアセスメントは、「ISMS の適用範囲及び境界を定義する（STEP1)」、「ISMS の基本方針を定義する（STEP2)」に引き続くリスクアセスメントのプロセスです。その基本的な枠組は、ISMS ユーザーズガイドーJIS Q 27001:2006（ISO/IEC 27001:2005)対応ー(平成２０年１月３１日)の STEP3 ないし STEP5 で述べたものと同じですが、法令及び規制の要求事項の特性に応じた留意点があります。

６．１ 法的リスクアセスメントとは

６．１．１ 本ガイドでいう法的リスクアセスメント

本ガイドでいう法的リスクアセスメントとは、ISMS の構築にあたり「ある脅威が、資産または資産グループのぜい弱性を利用して資産への損失、または損害を与える可能性」のうち、「組織が活動する際に準拠することを求められる法令及び規制の要求事項に故意若しくは過失又は不可抗力により違反することを原因としてもたらされるもの」を「分析評価する全てのプロセス」をいいます。

法的リスクアセスメントがこのように定義されるのは、以下の理由からです。

まず、「リスク」の定義は様々になされますが、ISMS 認証基準は、TR X 0036（GMITS）の考え方を基礎として、TR Q 0008 におけるリスクマネジメントの用語を採用しています。TR X 0036（GMITS）では、「リスク」を「ある脅威が、資産または資産グループのぜい弱性を利用して資産への損失、または損害を与える可能性」と定義しており、TR Q 0008 では、「事象の発生確率と事象の結果の組合わせ」と定義しています(3.1.1 リスク(risk))。従って、法的リスクとはそのうち「組織が活動する際に準拠することを求められる法令及び規制の要求事項に故意若しくは過失又は不可抗力により違反することを原因としてもたらされるもの」と理解することができるのです。次にリスクアセスメント(risk assessment)は、ISMS 認証基準 ３　用語及び定義、3.12 で、「リスク分析からリスク評価までのすべてのプロセス」と定義されています。こうした理由から法的リスクは、上記のように定義できるのです。

なお、TR Q 0008 が 3.1.1.リスク(risk)備考２で「ある場合には、リスクは期待した成果、又は事象からの偏差の可能性から生じる」として、リスクは良い結果の発生可能性をも含むことを示していること、また、経済産業省リスク管理・内部統制に関する研究会の「リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～」(平成１５年６月)第二部ＩＩ.１「リスクマネジメントのあり方」も、「リスク」を単に「事象発生の不確実性」と定義し、「リスクには損失等発生の危険性のみならず、新規事

業進出による利益又は損失の発生可能性等も含むと考える」として、良い結果の発生可能性をも含む考え方を取っていることには留意が必要です。「リスク」の定義を良い結果の発生可能性を含むと考えると、法的リスクアセスメントでは、法令及び規制の要求事項に違反して資産への損失、または損害を与える可能性という悪い結果だけでなく、良い結果、つまり、法令及び規制の要求事項を超える状態を実現することにより利益に結びつく可能性の識別評価を行い、その実現に向けた対処策の選定へと進むことができるようになるでしょう。

６．１．２ ISMS 適用範囲と法的リスクアセスメント

ISMS の適用範囲の特定は、適用すべき法令及び規制の要求事項を特定するために重要です。法律や条令、行政機関の命令、これらを根拠とする裁判などは、その効力の及ぶ範囲が原則としてその国の範囲に限られます。また、それらのうちには、対象や、義務を負う主体に制限を設けている場合があります。例えば、「個人情報の保護に関する法律」の属地的適用範囲は原則として日本国内に限られ、義務を負う主体は、個人情報取扱事業者です。このように、法令及び規制の要求事項には属地的・属人的適用範囲があります。そこで、事業、組織、所在地、資産、技術の特徴の観点から適用範囲を決定することは、法的リスクアセスメントに適用される法令及び規制の要求事項の範囲を決めることに直結します。従って、ISMS の適用範囲を定めるにあたっては、基本方針との関係を考慮しながら、事業、組織、所在地、資産、技術の特徴の観点から厳密に範囲を画することが重要です。

15 順守

15.1 法的要求事項の順守

目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

情報システムの設計，運用，利用及び管理には，法令，規制及び契約上のセキュリティ要求事項が適用される場合がある。

特定の法的要求事項については，組織の法律顧問又は適切な資格をもつ法律の実務家に助言を求めることが望ましい。法律の定める要求事項は，国ごとに異なっており，また，一つの国で作成され別の国へ伝送される情報（すなわち，国境を越えたデータの流れ）についても異なる場合がある。

注記　法的順守は，しばしば，コンプライアンスといわれることがある。

（JIS Q 27002:2006 15 順守　15.1 法的要求事項の順守　より引用）

６．１．３ 法的リスクアセスメントの対象

法的リスクアセスメントにおいても、その対象は、情報資産（JIS Q 27002では、資産という用語を用いている。）だけでなく情報資産を扱う人の行為にもおよぶことがあります。例えば、個人情報保護法第１６条の目的外利用への適合性を評価する場合、その対象は、システムだけでなくこのシステムを用いて個人情報を取り扱う人の行為であることがあります。著作権法でも、その規範が評価する対象は、著作物を扱う人の行為です。

ISMSが個人情報保護法の順守を含むコンプライアンス経営の構築・維持、立証に資するのは、このようにISMSのアセスメントの対象が単なる資産そのものでなく、組織や人の行動にまで及ぶことによるのです。

６．２ リスクアセスメントについての体系的な取り組み方法の定義

６．２．１ ISMS認証基準での定義

「リスクアセスメントについての体系的な取り組み方法の定義」の内容は以下のとおり定めています(ISMS認証基準(JIS Q 27001:2006) 4.2.1c))。

> c) リスクアセスメントに対する組織の取組み方を，次を満たすように定義する。
>
> 1) ISMS，特定された事業上の情報セキュリティの要求事項，並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法を特定する。
>
> 2) リスク受容基準を設定し，また，リスクの受容可能レベルを特定する［5.1 f) 参照］。
>
> 選択するリスクアセスメントの方法は，それを用いたリスクアセスメントが，比較可能で，かつ，再現可能な結果を生み出すことを確実にしなければならない。
>
> 注記　リスクアセスメントの方法には，幾つか異なるものがある。
>
> 参考　リスクアセスメントの方法の例については，TR X 0036-3による。
>
> （JIS Q 27001:2006　4.2.1ISMSの確立 c)　より引用）

「体系的な取組み方」とは、「リスクアセスメント手順や判断基準を明確にすること」です(ISMS ユーザーズガイドーJIS Q 27001:2006（ISO/IEC 27001:2005）対応ー(平成２０年１月３１日)4.2.3(2))。

①リスクアセスメントの方法

「リスクアセスメント」の方法は、「特定された法令及び規制の要求事項に適した」ものである必要があることを明らかにして、リスクアセスメントのプロセスで情報資産が法

令及び規制の要求事項に適合するか否かを評価することを求めています。

②評価基準の識別

法的リスクアセスメントにおける評価の基準は、「特定された法令及び規制の要求事項」です。この中には、「個人情報保護ガイドライン」、「企業が自主的に採用する例えば JIS Q 15001 などの規範の要求事項」、「契約上の要求事項」なども含まれます。これらの要求事項は、極めて多くに上ることでしょう。法的リスクアセスメントを「その ISMS に適し」たものとするには、その組織に適用される強行法規やそのガイドライン、顧客との契約、組織が社会に対して採用を宣言したセキュリティポリシーやプライバシーポリシー、組織が採用したガイドラインや JIS 規格などを無視すべきではありませんが、ISMS の適用範囲、目的に応じ、強行法規か否か、組織の社会的地位、規範の重要性などを考慮して、その組織の ISMS にふさわしい「法令及び規制の要求事項」を特定することが重要です。例えば、個人情報取扱事業者が個人情報の収集、取扱を行う情報資産を適用範囲内に持つ ISMS を構築する際には、個人情報保護法や主務大臣のガイドラインを識別することが重要です。また、財務会計情報を適用範囲とする ISMS の構築には、財務会計に関する強行法規、金融商品取引法による内部統制、その他の規制を識別することが求められます。

③評価の対象

法的リスクアセスメントの対象は、評価基準が対象とする情報資産そのものと、その情報資産を利用した組織の活動です。その結果、法的リスクアセスメントの対象は、情報資産そのものに留まらず、情報資産の設計、運用、使用及び管理に及ぶことがあります。

６．２．２ リスクアセスメントの手順を定める

リスクアセスメントの手順を定めるにあたっては、ISMS の適用範囲決定に際して考慮された事業、組織、所在地、資産、技術の特徴などと、ISMS の基本方針を定めるにあたって考慮された事業上の要求事項及び法令又は規制の要求事項並びに契約上のセキュリティ義務を考慮して、適用範囲にある情報資産に適用される法令又は規制の要求事項並びに契約上のセキュリティ義務を特定します。

６．２．３ 適切な分析手法の選択

ISMS ユーザーズガイドーJIS Q 27001:2006（ISO/IEC 27001:2005）対応ー(平成２０年１月３１日) 4.2.3(3)では、適切な分析手法としてベースラインアプローチ以下４つのリスクアセスメントの方法を紹介しています。法的リスクアセスメントでは、評価の基準と評価の対象、対処方針や対処策のありかたに応じてこれらを組み合わせて行われます。重要

な法令及び規制の要求事項に合致しているかどうかを評価するときは、ベースラインアプローチに類した方法（ギャップ分析を含む。）が適切でしょう。重要な法令及び規制の要求事項に反するときは、その組織の経営は順法性を著しく欠くため、速やかに違法状態を回避する必要があります。重要な法令及び規制の要求事項に合致していることが確認できた後は、その運用・保守に関する脅威の発生可能性、ぜい弱性などを詳細に見ることによって対処方針や対処策の選択を合理的に行う必要があります。その際は詳細リスク分析のほうが、ベースラインアプローチよりも対処方針や対処策の選択に多くの資料を提供することでしょう。

このように、法的リスクアセスメントにおいても、ベースラインアプローチや詳細リスク分析等を用いた組合わせアプローチを利用することが有用でしょう。

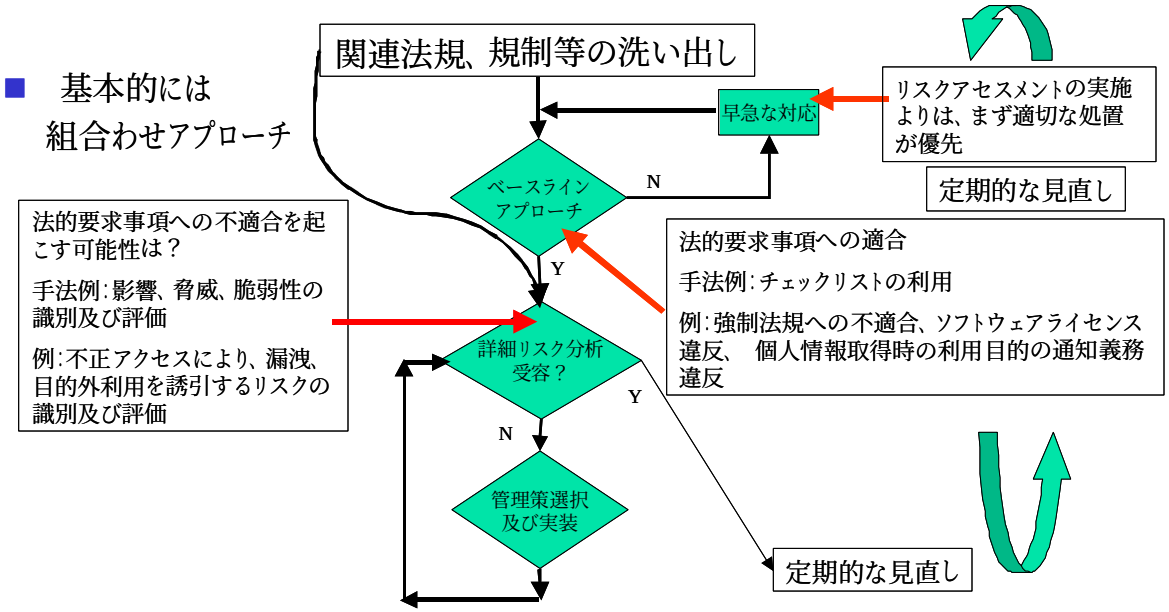


図 6-1 法令及び規制の要求事項に適したリスクアセスメントの方法

図 6-1 では、法令及び規制の要求事項に適したリスクアセスメントの方法を示しています。基本的には、組合わせアプローチを採用することが期待されます。また、リスクアセスメントの手法や結果は。定期的に見直されなければなりません。

法的リスクアセスメントでは、必要に応じ、情報資産の取扱いに関する設計、運用、使用及び管理等の状況を見る必要があります。この点について JIS Q 27002 では以下のとおり定めています。（JIS Q 27002　15.1）

15 順守 15.1 法的要求事項の順守

目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

情報システムの設計，運用，利用及び管理には，法令，規制及び契約上のセキュリティ要求事項が適用される場合がある。

特定の法的要求事項については，組織の法律顧問又は適切な資格をもつ法律の実務家に助言を求めることが望ましい。法律の定める要求事項は，国ごとに異なっており，また，一つの国で作成され別の国へ伝送される情報（すなわち，国境を越えたデータの流れ）についても異なる場合がある。

注記　法的順守は，しばしば，コンプライアンスといわれることがある。

（JIS Q 27002:2006 15 順守　15.1 法的要求事項の順守　より引用）

例えば、個人情報保護法への適合性を評価する場合には、適用範囲にある情報システムや人の行為から個人情報を洗い出し、個人情報、個人データ及び保有個人データを収集し取り扱う際に予め利用目的が特定されているか、利用目的達成に必要な範囲にとどめているか、安全対策が講じられているか、第三者提供を許容していないか、本人からの権利行使に応じられる条件が整備されているかなどの法律上の要件について、設計、運用、使用及び管理の全てにわたって評価するプロセスが必要です。このプロセスは、まず、仕様、運用、使用及び管理それぞれの設計を評価し、次にそれらの運用等を評価するという手順をとると便利です。

システムの仕様、運用、使用及び管理それぞれの設計を評価した結果、重要な法令及び規制の要求事項に適合していないことが判明したときは、リスクを受容することは許されませんから、リスクアセスメントの手順は、適法化のための対処を講じた後に進めることになります。

しかし、設計上適合性が確認されても、その運用、使用、管理の如何によっては適法状態が維持できなくなる可能性があります。例えば、個人情報の保護に関する法律の２４条以下にある本人の権利者対応を行うためのシステムが準備されていても、その CIA が確保されなければ適法状態は確保できません。また、CIA の確保を十二分に行えば、良い結果の実現に向けた対処ができることになるでしょう。このような場合、リスクの洗い出しのプロセスには、発生頻度やギャップの測定ができるアプローチが有効でしょう。仕様、運用、使用及び管理それぞれの設計上適法性が確認されている以上、その運用のリスクについては回避以外の対処方針を定め、これに応じた対処策を選ぶことも可能であり、その選択のためには、発生頻度やリスクの算定が役に立つからです。

６．２．４ 受容可能なリスクの水準を特定することについて

前項に述べたとおり、組織は、そもそも適用範囲の情報資産の仕様、運用、使用及び管

理それぞれの設計が、強行法規及びその組織の ISMS 基本方針で考慮された法令及び規制の要求事項並びに契約上のセキュリティ義務に反する以上 ISMS の適合性評価は受けられません。受容可能なリスクの水準を特定することができるのは、その運用、使用及び管理に関する CIA の喪失がもたらすリスクに関するものに限られます。

６．２．５ リスクアセスメントの手順について

このように、個人情報にかぎらず情報資産は事業上の重要な資産なので両者のリスクは一致します。しかし、上記のように法的リスクアセスメントでは、設計とその他の段階を分けて評価する、評価者が異なることがある、などの特殊性があります。そのため、リスクアセスメントにおいて「特定された事業上の情報セキュリティの要求事項」と「特定された法令及び規制の要求事項」のアセスメントを分けて行うことが便利な場合もあります。

６．３ リスクの識別

６．３．１ 法令及び規制の要求事項並びに契約上のセキュリティ義務の識別

(１)個人情報保護法と関連法規

ISMS の適用範囲に情報資産として、個人情報が収集または取扱われている場合、洗い出されるべき主な国内法令及び規制の要求事項としては以下があります。その具体的な規範内容を明らかにするには判例、裁判例も参照する必要があります。

■個人情報保護法とその内容を明らかにする規定類

①個人情報の保護に関する法律（平成１５年５月３０日法律第５７号）

②個人情報保護法の内容を明らかにする以下の規定類

ｱ 「個人情報保護に関する基本方針」閣議決定（平成１６年４月２日）

ｲ 主務大臣の個人情報保護法に関するガイドライン

ｳ 個人情報の保護に関する民法の不法行為法、契約法

ｴ 内部統制に関する会社法関連規定

■特定業種の個人情報の取扱を定める法令（順不同）

ｱ 職業安定法（第５条の４）・・・(求職者等の個人情報の取扱い)

ｲ 労働者派遣法（労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律）（第２４条の３）・・・(個人情報の取扱い)

ｳ 割賦販売法（第３９条）・・・(信用情報の適正な使用等)

ｴ　銀行法施行規則
ｵ　貸金業の規制等に関する法律（第３０条第２項）・・・（過剰貸付けの防止）

■特定の組織等について守秘義務や個人情報の収集や取扱いの方法を定める法令（順不同）
ｱ　刑法（第１３４条）
ｲ　医師法
ｳ　看護士法
ｴ　薬剤師法
ｵ　薬事法
ｶ　助産士法
ｷ　弁護士法
ｸ　司法書士法
ｹ　行政書士法
ｺ　公認会計士法（第２７条他）
ｻ　税理士法
ｼ　労働者派遣事業法（第２４条の４）
ｽ　有料職業紹介法

■組織の特定の行為を規制する法令
ｱ　住民基本台帳法

■情報資産保護を目的とする法令
ｱ　不正競争防止法（第２条第１項）
ｲ　著作権法

(２)契約中の個人情報保護の収集、取扱、守秘に関する条項

(３)個人情報保護に関する業界ガイドライン

(４)組織、企業の採用する個人情報保護に関する方針や規定
ｱ　プライバシーポリシー
ｲ　セキュリティ基本方針、規定、手順書
ｳ　外部委託契約書
ｴ　外部委託選定基準書
ｵ　従業員等の個人情報取扱規定

なお、上記は自組織に関するものですが、個人情報や個人データを他の組織から収集し、

委託を受け、または他の組織と共同利用するときには、その他組織が準拠する法令についても洗い出さなければ、他組織との間の取引途絶などのリスクをアセスメントすることができませんので注意が必要です。

６．３．２ 民法等にもとづく法的リスク

個人情報保護法の求める義務規定については、個人情報取扱事業者がこれに違反した場合には、民法等にもとづいての損害賠償請求や差止請求を主張される可能性があります。

法的リスクとしては、次のようなことが考えられます。

（１）損害賠償責任

個人情報取扱事業者が、その取り扱う個人データの安全管理のために必要かつ適切な措置を講ずべき義務を果たさなかった場合には、個人データの漏洩・改ざん事故などによって生じた損害についての賠償責任を問われることもあります。また、外部委託先で事故が発生した場合にも損害賠償責任を負う可能性があります。

（２）差止請求・株主代表訴訟など

人格権の侵害のおそれがある場合には、販売・頒布禁止仮処分、システム稼動の差止仮処分、侵害行為に対する差止請求あるいは廃棄請求などの主張もあり得ます。安全管理措置を怠ったことによって会社に重大な損害を与える可能性がある場合には、株主や監査役による差止仮処分や差止請求の可能性があります。安全管理に関する経営判断を誤り会社に損害を発生させたときには、株主代表訴訟の提起の可能性もあります。

６．４ リスクアセスメント

リスクアセスメントの方法、特に法的リスクアセスメントにおける留意事項、リスク対応方針や目標設定時の注意点などについては第７章で論じます。

７．情報セキュリティマネジメントシステム

ここでは、ISMS の法規準拠、なかでも個人情報保護法への準拠に際して必要とされる重要な事柄について、ISMS の構築、導入、維持、継続的改善のプロセスの説明に織り込んで解説します。

７．１ ISMS の確立と運用管理

ISMS 認証基準で採用されたプロセスアプローチに基づく PDCA モデルの導入は、ISMS の構築に不可欠な考え方です。

ISMS 認証基準の本文ではプロセスアプローチを採用することを推奨しており、PDCA の各ステップを表 7-1 のように規定しています。

表 7-1　ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための，リスクマネジメント及び情報セキュリティの改善に関連した，ISMS 基本方針，目的，プロセス及び手順の確立
Do－実行 (ISMS の導入及び運用)	ISMS 基本方針，管理策，プロセス及び手順の導入及び運用
Check－点検 (ISMS の監視及びレビュー)	ISMS 基本方針，目的及び実際の経験に照らした，プロセスのパフォーマンスのアセスメント（適用可能ならば測定），及びその結果のレビューのための経営陣への報告
Act－処置 （ISMS の維持及び改善）	ISMS の継続的な改善を達成するための，ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた，是正処置及び予防処置の実施

（JIS Q 27001:2006　0.2 ISMS の採用　0.2.2 プロセスアプローチ　より引用）

PDCA モデルの各ステップと ISMS 認証基準の条項は、表 7-2 のように対応しています。

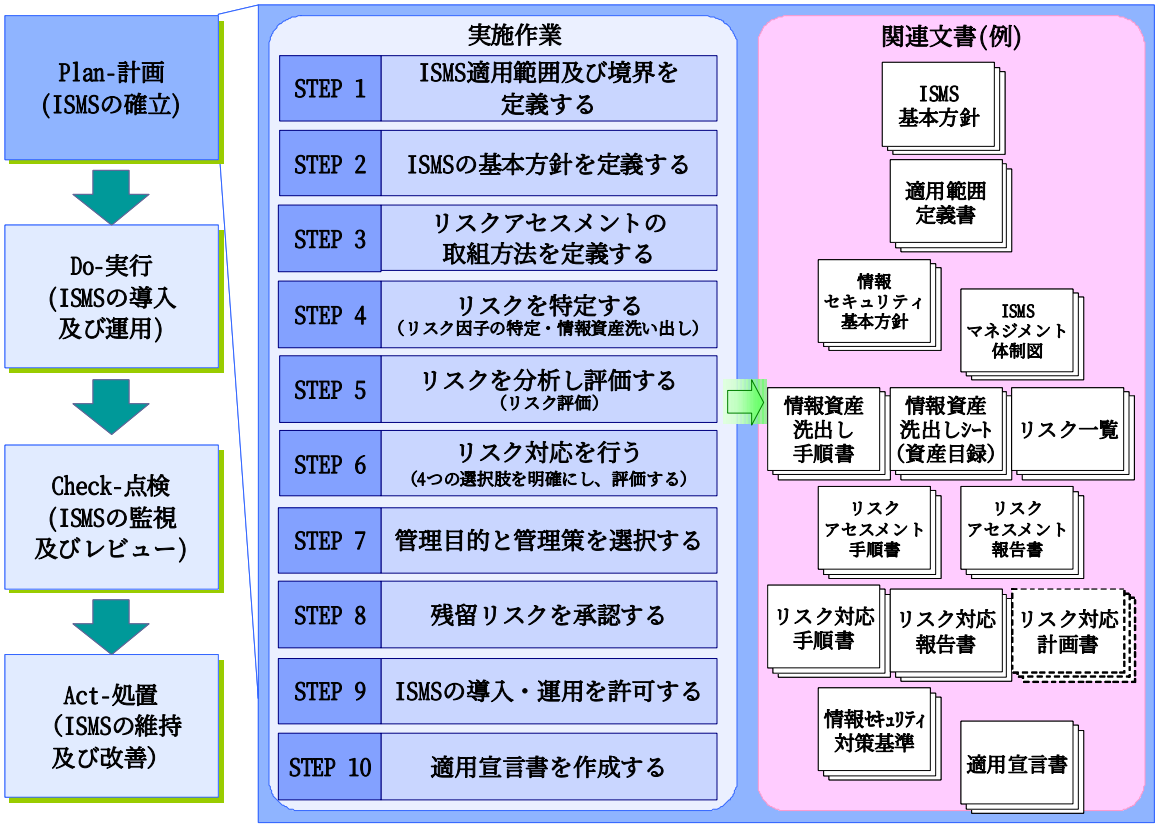
表 7-2　PDCA モデルの各ステップと JIS Q 27001:2006 の条項の対応

活動	認証基準の条項
Plan－計画（ISMS の確立）	4.2.1 a)～j)
Do－実行(ISMS の導入及び運用)	4.2.2 a)～h)
Check－点検(ISMS の監視及びレビュー)	4.2.3 a)～h)
Act－処置（ISMS の維持及び改善）	4.2.4 a)～d)

以下、ISMS 認証基準で求められる要求事項に関連する活動について個別に説明します。

7.2 ISMS の確立（Plan-計画）

ISMS 認証基準の「4.2 ISMS の確立及び運営管理」では、Plan-計画（ISMS の確立）の手順を図 7-1 に示す 10 のステップ（STEP 1～STEP 10）で規定しています。



注）文書名は全て例示

図 7-1　ISMS の確立の手順

＜参考＞
「ISMS の確立」については、上記 10 のステップを表 7-3 の 3 つのフェーズに分けて考えると分かり易い場合があります。この考え方は、JIPDEC が発行する「情報セキュリティマネジメントシステム適合性評価制度の概要」（パンフレット）で説明されていますので参考にして下さい。

表 7-3　フェーズ 1～3

フェーズ 1	ISMS の適用範囲及び基本方針を確立する	STEP1,2
フェーズ 2	リスクアセスメントに基づいて管理策の選択をする	STEP3～7
フェーズ 3	リスクについて適切に対応する計画を策定する	STEP8～10

ここでは、各々のステップに関して説明していきます。

７．２．１　STEP1　ISMS の適用範囲及び境界を定義する

ISMS の確立は、「事業・組織・所在地・資産・技術の特徴の見地から、ISMS の適用範囲及び境界を定義する」(ISMS 認証基準 4.2.1a))ことから始まります。

「適用範囲」とは、情報セキュリティの管理を当てはめる範囲のことです。

ISMS の適用範囲の如何によって、そこに求められる事業上の情報セキュリティ要求事項、並びに法令及び規制の要求事項は異なります。

そこで、適用範囲を定めるにあたっては、いろいろな要素を考慮することが求められます。

７．２．１．１ 適用範囲になり得る要素（観点）

> 4.2.1 ISMS の確立
>
> a) 事業・組織・所在地・資産・技術の特徴の見地から，ISMS の適用範囲及び境界を定義する。この定義には，適用範囲からの除外について，その詳細及びそれが正当である理由も含めるものとする（1.2 参照）。
>
> （JIS Q 27001:2006　4 2. ISMS の確立及び運営管理　より引用）

組織として真に効果的なマネジメントシステムを構築するためには、重要な資産の取り扱いが適正に保たれるために必要な範囲を 1 つの組織体として、ISMS の適用範囲を決定します。

企業全体を１つのマネジメントシステムとして適用範囲とすることも可能ですし、1事業部門を適用範囲にすることもできます。また、顧客に提供する「サービス」のように、複数の部門（部門全体または一部）にまたがった横断的なマネジメントシステムを 1 つの組織体として適用範囲とすることも可能です。

適用範囲を決定する上で重要なことは、1つのマネジメントとして網羅的であること、及び適用範囲の境界線が明確で、合理的に説明可能であることです。

ISMS 認証基準では、適用範囲を決定するにあたり、以下のようないくつかの観点から検討し、合理的に決定することを要求しています。

- 事業
- 組織
- 所在地
- 資産
- 技術

適用範囲の定義の内容により、今後実施する ISMS 構築の作業負荷が大きく影響されます。

また、資産の洗い出しやリスクアセスメントなどの作業のみならず、管理策の適用や運用管理など適用対象の情報セキュリティ水準を維持する活動全般に影響します。

「適用範囲からの除外について、その詳細及びそれが正当である理由も含める」ことについては、1.2 を参照して下さい。

７.２.１.２ 適用範囲の定義

（1）適用範囲を定義する文書

適用範囲を定義する文書に含むことが望ましい事項として、以下のような項目があげられます。

- ISMS の適用範囲及び内容を確立するために用いたプロセス
- 戦略上及び組織上の情況
- 組織で採用した情報セキュリティのリスクマネジメントのアプローチ
- 情報セキュリティのリスク評価の基準及び要求される保証の程度
- ISMS の適用範囲の中にある資産の特定

これらの事項は、必ずしもその全てが文書化される必要はありません。適用範囲を定義する際に考慮すべきポイントとして理解して下さい。適用範囲の定義に関する文書は、決定後も ISMS の構築作業の過程において常に見直されるべきものです。

（2）適用範囲の定義の作業

ISMS 認証基準に求められる適用範囲の定義に関する事項をまとめると図 7-2 のようになります。

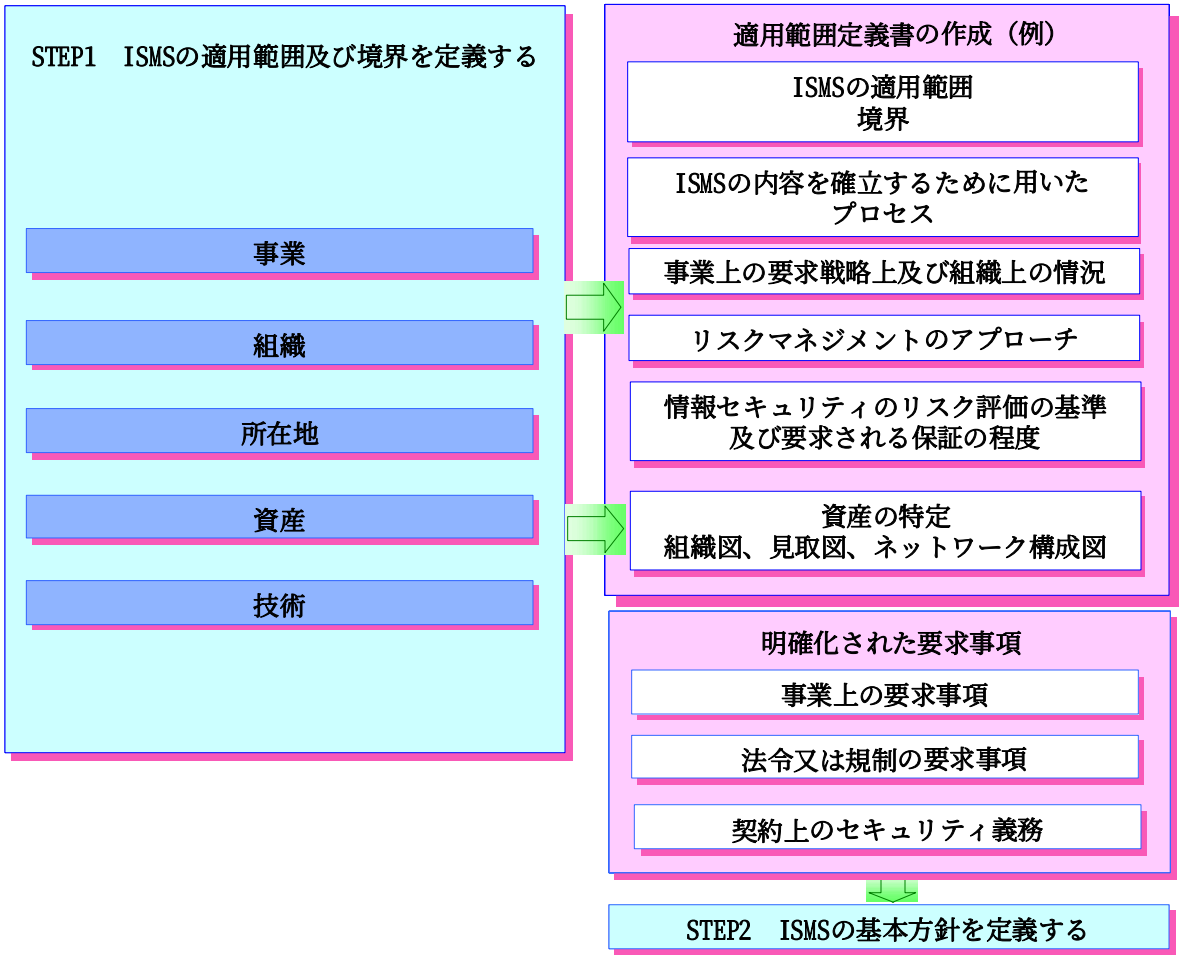


図 7-2　ISMS の適用範囲の定義

適用範囲を定義し、該当するマネジメントシステムを検討することによって、同時に情報セキュリティ上の要求事項も明確になります。特に、次の「ISMS の基本方針の定義」ステップで実施する作業に活用するために、以下の 3 つの要求事項については、特に明確化することに留意して下さい。

- 事業上の要求事項
- 法令又は規制の要求事項
- 契約上のセキュリティ義務

法令又は規制の要求事項を明確化するには，適用範囲として定められた場所その情報資産の内容及び技術を明確にすることが必要です。法令や規制要求事項にはその適用さ

れる場所如何や、適用範囲内の技術の如何によって、適用される法令が異なることがあるからです。個人情報保護法の場合は、日本法人の海外拠点、外国法人の日本拠点に適用になります。

また、法令又は規制の要求事項を明確化する際には、組織自らに適用されるものだけでなく、取引の機会や市場を確保するために必要とされる相手方や市場自体が求めるものについても明確にすべきことに留意しましょう。相手方は、こちらと取引をするにあたり、こちらが相手方の求める個人情報、個人データの取扱いに関する統制に合っていないと、相手方のコンプライアンス経営を維持できなくなるリスクを負います。そのため、相手方は、こちらに対し、相手方のルールに従うように求めます。その結果、こちらは自社のルールに従うだけでなく、相手方のルールにも適合しないと、相手方の参加する市場への参加を制限されたり、場合によっては取引の機会を失うリスクを負うことになるからです。

７.２.２　STEP2　ISMS の基本方針を定義する

ISMS の基本方針は、組織の情報セキュリティマネジメントに対する基本的な考え方を示したものです。同時に、組織として情報セキュリティに関する要求事項に対して責任を負うという意思表示の位置付けとして重要な文書です。その内容は、企業としての使命、目的を表明した経営方針（ビジョン）や行動規範（価値観）と整合性がとられている必要があります。従って、この ISMS 基本方針には要員の行動を規範するために情報セキュリティに関する全般的な方向性及び行動指針に関する内容が明記される必要があります。換言すると、ISMS 基本方針は、情報セキュリティ基本方針を包含する上位概念であるということがいえます。ただし、これらの方針（ISMS 基本方針、情報セキュリティ基本方針）を物理的にひとつの文書に記載することも可能です。

個人情報保護法との関係を見ると、個人情報取扱事業者である組織の ISMS が、適用範囲内に個人情報や個人データ、保有個人データを含むときは、個人情報保護法をはじめとする個人情報の取扱いや保護に関する重要な法令等に準拠する必要があるのは当然ですが、特に組織がその ISMS を個人情報保護のために機能させていることを明確にするために、基本方針において個人情報保護法への準拠を宣言することは意味あることです。基本方針の作り方によっては、その中で個人情報保護法にもとづく「個人情報の保護に関する基本方針(平成１６年４月閣議決定)」や各省ガイドラインで求められている個人情報保護に関するポリシー、ステートメント(基本方針、宣言)を行うことも可能でしょう。

ISMS 認証基準で要求される ISMS の基本方針の策定手順をまとめると図 7-3 の様になります。

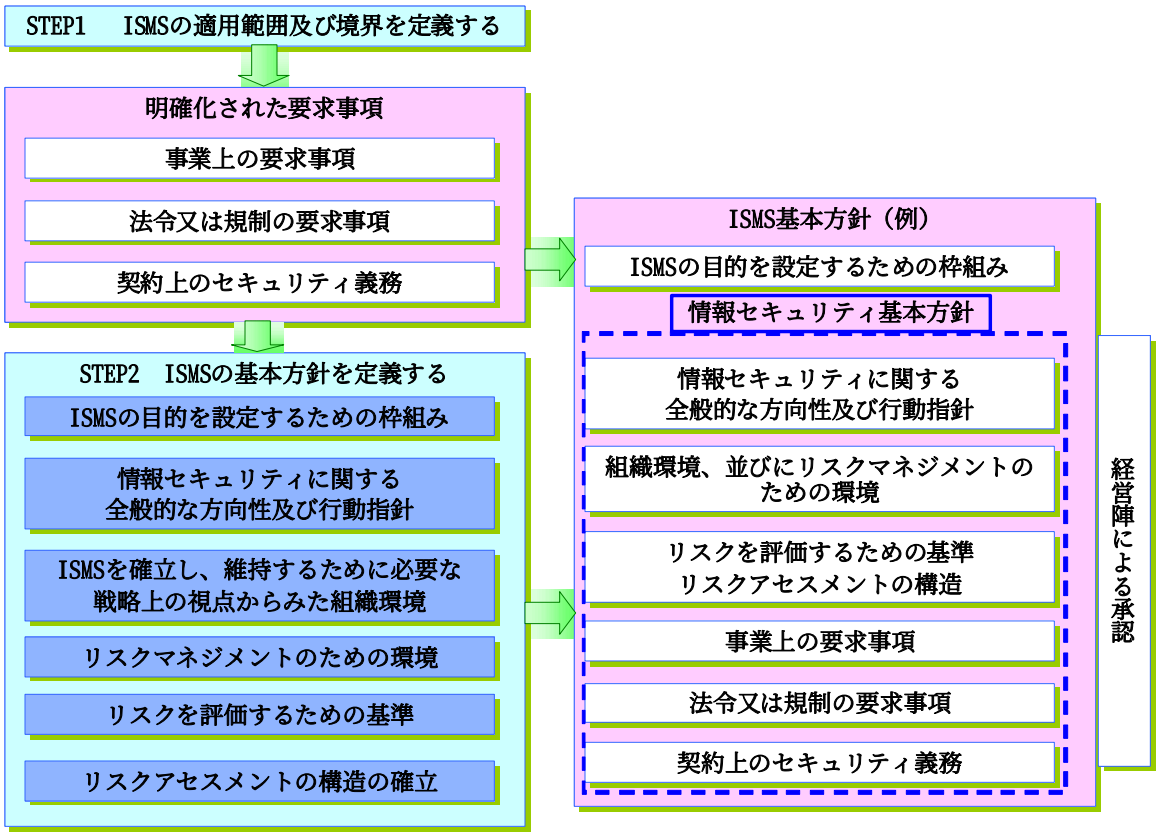


図 7-3　ISMS の基本方針の策定手順

ISMS 認証基準では、ISMS の基本方針の策定の手順を以下のように規定しています。

> 4.2.1 ISMS の確立
> b) ISMS 基本方針を，事業・組織・所在地・資産・技術の特徴の見地から，次を満たすように定義する。
> 1) 目的を設定するための枠組みを含め，また，情報セキュリティに関係する活動の方向性の全般的認識及び原則を確立する。
> 2) 事業上及び法令又は規制の要求事項，並びに契約上のセキュリティ義務を考慮する。
> 3) それのもとで ISMS の確立及び維持をする，組織の戦略的なリスクマネジメントの状況と調和をとる。
> 4) リスクを評価するに当たっての基軸を確立する[4 2.1 c)参照]。
> 5) 経営陣による承認を得る。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

上記要求事項の 1)～5)は、ISMS の基本方針の策定手順の観点から大別すると 3 つのポイントに絞り込むことができます。表 7-4 は、3 つのポイントをまとめたものです。

表 7-4　ISMS 基本方針の策定手順のポイント

	ポイント	要求事項
(1)	ISMS の基本方針の確立	1) 情報セキュリティに関係する活動の方向性の全般的認識及び原則を確立する。
(2)	ISMS 構築のための組織体制	2) 事業上及び法令又は規制の要求事項、並びに契　　約上のセキュリティ義務を考慮する。 3) 組織の戦略的なリスクマネジメントの状況と調和をとる。 4) リスクを評価するための基軸を確立する。
(3)	経営陣の承認	5) 経営陣による承認を得る。

（1）ISMS 基本方針の確立

ISMS 基本方針を策定するためには、適用範囲に適用される法令及び規制の要求事項並びに契約上のセキュリティ義務、及び適用範囲に含まれる組織の人員構成、規程類の整備状況、資産の保有状況、情報システムの利用状況等、広範に資産とそれを取り巻く環境を確認する必要があります。その上で、ISMS 基本方針では、大別すると以下に関連する記載が必要です。

- リスクマネジメント全般（CSR、雇用、財務、事業継続、安全、内部統制等）における情報セキュリティマネジメント（ISMS）の位置づけ
- ISMS の目的、枠組み、また情報セキュリティに関係する活動の方向性（指針）と行動の諸原則

但し、上記の 2 番目の項目を情報セキュリティ基本方針として記載することも可能です。

具体的には、図 7-4 に示すような資料調査やインタビュー調査を組み合わせて調査を実施します。

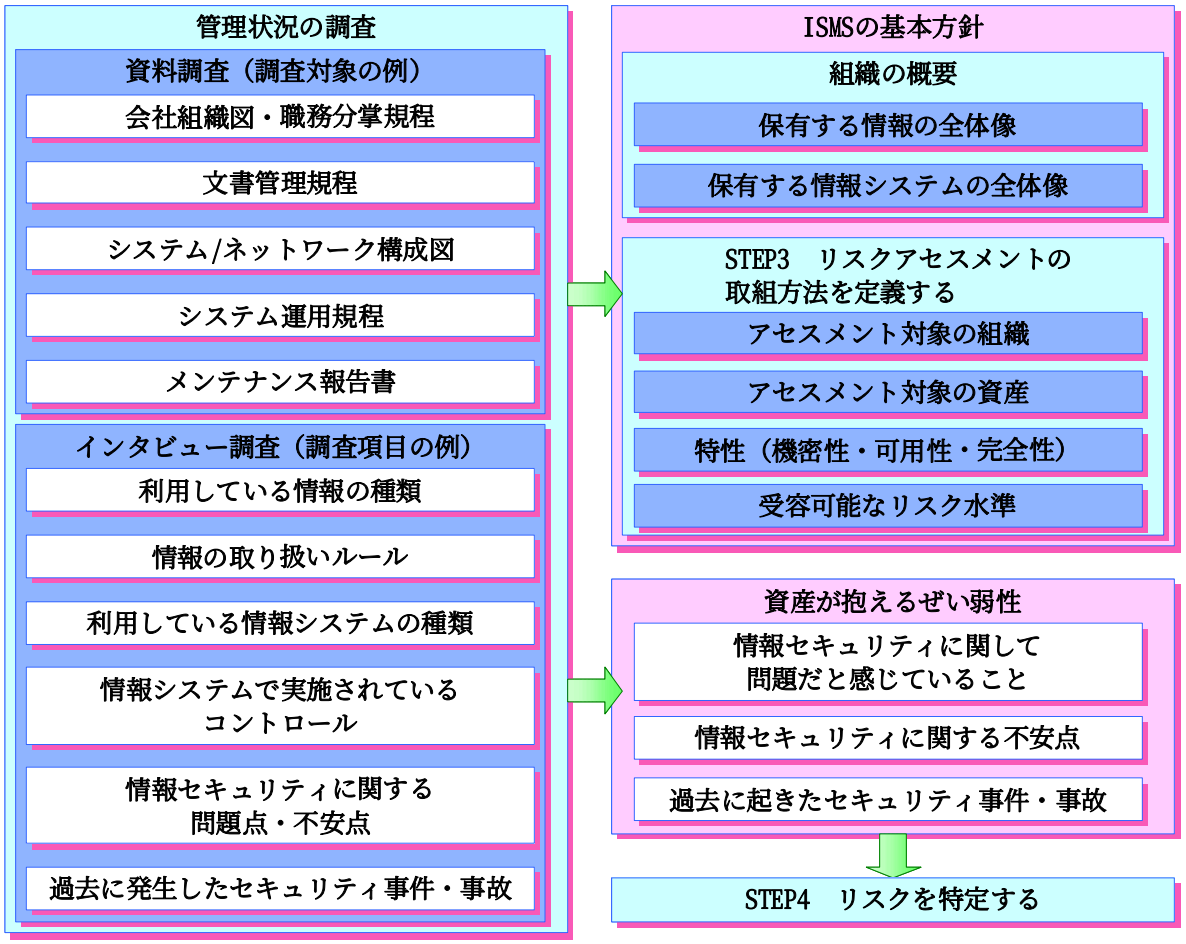


図 7-4　ISMS 基本方針の策定

調査結果は、ISMS 基本方針の内容に反映されるだけではなく、STEP3 以降に実施するリスクアセスメントにおいて使用する判断基準を決定する際の基礎的な情報となります。

「1)目的を設定するための枠組みを含め、また、情報セキュリティに関係する活動の方向性の全般認識及び原則を確立する。」とは、策定する ISMS の基本方針の内容を規定する要求事項といえます。

JIS Q 27002：2006 の「5.1.1　情報セキュリティ基本方針文書」には、基本方針に含まれる事が望ましい内容が以下のように規定されていますので参考にして下さい。

実施の手引

情報セキュリティ基本方針文書では，経営陣の責任を明記し，情報セキュリティの管理に対する組織の取組み方を示すことが望ましい。この情報セキュリティ基本方針文書には，次の事項に関する記述を含むことが望ましい。

a) 情報セキュリティの定義，その目的及び適用範囲，並びに情報共有を可能にする基盤としてのセキュリティの重要性（0.2 参照）
b) 事業戦略及び事業目的に沿った情報セキュリティの目標及び原則を支持する経営陣の意向の記述
c) リスクアセスメント及びリスクマネジメントの構造を含む，管理目的及び管理策を設定するための枠組み
d) 組織にとって特に重要な，セキュリティの個別方針，原則，標準類及び順守の要求事項の簡潔な説明。これらには，次のようなものがある。
    1) 法令，規制及び契約上の要求事項の順守
    2) セキュリティ教育，訓練及び意識向上に関する要求事項
    3) 事業継続管理
    4) 情報セキュリティ基本方針違反に対する処置
e) 情報セキュリティインシデントを報告することも含め，情報セキュリティマネジメントに関する一般的な責任及び特定の責任の定義
f) 情報セキュリティ基本方針を支持する文書（例えば，特定の情報システムのためのより詳細なセキュリティ方針及び手順，又は利用者が順守することが望ましいセキュリティ規則）への参照

この情報セキュリティ基本方針は，想定する読者にとって，適切で，利用可能で，かつ，理解しやすい形で，組織全体にわたって利用者に知らせることが望ましい。

（JIS Q 27002：2006　5.1.1 情報セキュリティ基本方針文書　より引用）

これらの事項は、例示であり、必ずしもその全てが策定する基本方針に含まれる必要はありません。前のステップで定義した適用範囲により内容が変わることも想定されま

す。

JIS Q 27002：2006 で規定された内容は、基本方針の内容を検討する際に考慮すべきポイントとして理解して下さい。

（2）ISMS 構築のための組織体制を確立する

「2) 事業上及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮する。」また「3) 組織の戦略的なリスクマネジメントの状況と調和をとる。」、「4)リスクを評価するための基軸を確立する。」とは ISMS の構築を担当する組織に求められる機能に関する要求事項です。

ISMS を構築する組織の人選においては、様々な情報の取り扱いに関する問題を討議するのに必要かつ十分な範囲から人を召集すると同時に、実際の ISMS 運用の体制についても考慮し、関連部門から広くメンバーを募るべきです。

ISMS で取り扱う情報セキュリティとは、単に「情報リスク」、「IT リスク」を考慮することにとどまりません。また、マネジメントシステムの局面も、日常の管理に属する部分の他、リスクが顕在化した後の被害を最小限にとどめるための対応なども要求されています。このような網羅的な「管理」を実現するためには、認証取得範囲に含まれる現場組織だけではなく、法務部門、総務部門など会社組織全体を横断する人材の登用が求められます。

図 7-5 は、「ISMS ガイド」に紹介された ISMS 構築のための組織体制の一例です。

この例を基に、主要な組織の役割と責任を紹介します。

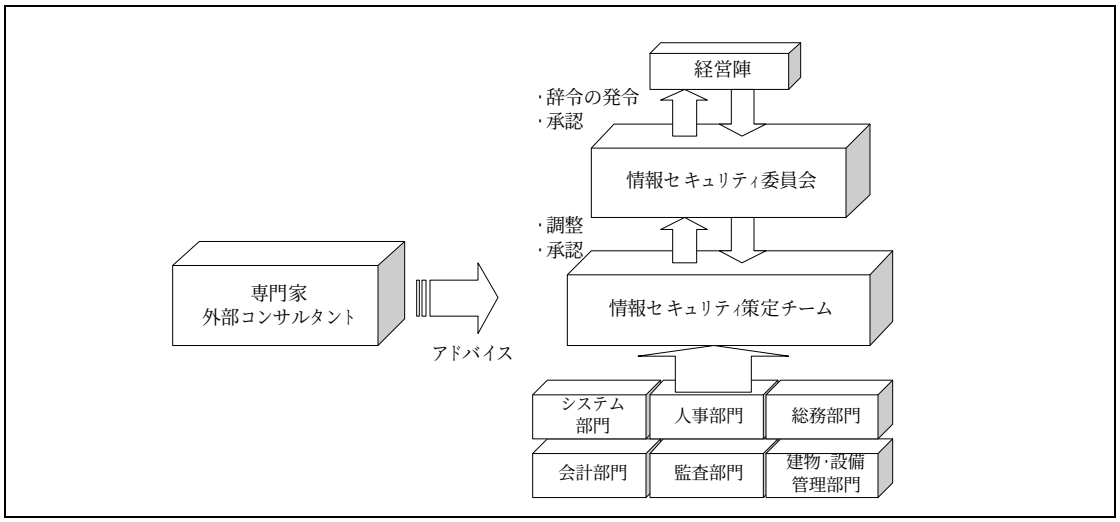


図 7-5　ISMS 構築のための組織体制

① 情報セキュリティ委員会の役割

情報セキュリティ委員会を中心とした体制で策定される ISMS 関連文書は、委員会だけでなく組織の経営陣により承認された規程として必要に応じて関係者に周知し、定期的に見直しを行います。

この委員会は、組織の保有する資産の取り扱いに責任を持ち、情報セキュリティの方向性を提言できるだけの情報セキュリティに関する理解と実行力をもった組織であるべきです。

情報セキュリティ委員会は、組織において ISMS の中心的役割を負います。以下は情報セキュリティ委員会の役割の例示です。

- **リスクマネジメントのための環境整備について検討機関となる**
- **ISMS 関連文書の策定時には内容について実質的な決定機関となる**
- **導入段階の ISMS を推進する各種施策や改訂を検討する**
- **運用段階でセキュリティ問題等が発生した場合の検討機関となる**
- **ISMS 運営の評価結果に基づいた改善について検討機関となる**

② 情報セキュリティ策定チームの役割

ISMS の構築実務を担当する策定チームは、適用範囲内の重要な資産について広く現状を把握し、その取り扱いを検討するのに十分な知見を持つメンバーで構成されるべきです。例えば、資産の取り扱い方法の決定に当り、適用範囲内の部署間での見解の相違や、利害関係の調整が必要になる場合があり、策定チームはそのような摩擦の調整役として、部門間の枠をこえて当事者に対してうまく働きかけることが求められます。この場合は、高いセキュリティ知識も当然必要ですが、調整能力や経験に基づくコミュニケーションのスキルも重要になります。

③ 専門家・外部コンサルタント

ISMS の構築作業は、組織が自前で（できれば専任の）要員を確保した上で進めるべきです。しかし、「情報セキュリティ」の対象とする範囲は「IT 技術」、「経営的な判断」や「ビジネスへの理解」など、求められる知識や経験は多岐にわたり、これらの領域をバランスよく俯瞰的に見通す力量が求められます。

組織の主要な業務はその業務に携わっている人が一番知っているものですが、時としてミクロな視点での判断に終始してしまうことがあります。基準に言及されている「外部の専門家・コンサルタントの登用」は、この判断にマクロな視点を与え、また最新の情報を提供してくれる窓口の機能が期待されます。情報セキュリティ委員会へのオブザ

ーバ参加、規定文書のレビューや監査計画策定など、必要な局面で彼らの持つ専門知識を効果的に活用することも良いと思います。しかし、外部の専門家やコンサルタントはあくまでも ISMS の構築支援を行うものであり、当事者ではないので、意思決定を含めた丸投げは避けなければなりません。

上記の例は、ISMS 構築のための組織体制として、役立つものではありますが、情報セキュリティ委員会、外部コンサルタント等の固有名詞にこだわる必要はありません。これらの機能をもつ、「内部組織」を策定し、「情報セキュリティの調整」、「専門組織との連絡」が行なわれることが重要です。(JIS Q 27002:2006　「6.1 内部組織」、「6.1.2　情報セキュリティの調整」、「6.1.6　関係当局との連絡」、「6.1.7　専門組織との連絡」等を参照してください。)

(3)　経営陣の承認

経営陣には、「情報セキュリティ基本方針」を含む ISMS 基本方針、つまり情報セキュリティに対する組織のビジョンを示し、ISMS の活動に対する支援についてコミットメントすることが求められています。コミットするということは、単に出来上がった「情報セキュリティ基本方針書」に承認印を押す事でありません。詳細は、本ガイドの「8.1 経営陣のコミットメント」を参照して下さい。

「5)経営陣による承認を得る。」という要求事項では、ISMS の構築に対する経営陣のコミットメントの証拠として、情報セキュリティ基本方針の確立をあげています。

情報セキュリティに対する組織の取り組み姿勢の定着に経営陣が積極的に関与し、その責任の下に継続的な改善を行なうことより、情報セキュリティは組織文化として定着します。

情報セキュリティについての意識が浸透している組織では、突発的な事態に対して要員が経営陣の意図する行動を自然に取ることが期待されます。これは、めまぐるしく変化する環境においては非常に重要なポイントです。

事業環境の変化の激しい組織における型にはまった手順書は、更新に時間がかかり、常に実業務との整合性を確保することに多大な労力を要することがあります。

そのような場合にも、情報セキュリティの意識を組織文化として浸透させる活動を実施すれば、規模が大きく業種や業態が多岐にわたる組織でも要員が等しく安全な行動をとるようになります。

7.2.3　STEP3　リスクアセスメントの取組み方法を定義する

前述までで、「ISMS を適用する範囲の定義」と「ISMS を確立するための基本方針の定義」

を説明しました。STEP3 では ISMS 構築に必要なリスクアセスメントを実施する前の準備として、リスクアセスメント手順や判断基準を明確にする、ということを説明します。その上で「STEP4　リスクの特定」で資産とそのリスクを洗い出し、「STEP5　リスクを分析し評価する」で洗い出したリスクの大きさを分析し、「STEP6　リスク対応」で各リスクへの取るべき対策を決定する、という流れで進みます。

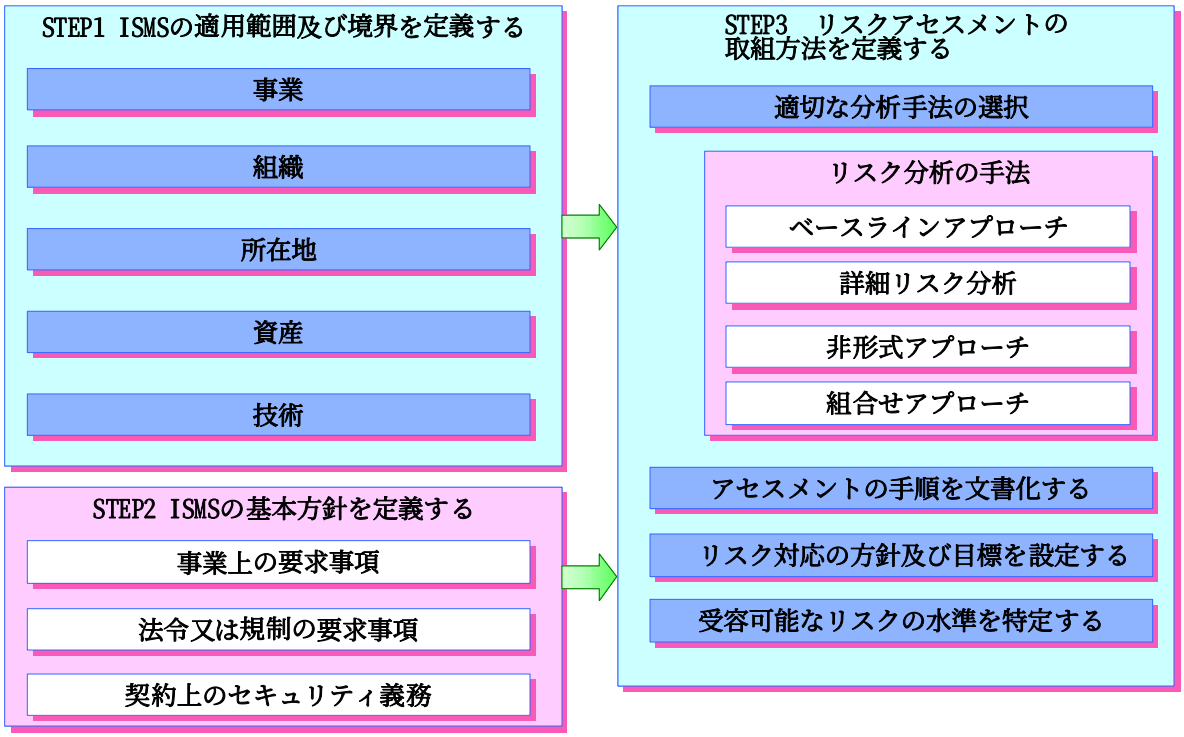


図 7-6　リスクアセスメントの取組方法の定義

７.２.３.１ リスクアセスメント

リスクアセスメントとは、識別された資産に対するリスクを識別し、それらの大きさを手順に従い決定することです。

> 3.12 リスクアセスメント（risk assessment）
> リスク分析からリスク評価までのすべてのプロセス（TR Q 0008:2003）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

リスクアセスメントでは組織が保有する資産を対象に以下の事項を把握します。

- どのような脅威が存在するのか

- その脅威はどの程度発生する可能性があると考えるか
- 脅威が顕在化したときにどの程度の影響を受けるか

リスクアセスメントでは、「リスク分析」を実施し算定されたリスクについて「リスク評価」を行います。

表 7-5　リスク分析とリスク評価

3.12 リスクアセスメント（risk assessment）	3.11 リスク分析（risk analysis）
	3.13 リスク評価（risk evaluation）

ISMS 認証基準では、リスク分析とリスク評価についてそれぞれ以下のように規定しています。

> 3.11 リスク分析（risk analysis）リスク因子を特定するための，及びリスクを算定するための情報の系統的使用（TR Q 0008:2003）。
> 3.13 リスク評価（risk evaluation）リスクの重大さを決定するために，算定されたリスクを与えられたリスク基準と比較するプロセス（TR Q 0008:2003）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

7.2.3.2 リスクアセスメントについての体系的な取組方法の確立

ISMS 認証基準では、リスクアセスメント手順や判断基準を明確にすることを、「組織の取組み方」として以下の様に規定しています。

> c) リスクアセスメントに対する組織の取組み方を，次を満たすように定義する。
> 1) ISMS，特定された事業上の情報セキュリティ要求事項，並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法を特定する。
> 2) リスク受容基準を設定し，またリスクの受容可能レベルを特定する［5 1.f) 参照］。
> 選択するリスクアセスメントの方法は，それを用いたリスクアセスメントが，比較可能で，かつ，再現可能な結果を生み出すことを確実にしなければならない。
>
> （JIS Q 27001:2006　4.2.1 ISMS の確立　より引用）

組織に偏在する多岐にわたる資産のリスクアセスメントを、複数の担当者で実施する上では特に必要な活動です。

リスクアセスメントの体系的な取組み方法の確立では

① 適切な分析手法の選択
② アセスメントの手順を文書化する
③ リスク対応の方針及び目標を設定する
④ 受容可能なリスクの水準を特定する

を行います。

（1）適切な分析手法の選択

リスクアセスメントには様々な手法があります。個々の手法には特徴があり、メリット、デメリットがあります。よって、手法の種類とそれらの長所・短所を知り、その上で組織の特徴に合わせてリスクアセスメント手法を選択する必要があります。

図 7-7 は GMITS「IT セキュリティマネジメントのための手法」に記載されているもので、セキュリティマネジメントを説明したものです。

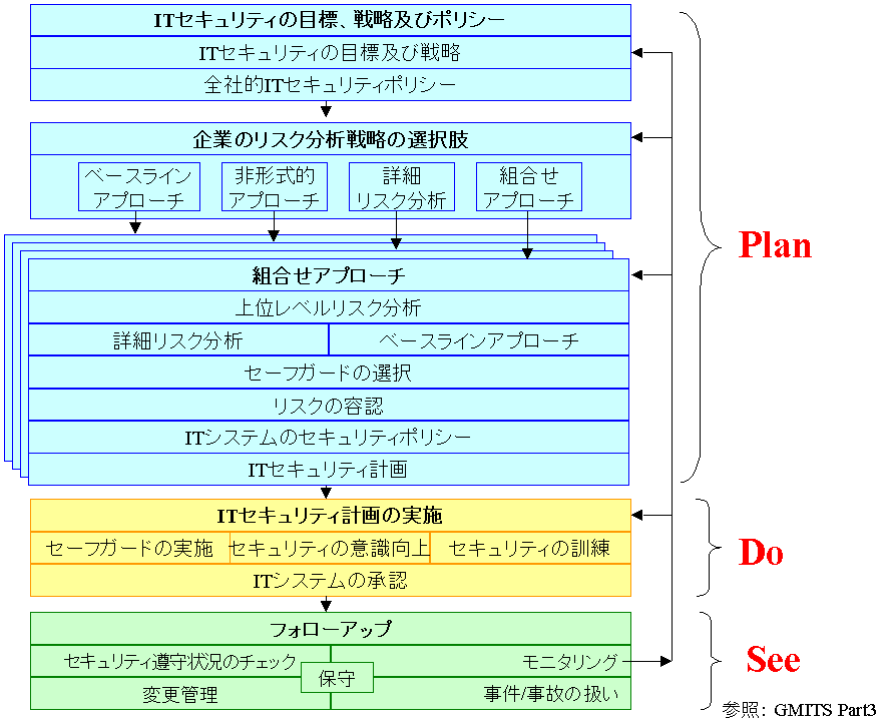


図 7-7　セキュリティマネジメント

ここでは、リスクアセスメントの方法として 4 つのアプローチを紹介します。

■　ベースラインアプローチ（Baseline　Approach）

一般的な情報セキュリティに関する基準や、業種・業界で採用されている標準やガイドラインなどを参照し、リスク評価することなくセキュリティ対策を実施しま

す。

【特徴】

簡便であるため、リスクアセスメントにかかる時間と費用を削減できるが、組織によってはガイドラインとのバランスが合わないこともあります。

■ 詳細リスク分析（Detail Risk Analysis）

資産の機密性、完全性又は可用性の喪失による潜在的な影響と、脅威及びぜい弱性の観点から起こりうるセキュリティ障害などを現在実施されている管理策を考慮した現実的な発生可能性からリスクを評価します。

【特徴】

厳密なリスク評価が行えるため、リスクに応じた適切な管理策を効率的に選択できるが、リスクアセスメントには時間と費用がかかります。

■ 組合せアプローチ（Combined Approach）

一般には、ベースラインアプローチと詳細リスク分析を組合せる手法です。

【特徴】

それぞれの手法の長所と短所を相互に補完するアプローチですが、重要な資産の特定に失敗すると組合せアプローチのメリットを生かせなくなります。

■ 非形式的アプローチ（Informal Approach）

組織や担当者の経験や判断によってリスクを評価する手法です。

【特徴】

改めて技術を習得することなくリスクの評価ができる反面、方法が構造化されていないために、漏れや見落としの可能性があります。

① ベースラインアプローチ

ベースラインアプローチとは、後述する詳細リスク分析とは異なり、資産ごとにリスクそのものを評価しません。

一般の情報セキュリティに関する基準や、業種・業界で採用されている標準やガイドラインなどを参照し、組織全体で共通のセキュリティ対策を実施します。実現可能な水準の管理策を採用し、組織全体でセキュリティ対策に抜け漏れが無いように補強していくアプローチです。

ベースラインアプローチは、大きく分けると以下の 2 つの手順で実施されます。

- **ベースラインの決定**
- **ギャップ分析の実施**

ベースラインアプローチでは、組織の達成する情報セキュリティ管理について独自の「対策の標準」を作成します。一般に、この対策の標準のことを「ベースライン」と呼びます。

しかし、ISMS 認証基準は、情報セキュリティマネジメントシステムに関する規格として一定の管理の枠組みが簡潔に規定されています。
実際に採用すべき管理策について余り詳細な記述が無く、採用する管理策についてもう少し詳細な情報がほしいと感じる時には、先ず JIS Q 27002:2006 を参照して下さい。特に新たに採用する管理策については、JIS Q 27002:2006 を精査して下さい。

本書の巻末に掲載している「参考文献」の一覧にも、ベースラインに採用すべきコントロールの例として参照可能な法律、ガイドライン、報告書、文献などが収集され、活用可能な内容となっています。

また、上記以外にも有用な情報源が入手できる機会があると思います。今後策定されるであろう情報セキュリティに関する基準、制度や、外部コンサルタントから提供されるノウハウなどです。実際にどのようなコントロールを導入するのか、「出来る、出来ない」の判断をする前に広く管理策についての情報を収集し、組織が要求する情報セキュリティの管理水準が、達成可能なベースラインであるかを検討して下さい。

次に、ギャップ分析について説明します。

ギャップ分析実施の目的は、組織の定める基準への準拠状況の把握にあります。
基準で要求される管理のレベルと事業者の管理レベルの現状を比較し「大きな差が認められる個所」、「明らかに管理策の適用を必要としている個所」、「過度に管理策が適用されている個所」等を確認します。
図 7-8 は、それぞれの資産を対象に、現状の対策の度合いと組織によって定められる「要求される保証の度合い」との乖離を示しています。図 7-8 の要求される保証の度合いはひとつの平面として表現されていますが、本来、要求される保証の度合いは一律ではなく、資産の属性や性質、組織における重要度により資産ごとに決定されます。

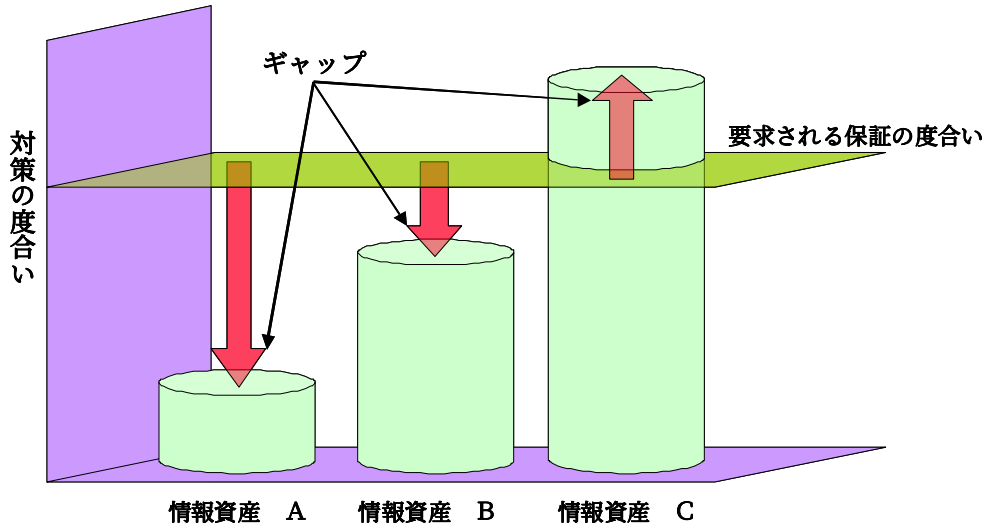


図 7-8　要求される保証の度合い

②　詳細リスク分析

詳細リスク分析では、資産ごとの関連するリスクの識別を個別に実施します。(図 7-9 参照)。

リスクが顕在化する頻度は、脅威が発生する（顕在化する）可能性、管理上の弱点につけ込まれる可能性（ぜい弱性）の他に、資産が攻撃者から見てどれほど魅力的なものであるのか等にも依存します。

まずリスク分析の対象範囲の定義付けをしなければなりません。プロセスが密接に絡み合っているにも関わらず、安易に範囲を狭め、慎重な定義付けを怠ると、後に不必要な作業が増えたり、抜けが見られたりすることに繋がるからです。

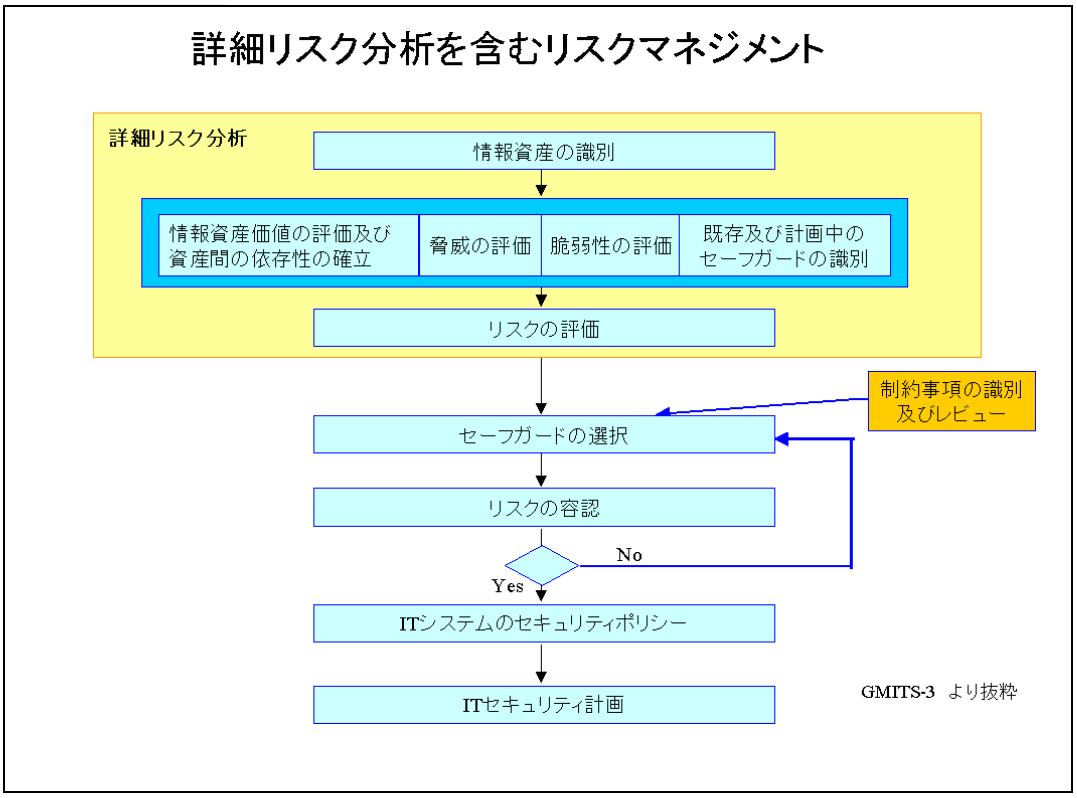


図 7-9　詳細リスク分析を含むリスクマネジメント

③　組合せアプローチ

一般には、ベースラインアプローチと詳細リスク分析を併用する組合せアプローチを採用することが効率的であると紹介されています。

どのような場合にどのアプローチを採用するかは一概には決定できません。適切なアプローチの採用のための判断材料は、資産に求められるセキュリティ要求事項（前述の事業上の要求事項、法令又は規制の要求事項、契約上のセキュリティ義務など）に依存します。組合せアプローチには、それぞれの資産を取り巻くリスク環境を確認し、適切なリスク分析のアプローチを採用し、それぞれのアプローチの弱点を相互に補完し合うことにより、ISMS 適用範囲全体のリスク分析を効率的に実施する目的があります。「ベースラインアプローチ」のみでは、高い水準でセキュリティ対策が実装されるべきリスクの高いシステムについて対応策が不充分になる可能性があること、また、「詳細リスク分析」をすべてのシステムに適応することは効率的な観点から現実的でないことが大きな理由です。

図 7-10 は、前述の GMITS で定義されている組合せアプローチの例です。

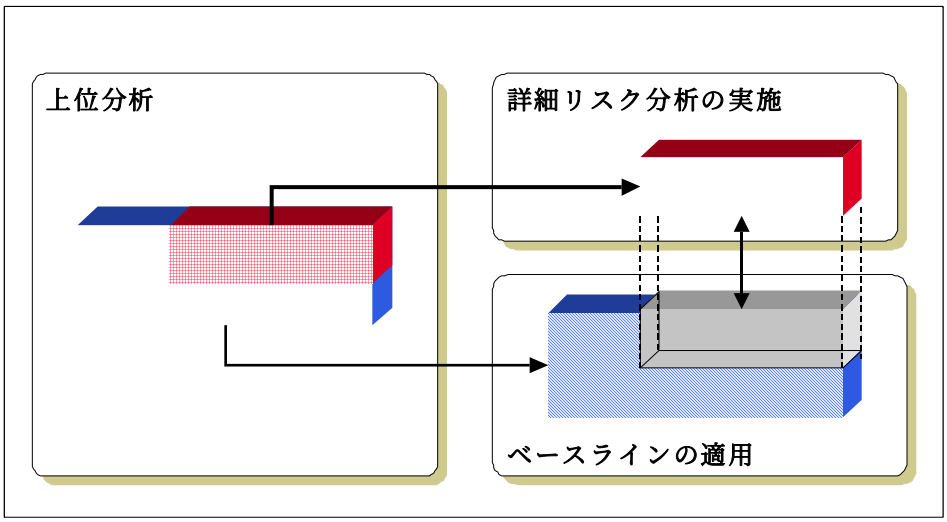


図 7-10　組合せアプローチ

④　非形式的アプローチ

非形式的アプローチは、ここまで説明をしてきたリスク分析と異なり体系的なアプローチをとりません。この手法は主に現場担当者の長年にわたり培われた経験、知見に基づいてリスク因子の特定や対策の選択を実施します。

このアプローチは、分析を実施する際に手法について新たに学習すべき事項も少なく迅速に作業に着手できます。また、詳細な分析を実施する場合に比べ投入する人的資源や時間が少なくて済みます。

一般にリスクの分析や評価の作業において、客観性がもっとも重視される事項です。このアプローチは担当者の特定の考え方に結果が影響される可能性があることは明らかです。しかし、体系的なリスク分析が実施できない場合などに対象を限定し、次項で説明する点に留意し、他のアプローチと組み合わせて実施することは有用です。

⑤ 留意事項

ISMS の構築の初期にある組織では、ここまで説明をしてきたリスク分析の体系的なアプローチを採用しても表 7-6 のような問題に直面することがあります。

表 7-6　リスク分析の留意事項

現状	問題点
資産の管理責任が不明確	詳細リスク分析を実施しても、資産の 重要度や取り扱い範囲が特定できない
リスク判断の基準が未整備	資産の価値を客観的に判断できない リスク管理の水準が属人的に偏る
セキュリティインシデントの事例収集が不十分	脅威・ぜい弱性を定量的に扱えない 対策が不適切になる（不足・過度になる）

組織の ISMS が未成熟の場合、要員の不足、周知・教育の不徹底、規程文書や記録の不備などにより円滑に運営できないことも想定されます。ISMS 適用範囲の一部に非形式的アプローチを採用し、担当者の経験に基づいて緊急性の高い対策の実施を優先することも考えられます。そのような場合には、先に述べた問題点に留意し、速やかに他の手法を用いて網羅的なリスク分析を実施することが望まれます。

⑥ 法的リスクアセスメントの留意事項

①から⑤では、リスクアセスメントの適切な分析手法としてベースラインアプローチ以下４つのリスクアセスメントの方法を紹介し、図 7-7 ではそれらがセキュリティマネジメント構造の中でどのような位置にあるのかを説明しました。

法的リスクアセスメントも、評価の基準と評価の対象、対処方針や対処策のありかたに応じてこれらを組み合わせて行われます。

組織の情報資産又はその設計(仕様、運用、保守設計を含みます)が「重要な法令及び規制の要求事項」に合致しているかどうかを評価するときは、ベースラインアプローチに類した方法が適切でしょう。ただし、その際に用いる評価の基準は、これら「重要な法令及び規制の要求事項」であって、組織が作成した「独自の」「対策の標準」ではありません。ここは、これを自らが定めるとするベースラインアプローチとは異なるところです。この方法で評価したところ、組織の情報資産又はその設計(仕様、運用、保守設計を含みます)が「重要な法令及び規制の要求事項」に反するときは、その組織の経営は順法性を著しく欠くため、ISMS の適合性評価に至る前に違法状態を回避する必要があるでしょう。

なお、組織の情報資産又はその設計(仕様、運用、保守設計を含みます)が「重要な法令及び規制の要求事項」に反するときは、リスクの受容、低減、転嫁は許されませんから、要求される保証の度合いとの乖離を測定して、対処方針や対処策の選択に資するギャップ分析は適切ではありません。

しかし、組織の情報資産又はその設計(仕様、運用、保守設計を含みます)が「重要な法令及び規制の要求事項」に合致していることが確認できた後は、その運用・保守に関する脅威の発生可能性、ぜい弱性などを詳細に見ることによって対処方針や対処策の選択を合理的に行う必要があります。その際は、ギャップ分析や詳細リスク分析、その組合わせアプローチのほうが、ベースラインアプローチよりも対処方針や対処策の選択に多くの資料を提供することでしょう。また、組織の情報資産を「重要な法令及び規制の要求事項」とまでは言えないものの、ISMS の構築にあたり選択すべき評価基準に基づいて評価した際のリスクを分析するときも、これらの分析手法が役立つでしょう。

表 7-6 では ISMS の構築初期にある組織の留意事項を掲げていますが、法的リスクアセスメントでも同様のことが言えます。特に、個人情報保護法などのように裁判例や学説の固まっていない法令などは、同ガイドの「リスク判断の基準が未整備」「セキュリティ事件・事故の事例収集が不十分」な状態にあるといえるでしょう。こうした場合には、要員の準備、周知・教育の不徹底など、組織の ISMS が未成熟な場合と同様の事態が想定されます。こうした場合には非形式アプローチの採用などにより権利者への対応や緊急対策を実施することも考えられ、その際には、次第に網羅的なリスク分析に進むというアプローチが望まれます。

（2） アセスメントの手順を文書化する

リスクアセスメントには、作業を実施するために必要な手順が文書化されている必要があります。

- **リスクアセスメントの定義**
- **リスクアセスメントの目的**
- **リスクアセスメントの方法**

また、上記の「リスクアセスメントの方法」には、以下のような判断の基準等が含まれます。

- **資産の価値判断の基準**
- **脅威の評価基準**
- **ぜい弱性の評価基準**

- **リスク値の算出方法**
- **リスクアセスメントを行う頻度**

これらの文書策定は、リスクアセスメントが比較可能で、かつ、再現可能な結果を生み出すために確実に行なう必要があります。このことは、仮にリスクアセスメントの方法を変更した場合でも、その変更を管理し、必要に応じてリスクアセスメントの結果の比較が可能な状態にしておくことを含みます。

法的リスクアセスメントにあたっても、作業を実施するために必要な手順が文書化される必要があります。

（3）リスク対応の方針及び目標を設定する

組織は、リスクアセスメントを実施し算出されたリスク値に基づいてリスク対応を実施します。

このステップでは、算出されたリスク値に基づきリスクマネジメントの枠組みの中でどのような対応を取るのかの選択肢を明らかにします。

組織は、リスクアセスメントの結果にもとづいて、リスク対応の方針を決定します。ただ、法的リスクアセスメントの場合は、リスクアセスメントの結果、組織の情報資産又はその設計(仕様、運用、保守設計を含みます)が「重要な法令及び規制の要求事項」に合致していないことが確認されたときには、直ちにこれを合致させるための是正を行うことになります。

処理方針及び目標の設定が必要となるのは、それ以外の場合、すなわち、対象が情報資産の運用・保守であるときや、評価基準が「重要な法令及び規制の要求事項」とまではいえない時です。

リスク対応の選択肢については、前述の TR Q 0008 に以下の 4 つが紹介されています。

- **リスクの回避**
- **リスクの最適化**
- **リスクの移転**
- **リスクの保有**

（注記）「リスクの最適化」、「リスクの保有」、「リスクの移転」は、JIS Q 27001:2006 では、「適切な管理策の適用」、「組織の方針及びリスク受容基準を明確に満たすリスクの、意識的、かつ客観的な受容」、「関連する事業上のリスクの、他者（例えば、保険業者、供給者）への移転」（4.2.1 f）参照）といいます。

「リスク対応」の内容については、7.2.6で詳細に説明します。

ここで決定したリスク対応の選択肢も、文書化しISMS文書に含めることが要求されています。

（4）受容可能なリスクの水準を特定する

ここでいう「受容可能なリスク」とは、組織として保有すること（「リスク保有」）が可能なリスクです。特に「受容」という言葉には、組織においてリスクを保有する積極的な「意思」が発生します。

> 3.10 リスクの受容（risk acceptance）
> リスクを受容する意思決定（TR Q 0008:2003）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

本来、リスクの受容可能な水準は、リスクアセスメントを実施しその結果に基づいて決定します。

ISMS認証基準に規定されているこのステップでは、（2）で文書化したリスクアセスメントの手順に従って算出したリスク値を用いてリスク評価を実施するかを明らかにし、リスク受容の意思決定の手順の確認を行います。

法的リスクアセスメントにおいては、組織が保有することが可能なリスクの特定は、情報資産の運用・保守を対象とするときや「重要な法令及び規制の要求事項」とまではいえないものの、ISMSの構築にあたり選択すべき評価基準を用いるときに限って行われ、組織の情報資産又はその設計(仕様、運用、保守設計を含みます)が「重要な法令及び規制の要求事項」に合致していないことが確認されたときには、リスクアセスメントの作業を一時中断してでも対応することが必要です。

７．２．４　STEP4　リスクを特定する

リスクアセスメントは、まず「リスクを特定する」ことから始めます。単にリスクを特定するといっても、リスクそのものは手に取って認識することは出来ません。

本来、リスクは様々なリスク因子の因果関係により成り立っています。図 7-11 は、GMITS においてリスクとリスク因子の関係を示したもので、リスク値がそれを取り巻く「資産価値」、「脅威」、「ぜい弱性」により決定されることが表現されています。

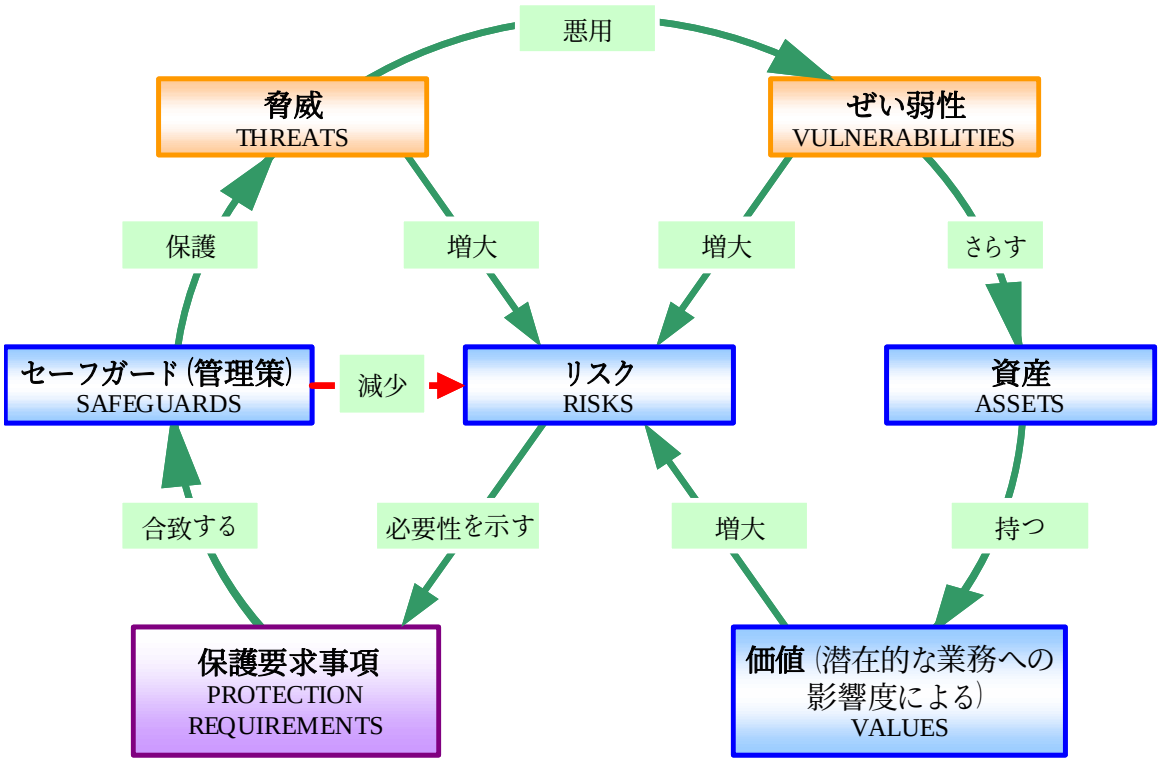


図 7-11　リスクとリスク因子の因果関係

リスクの特定では、具体的には以下の 2 つの作業が実施されます。

- **資産の洗い出し**
- **脅威・ぜい弱性の明確化**

以下、それぞれの内容について例示を用いて紹介します。

（1）資産の洗い出し

ここでは、組織の ISMS 適用範囲における資産の保有状況を確認します。ISMS の管理対象の詳細を把握し、適切な管理策を選択するためには、各々の資産の属性や価値を明確にすることが理想です。また ISMS 認証基準では、資産の洗い出しにおいて、それぞれの「資産の管理責任者」を特定することが求められています。

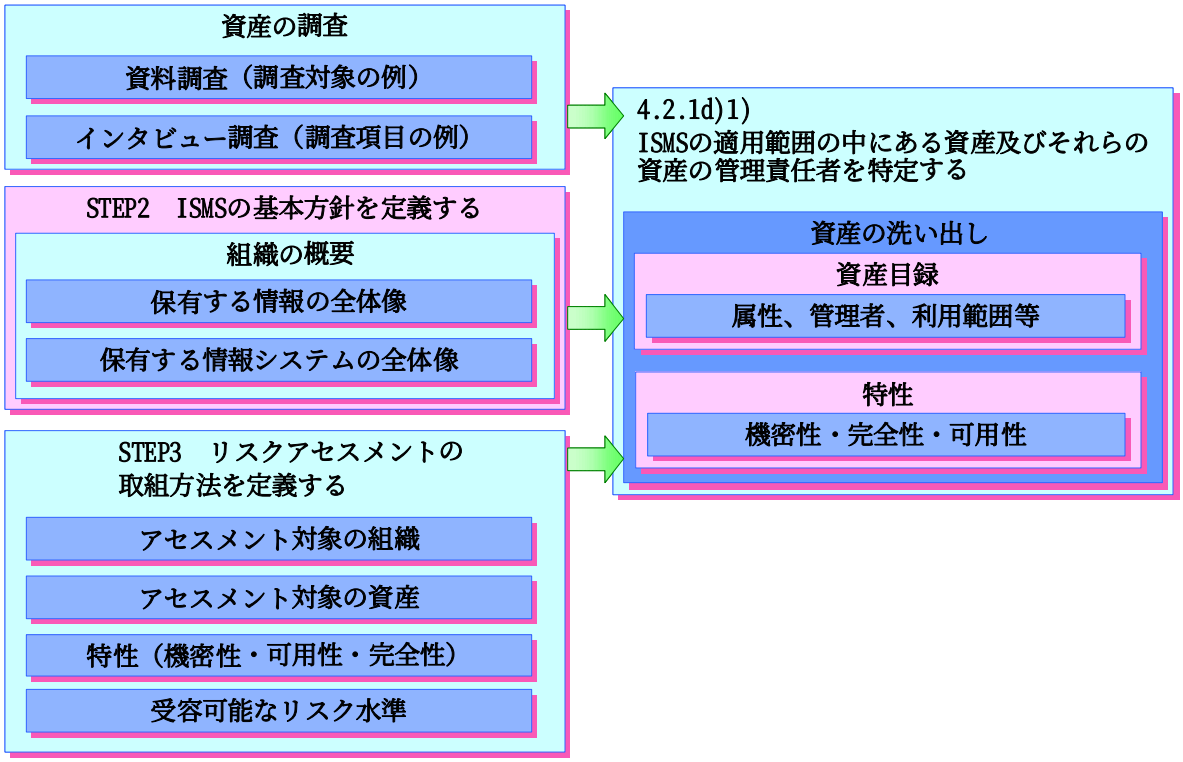


図 7-12　資産の洗い出し

①　資産目録の作成

「資産目録」を作成することは、JIS Q 27002:2006 では、「7.1.1　資産目録」という項目で推奨しています。

実施の手引 組織は，すべての資産を識別し，それら資産の重要度を記録することが望ましい。資産目録には，資産の種類，形式，所在，バックアップ情報，ライセンス情報及び業務上の価値を含め，災害から復旧するために必要なすべての情報を記載することが望ましい。目録は，他の目録と不必要に重複しないことが望ましく，その記載内容が他の目録と整合していることを確実にすることが望ましい。 さらに，各々の資産の管理責任者（7.1.2 参照）及び情報の分類（7.2 参照）について合意し文書化す

ることが望ましい。資産の重要度に応じた保護のレベルは，資産の重要度，業務上の価値及びセキュリティ上の分類に基づいて決めることが望ましい（資産の重要度を表すための評価手法については，TR X 0036-3 参照）。

（JIS Q 27002:2006　7.1.1 資産目録　より引用）

洗い出しの結果、資産目録に書き込む情報として以下の内容を参考に検討して下さい。

- **資産の管理責任者（資産の所有者・管理者名）**
- **資産の形態**
- **保管形態**
- **保管場所**
- **保管期間**
- **廃棄方法**
- **用途**
- **利用者の範囲（＋業務プロセス）**
- **他のプロセスとの依存性**

資産を個別に識別しその性質を理解することは、後の作業に関わる脅威やぜい弱性の識別と資産価値の判定の手助けとなります。

個人情報保護法との関係では、個人情報取扱事業者である組織の ISMS の適用範囲内に個人情報があるときは、個人情報、個人データ、保有個人データを洗い出すことが必要です。

この洗い出しの目的は、組織が ISMS の構築、維持、継続的改善を通じて、個人情報保護法その他個人情報を取り扱う重要な法令等に準拠した個人情報、個人データ、保有個人データの取扱いの内部統制とマネジメントを構築し、運用、維持、改善することにあるのですから、組織における不足を見いだせるように工夫することが重要です。例えば、個人情報の利用目的が収集したときの契約上の義務の履行やその契約上の事務にしか用いないという組織では、収集した個人情報や個人データ、保有個人データがその目的に利用される設計になっているかどうかを確認すれば、この設計に反した運用がなされているかどうかは、洗い出しのプロセスではなく、監視、予防、是正、監査のプロセスの中で考えれば足りるでしょう。第三者提供についても、事務の設計上、個人データの第三者提供を行わない組織では、個人情報や個人データの提供先の設計が本人以外に及ばないものになっていることを調査すれば足り、個人情報がどこにどのように流れていっているかを詳細に調査する必要はないといえるでしょう。第三者提供がおこなわれているかどうかは、上記同様、監視、予防、是正、監査のプロセスの中で見られるようになっているかどうかが重要であるというべきでしょう。

情報資産の形態との関係では、個人情報保護法は、個人情報、個人データ、保有個人データによって、組織がなすべきことを区別していますから、情報資産の形態を洗い出すに際しては、洗い出しの対象が個人情報、個人データ、保有個人データのいずれであるのかを区別してその取扱いに関する洗い出しを行うことも便利でしょう(後述③「情報資産のグループ化」)。

また、個人情報保護法は、個人情報や個人データ、保有個人データを取り扱える範囲を、利用目的達成に必要な範囲内としています。従って、情報資産の形態を洗い出すにあたっては、その利用目的も明確に調査しておくと、その後のリスクアセスメントや、その後必要な取扱い組織、人、手段、方法、保管期間や保管方法、利用者の範囲、利用を許される業務の範囲の適正さなどを評価するときに役立ちます。

個人情報保護法は、目的拘束だけでなく、必要かつ適切な安全管理と第三者提供の原則禁止を定めています。従って、個人情報、個人データ、保有個人データの利用目的、利用者の範囲(+業務プロセス)、他のプロセスとの依存性を洗い出すときには、安全管理と第三者への提供の有無、アクセス制御、業務プロセス上の個人情報、個人データ、保有個人データの流れを示すフローを明確にする必要があります。

② 資産の例示

JIS Q 27002:2006 の「7.1.1 資産目録」には、資産の例示があります。

表 7-7　資産の例示

資産の種類	例示
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、代替手段の取決め、監査証跡、保存情報
ソフトウェア資産	業務用ソフトウェア、システムソフトウェア、開発用ツール、ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取外し可能な媒体、その他の装置
サービス	計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
人	保有する資格、技能、経験
無形資産	例えば、組織の評判、イメージ

この例では、電子的なデータはもちろんそれらを処理するコンピュータ本体、記録媒体やファームウェアなども含まれています。また、紙媒体の情報や会話、物理的な施設・設備といったものも該当します。

③ 資産のグループ化

ISMS適用範囲に存在する資産の洗い出し作業の負荷が非常に大きいことは容易に想像できます。

リスク分析の作業を進めるにあたり、「資産のグループ化」は作業負荷軽減と今後の分析作業の効率化に有効な考え方です。

例えば、資産価値や属性（保管形態や保管期間、用途等）が一致するものを一つのグループとする等です。重要性や属性が同じで、結果的に適用されるセキュリティ対策が同じであれば、同じグループとしてまとめて管理することが効率的です。

そもそも資産の洗い出しをする目的は、ISMSの適用対象全体で適切なセキュリティ対策を決定することです。組織の全ての資産を網羅し、一つひとつの資産の属性を明記した詳細な資産台帳を作成することが必ずしも重要ではありません。

④ 情報区分（影響度の基準）

資産目録の作成後、資産価値を評価します。資産価値は、組織の事業上重要なプロセスに対する影響度ととらえることが可能です。

組織のニーズに基づく資産の識別と評価は、リスクアセスメントにおける重要な要因となります。従って、主要な資産の価値の評価は、組織のビジネスをよく理解した情報の管理責任者（「情報オーナ」などという場合もある。）によって行われなければなりません。

組織は、資産の価値を判定する際にC.I.A.の3要素に関する組織独自の判断基準を開発しなければなりません。表7-8に、機密性の判断基準の例を示します。

表7-8　機密性の基準の例

資産価値	クラス	説明
1	公開	第三者に開示･提供可能 内容が漏洩した場合でも、ビジネスへの影響はほとんど無い
2	社外秘	組織内では開示･提供可能（第三者には不可） 内容が漏洩した場合、ビジネスへの影響は少ない
3	秘密	特定の関係者または部署のみに開示･提供可能 内容が漏洩した場合、ビジネスへの影響は大きい
4	極秘	所定の関係者のみに開示･提供可能 内容が漏洩した場合、ビジネスへの影響は深刻かつ重大である

表 7-9　完全性の基準の例

資産価値(完全性)	クラス	説明
1	不要	参照程度でしか利用されていないので問題がない。
2	要	改ざんされると問題があるが、ビジネスへの影響はない
3	重要	完全性が維持できないとビジネスへの影響は深刻かつ重大である

表 7-10　可用性の基準の例

資産価値(可用性)	クラス	説明
1	低	情報が利用できなくてもビジネスに支障がない
2	中	情報が利用できないとビジネスへの支障はあるが、代替手段で業務ができる。または、情報が利用できるまでの遅延が許される。
3	高	必要時に確実に情報が利用できないとビジネスへの影響は深刻かつ重大である

個別の資産の価値は、表 7-8 の例示のように予め規定された情報区分に基づき、主に情報の管理責任者の主観で判定されます。

（2）　脅威・ぜい弱性の明確化

ISMS 認証基準では、リスク因子を個別の資産がさらされるであろう「脅威」と管理上の問題点などから「ぜい弱性」の組合せと規定しています。リスク因子とはリスクが顕在化する要因です。

> 3.1.5 リスク因子(source)
> 結果（3.1.2）をもたらす可能性が潜在する物事や行動。
>
> （TR Q 0008:2003　3.用語及び定義　より引用）

①　脅威の識別

「脅威」とは、情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因です。脅威は後述する「ぜい弱性」により誘引され、顕在化することにより組織及び組織の業務に影響を与えます。脅威の大きさは、その要因や対象となる資産ごと

に、その発生の可能性を評価して決定します。

GMITS では表 7-11 の様に大別して説明しています。

表 7-11　脅威の分類例

人為的脅威		環境的脅威
意図的（計画的）脅威	偶発的脅威	環境的脅威
deliberate ⇒ D	accidental ⇒ A	environmental ⇒ E

情報の管理責任者は、前述した資産の価値の決定同様、情報利用者や他事業部門の関係者、外部の専門家から提供される脅威に関する情報を元に、自らが管理する資産がさらされる脅威を識別し、表 7-12 の例示のような一覧表を作成します。

表 7-12　脅威の例示とその分類例

脅威	分類（D,A,E）
地震	E
停電	D, A ,E
静電気	E
オペレータの操作ミス	D, A
人的リソース（スタッフ）不足	A
ID の偽り	D
悪意のあるソフトウェア	D, A
……	……

脅威の洗い出しは、上記の表の例などを参考に実施します。

例えば、意図的（計画的）脅威は、攻撃者の動機、攻撃に必要とされるスキル、利用できるリソースを考慮に入れ、資産の特性、魅力、ぜい弱性から、どのような要因が脅威であるかを識別します。

偶発的な脅威は、立地条件、極端な気候条件の可能性及び要員によるミスや誤動作などから影響を及ぼす可能性を識別します。

次に、脅威の発生頻度を評価します。

頻度についても、脅威の識別と同様に自身の業務と関連する他部門と協力して整理します。作成した脅威一覧に基づき、業務上の経験や過去に収集した統計的なデータに基づいて検討します。

評価にどの程度の正確性を要求されるかにもよりますが、「低い」、「中程度」、「高い」の 3 つの区分とする場合が多いようです。表 7-13 に、3 つに区分した場合の判断基準を例示します。

表 7-13　脅威の判断基準

脅威		
発生可能性	区分	説明
1	低い	発生する可能性は低い。発生頻度は 1 年に 1 回あるかないかである。
2	中程度	発生する可能性は中程度である。発生頻度は半年以内に 1 回あるかないかである。
3	高い	発生する可能性は高い。発生頻度は 1 ヶ月に 1 回以上である。

②　ぜい弱性の識別

ぜい弱性とは、脅威発生を誘引する資産固有の弱点やセキュリティホールのことです。ぜい弱性は、それだけでは何ら障害とはなりませんが、脅威を顕在化させ、損害や障害を導く可能性があります。逆にいえば、脅威が存在しないぜい弱性は、あまり気を配らなくても良いということになります。

ぜい弱性の分類の例を表 7-14 に示します。ぜい弱性をリスト化する際には、表 7-14 のように脅威と関連づけて整理する必要があります。

表 7-14　ぜい弱性の識別

ぜい弱性の分類	ぜい弱性の例	関連する脅威の例
環境、施設	ドア、窓などの物理的保護の欠如	盗難
	不安定な電源設備	停電、誤作動
	災害を受けやすい立地条件	洪水、地震、災害
ハードウェア	温湿度変化に影響を受けやすい	故障、誤作動
	記憶媒体のメンテナンス不足	故障、情報漏洩
ソフトウェア	仕様書の不備	ソフトウェア障害、誤作動
	アクセスコントロールの欠如	なりすまし、改ざん、情報漏洩
	不適切なパスワード	不正アクセス、改ざん、情報漏洩
	監査証跡（ログ管理）の欠如	不正アクセス
	バックアップコピーの欠如	復旧不能
……	……	……

ぜい弱性は、資産の性質や属性と関連付けて検討すると識別が容易です。
例えばノート PC を例にとれば、その性質として、「持ち運びやすい」、「衝撃に弱い」、「公共の場で用いられる」などが挙げられます。と同時にその性質は、「盗難や置き忘れ」、「故障」、「情報漏洩」という脅威に対するぜい弱性を示しています。

このことは、その資産の利用環境や保管場所、プロセスの進行状況（ステージ）、形態、時間など、その環境によっては全く異なるぜい弱性が存在することを示しています。同じ資産（例えばノート PC）であっても、その利用形態や性質などから「ノート PC（社内利用）」、「ノート PC（社外利用）」などと分けて識別して管理すべき場合もあることに留意しなければなりません。

ぜい弱性の評価は、その資産の持つ弱点がどの程度であるかを評価することになります。何も対応策を施しておらずその弱点が剥き出しであるような場合は、ぜい弱性は高いと判断できます。組織によりどの程度分類するかは異なりますが、脅威同様、ぜい弱性に関しても、「低い」、「中程度」、「高い」などで区分します。

７.２.５　STEP5　リスクを分析し評価する

ここで述べるリスクアセスメントは、適用範囲にある、例えば顧客管理システムなどの情報資産の仕様、運用、保守それぞれの設計について、例えば個人情報保護法など法規適合性が識別された法令等への法規適合性が確認できた後、それらの実際の運用、保守に関する CIA の不備、喪失によってもたらされるリスクのアセスメントです。この過程で、上記各設計について法規適合性が認められないことが判明したときは、是正を行うことが先決で、法規適合性が認められない ISMS には ISMS 適合性評価は与えられません。

ISMS において、個人情報を適正管理するためには、個人情報の機密性と完全性を確保するだけでなく、ビジネスの観点からもセキュリティ事件・事故で事業継続(法律でもとめられているわけではない)ができない事態が発生するのは問題であり、個人情報の可用性の確保も必要となります。当該情報資産の機密性、完全性又は可用性の喪失による潜在的な影響を考慮してリスクアセスメントを実施し、受容可能なリスクの水準に基づき、当該リスクについて受容できるか対応が必要かを決めます(図 6-1)。

リスクアセスメントは、アセスメント手順を決定し、資産目録を作成し、資産の重要性の分類及び脅威・ぜい弱性の評価基準を明確にすることにより実施が可能になります。

資産の重要性は、前述の C.I.A.毎に分けて情報の管理責任者が評価します。

脅威・ぜい弱性の評価は、作業を専門家に依頼して実施した方が客観性や効率性の確保の面から良い場合もあります。また、情報セキュリティ監査制度を利用し、外部の専門家がぜい弱性評価の支援することも考えられます。

（１）リスク値の算出

リスク値は、前の作業で明確になった「資産の価値」、「脅威の大きさ」、「ぜい弱性の度合い」を用いて、例えば、簡易的に以下のような式で算出します。

リスク値 ＝ 「資産の価値」 × 「脅威」 × 「ぜい弱性」

（例）

特性	資産価値
C:機密性	4
I:完全性	2
A:可用性	1

脅威　　3（情報が関係者外に漏洩した場合、信用の失墜に繋がる）

ぜい弱性　3（すべての作業担当者に特権が付与されていたので）

この場合のリスク値は、以下のようになります。

機密性に関わるリスク値：4×3×3＝36

完全性に関わるリスク値：2×3×3＝18

可用性に関わるリスク値：1×3×3＝9

図 7-13　リスク値の計算例

また、リスク値を算出し表 7-15 の例のようなマトリクス「リスク値早見表」を作成すると、以降の作業を効率的に進める助けになります。

表 7-15　リスク値早見表例

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

例えば、受容可能なリスク値は表 7-16 の例のような一覧表になることが考えられます。

表 7-16　リスク受容一覧の例(1)

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

リスクを受容できる範囲

リスクに対して何らかの対策を講じる範囲

表 7-16 のリスク受容一覧の例(1)は、7.2.3.2(4)で特定した「受容可能なリスク水準」を[9]とした場合です。リスク評価作業の際に作成したリスク値のマトリクス（「リスク値早見表」）で、リスク値が「9」未満のものについては、現状の管理を受容し、受容したリスクについては「残留リスク」として管理します。残留リスクとは、以下のように定義されます。

> 3.9 残留リスク（residual risk）
> リスク対応の後に残っているリスク（TR Q 0008:2003）。
>
> （JIS Q 27001:2006　3 用語及び定義　より引用）

表 7-17　リスク受容一覧の例(2)

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

リスクを受容できる範囲

リスクに対して何らかの対策を講じる範囲

また、表 7-17 のリスク受容一覧の例(2)では、資産の価値が最大の「4」であれば無条件に対策をとるべきであるということで、リスク値の許容水準は「4」未満となります。

このリスク受容一覧は、あくまでリスク評価実施時のリスク環境を表わすもので、資産の価値や脅威、ぜい弱性等の環境に変化が生じた場合は、適宜リスク値の見直しを実施しなければなりません。

（2）作業上の留意点

リスクアセスメントは、体系だった手順の策定と、それに従った実施が求められます。例えば、経済産業省リスク管理・内部統制に関する研究会の「リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～」ではリスクの算定について以下の通り説明しています。

> 特定されたリスクは、それぞれのリスクが顕在化した場合の企業への影響度と発生可能性に基づき、企業にとっての重要度を算定されなければならない。必ずしも全てのリスクについて定量的に算定することができるわけではないが、リスクの算定は、関係者が納得できる合理的な指標を用いて、統一的な視点で相対的な比較が可能となるよう行われることが望ましい。例えば、リスクの影響度とその発生可能性をそれぞれ「大」、「中」、「小」に区分し、影響度と発生可能性の組合せにより評価すること等が考えられる。
>
> ＜中略＞
>
> また、リスクを定性的にしか把握できない場合には、経験等に基づく推測により、その影響度と発生可能性をそれぞれ「大」、「中」、「小」とランク付けし、評価すること等が考えられる。
>
> （リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～
> 第二部　ＩＩ.1.リスクマネジメントのあり方(3) リスクの算定
> 平成 15 年 6 月　経済産業省リスク管理・内部統制に関する研究会　より引用）

つまり前述の計算方法を採用した場合にも、リスク値が変わる可能性があります。

リスク値 ＝ 「資産の価値」 × 「脅威」 × 「ぜい弱性」

という計算式には厳密な理論性はありません。似た属性を持つ同種の資産であっても、個別の資産についての価値や脅威、ぜい弱性の評価結果や、評価者の判断でリスク値に差が出てしまうことはあり得ます。

また、資産の価値や、脅威、ぜい弱性の値を足し算してリスク値を算出しても評価は可能です。

ISMS 認証基準では、リスク値を算出することが要求事項に規定されています。しかし極論すれば、点数だけに頼ってリスク値を決定せず、人間の判断を優先して対策の必要性の有無を決定するというリスクアセスメントの枠組みの採用も、選択肢のひとつとなると思います。

例えば前述の、評価者の判断のばらつきについても、分析の初期の段階から十分な例を用意し、評価者に十分な説明を実施すれば、結果をある程度平準化することは可能になります。

更に、日常当該資産を利用している（もしくは主に管理している）情報の管理責任者の認識をリスク値の評価の参考として収集し確認することも、現状の対策の程度が十分であったかを検証する指標となります。

７.２.６　STEP6　リスク対応を行う

ここで述べるリスク対応は、適用範囲にある、例えば顧客管理システムなどの情報資産の仕様、運用、保守それぞれの設計について、例えば個人情報保護法など法規適合性が確認できた後、それらの実際の運用、保守に関するリスクアセスメントの結果明らかになった CIA の不備、喪失によってもたらされるリスクに対する対応です。ただし、この対応の結果、例えば個人情報保護法など識別された法規に適合しない結果となるときには、その対応方針を選択することはできません。

同様に、管理策の選択によって、組織の情報資産に対する取り組みが法規適合性を欠くときは、その管理策を選択することはできません。

> 3.15　リスク対応（risk treatment）
> リスクを変更させるための方策を，選択及び実施するプロセス（TR Q 0008:2003）。
> 注記　この規格では，“管理策”という用語を“方策”の類義語として使用する。
>
> （JIS　Q　27001:2006　3 用語及び定義　より引用）

リスク対応とは、「リスクを変更させるための方策を選択及び実施するプロセス」と説明されています。リスクを変更させるための方策として、次の 4 つの選択肢があります。

- **適切な管理策を採用する**
- **組織の方針及びリスク受容基準を明確に満たすリスクを、意識的、かつ、客観的に受容する**
- **リスクを回避する**
- **リスクを移転する**

リスクアセスメントで明確にされた管理対象とするリスクに対し、上記 4 つの選択肢からどれを選択するかについて評価します。

（1）適切な管理策を採用する

「適切な管理策を採用し、リスクを低減する」方法は、リスク対応の実施の際に最も多く採用されます。

例えば、ISMS 認証基準の附属書 A に記載されている 133 項目の管理策の適用や、要求事項に明記されていない対策の追加実施等はこれに相当します。

リスク低減について概念的に示したものを図 7-14 に示します。この場合、リスク低減は「リスクの発生の可能性を低減する」ことと、「リスクが顕在化した場合の影響度を低減する」ことにより実現されることが分かります。

図 7-14 で、

R はリスク：Risk

C はリスクを低減させるための対策：Control

E は対策を講じた後のリスク：Exposure

を示しています。

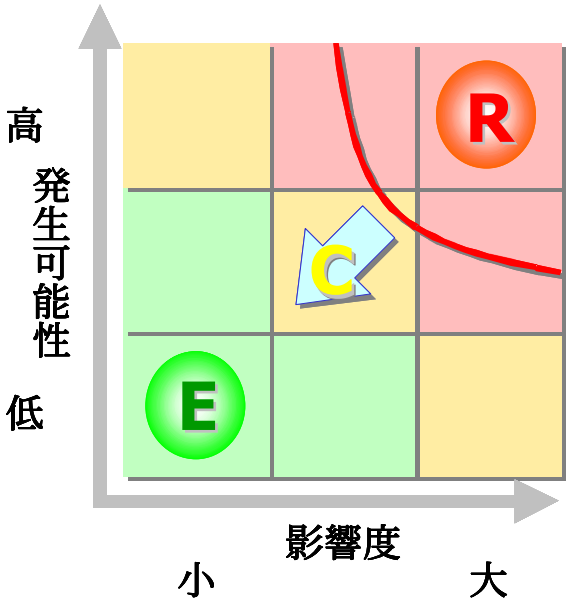


図 7-14　リスク低減の概念

リスク発生可能性の低減の例として、「入退室をより厳重に管理する」などの対策が考えられます。

影響度の低減では、「バックアップ頻度を増やし、修復可能なデータを増やす」などの対策が考えられます。

現実には、対策の実施によるリスクの完全な除去は不可能です。多くの場合、利便性の確保や、対策にかかる費用と効果の比較により、顕在化したときのリスクを受容可能な水準にとどめるのに十分な費用を投入して対策を実施し、残留リスクを次項「リスクを意識的、かつ、客観的に受容する」の対象として管理します。

（2）リスクを意識的、かつ、客観的に受容する

「リスクを意識的、かつ、客観的に受容する」とは、リスクが組織の方針及びリスクの受容のための評価基準を明らかに満たす場合に用いる選択肢です。保有されるリスク

は、以下の 2 つに大別できます。

- **識別され受容されるリスク**
- **識別されず組織に内在するリスク**

保有するリスクの内、リスクが組織の基本方針及びリスクの受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容することになります。

（3）リスクを回避する

「リスクを回避する」とは、リスク対応を考えてもコストの割に利益が得られない場合や適切な対応策が見出されない場合、リスクを回避するために、業務を廃止したり、資産を破棄するといった方法をとることです。

例えば、個人情報の保管には、漏えいするリスクがあります。また、それらの情報を各個人（各従業者）が保有し、管理する方法では、適切に開示できないというリスクが想定されます。これらのリスクに対し業務上の必要性が乏しくなった個人情報であれば、廃棄するというリスク対応が考えられます。

また、売上に寄与していないメーリングリストは、不注意で個人情報が漏えいしたり、ウィルス蔓延に利用されるリスクがあるので、メーリングリストを廃止するというリスク対応が考えられます。

（4）リスクを移転する

リスクを移転するとは、契約等によりリスクを他者（他社）に移転することです。

リスクを移転する方法は大別すると 2 種類あります。一つは資産や情報セキュリティ対策を外部に委託する方法（アウトソーシング）で、もう一つはリスクファイナンスの一種として保険等を利用する方法です。

例えば、前者の例として資産を外部のデータセンターに預けるというコロケーションサービスの利用や、運用を委託するという方法があります。一般にデータセンター、インターネットサービスプロバイダー、アプリケーションサービスプロバイダー、マネジメントサービスプロバイダーといわれている事業者がこのようなリスクの移転先となります。

組織は、このようなアウトソーシング等にリスクを移転する場合、「移転したリスク」、「移転しなかったリスク」、「移転したことにより新たに発生するリスク」の 3 つを明確にすることが重要となります。また、移転したリスクを明確にするために、セキュリティ対策について契約書等に織り込むことが重要となります。

ISMS 認証基準の附属書 A「管理目的及び管理策」には以下のような管理策が記載されており、リスクを移転することにより新たに発生するリスクを低減するための管理策と

いえます。

A.10.2 第三者が提供するサービスの管理 目的：第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。		
管理策		
A.10.2.1	第三者が提供するサービス	管理策 第三者が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義，及び提供サービスレベルが，第三者によって実施，運用，及び維持されることを確実にしなければならない。

（JIS Q 27001:2006　A.10.2 第三者が提供するサービスの管理　より引用）

リスク管理上は、ISMS 認証基準の管理策を適用できない場合や、適用してもリスク値が受容水準以上の場合、リスク移転を検討します。

リスクファイナンスとしてリスクの移転の典型的な例は保険の採用です。例えば、地震等の不可避な脅威について、事業に与える影響は大きいが、比較的発生する可能性が低いので保険の利用を検討する等ということが相当します。

今日では、情報システム障害に対応するための保険が販売されています。例えば、顕在化したリスクの影響から復旧するために必要な費用や機器の買い替え費用が保険により支払われるというものです。

保険の場合、保証されるのは損害に対する金銭的な保証の一部に過ぎません。そのため、保険のみを利用したリスク対策には限界があります。(例えば、情報漏えいをおこし、企業ブランドが低下しても保険により損害を補填することは困難です)。つまり、保険によるリスク対応は万能ではありません。あくまでも、管理策を実施しても補填できないリスクがある場合に予備的に利用するのが本来の目的と思われます。

また、保険は、免責事項などが細かく決められていますので、契約を結ぶ前に細かく確認することが重要です。

７．２．７　STEP7　管理目的と管理策を選択する

ISMS 認証基準の附属書 A「管理目的と管理策」より、リスク対応に関する管理目的及び管理策を選択します。適切な管理目的又は管理策が附属書 A に記載されていない場合は、独自に追加の管理策を採用することができます。

また、この選択については、リスクアセスメント及びリスク対応プロセスの結果に基づいてその妥当性を示すことが重要です。

また、附属書A「管理目的及び管理策」に記載されている管理策の幾つかは、すべての情報システム又は環境に適用できるとは限らないこと、及び組織によっては実施できない場合もあることを認識しておく必要があります。JIS Q 27002:2006 「4.2 セキュリティリスク対応」では例示として、「例えば，10.1.3 では，不正行為及び過失を防止するための職務の分割について規定している。比較的小規模の組織にとって，すべての職務を分割することは不可能であり，同じ管理目的を達成する他の方法が必要となる場合がある」と記載されています。しかし、このような場合でも、組織は管理目的を達成するにあたり、リスクが受容可能な範囲に低減できる代替措置を講じられるのであれば、附属書 A に記載されている管理策以外の管理策を選択し、確実に実装していく必要があります。

ISMS において個人情報を適正管理するためには、個人情報の機密性と完全性を確保するだけでなく、ビジネスの観点からもセキュリティ事件・事故で個人情報が使用できず業務が中断する状況が発生するのは問題であり、個人情報の可用性の確保も必要となります。当該情報資産の機密性、完全性又は可用性の喪失による潜在的な影響を考慮し、リスクアセスメントを実施します。受容可能なリスクの水準に基づき、当該リスクについて受容できるか対応が必要かを決めます。

７.２.８　STEP8　残留リスクを承認する

残留リスク（リスク対応の後に残っているリスク）が受容リスク水準以下であるか、又は受容リスク水準以下になる計画であることを経営陣が確認し、承認します。

７.２.９　STEP9　ISMSの導入・運用を許可する

経営陣がISMSを導入し、運用することに対して確認し、承認します。

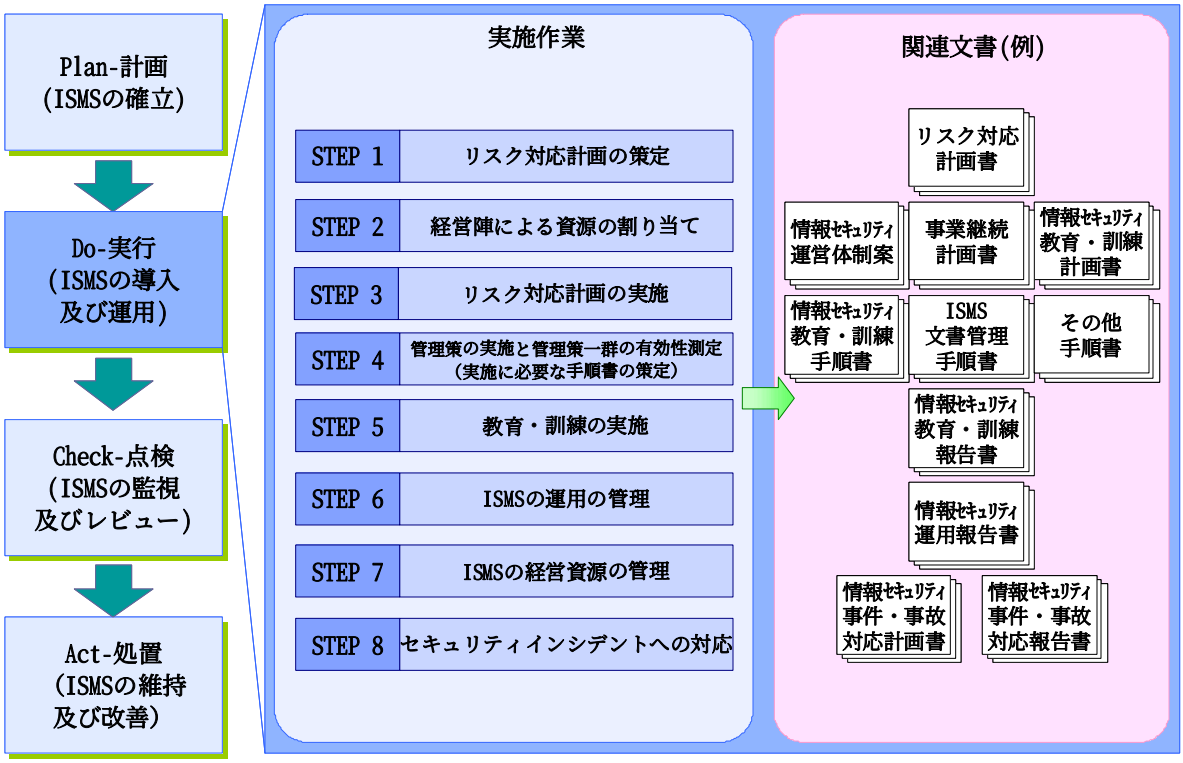
７.２.１０　STEP10　適用宣言書を作成する

STEP7で選択した管理目的及び管理策、並びにこれらを選択した理由を文書化し、適用宣言書を作成します。

また、附属書 A に記載された管理目的及び管理策の中から適用除外としたものは、当該管理策と除外した理由について記録を残すことが要求されています。

７．３　ISMS の導入及び運用（Do-実行）

ISMS 認証基準の「4.2　ISMS の確立及び運営管理」では、ISMS の導入及び運用の手順を図 7-15 の 8 つのステップで規定しています。



注）文書名は全て例示

図 7-15　ISMS 導入及び運用の手順

組織は，次の事項を実行しなければならない。

a) リスク対応計画を策定する。この計画では，情報セキュリティリスクを運営管理するための，経営陣の適切な活動，経営資源，責任体制及び優先順位を特定する。

b) 特定した管理目的を達成するためにリスク対応計画を実施する。この計画には，必要資金の手当て並びに役割及び責任の割当てへの考慮を含む。

c) 4.2.1 g) によって選択した管理策を，その管理目的を満たすために実施する。

d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し，また，比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために，それらの測定をどのように利用するかを規定する［4.2.3 c) 参照］。

注記　管理策の有効性の測定は，管理策が，計画した管理目的をよく達成していることを，管理者及び要員が判断することを可能にする。

e) 教育・訓練及び意識向上のためのプログラムを実施する（5.2.2 参照）。
f) ISMS の運用を管理する。
g) ISMS のための経営資源を管理する（5.2 参照）。
h) 迅速にセキュリティ事象を検知でき，かつ，セキュリティインシデントに対応できるための手順及びその他の管理策を実施する［4.2.3 a) 参照］。

（JIS Q 27001:2006　4.2.2 ISMS の導入及び運用　より引用）

７.３.１　STEP1　リスク対応計画の策定

リスク対応計画とは、リスクアセスメントの結果に基づき、受容できないリスクを低減するためにとるべき活動と、選択した管理目的及び管理策の実装に関する実行計画を明らかにすることです。

リスクマネジメントに必要な経営資源の割り当てや実際の作業は、このリスク対応計画に基づいて実施されます。

経営陣は、この計画が策定されることを確実にする責任があります。詳細は、次章「8. 経営陣の責任」でふれますが、ISMS 認証基準ではリスク対応計画に経営陣の適切な活動、責任及び優先順位を明確にすることが要求されています。

リスク対応計画に不備があれば、十分な管理目的及び管理策が実装できないことにも繋がりますので、様々な条件を考慮に入れて計画を策定する必要があります。

リスク対応計画では、単にリスクを低減するための管理目的及び管理策を策定するだけではなく、導入した管理目的及び管理策が適切かつ効果的に動作していることを確認するための管理目的及び管理策や、異常を検出するための管理目的及び管理策等を導入する計画も合わせて策定する必要があります。

例えば、管理策としてアンチウィルスソフト、ファイアウォール、アクセス制御などのセキュリティ製品を導入する場合について考えてみます。これらの製品を導入する際には、セキュリティを強化するための設定に留まらず、それらの状態を示す情報や、処理した結果のログなどを抽出して解析することにより、異常検出を考慮した設定を実装することなども計画に盛り込むことが必要です。

また、解析に必要な装置などが高価な場合、その導入による効果を確実にするための管理策も視野に入れて検討することが重要です。

リスク対応計画により、組織が識別したリスクに対する管理目的及び管理策の実施状況と、対策は実施したが残留リスクが受容可能な水準以下に低減されていないリスクへの追加的対策の進捗状況を容易に把握することが可能となります。

リスク対応計画に含むことが望ましい内容として、以下の 4 点があります。

- **日程表**
- **優先順位**
- **詳細な作業計画**
- **管理策を実施する責任**

７.３.２　STEP2　経営陣による資源の割り当て

本ガイドの「8. 経営陣の責任」を参照して下さい。

７.３.３　STEP3　リスク対応計画の実施

特定した管理目的を達成するためにリスク対応計画を実施します。ここでは、STEP1 及び STEP2 で定めたプロセスに従い、必要資金の手当て並びに役割及び責任の割当て等を考慮に入れ、確実に管理目的を達成するために当該責任者を中心にリスク対応計画を実施します。

７.３.４　STEP4　管理策の実施と有効性測定

リスク対応計画に従い、優先順位の高い管理策から実施していきます。

その際には、管理策の運用に関する手順や、セキュリティインシデントに対応する手順などを文書化し、関係者に周知する必要があります。

さらに新たな要求事項として、「管理策の有効性の測定」が加わりました。詳細は本ガイドの「9. 有効性の測定」を参照してください。

７.３.５　STEP5　教育･訓練の実施

本ガイドの「8.2.2 教育・訓練、認識及び力量」を参照して下さい。

７.３.６　STEP6　ISMS の運用の管理

導入した管理策が適切に運用されることを管理するための手順書を策定します。また、策定する各々の手順書には、運用管理者、利用者などの関係者の責任が明記されている必

要があります。

手順書に含まれる例を以下に示します。

- **バックアップに関する手順**
- **変更に関する手順**
- **復旧に関する手順**
- **正常動作確認のための手順**
- **緊急時の対応に関する手順**

７.３.７　STEP7　ISMS の経営資源の管理

本ガイドの「8.2 経営資源の運用管理」を参照して下さい。

７.３.８　STEP8　セキュリティインシデントへの対応

顕在化したセキュリティインシデントに対する被害を最小限に抑えるために、先ずそれらを適切に検出し、迅速な処置をとることが重要です。

セキュリティインシデントに対応するための手順書の策定と、その内容の定期的な検証は重要な作業です。特に、初期段階における対応の責任者の設定及び必要な関係者を対象とした連絡・報告の体制、適切な処置の実施に関する一連の手順の策定は重要です。

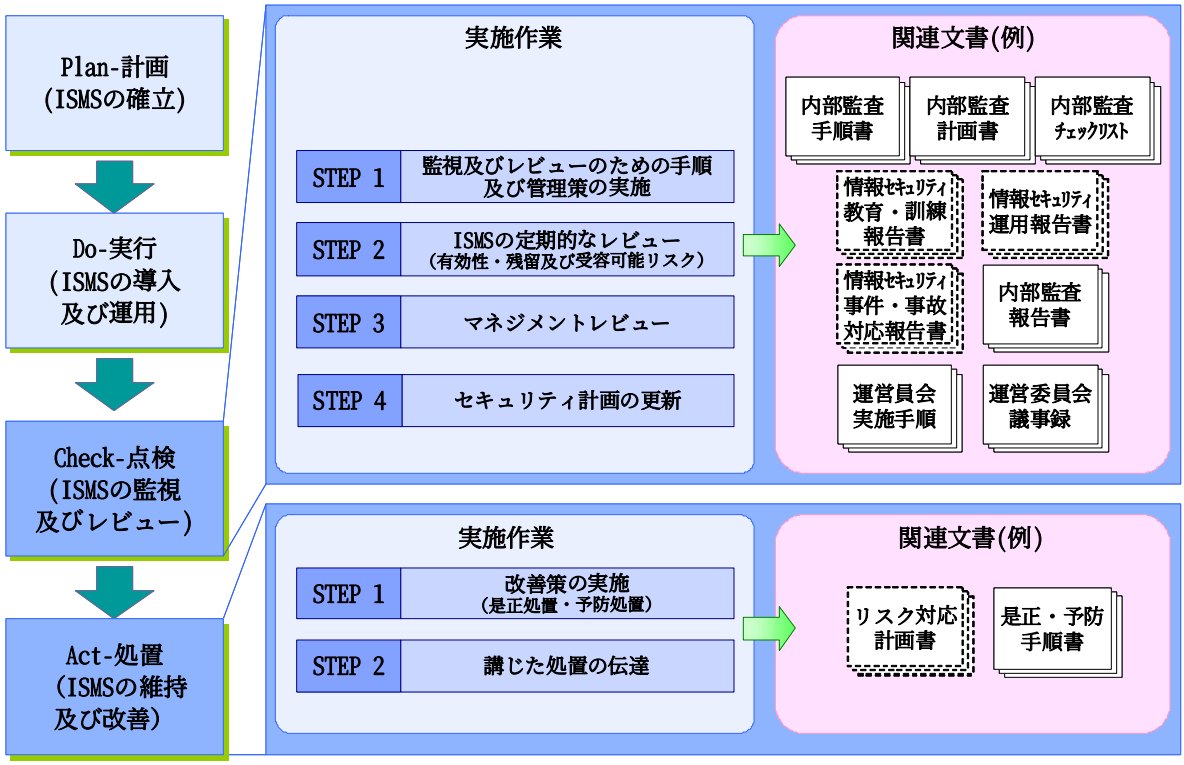
また、検出されたセキュリティインシデントを報告し、適切な処置として組織全体に反映することは、今後の再発防止のために重要です。セキュリティインシデントを報告する報告書には、以下の次項を含めることに留意して下さい。

- **セキュリティインシデントの記録**
- **管理策の不具合**
- **処置の内容**
- **必要な追加の管理策など**

報告をマネジメントレビューのインプットとすることは、情報セキュリティを継続的に向上させるうえで重要です。

７．４　ISMS の監視及びレビュー（Check-点検）・ISMS の維持及び改善（Act-処置）

ISMS 認証基準の「4.2 ISMS の確立及び運営管理」では、ISMS の監視及びレビュー、ISMS の維持及び改善の手順をそれぞれ図 7-16 の様に規定しています。



注）文書名は全て例示

図 7-16　ISMS の監視、レビュー、維持及び改善の手順

組織は，次の事項を実行しなければならない。

a) 監視及びレビューの手順並びにその他の管理策を，次のために実施する。

1) 処理結果の中の誤りを迅速に検知する。

2) 未遂であるか既遂であるかを問わず，セキュリティの違反及びインシデントを迅速に特定する。

3) 人力にゆだねて又は情報技術を導入して実施しているセキュリティ活動が期待どおりかどうかを経営陣が判断することを可能にする。

4) セキュリティ事象の検知を補助し，その結果の表示を利用してセキュリティインシデントを防止する。

5) セキュリティ違反を解決するためにとった処置が有効であるかどうかを判断する。

b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。

c) セキュリティ要求事項を満たしていることを検証するために，管理策の有効性を測定する。
d) リスクアセスメントをあらかじめ定めた間隔でレビューする。残留リスク及び特定したリスク受容可能レベルをレビューする。これらのレビューでは，次に起きた変化を考慮する。
   1) 組織
   2) 技術
   3) 事業の目的及びプロセス
   4) 特定した脅威
   5) 導入した管理策の有効性
   6) 外部事情（例えば，法令又は規制の状況，契約上の義務，社会的風潮）
e) あらかじめ定めた間隔で ISMS 内部監査を実施する。
   注記　第一者監査と呼ばれる内部監査は，内部目的のために，その組織自身又はその組織に代わる者が実施するものである。
f) 適用範囲が引き続き適切であること，及び ISMS のプロセスにおける改善策を特定（7.1 参照）することを確実にするために，ISMS のマネジメントレビューを定期的に実施する。
g) 監視及びレビューの活動から見出された事項を考慮に入れるために，セキュリティ計画を更新する。
h) ISMS の有効性又はパフォーマンスに影響を及ぼす可能性のある活動及び事象を記録する（4.3.3 参照）。

（JIS Q 27001:2006　4.2.3 ISMS の監視及びレビュー　より引用）

組織は，常に次の事項を実行しなければならない。
a) 特定した改善策を ISMS に導入する。
b) 8.2 及び 8.3 に従った適切な是正処置及び予防処置をとる。自他の組織のセキュリティの経験から学んだものを適用する。
c) すべての利害関係者に，状況に合った適切な詳しさで，処置及び改善策を伝える。該当するときは，処置及び改善策の進め方について合意を得る。
d) 改善策が意図した目的を達成することを確実にする。

（JIS Q 27001:2006　4.2.4 ISMS の維持及び改善　より引用）

Check（点検）のフェーズでは、主にマネジメントレビューに必要なインプット情報の収集について規定されています。経営陣はマネジメントレビューを実施し、PDCA サイクルの前半部分「Plan（計画）～Do（実行）」で決定した手順に従いプロセスが実施されているか、また計画の段階で期待されている成果が上がっているか検証します。これは ISMS の維持や継続的な改善活動に必要不可欠な作業です。

マネジメントレビューのインプット情報として、監視の対象とすべき事項には以下のよ

うな例があります。

■ 処理の誤りや、セキュリティインシデントの記録
■ セキュリティ活動の実施状況と管理策有効性の測定結果
■ 提案
■ 利害関係者からのフィードバック
■ 環境（社会的、技術的環境や法的規制、事業上の環境など）の変化
■ 内部監査からのフィードバック

ここに出てくる「提案」とは、JIS Q 27001:2006 の「7.2 レビューへのインプット」の
i) 改善のための提案
に該当します。

この i) が何を指すのか、JIS Q 27001:2006 では規定されていませんが、JIS Q 9001:2000 ではこれに相当するものが、「5.6.2 マネジメントレビューへのインプット」の中の
g) 改善のための提案
であり、さらにこの g) は「5.5.2 管理責任者」にある、以下の規定があることと関連して解釈されています。

> トップマネジメントは，管理層の中から管理責任者を任命すること。管理責任者は与えられている他の責任とかかわりなく次に示す責任及び権限をもつこと。
> b) 品質マネジメントシステムの実施状況及び改善の必要性の有無についてトップマネジメントに報告する。
>
> （JIS Q 9001:2000　5.5.2 管理責任者　より引用）

つまり、g) の指す「提案」とは、組織内部からの提案を想定している、ということになりますので、JIS Q 27001:2006 でもそれに従い、「組織内部からの提案」と想定されます。

経営陣は、マネジメントレビューの結果として以下の事項について判断しなければいけません。

■ ISMS の有効性
■ 経営資源の割り当て
■ 残留リスク及び受容可能なリスクの水準
■ セキュリティ計画の見直し

ここで出てくるセキュリティ計画とは、リスク対応計画や是正計画、資源計画、教育計

画などを含む、ISMS 構築に関連する様々な計画の総称として捉えることができます。

Act（処置）のフェーズでは、ISMS の有効性を継続的に改善するために、Check（点検）のフェーズで収集された情報を基に是正処置及び予防処置を講じることです。

これらの活動については、ISMS 認証基準の「5 経営陣の責任」、「6 ISMS 内部監査」、「7 ISMS のマネジメントレビュー」、「8 ISMS の改善」の章に詳細に規定されています。具体的内容については、本ガイドの「8. 経営陣の責任」以降の説明を参照して下さい。

７.５　文書化に関する要求事項

ISMS 認証基準は、ISMS の文書化について、以下を要求しています。

> 文書には，経営陣の決定に関する記録も含めなければならない。文書は，とった処置から，経営陣の決定及び方針へたどれること，並びに記録した結果が再現可能であることを確実にしなければならない。
> 選択した管理策からリスクアセスメント及びリスク対応のプロセスまで，更には ISMS 基本方針及び目的までにつながる関係を説明できることが重要である。
>
> （JIS Q 27001:2006　4.3 文書化に関する要求事項　4.3.1 一般　より引用）

ISMS の活動では、経営陣が決定した ISMS 基本方針及び目的に基づいて、リスクアセスメント及びリスク対応のプロセスを実施し、その結果によって管理策を選択します。

ISMS 認証基準では、管理策をリスクアセスメント及びリスク対応のプロセスの結果に基づき選択し、さらに、それらのプロセスが ISMS 基本方針及び目的に基づいて実施されていることを関連付けられるような文書の作成を求めています。

また、リスクアセスメントや有効性の測定の方法は、それを実施する人によって異なる方法となってしまっては結果を比較できず、情報セキュリティを効果的に管理することができません。

したがって、記録された結果が再現可能なことを確実にするために、文書化は重要になります。

また、定めた管理策について実施者がそのとおりに実施するように、手順を確立し明文化することが求められています。

> ISMS 文書には，次を含めなければならない。
> a) 文書化した ISMS 基本方針［4.2.1 b)参照］及び目的
> b) ISMS の適用範囲［4.2.1 a)参照］
> c) ISMS を支えている手順及び管理策
> d) リスクアセスメントの方法［4.2.1 c)参照］の記述
> e) リスクアセスメント報告［4.2.1 c)～4.2.1 g)参照］
> f) リスク対応計画［4.2.2 b)参照］
> g) 情報セキュリティのプロセスを有効に計画，運用及び管理することを確実にするために，組織が必要とする文書化した手順。管理策の有効性をどう測定するか［4.2.2 d)参照］を記述するために，組織が必要とする文書化した手順。
> h) この規格が要求する記録（4.3.3 参照）

i）適用宣言書

注記 1　この規格で“文書化した手順”という用語を使う場合には，その手順を確立し，文書化し，実施し，かつ，維持していることを意味する。

注記 2　ISMS の文書化の程度は，次の理由から組織によって異なることがある。

－ 組織の規模及び活動の種類

－ 適用範囲，並びにセキュリティの要求事項及び運営管理するシステムの複雑さ

注記 3　文書・記録の様式及び媒体の種類は，どのようなものでもよい。

（JIS Q 27001:2006　4.3 文書化に関する要求事項　4.3.1 一般　より引用）

ISMS 認証基準では、「文書化された手順」として、明確に記載している部分が 5 ヶ所あります。

4.3.1g)	情報セキュリティのプロセスを有効に計画，運用及び管理することを確実にするために，組織が必要とする文書化した手順。管理策の有効性をどう測定するか［4.2.2 d）参照］を記述するために，組織が必要とする文書化した手順。
4.3.2	ISMS が要求する文書は，保護し，管理しなければならない。次の事項を行うのに必要な管理活動を定義するために，文書化した手順を確立しなければならない。
6	監査の計画・実施に関する責任及び要求事項，並びに結果報告・記録維持（4.3.3 参照）に関する責任及び要求事項を，文書化した手順の中で定義しなければならない。
8 2.	組織は，ISMS の要求事項に対する不適合の原因を除去する処置を，その再発防止のためにとらなければならない。是正処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。
8 3.	組織は，ISMS の要求事項に対する不適合の発生を防止するために，起こり得る不適合の原因を除去する処置を決定しなければならない。とられる予防処置は，起こり得る問題の影響に見合ったものでなければならない。予防処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。

（JIS Q 27001:2006　上記各項　より引用）

７.６　文書管理

ISMS 文書は、版管理され適切な文書を必要とする人が必要なときに使用可能な状態で管理されている必要があります。ISMS 文書の管理について、以下の点を盛り込んだ管理手順を確立し、文書管理する必要があります。

ISMSが要求する文書は，保護し，管理しなければならない。次の事項を行うのに必要な管理活動を定義するために，文書化した手順を確立しなければならない。

a) 適切かどうかの観点から，文書を発行前に承認する。
b) 文書をレビューする。また，必要に応じて更新し，再承認する。
c) 文書の改変を特定すること及び現在の改版状況を特定することを確実にする。
d) 使用する必要があるとき，適用する文書の関連する版が使用可能であることを確実にする。
e) 文書は読みやすく，かつ，容易に識別可能であることを確実にする。
f) 文書を，それを必要とする者には利用可能にすることを確実にする。また，文書を，その分類区分に適用される手順に従って受け渡すこと，保管すること，及び最終的には処分することを確実にする。
g) 外部で作成された文書であることの識別を確実にする。
h) 文書配付の管理を確実にする。
i) 廃止文書の誤使用を防止する。
j) 廃止文書を何らかの目的で保持する場合には，適切な識別を施す。

（JIS Q 27001:2006　4.3.2 文書管理　より引用）

７.７　記録の管理

記録は、組織の ISMS が要求事項へ適合していること及び運用の効果を示す証拠として作成、維持、管理します。

PDCA プロセス全般における活動の記録、管理策の実施状況の記録、及び ISMS に関連する全てのセキュリティインシデントの発生に関する記録を維持することが要求されます。その際、該当する法的要求事項を考慮に入れることも要求されます。

ISMS 認証基準では、「記録」として、明確に記載している部分が 6 ヶ所あります。

4.2.3h)	ISMS の監視及びレビュー	ISMS の有効性又はパフォーマンスに影響を及ぼす可能性のある活動及び事象を記録する
5.2.2d)	教育・訓練，意識向上及び力量	教育，訓練，技能，経験及び資格についての記録を維持する
6	ISMS 内部監査	監査の計画・実施に関する責任及び要求事項，並びに結果報告・記録維持に関する責任及び要求事項を，文書化した手順の中で定義しなければならない
7.1	ISMS のマネジメントレビュー（一般）	レビューの結果は，明確に文書化し，記録を維持しなければならない
8.2e)	是正処置	とった処置の結果の記録
8.3d)	予防措置	とった処置の結果の記録

（JIS Q 27001:2006　上記各項　より引用）

記録の管理として、以下の事項の実施などが効果的です。

- **識別、保管、保護、検索、保管期間及び廃棄に関して必要な管理を文書化すること**
- **運営管理プロセスで記録の必要性及び記録の範囲を定めること**
- **法律等によって保管期間が定められている場合には、法的要求事項に適合した保存期間を決定すること**

ISMS 認証基準の附属書 A「A.15 順守」に、以下の管理策が挙げられています。

A.15.1.3	組織の記録の保護	重要な記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊及び改ざんから保護しなければならない。

（ JIS Q 27001:2006　附属書 A（規定）A.15.1 法的要求事項の順守　より引用）

8．経営陣の責任

本ガイドの「7. 情報セキュリティマネジメントシステム」では、ISMS を確立、導入、運用、維持及び改善するために重要な要求事項について説明しています。ISMS 認証基準の「5 経営陣の責任」では、その活動における経営陣の役割をより詳細に規定していますので、本章では視点を変えて、改めて説明します。

ISMS の活動のあらゆる段階において、様々な活動が確実に実施されていることについて、経営陣の果たすべき役割は非常に重要です。ISMS の対象を組織全体ではなく、ある組織階層とし、マネジメントの対象を限定する場合も多いと思われますが、その時でも組織全体としてのマネジメントを意識することが重要です。

経営陣が ISMS の構築に関与することは、コーポレートガバナンスの視点からも重要です。コーポレートガバナンスとは、株式会社においては経営者による会社の経営責任を株主からの受託責任ととらえ、その遂行責任を問うものです。
コーポレートガバナンスは、「株主による取締役会及びそれを通じた執行者の統治」と、「執行者による企業運営の統治」の 2 つの局面が考えられます。執行者による企業の統治（運営）が行われずして、株主による取締役会及びそれを通じた執行者の統治は意味がありません。従って、まず執行者による企業の統治が重要となります。この統治を行うためにマネジメントが必要となります。

コーポレートガバナンス（CG）の2つの局面

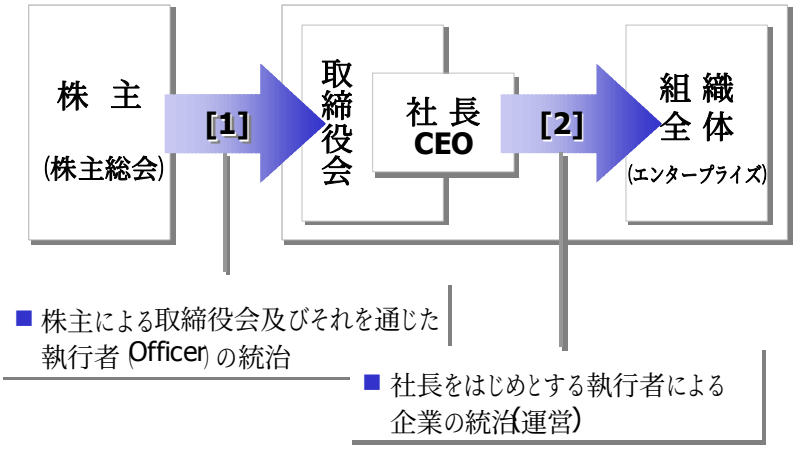


図 8-1　コーポレートガバナンス

執行者によるマネジメントの対象は多岐にわたります。マネジメントの対象の１つとし

て、情報セキュリティも考えることができます。その他、品質や、環境もマネジメントの対象となります。

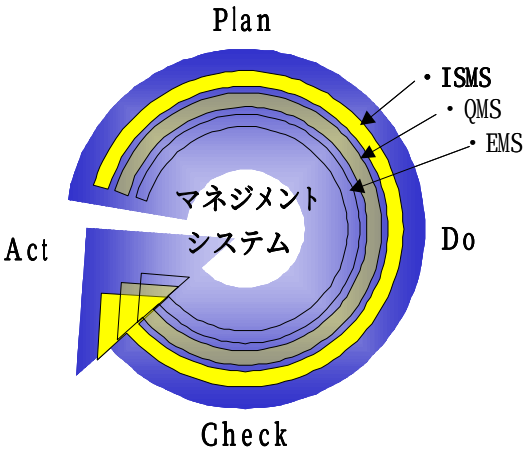


図 8-2　マネジメントシステムの対象

情報セキュリティ、品質、環境のマネジメント・プロセスを手順化したものが、それぞれ ISMS、QMS、EMS と言われるものです。これらのマネジメントシステムは事業全体を対象としたマネジメント、とりわけリスクマネジメントの一部として、企業の事業目的達成を側面から支援することになります。このことは組織論的には、事業全体のマネジメントができていないにもかかわらず、その一部にのみ力を入れても高い効果を得られないことを示唆しています。ISMS は、全体のマネジメントシステムとの関係を考えながら確立していくことが重要です。

とりわけ、法令を順守するという面からは組織の一部の取り組みではなく、法人全体、企業グループ全体の取り組みとして法令を順守するためのマネジメントシステム、つまりコンプライアンスプログラムを策定すべきです。

また、企業グループ全体を統治することを必要とする組織においては、最近コーポレートガバナンスの観点から、法律上の企業体ではなく、支配力の及ぶ企業グループ全体についての統治、マネジメントの重要性が強調されています。連結経営などはその象徴といえます。ISMS も企業グループ全体で構築することが、コーポレートガバナンスの観点からは必要となります。

典型的な組織のマネジメントは、図 8-3 のように階層構造を持ち、下位組織階層のマネジメントシステムは上位組織階層のマネジメントシステムと協調して活動します。

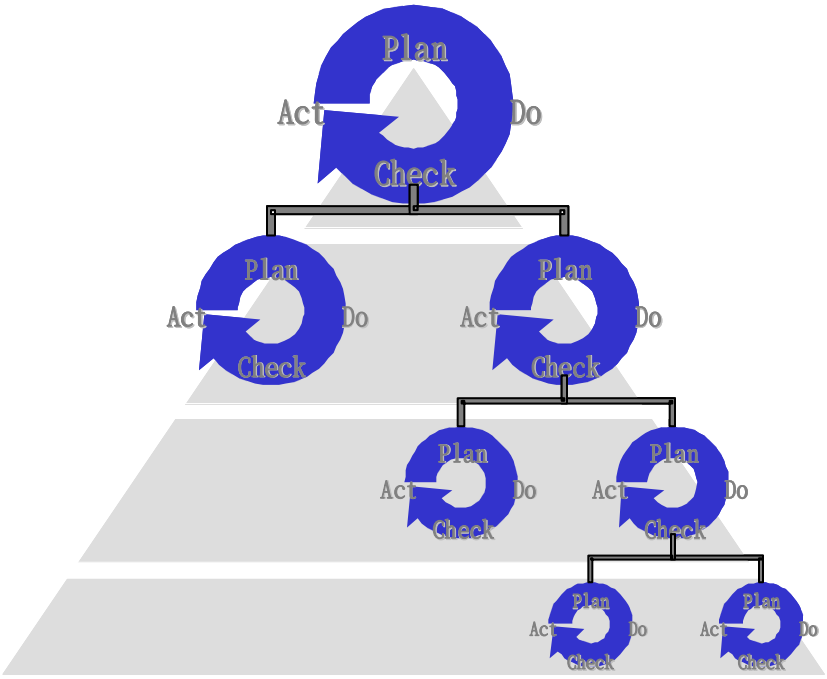


図 8-3　典型的な組織のマネジメントシステム

ISMS の構築の初期段階においては、適用範囲を限定し、特にリスクの大きい領域への対策を優先することに注力することもあります。しかし、経営陣はその場合においても前述のマネジメントシステム間の連携を認識し、最終的に想定したゴールに導く責任を負います。

８．１ 経営陣のコミットメント

経営陣の果たすべく重要な役割のひとつにコミットメントがあります。ISMS の確立、導入、運用及び維持等に関与し、組織として情報セキュリティの実施責任を利害関係者に宣言する「コミットメント」は、執行権限を有する経営陣にのみ実施する事が許されるからです。

ISMS 認証基準では、経営陣のコミットメントを次のように規定しています。

経営陣は，ISMS の確立，導入，運用，監視，レビュー，維持，及び改善に対する自らのコミットメントの証拠を，次によって提供しなければならない。

a) ISMS 基本方針を確立する。
b) ISMS の目的及び計画の確立を確実にする。
c) 情報セキュリティのための役割及び責任を確立する。
d) 組織に，次を伝える。
　－ 情報セキュリティ目的を満たすことの重要性
　－ 情報セキュリティ基本方針に適合することの重要性
　－ 法のもとでの責任
　－ 継続的改善の必要性
e) ISMS の確立，導入，運用，監視，レビュー，維持及び改善のために十分な経営資源を提供する（5.2.1 参照）。
f) リスク受容基準及びリスクの受容可能レベルを決定する。
g) ISMS 内部監査の実施を確実にする（箇条 6 参照）。
h) ISMS のマネジメントレビューを実施する（箇条 7 参照）。

（JIS Q 27001:2006　5 1 経営陣のコミットメント　より引用）

経営陣は、どの程度の水準でリスクを受容するのかを判断します。これは、経営陣が ISMS の確立、導入、運用及び維持等に最終的な責任を負っているからです。しかし、経営陣は組織のマネジメントシステムに責任を持ちますが、全ての活動に関与することは不可能です。

そこで、経営陣はまず情報セキュリティの方向性を示す ISMS 基本方針を確立します。ISMS 基本方針の確立については、「ISMS ユーザーズガイド　4.2.2　STEP2　ISMS 基本方針を定義する」で説明されていますので参考にして下さい。

次に、ISMS の目的を設定し、ISMS 実践のための計画が策定されることを明確に指示し、確実に実施されることに責任を負います。その中に法令を順守することも含まれます。組織の業務活動において、関係してくる法令を洗い出しそれを順守する必要があります。既存の業務において関連する法律のみならず、情報セキュリティ対策を新たに導入することに伴い新たな業務プロセスが生まれ、その業務プロセスに関連する法令の洗い出しも行わなければなりません。

また、ISMS の実効性を担保するために、組織における情報セキュリティ上の役割及び責任を定め、ISMS の確立、導入、運用及び維持等に十分な経営資源を提供しなければなりません。このことについては、後述の「8.2.1　経営資源の提供」で説明します。

最終的に経営陣は、構築した ISMS が意図した通り有効に機能していることを自身が ISMS 内部監査等を通じて把握し、改善のための意思決定等を行うためにマネジメントレビューを実施することが重要となります。このことについては、「9. ISMS 内部監査」及び「10. マネジメントレビュー」で説明します。

８.２ 経営資源の運用管理

８.２.１ 経営資源の提供

経営陣の重要な役割の一つとして、「人」、「物」、「金」といった経営資源の提供があります。経営陣は、ISMS の必要性を理解し、そのために必要な経営資源の提供を行わなければなりません。ISMS 認証基準では、経営資源の提供を次のように規定しています。

> 組織は，次の事項を行うのに必要な経営資源を決定し，提供しなければならない。
> a) ISMS を確立，導入，運用，監視，レビュー，維持及び改善する。
> b) 事業上の要求事項を満たすことに，情報セキュリティの手順が寄与することを確実にする。
> c) 法令及び規制の要求事項並びに契約上の情報セキュリティ義務を明確にし，これを扱う。
> d) 導入したすべての管理策を正確に適用することによって，十分なセキュリティを維持する。
> e) 必要に応じてレビューし，レビューの結果に対して適切に対応する。
> f) 必要な場合には，ISMS の有効性を改善する。
>
> （JIS Q 27001:2006 5 2 経営資源の運用管理　より引用）

経営陣の掛け声だけでは、ISMS の確立、導入、運用及び維持等は難しいと思われます。
ISMS の構築に必要な一連のプロセスには経営資源の割り当てが必要となります。

８.２.２ 教育・訓練、認識及び力量

経営資源の中でも「人」の問題は特に重要です。
ISMS 認証基準では、「人」に関連する教育・訓練、認識および力量を次の４つの事項を挙げて説明しています。

> 組織は，ISMS に定義された責任を割り当てた要員すべてが，要求された職務を実施する力量をもつことを，次の事項によって確実にしなければならない。
> a) ISMS に影響がある業務に従事する要員に必要な力量を決定する。
> b) 必要な力量がもてるように適切な教育・訓練するか，又は他の処置（例えば，適格な要員の雇用）をとる。
> c) とった処置の有効性を評価する。
> d) 教育・訓練，技能，経験及び資格についての記録を維持する（4.3.3 参照）。

組織は，また，関連する要員すべてが，自らの情報セキュリティについての活動がもつ意味と重要性とを認識し，ISMS の目的の達成に向けて，自分はどのように貢献できるかを認識することを確実にしなければならない。 （JIS Q 27001 5 2.経営資源の運用管理　より引用）

ISMS の確立、導入、運用及び維持等を行っているのは、人であるということを忘れてはなりません。組織の各個人が情報セキュリティに関連する責任を果たし、期待される役割を実行するためには、本人の力量が伴わなければならないことは明らかです。

経営陣には、明確にされた役割を割り当てられた要員全てが、要求される業務を実施する力量を持つことを確実にするために、教育・訓練を実施させる責任があります。また、実施する教育・訓練の内容は、全ての要員が自らの情報セキュリティについての活動の意味とその重要性を認識し、ISMS の目的の達成に向けてどのように貢献できるかを認識できるようなものが理想です。

実施した教育・訓練については、その有効性を評価し、力量を持った要員の確保に役立てることが重要です。必要とされる力量は、それぞれの業務により異なることになります。ISMS の確立、導入、運用及び維持等のために必要となる力量としては、表 8-1 のような分野が考えられます。

表 8-1　力量の分野

マネジメントに関連する力量	マネジメント論全般、リーダシップなど
監査に関連する力量	監査理論全般、監査の実務
セキュリティ技術に関連する力量	ネットワークセキュリティ、サーバアプリケーションセキュリティ、OS セキュリティ、ファイアウォール、侵入検知システム、ウィルス、セキュアプログラミング、暗号などに関する理論や実践
法律に関連する力量	憲法、民法、刑法、民事訴訟法、刑事訴訟法、商法、労働関連法、証券取引法、個人情報保護法、不正競争防止法、知財関連法、建築基準法等

これらの力量を適切に定義し、その達成度を確認することが重要となります。
また、この力量の有無を検討する一つの目安として、資格制度を利用することも有益と思われます。それぞれの力量と関連する資格の例としては表 8-2 のような資格、試験合格者が考えられます。

表 8-2　力量と関連する資格

内部監査	公認内部監査人(CIA)[5]、公認会計士、公認システム監査人[6]、システム監査技術

[5] 公認内部監査人(Certified internal Auditor）は内部監査人協会（The Institute of Internal Auditors,Inc.(IIA)　http://www.theiia.org）が認定する内部監査人の資格。内部監査人協会は 1941 年に米国で設立され、2003 年現在、全世界で 85,000 名が内部監査人協会に所属している。

	者[7]、公認情報システム監査人(CISA)[8]、ISMS 主任審査員、ISMS 審査員、公認情報セキュリティ監査人（CAIS）[9]
セキュリティ技術	情報セキュリティアドミニストレータ、上級システムアドミニストレータ 、テクニカルエンジニア(情報セキュリティ)[10]、公認情報セキュリティ管理者(CISM)[11]、公認情報システムセキュリティ専門家(CISSP)、公認システムセキュリティ熟練者(SSCP)[12]
法律	弁護士、弁理士、社会保険労務士、法学検定試験

また、情報セキュリティについての業務毎に必要とされる力量を決定する際に、経済産業省が発表している情報セキュリティ教育についての報告書[13] や、独立行政法人情報処理推進機構（IPA）が発表しているセキュリティスキル標準[14]、スキルマップ[15]、報告書[16]などを参考にされるとよいと思われます。

---

[6] 公認システム監査人は特定非営利活動法人日本システム監査人協会（http://www.saaj.or.jp）が認定するシステム監査人の資格。

[7] 独立行政法人情報処理推進機構により行われている、システム監査技術を有していることを認定するための国家試験。

[8] 公認情報システム監査人は、情報システムコントロール協会（Information Systems Audit and Control Association　http://www.isaca.org）により認定されるシステム監査人の資格。情報システムコントロール協会は 1967 年に米国で設立され、2006 年現在、全世界で約 50,000 名が協会に所属しています。

[9] 公認情報セキュリティ監査人は、特定非営利活動法人日本セキュリティ監査協会により認定される情報セキュリティ監査人の資格。

[10] 情報セキュリティアドミニストレータ、上級システムアドミニストレータ、テクニカルエンジニア（情報セキュリティ）は独立行政法人情報処理推進機構により行われている、情報セキュリティ管理、システム管理、情報セキュリティについての一定の専門的知識・能力を有していることを検定するための国家試験。

[11] 公認情報セキュリティ管理者（Certified information security manager）は、情報システムコントロール協会（Information Systems Audit and Control Association　http://www.isaca.org）により認定されるセキュリティ管理者としての専門的能力を有していることを証明する資格。

[12] 公認情報システムセキュリティ専門家（Certified information system security professional）、公認システムセキュリティ熟練者（System security certified practitioner）は(ISC)^2（International Information Systems Security Certification Consortium http://www.isc2.org）により認定される情報セキュリティについての専門的能力を有していることを保証する資格。

[13] http://www.meti.go.jp/policy/netsecurity/edu_report.html

[14] http://www.jitec.jp/1_17skill/skill_00.html

[15] http://www.ipa.go.jp/security/manager/edu/training/expert.html

[16] http://www.ipa.go.jp/security/fy14/reports/professional/sec-pro-outline.pdf

９．ISMS 内部監査

マネジメントレビューのインプットの重要なものとして、内部監査の結果があります。ISMS 認証基準では、内部監査についてより詳細に規定しています。

内部監査は、ISMS の管理目的、管理策、プロセス及び手順が次の事項を満たしているか否かを判断するために実施されます。

> 組織は，その ISMS の管理目的，管理策，プロセス及び手順について，次の事項を判断にするために，あらかじめ定めた間隔で ISMS 内部監査を実施しなければならない。
>
> a) この規格及び関連する法令又は規制の要求事項に適合しているかどうか。
>
> b) 特定された情報セキュリティ要求事項に適合しているかどうか。
>
> c) 有効に実施され，維持されているかどうか。
>
> d) 期待したように実施されているかどうか。
>
> 組織は，監査の対象となるプロセス及び領域の状況及び重要性，並びに前回までの監査結果を考慮して，監査プログラムを策定しなければならない。監査の基準，範囲，頻度及び方法を定義しなければならない。
>
> 監査員の選定及び監査の実施においては，監査プロセスの客観性及び公平性を確実にしなければならない。
>
> 監査員は，自らの仕事を監査してはならない。
>
> 監査の計画・実施に関する責任及び要求事項，並びに結果報告・記録維持（4.3.3 参照）に関する責任及び要求事項を，文書化した手順の中で定義しなければならない。
>
> 監査された領域に責任をもつ管理者は，発見された不適合及びその原因を除去するために遅滞なく処置がとられることを確実にしなければならない。フォローアップには，とった処置の検証及び検証結果の報告を含めなければならない（箇条 8 参照）。
>
> 注記 JIS Q 19011:2003 は，ISMS 内部監査の実施のための有益な手引となる場合がある。
>
> （JIS Q 27001:2006　6 ISMS 内部監査　より引用）

ISMS の認証を取得するためには、ISMS 認証基準に準拠していることが求められますが、それと同時に法令を順守することも当然に求められます。

ISMS に関連する法律としては、個人情報保護法、著作権法、不正競争防止法、建築基準法、消防法などがあります。また、各地方自治体が定める個人情報保護条例なども適合を要求される法令に含まれます。

組織は業界の規制事項、顧客や取引先との契約事項、情報セキュリティ要求事項にも適合している必要があります。

ISMS 内部監査では、ISMS が有効に実施され、維持されていること、期待通りに実施されていることを確認することが求められています。

ISMS 内部監査は計画的に実施される必要があり、監査員は、監査の対象となる管理目的、

管理策、プロセス及び手順の状況と重要性、並びにこれまでの監査結果を考慮して監査プログラムを策定します。監査の実施にあたり、監査のための評価基準、対象範囲、頻度及び方法を定義しなければなりません。

監査員の選定においては、監査プロセスの客観性及び公平性を確保しなければなりません。

監査員の選定について重要な点は、監査員にはセキュリティの運用者、管理者とは異なる力量が求められると言うことです。例えば、監査員には以下に示すように監査に関連する一連のプロセスを実施する力量が求められます。

- **監査の計画及び実施**
- **結果の報告**
- **是正及び予防処置の提案　等**

また、組織は上記のような監査員に関する責任並びに監査に関連する一連のプロセスを、文書化された手順の中で規定することが求められます。

要求する力量をもった監査員を組織内に確保することが困難な場合には、外部の監査員の利用も考えられます。なお、客観性を確保するためにも、自らの業務を監査することはできません。

監査を受けたプロセス等に責任をもつ管理者は、発見された不適合及びその原因を除去するための処置が遅滞無く確実に講じられるようにしなければなりません。これは、不適合となっている部分をすぐに改善しなければならないという事ではありません。また、実施した改善活動には、講じた処置の検証及び検証結果の報告を含めなければなりません。

ISMS についての内部監査は、企業全体の視点から考えると、企業全体の内部監査の一部として、あるいは連携して実施することが効果的です。また、監査の実施にあたっては、「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」である JIS Q 19011:2003 を参考にすると良いでしょう。

また、情報セキュリティ監査制度、システム監査制度を利用し、専門家に内部監査の実施を依頼することも考えられます。

１０．ISMS のマネジメントレビュー

１０.１ 一般

経営陣の責任として、マネジメントレビューの実施が重要であることは 8.1 項で触れましたが、このマネジメントレビューは、ISMS を維持し、今後の活動を効果的に実施するために必要な活動です。これは、PDCA サイクルにおける Check-点検のプロセスの一部と言えます。ISMS が意図した通り有効に機能していることを経営陣自身が把握し、改善のための意思決定等を行います。

マネジメントレビューとは、経営陣が ISMS の効果を把握し、改善のための意思決定をする一連のプロセスです。ISMS のマネジメントレビューは、1 年以内の予め定められた間隔で実施しなければなりません。

マネジメントレビューでは、ISMS に対する改善の機会の評価、情報セキュリティ基本方針及び目的を含む ISMS の変更の必要性に関する評価も実施することになります。また、マネジメントレビューの結果は、記録として維持されていることが必要です。

１０.２ マネジメントレビューへのインプット

マネジメントレビューのためのインプット情報として、ISMS 認証基準では次のものを挙げています。

7.2 レビューへのインプット

次の情報を，マネジメントレビューに対して提供しなければならない。

a) ISMS 監査及びレビューの結果

b) 利害関係者からのフィードバック

c) ISMS のパフォーマンス及び有効性を改善するために組織の中で利用可能な技術，製品又は手順

d) 予防処置及び是正処置の状況

e) 前回までのリスクアセスメントが十分に取り上げていなかったぜい弱性又は脅威

f) 有効性測定の結果

g) 前回までのマネジメントレビューの結果に対するフォローアップ

h) ISMS に影響を及ぼす可能性がある，あらゆる変化

i) 改善のための提案

（JIS Q 27001:2006　7.2 レビューへのインプット　より引用）

マネジメントレビューへのインプットとして具体的には次のようなものが挙げられます。

- **内部監査や外部監査の結果（例えば、認証機関による不適合の指摘や観察事項など）**
- **顧客、取引先、従業員といった利害関係者からのフィードバック**
- **新たに利用可能となった技術、ベンダー等が発表した新製品・新サービスに関する情報**
- **実施した予防処置及び是正処置の実施状況及びその効果**
- **過去において、予算上、環境上、法令上の制約等で取り扱わなかった、ぜい弱性又は脅威などに対するリスクアセスメントの見直しの必要性の判断**
- **管理策または一群の管理策に対して、有効性を測定するための測定表などを用いて測定したことによって把握できた内容（本ガイドの 12.3.1 を参照）**
- **過去のマネジメントレビューの結果に適切に対応したかどうかについてのフォローアップの状況等についての報告**
- **経営環境の変化、組織の変化などを含む ISMS に影響を及ぼす可能性のある全ての組織内外の変化**

１０.３ マネジメントレビューからのアウトプット

経営陣は、インプットされた情報に基づいて経営的な判断、つまり経営の意思決定を行わなければなりません。その際の意思決定のポイントつまりマネジメントレビューからのアウトプットとして、ISMS 認証基準では次の 3 つの事項を挙げています。

> 7.3 レビューからのアウトプット
>
> マネジメントレビューからのアウトプットには，次に関係する決定及び処置を含めなければならない。
>
> a) ISMS の有効性の改善
>
> b) リスクアセスメント及びリスク対応計画の更新
>
> c) ISMS に影響を与える可能性がある内外の事象に対応するために，必要に応じた，情報セキュリティを実現する手順及び管理策の修正
>
> d) 必要となる経営資源
>
> e) 管理策の有効性測定方法の改善
>
> （JIS Q 27001:2006　7.3 レビューからのアウトプット　より引用）

経営陣は、マネジメントレビューのアウトプットとして、現状の ISMS をより効果的なものにするための改善を示さなければなりません。

また、ISMS の内部、外部環境が変化している場合は、環境変化に対応して情報セキュリティを実現する手順を修正しなければなりません。この内部、外部の環境には次のようなものが含まれます。

c)ISMS に影響を与える可能性がある内外の事象に対応するために，必要に応じた，情報セキュリティを実現する手順及び管理策の修正。そのような事象には，次について起きた変化が含まれる。

1)事業上の要求事項

2)セキュリティ要求事項

3)現在の事業上の要求事項を実現する業務プロセス

4)法令又は規制の要求事項

5)契約上の義務

6)リスクのレベル及び／又はリスク受容基準

（JIS Q 27001:2006 7.3 レビューからのアウトプット より引用）

1)事業ドメインの重要性に変化が生じた場合及び 3)業務プロセスに変更が行われた場合は、現在実施されている情報セキュリティ対策が引き続き適切であることを確認しなければなりません。

4)新たな法令の施行、既存の法令の改正、規制の新設、改正が行われている場合、現在のプロセスが引き続き法令等に準拠していることを確認することは重要です。特に最近は、個人情報保護法の全面施行、ｅ文書法の施行とともに、知的財産関連の法令、IT 関連の法令、不正競争防止法などの施行、改正が頻繁に行われており、判例も多く出されているため、注意が必要です。

5) 他者との関係を持つ業務では、その相手方と締結した契約上の義務についても順守しなければなりません。これについては相手方が個別に求めてくるものですので、その内容を個々に確認することが必要です。また、求められる実施事項が具体的になっていない場合には、相手方に対して何を持って義務を果たしたことになるのかなどを確認しておくことが必要です。

2)や 6)に関しても注意が必要です。情報技術の進歩は著しく、それに伴って新たな脅威（例えば、新しい攻撃手法の出現）が生じたり、新たなぜい弱性（例えば、新たなオペレーティングシステムやアプリケーションシステムのぜい弱性）が発見されたりします。また、既存の対応策に関するぜい弱性が変化し、リスクの度合いが変化することもあります。このような環境変化に対応して情報セキュリティを実現する手順を修正することが重要です。特に、業務手順を変更した際には、その業務手順が法令に違反・抵触していないかを検討する必要があります。

経営陣は、マネジメントレビューを通じて必要と認識された、ISMS の改善のために必要となる経営資源の提供についても確約する必要があります。改善に必要な経営資源の提供が確約されなければ、改善の実施は達成されないからです。

１１． ISMS の改善

１１.１ 継続的改善

情報セキュリティの継続的な改善に経営陣が責任を持つことにより、セキュリティ対策が確実に実施され、組織の ISMS の水準も継続して向上することが期待できます。

情報セキュリティ基本方針及び目的、監査結果、監視した事象の分析、是正処置、予防処置並びにマネジメントレビューのアウトプットを通じて、ISMS の有効性を継続的に改善することが重要です。

改善には是正処置、予防処置の 2 つがあり、以下ではこれらについて説明します。

１１.１.１ 是正処置

監査やマネジメントレビューの結果等により ISMS の導入及び運用に関連する不適合が発見された場合、不適合の原因を除去するための処置及び再発防止のための処置を講じなければなりません。これを「是正処置」といいます。

この是正処置には、ISMS 認証基準で規定している次の事項を含む手順を文書化することが必要です。

> 組織は，ISMS の要求事項に対する不適合の原因を除去する処置を，その再発防止のためにとらなければならない。是正処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。
>
> a) 不適合の特定
> b) 不適合の原因の決定
> c) 不適合の再発防止を確実にするための処置の必要性の評価
> d) 必要な是正処置の決定及び実施
> e) とった処置の結果の記録（4.3.3 参照）
> f) とった是正処置のレビュー
>
> （JIS Q 27001:2006　8.2 是正処置　より引用）

１１.１.２ 予防処置

起こり得る不適合を早期に発見し、処置を講じることを「予防処置」といいます。ISMS 認証基準 4.2.3 d)で示したリスクの変化に着目して、組織は予防処置についての要求事項を特定する仕組みを持つ必要があります。そのため、マネジメントレビューを通じてリス

クアセスメントの結果に基づく優先順位で、予防処置が取られるよう留意することが求められます。

この予防処置には、ISMS 認証基準で規定している次の事項を含む手順を文書化することが必要です。

> 組織は，ISMS の要求事項に対する不適合の発生を防止するために，起こり得る不適合の原因を除去する処置を決定しなければならない。とられる予防処置は，起こり得る問題の影響に見合ったものでなければならない。予防処置のために文書化された手順の中で，次のための要求事項を定義しなければならない。
>
> a) 起こり得る不適合及びその原因の特定
>
> b) 不適合の発生を予防するための処置の必要性の評価
>
> c) 必要な予防処置の決定及び実施
>
> d) とった処置の結果の記録（4.3.3 参照）
>
> e) とった予防処置のレビュー
>
> 組織は，変化したリスクを特定し，大きく変化したリスクに注意を向けて，予防処置についての要求事項を特定しなければならない。
>
> 予防処置の優先順位は，リスクアセスメントの結果に基づいて決定しなければならない。
>
> 注記 不適合を予防するための処置は，多くの場合，是正処置よりも費用対効果が大きい。
>
> （JIS Q 27001:2006　8.3 予防処置　より引用）

不適合が起こってから改善する「是正処置」より、起こらないように未然に防止する「予防処置」を講じる方が望ましいのは言うまでもありません。多くの場合、是正処置よりも予防処置の方が費用対効果が高いと言われています。

予防処置には、起こり得る不適合や原因の早期発見が重要です。組織の ISMS 構築にあたり、変化したリスクを特定し、大きく変化したリスクに注意を向けて要求事項を特定する機能がマネジメントプロセスに組み込まれており、マネジメントレビューを通じてリスクアセスメントの結果に基づいた優先順位で予防処置が取られるよう留意することが求められます。

１２．有効性の測定

本章では、ISMS の有効性の測定について検討していきます。ISMS の有効性を測定することは、構築した ISMS を形骸化させることなく、継続的な改善を実施する上で有用です。

１２.１　有効性測定の目的

ISMS 認証基準では、ISMS 全体及び個々の管理策について、有効性を測定することを明確化しています。有効性の測定結果を、ISMS の継続的な改善の機会と捉え、適切な行動をとることを促し、組織固有のセキュリティ目的及び事業（業務）目的を達成する管理策を確実にすることは重要な意味を持ちます。このことは、有効性測定を図 12-1 を基に考えるとより明確になります。

マネジメントシステムにおいては、個々のプロセスが要求される事項や期待を満たしていることを確実にするために、必要な PDCA を構築し、アウトプットの妥当性や有効性を測定し、測定結果をプロセスの管理責任者にフィードバックさせる機能を有することが求められています。

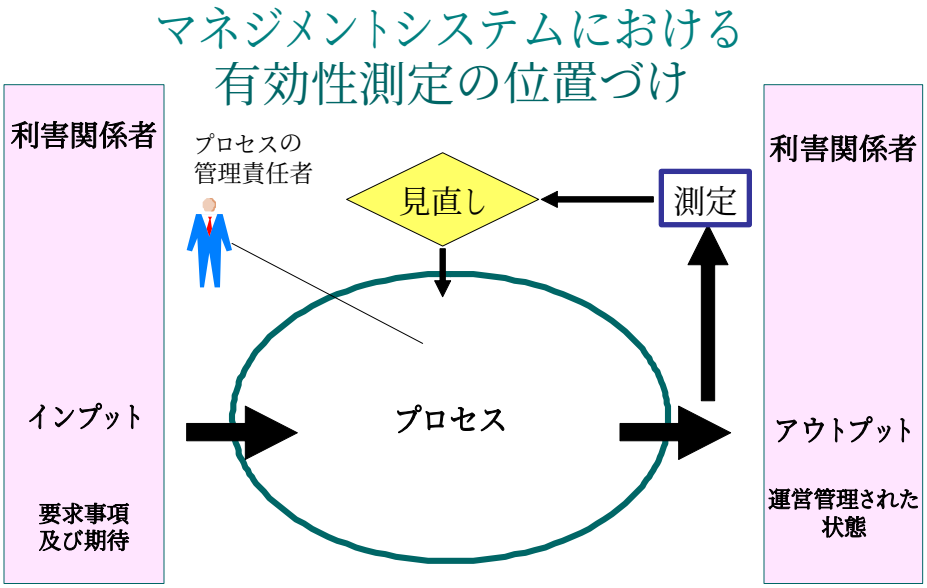


図 12-1　マネジメントシステムにおけるプロセスの有効性測定の位置づけ

図 12-1 では、要求事項、期待を含むインプットに対し、それらに応答するためのプロセス及びプロセスからのアウトプットの有効性測定を行い、適時、プロセスの管理責任者にフィードバックをしていることを示しています。

この図のプロセスを一連の ISMS の活動としたとき、図中の「測定」は ISMS 全体の有効

性について測定することになります。

他方、一連の ISMS の活動は、複数のプロセスから構成されていると捉えることも可能です。従って、図 12-2 のように、複数のプロセスの有効性の測定結果から、全体として、ISMS の有効性を図ることも可能です。

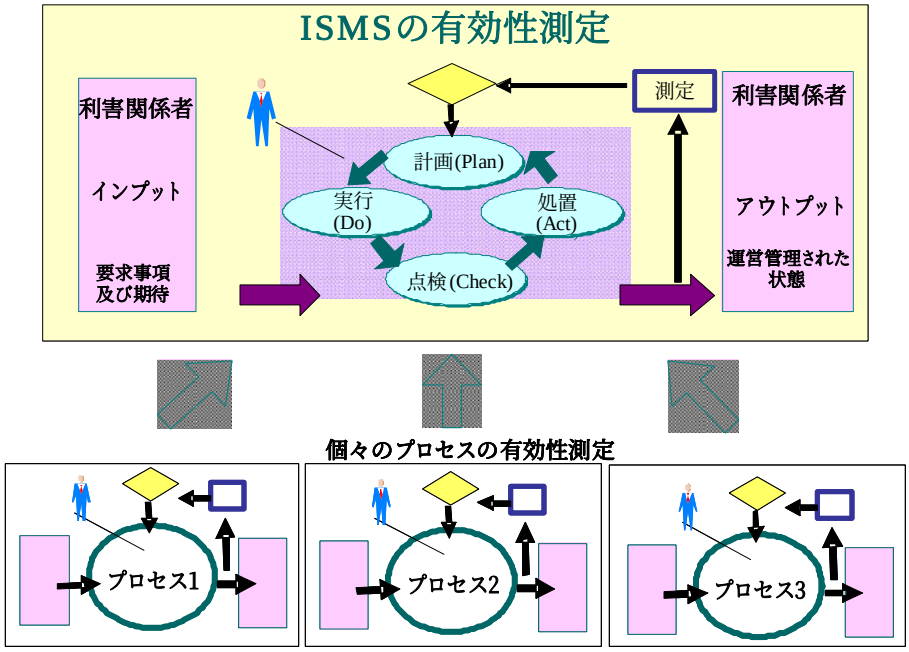


図 12-2　ISMS の有効性測定

個々のプロセスの有効性を測定する場合などは、そのプロセスに導入した管理策または一群の管理策の有効性を測定し、プロセス全体の有効性を把握するのに役立ちます。特に、一連のプロセスが複雑な場合、測定可能な個々のプロセスに分けて、各々の結果からプロセス全体の有効性を把握することは効果的な手法です。

ISMS 認証基準では、有効性の測定について ISMS 全体と管理策の有効性の 2 つのレベルについて規定しています。

ISMS 全体の有効性としては、以下のように規定しています。

> 8 ISMS の改善
>
> 8.1 継続的改善
>
> 組織は，情報セキュリティの基本方針及び目的，監査結果，監視した事象の分析，是正及び予防の処置，並びにマネジメントレビューを利用して，ISMS の有効性を継続的に改善しなければならない。
>
> （JIS Q 27001:2006　8.1 継続的改善　より引用）

また、管理策の有効性については以下のように規定しています。

> 4.2.2 ISMS の導入及び運用
> d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し，また，比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために，それらの測定をどのように利用するかを規定する(4.2.3c)参照)。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

ISMS 全体及び管理策の有効性を混在させた形では、以下のように規定しています。

> 4.2.3 ISMS の監視及びレビュー
> b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

これらの目的については、以下のように考えることができます。

- ISMS 全体の有効性の測定は、構築した ISMS が ISMS 基本方針及び目的を満たしていることを確実にするために実施する。
  - ISMS 全体の有効性の測定は、セキュリティリ監査の結果、インシデント、有効性測定の結果、提案、及び利害関係者からのフィードバックを考慮する。
- 管理策又は一群の管理策の有効性の測定結果は、最終的には ISMS の有効性の測定のためであり、ISMS 全体の継続的な改善のために活用する。

（注記１）有効性測定に関しては、ISMS 認証基準では「管理策又は一群の管理策の有効性測定」が要求事項となっています。（JIS Q 27001:2006 4.2.2 d）参照）
（注記２）ISMS 全体については、ISMS 認証基準では「ISMS 全体の有効性のレビュー」が要求事項となっており、「ISMS 全体の有効性測定」は要求事項となっていませんが、適用可能ならば測定することが提案されています。（JIS Q 27001:2006 0.2.2 プロセスアプローチ　点検より参照）

１２.２　有効性測定のプロセス

ここでは、有効性を測定することについて、説明します。
有効性の測定もひとつのプロセスと考えることができますから、プロセスアプローチの

考え方を適用すると図 12-3 のようになります。

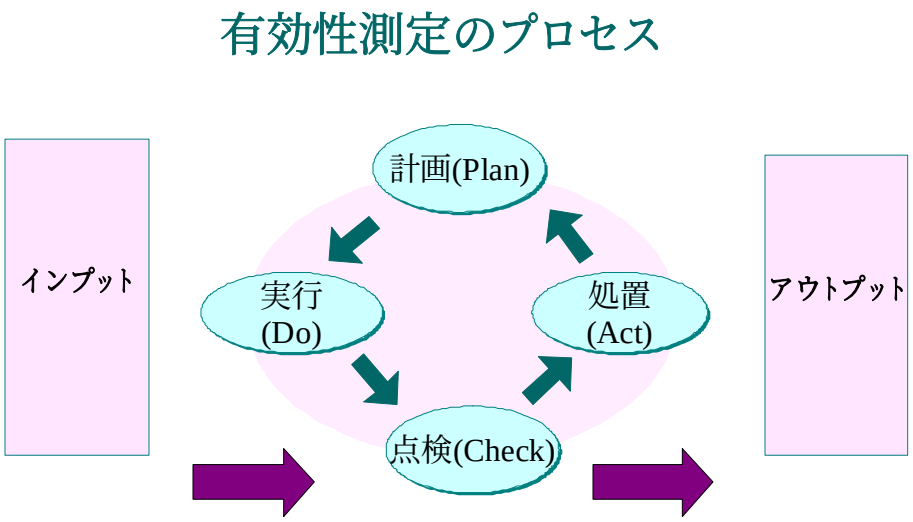


図 12-3　有効性測定のプロセス

図中の PDCA は、どのように有効性を測定するかを計画し、実行し、その結果について点検し必要に応じ、測定方法を見直すことを示しています。図中のインプットは、有効性測定をする上で考慮しなければならない事項であり、アウトプットは測定結果として捉えることができます。

１２.３　有効性測定の PDCA

１２.３.１　計画（Plan）

（１）ISMS 全体の有効性測定（ISMS 認証基準では有効性のレビュー）に関する計画

まず ISMS 全体の有効性測定のインプットとして、ISMS 認証基準では以下のように規定しています。

> 4.2.3 ISMS の監視及びレビュー
> b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

インプットとしては、
・ISMS 基本方針及び目的
・セキュリティ監査の結果
・インシデント
・有効性測定の結果
・提案
・利害関係者からのフィードバック
などが挙げられています。
また、これ以外にも管理策の有効性を測定する上で、
・管理策の配下にある資産やそれらを取巻く環境
・リスクアセスメントの結果等
なども有効性を測定する上のインプットとして役立ちます。
特に直感的に管理策の有効性を測定する上で役立つインプットとしては、インシデントや管理策の配下の資産の状態などが考えられます。影響が大きいインシデントが複数回起きた、又、管理策配下の資産が既に消去されているなどの場合、管理策はもはや有効でないと即座に導くことが可能です。このことは、有効性の測定プロセスにはインシデント管理、資産管理等との密接な連携を取り合う仕組みが必要であることを示唆しています。

上記のインプットの内の「有効性測定の結果」とは、管理策または、一群の管理策に対して、有効性を測定するための測定表などを用いて測定したことによって把握できた内容のことです。それらの結果を基に、最終的な判定を下すこともあります。このことについては、「管理策の有効性測定」の項で説明します。

アウトプットとしては、
・有効性測定の判定結果
と考えることができます。
この際、情報セキュリティの目的、すなわち情報の C(機密性)、I(完全性)、A（可用性）の維持という視点から、また必要に応じて真正性、責任追跡性、否認防止及び信頼性のような特性の維持のために、実行している管理策が有効であるのかを判定する必要があります。情報セキュリティでは、よく機密性と可用性の維持をバランスよく、とっていくことが困難であるといわれています。機密性を高めれば利便性が欠如し、可用性を高めればおのずと機密性は損なわれるという情報セキュリティの特性の中で、各プロセスのリスクに応じるために実施、運用している管理策の有効性を測定し、管理策をチューンアップしていくことは、重要なプロセスです。
また、管理策は維持させたい情報セキュリティの特性、すなわち C(機密性)、I(完全性)、A（可用性）毎に異なる場合があります。例えば、機密性であれば暗号化、可用性であればシステムの多重化という具合に管理策を考えることが通常です。その際、個別

に暗号化のみの有効性や二重化のみの有効性を測定しても、プロセスがもつ両方の管理策がはたして有効なものなのかを測定していなければ、バランスがとれた管理策の実施には繋がりません。プロセス全般のリスクを考慮した上で、管理策または一群の管理策の有効性を測定することが効果的です。

フィードバックとしては、
上記のようにプロセス全体を考慮して、管理策または一群の管理策の有効性について判定を導き出すことは当然重要ですが、これらの判定結果をどのように活用するかを考慮することも重要です。有効性測定結果のフィードバック先としては、以下のように考えることが可能です。

管理策または一群の管理策の有効性について測定した場合のフィードバック先

- ISMS 全体の有効性測定へのインプット
  ISMS 全体の有効性測定の一要素として活用する。
- リスクアセスメントプロセス
  プロセスの管理責任者やシステム管理者等に報告し、リスクアセスメント結果の妥当性確認や必要に応じて再リスクアセスメントを実施し、追加の管理策の必要性等を検討する。
- モニタリングプロセス
  測定する上で必要なモニタリングについて再検討する
- インシデント管理
  測定結果を基に、インシデント対応をするための基準等を再検討する
- 有効性測定プロセス
  測定結果を基に、測定方法自体や測定頻度などについて再検討する等

① リスクアセスメントプロセスへのフィードバック

上記のリスクアセスメントへのフィードバックに関して、ISMS 認証基準ではリスクアセスメント全体、及び残留リスク、特定したリスク受容可能レベルをあらかじめ定めた間隔でレビューすることを要求しています。リスクアセスメントのレビューでは、次に起きた変化を考慮することを要求しています。

4.2.3 ISMS の監視及びレビュー d) リスクアセスメントをあらかじめ定めた間隔でレビューする。残留リスク及び特定したリスク受容可能レベルをレビューする。これらのレビューでは，次に起きた変化を考慮する。 1) 組織 2) 技術

3) 事業の目的及びプロセス
4) 特定した脅威
5) 導入した管理策の有効性
6) 外部事情（例えば，法令又は規制の状況，契約上の義務，社会的風潮）

（JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

従って、導入した管理策の有効性の測定結果をリスクアセスメントにフィードバックし、必要に応じて再度、リスクアセスメントを実施する改善等に向けたアクションを取ることになります。

ISMS の有効性について測定した場合のフィードバック先

② マネジメントレビューへのフィードバック

マネジメントレビューのインプットとして活用し、ISMS の継続的な改善を検討する

ISMS 認証基準では、管理策の有効性に関する「ISMS のマネジメントレビュー」を以下のように規定しています。

7.2 レビューへのインプット
f) 有効性測定の結果
7.3 レビューからのアウトプット
a) ISMS の有効性の改善
e) 管理策の有効性測定方法の改善

（JIS Q 27001:2006　7 ISMS のマネジメントレビュー　より引用）

a) マネジメントレビューへのインプット

ISMS 認証基準では、以下の通り有効性測定の結果をマネジメントレビューへインプットすることを要求しています。

- 管理策の有効性測定結果から把握できた内容を、マネジメントレビューのインプットとする。
  - ✓ 各管理策の有効性測定結果
  - ✓ 各管理策の有効性評価結果
  - ✓ 有効性測定及び評価結果のまとめ

b) マネジメントレビューからのアウトプット

ISMS 認証基準では、以下の通りマネジメントレビューの結果、次の ISMS 有効性に関する決定や処置をアウトプットすることを要求しています。

- ISMS 全体について ISMS 基本方針や目的が達成されていない内容に関しての改善処置
- 各管理策の評価結果、有効でなかった管理策に対する改善処置
- 管理策の有効性測定結果により、有効でなかった管理策を発見できなかった等、管理策有効性測定に関して測定方法に要する改善処置

（2）管理策の有効性測定に関する計画

管理策の有効性を測定するためには、まずどのように測定するかを定義しておく必要があります。

ISMS 認証基準では、管理策の有効性測定の定義を以下のように規定しています。

> 4.2.2 ISMS の導入及び運用
> d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し，また，比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために，それらの測定をどのように利用するかを規定する［4.2.3c)参照］。
>
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

管理策の有効性測定を定義付ける場合、以下のような項目を考慮すると比較可能で再現可能な測定に役立つでしょう。

- 管理策の目的
  組織にとって当該管理策の目的は何なのかを明確化する。管理策を実施した結果、この目的を達成したかどうかが管理策が有効かどうかのポイントとなる。
- 測定する単位
  選択した管理策又は関連する管理策をグループ化した一群の管理策の単位で、測定を実施するのかを定義する。
- 有効性測定の方法
  有効性を測定するために必要な項目を定義する。
  また、その方法は比較可能で再現可能な結果を生み出す必要がある。
- 有効性を評価（判定）する方法
  測定された結果を基に、有効性を評価するための方法を定義する。
  また、その方法は比較可能で再現可能な結果を生み出す必要がある。
- 評価結果のフィードバック先
  評価結果のフィードバック先を定義する。
  評価結果は、管理策の有効性のレビュー及び ISMS 有効性のレビューで活用され、管理策や ISMS 全体が有効と認められない場合は、改善実施のために活用する。

① 有効性測定の方法に関するポイント

管理策の有効性測定を定義する場合、次の 2 つの視点を考慮すると、測定に対しレビューや判定を行なう上で有用であると考えられます。

管理策の有効性を測定するためには、まず何を測定するかを定義する必要があります。管理策有効性レビュー及び ISMS 有効性レビューのための活用を考慮して、例えば次の 2 つの項目の測定が考えられます。

a) 実施度

実施度は管理策を実装し運用した結果、計画した管理策に対してどの程度実施されたかを測定したものを言います。この測定値は、管理策の実装・運用の妥当性をチェックしたり、そのような実装・運用で不足しているものを特定するために使用します。

b) 達成度

達成度は計画した管理策を実施した結果、それに対して計画した管理目的が達成された程度（目的の達成度）を言います。この測定値は、セキュリティ管理策の実装・運用が、当初の当該管理策の目的や目標を達成するために有効に役割を果たしかどうか評価し、有効でない場合は管理策の実装・運用の仕方を改善するために使用します。

上記のように管理策の a)実施度、b)達成度を測定することにより、管理策の有効性を評価し、管理策の改善に向けた対応を実施することが可能となります。

② 有効性測定の実施例

前述の考慮事項を含む、有効性測定の実施のために有効だと思われる実施例を下表に示します。本表では、表中のステップ①からステップ⑩までの要領で、有効性測定を実施することを示しています。

目的	A.nn.n［管理目的タイトル記入］ 管理目的をそのまま転記する
管理策又は一群の管理策	A.nn.n.n［管理策タイトル記入］ 管理策をそのまま転記する
記述項目	記述内容
①管理策の目的、目標	当該組織における本管理策の目的は何なのかを具体的に記す。 その管理策を実施する事によって、具体的に何を実現しようとしているのか、或いはリスクをどう低減しようとしているのかを記す。 （注）この内容は、“目的の達成度”の測定に直接関連するので、充分考えて設定する必要がある。

②リスク	管理策に関連して想定されるリスクを挙げる。 （注）管理策に関連してリスクが直接的に想定できない場合は、“①管理策の目的、目標”から考える。
③測定の前提条件	実施度及び達成度を測定する前に、管理策を実施する前提として必要な事項を記す。 （注）“管理策が実施されている”と言う状況の明確な定義が必要であり、そう言う状況にある“対象”が識別されていることが必要である。すなわち、管理策の実施時にはその管理策の対象が識別されていなければならない（原則として測定式の分母として設定する）。
④測定項目	（１）実施度 ③の前提条件で定義した管理策を適用すべき対象に対して管理策が実施されている程度（実施度）を測定する。 （注）実施度を測定するための項目の設定には、各組織のセキュリティ標準書や手順書を参考にすることが出来る。これらが充分に整備されていない場合は、JIS Q 27002 の実施の手引に書かれている作業／行為／対策が、この実施度を設定する際に参考になる。 （２）達成度 ①で設定した管理策の目的／目標を達成したかどうかの程度（達成度）を測定する。 （注）例えば ・管理策の目的/目標に関係するインシデント発生 ・リスクアセスメント時に用いたリスクに関係するレベルの測定
⑤測定値(基礎データ)	（１）実施度を示す測定値（基礎データ） （２）達成度を示す測定値（基礎データ）
⑥測定責任組織(部門)	その管理策に関して実施責任を持っている部署 （１）実施度を示す測定値の測定組織 （２）達成度を示す測定値の測定組織 （３）実施度及び達成度より管理策の有効性を評価する組織
⑦測定の頻度	その管理策に関して測定する頻度 （１）実施度を示す測定値の測定頻度 （２）達成度を示す測定値の測定頻度
⑧有効性を評価するための算定式	④測定項目に基く算定式 （１）⑤実施度測定値（基礎データ）と③測定の前提で考慮した測定対象　等に基き、実施度を示す算定式を記す。 （２）⑤達成度測定値（基礎データ）と③測定の前提で考慮した測定対象　等に基き、達成度を示す算定式を記す。
⑨有効性指	管理策の有効性の評価（有効性指標）に関して記す。

標による評価	実施度であるから管理策で規定した個々の対応策の実施(実装及び運用)は 100%であるべきだが、実際はこの測定値は次のような特性を持つ。 目的・目標の設定により、測定の前提条件となる対象が異なり算定値が変わる。 測定の精度により算定値が変わる。管理策の目的・目標、成熟度により、測定に実装・運用する技術、費用等が異なり測定の精度が変わる。 対応策の不備・不足により有効性が損なわれる場合がある。又、実施度の未達成により、有効性が損なわれる場合がある。 達成度であるから、当該管理策の目的を達成したかどうかで計測するので、必ずしも 100%である必要はない。実際は、この測定値は次のような特性を持つ。 測定の前提条件となる対象の選択により算定値が変わる 実際は網羅的に 100%とはならない。例えば、 インシデント発生率が目標値以下に減少しているか リスクレベルが目標値以下に減少しているか 管理策の有効性の評価は、(1)実施度、及び(2)達成度の結果より、有効性の評価を行う。評価結果、管理策の実装・運用の改善は、次の段階である。例えば、 管理策を 100%実施(実施度)したにもかかわらず、目的を達成(達成度)していなければ、当該管理策として実施した対応策(実装及び運用)は有効でないと評価する。 有効でないと評価された管理策は、改善が必要となる。
⑩関連する他の管理策	例えば、 ・ 本管理策が実施されるために必要な他の管理策を記す。 ・ 本管理策の共通の管理目的・目標を持つ他の管理策を記す。
備考	例えば、JIS Q 27002:2006 実施の手引に有効な情報があれば参考にすることができる。

１２.３.２ 実行(Do)

ISMS 認証基準では、ISMS の監視及びレビュー(Check-点検)のステップにおいて、管理策有効性の測定の実施が要求されています。

4.2.3 ISMS の監視及びレビュー c) セキュリティ要求事項を満たしていることを検証するために, 管理策の有効性を測定する。 (JIS Q 27001:2006 4.2 ISMS の確立及び運営管理 より引用)

ここでは、前述の有効性測定の定義に従って、管理策の有効性測定を実行します。

そしてこれらの測定結果は、管理策の有効性レビュー及び ISMS の有効性レビューに使用されます。

ISMS 認証基準では、ISMS の有効性レビューについて以下のように規定しています。

> 4.2.3 ISMS の監視及びレビュー
> b) ISMS の有効性について定期的にレビューする。これには，ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは，セキュリティ監査の結果，インシデント，有効性測定の結果，提案，及びすべての利害関係者からのフィードバックを考慮する。
> （JIS Q 27001:2006　4.2 ISMS の確立及び運営管理　より引用）

ここでは、ISMS の有効性についての定期的なレビューが要求されています。ISMS 有効性レビューには、（1）ISMS 基本方針及び目的を満たしていることのレビューと（2）管理策のレビューとがあります。

（1）ISMS 基本方針及び目的を満たしていることのレビュー

- 導入した ISMS が、設定している ISMS 基本方針の各項目を満たしているかレビューする
- 導入した ISMS が、設定した ISMS の目的を満たしているかレビューする

（2）管理策の有効性のレビュー

- 管理策または一群の管理策に対して測定された結果に基づき、改善に向けた対応が必要かレビューを実施します。

（注記）

上記レビューには、

- セキュリティ監査の結果
- インシデント
- 有効性測定の結果
- 提案
- すべての利害関係者からのフィードバック　等

を考慮する必要があります。

１２.３.３　点検と処置（Check and Act）

管理策の有効性測定結果により、有効でなかった管理策を発見できなかった等、管理策有効性の測定方法に関しては、有効性測定のプロセスの中で監視し課題を発見して改善処置を取ります。管理策有効性の測定方法に関する課題としては、次のような場合が考えら

れます。このような場合、管理策有効性測定方法に関して改善処置をする必要があります。

- 有効性を判断するために管理目的を達成しているかどうかを正確に判断できるデータを測定できていない
- 有効性を判断するために管理策が実施できているかどうかを正確に判断できるデータを測定できていない
- 実施が充分出来ていないのに管理目的を達成していることが、有効性測定方法が不十分なことに起因している場合

１２.４　有効性測定手順書の概要例

ISMS 認証基準では、管理策の有効性に関する「文書化に関する要求事項」を以下のように規定しています。

> 4.3 文書化に関する要求事項
>
> 4.3.1 一般
>
> g) 情報セキュリティのプロセスを有効に計画，運用及び管理することを確実にするために，組織が必要とする文書化した手順。管理策の有効性をどう測定するか［4.2.2 d)参照］を記述するために，組織が必要とする文書化した手順。
>
> （JIS Q 27001:2006　4.3 文書化に関する要求事項　より引用）

これまでの有効性測定に関する内容をまとめて、以下に文書化する上で有用だと思われる項目を例示します。

「管理策有効性測定手順の概要」（例示）

１．管理策有効性測定概要
　　１－１　概要及び目的
　　１－２　適用範囲
　　１－３　改訂履歴
２．測定手法
　　２－１　管理策の目的/目標の設定
　　２－２　実施度と達成度
　　２－２　測定値及び算定式の定義
　　２－３　測定体制
３．有効性の評価
　　３－１　評価の方法
　　３－２　評価結果への対応
　　　３－２－１　有効であると評価された管理策
　　　３－２－２　有効でなく改善が必要と評価された管理策
　　　３－３－３　経過観察が必要と評価された管理策

添付１．管理策有効性測定票（管理策毎又は一群の管理策）

１３．個人情報保護ガイドラインへの対応

各省庁において公表されている個人情報保護ガイドラインは、個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき、事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針（ガイドライン）として定められたものです。経済産業省のガイドライン「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」（以下、経済産業省ガイドラインという）は、最も幅広い産業分野を網羅しています。また、ガイドラインは、主務大臣が法を執行する際の基準となるものです。そのため、個人情報取扱事業者は、個人情報保護ガイドラインに沿って必要な措置を講じなければなりません。組織は合理的な価値判断と資源配分により、個人情報保護ガイドラインに対応した社内体制を整備する必要があります。なお、用語の定義については、「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（平成 16 年 10 月　経済産業省）の「Ⅱ．法令解釈指針・事例　１．定義（法第２条関連）」を参照されたい。

１３.１ 個人情報取扱事業者の義務規定

１３.１.１ 個人情報の利用目的

個人情報の利用目的（法律第 15 条～第 16 条関連）をできる限り特定しなければなりません。また、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて個人情報を取扱うことは、原則として禁じられています。

これは、OECD８原則[17]の「目的明確化の原則（個人データの収集目的を明確にし、当該目的に矛盾しない範囲内において利用すべきとする原則）」と「利用制限の原則（本人の同意がある場合、法律に基づく場合以外は目的外利用を禁止する原則）」に対応しています。

１３.１.２ 個人情報の取得関連

個人情報の取得関連（法律第 17 条～第 18 条関連）は、偽りその他不正の手段により取得することを禁止しています。また、本人から直接書面等で個人情報を取得するときは利

[17] 個人情報の保護に配慮した OECD（経済協力開発機構）の８原則（プライバシー保護と個人データの国際流通についてのガイドライン）が 1980 年に勧告されました。

用目的を明示し、その他個人情報を取得したときは、あらかじめその利用目的を公表している場合を除いて、利用目的を通知又は公表しなければなりません。さらに、利用目的を変更した場合にも、変更された利用目的を通知又は公表しなければなりません。ただし、本人等の権利利益を害するおそれがある場合等には、その適用を受けません。

１３.１.３ 個人データの管理

（１）データ内容の正確性の確保（法律第 19 条関連）

個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤りなどを発見した場合の訂正の手続の整備、記録事項の更新、保存期間の設定などを行うことにより、個人データを正確かつ最新の内容に保つよう努めなければなりません（電話帳、カーナビゲーションシステム等の取扱いについての場合を除く）。この場合、保有する個人データを一律に又は常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すれば足ります。

（２）安全管理措置（法律第 20 条関連）

個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失又は毀損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的安全管理措置を講じなければなりません。その際、本人の個人データが漏洩、滅失又は毀損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況などに起因するリスクに応じ、必要かつ適切な措置を講じるものとします。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましいとされています。また、個人データの取扱いに関する規程等に記載することが望まれる事項についても示されています。

（３）従業者の監督（法律第 21 条関連）

個人情報取扱事業者は、第 20 条に基づく安全管理措置を順守させるよう、従業者に対し必要かつ適切な監督をしなければなりません。なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員も含まれます。

個人データの取扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリングを実施する場合は注意を要します。その際、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、

あらかじめ労働組合等に通知し、必要に応じて協議を行うことが望ましいとされています。また、その重要事項を定めたときは、労働者等に周知することが望ましいとされています。

（４）委託先の監督（法律第 22 条関連）

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、第 20 条に基づく安全管理措置を順守させるよう、受託者に対し必要かつ適切な監督をしなければなりません。「必要かつ適切な監督」には、委託契約において委託者である個人情報取扱事業者が定める安全管理措置の内容を契約に盛り込むとともに、当該契約の内容が順守されていることを、あらかじめ定めた間隔で定期的に確認することも含まれます。

また、委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要します。

個人データの取扱いを委託する場合に契約書への記載が望まれる事項は、次の通りです。

①委託者及び受託者の責任の明確化

②個人データの安全管理に関する事項

・個人データの漏洩防止、盗用禁止に関する事項
・委託契約範囲外の加工、利用の禁止
・委託契約範囲外の複写、複製の禁止
・委託処理期間
・委託処理終了後の個人データの返還、消去、廃棄に関する事項

③再委託に関する事項

・再委託を行うにあたっての委託者への文書による報告
・個人データの取扱状況に関する委託者への報告の内容及び頻度
・契約内容が順守されていることの確認
・契約内容が順守されなかった場合の措置
・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

１３.１.４ 個人データの第三者への提供

個人情報取扱事業者は、個人データを、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはなりません（法律第 23 条関連）。ただし、法令に基づく場合、人の生命、身体又は財産の保護に必要な場合、公衆衛生、児童の健全育成に特に必要な場合、国等に協力する場合には本人の同意なく第三者へ提供することができます。また、第三者提供におけるオプトアウトを行っている場合には、本人の同意なく個人データを第三者に

提供することができます。また、個人データの取扱いを外部へ委託することは第三者への提供にあたらないものとされています。

１３.１.５ 保有個人データの対応

個人情報取扱事業者は、保有個人データの利用目的、開示等の求めに応じる手続等を本人の知り得る状態に置かなければなりません。また、個人情報取扱事業者は、保有個人データの開示・訂正・利用停止等を求められたときは、遅滞なく当該保有個人データを開示するとともに、訂正・利用停止等を求められた場合には原則としてその措置を取らなければなりません。

１３．２ 義務規定に対する ISMS の対応

１３.２.１ 安全管理措置の内容と ISMS の対応

経済産業省ガイドラインにおける安全管理措置として、組織的、人的、物理的、技術的視点から情報セキュリティ対策を検討することが規定されています。

ISMS には、133 の管理策が規定されており、これらの管理策の中から個人情報保護対応として適切な安全管理策を選択することができます。ISMS 認証基準と「個人情報保護に関する経済産業分野ガイドライン」との対応は、附属書に示す通りです。

ここに附属書を示す目的の一つは、これから ISMS を用いて個人情報の保護を実現しようとする事業者が、ISMS 認証基準を参考にして策定するであろう各種の規程類等において、経済産業省ガイドラインの安全管理措置部分に規定されている要求事項をどこに記載することができるのか、その一例を示すことにあります。あるいは別の目的として、すでに ISMS を構築した事業者が、策定済みの ISMS に関連する各種の規程類において、経済産業省ガイドラインが安全管理措置として求める事項を実現しているかどうかを確認するための参考に資することにあります。

なお、ここに示した対応関係は、あくまで例示であり、必ずしも同表のように ISMS を構成しなくてはならない訳ではありません。また、同表に沿って ISMS の関連規程類を構成したからといって、直ちに経済産業省ガイドラインを満たしていることを保証するものではありません。さらに、表に沿って ISMS の関連規程類を構成しないからといって、経済産業省ガイドラインを満たしていないと直ちに結論づけることは妥当ではないことにも留意されたい。

１３.２.２ 個人情報保護法のその他の規定と ISMS の対応

(１)個人情報保護法規定に対応した組織作りと準拠規範

組織は、その仕事に際して個人情報を収集し、取扱うのであって、専ら個人情報を収集取り扱うことを目的として活動することは希有というべきでしょう。それは、個人特定情報は、たとえば株主など組織の構成員としての地位、取引における権利義務や責任の帰属点を示し、個人属性情報は、それらの権利義務の内容や、その人の評価など、他者との関係を表していることからも理解されることでしょう。このように個人情報は、権利義務の主体、責任の帰属点、権利義務の内容や人の評価など、権利義務で構成される私たちの社会になくてはならない要素として重要な機能を営んでいます。

そのため、個人情報保護法に対応した組織づくりは、個人情報を取り扱う組織の殆どの仕事の手順と管理の仕方を見直す、組織の再構築の様相を帯びることになります。

その際に組織が準拠すべき規範も多数に上ります。個人情報保護法に対応した組織作りは、個人情報保護法を具体化する「個人情報の保護に関する基本方針」（平成１６年４月２日閣議決定）（以下「基本方針」という）やこれに基づく各省ガイドライン、業界ガイドライン、組織のポリシー、組織が独自に採用する準拠規範(例えば JIS Q 15001:2006)などの個人情報に関するルールをはじめとして、もともとの事務を規定する契約、契約に関する法令などと整合させる必要があるからです。

(２)個人情報保護法に準拠した組織作りにおける ISMS の機能

このように組織が個人情報保護法へのコンプライアンスを実現しようとすれば、単に個人情報保護法や個人情報保護のルールだけに従う組織作りに終始するわけにはゆきません。また、多数の準拠すべきルールに従って組織を統制するには、個人情報を、他の情報資産と並ぶ企業の情報資産の一つとして把握し、その収集、取り扱いに係るすべての事務を対象として、個人情報保護法を含む、その組織に必要な規範に準拠するように設計し、その動きを設計通りに動かす組織と活動、教育、監視、見直し、継続的改善が必要になります。

ISMS は、個人情報保護法をはじめとして組織が必要とする多数の準拠規範に整合するように設計された企業の活動を、基本方針に則り、個人情報を含む情報資産すべてについて、これを取り扱う事務、これに適用される規範を識別し、それらが有するリスクを把握し、これを組織の基本方針、法の内容に従って、適切なリソース配分によって統制するマネジメントシステムです。個人情報保護法をはじめとするコンプライアンス経営を実現するために ISMS の構築がもっとも現実的で効果的である理由はここにあります。ISMS は、情報資産のセキュリティに関するリスクマネジメントシステムではありますが、企業活動の情報

資産への依存度が高まるにつれて、企業活動そのもののリスクマネジメントシステムとしても機能することが認識されつつあります。

なお、ISMS 認証基準の附属書 A「管理目的及び管理策」には、個人情報保護法の安全管理措置以外の規定に直接対応するものはありませんが、それは当然のことです。ISMS を構築する組織が従うべき法令は個人情報保護法に限られないからです。また、組織が従うべき法令は、組織に「これをせよ(命令)。これをするな(禁令)」と命じて、組織が実現すべき目標（いわばＷｈａｔ）を宣言しているのに対して、ISMS は、命令や禁令の定めた目標を情報セキュリティを確保してどう実現するかという方法論（いわばＨｏｗ）であり、管理目的及び管理策は、その ISMS を構築するにあたり参考とすべきベストプラクティスを示したものだからです。

(３)個人情報保護体制の実現と ISMS の機能

経済産業省ガイドラインは、個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格として、ISMS 認証基準の適用にあたり不可欠のものとされている JIS Q 27002 を挙げています。これは、ISMS のマネジメントシステムが、個人情報を含む情報資産を保護するため、十分でバランスのとれた適切な情報セキュリティ管理策を確保し、顧客及び他の利害関係者に対して信頼を与えるように設計されること（第１ 適用範囲 １．一般)、特に、ISMS の構築維持が、個人情報保護法の求める個人データの安全対策を行い、かつ、法を順守した組織づくりのリスクに対処するために極めて有効な機能を発揮することを評価したものといえるでしょう。

以下では、その具体的な現れを、基本方針や経済産業省ガイドラインの一部及び ISMS 認証基準の一部を例にとって説明します。

①　基本方針による体制構築の枠組みと ISMS

「基本方針」は、個人情報保護の基本理念にもとづき、国、地方公共団体、民間が積極的、かつ連携して個人情報保護に邁進することを求めており、特に第６項 個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項の(1) 個人情報取扱事業者に関する事項では、個人情報取扱事業者が行うべき重要な取り組みとして以下を求めています。

（ア）事業者の個人情報保護に関する考え方又は方針に関する宣言（プライバシーポリシー・プライバシーステートメント）の策定・公表
（イ）漏洩事件の際の事実関係の公表
（ウ）個人情報の安全管理に関する事業者内部の責任体制を確保する仕組みの整備
（エ）外部委託の際の責任の明確化と実効的監督体制の構築
（オ）教育研修の実施等を通じた従業者の啓発、個人情報保護意識の徹底

これらは、「基本方針」にもとづき実現すべき課題を定め、内部責任体制を確保してこれを実現し、実効的監督体制の確保と教育・研修による継続的見直しを図るというマネジメントシステムの中核的内容であり、マネジメントシステムを採用する ISMS が直ちに基本方針にもとづく体制構築に役立つことを明らかにしています。

② 経済産業省ガイドラインによる体制構築の枠組みと ISMS

また、経済産業省ガイドラインは、個人情報保護法の各本条ごとに具体的な解釈や例を示していまが、２０条の安全対策では、組織的安全管理措置として、以下を講じることを求めています。

（ア）個人データの安全管理措置を講じるための組織体制の整備
（イ）個人データの安全管理措置を定める規定等の整備と規定等に従った運用
（ウ）個人データの取扱状況を一覧できる手段の整備
（エ）個人データの安全管理措置の評価、見直し及び改善
（オ）事故又は違反への対処

これらは、ISMS のマネジメントシステムの中核的内容そのものです。ISMS の定めるマネジメントシステムの概要は以下の通りで、PDCA を明確に確保しようとするものであることが理解されます。

これらの規範に対応すべき適用範囲を明確にした上で
→組織としての明確な基本方針を鮮明にし、
→この基本方針を実現するための体制・組織を定めて、組織構成員に対して権限と責務を割り当て、教育を施し、
→組織全員で個人情報保護法対応の計画を立て、
→実施・運用し、
→運用状況を監査し、
→組織の責任においてこれを見直し継続的に改善する。

加えて、経済産業省ガイドラインは、【各項目について講じることが望まれる事項】を定めて、これらの記載を具体化する方策を示しています。これは、規格でマネジメントシステムの基本的枠組みを示し、これに続く管理策でその実現策を示すという ISMS の構成と同様です。

このように、個人情報保護法を具体化する「基本方針」も経済産業省ガイドラインも、その実現の枠組みとして ISMS のマネジメントシステムの枠組を背景に置いていることは明らかで、個人情報保護のための枠組みとして ISMS が極めて有効であることが理解できます。

③　プライバシーポリシーやステートメントと ISMS

「基本方針」は、事業者の個人情報保護に関する考え方又は方針に関する宣言（プライバシーポリシー・プライバシーステートメント）を策定・公表し、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、事業者が関係法令等を順守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要であるとしています（「基本方針」８頁)。

ISMS でも、その確立にあたり、基本方針を策定しますが、その基本方針は、「事業・組織・所在地・資産・技術の特徴の見地から、事業上及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮」したものでなければなりません（4.2.1 ISMS の確立 b)）。その結果、ISMS を確立した組織は、事業上の要求事項だけでなく、個人情報保護法など組織の意思にかかわらず適用を強制される法的規制要求事項、又は例えば JIS Q 15001:2006 など組織が自ら準拠することを選択した規制要求事項、例えばプライバシーマークの求めや外部委託事業者との契約にもとづく安全対策などの契約上のセキュリティ義務を考慮したものとなります。なお、上の例は、個人情報保護関連の要求を例としたものですが、ISMS の確立は、個人情報保護関連のルールに限らず組織が従うべきルールを洗い出した上で、これらを考慮して行われます。ISMS が個人情報保護法に限らず、広くコンプライアンス経営に適する組織を構築するのに役立つと言われる理由ここにあります。

その結果、例えば、準拠規範に JIS Q 15001:2006 を採用した組織に対する ISMS の認証は、その組織が JIS Q 15001:2006 に対応したマネジメントを構築していることの認証として機能します。

④　責任体制の構築と ISMS

「基本方針」は、個人情報の保護を適切に位置づける観点から、事業者の内部における責任体制を確保するための仕組みを整備することを求めています。

そのためには、組織が、個人情報保護法に適応するものとして設計されているか否かを把握し、また仮に設計されていたとしても、これに対する脅威、脆弱性、リスクを正しく把握することが重要です。

ISMS は、ISMS の確立維持のために必要な組織環境、並びにリスクマネジメントのための環境を整備し、さらに、リスクアセスメントについての体系的な取り組みを自ら構築し、実施します。策定されるリスクアセスメントについての体系的な取り組み方法は、構築されようとする ISMS に適しており、また、特定された事業上の情報セキュリティ要求事項、並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法を特定する必要があるとされています

こうして、組織は、自ら、最も適切な個人情報保護法をはじめとして組織が従うべき規範への準拠とそのリスクを把握する方法を定めることになるのです。(4.2.1c) リスクに対

する組織の取組み方を定義する）

⑤　監査体制・継続的改善と ISMS

「基本方針」は、事業者内部における責任体制を確保する仕組み（「基本方針」６（１）②）を求め、経済産業省ガイドライン（24 頁：2．個人情報取扱事業者の義務等 (3)個人データの管理 2）安全管理措置）は、実効的な監査体制と監査責任者のもとでの監査を求めています。

ISMS の構築は、こうした監視・監督・監査体制の整備と不断の見直しのために、以下のようなきめ細かな枠組みを設けています。

（ア）基本方針の策定にあたって

まず、ISMS は、基本方針の策定にあたっても、法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮し、情報資産に対するマネジメントがこれに準拠しているかどうかを監視・監督・監査する体制の整備と不断の見直しを求めます。

（イ）経営陣のコミットメント

そして、ISMS は、こうした体制を、経営陣のコミットメントによって確保します。経営陣は、ISMS の確立、導入、運用、監視、レビュー、維持及び改善に対するコミットメントをなします。ISMS は、この経営陣のコミットメントを証拠によって明らかにします。ISMS は、このコミットメントを、情報セキュリティ目的を満たすことの重要性及び情報セキュリティ基本方針に適合することの重要性、法のもとでの責任、並びに継続的改善の必要性を組織内に周知することなどの証拠によって明らかにすることを求めています（5.1 経営陣のコミットメント d)）。

（ウ）経営資源の提供

また、ISMS は、経営陣に対して、「法令及び規制の要求事項並びに契約上の情報セキュリティ義務を明確にし、これを扱うため、必要な経営資源を決定し、提供すること。」を求めています（5.2.1 経営資源の提供 c)）。

こうして ISMS の構築は、「法令及び規制の要求事項並びに契約上の情報セキュリティ義務を明確にし、これを扱う」ことができる組織づくりに役立つのです。

（エ）内部監査

さらに、ISMS では、組織は、その ISMS の管理目的、管理策、プロセス及び手順について、本基準の要求事項、関連する法令又は規制の要求事項に適合しているかを判断するため、あらかじめ定めた間隔で ISMS の内部監査を実施することとされています（6 内部監

査)。

(オ) マネジメントレビュー

ISMS ではこれらの監査・監督体制の維持のためにも、経営陣の理解と関与を求めており、ISMS の構築によって、組織を個人情報保護法をはじめとする法に準拠させるだけでなく、不断にこれを順守させるための経営陣の積極的関与がなされます。

また、組織は、過去の監査及びレビューの結果、利害関係者からのフィードバック、技術情報等、リスクアセスメントの資料、過去のマネジメントレビュー結果に対するフォローアップ、状況の変化、改善提案などあらゆる資料を駆使して、マネジメントレビューを行います。

(カ) 記録

こうしたレビューを可能とし、ISMS の有効性を常に把握するため、ISMS は、コントロールの実態を記録し、これを継続的改善に役立てています。すなわち、ISMS では、「記録は、要求事項への適合性及び ISMS の有効な運用の証拠を提供するために、作成し、維持しなければならない。記録は、関連する法令又は規制の要求事項及び契約上の義務を考慮して保護し、管理しなければならない。(4.3.3 記録の管理)」とされています。

(キ) 見直し・継続的改善

マネジメントレビューのアウトプットには、ISMS に影響を与える可能性がある内外の事象に対応するために、必要に応じた、情報セキュリティを実現する手順及び管理策の修正に関係する決定及び処置が含まれ、かつ、それらの事象には、法令又は規制の要求事項の変更が含まれます (7.3 レビューからのアウトプット)。

ISMS の見直し対象は、さらに残留リスクやリスク水準など、組織のリスクレベルの再設定や、新たな法環境への対応に及びます。たとえば、ISMS においては、「リスクアセスメントをあらかじめ定めた間隔でレビューする。残留リスク及び特定したリスク受容可能レベルをレビューする。これらのレビューでは, 外部事情 (例えば, 法令又は規制の状況, 契約上の義務, 社会的風潮) に起きた変化を考慮する。」旨が定められ (4.2.3 ISMS の監視及びレビューd)6)) いったん構築された ISMS そのものも、法的な規制環境が変化するのにつれて不断に見直しがなされます。個人情報保護法やガイドラインに限らず、変化の早い現在においては組織のリーガルコンプライアンスを維持するためにも ISMS は極めて有効です。

附属書
「JIS Q 27001」と「個人情報の保護に関する経済産業分野を対象とするガイドライン」との対応関係

【留意事項】

本表は「JIS Q 27001」と、「個人情報の保護に関する経済産業分野を対象とするガイドライン（以下、ガイドラインと呼ぶ）」における安全管理措置部分に規定されている要求事項との対応関係の例を示したものである。

ここで示した対応関係は、あくまで例示であり、必ずしも本表に示すように ISMS を構成しなくてはならない訳ではないし、これがガイドラインを満たしていることを保証するものではないことに留意されたい。

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
	管理目的及び管理策		**管理目的及び管理策**		
	表A.1に規定した管理目的及び管理策は，JIS Q 27002:2006の箇条5～15までに掲げられているものをそのまま取り入れて配列したものである。この表は，管理目的及び管理策のすべてを網羅してはいないので，組織は，管理目的及び管理策の追加が必要であると考えてよい。この表の中の管理目的及び管理策は，本体の4.2.1に規定するISMSのプロセスの一部として，選択しなければならない。				
	JIS Q 27002:2006の箇条5～15までは，A.5～A.15までに規定した管理策を支える，導入への助言及び最適な実施のための手引を提供している。				
A.5	**セキュリティ基本方針**	5	**セキュリティ基本方針**		
A.5.1	**A.5.1 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方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため。	5.1	**A.5.1 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方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため。 経営陣は，組織全体にわたる情報セキュリティ基本方針の発行及び維持を通じて，事業目的に沿った明確な情報セキュリティ基本方針の方向性を定め，情報セキュリティに対する支持及び責任を明示することが望ましい。		
A.5.1.1	A.5.1.1 **情報セキュリティ基本方針文書**	5.1.1	A.5.1.1 **情報セキュリティ基本方針文書**	【組織②】個人データの取扱いに関する規程等の整備とそれらに従った運用 【組織②】個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用 【組織②】個人データの取扱いに係る建物，部屋，保管庫等の安全管理に関する規程等の整備とそれらに従った運用 【組織②】個人データの取扱いを委託する場合における委託先の選定基準，委託契約書のひな型，委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用	①②③ ④⑤⑥
A.5.1.2	A.5.1.2 **情報セキュリティ基本方針のレビュー**	5.1.2	A.5.1.2 **情報セキュリティ基本方針のレビュー**	【組織④】監査責任者から受ける監査報告，個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善	①②③ ④⑤⑥
A.6	**A.6 情報セキュリティのための組織**	6	**情報セキュリティのための組織**		
A.6.1	**A.6.1 内部組織** 目的：組織内の情報セキュリティを管理するため。	6.1	**A.6.1 内部組織** 目的：組織内の情報セキュリティを管理するため。 組織内において情報セキュリティを導入し，その実施状態を統制するための管理上の枠組みを確立することが望ましい。 経営陣は，情報セキュリティ基本方針を承認し，セキュリティに対する役割を割り当て，組織全体にわたるセキュリティの実施を調整し，レビューすることが望ましい。 必要ならば，専門的な情報セキュリティの助言の出所を明らかにし，組織内で利用できるようにすることが望ましい。業界の動向に遅れないようにし，規格及び評価方法に目を配り，情報セキュリティインシデントに対処するときの適切な連絡窓口を確保するために，関係当局を含む，外部のセキュリティ専門家又はその一団との連絡網を築くことが望ましい。情報セキュリティに対して多角的に取り組むことが望ましい。		
A.6.1.1	A.6.1.1 **情報セキュリティに対する経営陣の責任**	6.1.1	A.6.1.1 **情報セキュリティに対する経営陣の責任**		
A.6.1.2	A.6.1.2 **情報セキュリティの調整**	6.1.2	A.6.1.2 **情報セキュリティの調整**		

※参考は，「BS 7799 PD 3005：2002 (第2部　管理策の選択)」における第12節に示した法的要求事項の根拠，又はその法的要求事項と併せてどの管理目的及び管理策を検討したらよいかについて該当する管理策を対応付けたものです，ただし，これが法的要求事項の完全な対応付けではないことに注意が必要です。これは組織がその固有の事業環境に基づいて，適用できる法的，法令上又は規制上の要求事項を識別し，これを受けてさらに満たすべきすべての追加の要求事項を識別し，確実にすることが望ましい。

①：知的財産権(IPR)及びソフトウェアの著作権
②：組織の記録の保護
③：データ保護及び個人情報の機密保持
④：情報処理設備の誤用の防止
⑤：暗号による管理策の規制
⑥：証拠

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.6.1.3	A.6.1.3 **情報セキュリティ責任の割当て**	6.1.3	A.6.1.3 **情報セキュリティ責任の割当て**	【組織①】従業者の役割・責任の明確化 【組織①】個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））の設置 【組織①】個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定 【組織①】個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定 【組織①】個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化 【組織①】監査責任者の設置 【組織①】監査実施体制の整備 【取得①】個人データを取得する際の作業責任者の明確化 【取得①】取得した個人データを情報システムに入力する際の作業責任者の明確化（以下、併せて「取得・入力」という。） 【移送①】個人データを移送・送信する際の作業責任者の明確化 【利用①】個人データを利用・加工する際の作業責任者の明確化 【保管①】個人データを保管・バックアップする際の作業責任者の明確化 【消去①】個人データを消去する際の作業責任者の明確化 【消去①】個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化	⑥
A.6.1.4	A.6.1.4 **情報処理設備の認可プロセス**	6.1.4	A.6.1.4 **情報処理設備の認可プロセス**		④
A.6.1.5	A.6.1.5 **秘密保持契約**	6.1.5	A.6.1.5 **秘密保持契約**	【人①】従業者の採用時又は委託契約時における非開示契約の締結	③
A.6.1.6	A.6.1.6 **関係当局との連絡**	6.1.6	A.6.1.6 **関係当局との連絡**	【組織①】漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備	⑥
A.6.1.7	A.6.1.7 **専門組織との連絡**	6.1.7	A.6.1.7 **専門組織との連絡**		
A.6.1.8	A.6.1.8 **情報セキュリティの独立したレビュー**	6.1.8	A.6.1.8 **情報セキュリティの独立したレビュー**	【組織④】監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施 【取得④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【取得④】アクセスの記録、保管と、権限外作業の有無の確認 【移送④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【移送④】アクセスの記録、保管と、権限外作業の有無の確認 【利用④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【利用④】アクセスの記録、保管と権限外作業の有無の確認 【保管④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【保管④】アクセスの記録、保管と権限外作業の有無の確認 【消去④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【消去④】アクセスの記録、保管、権限外作業の有無の確認	
A.6.2	**A.6.2 外部組織** 目的：外部組織によってアクセス，処理，通信，又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。	6.2	**A.6.2 外部組織** 目的：外部組織によってアクセス，処理，通信，又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。 外部組織の製品又はサービスの導入によって，組織の情報及び情報処理施設のセキュリティが弱められることは望ましくない。 外部組織による組織の情報処理施設へのアクセス，並びに情報の処理及び通信を管理することが望ましい。 組織の情報及び情報処理施設へのアクセスを要求する外部組織との活動が業務上必要となる場合，又は外部組織との間で製品及びサービスの受入れ若しくは提供を行う場合には，セキュリティ関連事項を決定し，要求事項を管理するためにリスクアセスメントを実施することが望ましい。管理策は，その外部組織との間で合意し，契約書に明記することが望ましい。		
A.6.2.1	A.6.2.1 **外部組織に関係したリスクの識別**	6.2.1	A.6.2.1 **外部組織に関係したリスクの識別**		①
A.6.2.2	A.6.2.2 **顧客対応におけるセキュリティ**	6.2.2	A.6.2.2 **顧客対応におけるセキュリティ**		
A.6.2.3	A.6.2.3 **第三者との契約におけるセキュリティ**	6.2.3	A.6.2.3 **第三者との契約におけるセキュリティ**	【人①】従業者の採用時又は委託契約時における非開示契約の締結 【組織②】個人データの取扱いを委託する場合における委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用	①

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.7	**A.7 資産の管理**	7	**資産の管理**		
A.7.1	**A.7.1 資産に対する責任** 目的: 組織の資産を適切に保護し，維持するため。	7.1	**A.7.1 資産に対する責任** 目的:組織の資産を適切に保護し，維持するため。 すべての資産を明らかにし，その管理責任者を指名することが望ましい。管理責任者をすべての資産について明確にし，適切な管理策を維持する責任を割り当てることが望ましい。組織が適切と判断した場合には，管理責任者は具体的な管理策の実施を委任してもよいが，資産の適切な保護に関する責任は管理責任者にとどまる。		
A.7.1.1	A.7.1.1 **資産目録**	7.1.1	A.7.1.1 **資産目録**	【組織③】個人データについて、取得する項目、明示･公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備 【組織③】個人データ取扱台帳の内容の定期的な確認による最新状態の維持	①②
A.7.1.2	A.7.1.2 **資産の管理責任者**	7.1.2	A.7.1.2 **資産の管理責任者**		
A.7.1.3	A.7.1.3 **資産利用の許容範囲**	7.1.3	A.7.1.3 **資産利用の許容範囲**		
A.7.2	**A.7.2 情報の分類** 目的: 情報の適切なレベルでの保護を確実にするため。	7.2	**A.7.2 情報の分類** 目的:情報の適切なレベルでの保護を確実にするため。 情報の必要性，優先順位及びその情報を取り扱う場合に期待する保護の程度を示すために，情報を分類することが望ましい。 情報の，取扱いに慎重を要する度合い及び重要性の度合いは様々である。情報によっては，保護レベルの引上げ又は特別な取扱いが必要なこともある。情報の分類体系は，一連の適切な保護レベルを定め，特別な取扱い方法の必要性を伝えるために利用することが望ましい。		
A.7.2.1	A.7.2.1 **分類の指針**	7.2.1	A.7.2.1 **分類の指針**		①②③
A.7.2.2	A.7.2.2 **情報のラベル付け及び取扱い**	7.2.2	A.7.2.2 **情報のラベル付け及び取扱い**	【組織②】個人データの取扱いに関する規程等の整備とそれらに従った運用 【取得②】取得･入力する際の手続の明確化 【移送②】個人データを移送･送信する際の手続の明確化 【利用②】個人データを利用･加工する際の手続の明確化 【保管②】個人データを保管･バックアップする際の手続の明確化 【消去②】消去･廃棄する際の手続の明確化 【物理②】氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管	①②③
A.8	**A.8 人的資源のセキュリティ**	8	**人的資源のセキュリティ**		
A.8.1	**A.8.1 雇用前** 目的: 従業員，契約相手及び第三者の利用者がその責任を理解し，求められている役割にふさわしいことを確実にするとともに，盗難，不正行為，又は施設の不正使用のリスクを低減するため。	8.1	**A.8.1 雇用前** 目的:従業員，契約相手及び第三者の利用者がその責任を理解し，求められている役割にふさわしいことを確実にするとともに，盗難，不正行為又は施設の不正使用のリスクを低減するため。 セキュリティの責任は，雇用に先立って，適切な職務定義書及び雇用条件において，言及することが望ましい。 従業員，契約相手及び第三者の利用者のすべての候補者について，十分に審査することが望ましい。特に，慎重を要する業務に就く者については，そうすることが望ましい。 従業員，契約相手及び情報処理施設の第三者の利用者は，セキュリティの役割及び責任についての契約書に署名することが望ましい。		
A.8.1.1	A.8.1.1 **役割及び責任**	8.1.1	A.8.1.1 **役割及び責任**	【組織①】従業者の役割･責任の明確化 【取得②】定められた手続による取得･入力の実施 【移送②】定められた手続による移送･送信の実施 【利用②】定められた手続による利用･加工の実施 【保管②】定められた手続による保管･バックアップの実施 【消去②】定められた手続による消去･廃棄の実施	
A.8.1.2	A.8.1.2 **選考**	8.1.2	A.8.1.2 **選考**		④⑤
A.8.1.3	A.8.1.3 **雇用条件**	8.1.3	A.8.1.3 **雇用条件**	【人①】従業者の採用時又は委託契約時における非開示契約の締結 【人①】非開示契約に違反した場合の措置に関する規程の整備	①②③ ④⑤⑥
A.8.2	**A.8.2 雇用期間中** 目的: 従業員，契約相手及び第三者の利用者の，情報セキュリティの脅威及び諸問題，並びに責任及び義務に対する認識を確実なものとし，通常の業務の中で組織の情報セキュリティ基本方針を維持し，人による誤りのリスクを低減できるようにすることを確実にするため。	8.2	**A.8.2 雇用期間中** 目的:従業員，契約相手及び第三者の利用者の，情報セキュリティの脅威及び諸問題，並びに責任及び義務に対する認識を確実なものとし，通常の業務の中で組織の情報セキュリティ基本方針を維持し，人による誤りのリスクを低減できるようにすることを確実にするため。 経営陣の責任は，組織内の構成員全体にセキュリティを適用することを確実にするために，明確にすることが望ましい。 起こり得るセキュリティリスクを最小とするために，すべての従業員，契約相手及び第三者の利用者にセキュリティ手順及び情報処理設備の正しい利用方法に関する十分なレベルの意識，教育及び訓練を与えることが望ましい。セキュリティ違反の取扱いに関する正式な懲戒手続を設けることが望ましい。		
A.8.2.1	A.8.2.1 **経営陣の責任**	8.2.1	A.8.2.1 **経営陣の責任**		

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.8.2.2	A.8.2.2 **情報セキュリティの意識向上，教育及び訓練**	8.2.2	A.8.2.2 **情報セキュリティの意識向上，教育及び訓練**	【人②】個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知 【人②】個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施 【人②】従業者に対する必要かつ適切な教育・訓練が実施されていることの確認	
A.8.2.3	A.8.2.3 **懲戒手続**	8.2.3		【人①】非開示契約に違反した場合の措置に関する規程の整備	①②③ ④⑤⑥
A.8.3	**A.8.3 雇用の終了又は変更** 目的：従業員，契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。	8.3	**A.8.3 雇用の終了又は変更** 目的：従業員，契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。 責任者は，従業員，契約相手及び第三者の利用者の組織からの離脱を管理し，すべての装置の返却及びすべてのアクセス権の解除の完了を確実にすることが望ましい。 組織内の責任及び雇用の変更は，この箇条に沿って対応する責任又は雇用の終了として管理することが望ましい。また，新規の雇用は，8.1に示すとおりに管理することが望ましい。		
A.8.3.1	A.8.3.1 **雇用の終了又は変更に関する責任**	8.3.1	A.8.3.1 **雇用の終了又は変更に関する責任**		
A.8.3.2	A.8.3.2 **資産の返却**	8.3.2	A.8.3.2 **資産の返却**		
A.8.3.3	A.8.3.3 **アクセス権の削除**	8.3.3	A.8.3.3 **アクセス権の削除**		
A.9	**A.9 物理的及び環境的セキュリティ**	9	**物理的及び環境的セキュリティ**		
A.9.1	**A.9.1 セキュリティを保つべき領域** 目的：組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。	9.1	**A.9.1 セキュリティを保つべき領域** 目的：組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。 重要又は取扱いに慎重を要する情報処理設備は，適切なセキュリティ障壁及び入退管理を伴う明確なセキュリティ境界によって保護された，セキュリティが保たれた領域の中に設置することが望ましい。これらの設備は，認可されていないアクセス，損傷及び妨害から，物理的に保護することが望ましい。 取る保護は，識別されたリスクに相応することが望ましい。		
A.9.1.1	A.9.1.1 **物理的セキュリティ境界**	9.1.1	A.9.1.1 **物理的セキュリティ境界**	【組織②】個人データの取扱いに係る建物，部屋，保管庫等の安全管理に関する規程等の整備とそれらに従った運用	②③④
A.9.1.2	A.9.1.2 **物理的入退管理策**	9.1.2	A.9.1.2 **物理的入退管理策**	【物理①】個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置	②③④
A.9.1.3	A.9.1.3 **オフィス，部屋及び施設のセキュリティ**	9.1.3	A.9.1.3 **オフィス，部屋及び施設のセキュリティ**	【組織②】個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用 【保管②】個人データを記録している媒体の遠隔地保管	②③④
A.9.1.4	A.9.1.4 **外部及び環境の脅威からの保護**	9.1.4	A.9.1.4 **外部及び環境の脅威からの保護**		
A.9.1.5	A.9.1.5 **セキュリティを保つべき領域での作業**	9.1.5	A.9.1.5 **セキュリティを保つべき領域での作業**	【物理①】個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施 【取得②】権限を与えられていない者が立ち入れない建物，部屋（以下「建物等」という。）での入力作業の実施 【利用②】権限を与えられていない者が立ち入れない建物等での利用・加工の実施 【消去②】権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施	②③④
A.9.1.6	A.9.1.6 **一般の人の立寄り場所及び受渡場所**	9.1.6	A.9.1.6 **一般の人の立寄り場所及び受渡場所**	【物理①】個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施	②③④
A.9.2	**A.9.2 装置のセキュリティ** 目的：資産の損失，損傷，盗難又は劣化，及び組織の活動に対する妨害を防止するため。	9.2	**A.9.2 装置のセキュリティ** 目的：資産の損失，損傷，盗難又は劣化，及び組織の活動に対する妨害を防止するため。 装置は，物理的及び環境的脅威から保護することが望ましい。 装置（構外で用いるもの及び移動するものを含む。）の保護は，情報への認可されていないアクセスのリスクを低減し，損失又は損傷から情報を保護するために必要である。装置の保護に関しては，装置の設置場所及び処分についても考慮することが望ましい。物理的な脅威から保護するため，また，サポート設備（例えば，電源，ケーブル配線施設）を保護するために，特別な管理策が要求される場合がある。		
A.9.2.1	A.9.2.1 **装置の設置及び保護**	9.2.1	A.9.2.1 **装置の設置及び保護**	【物理③】個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護	②③④
A.9.2.2	A.9.2.2 **サポートユーティリティ**	9.2.2	A.9.2.2 **サポートユーティリティ**	【物理③】個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護	②③④
A.9.2.3	A.9.2.3 **ケーブル配線のセキュリティ**	9.2.3	A.9.2.3 **ケーブル配線のセキュリティ**	【物理③】個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護	②③④
A.9.2.4	A.9.2.4 **装置の保守**	9.2.4	A.9.2.4 **装置の保守**		②③④

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.9.2.5	A.9.2.5 **構外にある装置のセキュリティ**	9.2.5	A.9.2.5 **構外にある装置のセキュリティ**	【技術⑥】移送時における紛失･盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化）	②③④
A.9.2.6	A.9.2.6 **装置の安全な処分又は再利用**	9.2.6	A.9.2.6 **装置の安全な処分又は再利用**	【消去②】個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に1回又は複数回上書きする。）	②③④
A.9.2.7	A.9.2.7 **資産の移動**	9.2.7	A.9.2.7 **資産の移動**	【移送②】定められた手続による移送･送信の実施	①②③④
A.10	**A.10 通信及び運用管理**	10	**通信及び運用管理**		
A.10.1	**A.10.1 運用の手順及び責任** 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。	10.1	**A.10.1 運用の手順及び責任** 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。 すべての情報処理設備の管理及び運用のための責任体制及び手順を確立することが望ましい。この手順には，適切な操作手順の策定を含む。不注意又は故意によるシステムの不正使用のリスクを低減するために，適切ならば，職務の分割を実施することが望ましい。		
A.10.1.1	A.10.1.1 **操作手順書**	10.1.1	A.10.1.1 **操作手順書**	【組織②】個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用	④
A.10.1.2	A.10.1.2 **変更管理**	10.1.2	A.10.1.2 **変更管理**	【技術⑦】情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証	
A.10.1.3	A.10.1.3 **職務の分割**	10.1.3	A.10.1.3 **職務の分割**	【技術②】個人データへのアクセス権限を付与すべき者の最小化 【技術②】アクセス権限を有する者に付与する権限の最小化	③④
A.10.1.4	A.10.1.4 **開発施設，試験施設及び運用施設の分離**	10.1.4	A.10.1.4 **開発施設，試験施設及び運用施設の分離**		④
A.10.2	**A.10.2 第三者が提供するサービスの管理** 目的: 第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。	10.2	**A.10.2 第三者が提供するサービスの管理** 目的:第三者の提供するサービスに関する合意に沿った，情報セキュリティ及びサービスの適切なレベルを実現し，維持するため。 組織は，提供されるサービスが第三者と同意したすべての要求事項を満たしていることを確実にするために，合意の実施状況を点検し，その合意への順守状況を監視し，また，順守状況の変化を管理することが望ましい。		
A.10.2.1	A.10.2.1 **第三者が提供するサービス**	10.2.1	A.10.2.1 **第三者が提供するサービス**	【組織②】個人データの取扱いを委託する場合における委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用	
A.10.2.2	A.10.2.2 **第三者が提供するサービスの監視及びレビュー**	10.2.2	A.10.2.2 **第三者が提供するサービスの監視及びレビュー**		
A.10.2.3	A.10.2.3 **第三者が提供するサービスの変更に対する管理**	10.2.3	A.10.2.3 **第三者が提供するサービスの変更に対する管理**		
A.10.3	**A.10.3 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。	10.3	**A.10.3 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。 必要とされるシステム性能を満たす十分な容量及び資源の可用性を確実にするためには，事前の計画及び準備を行う必要がある。 システムの過負荷のリスクを低減するために，将来の容量･能力の要求を予測することが望ましい。新しいシステムの運用上の要求事項を，その受入れ及び利用に先立って，設定し，文書化し，試験することが望ましい。		
A.10.3.1	A.10.3.1 **容量･能力の管理**	10.3.1	A.10.3.1 **容量･能力の管理**		
A.10.3.2	A.10.3.2 **システムの受入れ**	10.3.2	A.10.3.2 **システムの受入れ**		
A.10.4	**A.10.4 悪意のあるコード及びモバイルコード[3]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。 注3) モバイルコードとは，あるコンピュータから別のコンピュータへ移動するソフトウェアであって，利用者とのやり取りがほとんどない，又はまったくない状態で自動的に起動し，特定の機能を実行するものをいう。	10.4	**A.10.4 悪意のあるコード及びモバイルコード3)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。 悪意のあるコード及び認可されていないモバイルコード1)の侵入を防止し，検出するために予防対策が必要となる。 ソフトウェア及び情報処理設備は，悪意のあるコード（例えば，コンピュータウィルス，ネットワークワーム，トロイの木馬，ロジック爆弾，スパイウェア）に対してぜい弱である。利用者には，悪意のあるコードの危険性を知らせることが望ましい。管理者は，適切な場合には，悪意のあるコードを防止し，検知し，取り除くための管理策を導入することが望ましく，また，モバイルコードを管理することが望ましい。 注1) モバイルコードとは，あるコンピュータから別のコンピュータへ移動するソフトウェアであって，利用者とのやり取りがほとんどない，又は全くない状態で自動的に起動し，特定の機能を実行するものをいう。		
A.10.4.1	A.10.4.1 **悪意のあるコードに対する管理策**	10.4.1	A.10.4.1 **悪意のあるコードに対する管理策**	【技術⑤】ウイルス対策ソフトウェアの導入 【技術⑤】オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用 【技術⑤】不正ソフトウェア対策の有効性･安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）	②③④⑥
A.10.4.2	A.10.4.2 **モバイルコードに対する管理策**	10.4.2	A.10.4.2 **モバイルコードに対する管理策**		

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.10.5	**A.10.5 バックアップ** 目的: 情報及び情報処理設備の完全性及び可用性を維持するため。	10.5	**A.10.5 バックアップ** 目的:情報及び情報処理設備の完全性及び可用性を維持するため。 データのバックアップ取得と時機を失しないデータ復旧の訓練とに関する, 合意されたバックアップ方針及び戦略 (14.1参照) を実施するために, 日常の作業手順を確立することが望ましい。		
A.10.5.1	A.10.5.1 **情報のバックアップ**	10.5.1	A.10.5.1 **情報のバックアップ**	【保管②】個人データを記録している媒体を保管する場合の施錠管理 【保管②】個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理 【保管②】個人データを記録している媒体の遠隔地保管 【保管②】個人データのバックアップから迅速にデータが復元できることのテストの実施	②⑥
A.10.6	**A.10.6 ネットワークセキュリティ管理** 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。	10.6	**A.10.6 ネットワークセキュリティ管理** 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。 組織の境界を越えて広がることもあるネットワークのセキュリティ管理には, データの流れ, 法的背景, 監視, 保護についての注意深い考慮が必要である。 公衆ネットワークを通過する, 又は取扱いに慎重を要する情報の保護には, 追加の管理策が要求される場合もある。		
A.10.6.1	A.10.6.1 **ネットワーク管理策**	10.6.1	A.10.6.1 **ネットワーク管理策**	【技術⑥】盗聴される可能性のあるネットワーク (例えば, インターネットや無線LAN等) で個人データを送信 (例えば, 本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等) する際の、個人データの暗号化等の秘匿化	②③④
A.10.6.2	A.10.6.2 **ネットワークサービスのセキュリティ**	10.6.2	A.10.6.2 **ネットワークサービスのセキュリティ**		①②③④
A.10.7	**A.10.7 媒体の取扱い** 目的: 資産の認可されていない開示, 改ざん, 除去又は破壊, 及びビジネス活動の中断を防止するため。	10.7	**A.10.7 媒体の取扱い** 目的:資産の認可されていない開示, 改ざん, 除去又は破壊, 並びにビジネス活動の中断を防止するため。 媒体を管理し, かつ, 物理的に保護することが望ましい。 認可されていない (情報) 開示, 改ざん, 除去及び破壊から文書, コンピュータの媒体 (例えば, テープ, ディスク), 入力データ, 出力データ及びシステムに関する文書を保護するために, 適切な操作手順を確立することが望ましい。		
A.10.7.1	A.10.7.1 **取外し可能な媒体の管理**	10.7.1	A.10.7.1 **取外し可能な媒体の管理**	【物理②】個人データを含む媒体の施錠保管 【保管②】個人データを記録している媒体を保管する場合の施錠管理 【保管②】個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理 【保管②】個人データを記録している媒体の遠隔地保管	②③
A.10.7.2	A.10.7.2 **媒体の処分**	10.7.2	A.10.7.2 **媒体の処分**	【消去②】個人データが記録された媒体の物理的な破壊 (例えば、シュレッダー、メディアシュレッダー等で破壊する。)	③
A.10.7.3	A.10.7.3 **情報の取扱手順**	10.7.3	A.10.7.3 **情報の取扱手順**	【取得②】定められた手続による取得・入力の実施 【取得②】個人データを入力できる端末の、業務上の必要性に基づく限定 【移送②】個人データを移送・送信する場合の個人データの暗号化等の秘匿化 (例えば、公衆回線を利用して個人データを送信する場合) 【移送②】移送時におけるあて先確認と受領確認 (例えば、配達記録郵便等の利用) 【移送②】FAX等におけるあて先番号確認と受領確認 【移送②】個人データを記した文書をFAX機等に放置することの禁止 【利用②】個人データを利用・加工できる端末の、業務上の必要性に基づく限定 【保管②】個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化 【消去②】個人データを消去できる端末の、業務上の必要性に基づく限定	②③
A.10.7.4	A.10.7.4 **システム文書のセキュリティ**	10.7.4	A.10.7.4 **システム文書のセキュリティ**	【物理②】個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止	
A.10.8	**A.10.8 情報の交換** 目的: 組織内部で交換した及び外部と交換した, 情報及びソフトウェアのセキュリティを維持するため。	10.8	**A.10.8 情報の交換** 目的:組織内部で交換した及び外部と交換した, 情報及びソフトウェアのセキュリティを維持するため。 組織間での情報及びソフトウェアの交換は, 正式な交換方針に基づいていること, 情報交換に関する合意に沿って実施していること, また, いかなる関連法令をも順守していることが望ましい (箇条15参照)。 配送中の情報及び情報を格納した物理的媒体を保護するための手順及び標準を確立することが望ましい。		

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.10.8.1	A.10.8.1 **情報交換の方針及び手順**	10.8.1	A.10.8.1 **情報交換の方針及び手順**	【技術⑥】盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化 【移送②】FAX等におけるあて先番号確認と受領確認 【移送②】個人データを記した文書をFAX機等に放置することの禁止	③④⑤
A.10.8.2	A.10.8.2 **情報交換に関する合意**	10.8.2	A.10.8.2 **情報交換に関する合意**	【技術⑥】盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化	①③
A.10.8.3	A.10.8.3 **配送中の物理的媒体**	10.8.3	A.10.8.3 **配送中の物理的媒体**	【技術⑥】移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化）	③
A.10.8.4	A.10.8.4 **電子的メッセージ通信**	10.8.4	A.10.8.4 **電子的メッセージ通信**	【技術⑥】盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化	①③④⑤
A.10.8.5	A.10.8.5 **業務用情報システム**	10.8.5	A.10.8.5 **業務用情報システム**		①③④⑤
A.10.9	**A.10.9 電子商取引サービス** 目的：電子商取引サービスのセキュリティ，及びそれらサービスのセキュリティを保った利用を確実にするため。	10.9	**A.10.9 電子商取引サービス** 目的：電子商取引サービスのセキュリティ，及びそれらサービスのセキュリティを保った利用を確実にするため。 電子商取引サービス（オンライン取引を含む。）の利用に関連するセキュリティ上の影響及び管理策のための要求事項を考慮することが望ましい。公開されているシステムを通じて電子的に発行した情報の完全性及び可用性についても，考慮することが望ましい。		
A.10.9.1	A.10.9.1 **電子商取引**	10.9.1	A.10.9.1 **電子商取引**	【技術⑥】盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化	③④⑤
A.10.9.2	A.10.9.2 **オンライン取引**	10.9.2	A.10.9.2 **オンライン取引**		
A.10.9.3	A10.9.3 **公開情報**	10.9.3	A10.9.3 **公開情報**		①③④⑤
A.10.10	**A.10.10 監視** 目的：認可されていない情報処理活動を検知するため。	10.10	**A.10.10 監視** 目的：認可されていない情報処理活動を検知するため。 システムを監視することが望ましく，また，情報セキュリティ事象を記録することが望ましい。 システム運用担当者の作業ログ及び障害ログは，情報システムの問題を識別することを確実とするために利用することが望ましい。 組織は，監視及び記録の活動に適用されるすべての関連した法的要求事項を順守することが望ましい。 システムの監視は，採用している管理策の有効性の点検及びアクセス方針モデルに対する適合性の確認のために利用することが望ましい。		
A.10.10.1	A.10.10.1 **監査ログ取得**	10.10.1	A.10.10.1 **監査ログ取得**	【技術④】個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録） 【技術⑧】個人データへのアクセス状況（操作内容も含む。）の監視 【組織②】定められた規程等に従って業務手続が適切に行われたことを示す監査証跡の保持 【取得③】個人データの取得・入力業務を行う作業担当者に付与した権限の記録 【取得④】アクセスの記録、保管と、権限外作業の有無の確認 【移送③】個人データの移送・送信業務を行う作業担当者に付与した権限の記録 【移送④】アクセスの記録、保管と、権限外作業の有無の確認 【利用③】個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録 【利用④】アクセスの記録、保管と権限外作業の有無の確認	⑥

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
				【保管③】個人データの保管・バックアップ業務を行う作業担当者に付与した権限 (例えば、バックアップの実行、保管庫の鍵の管理等) の記録 【保管④】アクセスの記録、保管と権限外作業の有無の確認 【消去③】個人データの消去・廃棄を行う作業担当者に付与した権限の記録 【消去④】アクセスの記録、保管、権限外作業の有無の確認	
A.10.10.2	A.10.10.2 **システム使用状況の監視**	10.10.2	A.10.10.2 **システム使用状況の監視**	【保管②】個人データのバックアップに関する各種事象や障害の記録 【技術④】個人データへのアクセスや操作の成功と失敗の記録 (例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録) 【技術⑧】個人データを取り扱う情報システムの使用状況の定期的な監視	⑥
A.10.10.3	A.10.10.3 **ログ情報の保護**	10.10.3	A.10.10.3 **ログ情報の保護**		
A.10.10.4	A.10.10.4 **実務管理者及び運用担当者の作業ログ**	10.10.4	A.10.10.4 **実務管理者及び運用担当者の作業ログ**	【保管②】個人データのバックアップに関する各種事象や障害の記録 【技術④】個人データへのアクセスや操作の成功と失敗の記録 (例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録)	⑥
A.10.10.5	A.10.10.5 **障害のログ取得**	10.10.5	A.10.10.5 **障害のログ取得**	【保管②】個人データのバックアップに関する各種事象や障害の記録 【技術④】個人データへのアクセスや操作の成功と失敗の記録 (例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録)	⑥
A.10.10.6	A.10.10.6 **クロックの同期**	10.10.6	A.10.10.6 **クロックの同期**		⑥
A.11	**A.11 アクセス制御**	11	**アクセス制御**		
A.11.1	**A.11.1 アクセス制御に対する業務上の要求事項** 目的: 情報へのアクセスを制御するため。	11.1	**A.11.1 アクセス制御に対する業務上の要求事項** 目的:情報へのアクセスを制御するため。 情報・情報処理設備及び業務プロセスへのアクセスにおいては, 業務及びセキュリティの要求事項に基づいて管理することが望ましい。 アクセス制御規則には, 情報を伝える範囲及びアクセスの認可に対する方針を考慮することが望ましい。		
A.11.1.1	A.11.1.1 **アクセス制御方針**	11.1.1	A.11.1.1 **アクセス制御方針**	【取得③】個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定 【取得③】作業担当者に付与する権限の限定 【移送③】個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定 【移送③】作業担当者に付与する権限の限定 (例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。) 【利用③】個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定 【利用③】作業担当者に付与する権限の限定 (例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。) 【保管③】個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定 【保管③】作業担当者に付与する権限の限定 (例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。) 【消去③】個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定 【消去③】作業担当者に付与する権限の限定 【技術②】個人データを格納した情報システムへの同時利用者数の制限	①②③④
A.11.2	**A.11.2 利用者アクセスの管理** 目的: 情報システムへの, 認可された利用者のアクセスを確実にし, 認可されていないアクセスを防止するため。	11.2	**A.11.2 利用者アクセスの管理** 目的:情報システムへの, 認可された利用者のアクセスを確実にし, 認可されていないアクセスを防止するため。 情報システム及びサービスへのアクセス権の割当てを管理するための正式の手順が備わっていることが望ましい。 この手順は, 利用者アクセスのライフサイクル (すなわち, 新しい利用者の初期登録から, 情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除まで) におけるすべての段階を対象とすることが望ましい。アクセスの特権を与えると, システムの管理策ではその利用者を制御することができなくなる。適切な場合には, アクセス特権の付与を管理する必要性について, 特別の注意を払うことが望ましい。		

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.11.2.1	A.11.2.1 **利用者登録**	11.2.1	A.11.2.1 **利用者登録**	【技術③】個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。） 【技術③】個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施	①②③④⑥
A.11.2.2	A.11.2.2 **特権管理**	11.2.2	A.11.2.2 **特権管理**	【技術③】個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）	①②③④
A.11.2.3	A.11.2.3 **利用者パスワードの管理**	11.2.3	A.11.2.3 **利用者パスワードの管理**	【移送②】暗号鍵やパスワードの適切な管理	①②③④⑥
A.11.2.4	A.11.2.4 **利用者アクセス権のレビュー**	11.2.4	A.11.2.4 **利用者アクセス権のレビュー**	【技術③】個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）	①②③④
A.11.3	**A.11.3 利用者の責任** 目的：認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。	11.3	**A.11.3 利用者の責任** 目的：認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。 認可されてい る利用者間の協力は，有効なセキュリティのために不可欠である。 利用者に，有効なアクセス制御を維持するための自分自身の責任を認識させることが望ましい。特にパスワードのセキュリティ及び利用者が利用する装置のセキュリティに関して，その責任を認識させることが望ましい。 クリアデスク・クリアスクリーン2) 方針は，書類，媒体及び情報処理設備に対する認可されていないアクセス又は損傷のリスクを低減するために，実施することが望ましい。 注2) クリアデスクは，机上に書類を放置しないことである。また，クリアスクリーンは，情報をスクリーンに残したまま離席しないことである。		
A.11.3.1	A.11.3.1 **パスワードの利用**	11.3.1	A.11.3.1 **パスワードの利用**	【移送②】暗号鍵やパスワードの適切な管理 【保管②】暗号鍵やパスワードの適切な管理	①②③④⑥
A.11.3.2	A.11.3.2 **無人状態にある利用者装置**	11.3.2	A.11.3.2 **無人状態にある利用者装置**		①②③④
A.11.3.3	A.11.3.3 **クリアデスク・クリアスクリーン*方針**	11.3.3	A.11.3.3 **クリアデスク・クリアスクリーン**4)**方針**	【物理②】個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止 【物理②】離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止	①②③④
A.11.4	**A.11.4 ネットワークのアクセス制御** 目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。	11.4	**A.11.4 ネットワークのアクセス制御** 目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。 内部及び外部のネットワークを利用したサービスへのアクセスを，制御することが望ましい。 ネットワーク及びネットワークサービスへの利用者のアクセスは，次の条件を確実にすることによって，ネットワークサービスのセキュリティを損なわないことが望ましい。 a) 組織のネットワークと他の組織が管理するネットワーク又は公衆ネットワークとの間に適切なインタフェースを備える。 b) 利用者及び装置に適切な認証機構を適用する。 c) 情報サービスへの利用者アクセスを制御する。		
A.11.4.1	A.11.4.1 **ネットワークサービスの利用についての方針**	11.4.1	A.11.4.1 **ネットワークサービスの利用についての方針**		①②③④
A.11.4.2	A.11.4.2 **外部から接続する利用者の認証**	11.4.2	A.11.4.2 **外部から接続する利用者の認証**		①②③④⑥
A.11.4.3	A.11.4.3 **ネットワークにおける装置の識別**	11.4.3	A.11.4.3 **ネットワークにおける装置の識別**	【技術①】個人データへのアクセス権限を有する者が使用できる端末又はアドレス等の識別と認証（例えば、MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施	①②③④
A.11.4.4	A.11.4.4 **遠隔診断用及び環境設定用ポートの保護**	11.4.4	A.11.4.4 **遠隔診断用及び環境設定用ポートの保護**		①②③④
A.11.4.5	A.11.4.5 **ネットワークの領域分割**	11.4.5	A.11.4.5 **ネットワークの領域分割**		①②③④
A.11.4.6	A.11.4.6 **ネットワークの接続制御**	11.4.6	A.11.4.6 **ネットワークの接続制御**		①②③④
A.11.4.7	A.11.4.7 **ネットワークルーティング制御**	11.4.7	A.11.4.7 **ネットワークルーティング制御**		①②③④

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.11.5	**A.11.5 オペレーティングシステムのアクセス制御** 目的: オペレーティングシステムへの, 認可されていないアクセスを防止するため。	11.5	**A.11.5 オペレーティングシステムのアクセス制御** 目的:オペレーティングシステムへの, 認可されていないアクセスを防止するため。 オペレーティングシステムにアクセスする者を, 認可された利用者に限定するために, セキュリティ設備を用いることが望ましい。それらの設備は, 次の能力をもつことが望ましい。 a) 既定のアクセス制御方針に従って認可されている利用者本人であることの認証 b) システムへの認証の成功及び失敗の記録 c) 特別なシステム特権の使用の記録 d) システムセキュリティ方針に違反したときの警告発信 e) 認証のための適切な手段の提供 f) 適切な場合, 利用者の接続時間の制限		
A.11.5.1	A.11.5.1 **セキュリティに配慮したログオン手順**	11.5.1	A.11.5.1 **セキュリティに配慮したログオン手順**		①②③ ④⑥
A.11.5.2	A.11.5.2 **利用者の識別及び認証**	11.5.2	A.11.5.2 **利用者の識別及び認証**	【技術①】個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証(例えば、ID とパスワードによる認証、生体認証等)の実施 【取得③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【移送③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【利用③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【保管③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【消去③】IDとパスワードによる認証、生体認証等による作業担当者の識別	①②③ ④⑥
A.11.5.3	A.11.5.3 **パスワード管理システム**	11.5.3	A.11.5.3 **パスワード管理システム**		①②③ ④⑥
A.11.5.4	A.11.5.4 **システムユーティリティの使用**	11.5.4	A.11.5.4 **システムユーティリティの使用**		①②③ ④
A.11.5.5	A.11.5.5 **セッションのタイムアウト**	11.5.5	A.11.5.5 **セッションのタイムアウト**		①②③ ④
A.11.5.6	A.11.5.6 **接続時間の制限**	11.5.6	A.11.5.6 **接続時間の制限**	【技術②】個人データを格納した情報システムの利用時間の制限(例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等)	①②③ ④
A.11.6	**A.11.6 業務用ソフトウェア及び情報のアクセス制御** 目的: 業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。	11.6	**A.11.6 業務用ソフトウェア及び情報のアクセス制御** 目的:業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。 業務用ソフトウェアシステムへのアクセス及びその中でのアクセスを制限するために, セキュリティ機能を用いることが望ましい。 業務用ソフトウェア及び情報への論理的アクセスは, 認可されている利用者に制限することが望ましい。業務用ソフトウェアシステムは, 次の条件を満たすことが望ましい。 a) 既定のアクセス制御方針に従って, 情報及び業務用ソフトウェアシステム機能への利用者アクセスを制御する。 b) システム又は業務用ソフトウェアの制御を無効にできるユーティリティ, オペレーティングシステムのソフトウェア及び悪意のあるソフトウェアによる認可されていないアクセスから保護する。 c) 情報資源を共有している他の情報システムのセキュリティを脅かさない。		
A.11.6.1	A.11.6.1 **情報へのアクセス制限**	11.6.1	A.11.6.1 **情報へのアクセス制限**	【取得②】個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定(例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。) 【利用②】個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定(例えば、個人データを閲覧だけできる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。) 【技術②】識別に基づいたアクセス制御(パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。)の実施 【技術②】個人データにアクセス可能なアプリケーションの無権限利用の防止(例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等)	①②③ ④
A.11.6.2	A.11.6.2 **取扱いに慎重を要するシステムの隔離**	11.6.2	A.11.6.2 **取扱いに慎重を要するシステムの隔離**		①②③ ④

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.11.7	**A.11.7 モバイルコンピューティング及びテレワーキング**[5] 目的: モバイルコンピューティング及びテレワーキング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。 注5) モバイルコンピューティングとは，移動中又は外出先でコンピュータを利用することであり，テレワーキングとは，要員が，自分の所属する組織の外の決まった場所で，通信技術を用いて作業することである。	11.7	**A.11.7 モバイルコンピューティング及びテレワーキング** 目的：モバイルコンピューティング及びテレワーキング4) 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。 要求される保護は，これら特異な作業形態が引き起こすリスクに応じたものであることが望ましい。モバイルコンピューティングを用いるとき，保護されていない環境における作業のリスクを考慮し，適切な保護を施すことが望ましい。テレワーキングに関しては，組織は，テレワーキングを行う場所に保護を施し，この作業形態のために適切な取決めがあることを確実にすることが望ましい。 注4) モバイルコンピューティングとは，移動中，又は外出先でコンピュータを利用することであり，テレワーキングとは，要員が，自分の所属する組織の外の決まった場所で，通信技術を用いて作業することである。		
A.11.7.1	A.11.7.1 **モバイルのコンピューティング及び通信**	11.7.1	A.11.7.1 **モバイルのコンピューティング及び通信**		①③④⑤
A.11.7.2	A.11.7.2 **テレワーキング**	11.7.2	A.11.7.2 **テレワーキング**		①③④⑤
A.12	**A.12 情報システムの取得，開発及び保守**	12	**情報システムの取得，開発及び保守**		
A.12.1	**A.12.1 情報システムのセキュリティ要求事項** 目的: セキュリティは情報システムの欠くことのできない部分であることを確実にするため。	12.1	**A.12.1 情報システムのセキュリティ要求事項** 目的：セキュリティが情報システムに欠くことのできない部分であることを確実にするため。 情報システムには，オペレーティングシステム，システム基盤，業務用ソフトウェア，既成の製品，サービス及び利用者が開発したソフトウェアが含まれる。業務プロセスを支える情報システムの設計及び実装は，セキュリティへの影響が極めて大きい。セキュリティ要求事項は，情報システムを開発及び／又は実装する前に，特定し，合意することが望ましい。すべてのセキュリティ要求事項は，プロジェクトの要求仕様検討段階で特定して，その正当性を実証し，合意した上で，情報システムの包括的な作業の一環として，文書化することが望ましい。		
A.12.1.1	A.12.1.1 **セキュリティ要求事項の分析及び仕様化**	12.1.1	A.12.1.1 **セキュリティ要求事項の分析及び仕様化**		
A.12.2	**A.12.2 業務用ソフトウェアでの正確な処理** 目的: 業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。	12.2	**A.12.2 業務用ソフトウェアでの正確な処理** 目的：業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。 利用者が開発した業務用ソフトウェアを含め，正しい処理を確実にするために，業務用ソフトウェアに適切な管理策を設計して組み入れることが望ましい。これらの管理策には，入力データ，内部処理及び出力データの妥当性確認を含めることが望ましい。 慎重な取扱いを要する，価値の高い，又は重要な情報を処理するシステム，又はそれらに影響を及ぼすシステムには，更なる管理策が必要となる場合もある。そのような管理策は，セキュリティ要求事項及びリスクアセスメントに基づいて決めることが望ましい。		
A.12.2.1	A.12.2.1 **入力データの妥当性確認**	12.2.1	A.12.2.1 **入力データの妥当性確認**	【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施	
A.12.2.2	A.12.2.2 **内部処理の管理**	12.2.2	A.12.2.2 **内部処理の管理**	【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施	
A.12.2.3	A.12.2.3 **メッセージの完全性**	12.2.3	A.12.2.3 **メッセージの完全性**	【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施	
A.12.2.4	A.12.2.4 **出力データの妥当性確認**	12.2.4	A.12.2.4 **出力データの妥当性確認**	【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施	
A.12.3	**A.12.3 暗号による管理策** 目的: 暗号手段によって，情報の機密性，真正性又は完全性を保護するため。	12.3	**A.12.3 暗号による管理策** 目的：暗号手段によって，情報の機密性，真正性又は完全性を保護するため。 暗号による管理策の利用に関する方針を策定することが望ましい。暗号技術の利用を支持するために，かぎ管理を備えることが望ましい。		
A.12.3.1	A.12.3.1 **暗号による管理策の利用方針**	12.3.1	A.12.3.1 **暗号による管理策の利用方針**	【移送②】個人データを移送・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆回線を利用して個人データを送信する場合） 【移送②】移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用） 【保管②】個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化 【技術⑥】盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化	②③⑤
A.12.3.2	A.12.3.2 **かぎ（鍵）管理**	12.3.2	A.12.3.2 **かぎ（鍵）管理**	【移送②】暗号鍵やパスワードの適切な管理 【保管②】暗号鍵やパスワードの適切な管理	②③⑤

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.12.4	**A.12.4 システムファイルのセキュリティ** 目的: システムファイルのセキュリティを確実にするため。	12.4	**A.12.4 システムファイルのセキュリティ** 目的:システムファイルのセキュリティを確実にするため。 システムファイル及びプログラムソースコードへのアクセスを制御することが望ましい。ITプロジェクト及びサポート活動は，セキュリティを確保した上で実施することが望ましい。取扱いに慎重を要するデータが試験環境から漏えいすることを防止するように留意することが望ましい。		
A.12.4.1	A.12.4.1 **運用ソフトウェアの管理**	12.4.1	A.12.4.1 **運用ソフトウェアの管理**	【技術⑤】オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用	
A.12.4.2	A.12.4.2 **システム試験データの保護**	12.4.2	A.12.4.2 **システム試験データの保護**	【技術⑦】情報システムの動作確認時のテストデータとして個人データを利用することの禁止	
A.12.4.3	A.12.4.3 **プログラムソースコードへのアクセス制御**	12.4.3	A.12.4.3 **プログラムソースコードへのアクセス制御**		
A.12.5	**A.12.5 開発及びサポートプロセスにおけるセキュリティ** 目的: 業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。	12.5	**A.12.5 開発及びサポートプロセスにおけるセキュリティ** 目的:業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。 プロジェクト及びサポート環境は，厳しく管理することが望ましい。 業務用ソフトウェアシステムに責任をもつ管理者は，プロジェクト又はサポート環境のセキュリティにも責任を負うことが望ましい。変更によってシステム又は運用環境のセキュリティが損なわれないことを点検するために，管理者は，提案されているすべてのシステム変更のレビューを，確実にすることが望ましい。		
A.12.5.1	A.12.5.1 **変更管理手順**	12.5.1	A.12.5.1 **変更管理手順**	【技術⑦】情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証	
A.12.5.2	A.12.5.2 **オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー**	12.5.2	A.12.5.2 **オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー**		
A.12.5.3	A.12.5.3 **パッケージソフトウェアの変更に対する制限**	12.5.3	A.12.5.3 **パッケージソフトウェアの変更に対する制限**		
A.12.5.4	A.12.5.4 **情報の漏えい**	12.5.4	A.12.5.4 **情報の漏えい**	【技術⑤】オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用	
A.12.5.5	A.12.5.5 **外部委託によるソフトウェア開発**	12.5.5	A.12.5.5 **外部委託によるソフトウェア開発**		①
A.12.6	**A.12.6 技術的ぜい弱性の管理** 目的: 公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。	12.6	**A.12.6 技術的ぜい弱性の管理** 目的:公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。 技術的ぜい弱性の管理は，効果的，体系的及び再現可能な方法で，その効果を確かめるための測定を伴って実施することが望ましい。これらの考慮は，利用しているオペレーティングシステム及びあらゆる業務用ソフトウェアに適用することが望ましい。		
A.12.6.1	A.12.6.1 **技術的ぜい弱性の管理**	12.6.1	A.12.6.1 **技術的ぜい弱性の管理**	【技術②】個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証）	
A.13	**A.13 情報セキュリティインシデントの管理**	13	**情報セキュリティインシデントの管理**		
A.13.1	**A.13.1 情報セキュリティの事象及び弱点の報告** 目的: 情報システムに関連する情報セキュリティの事象及び弱点を，時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。	13.1	**A.13.1 情報セキュリティの事象及び弱点の報告** 目的:情報システムに関連する情報セキュリティの事象及び弱点を，時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。 事象の報告及び段階的取扱いの正式な手順を備えることが望ましい。すべての従業員，契約相手及び第三者の利用者に，組織の資産のセキュリティに影響を及ぼす場合がある様々な形態の事象及び弱点についての報告手順を認識させておくことが望ましい。すべての従業員，契約相手及び第三者の利用者に，いかなる情報セキュリティの事象及び弱点も，できるだけすみやかに指定された連絡先に報告するよう要求することが望ましい。		
A.13.1.1	A.13.1.1 **情報セキュリティ事象の報告**	13.1.1	A.13.1.1 **情報セキュリティ事象の報告**	【組織①】個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備 【組織①】個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 【組織①】漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 【組織①】漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備 【組織⑤】以下の(ア)から(カ)までの手順の整備 ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には，以下の対処をする必要はないものと考えられる。	②③④⑤⑥

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
				(ア)事実調査、原因の究明 (イ)影響範囲の特定 (ウ)再発防止策の検討・実施 (エ)影響を受ける可能性のある本人への連絡 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。	
				ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合） (オ)主務大臣等への報告 a. 個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合 認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。 ・機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合 ・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合 ・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合 ・その他認定個人情報保護団体が必要と考える場合 b. 個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合 経済産業大臣（主務大臣）に報告を行う。なお、認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。" (カ)事実関係、再発防止策等の公表 二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。 ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。 ・影響を受ける可能性のある本人すべてに連絡がついた場合 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合 （事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）	
A.13.1.2	A.13.1.2 **セキュリティ弱点の報告**	13.1.2	A.13.1.2 **セキュリティ弱点の報告**	【組織①】個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備	
A.13.2	**A.13.2 情報セキュリティインシデントの管理及びその改善** 目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。	13.2	**A.13.2 情報セキュリティインシデントの管理及びその改善** 目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。 情報セキュリティの事象及び弱点の報告があったとき直ちに，それらを効果的に取り扱える責任体制及び手順を備えることが望ましい。情報セキュリティインシデントへの対応，並びに情報セキュリティインシデントの監視，評価及び包括的管理に対して，継続的改善の手続をとることが望ましい。 証拠が必要となる場合は，法的要求事項を順守することを確実にするために，証拠を収集することが望ましい。		

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.13.2.1	A.13.2.1 **責任及び手順**	13.2.1	A.13.2.1 **責任及び手順**	【組織①】個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 【組織①】漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 【組織①】漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備 【組織⑤】以下の(ア)から(カ)までの手順の整備 ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。 (ア)事実調査、原因の究明 (イ)影響範囲の特定 (ウ)再発防止策の検討・実施 (エ)影響を受ける可能性のある本人への連絡 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。 ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合	②⑥
				・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合） (オ)主務大臣等への報告 a. 個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合 認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。 ・機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合 ・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合 ・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合 ・その他認定個人情報保護団体が必要と考える場合 b. 個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合 経済産業大臣（主務大臣）に報告を行う。なお、認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。" (カ)事実関係、再発防止策等の公表 二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。 ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。 ・影響を受ける可能性のある本人すべてに連絡がついた場合 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合 （事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）	
A.13.2.2	A.13.2.2 **情報セキュリティインシデントからの学習**	13.2.2	A.13.2.2 **情報セキュリティインシデントからの学習**		
A.13.2.3	A.13.2.3 **証拠の収集**	13.2.3	A.13.2.3 **証拠の収集**		⑥

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.14	**A.14 事業継続管理**	14	**事業継続管理**		
A.14.1	**A.14.1 事業継続管理における情報セキュリティの側面** 目的: 情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに, それらから重要な業務プロセスを保護し, また, 事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。	14.1	**A.14.1 事業継続管理における情報セキュリティの側面** 目的:情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに, それらから重要な業務プロセスを保護し, また, 事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。 組織への影響を最小に抑えるため, 及び予防的管理策と回復のための管理策との組合せによって, 情報及び情報処理施設に関連する資産の損失 (例えば, 自然災害, 事故, 装置の故障及び悪意による行為の結果の場合がある。) を受容可能なレベルにまで回復するために, 事業継続管理手続を実施することが望ましい。この手続では, 重要な業務プロセスを識別すること, 並びに運用, 要員配置, 資材, 配送及び設備といった点で関連する, 情報セキュリティ管理面以外の事業継続の要求事項と情報セキュリティ管理面の事業継続の要求事項とを統合することが望ましい。災害, セキュリティ不具合及びサービス停止の結果, 並びにサービスの可用性を, 事業の影響分析の対象とすることが望ましい。必要不可欠な運用の時機を失しない再開を確実にするために, 事業継続計画を策定し, 実施することが望ましい。情報セキュリティは, 組織の包括的な事業継続手続及びその他の管理手続の, 必要不可欠な部分であることが望ましい。 事業継続管理には, リスクを特定して低減するための管理策のほか, リスクアセスメントの手続に加え, 損害を与えるインシデントの影響を抑制するための管理策, 及び業務プロセスに必要な情報が常に利用可能であることを確実にするための管理策を含むことが望ましい。		
A.14.1.1	A.14.1.1 **事業継続管理手続への情報セキュリティ の組込み**	14.1.1	A.14.1.1 **事業継続管理手続への情報セキュリティ の組込み**		②
A.14.1.2	A.14.1.2 **事業継続及びリスクアセスメント**	14.1.2	A.14.1.2 **事業継続及びリスクアセスメント**		②
A.14.1.3	A.14.1.3 **情報セキュリティを組み込んだ事業継続計画の策定及び実施**	14.1.3	A.14.1.3 **情報セキュリティを組み込んだ事業継続計画の策定及び実施**		②
A.14.1.4	A.14.1.4 **事業継続計画策定の枠組み**	14.1.4	A.14.1.4 **事業継続計画策定の枠組み**		②
A.14.1.5	A.14.1.5 **事業継続計画の試験, 維持及び再評価**	14.1.5	A.14.1.5 **事業継続計画の試験, 維持及び再評価**		②
A.15	**A.15 順守**	15	**順守**		
A.15.1	**A.15.1 法的要求事項の順守** 目的: 法令, 規制又は契約上のあらゆる義務, 及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 注記 法的順守は, しばしば, コンプライアンスといわれることがある。	15.1	**A.15.1 法的要求事項の順守** 目的:法令, 規制又は契約上のあらゆる義務, 及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 情報システムの設計, 運用, 利用及び管理には, 法令, 規制及び契約上のセキュリティ要求事項が適用される場合がある。 特定の法的要求事項については, 組織の法律顧問又は適切な資格をもつ法律の実務家に助言を求めることが望ましい。法律の定める要求事項は, 国ごとに異なっており, また, 一つの国で作成され別の国へ伝送される情報 (すなわち, 国境を越えたデータの流れ) についても異なる場合がある。 注記 法的順守は, しばしば, コンプライアンスといわれることがある。		
A.15.1.1	A.15.1.1 **適用法令の識別**	15.1.1	A.15.1.1 **適用法令の識別**		①②③ ④⑤⑥
A.15.1.2	A.15.1.2 **知的財産権 (IPR)**	15.1.2	A.15.1.2 **知的財産権 (IPR)**		①
A.15.1.3	A.15.1.3 **組織の記録の保護**	15.1.3	A.15.1.3 **組織の記録の保護**	【技術④】採取した記録の漏えい、滅失及び き損からの適切な保護 【組織②】定められた規程等に従って業務手続が適切に行われたことを示す監査証跡の保持	②
A.15.1.4	A.15.1.4 **個人データ及び個人情報の保護**	15.1.4	A.15.1.4 **個人データ及び個人情報の保護**	『他に該当しないものすべて』	③
A.15.1.5	A.15.1.5 **情報処理施設の不正使用防止**	15.1.5	A.15.1.5 **情報処理施設の不正使用防止**		④
A.15.1.6	A.15.1.6 **暗号化機能に対する規制**	15.1.6	A.15.1.6 **暗号化機能に対する規制**		⑤
A.15.2	**A.15.2 セキュリティ方針及び標準の順守, 並びに技術的順守** 目的: 組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。	15.2	**A.15.2 セキュリティ方針及び標準の順守, 並びに技術的順守** 目的:組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。 情報システムのセキュリティは, 定めに従ってレビューすることが望ましい。 このようなレビューは, 適切なセキュリティ方針及び技術的基盤と対照して行うことが望ましい。また適用されるセキュリティ実施標準及び文書化されたセキュリティ管理策を順守していることについて, 情報システムを監査することが望ましい。		
A.15.2.1	A.15.2.1 **セキュリティ方針及び標準の順守**	15.2.1	A.15.2.1 **セキュリティ方針及び標準の順守**	【組織④】監査計画の立案と、計画に基づく監査 (内部監査又は外部監査) の実施 【組織④】監査実施結果の取りまとめと、代表者への報告 【組織④】監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善	
A.15.2.2	A.15.2.2 **技術的順守の点検**	15.2.2	A.15.2.2 **技術的順守の点検**	【技術②】個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証 (例えば、ウェブアプリケーションのぜい弱性有無の検証) 【技術⑤】不正ソフトウェア対策の有効性・安定性の確認 (例えば、パターンファイルや修正ソフトウェアの更新の確認)	

JIS Q 27001:2006 附属書A (規定)		JIS Q 27002:2006		経済産業分野を対象とするガイドライン (H20.2)	参考
項番	条文	項番	条文		
A.15.3	**A.15.3 情報システムの監査に対する考慮事項** 目的: 情報システムに対する監査手続の有効性を最大限にするため, 及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。	15.3	**A.15.3 情報システムの監査に対する考慮事項** 目的:情報システムに対する監査手続の有効性を最大限にするため, 及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。 情報システムの監査中には, 運用システム及び監査ツールを保護するための管理策があることが望ましい。 監査ツールの完全性を守るため, 及びその不正使用を防止するための保護も要求される。		
A.15.3.1	A.15.3.1 **情報システムの監査に対する管理策**	15.3.1	A.15.3.1 **情報システムの監査に対する管理策**		⑥
A.15.3.2	A.15.3.2 **情報システムの監査ツールの保護**	15.3.2	A.15.3.2 **情報システムの監査ツールの保護**		④⑥

おわりに

法規 WG メンバー

氏名	所属／役職
メンバー	
稲垣　隆一	稲垣隆一法律事務所 弁護士
大沼　靖秀	ＫＰＭＧビジネスアシュアランス㈱ 執行役員 ディレクター
駒瀬　彰彦	㈱アズジェント 取締役 技術本部長
松尾　正浩	㈱三菱総合研究所 経営コンサルティング本部 研究部長　主席研究員
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 パートナー
オブザーバー	
片山　博	ISMS 審査登録機関協議会(JISR)
井土　和志	経済産業省　商務情報政策局　情報セキュリティ政策室 課長補佐

2009 年 4 月

情報マネジメントシステム運営委員会/
ISMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会