16－H002

個人情報保護とリスクマネジメント

－JRMS個人情報保護編－

平成17年3月

財団法人　日本情報処理開発協会

KEIRIN この資料は、競輪の補助金を受けて作成したものです。

まえがき

（財）日本情報処理開発協会（JIPDEC）は、平成 16 年１月に情報化社会におけるリスクのインパクトへの対応の重要性に鑑みて『JIPDEC リスクマネジメントシステム（ＪＲＭＳ）解説書－「企業経営と情報リスクマネジメント分析」手法－』を公刊した。

情報リスクの影響が組織の命運を握る現代社会の情報システム環境において、ＪＲＭＳに対する認識の高まりには予想以上のものがあった。しかしながら、個人情報を取扱う事業者に係る個人情報の漏えい・窃盗等の問題がメディアで取り上げられ、組織にとり情報リスクへの対応がいかに重要な課題であるかが浸透しつつある現在、ＪＲＭＳの質問項目が個人情報保護に十分に堪えうるのか、またその有効性はどうなのか、種々検討する必要性が出てきた。

そこで、ＪＲＭＳの質問項目を見直した結果、基本的な部分で修正が必要であることが判明した。とりわけ、「個人情報の保護に関する法律（平成十五年法律五十七号）」が平成 17 年４月１日から全面施行になるという現実への対応という背景があった。

JIPDEC としては、社会的なニーズに応えるため、新たに「平成 16 年度マネジメントシステム評価検討委員会」を立ち上げることにした。当該委員会において、ＪＲＭＳ解説書の質問項目（1,004 項目）を見直し、個人情報の保護にとり必要と思われる部分（約 300 項目）を修正し、958 項目で構成する『ＪＲＭＳ個人情報保護編』を作成した。その検討の成果が本報告書である。

ＪＲＭＳ解説書においては、情報化社会の現実に照らして質問項目の再検討の必要性が生じること、そうした事態に対応するには不要と思われる項目を削除し、新たな項目を追加すれば、利便性を高めることができることを指摘しておいたが、まさに今日的な情報リスク環境において個人情報保護という重要な課題への対応が求められたのであった。

これまでに個人情報保護に関して種々の書物が刊行されており、参考にはなるが、リスクマネジメントの方法論・実践性という点からは必ずしも要件を満たしているとは思われない。情報リスクマネジメントシステムであるＪＲＭＳのツールを生かした『個人情報保護編』はまさに経営情報環境への対応にとり有効性を示すものといえる。たしかに、個人情報の保護について法律の条文解釈等は書物を通して理解することができるとしても、個人情報の漏えい等には組織が関係するものであり、経営陣、リスクマネジメント部門、情報システム部門、ユーザ部門等、それぞれの現場における個々人の情報システムと情報リスクに関する認識とリスク対応の実行が鍵を握っている。

しかも、リスクマネジメントの実践において重要なのは一人ひとりのリスクセンスやリスクマインドに拠ることが多いのである。そのためには、ＪＲＭＳ質問項目に対する関係者の回答から認識ギャップを明らかにし、問題点を抽出し、ソリューションを見出す努力が求められる。ＪＲＭＳの考え方を理解し、実践することが個人情報の保護についても有効であると思われる。本報告書が今日の情報システム社会において個人情報保護に役立つことを期待している。

平成 17 年３月

（財）日本情報処理開発協会

平成１６年度マネジメントシステム評価検討委員会　委員名簿

委員長	森宮　康	明治大学　商学部　教授
委　員	指田　朝久	東京海上日動リスクコンサルティング（株） リスクコンサルティング室情報グループグループリーダー
委　員	佐藤　厚夫	社団法人情報サービス産業協会　調査企画部　主任調査役
委　員	新保　史生	筑波大学大学院　図書館情報メディア研究科　助教授
委　員	鶴岡　眞	セコム情報システム（株）情報セキュリティ事業部 コンサルティング１Ｇ
委　員	原田要之助	（株）情報通信総合研究所　情報流通プラットフォーム研究グループ グループリーダー／エグゼクティブリサーチャー
委　員	山口　雅敏	（財）医療情報システム開発センター プライバシーマーク付与認定審査室

目　次

1．個人情報保護とは

「個人情報保護」の問題は、社会的に大きな関心事となっている。その理由は、個人情報保護関連五法の制定によって、従来は行政機関が取り扱う電子計算機処理された個人情報のみが法規制の対象となっていた状況から、民間の事業者が取り扱う個人情報についても法律の規制が及ぶことになったことが大きな要因となっている。しかし、法律の制定以前から、個人情報のコンピュータ処理やネットワーク利用が行われており、コンピュータの処理能力の向上やネットワークのブロードバンド化によって検索性の飛躍的な向上やデータベースに記録されている個人情報の相互参照および結合が容易になっている。それに伴い、個人情報の漏えいや不正利用に伴う弊害が顕著となり、その保護と適正な取扱いが求められてきた。

民間部門をも対象にした法律が制定されたことによって、個人情報の漏えいや不正利用に対してようやく法的責任が問われるようになったという誤解も多いが、個人の権利利益の侵害に対する法的責任は、法律の制定によって初めて問われるようになったものではないことはいうまでもない。

このように、個人情報保護への要請が高まっているのはたしかではあるが、人間が社会生活を営んでいくためには、自らの存在を証明するために個人情報を第三者に提供しなければならない場面も多い。買い物をする際にクレジットカードを利用したいのであれば、カードの利用申込みを行い、一定の審査を受ける必要がある。そして、カードの発行が可能であるかを判断するためには、その人物の収入や経済状況などの与信判断に必要な情報を調査する必要がある。その際には、必然的に詳細な個人情報の利用が不可欠となる。そのため、自分の個人情報を絶対的な保護下に置き、一切の公開を望まないのであれば、個人情報を開示しなければ利用できないサービスなどはまったく利用できないことになる。つまり、個人情報とは、「保護」することが重要であるだけでなく、「適正な取扱い」を行うことが「個人情報保護」の目的である。個人が一定の社会的な関係を築き、それを維持・向上させていくために個人情報を利用することは社会生活上必要であり、文化的な社会生活を遂行するうえで不可欠なことであるといえよう。

しかしながら、本人が公開を望まない情報を第三者へ開示したり、本人が同意した範囲を越えた利用や目的外の利用を行うことは、本人の権利利益を侵害することになる。それを防ぐために、個人情報の取扱いについて最低限のルールを定めた制度が「個人情報保護制度」である。

1.1　個人情報保護法・経済産業分野ガイドラインの求めるもの

個人情報保護法と呼ばれている法律は、民間部門を対象とする「個人情報の保護に関する法律（平成 15 年法律第 57 号）」を指すことが多い。しかし、平成 15 年 5 月 23 日に成立し、同月の 30 日に公布された法律は本法だけでなく、「行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）」、「独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）」、情報公開・個人情報保護審査会設置法（平成 15 年法律第 60 号）、行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関す

る法律（平成 15 年法律第 61 号）の５つの法律が制定され、これらの法律を「個人情報保護関連五法」と呼んでいる。

さらに、個人情報保護関連五法に加えて、個人情報保護に関する政府の基本的な方針を定めた「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）が制定されている。

その他、「個人情報の保護に関する法律の一部の施行期日を定める政令」（平成 15 年 12 月 10 日政令第 506 号）、「個人情報の保護に関する法律施行令」（平成 15 年 12 月 10 日政令第 507 号）、「個人情報の保護に関する法律施行令の一部を改正する政令」（平成 16 年 12 月 10 日政令第 389 号）、「行政機関の保有する個人情報の保護に関する法律の施行期日を定める政令」（平成 15 年 12 月 25 日政令第 547 号）、「行政機関の保有する個人情報の保護に関する法律施行令」（平成 15 年 12 月 25 日政令第 548 号）、「独立行政法人等の保有する個人情報の保護に関する法律施行令」（平成 15 年 12 月 25 日政令第 549 号）、「情報公開・個人情報保護審査会設置法施行令」（平成 15 年 12 月 25 日政令第 550 号）、「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係政令の整備等に関する政令」（平成 15 年 12 月 25 日政令第 551 号）、「行政機関の保有する個人情報の保護に関する法律に係る行政手続等における情報通信の技術の利用に関する法律施行規則」（平成 16 年 10 月７日総務省令第 125 号）、「独立行政法人等の保有する個人情報の保護に関する法律に係る行政手続等における情報通信の技術の利用に関する法律施行規則」（平成 16 年 10 月７日総務省令第 126 号）、「行政機関の保有する個人情報の適切な管理のための措置に関する指針」（平成 16 年９月 14 日総務省）、「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針」（平成 16 年９月 14 日総務省）が制定されている。

これらの法令は、民間部門や公的部門でそれぞれ適用分野が異なる。

「個人情報の保護に関する法律」（以下、「個人情報保護法」という。）個人情報保護法の第３条「基本理念」、第２章および第３章は、民間部門、公的部門を問わず、全分野に包括的に適用される。ここでは、基本理念、国および地方公共団体の責務等、および個人情報保護に関する施策等について定めている。

個人情報保護関連五法の義務規定の適用関係は、民間部門と公的部門で区別される。民間部門に適用されるのは個人情報保護法である。公的部門のうち、行政機関については行政機関個人情報保護法、独立行政法人等については独立行政法人等個人情報保護法がそれぞれ適用される。両機関に対する個人情報の開示等の請求に係る不服申立の審査等は、情報公開・個人情報保護審査会設置法に基づいて設置される審査会が行う。

なお、地方公共団体については、個人情報保護関連五法は適用されず、地方公共団体の個人情報保護条例が適用される。

これらの法令に加えて、各省庁の主務大臣が法を執行するための基準として、個人情報保護法第８条に基づいて各省庁が告示する省庁ガイドラインが制定されている。

省庁ガイドライン制定の目的は、個人情報保護法が事業分野ごとに主務大臣が所管する形をとっていることから、事業所管分野ごとに個人情報の保護の推進に関するガイドラインの策定・見直しを行うことにある。

ガイドラインを策定または見直す目的としては、いくつかの目的をあげることができる。まず、個人情報保護法の解釈の基準を明確にすることがあげられる。個人情報保護法の規定には、具体

的な基準を法律では定めずに、法改正を伴わずにその内容の見直しができるよう政令に委ねられている「政令事項」とされている点が多い。また、義務規定の内容についても、「できる限り」といった表現にも見られるように、具体的な判断基準が条文解釈からは必ずしも明確に示されておらず、その判断が、事実上、各個人情報取扱事業者の判断に委ねられている部分もあることから、その基準をガイドラインにおいて明確にすることがあげられる。

また、事業分野ごとに個人情報の取扱実態は大きく異なる。したがって、それに応じて必要と考えられる手続や基準を明確にすることが求められ、政令事項となっている部分も含めて、解釈基準を明確にする上で必要な事柄をガイドラインで定める必要がある。

さらに、個人情報保護法が事業所管分野ごとに主務大臣を指定する仕組みをとっていることもガイドラインの役割が大きい理由となっている。主務大臣の役割は、事業者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こと、そして、個人情報保護法の執行である。その際に、ガイドラインが当該支援を行うための指針となり、かつ、法を執行する際の基準との役割を果たすこととなる。

これらのガイドラインの一つとして、事業分野全般を対象とする経済産業分野ガイドラインがある。このガイドラインは、経済産業省および厚生労働省共管で策定され、「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（厚生労働省・経済産業省告示第4号）」として平成16年10月22日に告示された。

ガイドライン策定にあたっての検討は、「ガイドライン検討委員会」において行われた。経済産業分野ガイドラインが対象とする事業分野は、「事業全般」であり、他の分野とは異なり、特定の事業所管分野を対象とするわけではない。そのため、ガイドラインの内容も個人情報保護法の解釈基準の明確化に重点が置かれた内容となっており、特定事業分野において特に求められる個人情報の取扱手続などを別途定めるものとはなっていない。

経済産業分野ガイドラインの特色としては、①保護法の条文の趣旨の明確化、②実用性、③モデル規定としての役割などがあげられる。

はじめに、①保護法の条文の趣旨の明確化である。個人情報保護法に基づいて個人情報取扱事業者が必要最低限求められる義務について、ガイドラインでは業種を横断的に規定しており、適用対象は個人情報取扱事業者一般であることから、事実上、個人情報保護法の解釈準則としての役割を果たすものである。

また、ガイドラインは主務大臣の関与にあたっての判断基準としての役割も果たすことになる。そのため、ガイドラインに基づいて個人情報の適正な取扱いを行うにあたって、事業者の規模や取組状況によっては、必ずしもすべての要求事項を満たした対応がなされることを期待することは困難である。そのため、個人情報の取扱手続については、「しなければならない」とする事項と「望ましい」とする事項に分けたうえで、前者については事業者が講じなければならない義務として、一方、後者については、より適正な取扱いや実効性ある安全管理措置を講ずるにあたっては対応することが望ましい事項として区別している。

よって、「しなければならない」と記載されている規定については、それに従わなかった場合は、経済産業大臣によって法の規定違反と判断され得る。一方、「望ましい」と記載されている規定については、その規定に従わなかった場合でも、法の規定違反と判断されることはない。「望ましい」と記載されている規定は、それを遵守しなかった場合に法の規定違反とは判断され

ないものの、保護法第３条の定める「基本理念」に鑑みても個人の権利利益保護のための適正な取扱いにあたって求められるものであり、個人情報の保護と適正な取扱いを実効あらしめるためには可能な限り取り組むことが求められるものである。

なお、個人情報の保護と適正な取扱いにあたっては、保護法第１条の定めるとおり「保護」と「有用性」に配慮することが求められ、当然のことながら公益上必要な活動や正当な事業活動を制限するような取組みが求められているわけではない。

②実用性については、具体例の列挙と推奨規定をあげるなど、個人情報保護法への具体的対応の内容がわかりやすく平易な表現で書かれている点に特徴がある。個人情報保護法の義務規定の解釈にあたっては、条文解釈だけでは定義規定やその他の文言解釈や、適正な取扱いの具体的レベルが必ずしも明確ではない点が多い。そのため、保護法の規定を解釈するにあたって、その解釈を補完する役割を果たす「具体的事例」を列挙している。

このように、ガイドラインの規定だけでなく、解釈準則としての機能も具備するものとしては、「電子商取引に関する準則」があるが、経済産業分野ガイドラインが列挙している具体的事例も、電子商取引に関する準則で示されているような具体的事例の例示が念頭に置かれている。

さらに、解釈準則としての機能を有しつつ、実用性の観点から、コンプライアンス・プログラムを念頭に置いた「推奨規定」が定められている点も特徴である。特に、安全管理措置に関する義務規定は、保護法の条文では抽象的な内容が規定されているにすぎない。そのため、具体的な安全管理措置義務の内容を、保護法の解釈から導き出すのは至難である。現に、個人情報の安全管理のための対策のレベルは事業者ごとに千差万別であり、安全管理措置を講ずるうえで必要な一定の基準を明確にすることが求められてきた。そのような背景から、条文では抽象的な規定にとどまっている安全管理措置義務の内容を、ガイドラインでは「組織」、「人」、「物」、「技術」の４つの側面から具体的対応事項を示している。

最後に、③モデル規定としての役割についてである。個人情報保護法の義務規定は最低限のルールを定めているにすぎないことから、個別分野において個別・具体的に対応が必要な措置を講ずるために、各分野の商取引慣行等を踏まえて必要に応じてガイドライン等を策定することになる。経済産業分野との関係において策定されるガイドラインや指針としては、個人信用情報および個人遺伝情報などの個別分野ごとの経済産業省ガイドライン、認定個人情報保護団体における個人情報保護指針、業界団体等における自主ガイドライン等である。

経済産業分野ガイドラインの主な規定内容は、①ガイドラインの「目的」規定、②保護法により定義される「用語」の具体的な内容、③保護法が定める個人情報取扱事業者の義務の内容、である。

①ガイドラインの「目的」規定については、前述の各省庁ガイドライン制定の根拠等も含め、ガイドラインの策定目的と役割について記述されている。

②保護法により定義される「用語」の具体的な内容については、保護法の定義規定に加えて、保護法の条文において用いられている用語の具体的な解釈を明示することによって、各規定の解釈の際の判断基準を明確化することが目的となっている。

③保護法が定める個人情報取扱事業者の義務の内容については、単に、保護法の義務規定の内容を列挙するのではなく、具体例も踏まえて義務規定の内容をわかりやすく解説している点に特徴がある。

その他、インハウス情報の取扱いに関する部分については、保護法によって主務大臣は厚生労働大臣と指定されていることから、厚生労働省との協議によって策定されている。そのため、経済産業分野ガイドラインは、経済産業大臣が法を執行する際の基準となるものではあるものの、雇用管理に関する従業員の個人情報の取扱いに関係する部分については、「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（厚生労働省告示第259号）との整合性に留意する形となっている。

1.2 個人情報の取扱いに係るリスク

個人情報は適正ではない取扱いをすることによって本人の権利利益を侵害するおそれがある。では、個人情報の取扱いに係るリスクとして、「適正ではない」取扱いとはどのような行為を指すのであろうか。

まず、個人情報の「漏えい」はその顕著な例である。本来、第三者に提供したり開示しない情報が、本人の意思に反して提供されることは本人の権利利益を侵害するおそれが高い。とりわけ、個人の身体や財産、信用等のいわゆるセンシティブ性が高い個人情報は、第三者がそれらを不正に取得して利用することにより本人の社会生活上著しい不利益を伴うこともある。

「不正利用」も本人の権利利益を侵害するおそれが高い。ただし、不正利用とは、当初の利用目的以外の目的で個人情報を利用する目的外利用のことを指すのか、利用にあたって何らかの不正行為が介在する利用を指すのかは必ずしも定かではない。しかし、いずれの場合においても、本人が当該個人情報の利用について、事前に把握している利用目的や利用態様とは異なる目的や態様で利用されることになり、結果的に、本人の権利利益が侵害されることがある。

不正確な個人情報が利用されることによって生ずる問題もある。たとえば、違法行為に従事した第三者の個人情報と自分の情報が誤って利用されるようなことがあると、社会生活上不利益を被るおそれがある。

その他、個人情報の全部または一部の「滅失」や「き損」によって、本来利用できるはずの個人情報が利用できなくなることによって生ずる弊害などの問題もある。

このように、個人情報の取扱いにあたっては、「漏えい」だけがリスクではなく、その取扱い全般にわたって何らかの問題が生じると本人に直接不利益が及ぶ可能性が高いという問題がある。

2．ＪＲＭＳの考え方を基にした個人情報保護のリスク対応

現代社会においては、あらゆる組織は何らかの形で個人情報に関与している。しかも、情報リスクの視点からアプローチは必ずしも十分とはなっていない。しかし、個人情報保護法の施行により状況は一変する。したがって、情報リスクについての対応の可否は組織の信頼性と深く係ることになった。個人情報に係るリスク対応のため、ＪＲＭＳの考え方に従い展開することから、まずＪＲＭＳについて簡潔に触れておくことにする。

2.1　ＪＲＭＳとは

2.1.1　ＪＲＭＳの構造

ＪＲＭＳは情報リスク対応のため脆弱性分析を採用した方法論に基づいている。組織の脆弱性を認識するには、関係者のリスク認識の度合いについてＪＲＭＳの質問項目を通して把握し、そこから現状を捉えることになる。ＪＲＭＳの構造を示したのが図２－１である。

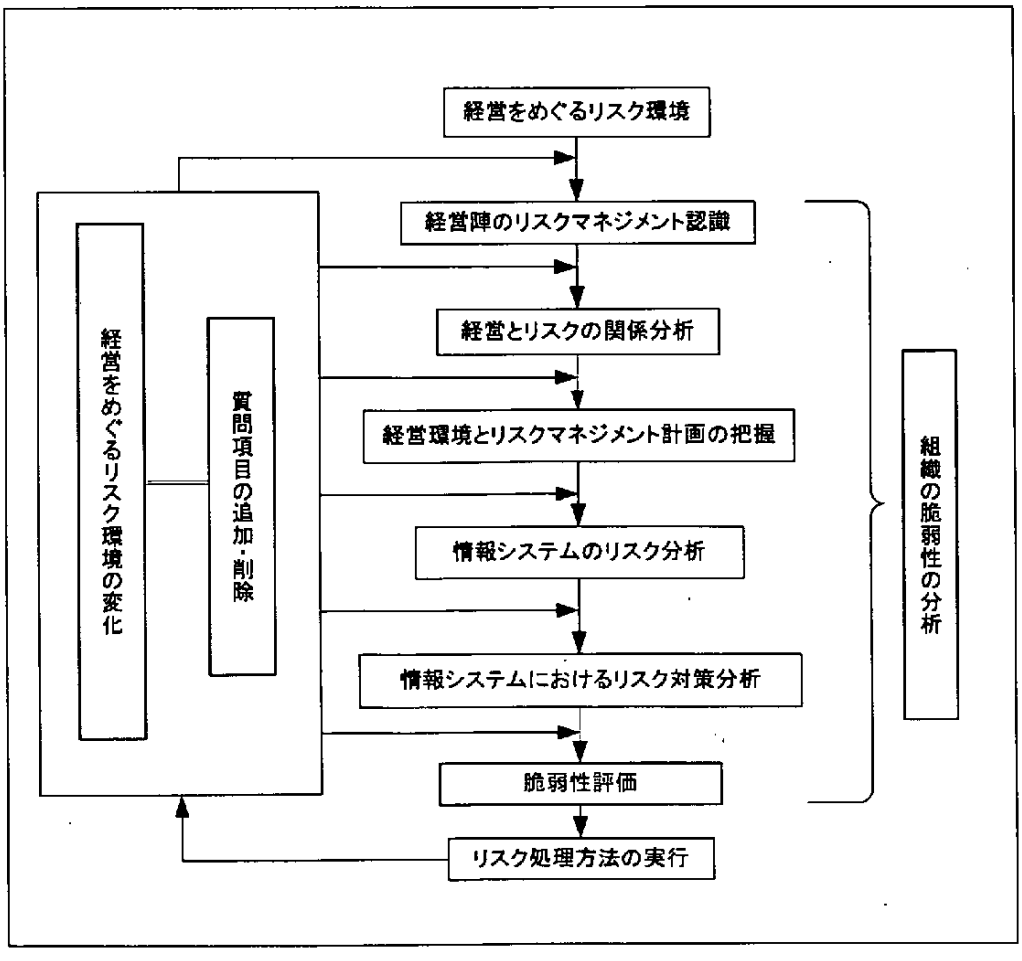

図2－1. JRMSの構造

高度情報化の流れの中で情報システムや情報そのものがあふれ、コンピュータの性能も日進月歩で高度化し、従業員一人ひとりが端末機器を操作し、情報端末なくしては業務が滞ることとなった。反面、不正アクセスやコンピュータウイルスが蔓延し、情報リスク対応について真剣に取り組む必要が生じてきた。こうした側面を考慮に入れたＪＲＭＳの構造は、すでにＪＲＭＳ解説書に示したように、「組織にとり情報リスク対応だけでは情報を神経系とする組織は守れない」ことから、組織の経営者のコミットメントを前提にしている。この点は、図２－１に明示されている。

しかし、組織のリスクに関する脆弱性をかなり定期的に把握しているとしても経営環境は可変的であり、必要に応じて見直す視点が不可欠である。したがって、組織全体にとり神経系となる「システム」と「情報」に関するリスクとその対応に焦点をあてたのがＪＲＭＳである。そのため、『JIS Q 2001：2001 リスクマネジメントシステム構築のための指針』（以下、「JIS Q 2001」という。）の方法論に基づき、マネジメントシステムである PDCA（Plan-Do-Check-Act）サイクルに則って構成されている。

2.1.2　マネジメントシステムの仕組みと個人情報保護

ＪＲＭＳはマネジメントシステムに則っているため、リスクマネジメントにおける意思決定のプロセスが経営環境の変化に応じフィードバックすることを前提に構築されている。とりわけ、個人情報の漏えい等に起因するリスクの作用が組織にいかなる影響を及ぼすのか、それへの対応について安全管理の側面を含めて考慮するには、実践性を重視しているＪＲＭＳの採用が意味をもってくる。いわば、個人情報取扱事業者としてトップから現場に至るまで、それぞれの業務において個人情報に関わるリスク対応のための行動指針と基本目的を明確にしなければならないからである。したがって、抽象的になりがちなリスク対応の基本目的をできるだけ具体的に設定することが求められるのである。そして、明示されたリスクマネジメント方針に従い、リスクマネジメントの計画が策定され、それぞれの部署においてリスクマネジメントを実施し、そのパフォーマンスを評価し、環境変化に応じた是正・改善を行うというプロセスが個人情報保護にも有効となる。

その際、リスクマネジメントシステムの有効性がリスクマネジメントの基本目的・リスクマネジメントの目標達成との関わりから評価を行うことが重要であり、そのための手順を確立・維持することが求められている。リスクマネジメントシステムの有効性を高めるためには、リスクマネジメント計画、リスク対策、リスクマネジメントシステムの体制・仕組みを見直し、是正・改善がどの程度必要なのか、必要であればどの領域なのかといったことを確定するため、ＪＲＭＳでは判定基準に照らしたギャップ分析を重視しているのである。

とりわけ個人情報保護に関して重要なのは、取扱者についてそれぞれの能力を高めるための教育・訓練が必要となることである。関係する部署における役割ごとに必要な能力が求められ、対策実施のために必要な能力を身に付けさせ、しかもそうした能力を維持させるため、継続的な取組みが不可欠となる。個人情報保護に係わる知識等については、経営陣のみならず各部門・部署における関係者にも当然望まれる。特に社会環境の変化の著しさ、情報システム環境の変化（スピードの速さ、経営に関わる変化の影響の大きさ等）を考慮するとき、教育・訓練の重要さはこれまでの比ではない。

そこで、ＪＲＭＳではリスク対応の実施手順の有効性を検証する目的をもってシミュレーションを行い、リスクの発見・特定のための情報収集、誤解なり理解不足に基づくリスク顕在化の防止等のためのリスクコミュニケーションの重要性が謳われている。この他、リスクへの対応に関して組織としていかに対処しているかを明らかにするために広報活動計画を策定すること、さらに関係機関・関係者に正確なリスク情報を適切な方法で開示することが重要である。いずれにしても、最終的には組織の最高経営責任者のコミットメントが前提となる。

2.2　ＪＲＭＳの３つのポイント

ＪＲＭＳがねらいとするのは次の３つのポイントである。

第１には、経営者が経営に関わるリスクセンス・リスクマインドを有するため、ＪＲＭＳの実践にコミットすることである。情報システムに直接関わる場合もそうでない場合も、社会的に問題とされた状況には経営陣の判断の誤りに拠る場合が多い。問題の所在として指摘できるのは、リスクマネジメントの導入・実施が組織に利益をもたらさないと考える傾向が経営陣に見られることである。問題発生後の処理に膨大な時間とコストをかけるまで認識できないのでは経営者としていかがなものであろうか。ちなみに、平成 15 年度に JIPDEC が行った「情報セキュリティに関する調査」のコストに関する意識調査結果として、回答者は経営陣ではないにしろ、リスク対応の一環としての情報セキュリティ管理の問題点として「コストがかかりすぎる」との回答が 53.6%（平成 13 年度は 51.9%）を占めていた。こうした回答は経営者の認識の低さを反映していないとはいえない（『平成 13 年度・15 年度　情報セキュリティに関する調査』結果を想起されたい[1]）。個人情報に関わるリスクについては現場の理解が不可欠であるが、上記のような回答結果が出された背景には対応の不備が組織を壊滅に導くとまで考えないきらいがあるからかもしれない。しかし、組織としては説明責任が問われる対象であり、組織に対する信頼性の面からも求められるといえる。そのためには、リスクに対する感性を磨くことが重要となるのである。

第２は、リスクに対する認識の共有である。リスクマネジメント担当部門・情報システム担当部門・ユーザ部門の管理職ならびに現場の関係者がリスクについての理解が十分ではなく、組織に対するリスクの作用なり影響を認識できないようでは組織の事業継続性（ビジネスコンティニュイティ）が脅かされることになる。経営陣の判断の誤りに原因がある場合もあるが、現場のミスジャッジがリスクを拡大させ、組織の存続を危うくすることがあるからである。それゆえ、リスクの影響とその対応に関する認識の共有の意義を重視すべきである。

第３には、組織を取り巻く環境の変化の速さについての認識と変化への対応に関する相互連関的なチェック体制の重要性である。特定の部署だけがリスクセンス・リスクマインドをもって対応してきたとしても、リスクの作用なり影響についての認識において他の部署との間で温度差が大きければ、組織としてボトルネックを抱え、全体としての対応に自ずと制約が存在することになる。それだけに第２で触れたリスクに対する共有認識をもつことが不可欠となる。他の部署の

1　「情報セキュリティに関する調査」集計結果は、JIPDEC ホームページに掲載されている。
（http://www.jipdec.jp/security/03sec.htm）

ことは自分に関係ないとする「他人事症候群」に陥らないための日頃の努力に関わる課題であり、ＪＲＭＳでは質問項目への回答者間のギャップ認識からそうした事態に陥らないようにすることが重要なポイントとされている。

現代社会における特徴の一つである高度情報化の動きの中で、組織の内外に多様な情報システムと情報そのものが満ち溢れており、情報の価値のみならずその取扱いは非常に複雑になってきている。それだけに、情報をめぐる環境についての枠組みを広げ、組織内の各部署・ステージにおいて情報のライフサイクル（取得から廃棄・消去まで）をアカウンタビリティの視点から明確にする必要性が出てきている。したがって、組織において情報との関連からどのようなリスクの発生が考えられるのか、その特徴は何なのか、組織に対する影響（インパクト）はどうなのか、対策は十分なのか明確に把握しておくことが不可欠である。そうした視点を重視する意味から組織のリスクマネジメントシステムという枠組みからのアプローチが重要となってきたのである。

そこで、ＪＲＭＳでは組織全体に係る「経営とリスクの関係」についてリスク認識のため「経営環境とリスクマネジメント」を経営陣、リスクマネジメント担当者層、ユーザ層を対象にした構成としている。その根拠は、特定の部署の限られた人だけがリスクマネジメントに理解があっても、情報に関する組織の脆弱性を低めることができないからである。

とりわけ、ＪＲＭＳではリスクマネジメントにおける出発点に計画のステージを置き、それに従ってリスクマネジメントの実行組織が行動することになる。しかも、リスクマネジメントをシステムとして捉えたのは、リスクマネジメントについての質問票によるチェックを特定の時期に仮に１回でも行えばそれでよいという性質ではなく、組織に関わるリスク環境変化に鑑みて、常にリスクマネジメントシステムを継続的に維持しておくことが求められているからである。いわば、組織の特定の部署における問題解決という「部分最適」指向ではなく、特定の部署での問題が全体に影響を及ぼすという現実を踏まえ「全体最適」を考慮に入れたシステムとしてリスクマネジメントに取り組むことの意味を強調しているのである。

2.3　マネジメントシステムと成熟度モデル

リスクマネジメントの実施にあたって重要なのは、経営者がリスクについてよく認識し、組織の構成員にリスク対応の意義を平易に説明し、構成員の理解のもと必要な資源・コストを投入することである。ところで、経営に対するリスクの影響に関して、上記の「情報セキュリティに関する調査」で基幹システムが１時間以上停止した場合の経営に対する影響の想定分析について、平成 15 年度調査では 77.0％（平成 13 年度は 75.9％）の事業体が実施していなかった。しかも、回答年度により実施していない数値が多少なりとも上昇している。こうした組織では、情報システムリスクを経営者が明確に理解し、構成員に説明し、情報リスクが経営者から見える状態にはなっていないのではないかと思われるが、これは大きな問題である。

ＪＲＭＳでは、経営者のみならずそれぞれの関連部署の担当者なり関係者について現状を把握するための仕組みを取り入れ、問題があればその原因を究明し、改善を行うという視点にたち、リスクマネジメントに「成熟度の考え方」を導入している。組織においてリスクマネジメントを実行する各領域について、それぞれの質問票への回答部署の成熟度を数値化する仕組みを作って

いる。これにより、成熟度レベルというわかりやすい指標が得られ、この数値を組織内の担当部門で比較し、問題があれば改善のための行動に結び付けることが可能になる[2]。特に重要なことは、自組織内の各部署における成熟度を経年的に見ることにより、自社のリスクマネジメントの実践レベルを継続的に向上させることができるのである。JIS Q 2001 で示されている PDCA のマネジメントサイクルを動かしていく際に、基準に基づいてチェックを行うことが重要な意義をもつことになる[3]。後述するＪＲＭＳの成熟度のレベルは、こうした場合の判定基準として利用可能となっている。

ＪＲＭＳ質問票は、質問項目の内容により回答者を経営者層、リスクマネジメント部門、情報システム部門、ユーザ部門に分けている。すなわち、組織内では質問の内容について組織の職位に応じたアカウンタビリティ（説明責任）があるはずであり、その点に鑑みてＪＲＭＳ質問票のそれぞれの回答欄に回答すべき関係者を割り当てているのである。

経営者は、その立場からステークホールダにより組織経営を任されており、最終的な責任を持ち、組織としての目的を成し遂げることである。したがって、リスクマネジメントはその大きな柱の一つといえる。

たとえば、ある会社で 5,000 万円の価値のある資産が紛失した場合、経営者は部下に対する管理が十分でなかったとして責任を回避することはできない。経営者として内部統制の仕組みを明確にし、設置していなかった責任がある。しかし、これと同等の金額の被害がコンピュータウイルスの感染で実際に起きている。ちなみに、2001 年９月に発生した Nimda ウイルスの感染により、パソコンの再設定費用、ユーザ業務の阻害等を換算すれば、6,000 万円以上の被害と算定されたケースもあった[4]。この例のように、情報システムに関わるリスクは情報システム部門に任せておけばよいレベルを超え、経営者が関与すべき段階に達しているといえる。

経営者が行わなければならないのは、組織として適切にリスクを管理する仕組みを作ることである。そのため、リスクマネジメントを実施する部門に適切なアカウンタビリティを割り当て、経営として通常行っている PDCA のサイクルをリスクマネジメントについて適用する。経営者は、リスクをビジネスの言葉で組織全体に説明すべきなのである。いずれの部門も、それぞれの役割認識にたち、部署における責任を明確に理解し、それぞれの役割を実施することが望まれる。

2.3.1　経営者の理解の必要性

組織の経営は構成員の一人ひとりの業務遂行能力によるが、重要なのは経営者の経営判断能力・リーダーシップにあるといえる。これまで経営トップの判断ミスにより組織が揺らぐだけでなく破綻を余儀なくされたケースがある。その判断に大きく関係するのがリスクセンス[5]であり、

---

[2] JRMS の普及により同業他社や同規模企業の平均値と比較することができれば、自社のリスクマネジメントの状況が他の企業と比較してどの位置にあるかを客観的に把握することもできなくはない。

[3] なお、JIS Q 2001 ではこうした基準について具体的な指摘はなされていないが、リスクマネジメントシステムとしてはそれぞれの組織が何らかの判定基準をもつことが望ましいのは当然のことである。

[4] 『JIPDEC リスクマネジメントシステム(JRMS)解説書』P.45.

[5] リスクセンス(risk sense)について「リスクの重要性を認識する智恵なり感性」であるとしている(森宮康「医療リスクマネジメントの実践－JRMSの医療リスクマネジメントへの応用のために－」『同志社商学』第 56 巻 2･3･4 号、P.23。

リスクマインド[6]である。特に経営者にこれらの概念の理解が求められる。変化が著しい経営環境にあって変化こそリスクの源泉であることを経営者自らが率先して認識し、組織の構成員も理解しなければならないといえる。問題が生じてから緊急に対処するというのでは遅すぎるのである。また、他の組織なり他の部署で生じた問題を「他人事」で片づけるような認識では、組織のステークホールダ（従業員・株主・顧客・消費者・取引業者・内外関係諸機関・行政府・マスメディア等）に対する説明責任を果たせないはずである。しかも情報システムは組織のあらゆる部面で神経系の働きをなしている。情報システムは経営環境の変化に包含されると共にリスクの発生源にもなりうるだけに、情報リスクマネジメントをマネジメントシステムから捉え、実践に生かすことが経営者にとっての最重要課題であろう。

ところで、ＪＲＭＳはリスクマネジメントを適切に行うために組織の各部署（経営者層・リスクマネジメント部門・情報システム部門・ユーザ部門）における回答者に質問項目への回答を求め、その結果をＪＲＭＳのシステムに入力することによりリスクマネジメントの全体像についての現状の成熟度をレーダーチャートで表示することができるようになっている[7]。これにより、自組織のリスクマネジメントの強みと弱みが明らかとなり、たとえ情報システムリスクに関心の低い経営者でも、レーダーチャートを通して状況を容易に理解することが可能となっている。ＪＲＭＳが効果を発揮するには、ＪＲＭＳの質問項目への回答結果の相互チェックに始まるギャップ分析が必要である。いずれにしても、経営者を筆頭に組織の担当者・関係者が組織にとってのリスクの影響を認識・評価し、リスク対応の必要性があれば、それを実現させる経営者の実行力が重要となる。

2.3.2　成熟度モデルの考え方

ＪＲＭＳでは、利用者が自組織のリスクマネジメントの現状を評価するために、成熟度モデルの考え方を取り入れている[8]。この場合の成熟度モデルとは、リスクマネジメントの各領域の管理プラクティスについて、どの程度のレベルに達しているかを評価するためのモデルである。ＪＲＭＳで採用した成熟度モデルは、ＣＯＢＩＴ－Ⅲの成熟度モデル（後記）を参考にし、リスクマネジメントの各領域について、成熟度のレベルを４段階（表２－１）に定めている。

表２－１．ＪＲＭＳの成熟度レベル

レベル0	未認識	組織内で全く意識されておらず、何もしていない
レベル1	初　期	組織内で部分的にしか実施されていない
レベル２	反復可能	組織内で概ね実施されているが、標準がない
レベル３	定　義	組織内で標準が作られ、大体それに従って実施されている

---

[6] リスクマインド(risk mind)について「リスクの発生からその影響について推論し判断するという考える力」を意味する（上掲論文）。

[7] レーダーチャートについては、操作によりドリルダウンできる仕組みとなっている。

[8] 『JIPDEC リスクマネジメントシステム(JRMS)解説書』日本情報処理開発協会、2004.2、PP.20～23.　JRMS 成熟度モデルに従い、JRMS 判定基準として用いている（P.49）。

４段階に設定した理由は、少なくとも現状のシステム環境に鑑みて、レベル３を達成できれば組織のリスク対応として一応の水準にあると考えたことによる。今後の課題は、次に示すCOBIT-Ⅲの成熟度モデルのレベル５を目標値にもっていけるかどうかにある。

（１）COBITの成熟度モデルとリスクマネジメント

ＪＲＭＳで参考にしているCOBIT-Ⅲは、情報システムの全業務を34のプロセスに分け、各プロセスについてその成熟度を定義したものである。成熟度はレベル０からレベル５までの６段階があり、それぞれのレベルの内容は表２－２のように定義されている。

表２－２．COBIT－Ⅲの成熟度モデル

レベル0	未認識	組織として、当該プロセスの標準が必要なことすら認識されておらず、標準のプロセスも全くない。
レベル1	初　期	組織として、当該プロセスの標準が必要なことは認識されているが、標準は確立されておらず、個人や場合によりその場限りの対応が行われている。プロセス全体についての組織的な対応はない。
レベル2	反復可能	ある作業を行う人たちが、同じ手続きを使うようになっている。しかし、標準手続きが公式的に教育・周知されてはおらず、個人任せになっている。各個人の知識に頼るところが多く、エラーも発生する。
レベル3	定　義	手続きの標準化、文書化、教育・周知が行われている。しかし、標準のプロセスに従うかは個人任せなので、逸脱が見られる。各手続きはあまり洗練されてはおらず、既存のやり方を公式化したものである。
レベル4	管　理	標準の手続きに従っているかをモニターし測定することが可能で、標準プロセスが有効でないときには是正措置を取ることができる。プロセスには絶えず改良が加えられ、グッドプラクティスが提供される。自動化ツールが部分的に利用されている。
レベル5	最適化	継続的な改良と他組織の成熟度モデルを使って、プロセスはベストプラクティスのレベルまで改良されている。ITは自動化されたワークフローに組み込まれ、品質や効率を改良するツールや企業の対応速度向上に役立っている。

出典：COBIT-Ⅲ（ISACA　2000.7）

情報システムに関するリスク評価を行う場合、ペリル（リスクをもたらす特定の原因事象）について、関連するプロセスの成熟度によりリスクが発生する確率は大きく異なってくる。したがって、情報システムに関するリスク評価を実施する際には、関連するプロセスの成熟度の評価を行う必要がある。もしも成熟度が低い場合には、何らかのハザード、すなわち損害が発生しやすい状況が存在していると判断すべきである。つまり、情報システムの各プロセスに内在するリスクは、各プロセスの成熟度が高ければ顕在化するおそれが低いが、成熟度が低いと種々の問題、たとえばプロジェクト開発の失敗や重大なシステム障害の形で顕在化するといえる。

各プロセスに内在するリスクを評価する時には、まずそれぞれのプロセスの成熟度があるレベルに達していることが前提条件として必要であり、もしもレベル２以下のものがあったら、リスクマネジメントシステム維持のため、そのプロセスの成熟度向上について検討を行う必要がある。

ＪＲＭＳの成熟度モデルもこうした考え方にたち、構築されているのである。

（２）CMM／NISTの成熟度モデル

参考のためCOBIT-Ⅲの成熟度モデルの基礎となったCMM(Capability Maturity Model)の成熟度モデルならびにNISTのモデルについても再録しておくことにする[9]。CMMはカーネギーメロン大学のソフトウェアエンジニアリングインスティテュートが提唱したモデルで、ソフトウェア開発のプロセスを対象に作られている。CMMの成熟度モデルでは、各プロセスの成熟度レベルを表２－３のように５段階で定義している。

表２－３．ＣＭＭの成熟度モデル

レベル1	個別実施	開発方法論が存在せず、ほとんどコントロールされていない。プロセスが達成できたとしても、評価尺度が存在していないために認識されない。
レベル2	反復可能	プロジェクトの結果を妥当な精度で予測するのに十分な、一連の作業とプロセスが定義されている。しかし、改善点をあらかじめみつけたり、複数の選択を比較する手法は含まれていない。
レベル3	定　義	開発プロセスは実装され、理解されている。評価尺度が用いられ、新たなテクノロジーの実装の効果が予測できる程度に、プロセスの予測が可能である。
レベル4	管　理	プロセスが管理され発展することで、数量的、品質的な改善が可能である。それぞれの技術の実装は、全体的なアーキテクチャの一部となっている。
レベル5	最　適	環境がプロセスを推進する、開発組織における理想的なレベル。プロセスの実行よりも、改善に注力される。

出典:ISO/IEC TR15504-4

COBIT-Ⅲでは、CMMの成熟度モデルを参照しながら、開発プロセスに集中したCMMに対し、対象を情報システムの全プロセスに拡大し、成熟度のレベルを定義している。また、CMMのレベル分けがレベル１～５となっているのに対し、レベル０を定義しているところが大きな違いである。

またNISTのSecurity Self-Assessment Guide for Information Technology Systemsでは、セキュリティに関わる17のトピックについて、表２－４のような成熟度のレベルを５段階で定義している。

表２－４．ＮＩＳＴの成熟度レベル

レベル1	ポリシー	管理目標がセキュリティポリシーで定められている。
レベル2	手続き	セキュリティコントロールの手続きが定められている。
レベル3	実　施	セキュリティコントロールの手続きが実施されている。
レベル4	テスト	セキュリティコントロールの手続きがテストされ、レビューされている。
レベル5	統　合	セキュリティコントロールの手続きが広範なプログラムに統合されている。

出典:National Institute Standard Technology(NIST)

[9] 『JIPDECリスクマネジメントシステム(JRMS)解説書』日本情報処理開発協会、2004.2、PP.20～23.

（3）ギャップ分析（バラツキの理解）の重要性

ＪＲＭＳにおける考え方において着目すべきはギャップ分析にある。組織のそれぞれの部署の回答担当者に質問項目に回答してもらうとしても、回答者間で回答結果が必ずしも一致しないことである。むしろ、一致する場合の方が問題かもしれない[10]。『情報化社会におけるリスクとＪＲＭＳ－リスク対策検討委員会　調査報告書』（JIPDEC、平成 14 年度）によると、実証実験にご協力いただいた組織の回答者間の回答がばらついていたことが報告されている[11]。

特記すべき事項としてあげられていたのは以下のとおりである。

①経営者層・情報システム部門・ユーザ部門ではそれぞれ回答項目数が異なるため、レーダーチャートの評価結果には、若干の誤差があること。

②回答者の役職上の責任範囲が異なることから、質問項目の受け止め方に差異が生じうること。

③質問項目の理解の仕方（正確か否か、厳しく捉えるか否か）・回答者の判断（的確か否か、組織としての判断か・個人的な印象か）により回答にバラツキが生じうること。

④同じ質問であっても回答者間での認識ギャップがあること。

⑤バラツキや認識ギャップの存在を踏まえ、それぞれの部門において意見調整を行い、実態についての情報を共有し、共通認識を有すること。

⑥情報を共有したうえで、再度、回答を持ち寄り、レーダーチャートを描き、リスク対応の実態についての傾向を組織として捉え、リスクマネジメントに資すること。

①、②の階層によってギャップがあることについては、回答する層によって問題の捉え方、すなわち経営への責任、リスクへの対策などが異なることがあげられる。むしろ、回答の違いが鮮明に分かれることの方が大切で、組織として一致しなければならない問題ではない。組織としてのリスクの捉え方が経営層がリスク管理者よりも甘いのは仕方がない。しかし、乖離が大きすぎると、リスクについて経営層に正しい情報が伝わっていないことが推定され、大きな問題であることがわかる。すなわち、ギャップの異なり方を対象とする組織の特性分析に利用できる。

次に、③～⑥の同一層の中でのギャップについては、次の３つの問題から起きていると考えられる。まず、第１に設問自体の問題で、一意的に答えられない設問となっているためである。第２には、回答者の主観や経験によって、設問に対する認識、理解度が異なることである。第３には、回答するときの判断基準が人によって異なるためである。これは、厳しく判断する人と、甘く判断する人が存在するためである。リスクマネジメントに、分析で得られた数値を経年的に活用するためには、これらのギャップをなくす必要がある。

ＪＲＭＳでは、第１点については質問項目に解説を加え、回答者の理解度のバラツキを少なくするようにした。第２の回答者の主観によって異なる問題と第３の回答者の評価基準による問題については、組織において質問項目に絶対的な尺度を決めて、これに従って判定する方法を採用

10　一致することが望ましい場合もあるが、リスクセンス、リスクマインドに個人差があるとすれば、業務関連のリスクに対する認識の共有のためのプロセスを通して実現できるのが一般的と思われる。それゆえ、ここでは、回答者の質問項目の理解、業務における責任とリスクとの関連に鑑みて、出発時点から一致するのがむしろ問題とした。

11　『JIPDEC リスクマネジメントシステム(JRMS)解説書』日本情報処理開発協会、PP.54～55.

するのが望ましいと考え、ＪＲＭＳでは成熟度分析モデルに準じた判定基準（表２－１）を設けている。

2.4　ＪＲＭＳ質問票の構成

ＪＲＭＳでは、階層構造を基に組織の脆弱性を分析するため、1,004 項目の質問を構築した。重要な点は、組織におけるリスクマネジメントの有効性を高めるためには、役割・責任はそれぞれの立場なり部署において異なるにしても、リスクの視点から上位者が下位者の職務実態を把握できず、下位者が上位者の方針・考え方・指示を理解し、実行できないようでは、組織の存続を守ることは不可能である。

ＪＲＭＳでは、経営者層、リスクマネジメント部門、情報システム部門、ユーザ部門から回答者を出し、それぞれに回答を求め、その結果をレーダーチャートに集約し、さらに回答結果のバラツキを分析し、問題があれば改善を指向するプロセスを採っている。たとえば、経営者層には「経営とリスクの関係」、「経営環境とリスクマネジメント」について回答を求める仕組みとなっている。回答する質問項目数は部門によって異なっている。

2.4.1　ＪＲＭＳ質問項目の構成

ＪＲＭＳの質問項目は大きく２つの部分から成り立っている。

第１は経営全般としての経営に関わるリスクマネジメントシステムの部分である。経営全般に関する部分は、経営者層とし、そこには最高経営責任者（CEO：Chief Executive Officer）、最高業務執行責任者（COO： Chief Operating Officer）、財務執行役員等（CFO：Chief Financial Officer）、リスクマネジメント執行役員（たとえば CRO：Chief Risk Officer）等、情報システム執行役員（CIO：Chief Information Officer）、ユーザ部門の役員などが組織のリスクマネジメント全般についての実態を把握するために回答する。

第２は、情報システム部門が関わるリスクマネジメントの部分である。情報リスクに関して、経営全般に対するリスクマネジメントの実態を踏まえながら情報システムに関わるリスクマネジメント全般を把握するための質問項目である。

一般に、経営者層は経営全般のリスクを把握する責務があり、リスクマネジメント部門（担当責任者）は経営に関わるリスクの分析・対応に責務がある。情報システム部門は情報システムに関わるリスクの分析・対応に責務がある。

現在の組織は一般的に情報システムを通して相互依存関係がこれまで以上に密になっており、一つの部署の問題（制約条件）が他の部署に大きな影響を与え、結果として経営そのものにも影響が及ぶようになっている。

このような現在の経営環境下において、情報システムのリスクマネジメント責任者は自部門のみならず、ユーザ部門など組織のあらゆる部門と接点をもち、リスク対応を実践することが非常に重要となっている。

しかも、情報システムに関わるリスクが組織全体に作用する環境下で、情報システム部門が情報システムだけのリスクに目を配るだけでは十分ではない。そのため、情報システムに関わるリ

スク対応を行うにあたっては、経営全般に関係するリスクについても理解し、リスクマネジメント部門と協同してリスク対応を図ることが大切である。実際にリスクマネジメントを実施しようとする場合には、関係者の共通認識が不可欠であり、これまで論じてきたように、経営者層との関わりが重要なのである。

ＪＲＭＳ質問項目では、経営者層が関与（回答）することにより、経営者層のリスクに対する関わりが強くなり、これによって情報システムに関わるリスクマネジメントの有効性が確保されることになる。

2.4.2　ＪＲＭＳ質問票の階層構造[12)]

ＪＲＭＳ質問項目は質問票にまとめられており、1,004項目で構成されている。

これらの質問項目は、一定の規則に従って階層化され、５階層の階層構造になっている。以下、簡潔に質問票の階層構造について解説する。

（1）質問票の大項目（第１階層・第２階層）について

質問票の大項目は４つの内容から構成されており、それぞれが第１階層項目を構成している。第１階層項目を構成する内容は表２－５のとおりである。

表２－５．ＪＲＭＳの第１階層項目

大項目	第1階層	
経営全般に関するリスクマネジメント	Ⅰ	経営とリスクの関係
	Ⅱ	JRMSにおけるリスクマネジメント計画
情報システムに関するリスクマネジメント	Ⅲ	情報システムのリスク分析
	Ⅳ	情報システムにおけるリスク対策

ＪＲＭＳは情報システムのリスクマネジメントを対象としているが、情報システムのリスクマネジメントの目的は、単に情報システムのセキュリティのみではなく、経営事業体そのもののセキュリティを対象としている。そのため、経営全般に関わるリスクを把握することが情報システムのリスクマネジメントを考えるうえで必要であるとの認識から、以下のような構成とした：

経営全般に関するリスクマネジメントについては、【Ⅰ．経営とリスクの関係】と【Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画】において「計画・実行組織・維持・リスク分析・リスク対策」を対象とした。情報システムに関するリスクマネジメントについて、【Ⅲ．情報システムのリスク分析】において「情報セキュリティポリシーのリスク分析・情報システムのリスク分析」を対象とし、【Ⅳ．情報システムにおけるリスク対策】はＪＲＭＳにおけるリスク対策である「対策」を対象とした４つの大項目からなっている。そのうえで、以下のような階層構造を採用している：

・第１階層と第２階層によって質問項目はカテゴリ化されている。

・第２階層項目を構成する内容は表２－６のとおりである。

12　『JIPDEC リスクマネジメントシステム（ＪＲＭＳ）解説書』日本情報処理開発協会、PP. 29～31 による。

表２－６．ＪＲＭＳの第１／第２階層項目

第1階層		第2階層	
Ⅰ	経営とリスクの関係	Ⅰ－1	経営環境とリスクマネジメント
Ⅱ	JRMSにおけるリスクマネジメント計画	Ⅱ－1	JRMSの計画
		Ⅱ－2	JRMSの実行組織
		Ⅱ－3	JRMSの維持
		Ⅱ－4	JRMSのリスク分析
		Ⅱ－5	JRMSのリスク対策
Ⅲ	情報システムのリスク分析	Ⅲ－1	情報セキュリティポリシーのリスク分析
		Ⅲ－2	情報システムのリスク分析
			(1)情報システムのリスク分析
			(2)システム開発
			(3)システム運用
			(4)アウトソーシング
		Ⅲ－3	情報システムの個別リスク分析
			(1)不正アクセス・コンピュータウイルス関連
			(2)災害
			(3)障害
Ⅳ	情報システムにおけるリスク対策	Ⅳ－1	リスク対策における情報セキュリティ
		Ⅳ－2	情報システムのリスク対策
			(1)情報システム総合企画
			(2)システム開発
			(3)システム運用
			(4)アウトソーシング
			(5)システム監査
		Ⅳ－3	不正アクセス・コンピュータウイルス関連
			(1)コンピュータ犯罪
			(2)不正アクセス
			(3)コンピュータウイルス
			(4)E－Commerce
			(5)電子メール
		Ⅳ－4	災害対策
		Ⅳ－5	障害対策
		Ⅳ－6	その他関連項目
		Ⅳ－7	バックアップ
		Ⅳ－8	緊急時対策

（2）第３階層、第４階層と第５階層について

２階層項目ごとのそれぞれに第４階層・第５階層があり、具体的な質問内容となっている。回答者はこの第４階層・第５階層の該当項目を回答する。各階層の主要な内容はキーワードとして示されており、さらに第４階層、第５階層の質問項目ごとには識別コードが付けられている。この識別コードによって質問項目に対する回答結果の集計、分析が行われることになる。なお、第３階層は、識別コードの３番目にあたるが、実際には、【Ⅲ．情報システムのリスク分析】と【Ⅳ．情報システムにおけるリスク対策】の質問構成を明示するために用いられている。

階層構造化された質問項目の一例は表２－７のとおりである。

表２－７．ＪＲＭＳの階層別項目例

階層	キーワード	キーワード	識別コード	質問項目
第1階層	経営とリスク	経営とリスク	Ⅰ．経営とリスクの関係	
第2階層	経営環境とリスクマネジメント	経営環境とリスクマネジメント	Ⅰ－1．経営環境とリスクマネジメント	
第4階層	1．経営者の関心	経営者の関心	1-1-1-1	Q 経営者は役員会において経営に関するリスクについて議論をしていますか？
	2．リスクマネジメントポリシー	全社的なリスクマネジメントポリシー	1-1-1-2	Q 全社的なリスクマネジメントポリシー(方針)を有していますか？
第5階層	リスクマネジメントポリシー	最高経営者の承認	1-1-1-2-1	Q リスクマネジメントポリシーは、最高経営者の承認のもと全社的に策定されていますか？
		経営理念との整合	1-1-1-2-2	Q リスクマネジメントポリシーは、貴社の経営理念に基づいて定めていますか？

注1）最高経営者とは、CEOを想定している。

注2）ここでは【Ⅰ．経営とリスクの関係】を例示しているため、大項目【Ⅲ】、【Ⅳ】に関わる階層を意味する第3階層は、上記の表では示していない。

なお、ＪＲＭＳ質問項目の全体の項目数は表２－８のとおりである。

表２－８．ＪＲＭＳの質問項目数

大項目		質問項目数	
		第4階層の項目数	全項目数
Ⅰ	経営とリスクの関係	9	21
Ⅰ－1	経営環境とリスクマネジメント	9	21
Ⅱ	JRMSにおけるリスクマネジメント計画	79	237
Ⅱ－1	JRMSの計画	15	44
Ⅱ－2	JRMSの実行組織	8	11
Ⅱ－3	JRMSの維持	19	31
Ⅱ－4	JRMSのリスク分析	27	125
Ⅱ－5	JRMSのリスク対策	10	26
Ⅲ	情報システムのリスク分析	54	152
Ⅲ－1	情報セキュリティポリシーのリスク分析	10	26
Ⅲ－2	情報システムのリスク分析	19	64
	(1)情報システムのリスク分析	7	36
	(2)システム開発	5	15
	(3)システム運用	3	6
	(4)アウトソーシング	4	7
Ⅲ－3	情報システムの個別リスク分析	25	62
	(1)不正アクセス・コンピュータウイルス関連	12	23
	(2)災害	6	21
	(3)障害	7	18
Ⅳ	情報システムにおけるリスク対策	245	594
Ⅳ－1	リスク対策における情報セキュリティ	29	91
Ⅳ－2	情報システムのリスク対策	94	167
	(1)情報システム総合企画	29	36
	(2)システム開発	22	61
	(3)システム運用	7	23
	(4)アウトソーシング	36	36
	(5)システム監査	6	11
Ⅳ－3	不正アクセス・コンピュータウイルス関連	60	151
	(1)コンピュータ犯罪	9	22
	(2)不正アクセス	19	53
	(3)コンピュータウイルス	10	22
	(4)E－Commerce	11	31
	(5)電子メール	11	23
Ⅳ－4	災害対策	28	57
Ⅳ－5	障害対策	12	37
Ⅳ－6	その他関連項目	7	18
Ⅳ－7	バックアップ	10	41
Ⅳ－8	緊急時対策	5	32
計		387	1,004

3．ＪＲＭＳ個人情報保護編の考え方

3.1　個人情報の漏えい問題の増加

パソコンは 90 年代以降、処理能力の向上と Windows によって急速に普及し、中小企業を始め多くの企業が利用するようになった。企業の多くは顧客情報をデータベースに入力して印刷するようになった。現在、企業から送られてくる郵便物は、そのほとんどがパソコンで印刷されている。しかし、企業の多くはこのような個人情報の管理におけるリスクに気づいていなかった。さらに、企業や組織体の多くがこのような個人情報の入力作業を外注するようになった。

このような中、平成 13 年以降、パソコン管理上の問題から個人情報が漏えいする事件が多発するようになった。

企業は、個人情報保護法の成立とともに、個人情報のもつ本当のリスクを認識し始めたようである。当初、企業は個人情報のリスクを個人のリスクと捉えており、自分たちのリスクについてほとんど認識できていなかった。しかし、多くの企業が個人情報の漏えい事件を引き起こしたことから、企業が信用されなくなった。個人情報保護法の成立とともに、企業が集めた個人情報が企業のものではなくなり、個人のものであることが明確になった。すなわち、企業側は、自分が保有している個人情報の持ち主から、いつでも修正、変更、削除などを要求される。また、情報の利用目的の制限がある。いつ、個人情報の取扱いに不満をもった個人が法的な手段をとるかもしれない。そのため、個人情報を利用するには、保有のためのコスト（情報システムの整備、情報セキュリティ対策の準備、従業員教育、法的な準備など）がかかるようになった。

今までほとんどコスト要因でなかったものが大きなコスト要因になる。財務的な観点からは大きなリスクである。また、個人情報は十分な取扱いを行わないと、多大な法的なリスクを負うことになる。

平成 16 年度に JIPDEC が実施した「システム監査普及状況調査」から動向を探ってみると、次のような傾向が確認できた。

「現在の個人情報の管理状況についてリスクをどのように認識していますか」という設問への回答について、監査担当部門（回答組織数 421）では「対策を講じているので、リスクはないと認識している」8.3%、「現状の管理方法で何も問題が発生していないので、リスクはないと認識している」10.7%と合わせると 19.0%が「リスクはない」という。被監査部門（回答組織数 507）でもそれぞれ 8.5%、12.2%で、合計 20.7%が同様の回答を示した。約５社に１社の割合でリスク認識がないことがわかる。ただ、こうした動向を「平成 15 年度情報セキュリティに関する調査」の結果（それぞれ 6.4%、17.9%、合計 24.3%）と比べると、それぞれの割合が低くなり、リスク認識に変化が生じてきている。

また、監査担当部門で「何度かヒヤリ・ハッとした経験があり、リスクがあると認識している」33.3%、「いつ問題が発生してもおかしくない状況であると認識している」28.5%と合計すると 61.8%、被監査部門の場合にはそれぞれ 27.2%、30.6%、合計すると 57.8%と、両部門とも約６割が「リスク認識」を示していた。この点を上記同様に「情報セキュリティに関する

調査」の回答結果（それぞれ 20.0%、27.9%、合計 47.9%）に比較すると、10 ポイント以上増加しており、リスク認識の高まりを感じることができる。

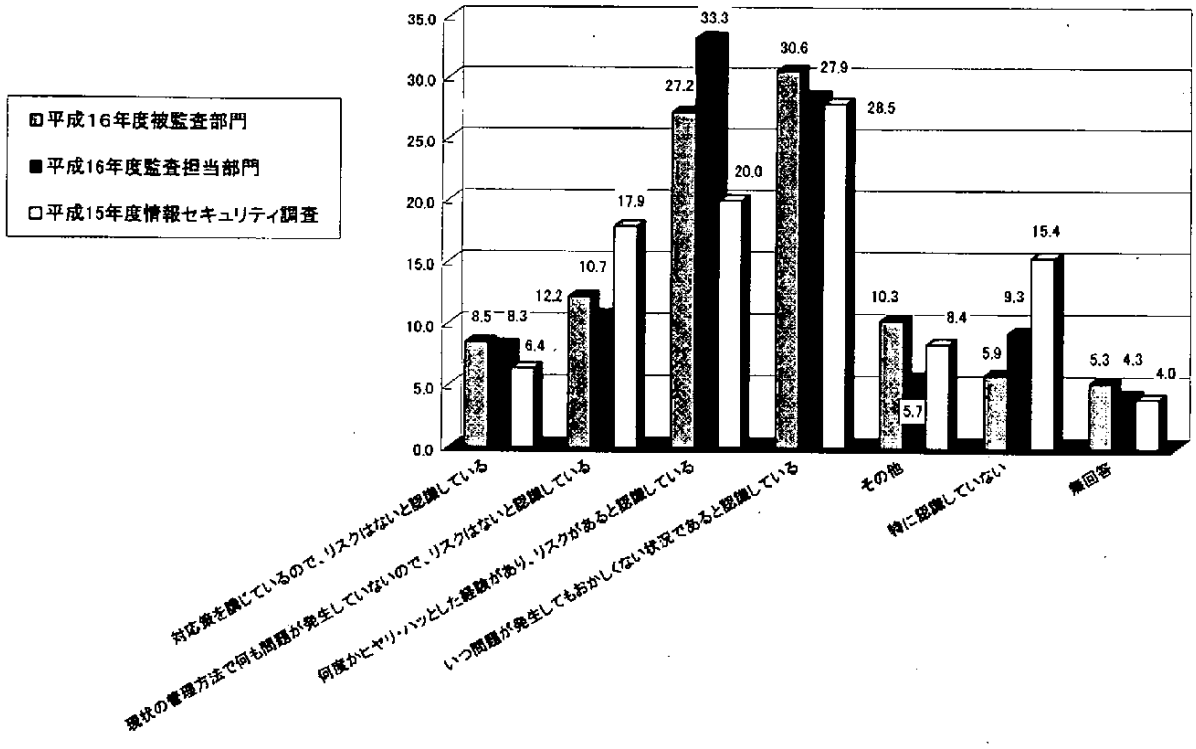

図3-1．個人情報の管理状況についてのリスク認識

出典：「システム監査普及状況調査」（H16 年度）および「情報セキュリティに関する調査」（H15 年度）の「個人情報の管理状況についてのリスク」調査結果より

個人情報保護対策として、現在実施している内容についてのそれぞれの回答結果は、表３－１のとおりである。

表３－１．現在実施している個人情報保護対策

実施対策	監査担当部門	被監査部門	情報セキュリティ
プライバシーポリシーを策定している	32.8%	27.2%	選択肢なし
管理責任者を置いている	42.5%	40.0%	36.0%
個人情報保護に関する規程を定め運用している	39.7%	32.5%	34.7%
社員教育に個人情報保護に関するカリキュラムを追加して、定期的に教育している	29.2%	23.3%	18.3%
リスク分析を実施して必要な安全対策を構築している	26.8%	21.9%	13.4%

監査担当部門と被監査部門とで若干の差異があるものの、平成 15 年度調査に比べ、個人情報保護とリスクに関する認識に好ましい変化がみられる。

しかし、調査結果からリスク認識が高まってきたことがわかる。しかし、現実には、企業がリスクをどのように対応していくか、厳しい状況にあるといわざるを得ない。

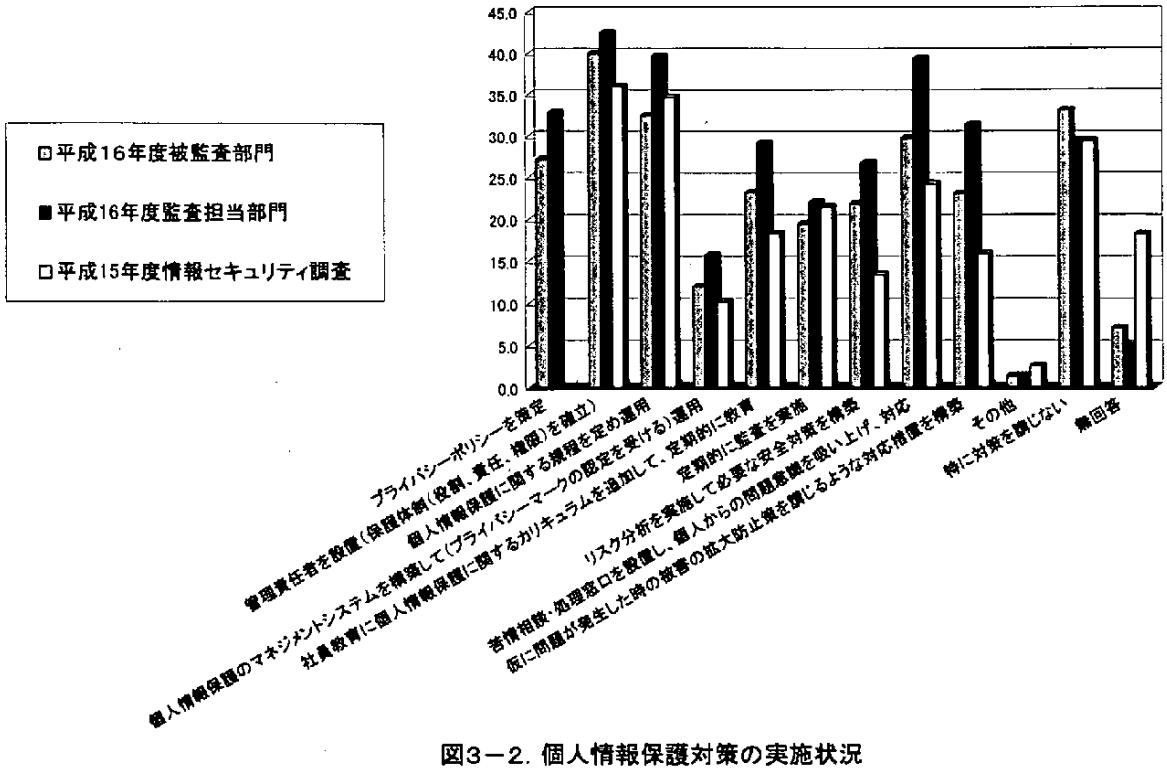

図3－2. 個人情報保護対策の実施状況

出典：「システム監査普及状況調査」（H16 年度）および「情報セキュリティに関する調査」（H15 年度）の「個人情報保護対策の実施状況」調査結果より

3.2 ＪＲＭＳの「Ⅰ」と「Ⅱ」の関係

3.2.1 ITの発展と個人情報に関するリスクの高まり

1990 年以降、パソコンの急激な進歩の中で、企業や組織はパソコンを経営に活用するようになった。具体的には、パソコンで経営情報や顧客情報を管理するようになった。また、IT 化が進んだ中、多くの企業や組織ではパソコンに個人情報を蓄積して利用するようになった。1980 年代までは、大企業が大型コンピュータで利用していただけであったが、パソコンのハードウェアとソフトウェアの進歩によって、ほとんどの企業が利用するようになった。さらに、1990 年代後半から、企業はグローバルでオープンなインターネットをビジネスで利用し始めた。インターネットは、ネットワークが海外とも繋がっており、通信費用や機器も安い。このため、企業は、パソコンとインターネットを大きく活用するようになった。

一方、大型コンピュータの時代は、データの入力、システムの管理などが十分になされていたために個人情報の漏えいや事故が起きにくかった。しかし、パソコンを普及させること、個人をマーケットの中心としていたため、大型コンピュータが採用したような情報セキュリティ対策は採られなかった。

このような帰結として、企業の重要情報や個人情報の漏えいなどの事件・事故が発生するようになった。これは、重要な情報をきちんと管理すること、そのリスクが十分に省みられずに情報化が進んだためである。特に、このような中で粗末に扱われてきた個人情報が巷に溢れ、社会は個人情報の管理を厳しくすることを望むようになり、「JIS Q 15001:1999　個人情報保護に関するコンプライアンス・プログラムの要求事項」（以下、「JIS Q 15001」という。）や、個人情報保護法が成立した。

個人情報保護法の施行は、組織の経営に大きな影響をもたらすことになった。民間の事業者のうち、過去６か月間継続して 5,000 人の個人データを保有していなければ個人情報取扱事業者から除外されるが、社員情報のみならず顧客情報を考慮すれば、組織の大小を問わず、ほとんどの民間の事業者は個人情報取扱事業者となる。すなわち、組織として個人情報保護に関してリスクマネジメントの視点からアプローチせざるをえないことになったといえよう。

3.2.2　ＪＲＭＳ個人情報保護編

ＪＲＭＳでは、企業が IT に対するリスクマネジメントを実施する中で、どのようにリスクを漏れなく見つけるか、また、見つかったリスクが企業にとってどの程度クリティカルなのか、IT ガバナンスとどのように連携するかが重要となっている。IT に関するリスク分析ツールは、ＪＲＭＳの前身であるＪＲＡＭ（JIPDE リスク分析方法論）を始めとして多数開発され、多くのユーザに利用されている。しかし、多くの IT 関係のリスクに関する分析手法では、IT に特化するあまり、IT を利用する企業の立場や IT ガバナンスが十分とはいえない。これは、企業の経営の視点からのリスクと IT のリスクの関係について明確になっていないからである。

一方、ＪＲＭＳでは、Ｉ章とⅡ章で企業を取り巻くリスクについて、主に経営者やリスクマネジャーの立場からの分析を組み入れることで、企業経営の視点と情報システムの構築や運用に係わる IT リスクの両方の視点からリスクについて俯瞰できるようになっている。

一方、個人情報保護法が平成 17 年４月に完全施行となる中、「3.1　個人情報の漏えい問題の増加」で取り上げた調査結果をみても、個人情報漏えい問題が多発し、個人情報に関するリスク分析のニーズが高まっていることがわかる。

ＪＲＭＳは個人情報について全体のリスクの中で捉えてはいるものの、個人情報の観点からの IT リスクには十分とはいえない。そのため、委員会ではＪＲＭＳの利点を残しながら、個人情報に特化して使えるようにできないかを検討した。その結果、ＪＲＭＳは企業のリスクを広く捉えているので、これを個人情報に特化させればＪＲＭＳの構造のままで企業の個人情報のリスクについて網羅的に分析できることがわかった。今回、Ｉ章とⅡ章を大きく入れ替え、個人情報保護のリスクを捉えられるツールとして「ＪＲＭＳ個人情報保護編」（以下、「個人情報保護編」という。）を完成させることができた。

3.3　個人情報保護編のＩ章、Ⅱ章

「Ｉ章：経営と個人情報保護」は、経営からの個人情報に関するリスクを多面的に捉えている。これは、JIS Q 15001 の「4.1 章」および「4.2 章」に対応している。特に、経営面での判断な

ど、企業としての個人情報全般に対する点からのチェックを行う。ここでは、評価は経営者やリスクマネジャーをターゲットとしている。

また、ＪＲＭＳはマネジメントシステムをターゲットとしており、JIS Q 15001 の構造とほぼ一致する。したがって、JIS に詳しい読者にとっては比較的わかりやすく利用できると考えている。企業のマネジメントが、どの分野で、どの程度対応できているかについては、重要と思われるチェック項目を選択して、成熟度モデルを用いて評価していくのがよい。

（JIS では、成熟度モデルを用いていないが、ＪＲＭＳでは、成熟度モデルを用いてマネジメントの段階を判定している。この点が、JIS や他の ISO とは異なる点である。成熟度モデルを用いて、マネジメントを評価する手法については、４章で述べている。）

表３－２．JIS Q 15001 のマネジメントサイクル

方針	4.1	一般要求事項
	4.2	個人情報保護方針
Plan	4.3	計画
Do	4.4	実施及び運用
Check	4.5	監査
Act	4.6	事業者の代表者による見直し

なお、JIS Q 15001 に詳しい読者のために、参考として、資料編「ＪＲＭＳ個人情報保護編」の質問票に JIS Q 15001 対照表を付記している。

ＪＲＭＳでは階層構造をとっているため、JIS の大項目がＪＲＭＳの第５階層にあてはまる場合でも、第４階層が JIS の大項目と合っていない場合は対象外とした。すなわち JIS とＪＲＭＳの階層がある程度近いものを選んだ。（下位の階層での内容が一致しない場合は対応させていない。）

- ＪＲＭＳ質問項目のキーワードと項目が JIS Q 15001 の内容をカバーしている場合は、その見出しに相当する章番号を記載している。
- （　）がついた項目はＪＲＭＳで述べていることと JIS Q 15001 との内容が近く、関連があることを示す。
- ［　］がついた項目はＪＲＭＳと JIS Q 15001 との内容で大きく異なるが、共通するものを含んでいることを示す。なお、章番号は JIS Q 15001 の下記に示す番号である。

表３－３．JIS Q 15001 の構成

4.1　一般要求事項
4.2　個人情報保護方針
4.3　計画
4.3.1　個人情報の特定
4.3.2　法令及びその他の規範
4.3.3　内部規程
4.3.4　計画書
4.4　実施及び運用
4.4.1　体制及び責任
4.4.2　個人情報の収集に関する措置
4.4.2.1　収集の原則
4.4.2.2　収集方法の制限
4.4.2.3　特定の機微な個人情報の収集の禁止
4.4.2.4　情報主体から直接収集する場合の措置
4.4.2.5　情報主体以外から間接的に収集する場合の措置
4.4.3　個人情報の利用及び提供に関する措置
4.4.3.1　利用及び提供の原則
4.4.3.2　収集目的の範囲外の利用及び提供の場合の措置
4.4.4　個人情報の適正管理義務
4.4.4.1　個人情報の正確性の確保
4.4.4.2　個人情報の利用の安全性の確保
4.4.4.3　個人情報の委託処理に関する措置
4.4.5　個人情報に関する情報主体の権利
4.4.5.1　個人情報に関する権利
4.4.5.2　個人情報の利用又は提供の拒否権
4.4.6　教育
4.4.7　苦情及び相談
4.4.8　コンプライアンス・プログラム文書
4.4.9　文書管理
4.5　監査
4.6　事業者の代表者による見直し

『個人情報保護編』の全体の項目数は表３－４のとおりである。

表３－４．ＪＲＭＳ質問票　個人情報保護編　質問項目数

大項目		質問項目数	
		第4階層の項目数	全項目数
Ⅰ	経営と個人情報保護	9	21
Ⅰ－1	個人情報保護とリスク	9	21
Ⅱ	個人情報保護に関するリスクマネジメント計画	79	191
Ⅱ－1	個人情報保護に関するリスクマネジメント計画	15	44
Ⅱ－2	個人情報保護の実行組織	8	11
Ⅱ－3	個人情報保護に関するマネジメントシステムの維持	19	31
Ⅱ－4	個人情報保護に関わるリスク分析	27	79
Ⅱ－5	個人情報保護に関わるリスク対策	10	26
Ⅲ	情報システムのリスク分析	54	152
Ⅲ－1	情報セキュリティポリシーのリスク分析	10	26
Ⅲ－2	情報システムのリスク分析	19	64
	(1)情報システムのリスク分析	7	36
	(2)システム開発	5	15
	(3)システム運用	3	6
	(4)アウトソーシング	4	7
Ⅲ－3	情報システムの個別リスク分析	25	62
	(1)不正アクセス・コンピュータウイルス関連	12	23
	(2)災害	6	21
	(3)障害	7	18
Ⅳ	情報システムにおけるリスク対策	245	594
Ⅳ－1	リスク対策における情報セキュリティ	29	91
Ⅳ－2	情報システムのリスク対策	94	167
	(1)情報システム総合企画	29	36
	(2)システム開発	22	61
	(3)システム運用	7	23
	(4)アウトソーシング	36	36
	(5)システム監査	6	11
Ⅳ－3	不正アクセス・コンピュータウイルス関連	60	151
	(1)コンピュータ犯罪	9	22
	(2)不正アクセス	19	53
	(3)コンピュータウイルス	10	22
	(4)E－Commerce	11	31
	(5)電子メール	11	23
Ⅳ－4	災害対策	28	57
Ⅳ－5	障害対策	12	37
Ⅳ－6	その他関連項目	7	18
Ⅳ－7	バックアップ	10	41
Ⅳ－8	緊急時対策	5	32
計		387	958

4．ＪＲＭＳ個人情報保護編

「ＪＲＭＳ個人情報保護編」「は、個人情報保護法の平成 17 年４月の全面施行に対応し、ＪＲＭＳのツールを利用してリスクマネジメントを実践するために作成されたシステムである。

ところで、「個人情報保護編」は、基本的にＪＲＭＳと同様の質問項目の構成になっている。経営全般に関するリスクマネジメントについては、【Ⅰ．経営と個人情報保護】と【Ⅱ．個人情報保護に関するリスクマネジメント計画】において「計画・実行
・組織・維持・リスク分析・リスク対策」を対象とした。情報システムに関するリスクマネジメントについては、ＪＲＭＳの質問項目を活用したが、【Ⅲ．情報システムのリスク分析】では「情報セキュリティポリシーのリスク分析・情報システムのリスク分析」を、また【Ⅳ．情報システムにおけるリスク対策】では「リスク対策」に関して、若干、個人情報保護に視点を合わせ質問項目の修正を行った。

4.1　経営と個人情報保護

ＪＲＭＳにおいて【Ⅰ．経営とリスクの関係】を最初に取り上げたように、「個人情報保護編」においても同様に、まず【Ⅰ．経営と個人情報保護】を取り上げた。その理由は、組織の経営にとり個人情報保護がきわめて重要な意味を有することにある。状況によっては、個人情報の取扱い如何により組織の存続が脅かされることが考えられるからである。したがって、組織の存続を目標の一つとして考えた場合、経営環境が著しく変化する今日、経営の視点から個人情報保護を重視しなければならないといえる。

ＪＲＭＳに則り、第２階層が［Ⅰ－1．個人情報保護とリスク］の１項目、第３階層は《1．経営者の関心》、《2．個人情報保護方針》、《3．個人情報保護方針のフレームワーク》、《4．個人情報保護の監査》、《5．個人情報保護方針の周知》の５つをキーワードとして取り上げている。回答質問数は、経営者層 11 項目、リスクマネジメント部門 20 項目、ユーザ部門 18 項目となっている。

最初に、組織全体としての【Ⅰ．経営と個人情報保護】に係るリスク認識を把握するため、《経営者の関心》（回答者は経営者層）は役員会において個人情報保護のリスクが議論の対象となっているかが問われる。経営者層が個人情報保護とリスクとの関係に着目しているか否かは、組織全体の判断に関係してくるため、重要な意味を有している。経営者層が回答するのは、アカウンタビリティとの関連から判断して構成されたＪＲＭＳの考え方に基づいている。「個人情報保護編」においても同様の位置づけになっており、経営と個人情報保護について第４階層が中心であるが、すべてではない。《個人情報保護方針》について、第４階層の「全社的な個人情報保護方針」の有無と第５階層の「最高経営者の承認」の可否となっている。

《個人情報保護方針のフレームワーク》については「基本目的」が明確に設定されているかの可否、「経営への脅威」の明確さの有無、「責任部門」の明記の有無、「行動方針」の明確さの

有無がそれぞれ第４階層、「個人情報保護関連リスクの連絡体制」整備の有無が第５階層となっている。

《個人情報保護の監査》および《個人情報保護方針の周知》については経営者層以外の部門が回答することになっている[13]。

リスクマネジメント部門は「経営者の関心」を除く全質問項目に回答し、ユーザ部門はそれに加え「最高経営者の承認」、「経営理念との整合」以外の項目に回答することが求められている。

ＪＲＭＳにおいて基本的な視点は、組織の構成員がリスクマネジメントに関する共通の認識を持つことである。しかし、コストとベネフィットとの関係には時間という要素を加味しなければならない。この点に関し、ＪＲＭＳ解説書（P.11）に示した内容を再録しておくことにしたい。

> リスク認識の共有：
> 組織においては、リスクに関する認識ギャップが大きければ大きいほど、迅速なリスク対応ができない場合がある。その背景には、リスク対応にかかるコストとそれにより生じるベネフィットの評価に差が生じるため、時間がかかりすぎることがあげられる。時間をかけて認識を共有することも大事であるが、タイミングが遅れることにより、場合によっては、コストが余計にかかることもある。

この点は、現場における最適なリスク対応という意味での「部分最適」も必要であるが、部分がいかに最適化を計っても、そこだけよくても全体が改善されなくては意味がないわけで、リスクマネジメントにおいては「全体最適」を指向することが重要である。

4.2 個人情報保護に関するリスクマネジメント計画

4.2.1 個人情報保護に関するリスクマネジメント計画

【Ⅱ．個人情報保護に関するリスクマネジメント計画】では、組織としてのリスクマネジメントに関する枠組みを計画の面から把握する。ここでは、ＪＲＭＳと同様に「個人情報保護に関するリスクマネジメント計画」がどうなっているかについて明らかにしている。第２階層は、［Ⅱ－１．個人情報保護に関するリスクマネジメント計画］、［Ⅱ－２．個人情報保護の実行組織］、［Ⅱ－３．個人情報保護に関するマネジメントシステムの維持］、［Ⅱ－４．個人情報保護に関するリスク分析］、［Ⅱ－５．個人情報保護に関するリスク対策］の５項目で構成されている。

［Ⅱ－１．個人情報保護に関するリスクマネジメント計画］では、《１．経営理念と個人情報保護計画》、《２．個人情報保護のリスク管理体制の組織化》、《３．個人情報保護の管理目標》、《４．個人情報保護の目標脅威》、《５．個人情報保護の分析》、《６．対策》、《７．緊急時対応》、《８．個人情報保護計画の周知》の８項目をキーワードとして取り上げている。

---

[13] 個人情報保護との関連からすると回答すべき質問項目の重みの点で整合性が取れているか否か、問題があると思われた部分もあったが、JRMS の現在のシステム構成（バージョン）を活用するという委員会方針に従ったため、今後に課題を抱えることになったことは否めない。

ここで経営者は、経営理念に基づいた個人情報保護の計画を立て、経営の観点から守るべき個人情報を明確にする必要がある。また、特定のリスクごとに責任部門を定め、管理目標を具体的に示すことが重要となる。また、リスク対策の採用にあたっては、要員の配置や予算手当てなど経営資源の充当が必要となるため、最終的な承認は経営者が行うこととなる。リスクマネジメント部門はすべての項目に回答する必要があるが、特に各々のリスクごとにリスク対策を実施する責任者を定め、責任権限や具体的な管理目標、分析方法、対策の実施基準を明確に示し、取扱いにバラツキが生じないように管理していく必要がある。

特に緊急時対応は重要で、事故発生時に適切な対応を行うためには、あらかじめ起こりうる事故を想定して対応に関するシナリオを準備しておくことが有効である。その中で連絡体制や対応手順、被害の拡大防止策、再発防止策等を定めておく必要がある。また、対応に係るコスト計算を行い、費用対効果の観点から最適な対応手順を選択できるよう、いくつかの対応策を用意しておく。対策本部を設置して対応にあたる場合は、社長もしくは経営層が最高統括責任者となるが、事故内容により、そのつど最適のメンバーを構成することが望ましい。連絡体制や対応手順については模擬訓練等を行うなど、円滑に機能することを定期的にチェックしたり、複数の連絡手順を確保するなど、緊急時に滞りがないようにしておくことが望ましい。

事件の経過は Web などを通じて随時行うとともに、２次被害等の影響を心配する顧客を考慮して、現在の状況だけでなく、具体的な注意事項や今後の対策などをタイムリーに報告すべきである。事態が沈静化した後はすみやかに再発防止策を講じる。また、さまざまな事故事例がマスコミ報道されるつど、自社の対策手順で類似の事故が発生しないかどうかを検証し、問題があれば対策に反映することが望ましい。

4.2.2　個人情報保護の実行組織

［Ⅱ－２．個人情報保護の実行組織］では、《１．個人情報保護に係るリスクマネジメント組織》、《２．情報システムの個人情報取扱い組織》、《３．個人情報を扱うユーザの組織》の３項目をキーワードとして取り上げている。

経営者はリスクマネジメント担当役員を任命するとともに、必要な職務権限を与える必要がある。リスクマネジメント部門は部門ごとに個人情報を扱う情報システムのリスク管理責任者や運用管理責任者を定め、情報セキュリティ対策を推進する組織体制を確立する必要がある。各部門担当者は兼務でもよいが、各々の管理状況を確認し、コンプライアンス・プログラムに沿った運用が行われていることを確認するため、リスクマネジメント部門は定期的に各担当者を招集して管理状況を確認することが望ましい。

4.2.3　個人情報保護に関するマネジメントシステムの維持

［Ⅱ－３．個人情報保護に関するマネジメントシステムの維持］では、《１．評価》、《２．是正改善》、《３．監査》、《４．監視》、《５．文書化》、《６．リスクコミュニケーション》、《７．教育の承認》、《８．教育の実施》、《９．経営者のレビュー》の９項目をキーワードとして取り上げている。

経営者は、個人情報保護に係るマネジメントシステムのパフォーマンスや有効性を評価し、必要な是正措置が行われていることを確認しなければならない。個人情報を取り巻く環境やリスク

要因は常に変化するため、年に１回以上は監査を行い、そこで指摘された事項や改善指摘への対応が正しく行われていることを確認する義務を持つ。また、経営者層を含む従業員全員に教育・訓練が行われているかを確認し、漏れが出ないように監督しなければならない。

リスクマネジメント部門は、個人情報保護に係るパフォーマンスや有効性の評価を行い、継続的に是正・改善を行う機能を維持しなければならない。また、リスク環境は常に変化するため、定期的にリスク情報を収集し、適切な措置を行うための仕組みを持ち、運用しなければならない。教育・訓練の実施は特に重要なため、一方的な説明に終始することなく、理解度テストを行って習熟度を確認したり、次回の教育内容にフィードバックしながら継続的に行わなければならない。また、経営者を含めた全員で個人情報保護マネジメントシステムのレビューを行い、継続的にスパイラルアップすることが重要である。

4.2.4　個人情報保護に関わるリスク分析

個人情報保護に関するリスクマネジメントにおいて重要なのはリスク分析である。［Ⅱ－４．個人情報保護に関わるリスク分析］は、《１．リスク分析の仕組み》、《２．リスク分析の体制》、《３．リスク分析の実施》、《４．利用目的》、《５．取得》、《６．第三者提供》、《７．安全管理》、《８．本人関与・苦情処理》」の８項目をキーワードとして取り上げている。

個人情報保護に関わるリスク分析を行うためには、リスクマネジメントにおける個人情報保護の位置づけを明確にするとともに、常に状況の変化によって増減するリスクを分析するための社内体制の整備、そして、マネジメントシステムの基本である PDCA サイクルを意識した、リスク分析の評価から対応策の実施に至る機能を組織として確立することが重要である。

法令やガイドラインなどを遵守してルールを守った活動を実践すること、また、個人情報についても適法、かつ、公正な取扱いを実施することは事業者の責務であり、それを実行させることは経営者の責任である。このような考えに則り、コンプライアンスに関するチェック項目をリスク分析においても記載している。

個人情報保護を行うためには、個人情報の取得（収集）、利用、保管、預託、提供、廃棄にわたる個人情報のライフサイクル全体を視野にいれたリスク分析が不可欠である。

《リスク分析の実施》にあたって最初に取り組むことは、事業者で保有している個人情報をすべて洗い出すことである。そして、洗い出された個人情報に関するリスクを検討し、発生するリスクの頻度や影響度を考慮しつつ、リスク評価のための評価基準を設定する。リスク評価はその評価基準に基づき決定されることとなる。また、定期的なリスク分析の実施と新規に個人情報の収集が発生した場合や個人情報の取扱いに変化が生じた場合、リスク分析を行う手順を規定化することも重要である。新たに取得した個人情報やすでに保有している個人情報については、利用目的を通知または公表し、本人の知り得る状態にしておく必要があり、利用目的の通知又は公表を行わなかった場合や目的外利用が生じた場合の手続も含めたリスク分析が必要である。

《取得》については、適法かつ公正な手段で取得が行われているか、取得した情報の中に機微情報があるかなどのリスク分析が必要である。

《第三者提供》について、個人情報保護法では第三者提供と目的外利用については、いくつかの例外事項を除いてあらかじめ本人の同意を必要としており、注意が必要である。委託先への対応を含め慎重にリスクを洗い出す必要がある。また、共同利用については第三者提供に該当しな

いが、通知又は本人の知り得る状態におく事項が定められているので、これらの事項への対応についてリスク分析を行う必要がある。

《安全管理》については、取り扱う個人情報の漏えい、滅失又はき損を防止するためのリスク分析を行うこととなる。規程類の整備、組織体制の整備、問題が発生した場合の報告連絡体制、人的安全管理措置としての雇用契約、就業規則、従業員の教育研修、物理的安全管理措置としての入退室管理、個人情報や機器装置等の盗難防止、技術的安全管理措置としての情報システムへのアクセス制御、不正アクセス防止、ウイルス対策、ログの取得、情報システムやネットワークの監視、さらに、委託業者の選定、契約、監督などのさまざまな内容についてリスク分析を行う必要がある。

そして、《本人関与・苦情処理》については本人への個人情報の利用目的等の周知方法、開示請求等が発生した場合の本人確認から開示請求等に至るまでの手順、苦情処理への対応手順についてリスク分析が必要である。

このように個人情報保護に関するリスク分析を行うためには、幅広い観点からの分析が必要である。このためにも［Ⅱ－４．個人情報保護に関わるリスク分析］を用いてリスク分析を実施し、個人情報保護に関するリスクを把握するとともに、リスク対策へと通じる流れを確立することが重要である。

4.2.5　個人情報保護に関わるリスク対策

［Ⅱ－５．個人情報保護に関わるリスク対策］では、［Ⅱ－４．個人情報保護に関わるリスク分析］の項目の中で、特にリスク対策に必要な項目を抽出し、その実施状況を確認する内容となっている。キーワードとしては、《１．安全管理対策》、《２．適切な取扱い》、《３．リスクファイナンス》、《４．第三者提供対策》、《５．本人関与対策》の５項目を取り上げている。

《安全管理対策》では、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置、委託業者への対応、事故時の対処などについて確認を求めている。

《適切な取扱い》では、利用目的の特定、目的外利用の際の手順と対応などについて、《リスクファイナンス》では、個人情報の漏えいなどが発生した場合のリスクファイナンスの実施について、《第三者提供対策》では、第三者提供をする場合のあらかじめの同意の取得や共同利用を行う際の対応について確認を求めている。

そして、《本人関与対策》では本人への利用目的の周知、開示請求への対応、苦情処理体制の整備について確認を求めている。

このように個人情報保護を行うためには、個人情報保護計画の中にリスク分析とリスク分析結果の反映を位置づけ、個人情報保護体制の確立を図ることが必要である。

4.3　情報システムのリスク分析

4.3.1　情報システムのリスク分析および情報システムのリスク対策の位置づけ

ＪＲＭＳが４部構成になっていることは前述のとおりである。第Ｉ章、第Ⅱ章は個人情報保護を対象とした企業全体のリスク分析とリスク対策である。そして第Ⅲ章が情報システムのリスク分析、第Ⅳ章が情報システムのリスク対策となっている。

個人情報保護は全社的な取組みであることは明らかであるが、そのリスクの性質上、やはり情報システム部門の占める割合は高い。たとえば、最近の情報漏えい事故の原因のいくつかは情報システム部門が関与しなければ是正できないものがある。

表４－１．個人情報漏えい事故事例および対応策

事故事例	対応策
モバイルパソコンを社内に放置しておいたところ車上荒らしに遭い、盗まれた。	モバイルパソコンへの個人情報のダウンロード件数を制限する。あるいはファイルに暗号をかけたり、ファイルへのパスワード設置、起動時のパスワード設置が必要。
顧客データベースのバックアップファイルがひそかにコピーを取られていた。	ファイル管理やアクセス管理が必要。
メールからウイルスが侵入しパソコンにあったファイルが自動的にメール添付で発信された。	ウイルス対策ソフトの導入と正しい運用管理が必要。またファイアウォールの設定とファイルの格納場所の変更などが必要。
データ交換ソフトの誤用により個人情報のファイルを誤って送信してしまい、そのファイルを電子掲示板に公開された。	ファイル持出し規則の制定および従業員の教育などが必要。
インターネットによるアンケートにより収集していた個人情報データベースにハッカーが侵入し内容が書き換えられていた。	ファイアウォールの設置やファイルの格納場所の変更、ハッカー侵入検知などの監視システムの導入などの対策が必要。

この他にもさまざまな事例があり、当然第Ｉ章、第Ⅱ章で触れたように経営者の判断と従業員の日常業務での取組みが必要なため、全社的なリスクマネジメントとしても取組みが必要であるが、情報システム部門固有の実施事項も多い。そのため、ここでは情報システム部門を中核において個人情報を対象としたリスク分析とリスク対策の章を設けることとした。

4.3.2　情報システムのリスク分析およびリスク対策の構造

第Ｉ章、第Ⅱ章と同様、ここでも第Ⅲ章、第Ⅳ章がペアとなっている。これはＪＲＭＳの基本的な考え方であるもので、従来の日本の一般的なリスク対策が、「はじめに対策ありき」でスタートしていることを改める意図がある。リスク分析をまず実施し、そのリスクに応じてリスク対策を行うことを基本的な考えとしている。

次に回答者の選定であるが、ここでは第Ｉ章、第Ⅱ章とは異なり、リスクマネジメント部門のかわりに情報システム部門を事務局部門としている。経営者層およびユーザ層は第Ｉ章、第Ⅱ章と同様であるが、経営者層の質問項目は情報システムの技術的な項目を対象とはせず、全体的に質問数を絞っている。

情報システム部門の回答者は情報システム担当役員（CIO）のほか、情報システムリスクマネジメント担当者、情報システムリスク管理者、情報システム運用管理責任者、情報セキュリティ対策推進組織、情報セキュリティ管理者は必須とし、この他、企業の実態に応じてアウトソーシングの責任者や個人情報を取り扱うシステムの開発責任者などを想定している。

4.3.3 『個人情報保護編』の情報システムのリスク分析および情報システムのリスク対策の考え方

情報システムの一般的なリスクを対象として作成されたＪＲＭＳ質問項目が個人情報および個人情報を取り扱うシステム対象を絞った場合に適応できるかどうかについて、すべての項目について検討を行った。その結果、基本的な質問はそのまま適応できると判断した。ただし一部の質問については、個人情報に焦点をあてた場合によりふさわしい質問に変更することが適当と判断されたため、差替えを行った。

なお、ここで個人情報のリスクを考える際の重要事項を指摘しておく。それは個人情報のリスクを考えた場合、どうしても真っ先に頭に浮かぶのが個人情報漏えいによる損害賠償リスクや個人情報保護法違反による罰則の適用、行政処分の適用およびそれに伴う信用失墜などのリスクに偏ってしまうことである。個人情報のリスクには漏えいのみならず正確性の喪失による誤用や個人情報そのものの滅失、き損も大きなリスクであることを改めて認識していただきたい。機械の故障や火災・地震対策も個人情報の大きなリスクの一つの要素であることを忘れないでほしい。

4.3.4 情報システムのリスク分析

情報システムのリスク分析は全体を大きく３つに分け、さらにそれぞれをいくつかの小項目に分類している。以下、順にその内容を概括するとともに、「個人情報保護編」で従来のＪＲＭＳから修正したところを説明する。

表４－２．「Ⅲ．情報システムのリスク分析」の項目

Ⅲ－１	情報セキュリティポリシーのリスク分析
Ⅲ－２	情報システムのリスク分析
（１）	情報システムのリスク分析
（２）	システム開発
（３）	システム運用
（４）	アウトソーシング
Ⅲ－３	情報システムの個別リスク分析
（１）	不正アクセス・コンピュータウイルス関連
（２）	災害
（３）	障害

（１）【Ⅲ－１．情報セキュリティポリシーのリスク分析】

情報セキュリティポリシーの対象は個人情報を含めた情報セキュリティ全般を定めていくことが基本と考えられる。実際、多くの先進的な企業では個人情報のほかに営業情報や機密情報なども含めた統合的な情報セキュリティを検討・構築している。したがって、個人情報に注目した場合であってもＪＲＭＳの項目は適用できる。

以下、若干修正したところを述べる。

識別コード	＜KW＞および修正内容
3-1-1-3-1	＜機密漏えい＞ 機密漏洩について個人情報を括弧にて明記し、機密情報に個人情報を含めて検討するよう促すこととした。
3-1-1-6	＜ホームページ＞ 旧来の 3-1-1-7 より項目を移動させた。
3-1-1-7	＜複次的なリスク＞ 従来のシステミックリスクが金融機関などの風評リスクを対象とした用語であったため、より一般的な用語に修正した。意味としては業界のある企業で発生した事件により業界全体が対応策をとらなければならないような事件、および漏えいした情報が伝播する可能性を分析することである。

（２）【Ⅲ－２．情報システムのリスク分析】

情報システムの企画、開発、運用の各段階に発生するさまざまなリスクを対象としている。個人情報漏えいのみで考えると、どうしても運用時のリスクに眼がいってしまうが、本来は個人情報を取り扱うアプリケーションそのものの業務フローの検討や、個人情報を扱うシステムの企画、開発の段階での要件定義の段階でリスク分析が必要である。そのため、ここでは企画、開発、運用、そして個人情報保護でも重要な項目である委託、つまりアウトソーシングでのリスク分析をそれぞれ実施することを求めており、これらは個人情報に特化したものではなく、一般のリスクを対象としたＪＲＭＳの質問項目で包括されている。

以下、個人情報に特化した場合の若干の修正点を述べる。

①３－２－（１）情報システムのリスク分析：変更点なし

②３－２－（２）システム開発

識別コード	＜KW＞および修正内容
3-2-2-1	＜プロジェクトリスク＞ 個人情報に関するリスクを明記する。
3-2-2-2	＜企画段階＞ 個人情報保護の要件定義の確認を怠った場合、後からの要件の変更を余儀なくされると開発の遅延、コストの大幅な増加など、プロジェクトリスクの発生の可能性が高くなるため、プロジェクトリスクの検討にあたってのチェックポイントに個人情報保護の観点を加える必要がある。

③３－２－（３）システム運用

識別コード	＜KW＞および修正内容
3-2-3-2	＜ファイル管理＞ 個人情報を含むファイルとした。
3-2-3-2-2	＜バックアップ＞ バックアップの情報はあまり重視されないことが多いが、バックアップファイルを狙われた漏えい事件も発生している。 「Q3-2-3-2 ファイル管理」でリスクの想定を問うているので個人情報漏えいが含まれていることを明記した。

④３－２－（４）アウトソーシング：変更点なし

（3）【Ⅲ－3．情報システムの個別リスク分析】

ここでは情報リスクに大きな特徴であるリスク原因であるコンピュータウイルス、不正アクセス、災害、障害のそれぞれについてリスク分析を実施している。情報セキュリティの3つの要素である機密性、完全性、可用性の3点は個人情報でも同様であるため、本章はＪＲＭＳの項目がそのまま適用できる。

4.4 情報システムにおけるリスク対策

第Ⅲ章で情報システムのリスク分析を実施した。実際の企業ではこのリスク分析によりリスク発生の可能性、現時点でのリスク対策の実施状況や組織の脆弱性、そして万一リスクが発生した場合の損害程度の大きさを分析することが理想である。そしてそのリスクの大きさに応じてリスク対策を実施していくこととなる。ここではリスク対策について以下の各項目を提供している。実際の企業ではビジネス上該当しないもの、あるいはリスクが小さくて保有する方針を立てたために対策を実施しないものもある。これらの場合は得点のウエイトの修正を実施してもかまわない。くれぐれも「はじめに対策ありき」で対応策を実施しないことが重要である。

表4－3．「Ⅳ．情報システムにおけるリスク対策」の項目

Ⅳ－1	リスク対策における情報セキュリティ
Ⅳ－2	情報システムのリスク対策
（1）	情報システム総合企画
（2）	システム開発
（3）	システム運用
（4）	アウトソーシング
（5）	システム監査
Ⅳ－3	不正アクセス・コンピュータウイルス関連
（1）	コンピュータ犯罪
（2）	不正アクセス
（3）	コンピュータウイルス
（4）	E-Commerce
（5）	電子メール
Ⅳ－4	災害対策
Ⅳ－5	障害対策
Ⅳ－6	その他関連項目
Ⅳ－7	バックアップ
Ⅳ－8	緊急時対策

4.4.1 【Ⅳ－1．リスク対策における情報セキュリティ】

リスク分析を実施した後で経営者が定めたリスクマネジメントポリシーに基づいて情報セキュリティポリシーを定めていく。ここでは対策として情報セキュリティポリシーが要件どおり定められているかについて確認していく。具体的なリスク対策をとる場合はその項目が必ずポリシーの中に定められていなければならない。

個人情報の観点から修正した点は以下のとおり。

識別コード	＜KW＞および修正内容
4-1-1-2-11	＜災害・障害対策＞ 災害・障害対策として一つに集約した。
4-1-1-2-12	＜権限付与＞ 権限付与について追加した。個人情報保護についてはアクセス権限が重要なため、従来の実施基準に追加することとした。
4-1-1-3-5	＜JIS Q 15001との整合性＞ JRMSでは ISO15408 との整合性をチェックポイントとしていたが、個人情報を念頭においた場合、製品の認証規格より個人情報保護のJIS規格との整合性の方がより重要と判断した。
4-1-1-5	＜コンプライアンス＞ コンプライアンスおよび罰則規定を統合した。
4-1-1-6	＜廃棄基準＞ 個人情報については特に消去や廃棄が十分にされないために漏えい事故が発生する可能性があるため、新たに追加した。
4-1-1-14	＜情報セキュリティ・個人情報保護管理責任者＞ 個人情報を念頭においた場合、官公庁のガイドラインで個人情報の管理責任者の設置を求められているため、明記した。
4-1-1-14-3	＜個人情報作業責任者＞ 外部のコンサルタントやサービスを利用する形態が情報システムの分野では一般的であるが、個人情報保護の観点から外部のコンサルタントやサービスの利用についても責任者を明確にすることとした。
4-1-1-16	＜出張、移動中の実施基準＞ 車上荒しへの備えが必要であることが周知となっていることから、移動中の個人情報の管理の観点を明記した。
4-1-1-17-2	＜携帯端末紛失連絡体制＞ 個人情報を含む携帯端末と明記した。
4-1-1-18	＜授受記録＞ 旧Q4-1-1-24を移動した。
4-1-1-20	＜データ、媒体利用＞ 個人情報を含む媒体であることを明記した。個人情報の場合は特に物理的な媒体管理が重要である。
4-1-1-21	＜ログの定期的な確認・保管＞ ログについては定期的な取得に加え、さらに改ざんがされないようにアクセスログを安全に保管、管理する必要がある。
4-1-1-24	＜情報システム利用手続＞ 旧Q4-1-1-18を移動した。
4-1-1-28	＜情報システム部門の教育内容＞ 個人情報を念頭におくと個人情報保護の安全管理措置のうち、人的安全管理措置の中で教育が重要な位置を占めていることから、個人情報保護を網羅した教育内容であることを明記した。
4-1-1-29	＜ユーザ部門の教育内容＞ 情報システム部門同様に個人情報保護を網羅することを明記した。

4.4.2 【Ⅳ－2．情報システムのリスク対策】

情報システムリスク対策を行うためには情報システムの企画、開発段階からリスク対策を実施する必要がある。IT戦略やIT計画でのリスク対策や組織体制などの整備、スタッフのスキ

ルなどの対策も検討する必要がある。ここでは戦略や財務などを含む総合企画、プロジェクト管理、要件定義などの開発など、上位工程のリスク対策を検討する。また開発にあたってはテストデータの取扱い、変更管理などの技術的な要件も含む。そして運用ではモニタリング、復旧時間の設定、アウトソーシングでは役割分担、アウトソーサ管理、契約、知的財産権などに触れ、最後にシステム監査のチェック項目を網羅している。

以下個人情報の観点から修正した点は以下のとおり。

識別コード	＜KW＞および修正内容
4-2-2-11-2	＜保護データの排除＞ テストデータから個人情報が漏えいする事件が発生していることから、個人情報をテストに実施することの禁止などを確認することを明記した。
4-2-3-2	＜システム運用実施＞ 個人情報に利用するシステムは利用時間を制限することが望まれていることを明記した。
4-2-4-18	＜事件・事故報告・連絡体制＞ アウトソーシング先の事故は、個人情報保護法では事故が発生した場合には管理責任が問われるため、アウトソーシング契約に明記した。
4-2-4-21	＜委託契約ルール＞ 質問項目自体の変更はないが、個人情報保護問題を含むことを念頭においておくこととした。
4-2-4-23	＜安全管理＞ アウトソーシング先の事故は、個人情報保護法では事故が発生した場合には管理責任が問われるため、委託契約に安全管理を明記した。
4-2-4-25	＜従事者の監督＞ アウトソーシング先の事故は、個人情報保護法では事故が発生した場合には管理責任が問われるため、委託契約に安全管理を明記した。
4-2-4-33	＜委託先情報セキュリティ実施状況＞ 質問項目自体の変更はないが、個人情報の加工、利用、コピーなどの制限について注意することを念頭においておくこととした。

4.4.3 【Ⅳ－３．不正アクセス・コンピュータウイルス関連】

もっとも情報リスクの特徴をあらわす管理項目である。コンピュータ犯罪対策、不正アクセス対策、コンピュータウイルス対策、電子メール対策を網羅している。また、電子商取引を実施している場合はE-Commerceに対するリスク対策をノミネートしている。

主な項目として、内部犯罪の防止、データ保護、盗聴対策、論理的アクセス管理、物理的アクセス管理、認証、暗号、ファイアウォール、ログ取得、不正検出、緊急時対応、ウイルス対策、セキュリティホール対策、インターネット接続対策、電子的証拠の取得、サーバ管理、メール転送などについて記載している。

個人情報の観点から修正した点は以下のとおり。

識別コード	＜KW＞および修正内容
4-3-2-1-1	＜認証＞ 個人情報保護の観点から作業担当者のID、パスワードによる認証、生体認証などによる識別が定められているか、具体的に質問項目を明記した。
4-3-4-2	＜プライバシー保護対策＞ ここでは JIS Q 15001 の取得に触れているが、この質問は E-Commerce を採用している場合に限定しての質問項目となる。 E-Commerce を採用していない場合はこの4－3－(4)の項目全体が対象外となるため、別途 JIS Q 15001 の関連を配慮する項目を設けていることは前述のとおりである。

4.4.4 【Ⅳ－4．災害対策】

地震、洪水、火災などの災害対策に対する質問である。以前に比較して物理的なセキュリティについては関心度合いが下がっているが、平成16年度は大型台風が10個上陸、梅雨前線の影響で豪雨も多く発生し、浸水による情報システムの利用停止の問題が再認識された。また、新潟県中越地震も含め、これらの災害で情報システムの利用停止あるいは情報そのものの滅失があった場合の対策を再点検する必要がある。個人情報に焦点をあてて検討したが、ＪＲＭＳの項目に修正はない。

4.4.5 【Ⅳ－5．障害対策】

従来から比較するとハードウェアや基幹ソフトウェアの安定性は増してきているが、やはり一定の頻度で機械の故障などは避けられない。ハードウェア障害、ソフトウェア障害、ネットワーク障害、トランザクション管理、ユーティリティ管理など、基礎的な管理項目を述べている。個人情報に焦点をあてて検討したが、ＪＲＭＳの項目に修正はない。

4.4.6 【Ⅳ－6．その他関連項目】

情報リスクを社会的な観点からみた場合のリスク対策を述べている。政治・経済・社会的リスク対策、テロ対策、会員制の場合の会員規則、規約違反、ユーザ間のトラブル対策、苦情対応および危機管理などがある。なお、苦情対応については個人情報保護法でも苦情対応について努力義務が課せられているため、今後充実させる必要がある。個人情報に焦点をあてて検討したが、ＪＲＭＳの項目に修正はない。

4.4.7 【Ⅳ－7．バックアップ】

情報リスクの軽減対策のうち、重要な対策の一つが情報のバックアップ対策である。ここではそのバックアップに特化した対策項目を設けている。チャネルや機器の二重化対策、ファイルのバックアップ、ネットワーク対策、予備サイトの確保などがある。個人情報に焦点をあてて検討したが、ＪＲＭＳの項目に修正はない。

4.4.8 【Ⅳ－8．緊急時対策】

実際にリスク対策を実施していても残念ながら事件や事故は発生することを覚悟しておかなければならない。またその事件や事故があることを想定し、あらかじめ緊急時対策を講じてお

くと迅速・的確な対応をとる可能性が高くなり、その結果、万一発生した事件や事故の損害を大きく軽減できる。ここでは事前準備、対策本部、業務の優先順位、障害の切分け、復旧計画などを定めている。

個人情報の観点から修正した点は以下のとおり。

識別コード	＜KW＞および修正内容
4-8-1-1-2	＜機密・個人情報漏えい対策＞ 重要な情報に個人情報を明記した。
4-8-1-3-9	＜情報資産＞ 個人情報に特化して記載した。
4-8-1-3-10	＜情報漏えい等の発見時の通報・究明手順＞ 情報漏えいを明記した。

JRMS個人情報保護編
―質問項目および解説―

（JIS　Q 15001　対照表付）

JIS Q 15001対照表の見方

JRMSでは階層構造をとっているため、JISの大項目がJRMSの第5階層にあてはまる場合でも、第4階層がJISの大項目と合っていない場合は対象外としている。すなわちJISとJRMSの階層がある程度近いものを選んでいる。（下位の階層での内容が一致しない場合は対応させていない。）

- JRMS質問項目のキーワードと項目がJIS Q 15001の内容をカバーしている場合は、その見出しに相当する章番号を記載している。
- （ ）がついた項目は、JRMSで述べていることとJIS Q 15001との内容が近く、関連があることを示している。
- [ ] がついた項目は、JRMSとJIS Q 15001との内容で大きく異なるが、共通するものを含んでいることを示す。なお、章番号はJIS Q 15001の下記に示す番号である。

大項目		識別コード	質問項目数		該当項目数			
			第4階層の項目数	全項目数	経営者	RM	IS	ユーザ
Ⅰ	**経営と個人情報保護**		**9**	**21**	**11**	**20**	**0**	**18**
Ⅰ－1	個人情報保護とリスク	1－1－1－ 1 ～ 9	9	21	11	20		18
Ⅱ	**個人情報保護に関するリスクマネジメント計画**		**79**	**191**	**46**	**191**	**0**	**176**
Ⅱ－1	個人情報保護に関するリスクマネジメント計画	2－1－1－ 1 ～ 15	15	44	12	44		40
Ⅱ－2	個人情報保護の実行組織	2－2－1－ 1 ～ 8	8	11	5	11		7
Ⅱ－3	個人情報保護に関するリスクマネジメントシステムの維持	2－3－1－ 1 ～ 19	19	31	7	31		25
Ⅱ－4	個人情報保護に関わるリスク分析	2－4－1－ 1 ～ 27	27	79	17	79		79
Ⅱ－5	個人情報保護に関わるリスク対策	2－5－1－ 1 ～ 10	10	26	5	26		25
Ⅲ	**情報システムのリスク分析**		**54**	**152**	**0**	**0**	**152**	**87**
Ⅲ－1	情報セキュリティポリシーのリスク分析	3－1－1－ 1 ～ 10	10	26	0		26	13
Ⅲ－2	情報システムのリスク分析		19	64	0	0	64	44
	(1)情報システムのリスク分析	3－2－1－ 1 ～ 7	*7*	*36*	*0*		*36*	*22*
	(2)システム開発	3－2－2－ 1 ～ 5	*5*	*15*	*0*		*15*	*13*
	(3)システム運用	3－2－3－ 1 ～ 3	*3*	*6*	*0*		*6*	*3*
	(4)アウトソーシング	3－2－4－ 1 ～ 4	*4*	*7*	*0*		*7*	*6*
Ⅲ－3	情報システムの個別リスク分析		25	62	0	0	62	30
	(1)不正アクセス・コンピュータウイルス関連	3－3－1－ 1 ～ 12	*12*	*23*	*0*		*23*	*7*
	(2)災害	3－3－2－ 1 ～ 6	*6*	*21*	*0*		*21*	*19*
	(3)障害	3－3－3－ 1 ～ 7	*7*	*18*	*0*		*18*	*4*
Ⅳ	**情報システムにおけるリスク対策**		**245**	**594**	**0**	**0**	**592**	**287**
Ⅳ－1	リスク対策における情報セキュリティ	4－1－1－ 1 ～ 29	29	91	0		89	74
Ⅳ－2	情報システムのリスク対策		94	167	0	0	167	105
	(1)情報システム総合企画	4－2－1－ 1 ～ 29	*29*	*36*	0		*36*	*29*
	(2)システム開発	4－2－2－ 1 ～ 22	*22*	*61*	0		*61*	*20*
	(3)システム運用	4－2－3－ 1 ～ 7	*7*	*23*	0		*23*	*10*
	(4)アウトソーシング	4－2－4－ 1 ～ 36	*36*	*36*	0		*36*	*36*
	(5)システム監査	4－2－5－ 1 ～ 6	*6*	*11*	0		*11*	*10*
Ⅳ－3	不正アクセス・コンピュータウイルス関連		60	151	0	0	151	59
	(1)コンピュータ犯罪	4－3－1－ 1 ～ 9	*9*	*22*	*0*		*22*	*13*
	(2)不正アクセス	4－3－2－ 1 ～ 19	*19*	*53*	*0*		*53*	*23*
	(3)コンピュータウイルス	4－3－3－ 1 ～ 10	*10*	*22*	*0*		*22*	*13*
	(4)E－Commerce	4－3－4－ 1 ～ 11	*11*	*31*	*0*		*31*	*6*
	(5)電子メール	4－3－5－ 1 ～ 11	*11*	*23*	*0*		*23*	*4*
Ⅳ－4	災害対策	4－4－1－ 1 ～ 28	28	57	0		57	8
Ⅳ－5	障害対策	4－5－1－ 1 ～ 12	12	37	0		37	12
Ⅳ－6	その他関連項目	4－6－1－ 1 ～ 7	7	18	0		18	18
Ⅳ－7	バックアップ	4－7－1－ 1 ～ 10	10	41	0		41	2
Ⅳ－8	緊急時対策	4－8－1－ 1 ～ 5	5	32	0		32	9
計			**387**	**958**	**57**	**211**	**744**	**568**

カテゴリ		キーワード一覧								
Ⅰ．経営と個人情報保護	Ⅰ－1．個人情報保護とリスク	1.経営者の関心	2. 個人情報保護方針	3. 個人情報保護方針のフレームワーク	4. 個人情報保護の監査	5. 個人情報保護方針の周知				
		経営者の関心	全社的な個人情報保護方針	基本目的	監査	周知				
			最高経営者の承認	経営への脅威	内部監査					
			経営理念との整合	守るべき対象	外部監査					
				役割・責任						
				課題の明確化						
				社会的責任の明確化						
				個人情報保護関連リスクの報告体制						
				緊急事態発生時対応						
				コンプライアンス違反						
				責任部門						
				実施基準						
				フィードバックループ						
				行動指針						
Ⅱ．個人情報保護に関するリスクマネジメント計画	Ⅱ－1．個人情報保護に関するリスクマネジメント計画	1．経営理念と個人情報保護計画	2. 個人情報保護のリスク管理体制の組織化	3. 個人情報保護の管理目標	4. 個人情報保護の目標脅威	5. 個人情報保護の分析	6. 対策	7. 緊急時対応	8. 個人情報保護計画の周知	
		経営理念	管理体制	管理目標	目標脅威	分析方法	リスク対策への反映	緊急時対応	周知	
		保護対象	リスク分析責任者	物理的資産	物理的資産	費用対効果分析	対策策定方法	事故		
			リスク対策責任者	情報資産	情報資産	ハザード分析	対策実施基準	災害		
			リスクファイナンス責任者	経済的損失	経済的損失	ギャップ分析	経営者の承認	サービス欠陥		
			基本目的	機会損失	機会損失			サービス供給停止		
			対策実施の責任権限	実施基準	企業信用、ブランド価値			企業信用、ブランド価値		
			意思決定プロセス	雇用管理情報	雇用管理情報			雇用管理情報の喪失		
				コンプライアンス	コンプライアンス違反			コンプライアンス違反		
					サイバーテロ			サイバーテロ		

カテゴリ		キーワード一覧								
Ⅱ．個人情報保護に関するリスクマネジメント計画	Ⅱ－2．個人情報保護の実行組織	**1．個人情報保護に係るリスクマネジメント組織**	**2．情報システムの個人情報取扱い組織**	**3．個人情報を扱うユーザの組織**						
		リスクマネジメント担当役員の任命	**情報システムリスク管理体制**	**適用業務別オーナー**						
		リスクマネジメント推進体制	情報システムリスク管理者	**ユーザ部門リスク担当責任者**						
		リスクマネジメント担当者の役割権限	情報システム運用管理責任者							
		情報システムリスクマネジメント担当者の役割権限	**情報セキュリティ対策推進組織**							
			情報システム情報セキュリティ管理者							
	Ⅱ－3．個人情報保護に関するリスクマネジメントシステムの維持	**1．評価**	**2．是正改善**	**3．監査**	**4．監視**	**5．文書化**	**6．リスクコミュニケーション**	**7．教育の承認**	**8．教育の実施**	**9．経営者のレビュー**
		パフォーマンス評価	**是正改善**	**個人情報保護監査**	**監視手段**	**基準の文書化**	**リスクコミュニケーションの実施**	**経営者の教育承認**	**個人情報取扱責任者・担当者の教育訓練計画**	**リスクマネジメントシステムレビュー**
		パフォーマンス評価基準	是正改善行動採択基準	内部監査	**変化の監視**	**リスクマネジメント文書管理**	リスクコミュニケーション手段	個人情報取扱責任者・担当者の教育訓練計画	**情報システム部門の教育**	
		パフォーマンス監視	フィードバックループ機能	外部監査		**リスク変化の記録**	**リスク情報開示**	情報システム部門の教育訓練計画	**従業者の教育**	
		有効性評価	是正改善状況の点検			**実績記録**		従業者の教育訓練計画		
			是正改善の有効性評価					**教育の位置づけ**		
			ボトルネックの排除							

カテゴリ		キーワード一覧								
Ⅱ．個人情報保護に関するリスクマネジメント計画	Ⅱ－4．個人情報保護に関わるリスク分析	1．リスク分析の仕組み	2．リスク分析の体制	3．リスク分析の実施	4．利用目的	5．取得	6．第三者提供	7．安全管理	8．本人関与・苦情処理	
		リスク分析の実施	変化を含めた社内体制	リスク洗出し	利用目的の特定の手続	不正取得	第三者提供	正確性の確保	周知	
		未実施の場合の問題の認識	対応優先順位	洗出し実施基準	直接取得時の利用目的明示	機微情報の取得	第三者提供の禁止	個人情報保護組織・体制の整備	保有する個人情報の把握	
		関連情報提供システム	フィードバック	日常的な洗出し	間接取得後の利用目的明示	保存期間	第三者提供停止（オプトアウト）	安全管理措置の組織・体制の整備	保有する個人情報の公表	
		保護対象リスク分析	分析の予算・スタッフ	特定部門からの要請による洗出し	利用目的の特定		外部委託先への提供	組織体制の整備	開示	
				頻度算定	利用目的の特定手順の承認方法		共同利用	個人情報保護規程の整備	利用目的非通知時の取扱い	
				頻度算定実施基準	利用目的の変更			マニュアル	利用停止等の手続	
				影響度算定	目的外利用の同意			個人情報取扱台帳	本人対応（理由）手続	
				影響度算定実施基準				個人情報の消去・廃棄	開示手続	
				リスク評価				事故・違反への対応	開示手数料	
				リスク評価基準				社内不正	利用目的の通知の求めに応じないリスク	
								漏えいの影響	非開示情報の取扱いの通知	
								滅失又はき損の影響	訂正・削除等	
								二次被害	苦情処理体制の整備	
								事故の公表	苦情対応手順	
								人的安全管理措置		
								非開示契約		
								物理的安全管理措置		
								入退室（館）管理		
								盗難防止対策		
								機器・装置の物理的保護		
								技術的安全管理		
								アクセス制御		
								不正ソフトウェア対策		
								情報システムの監視		

カテゴリ		キーワード一覧								
Ⅱ．個人情報保護に関するリスクマネジメント計画	Ⅱ－4．個人情報保護に関わるリスク分析							**従業者の監督**		
								教育・研修		
								外部委託		
								委託先選定		
								委託契約		
								委託先の監督		
								委託先(安全)管理		
								委託先の定期確認		
	Ⅱ－5．個人情報保護に関わるリスク対策	**1．安全管理対策**	**2．適切な取扱い**	**3．リスクファイナンス**	**4．第三者提供対策**	**5．本人関与対策**				
		正確性の確保	**利用目的の特定の手続の実施**	**リスクファイナンス**	**本人の同意**	**周知**				
		安全管理対策の実施	直接取得時の利用目的明示		第三者提供停止(オプトアウト)	開示				
		組織的安全管理措置の実施	間接取得後の利用目的明示		共同利用	苦情処理体制の構築				
		人的安全管理措置の実施	利用目的の特定							
		物理的安全管理措置の実施	利用目的特定手順の承認							
		技術的安全管理措置の実施	利用目的の変更							
		監督の実施	目的外利用							
		従業者の監督の実施	**適正な取得**							
		委託先の監督の実施	**取得の制限**							
		事故・違反への対策								

カテゴリ		キーワード一覧								
Ⅲ.情報システムのリスク分析	Ⅲ-1.情報セキュリティポリシーのリスク分析	1.情報セキュリティの経営からの視点	2.情報セキュリティポリシーの対象	3.特筆する情報リスク	4.時間分析	5.情報リスク洗出し実施基準				
		経営の視点からの分析	リスク分析の対象	基幹システム情報漏えい(情報)	機能停止	情報リスク洗出し実施基準				
			災害	複次的なリスク						
			障害	ホームページ						
			不正アクセス	基幹システムダウン						
			偽造・不正使用リスク							
			コンピュータウイルス							
			アウトソーシングのリスク							
			SLA							
			緊急時対応							
			機密漏えい							
			不正アクセス							
			コンピュータウイルス							
			ネットワーク障害							
			災害							
			障害							
			緊急時対応							
			ファシリティ移動							
			情報セキュリティ推進組織内容							
			監査内容							

カテゴリ			キーワード一覧								
Ⅲ.情報システムのリスク分析	Ⅲ-2.情報システムのリスク分析	3-2-(1)情報システムのリスク分析	1.IT戦略のリスク分析	2.情報資産リスク	3.システム不全	4.適用業務責任・権限	5.適用業務とリスクマネジメント				
			IT戦略のリスク分析	情報資産リスク	機能不全	適用業務責任・権限	情報システム適用業務				
			情報システムの重要度測定	重要性ランキング	ネットワーク	企画業務	設計時の前提				
			情報の重要度測定	オーナーの明確化	誤作動	開発業務					
			業務への影響	機密度ランク	犯罪	運用業務					
			E-Commerce	可用性維持	対応ミス	保守業務					
			情報リスクと経営存続	複数人によるリスク分析	質低下	予算業務					
				人的リスク	安全性・機密保持の悪化	その他機能分野					
				改ざんリスク	変化への対応性欠如						
				破棄							
				盗難							
				物理的侵入							
				物理的攻撃							
				倒産							
		3-2-(2)システム開発	1.プロジェクトリスク	2.ライフサイクル	3.開発管理	4.運用テスト					
			プロジェクトリスク	ライフサイクル	開発管理	運用テスト結果					
			企画段階		スタッフのスキルの妥当性	稼働開始による障害発生					
			技術面		コンプライアンス	運用テスト結果					
			ビジネス面		開発環境						
			組織面		ソフトウェアのサポート切れ						
					ソフトウェアのバージョンアップ						
		3-2-(3)システム運用	1.システム運用	2.運用管理	3.キャパシティ管理						
			円滑運用	ファイル管理	キャパシティ管理						
				ライブラリ管理							
				バックアップ							
				適用業務管理							

カテゴリ			キーワード一覧								
Ⅲ.情報システムのリスク分析	Ⅲ-2.情報システムのリスク分析	3-2-(4)アウトソーシング	1.アウトソーサの決定	2.役割分担	3.守秘義務						
			アウトソーサの選定手続	契約内容	守秘義務						
				責任分担	再委託時の守秘義務						
				作業内容							
				変更管理							
	Ⅲ-3.情報システムの個別リスク分析	3-3-(1)不正アクセス・コンピュータウイルス関連	1.コンピュータ犯罪のリスク	2.不正アクセスのリスク	3.コンピュータウイルスのリスク	4.電子メールのリスク	5.ネットワークのリスク				
			経営に与える影響	モバイル機器盗難	コンピュータウイルス被害・復旧コスト	コンピュータウイルス誤配	ネットワークの大規模なダウン				
			内部犯罪による信頼への影響	インターネット経由内部犯罪	コンピュータウイルス被害による機会損失						
			経営者・従業員の意識	ネッティングリスク	感染の影響						
			盗聴による影響	妨害行為	取引先への影響						
			脅迫による影響		株価への影響						
			改ざん		損害賠償請求						
			破壊		ベンダ緊急時対応の遅れ						
			情報漏えい		アンチウイルス更新遅れ						
					定期検診以上の要延						
		3-3-(2)災害	1.管理	2.災害	3.事故	4.人的災害	5.委託先リスクの可能性				
			情報システムへの影響	自然災害	事故	人的災害	委託先リスクの可能性				
			災害復旧手順	地震・津波・噴火	火災・爆発	戦争・動乱・暴動による影響					
				台風・高潮	停電	人的リスクの可能性					
				水災・洪水	人的損失						
				竜巻・風災	漏水						
				落雷	動物害						
				雪害							
				雹害							
				天候不良・異常気象							

カテゴリ			キーワード一覧								
Ⅲ.情報システムのリスク分析	Ⅲ-3.情報システムの個別リスク分析	3-3-(3)障害	1.管理	2.ハードウェア障害	3.ソフトウェア障害	4.運用ミス障害					
			情報システムへの影響	ハードウェア障害	ソフトウェア障害	運用ミス障害					
			復旧手順	ネットワーク(WAN)障害	OS、ライセンスプログラム障害	バックアップ不備					
				サーバ障害	アプリケーションプログラム停止	ソフトウェア更新手続ミス					
				ISPサービス機能障害	アプリケーションプログラム誤処理	人的リスクの可能性					
				端末機器障害	端末機器障害						
				停電	その他ソフトウェア障害						
Ⅳ.情報システムにおけるリスク対策	Ⅳ-1.リスク対策における情報セキュリティ		1.情報セキュリティポリシー	2.情報セキュリティポリシーに基づく実施基準	3.情報資産インベントリ	4.スタッフ	5.情報セキュリティ個別対策	6.自社ホームページ承認	7.教育内容		
			情報セキュリティポリシー	情報セキュリティポリシーに基づく実施基準	情報資産目録	情報セキュリティ・個人情報保護管理担当者	操作と業務処理手順	自社ホームページ承認	情報システム部門の教育内容		
				情報システム総合企画	劣化媒体の排除	スタッフ	出張、移動中の実施基準	掲載許可	緊急事態対応		
				システム開発	重要資産の取扱いと重要装置の仕様	業務ローテーション	携帯端末利用	コンテンツの知的財産権	誤作動対応		
				システム運用	機密度ランク	個人情報作業責任者	ユーザ認証、アクセス管理	ホームページ記載内容のチェック	システム停止対応		
				アウトソーシング			携帯端末紛失連絡体制	コンテンツ侵害への手続	システム侵入対応		
				システム監査			授受記録	営業機密漏えいチェック	ユーザ部門の教育内容		
				コンピュータ犯罪			リスク管理文書化		緊急事態対応		
				不正アクセス			データ、媒体利用				
				コンピュータウイルス			ログの定期的な確認・保管				
				E-Commerce			アクセスログ権限				
				電子メール			機密情報ログ				
				災害・障害対策			プログラムソースライブラリ管理				
				権限付与			基幹システムの国際利用				
				その他関連項目			情報システム利用手続				
				バックアップ			プロバイダ選定基準				
				緊急時対策							

カテゴリ		キーワード一覧								
Ⅳ. 情報システムにおけるリスク対策	Ⅳ-1. リスク対策における情報セキュリティ		**リスクマネジメントシステム計画との整合性**							
			企業特性							
			論理的な構築							
			評価リスト							
			緊急事態復旧計画							
			JIS Q 15001との整合性							
			ISO17799との整合性							
			実施基準での禁止事項							
			市販ソフトのコピー使用							
			データ・プログラムの無断使用							
			機密情報搾取行為							
			覗き見							
			コンピュータ私的利用							
			コンピュータウイルス伝染行為							
			不正侵入行為							
			WWWの私的利用							
			データ不正入力							
			私用電子メール使用							
			ファイルの覗き見行為							
			仕事以外のファイルの覗き見行為							
			他人のID無断使用							
			接続されたマシンの無断操作							
			個人情報の不正な取扱い							
			顧客情報の売却							
			ホームページによる誹謗中傷行為							
			電子掲示板による誹謗中傷行為							
			動作障害行為							

カテゴリ			キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-1.リスク対策における情報セキュリティ			プログラム・データ改ざん							
				無許可情報の開示行為							
				スパムメール発信行為							
				社会秩序を乱す情報提供							
				コンプライアンス							
				廃棄基準							
				情報オーナーの責任							
				自己点検システム・監査システム							
				実施基準の定期的見直し							
				企業内教育							
				情報セキュリティポリシーの徹底							
	Ⅳ-2.情報システムのリスク対策	4-2-(1)情報システム総合企画	1.実施基準	2.IT戦略	3.IT計画	4.組織体制・機能	5.スタッフ	6.財務	7.管理（文書化を含む）	8.モニタリング	
			情報システム総合企画	経営戦略との整合	IT戦略とITインフラ計画	指揮命令系統	人事計画	投資収益方針	全社データ管理	規制監視	
				標準ステップ	ITインフラ計画	インターナルコントロール機能	スキル	投資決定方法	全社データ標準化	是正措置	
				外部規制	導入計画	セキュリティ機能	プロジェクト管理スキル	短期的影響の想定	全社データ所有者の識別		
						品質管理機能	品質管理教育	長期的影響の想定	管理工程分割		
						決裁権限		他部門への影響の想定	工程ごとの品質基準		
						リスク別担当部門		ビジネス上の採算	ライセンス管理		
								予定利益	プロジェクト管理標準		
								IT資産管理目録	方法論		
								関連費用識別			

カテゴリ			キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-2.情報システムのリスク対策	4-2-(2)システム開発	1.実施基準	2.プロジェクト管理	3.システム要件定義	4.プログラム開発	5.テストデータ	6.運用テスト	7.変更管理		
			システム開発	システム開発方法論	セキュリティ基準の遵守	開発環境	テストデータ	テスト仕様書の内容	管理責任者		
			決裁実施基準	作業内容と成果物	要件の反映	機密保持のクラス分け	テストの機密保持規定	運用テストの結果	バージョンアップ手続		
			開発に応じた決裁	技法／ツール	SLA合意	プログラムライブラリへのアクセス管理	保護データの排除	導入の妥当性	管理方針		
			システム調達のライフサイクルにおけるセキュリティ	判定基準	システム要件の反映	高機密プログラムの保管	本番データ使用時の保護対策	システム性能	非常時の実施基準		
			調達	進捗管理手続	システム構成要素の入手可能性	設計文書保管	本番データとの分離	操作性確認	バックアップ・他所保管の実施基準		
			不正防止・機密保護基準			不正ソフトの混入対策		異常時バックアップ対応	区分によるバージョンアップ		
			破棄基準			コンプライアンス			変更管理		
			品質管理			知的財産権放棄・契約の要求事項			識別のための体系		
			要員			個人情報保護			ネーミングルール		
			職務定義			暗号輸出入管理			高機密プログラム保管		
			職務分離			各国法規遵守			レビュー検証		
			情報セキュリティ保持の役割・責任						レビュー内容の文書化		
			機密保持合意						管理責任者の承認		
									作業とレビューの分離		
									アクセスの職務分離		
									配布先でのバージョン管理		
		4-2-(3)システム運用	1.実施基準	2.システム運用	3.モニタリング機能	4.管理機能	5.復旧時間				
			システム運用	システム運用実施	記録・状況把握	ファイル世代管理	SLA				
			システム運用計画	定期的見直し	記録・監視	ライブラリ管理					
				システム運用管理	報告体制	障害管理					
				運用マニュアル	障害監視	適用業務管理方針					
				スケジュール運用確認	オンライン監視						
				運用手順	サーバの監視						
				データの適切性	クライアントPCの監視						
				スキルの妥当性	ネットワークの監視						

カテゴリ			キーワード一覧								
Ⅳ. 情報システムにおけるリスク対策	Ⅳ-2. 情報システムのリスク対策	4-2-(4)アウトソーシング	1.実施基準	2.目的	3.役割分担	4.プロジェクト管理	5.アウトソーサ管理	6.契約	7.知的財産権	8.セキュリティ上の留意点	
			アウトソーシング	TCC	責任分担	共通開発方法論	選定評価基準	委託契約ルール	知的財産権	委託先情報セキュリティ遵守	
				コスト削減	受託者内の責任範囲	プロジェクト管理手法	SLA	賠償上限	再委託における知的財産権	委託先情報セキュリティ実施状況	
				スリム化	受託者の役割分担	外注委託のレビュー	ペナルティ	安全管理	知的財産権侵害の責任分担	委託先情報セキュリティのマネジメント	
				関連技術の安価利用	委託者の役割分担	合意形成	事件・事故報告・連絡体制	開発納期延期		秘密保持	
				コスト削減			ソフトウェア障害時対応	従事者の監督		再委託時の秘密保持	
							品質管理	契約のチェック			
								受託先監査			
								変更手続			
		4-2-(5)システム監査	1.実施基準	2.監査	3.監査基準						
			システム監査	重要性の認識	監査基準						
				システム監査の実施							
				内部監査							
				外部監査							
				監査人の選任							
				リスクマネジメント責任者と監査人の位置づけ							
				報告先							
				勧告のフォロー							
				監査未実施							

カテゴリ			キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-3.不正アクセス・コンピュータウイルス関連	Ⅳ-3-(1)コンピュータ犯罪	1.実施基準	2.内部犯罪の防止	3.データ保護対策	4.盗聴対策	5.緊急時対応				
			コンピュータ犯罪	パスワードの変更	データ保護対策	盗聴対策	ネットワーク対策				
			内部犯罪対策	内部犯罪の定義	暗号化	録音機器持込管理	外部機関への相談				
			個人利用禁止	ネットワーク機器	デジタル署名	携帯電話持込	証拠保全				
			不正使用対策	個人使用システム	暗合鍵	PDA					
					セキュリティホール対策	無線LAN					
						電磁波漏れ					
		Ⅳ-3-(2)不正アクセス	1.実施基準	2.アクセス管理	3.物理的アクセス対策	4.論理的アクセス対策	5.ネットワーク上のデータ保護	6.外部アクセスからのデータ保護	7.不正検出	8.緊急時対応	
			不正アクセス	アクセス管理	不正侵入防止	重要なデータ保護対策	ネットワークの不正アクセス対策	移動体内蔵データ保護	アクセスログ確認	緊急対処方法	
			認証	不正アクセス防止	ネットワーク機器の不正防止	暗号	暗号化転送	接続方式	プロトコル	IPAへの届出	
			物理的アクセス対策	データ保護	入退室	デジタル署名	ファイアウォール	認証	ログ保存	JPCERT/CCへの相談	
			論理的アクセス対策	暗号利用		暗号鍵管理	DMZ	ネットワークサービス	ログ確認	外部機関への相談	
			外部からのアクセス	ID付与・パスワード管理		個人認証	ファイアウォールレイアウト	ソーシャルエンジニアリング対策			
			緊急時対策	ID付与・パスワード管理のレビュー		ペネトレーションテスト	重要データ保存管理				
				不正入手		システム個人認証	ログ記録機能				
				アクセス権付与チェック・レビュー		中継地回避の実施基準	ログ自動分析ツール				
				機密度・アクセス制限		中継地懸念とログ分析	検知機能				
				職務分離							
				インターネット利用							
				教育・訓練							
				不正アクセス対策教育							

カテゴリ			キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-3.不正アクセス・コンピュータウイルス関連	4-3-(3)コンピュータウイルス	1.実施基準	2.事前対策	3.教育・訓練	4.ウイルス対策	5.事後対策				
			コンピュータウイルス対策	ウイルス防止ソフト	教育・訓練体制	緊急連絡体制	事後対策				
			感染時の緊急時・事後対策	ウイルス検出・駆除	社員の教育・訓練	影響判断	感染情報				
					システム管理者の教育・訓練	情報収集	通知				
						感染ルート	体制強化				
						感染の緊急時対策	復旧対策				
						感染防止対策	再発防止対策				
						伝染防止	経験の共有化				
							IPAへの届出				
		4-3-(4)E-Commerce	1.実施基準	2.プライバシー保護	3.不良客情報管理	4.データ保護対策	5.ネットワーク機器対応	6.インターネット接続管理	7.電子的証拠		
			E-Commerce	プライバシー保護対策	不払い、不良客情報管理	電子商取引時のデータ保護対策	ネットワーク機器、サーバの信頼性	インターネット接続の規制	デジタル署名		
			個人情報保護対策	コンプライアンスプログラム	不良客情報入手	インターネットからの攻撃	ネットワーク機器、サーバの性能	インターネット接続機器管理	時刻証明		
			データ保護対策	プライバシーマーク取得		Dos攻撃対策		ファイアウォール管理			
			インターネット利用対策	クッキー対策		アタック対策		IDS			
			電子商取引規定			セキュリティホール対策		DNS管理			
						コンピュータウイルス対策		暗号			
						スパムメール対策		暗号利用に関する通知			
						改ざん対策		不正行為監視			
		4-3-(5)電子メール	1.実施基準	2.メールサーバ管理	3.ネットワーク機器管理	4.デジタル署名	5.悪質メール対策	6.転送エラー対策			
			電子メール利用対策	メールサーバのデータ保護対策	ネットワーク機器、サーバの信頼性	デジタル署名	添付ファイル	転送エラー			
			ユーザ利用	メールサーバへの攻撃	ネットワーク機器、サーバの性能		スクリプト				
			サーバ管理	Dos攻撃対策	インターネット接続機器管理		不正メール対策				
			インターネット利用	不正アクセス対策	ファイアウォール管理						
				セキュリティホール対策	DNS管理						
				コンピュータウイルス対策	暗号						
				不正メール転送	不正行為監視						

カテゴリ		キーワード一覧								
Ⅳ. 情報システムにおけるリスク対策	Ⅳ-4. 災害対策	1.実施基準	2.管理	3.防火対策	4.耐震対策	5.水害対策				
		災害対策	経営者の決定	防火壁	フリーアクセス耐震補強	コンピュータ室				
		自然災害対策	災害復旧レベル	コンピュータ室	コンピュータ機器の固定	上げ床				
		事故災害対策	事業再開	データ保管場所	転倒防止	防水堤・ピット				
		人的災害対策	災害復旧レベル	ネットワーク設備室	機器・ラックの固定	漏水検知機				
			改善レベル	コンピュータ設置場所	テープ落下防止策	排水口				
			是正措置	自動消火装置	機器の落下防止策	水落下防止策				
			避難対策	コンピュータ室	電源設備	吹込み対策				
				データ保管場所		防水シート				
				ネットワーク設備室		電源設備				
				コンピュータ設置場所						
				区画放出対応消火システム						
				コンピュータ室						
				データ保管場所						
				ネットワーク設備室						
				消火器						
				コンピュータ室						
				データ保管場所						
				ネットワーク設備室						
				コンピュータ設置場所						
				消火栓						
				コンピュータ室						
				データ保管場所						
				ネットワーク設備室						
				コンピュータ設置場所						

カテゴリ		キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-4.災害対策			**遮断装置**						
				コンピュータ室						
				データ保管場所						
				ネットワーク設備室						
				コンピュータ設置場所						
				2方向非常口						
	Ⅳ-5.障害対策	**1.実施基準**	**2.管理**	**3.手続**	**4.情報システム**	**5.ユーティリティ**	**6.ネットワーク対策**	**7.復旧**		
		障害対策	**障害対策**	**ソフトウェア更新手続**	**ディスク障害対策**	**施設障害対策**	**回線障害対策**	**復旧レベル**		
		ハードウェア障害対策	運用監視機能	最終テスト結果確認		適用業務優先順位	避雷針	代替手段		
		ソフトウェア障害対策	障害検出機能	更新記録整備		無停電装置	ネットワーク障害対策	是正措置		
		運用ミス障害	縮退運転機能	記録内容		無停電装置テスト				
			代替運転機能	**更新確認**		供給能力				
			回復機能	**ソフトウェア更新**		空調設備の多重化				
			サービスレベル	**障害管理票**		水冷				
			ポリシーとの整合性	**変更後障害**						
			管理責任者の承認							
			トランザクション量							
			トランザクション量の測定							
	Ⅳ-6.その他関連項目	**1.実施基準**	**2.サービス提供**	**3.ユーザ間トラブル**	**4.苦情処理対応**	**5.危機管理計画徹底**				
		その他関連項目	**会員規約**	**ユーザ間トラブル対策の決定**	**苦情処理対応の決定**	**危機管理計画の内外関係者への徹底**				
		経営リスク	**規約違反**	ユーザ間トラブル対策	苦情処理対応策	物的資産喪失・破壊				
		政治・経済・社会リスク	**通信の秘密保護教育**	法的責任・事後対応	苦情処理対応マネジメントシステム	情報資産喪失・破壊				
		テロ対策		法的責任・事後対応対象		その他資産喪失・破壊				

カテゴリ		キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-7.バックアップ	1.実施基準	2.二重化対策	3.ファイルのバックアップ	4.ネットワーク対策	5.予備サイト				
		バックアップ対策	二重化対策	プログラムバックアップ	代替回線	予備サイト設置				
			交換機、チャネル	実施方法	代替機	同一室内のバックアップ用コンピュータ				
			機器	遠隔地保管	手作業による代替手段	同一建物内のバックアップ用コンピュータ				
			LAN	同一サイト内保管		バックアップセンタ				
			WAN	OSファイルバックアップ		遠隔地バックアップセンタ				
			切替テスト	実施方法		バックアップサービス業者				
				遠隔地保管		相互バックアップ契約				
				同一サイト内保管						
				データファイルバックアップ						
				実施方法						
				遠隔地ミラーデータ						
				遠隔地保管						
				同一サイト内保管						
				保存期間						
				バックアップ頻度						
				DBファイルバックアップ						
				実施方法						
				遠隔地ミラーDB						
				遠隔地保管						
				同一サイト内保管						
				ボリューム						
				災害時用同一ディスク保有						
				ログバックアップ						
				ログの分別化						

カテゴリ		キーワード一覧								
Ⅳ.情報システムにおけるリスク対策	Ⅳ-8.緊急時対策	1.実施基準	2.事前対応	3.緊急時対応手続	4.復旧計画					
		緊急時対策	緊急時対応の訓練	緊急時対応手続の明確化	復旧計画					
		障害発生		緊急連絡網	復旧オーナー、管理者の選定					
		機密・個人情報漏えい対策		緊急時対応体制	代替手段					
		不正アクセス		代替対応手順	計画維持・テストのスケジュール化					
		マクロウイルス		障害解決のフローチャート化						
		自然災害		教育訓練計画						
		倒産		対策本部						
		法令侵害		判定基準						
		バックアップ		緊急事態宣言						
		ファシリティ移動		情報資産						
				情報漏えい等の発見時の通報・究明手順						
				バックアップ手順						
				危機障害発生時の適用業務優先順位						
				障害切分け						
				障害発生アラーム						
				障害管理票						
				定期的評価、是正改善						

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
経営と個人情報保護	経営と個人情報保護	Ⅰ．経営と個人情報保護					
個人情報保護とリスク	個人情報保護とリスク	Ⅰ－1．個人情報保護とリスク					
1．経営者の関心	経営者の関心	1- 1- 1- 1	Q 経営者は役員会において個人情報保護に関するリスクについて議論をしていますか？ (個人情報保護に係わるリスクは、組織としての判断によりますが、議論の内容によって役員のリスク認識が問われることになります。)	●			4.4.1
2．個人情報保護方針	全社的な個人情報保護方針	1- 1- 1- 2	Q 全社的な個人情報保護方針を有していますか？ (用語解説「個人情報保護方針」:事業者の個人情報保護に関する考え方を宣言するものです。)	●	●	●	4.2
	最高経営者の承認	1- 1- 1- 2- 1	Q 個人情報保護方針は、最高経営者の承認のもと全社的に策定されていますか？ (全社的にリスクマネジメントの実効性が確保できるためには最高経営者の承認を得ていることが必要ですが、個人情報保護方針がそのように策定されているかを確認します。) (用語解説「最高経営者」:組織の運営において最高の責任を担う者を指します。執行役員体制では、最高経営者はCEOを想定しています。)	●	●		4.2
	経営理念との整合	1- 1- 1- 2- 2	Q 個人情報保護方針は、貴社の経営理念に基づいて定めていますか? (経営理念を明確に反映して個人情報保護方針を定めているかを確認します。)		●		4.1
3．個人情報保護方針のフレームワーク	基本目的	1- 1- 1- 3	Q 個人情報保護方針は、基本目的が明確に設定されていますか? (リスク対応の基本目的が個人情報保護方針に明確に示されてこそ、組織として行動が可能となります。)	●	●	●	4.2
	経営への脅威	1- 1- 1- 4	Q 個人情報保護方針では、個人情報に係わるリスクが明確にされていますか? (個人情報保護を脅かすリスクすべてを具体的に示すことは困難ですが、全体に関わるリスクや各部署の諸活動に特有のリスクについて例示することは不可欠です。)	●	●	●	4.2
	守るべき対象	1- 1- 1- 4- 1	Q 個人情報保護方針では、組織が個人情報を守るべき対象として明確にしていますか? (組織の存続のため、何を守るべきか、その対象が明確に示されているかを確認します。)		●	●	4.2(a)
	役割・責任	1- 1- 1- 4- 2	Q 個人情報保護方針では、守るべき対象との関連において、個人情報保護に関する役割・責任・権限が文書化されていますか? (何をどう守るか、担当者の役割・責任・権限について、言葉ではなく、文書で明示されているかを確認します。)		●	●	4.2(a) 4.3.3
	課題の明確化	1- 1- 1- 4- 3	Q 個人情報保護方針では、組織における個人情報保護の課題を明確に定めていますか? (個人情報保護対応上の課題を具体的に示すことによって、ポリシーとしての意味がでてきます。この点が明確かを確認します。)		●	●	4.2(b)
	社会的責任の明確化	1- 1- 1- 4- 4	Q 個人情報保護方針では、個人情報保護に係わる課題に社会的責任を含んでいますか？ (組織が社会的存在であることからすれば、社会的責任との関連から個人情報保護に対応するのは当然のことですが、個人情報保護方針にこの点を含んでいるかを確認します。)		●	●	4.2(c)
	個人情報関連リスクの報告体制	1- 1- 1- 4- 5	Q 個人情報保護方針では、個人情報の漏えい、滅失又はき損、不正利用等により組織の存続を脅かすリスクについて、経営者層への報告体制を整備していますか? (経営にとって重要なのは、対応の遅れが組織の存続に作用するマイナス情報です。そうした情報を種々のルートから入手する機能があるかを確認します。)	●	●	●	4.2(d) 4.6

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
経営と個人情報保護	経営と個人情報保護	Ⅰ．経営と個人情報保護					
個人情報保護とリスク	個人情報保護とリスク	Ⅰ－1．個人情報保護とリスク					
3．個人情報保護方針のフレームワーク	緊急事態発生時対応	1- 1- 1- 4- 6	Q 個人情報保護方針では、個人情報の取扱いに関し緊急事態が発生した時の役員、スタッフ、担当者の役割が定められていますか？ (緊急事態発生時には時間との勝負で即応性が求められます。そのために、それぞれの担当者の役割を決めておくことが重要です。)		●	●	4.2(b)
	コンプライアンス違反	1- 1- 1- 4- 7	Q 個人情報保護方針では、コンプライアンス違反に対する処置を明示していますか？ (コンプライアンスは経営上の前提であり、それに対する違反はリスク発生の重大な原因の1つです。コンプライアンス違反のための対応措置が、個人情報保護方針に明示されているかを確認します。)	●	●	●	4.2(c) 4.3.3(f)
	責任部門	1- 1- 1- 5	Q 個人情報保護方針では、個人情報保護に関する責任部門が明記されていますか？ (経営上、個人情報保護に係わる責任の所在(部門)を明示しておくことが組織として不可欠です。この点が明記されているかを確認します。)	●	●	●	4.2
	実施基準	1- 1- 1- 6	Q 個人情報保護方針では、個人情報保護に関する実施基準が明確ですか？ (実施基準が明確でなければ、個人情報保護対策は具体性を欠くことになります。この点が組織として明確になっているかを確認します。)		●	●	4.2
	フィードバックループ	1- 1- 1- 6- 1	Q 個人情報保護方針が有効に機能するようフィードバックループ構成になっていますか？ (個人情報保護に係わるリスクは経営環境の変化と関係しており、個人情報保護対応を有効にするにはリスク分析を含め、常に見直し作業が不可欠です。そのためにフィードバックループ構成をとっているかを確認します。)		●	●	4.2(d) 4.6
	行動指針	1- 1- 1- 7	Q 個人情報保護に関して、組織としてなすべき行動指針が明確ですか？ (個人情報の保護は組織の目的・目標達成・社会的責任等に関係しますが、果たすべき個人情報保護対応の行動指針が明確かを確認します。)	●	●	●	4.2 4.3.3
4．個人情報保護の監査	監査	1- 1- 1- 8	Q 個人情報保護方針では、個人情報保護に関する監査の実施が明確に定められていますか？ (個人情報保護の監査に関しては、JIPDECの「プライバシーマーク監査ガイドライン」を参考にするとよいでしょう。)	●	●	●	4.5 4.3.3(e)
	内部監査	1- 1- 1- 8- 1	Q 個人情報保護方針では、個人情報保護に関する内部監査の実施を明記していますか？ (監査について内部的にも重視し、個人情報保護方針に明記していることが求められます。)		●	●	(4.5)
	外部監査	1- 1- 1- 8- 2	Q 個人情報保護方針では、個人情報保護に関する外部監査の実施を明記していますか？ (監査においては客観性(第三者の目)が不可欠です。そこで、外部機関による監査の実施が定められているかが問われます。)		●	●	(4.5)
5．個人情報保護方針の周知	周知	1- 1- 1- 9	Q 個人情報保護方針を関係者に周知し、一般に公表していますか？ (個人情報保護方針は特定の部署の者だけ知っていればよいものではありません。そこで、広く関係者に周知しているかが問われます。)	●	●	●	4.2 4.4.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
個人情報保護計画	個人情報保護計画	Ⅱ－1．個人情報保護に関するリスクマネジメント計画					
1．経営理念と個人情報保護計画	経営理念	2- 1- 1- 1	Q 経営理念に基づいた個人情報保護のための計画を明確にしていますか？ (経営理念の実現を阻害する要因が個人情報保護に係わるリスクであることがわかりやすく記載されている必要があります。個人情報保護計画に経営理念との関連が明記されているかを確認します。)	●	●		4.3.1
	保護対象	2- 1- 1- 2	Q 個人情報保護計画では、守るべき対象として個人情報が明確になっていますか？ (作成されている個人情報保護計画に守るべき対象を明確にしているかを確認します。)	●	●	●	4.3.1
2．個人情報保護のリスク管理体制の組織化	管理体制	2- 1- 1- 3	Q 個人情報保護計画では、個人情報のリスク管理体制が定義されていますか？ (個人情報保護に係わるリスクを日常的に予防、対処するための総合的な責任部門、および特定のリスクごとの責任部門が定められている必要があります。)	●	●	●	4.3.3
	リスク分析責任者	2- 1- 1- 3- 1	Q 個人情報保護に関するリスク分析の責任者が定められていますか？ (各リスクごとにリスク分析を行う責任者・部署が定められている必要があります。) (用語解説「リスク分析」:リスクごとに発生頻度と発生した場合の損失(経営への影響なども含む)について、定性的、定量的に程度を把握することをいいます。)		●	●	(4.3.3(a))
	リスク対策責任者	2- 1- 1- 3- 2	Q 個人情報保護に関するリスク対策の責任者が定められていますか？ (各リスクごとにリスク対策を実施する責任者が定められているか、および部、支社ごとに責任者が定められている必要があります。)		●	●	(4.3.3(a))
	リスクファイナンス責任者	2- 1- 1- 3- 3	Q 個人情報保護に関するリスクファイナンスに関する責任者が定められていますか？ (保険、為替管理、積立金などについて、計画、実施に関する責任者が定められている必要があります。)		●	●	(4.3.3(a))
	基本目的	2- 1- 1- 4	Q 個人情報保護計画では、個人情報保護のための基本的な目的がわかりやすく示されていますか？ (個人情報保護計画には、個人情報の保護を行うための基本的な目的をわかりやすく明示している必要があります。)	●	●	●	4.3.4
	対策実施の責任権限	2- 1- 1- 5	Q 個人情報保護計画では、リスク対策の実施にあたって責任権限が明確ですか？ (リスク対策を実施する場合に役員の権限、部長の権限、支社長の権限、緊急時の権限などが明確に定められている必要があります。)		●	●	4.3.3(a)
	意思決定プロセス	2- 1- 1- 6	Q 個人情報保護計画では、意思決定プロセスが明確ですか？ (リスク方針、リスクの分析、分析結果の評価、リスク対策の立案、予算化、経営資源の投入、評価などのそれぞれにおいて、取締役会、個人情報保護委員会、常務会、部長、課長稟議など、時期と決定手続が明確になっている必要があります。)		●	●	4.4.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
個人情報保護計画	個人情報保護計画	Ⅱ－1. 個人情報保護に関するリスクマネジメント計画					
3. 個人情報保護の管理目標	管理目標	2- 1- 1- 7	Q 個人情報保護計画では、個人情報保護に係るリスクの管理目標を具体的に明示していますか？ (企業全体の損失の下限、リスクごとの事故件数、損害の許容範囲など、全員が理解して取り組むべき目標がわかりやすく明示している必要があります。)	●	●	●	4.3.1
	物理的資産	2- 1- 1- 7- 1	Q 個人情報の観点から物理的資産の管理目標を具体的に明示していますか？ (用語解説「物理的資産の管理目標」: 入退館(室)管理の実施、盗難等に対する対策、機器・装置等の物理的保護をいいます。)		●	●	4.3.1
	情報資産	2- 1- 1- 7- 2	Q 個人情報を管理目標の対象として具体的に明示していますか？ (情報システム上のデータ、コンテンツ、および特許などの無形資産について、喪失、盗難の許容範囲などを具体的に明示している必要があります。)		●	●	4.3.1
	経済的損失	2- 1- 1- 7- 3	Q 個人情報の漏えい、滅失又はき損に伴う経済的損失の管理目標を具体的に明示していますか？ (企業の財務諸表において、単年度あるいは数年の期間で許容できる損失の金額を管理目標として明示している必要があります。)		●	●	4.3.1
	機会損失	2- 1- 1- 7- 4	Q 個人情報の漏えい、滅失又はき損に伴う機会損失の管理目標を具体的に明示していますか？ (対応によっては発生する機会損失について、その財務諸表上の許容できる損失の金額について目標を明示している必要があります。)		●	●	4.3.1
	実施基準	2- 1- 1- 7- 5	Q 個人情報保護方針では、個人情報保護に関する実施基準を明確にしていますか？ (実施基準が明確でなければ、個人情報の取扱いにバラツキが生じ、正確性を欠き、その結果、ステークホルダからの信頼を失うことになります。さらにリスク対策が具体性を欠くことになりかねません。したがって、実施基準を組織として明確にすることが必要です。)		●	●	4.3.3
	雇用管理情報	2- 1- 1- 7- 6	Q 個人情報保護の視点から、雇用管理情報を管理目標として明確にしていますか？		●	●	4.3.1
	コンプライアンス	2- 1- 1- 7- 7	Q 個人情報保護のためのコンプライアンスの管理目標を具体的に明示していますか？ (コンプライアンスや企業倫理に関する事件や事故に関する損失の許容範囲や削減目標などについて、明確に定めている必要があります。)	●	●	●	4.3.3

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
個人情報保護計画	個人情報保護計画	Ⅱ－1．個人情報保護に関するリスクマネジメント計画					
4．個人情報保護の目標脅威	目標脅威	2- 1- 1- 8	Q 個人情報の保護を脅かすリスクやハザードについて、個人情報保護の観点から分析を行っていますか？ (企業全体の個人情報保護対策において、具体的な企業目標の達成を脅かすリスクやハザードについて、情報というキーワード、たとえば情報システムの停止、情報漏えいなどからリスクを洗い出し、リスク分析を実施する必要があります。)	●	●	●	4.3.1
	物理的資産	2- 1- 1- 8- 1	Q 個人情報に関する物理的資産を脅かすリスクやハザードについて、情報の視点から分析を行っていますか？ (ここでいう物理的資産とは、記録媒体、入っている箱、空調等を指します。)		●	●	4.3.1
	情報資産	2- 1- 1- 8- 2	Q 個人情報に関する無形の資産を脅かすリスクやハザードについて、情報の視点から分析を行っていますか？ (コンテンツ、プログラム、データベースなどの情報資産を脅かすリスクやハザードについて、情報のキーワード、たとえば不法コピーなどからリスクを洗い出し、リスク分析を実施する必要があります。)		●	●	4.3.1
	経済的損失	2- 1- 1- 8- 3	Q 個人情報保護に関して発生する、済的損失をもたらすリスクやハザードについて、情報の視点から分析を行っていますか？ (ここでいう経済的損失とは、個人情報の漏えい、滅失又はき損に伴う損失を指します。)		●	●	4.3.1
	機会損失	2- 1- 1- 8- 4	Q 個人情報保護に関して発生する機会損失をもたらすリスクやハザードについて、情報の視点から分析を行っていますか？ (ある対応を実施した時、あるいは実施しなかった時にその結果として発生する機会損失について、個人情報の漏えい、滅失又はき損に伴うものとして把握します。)		●	●	4.3.1
	企業信用、ブランド価値	2- 1- 1- 8- 5	Q 企業の信用やブランド価値を脅かすリスクやハザードについて、個人情報保護の視点から分析を行っていますか？ (企業の信用やブランド価値を脅かすリスクやハザードについて、情報のキーワード、たとえば情報漏えい、情報システムの不正操作などのリスクを洗い出し、リスク分析を実施する必要があります。)		●	●	4.3.2
	雇用管理情報	2- 1- 1- 8- 6	Q 雇用管理情報について、リスクの視点から分析を行っていますか？ (たとえば、組織にとり重要な人的資産(人財)の情報が流出すると、ヘッドハンティングされるリスクがあります。この点についてリスクの視点から分析する必要があります。)		●	●	4.3.3
	コンプライアンス違反	2- 1- 1- 8- 7	Q 個人情報保護法、ガイドラインへのコンプライアンス違反によるリスクについて、個人情報の損失又は漏えいに係わるリスク分析を行っていますか？ (コンプライアンス違反によるリスクについて、情報のキーワード、たとえば不正ソフトのコピーなどのリスクを洗い出し、リスク分析を実施する必要があります。)	●	●	●	4.3.2
	サイバーテロ	2- 1- 1- 8- 8	Q サイバーテロ(踏み台攻撃を含む)による個人情報の漏えいのリスクやハザードについて分析を行っていますか？ (地域社会の安全保障を損なうリスクやハザードが自社の中に存在するか否かについて、情報のキーワード、たとえば、コンピュータウイルスやハッキング、Dos攻撃などのリスクを洗い出し、リスク分析を実施する必要があります。)		●	●	4.3.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
個人情報保護計画	個人情報保護計画	Ⅱ－1．個人情報保護に関するリスクマネジメント計画					
5．個人情報保護の分析	分析方法	2- 1- 1- 9	Q 個人情報保護に係るリスク分析の方法は明確ですか？ (リスクを分析する方法について、アンケートやイベントツリー、モンテカルロシミュレーションなど、どの方法を用いるかについて、またどの組織で、誰が、いつ行うかなどを明確にしている必要があります。) (用語解説「リスク分析」:リスクごとに発生頻度と発生した場合の損失(経営への影響なども含む)について、定性的、定量的に程度を把握することをいいます。)		●	●	4.3.1
	費用対効果分析	2- 1- 1- 9- 1	Q 個人情報保護に係る費用対効果分析の方法は明確ですか？ (対策をとった場合の費用対効果分析を行うにあたって、費用、被害程度、損害額の算出方法や、どの組織で、いつ行うかなどを明確にしている必要があります。)		●		4.3.1
	ハザード分析	2- 1- 1- 9- 2	Q 個人情報保護に係るハザード分析の方法は明確ですか？ (リスクの発生源となるさまざまな状況や脅威、事業を取り巻く外部状況などを分析する方法について、ブレーンストーミング、過去の事故事例の分析などの手法や、どの組織で、いつ行うか、などを明確にしている必要があります。) (用語解説「ハザード分析」:リスク(組織にとっての損失)が発生する可能性のある状況をいいます。情報セキュリティの分野では外来のものを脅威、組織に内在する弱点を脆弱性という場合がありますが、双方を含みます。)		●		4.3.1
	ギャップ分析	2- 1- 1- 9- 3	Q 個人情報保護に係るギャップ分析の方法は明確ですか？ (ギャップ分析(あるべき姿と現状との差、部門別、階層別の対応状況の差を把握する方法)について、手法の選択のほか、どの組織で、いつ行うかなどを明確にしている必要があります。)		●		4.3.1
6．対策	リスク対策への反映	2- 1- 1- 10	Q 個人情報保護に係るリスク分析の結果をリスク対策に反映させていますか？ (リスク分析を行った結果、発生頻度や損害の程度が把握されますが、その大きさと低減する目標に向けたリスク対策をとるように見直しが行われている必要があります。)		●	●	4.3.4
	対策策定方法	2- 1- 1- 11	Q 個人情報保護に係るリスク対策の策定方法は明確ですか？ (リスク対策の策定にあたっては、どの組織で、誰が、いつ行うかについて明確になっている必要があります。)		●	●	4.3.4
	対策実施基準	2- 1- 1- 12	Q 個人情報保護に係るリスク対策の内部規程を有していますか？ (リスク対策を実施するか否かを判断するための合理的な安全対策を実施する内部規程を指します。)		●	●	4.3.4
	経営者の承認	2- 1- 1- 13	Q 個人情報保護のためのリスク対策の採用について、経営者が最終承認していますか？ (リスク対策の採用については、要員、予算、時間などといった経営資源が必要になります。そのため、リスク対策の採用にあたっては、権限委譲の範囲の決定なども含めて経営者が承認することが必要です。)	●	●	●	4.3.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
個人情報保護計画	個人情報保護計画	Ⅱ－1．個人情報保護に関するリスクマネジメント計画					
7．緊急時対応	緊急時対応	2- 1- 1- 14	Q 個人情報保護に係るリスクマネジメント計画では、緊急時対応について明記していますか？ (個人情報保護計画の中で、万一のリスクが発生した場合の報告先、本部長の指名、対応策のレベルなどについて定めている必要があります。)	●	●	●	(4.3.1)
	事故	2- 1- 1- 14- 1	Q 個人情報保護に係る事故の発生時における緊急時対応を明記していますか？ (ここでいう事故とは、個人情報の漏えい、滅失、き損、盗難、紛失、不正利用などが発生した場合を指します。)		●	●	(4.3.1)
	災害	2- 1- 1- 14- 2	Q 災害時における個人情報保護に係る緊急時対応を明記していますか？ (自然災害(地震、洪水、台風、火災等)が発生した場合の個人情報の滅失、き損、紛失に対する対応を意味します。)		●	●	(4.3.1)
	サービス欠陥	2- 1- 1- 14- 3	Q サービスの欠陥により個人情報が漏えいするような場合の緊急時対応を明記していますか？ (この場合のサービスの欠陥とは、Webアプリケーションの脆弱性や欠陥による漏えい等を指します。)		●	●	(4.3.1)
	サービス供給停止	2- 1- 1- 14- 4	Q サービスが供給停止した場合の緊急時対応を明記していますか？ (この場合のサービスの供給停止とは、サーバ等の停止を指します。)		●	●	(4.3.1)
	企業信用、ブランド価値	2- 1- 1- 14- 5	Q 個人情報保護に係る事故等により、企業の信用やブランド価値が損なわれた場合の緊急時対応を明記していますか？ (企業信用やブランド価値の損失により、急速な顧客離れを想定しています。)		●	●	(4.3.1)
	雇用管理情報の喪失	2- 1- 1- 14- 6	Q 雇用管理情報が損なわれた場合の緊急時対応を明記していますか？ (災害、事故などによって雇用管理情報が失われる場合があります。その場合の対応策を明記している必要があります。)		●	●	(4.3.1)
	コンプライアンス違反	2- 1- 1- 14- 7	Q 個人情報に係るコンプライアンス違反を犯した場合の緊急時対応を明記していますか？ (法令違反および社内規範、企業倫理に違反する行為が発生した場合の対応策について明記している必要があります。)	●	●	●	4.3.3
	サイバーテロ	2- 1- 1- 14- 8	Q サイバーテロ(踏み台攻撃を含む)によって個人情報漏えいが起きた場合の緊急時対応を明記していますか？ (自社への攻撃のほか、社会の安全を損なうサイバーテロの中継地に自社のサーバなどが使用された場合の対応策について明記している必要があります。)		●	●	(4.3.1)
8．個人情報保護計画の周知	周知	2- 1- 1- 15	Q 個人情報保護計画を関係者に周知させていますか？ (個人情報保護計画は規範やマニュアルを作成するだけではなく、役員・従業員に周知徹底され、実際に実行される必要があります。)	●	●	●	4.3.4

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
実行組織	実行組織	Ⅱ－2．個人情報保護の実行組織					
1．個人情報保護に係るリスクマネジメント組織	リスクマネジメント担当役員の任命	2－ 2－ 1－ 1	**Q 個人情報に係るリスクマネジメントのための担当役員は最高経営者によって任命されていますか？** （全社的に個人情報に係わるリスクマネジメントを実施するためには、その担当役員が明確に定められている必要があります。中小企業では社長が兼務しても構いません。）	●	●	[redacted]	4.4.1
	リスクマネジメント推進体制	2－ 2－ 1－ 2	**Q 個人情報に係るリスクマネジメントシステム推進のための体制がありますか？** （個人情報に係わるリスクマネジメントの事務局を担う組織を定めます。メンバーは各部門から参加することでも構いませんが、責任体制は明確にする必要があります。）	●	●	●	4.4.1
	リスクマネジメント担当者の役割権限	2－ 2－ 1－ 3	**Q 個人情報に係るリスクマネジメント担当者の役割権限が明確ですか？** （個人情報に係わるリスクマネジメントの計画策定や、さまざまな具体策を実施するそれぞれの役割や権限を明確に定める必要があります。部門や職制に応じて職務権限を定めることも考えられます。）	●	●	●	4.4.1
	情報システムリスクマネジメント担当者の役割権限	2－ 2－ 1－ 4	**Q 個人情報を扱う情報システムのリスクマネジメント担当者が任命されていますか？** （個人情報を扱う情報システムリスクの掌握や対応体制の構築のために情報システムリスクマネジメントの担当者を任命することが必要です。場合によって全社的なリスクマネジメント担当者が兼務しても構いません。）	●	●	●	4.4.1
2．情報システムの個人情報取扱い組織	情報システムリスク管理体制	2－ 2－ 1－ 5	**Q 個人情報を扱う情報システムのリスク管理体制がありますか？** （個人情報を扱う情報システムに係わるリスクを一元的に把握し、対応策を策定する体制を定めます。） （用語解説「リスク管理体制」：組織と責任体制、担当者の役割、予算や計画の策定・執行を行うことを含めて体制といいます。）	●	●	●	4.4.1
	情報システムリスク管理者	2－ 2－ 1－ 5－ 1	**Q 個人情報を扱う情報システムのリスク管理者がいますか？** （個人情報を扱う情報システムリスク管理体制の中に、管理責任者を定める必要があります。細分化して決めても構いません。）	[redacted]	●	[redacted]	4.4.1
	情報システム運用管理責任者	2－ 2－ 1－ 5－ 2	**Q 個人情報を扱う情報システムの運用管理責任者がいますか？** （個人情報を扱う情報システムリスクのうち、システムやネットワークの運用に係わる管理者を定めます。）	[redacted]	●	[redacted]	4.4.1
	情報セキュリティ対策推進組織	2－ 2－ 1－ 6	**Q 個人情報を扱う情報システムの情報セキュリティ対策推進組織がありますか？** （実際の運用において発生する個人情報に係わる事故や事件およびそれを起こさないようにする管理者とは別に、セキュリティを推進するための組織を定めます。メンバーは兼務者であっても構いません。）	[redacted]	●	●	4.4.1
	情報システム情報セキュリティ管理者	2－ 2－ 1－ 6－ 1	**Q 個人情報を扱う情報システムの情報セキュリティの管理者がいますか？** （個人情報に係わる情報セキュリティの推進のための責任者を定めます。）	[redacted]	●	[redacted]	4.4.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
実行組織	実行組織	Ⅱ－2．個人情報保護の実行組織					
3．個人情報を扱うユーザの組織	適用業務別オーナー	2－ 2－ 1－ 7	**Q 個人情報を扱う情報システムの適用業務に関する利用者側のオーナーは明確ですか？** (個人情報を扱う情報システムは一般には情報システム部門だけのものと思われがちですが、情報漏えいや情報システムの使用上のミスなど、ユーザ側のリスクも大きいことを十分に認識する必要があります。そのため、アプリケーションシステムごとに個別に責任の所在を明確にする必要があります。)		●	●	4.4.1
	ユーザ部門リスク担当責任者	2－ 2－ 1－ 8	**Q 個人情報を扱うユーザ部門の適用業務における個人情報に関するリスク担当責任者がいますか？** (全社的な個人情報保護対策を実施していく場合には、各部門に個人情報保護責任者や担当者が置かれることになります。一方、個人情報を扱う情報リスクでは主に情報システム部門がその推進や管理体制を担いますが、ユーザのリスクも大きいため、各部門のリスク管理体制の中で、個人情報に係わる情報リスク担当責任者を明確にしておく必要があります。兼務であっても構いません。)		●	●	4.4.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
維持	維持	Ⅱ-3．個人情報保護に関するマネジメントシステムの維持					
1．評価	パフォーマンス評価	2- 3- 1- 1	Q 個人情報保護に係るパフォーマンス評価を実施していますか？ (用語解説「パフォーマンス評価」：個人情報保護の基本目的や目標達成のために組織が行う行動結果(成果)を指します。)	●	●		4.6
	パフォーマンス評価基準	2- 3- 1- 1- 1	Q 個人情報保護に係るパフォーマンス評価基準がありますか？ (個人情報保護についての行動結果を評価する、客観的で検証可能な基準があるかを確認します。)		●		4.3.3
	パフォーマンス監視	2- 3- 1- 1- 2	Q 個人情報保護の実施に係るパフォーマンス監視を行っていますか？ (個人情報保護の実施において重要な監視を継続的に行っているかを確認します。)		●		4.6
	有効性評価	2- 3- 1- 2	Q 個人情報保護に係る有効性評価を行っていますか？ (有効性は、個人情報保護の基本目的や目標の達成度を個人情報保護計画・個人情報に係わるリスク対策の実施・是正改善・体制の見直しなどから判断されますが、有効性の評価を行っているかを確認します。)		●	●	4.6
2．是正改善	是正改善	2- 3- 1- 3	Q 個人情報保護に係るマネジメントシステムに対し、是正・改善を実施していますか？ (個人情報保護に係わるマネジメントの実施・監視、パフォーマンスの評価、有効性の評価等に基づき、是正・改善を行っているかを確認します。)	●	●	●	4.6
	是正改善行動採択基準	2- 3- 1- 3- 1	Q 個人情報保護に係るリスク対応のため、是正改善行動を採択する基準がありますか？ (是正・改善にあたり、関係部署の責任者が検討を行うことになりますが、その際、採択のための基準があるかを確認します。)		●	●	4.6
	フィードバックループ機能	2- 3- 1- 3- 2	Q 個人情報保護に係る是正改善を繰り返し反映させる機能はありますか？ (是正・改善は継続的に行うことが望ましいですが、そのためのフィードバックループがあるかを確認します。)		●	●	4.6
	是正改善状況の点検	2- 3- 1- 3- 3	Q 個人情報保護に係る是正改善の状況を点検していますか？ (是正・改善を行った後で点検を行うことが必要です。)		●		4.6
	是正改善の有効性評価	2- 3- 1- 3- 4	Q 個人情報保護に係る是正改善の実施後に有効性評価を行っていますか？ (是正・改善を行った後で、その有効性を評価しているかを確認します。)		●	●	4.6
	ボトルネックの排除	2- 3- 1- 4	Q 個人情報保護に係るマネジメントシステムの実施にあたって、ボトルネックの排除を行っていますか？ (個人情報保護に係わるマネジメントシステムの実施にあたって障害となるボトルネックの存在は問題ですが、その排除を行っているかを確認します。)		●	●	4.6

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
維持	維持	Ⅱ-3．個人情報保護に関するマネジメントシステムの維持					
3．監査	個人情報保護監査	2- 3- 1- 5	Q 個人情報保護の監査を実施していますか？ （個人情報保護に係わるマネジメントシステムにおいて客観的（第三者的）な視点から監査を行っているかを確認します。）	●	●	●	4.5
	内部監査	2- 3- 1- 5- 1	Q 内部監査による個人情報保護の監査を実施していますか？		●	●	(4.5)
	外部監査	2- 3- 1- 5- 2	Q 外部監査による個人情報保護の監査を実施していますか？		●	●	(4.5)
4．監視	監視手段	2- 3- 1- 6	Q 個人情報に係るリスクの変化を監視する手段を持っていますか？ （個人情報保護に係わるリスクの変化を監視する手段を機能させているかを確認します。） （用語解説「監視する手段」：たとえば、専門委員会による情報交換等をいいます。）		●	●	(4.4.1)
	変化の監視	2- 3- 1- 7	Q 個人情報保護方針では、個人情報保護に関する実施基準を明確にしていますか？ （実施基準が明確でなければ、個人情報保護対策は具体性を欠くことになります。この点が組織として明確になっているかを確認します。）		●	●	(4.4.1)
5．文書化	基準の文書化	2- 3- 1- 8	Q 個人情報保護に係る実施基準は文書化されていますか？ （実施基準を組織内で機能させるには、口頭だけでは不十分なため、文書化が求められることになります。）		●	●	4.4.9
	リスクマネジメント文書管理	2- 3- 1- 9	Q 個人情報保護の実施に係る文書管理を行っていますか？ （個人情報保護に係わるマネジメントシステムの実施に関する文書の作成・改訂、管理手段等を含めて、文書管理を行っているかを確認します。）		●	●	4.4.9
	リスク変化の記録	2- 3- 1- 10	Q 個人情報に係るリスクの変化について記録を取っていますか？ （個人情報保護に係わるリスクの変化の内容を組織における共有財産とするため、記録を取っていることが重要です。）		●	●	4.4.9
	実績記録	2- 3- 1- 11	Q 個人情報保護に係る記録を取っていますか？ （個人情報保護に係わる実施記録は担当者が代わっても活用できる、組織にとって重要な情報財産です。そのための記録を取っているかを確認します。）		●	●	4.4.9
6．リスクコミュニケーション	リスクコミュニケーションの実施	2- 3- 1- 12	Q 個人情報保護に係るリスクコミュニケーションを実施していますか？ （用語解説「リスクコミュニケーション」：組織内における個人情報保護に係わるリスク情報の収集、リスク対策の徹底、リスク対応の広報活動に至るまで広く関係し、関係者の間での認識の共有にとって重要となるのがリスクコミュニケーションです。）	●	●	●	(4.4.6) (4.6)
	リスクコミュニケーション手段	2- 3- 1- 12- 1	Q 個人情報保護に係るリスクコミュニケーション手段（電子メール、説明会等）を明確にしていますか？		●	●	(4.4.6) (4.6)
	リスク情報開示	2- 3- 1- 13	Q 個人情報保護に係るリスク情報の開示に関する実施基準を策定していますか？ （個人情報保護に係わるリスク情報の開示について組織として基準が必要です。そこで、実施基準があるかが問われることになります。）		●	●	(4.2) (4.4.8)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
維持	維持	Ⅱ-3．個人情報保護に関するマネジメントシステムの維持					
7．教育の承認	経営者の教育承認	2- 3- 1- 14	Q 経営者は個人情報保護に係る教育訓練計画を承認していますか？ (個人情報保護に係わる教育訓練は利益に直結するわけではないため、時としてカットの対象とされやすいですが、計画については経営者の承認が不可欠です。)	●	●	●	4.4.6
	個人情報取扱責任者・担当者の教育訓練計画	2- 3- 1- 14- 1	Q 個人情報取扱責任者・担当者に対する個人情報保護に係る教育訓練計画を承認していますか？		●	●	4.4.6
	情報システム部門の教育訓練計画	2- 3- 1- 14- 2	Q 情報システム部門に対する個人情報保護に係る教育訓練計画を承認していますか？		●		4.4.6
	従業者の教育訓練計画	2- 3- 1- 14- 3	Q 個人情報取扱責任者・担当者、情報システム部門を除く従業者全員(ユーザ部門を含む)に対する個人情報保護に係る教育訓練計画を承認していますか？ (用語解説「従業者」:正社員、契約社員、嘱託社員、パートタイマ、アルバイト、派遣社員等)および役員(取締役、執行役、監査役、理事、監事等)を指します。)		●	●	4.4.6 4.3.3(d)
	教育の位置づけ	2- 3- 1- 15	Q 個人情報保護に係るマネジメントシステム維持のための教育の位置づけは明確ですか？ (個人情報保護に係わるリスクへの対応を誤れば、組織の維持は不可能となります。そのため、組織において個人情報保護に係わるマネジメントシステムについての教育の位置づけは重要です。)		●	●	4.4.6 4.3.3(d)
8．教育の実施	個人情報取扱責任者・担当者の教育	2- 3- 1- 16	Q 個人情報取扱責任者・担当者に対する個人情報保護に係る教育訓練を行っていますか？		●	●	4.4.6
	情報システム部門の教育	2- 3- 1- 17	Q 情報システム部門に対する個人情報保護に係る教育訓練を行っていますか？		●		4.4.6
	従業者の教育	2- 3- 1- 18	Q 個人情報取扱責任者・担当者および情報システム部門を除く従業者に対する個人情報保護に係る教育訓練を行っていますか？ (組織にとって経営者層の各人が個人情報に係わるリスクセンス(リスクマインド)を有していることが不可欠です。特にさまざまなリスクが組織を取り巻いており、個人情報保護に係わる教育は経営の根幹に係わるので、経営者層にとっても教育訓練は必要です。)	●	●	●	4.4.6
9．経営者のレビュー	リスクマネジメントシステムレビュー	2- 3- 1- 19	Q 最高経営者による個人情報保護マネジメントシステムのレビューを行っていますか？ (個人情報保護に係わるマネジメントシステムのレビューに最高経営者が関与することがきわめて重要です。この点、組織として明確に捉えているかが問われます。)	●	●	●	4.6

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4. 個人情報保護に関わるリスク分析					
1．リスク分析の仕組み	リスク分析の実施	2- 4- 1- 1	Q 個人情報保護に係るリスク分析(発見・算定・評価)の実施について、リスクマネジメント計画上明確にしていますか？ (個人情報保護に係わるマネジメントシステムのレビューに最高経営者が関与することがきわめて重要です。この点、組織として明確に捉えているかが問われます。)	●	●	●	4.3.1 4.4.4.2
	未実施の場合の問題の認識	2- 4- 1- 2	Q 個人情報保護に係るリスク分析を実施していない場合の問題を認識していますか？ (個人情報保護に係わるリスクの分析を行っていない場合、問題が発生したら事後的に対応しなければなりません。その場合の損失の広がりは内容により異なりますが、時として組織の存続を揺るがすことにもなりかねません。したがって、そうした場合の問題認識が問われます。)	●	●	●	(4.3.1) (4.4.4.2)
	関連情報提供システム	2- 4- 1- 3	Q 個人情報の保護に関するリスク関連情報を個人情報保護管理者もしくはリスク分析担当者に提供する仕組みが構築されていますか？ (個人情報保護に係わるリスク分析担当者がリスク関連情報をすべて熟知しているわけではありません。そこで、担当者にそうした関連情報を提供する仕組みが個人情報保護に係わるリスク分析の巧拙・適否に関係するので、仕組みの構築が問われるのです。) (用語解説「リスク関連情報」：守るべき対象、リスク分析の手法ならびにリスクデータ等、組織内・外部に種々の情報源があります。)	●	●	●	-
	保護対象リスク分析	2- 4- 1- 4	Q 明確にされた守るべき個人情報についてリスクを分析していますか？ (ここでいう個人情報には保有する個人情報を含みます。)		●	●	4.3.1 4.4.4.2
2．リスク分析の体制	変化を含めた社内体制	2- 4- 1- 5	Q 内外の個人情報保護に係る環境の変化を含めたリスク環境の動きを捉える体制を有していますか？ (経営環境の変化はリスク発生に関係します。個人情報保護に係わるリスクをもたらす環境として、その動きを捉えるための体制が社内において不可欠です。)	●	●	●	4.3.1 4.4.4.2
	対応優先順位	2- 4- 1- 6	Q 個人情報の取扱いに係るリスクの評価を行い、リスク対応の優先順位を確定していますか？ (個人情報の取扱いに係わるリスクの評価を行うのは、組織として何からとりかかるべきか、優先順位の確定が重要となるので、この点が問われます。)		●	●	(4.3.1) (4.4.4.2)
	フィードバック	2- 4- 1- 7	Q 個人情報の取扱いに係るリスク発見・評価の見直しを繰り返し反映する機能をもっていますか？ (個人情報の取扱いに係わるリスクは一旦分析されればそれですむ、という性質のものではありません。経営環境の変化によって絶えず増減するため、絶えずリスクを発見・評価することが求められます。したがって、リスクの分析にもPDCA(Plan-Do-Check-Act)の視点が不可欠です。そこで組織としてリスク分析を繰り返し行うことを認知された機能があるかが重要となります。)		●	●	4.3.1 4.6
	分析の予算・スタッフ	2- 4- 1- 8	Q 個人情報保護に係るリスク分析のため予算・スタッフを適切に導入していますか？ (個人情報保護に係わるリスクの分析にはそれなりの予算・スタッフの投入が必要です。投入に関する基準として確定したものはありませんが、重要なのは組織として導入の仕方が適切かどうかになります。)	●	●	●	-

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4．個人情報保護に関わるリスク分析					
3．リスク分析の実施	リスク洗出し	2- 4- 1- 9	Q 個人情報に関して、定期的にリスクを洗い出していますか？ （個人情報保護に係わるリスクの洗出しは1回行えばそれで終わりといったものではありません。実施基準を持ち、定期的に行うというパターンが重要です。）		●	●	4.4.4.2
	洗出し実施基準	2- 4- 1- 9- 1	Q 個人情報の取扱いに係るリスクをもれなく洗い出す内部規程を有していますか？		●	●	
	日常的な洗出し	2- 4- 1- 9- 2	Q 個人情報に関して、経営環境の変化から生じるリスクを日常的に洗い出していますか？		●	●	
	特定部門からの要請による洗出し	2- 4- 1- 9- 3	Q 個人情報の取扱いに関して、特定機能部門からの要請によってリスクを洗い出していますか？		●	●	
	頻度算定	2- 4- 1- 10	Q 個人情報の取扱いに関してリスク頻度を算定していますか？ （どの程度の割合でこれまで損失が発生してきたのか、今後、発生すると思われるのか、データに基づきリスクの発生頻度を把握することはリスク対応のため重要です。）		●	●	4.4.4.2
	頻度算定実施基準	2- 4- 1- 10- 1	Q 個人情報の取扱いに関してリスク頻度を算定する内部規程を有していますか？		●	●	
	影響度算定	2- 4- 1- 11	Q 個人情報の取扱いに関して経営に与えるリスクの影響度を算定していますか？		●	●	－
	影響度算定実施基準	2- 4- 1- 11- 1	Q 個人情報の取扱いに関して経営に与えるリスクの影響度を算定する内部規程を有していますか？		●	●	
	リスク評価	2- 4- 1- 12	Q 個人情報の取扱いに関して経営に与えるリスク評価を実施していますか？ （どの位の規模の損失が発生したのか、今後、発生すると思われるのか、データを基にリスクの大きさ（強度）を把握することはリスク対応のために重要です。）	●	●	●	－
	リスク評価基準	2- 4- 1- 12- 1	Q 個人情報の取扱いに関して経営に与えるリスクの評価基準を有していますか？ （個人情報の取扱いに関して経営に与えるリスクの評価について、評価基準（金額値なのか、（○○百万～○○○百万までといった）損失の規模区間で捉えるのか、さらに規模を大・中・小といったカテゴリで分けるのか等）を組織として業務部門別・地区別等、必要に応じて明確にしておくことが重要です。）		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4. 個人情報保護に関わるリスク分析					
4. 利用目的	利用目的の特定の手続	2- 4- 1- 13	Q利用目的を特定するための手続を定めない場合のリスクを分析していますか？	●	●	●	4.4.2.1
	直接取得時の利用目的明示	2- 4- 1- 13- 1	Q 個人情報を本人から直接取得するにあたり、利用目的を明示しない場合のリスクを分析していますか？		●	●	4.4.2.4
	間接取得後の利用目的明示	2- 4- 1- 13- 2	Q 個人情報を間接的に取得するにあたり、本人に通知又は公表しない場合のリスクを分析していますか？		●	●	4.4.2.5
	利用目的の特定	2- 4- 1- 13- 3	Q 個人情報の取扱いにあたり、利用目的を特定しない場合のリスクを分析していますか？		●	●	4.4.3.1
	利用目的の特定手順の承認方法	2- 4- 1- 13- 4	Q 個人情報の利用目的の特定手順の承認方法を定めていない場合のリスクを分析していますか。 (利用目的を限定する手順について、社内で承認を得ることが必要です。)		●	●	4.4.3.1
	利用目的の変更	2- 4- 1- 13- 5	Q 利用目的を変更する場合に、速やかに、その利用目的を本人に通知又は公表しない場合のリスクを分析していますか？		●	●	4.4.3.2
	目的外利用の同意	2- 4- 1- 13- 6	Q 個人情報の目的外利用に際して、あらかじめ本人の同意を得ていない場合のリスクを分析していますか？		●	●	4.4.3.2
5. 取得	不正取得	2- 4- 1- 14	Q 個人情報を不正に取得した場合のリスクを分析していますか？	●	●	●	4.4.2.2
	機微情報の取得	2- 4- 1- 14- 1	Q 機微情報を取得した場合のリスクを分析していますか？		●	●	4.4.2.3
	保存期間	2- 4- 1- 14- 2	Q 個人情報の保存期間を設定していない場合のリスクを分析していますか？		●	●	－
6. 第三者提供	第三者提供	2- 4- 1- 15	Q 個人情報を第三者に提供する場合のリスクを分析していますか？	●	●	●	4.4.5.2
	第三者提供の禁止	2- 4- 1- 15- 1	Q 本人の同意を得ていない個人情報を第三者に提供する場合のリスクを分析していますか？		●	●	4.4.5.2
	第三者提供停止(オプトアウト)	2- 4- 1- 15- 2	Q オプトアウトの措置を講じない場合のリスクを分析していますか？ (用語解説「オプトアウト」:本人の求めに応じて第三者への提供を禁止することです。)		●	●	4.4.5.2
	外部委託先への提供	2- 4- 1- 15- 3	Q 個人情報の取扱いの一部又は全部を外部に委託する場合、委託のための手続を定めていない場合のリスクを分析していますか？		●	●	4.4.4.3
	共同利用	2- 4- 1- 15- 4	Q 共同利用を行う場合のリスクを分析していますか？ (共同利用を行う場合は、共同で利用される個人情報の項目、共同利用者の範囲、共同で利用する者の利用目的、および共同で利用する者のうち個人情報の管理について責任を有する者の氏名又は名称を本人に通知又は公表する必要があります。)		●	●	－

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4. 個人情報保護に関わるリスク分析					
7. 安全管理	正確性の確保	2- 4- 1- 16	Q 個人情報の正確性を確保できない場合のリスクを分析していますか？ (正確かつ最新の内容に保つとは、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、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人情報を正確かつ最新の内容に保つよう努めることをいいます。)		●	●	4.4.4.1
	個人情報保護組織・体制の整備	2- 4- 1- 17	Q 個人情報保護のための組織・体制を整備していない場合のリスクを分析していますか？	●	●	●	4.4.1
	安全管理措置	2- 4- 1- 17- 1	Q 個人情報の漏えい、滅失又はき損を防止するための安全管理措置を行わない場合のリスクを分析していますか？		●	●	4.4.4.2
	安全管理措置の組織・体制の整備	2- 4- 1- 18	Q 個人情報の安全管理措置を講じるための組織・体制の整備を行っていない場合のリスクを分析していますか？	●	●	●	4.4.4
	個人情報保護規程の整備	2- 4- 1- 18- 1	Q 個人情報保護のための内部規程を整備していない場合のリスクを分析していますか？		●	●	4.3.3
	マニュアル	2- 4- 1- 18- 2	Q 個人情報保護のためのマニュアルを整備していない場合のリスクを分析していますか？ (用語解説「マニュアル」:内部規程に基づいて個人情報の取扱手続の明確化と手続に従った実施を確保するための手順書等をいいます。)		●	●	-
	個人情報取扱台帳	2- 4- 1- 18- 3	Q 個人情報の取扱い状況を一覧できる手段を整備していない場合のリスクを分析していますか？ (用語解説「個人情報の取扱い状況を一覧できる手段」:個人情報を取り扱うにあたって、取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人情報の適正な取扱いに必要な情報を記した台帳等を整備することをいいます。)		●	●	-
	個人情報の消去・廃棄	2- 4- 1- 18- 4	Q 個人情報を消去又は廃棄する場合の手順を定めていない場合のリスクを分析していますか？ (不要となった個人情報を廃棄する場合は、焼却や溶解など復元不可能な形にして廃棄すべきです。)		●	●	4.4.5.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4. 個人情報保護に関わるリスク分析					
7. 安全管理	事故・違反への対応	2- 4- 1- 19	Q 漏えい等の事故又は取扱規程に違反する場合のリスクを分析していますか？	●	●	●	4.4.6
	社内不正	2- 4- 1- 19- 1	Q 社内不正による個人情報の漏えい等のリスクを分析していますか？ (個人情報の漏えいの多くは社内不正によるものです。)		●	●	4.4.4.2
	漏えいの影響	2- 4- 1- 19- 2	Q 個人情報の漏えいによる影響を分析していますか？		●	●	4.4.4.2
	滅失又はき損の影響	2- 4- 1- 19- 3	Q 個人情報の滅失又はき損による影響を分析していますか？		●	●	4.4.4.2
	二次被害	2- 4- 1- 19- 4	Q 漏えい、滅失又はき損等の事故による二次被害の影響を分析していますか？		●	●	–
	事故の公表	2- 4- 1- 19- 5	Q 個人情報の漏えい等の事故が発生したことを公表しない場合のリスクを分析していますか？		●	●	–
	人的安全管理措置	2- 4- 1- 20	Q 個人情報保護のための人的安全管理措置を定めていない場合のリスクを分析していますか？ (雇用契約時、委託契約時に非開示契約を締結し、従業者に対する教育・訓練を実施していることが必要です。)		●	●	4.4.6
	非開示契約	2- 4- 1- 20- 1	Q 非開示契約を締結していない場合のリスクを分析していますか？ (従業者の役割・責任を定めた職務分掌規程、職務権限規程、就業期間中はもとより、離職後も含めた守秘義務等の内部規程を定めておくことが不可欠です。)		●	●	–
	物理的安全管理措置	2- 4- 1- 21	Q 個人情報保護のための物理的安全管理措置を定めていない場合のリスクを分析していますか？ (用語解説「物理的安全管理措置」:入退館(室)の管理、個人情報の盗難の防止等の措置をいいます。)		●	●	4.4.4.2
	入退室(館)管理	2- 4- 1- 21- 1	Q 入退室管理を行っていない場合のリスクを分析していますか？ (関係者以外の者が個人情報を取り扱えないようにすることが重要です。)		●	●	–
	盗難防止対策	2- 4- 1- 21- 2	Q 盗難防止措置を行っていない場合のリスクを分析していますか？ (関係者以外の者が個人情報を取り扱えないようにするために、室内への記録媒体の持込み禁止策、個人情報を記録したノートパソコンの持出し禁止などの措置が必要です。)		●	●	4.4.4.2
	機器・装置の物理的保護	2- 4- 1- 21- 3	Q 機器・装置を物理的に保護していない場合のリスクを分析していますか？ (機器・装置の物理的保護とは、個人情報を取り扱う機器・装置等の安全管理上の脅威(例:盗難、破壊、破損)や環境上の脅威(例:漏水、火災、停電)からの物理的な保護を行っていることをいいます。)		●	●	–

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4. 個人情報保護に関わるリスク分析					
7. 安全管理	技術的安全管理	2- 4- 1- 22	Q 個人情報保護のための技術的安全管理措置を定めていない場合のリスクを分析していますか？ (技術的安全管理措置とは、個人情報およびそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人情報に対する技術的な安全管理措置をいいます。)		●	●	(4.4.4.2)
	アクセス制御	2- 4- 1- 22- 1	Q アクセス制御を行っていない場合のリスクを分析していますか？		●	●	(4.4.4.2)
	不正ソフトウェア対策	2- 4- 1- 22- 2	Q 不正ソフトウェア対策を実施しないリスクを分析していますか？ (不正ソフトウェアとはウイルス、スパイウェア、ワームなどを指します。)		●	●	-
	情報システムの監視	2- 4- 1- 22- 3	Q 情報システムを監視しないことによるリスクを分析していますか？ (情報システムの利用状況の監視とは、個人情報を取り扱う情報システムの使用状況の定期的な監視や操作内容も含むアクセス状況を監視することをいいます。)		●	●	-
	従業者の監督	2- 4- 1- 23	Q 従業者を監督しない場合のリスクを分析していますか？ (従業者とは、正社員、契約社員、嘱託社員、パートタイマ、アルバイト、派遣社員等)および役員(取締役、執行役、監査役、理事、監事等)を指します。) (従業者の監督とは、個人情報の安全管理措置を定める規程等に従って従業者が業務を行っていることを監督することをいいます。必要かつ適切な監督を行う対象は、正社員、契約社員、嘱託社員、パートタイマ、アルバイト、派遣社員等)および役員(取締役、執行役、監査役、理事、監事等)が含まれます。)	●	●	●	(4.4.1)
	教育・研修	2- 4- 1- 23- 1	Q 従業者に対し教育・研修を行わないことにより発生するリスクを分析していますか？		●	●	4.4.6
	外部委託	2- 4- 1- 24	Q 個人情報の取扱いを委託する場合のリスクを分析していますか？	●	●	●	4.4.4.3
	委託先選定	2- 4- 1- 24- 1	Q 個人情報の取扱いを委託する場合の委託先の選定基準を定めなかった場合のリスクを分析していますか？		●	●	4.4.4.3
	委託契約	2- 4- 1- 24- 2	Q 委託先との契約内容について、責任分担、非開示契約等を締結しない場合のリスクを分析していますか？		●	●	4.4.4.3
	委託先の監督	2- 4- 1- 24- 3	Q 委託先に対して必要かつ適切な監督を行わない場合のリスクを分析していますか？		●	●	4.4.4.3
	委託先(安全)管理	2- 4- 1- 24- 4	Q 委託先の安全管理を確認しないことのリスクを分析していますか？		●	●	4.4.4.3
	委託先の定期確認	2- 4- 1- 24- 5	Q 委託先における個人情報の取扱い状況を定期的に分析していますか？		●	●	(4.4.4.3)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク分析	リスク分析	Ⅱ-4. 個人情報保護に関わるリスク分析					
8. 本人関与・苦情処理	周知	2- 4- 1- 25	Q 本人に対し、個人情報を保有していることを周知していないことのリスクを分析していますか？	●	●	●	4.4.3.1
	保有する個人情報の把握	2- 4- 1- 25- 1	Q 保有している個人情報を把握していない場合のリスクを分析していますか？ (「保有個人情報」という用語は行政機関等個人情報保護法の定義で用いられている用語のため、ここでは「保有する個人情報」とします。)		●	●	4.4.4.1
	保有する個人情報の公表	2- 4- 1- 25- 2	Q 保有している個人情報について、本人の同意なしに公表する場合のリスクを分析していますか？		●	●	-
	開示	2- 4- 1- 26	Q 本人からの開示の求めに応じない場合のリスクを分析していますか？	●	●	●	4.4.5.2
	利用目的非通知時の取扱い	2- 4- 1- 26- 1	Q 本人の生命、身体、財産等の権利利益を害する恐れがある場合、利用目的を通知又は公表することのリスクを分析していますか？		●	●	4.4.3.1
	利用停止等の手続	2- 4- 1- 26- 2	Q 個人情報の利用の停止又は第三者への提供の停止を求められたときに、手続を行わなかった場合のリスクを分析していますか？ (利用の停止・第三者提供の停止に応ずる義務が生じるのは、本人からの求めに理由がある場合であって、個人情報の取扱いが、目的外利用、不正取得、第三者への無断提供に該当する場合のみをいいます。)		●	●	4.4.5.2
	本人対応(理由)手続	2- 4- 1- 26- 3	Q 本人からの利用目的の通知・開示・訂正・利用停止等に応じない場合のリスクを分析していますか？		●	●	4.4.5.2
	開示手続	2- 4- 1- 26- 4	Q 開示手続が定められていない場合のリスクを分析していますか？		●	●	4.4.5.1
	開示手数料	2- 4- 1- 26- 5	Q 実費を勘案して合理的であると認められる範囲内において、開示等の求めに応ずる際の手数料の額を定めていない場合のリスクを分析していますか？		●	●	4.4.5.1
	利用目的の通知の求めに応じないリスク	2- 4- 1- 26- 6	Q 本人からの利用目的の通知の求めに対し、利用目的を通知しない場合のリスクを分析していますか？		●	●	4.4.5.1
	非開示情報の取扱いの通知	2- 4- 1- 26- 7	Q 本人からの開示の求めに対し、保有する個人情報の全部又は一部を開示しないことを通知しない場合のリスクを分析していますか？		●	●	4.4.5.1
	訂正・削除等	2- 4- 1- 26- 8	Q 個人情報の訂正等(訂正、追加又は削除)の求めに応じない場合のリスクを分析していますか？		●	●	4.4.5.2
	苦情処理体制の整備	2- 4- 1- 27	Q 個人情報の取扱いについて、苦情処理体制が整備されていない場合のリスクを分析していますか？	●	●	●	4.4.7
	苦情対応手順	2- 4- 1- 27- 1	Q 個人情報の取扱いへの苦情について、適切かつ迅速な処理を行わない場合のリスクを分析していますか？		●	●	4.4.7

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ．個人情報保護に関するリスクマネジメント計画					
リスク対策	リスク対策	Ⅱ-5. 個人情報保護に関わるリスク対策					
1．安全管理対策	正確性の確保	2- 5- 1- 1	Q 個人情報保護の正確性を確保するための対策を実施していますか？ (正確性を確保するための対策とは、入力ミス、修正ミス等がないように整合性をチェックする対策をいいます。)	●	●	●	4.4.4.1
	安全管理対策の実施	2- 5- 1- 2	Q 安全管理対策を実施していますか？ (あたり前のことのようですが、リスクマネジメントの対策を実施することを明確にします。)	●	●	●	4.4.4.2
	組織的安全管理措置の実施	2- 5- 1- 2- 1	Q 個人情報保護のための体制の下で安全管理措置を実施していますか？ (従業者の責任体制の明確化を図り、具体的な取組みを進めるため、個人情報保護に関する十分な知識を有する管理者を定めたり、個人情報保護の推進を図るための組織を設置することが重要です。)		●	●	(4.4.4.2)
	人的安全管理措置の実施	2- 5- 1- 2- 2	Q 個人情報保護のための人的安全管理措置を実施していますか？ (雇用契約時、委託契約時に非開示契約を締結し、従業者に対する教育・訓練を実施していることが必要です。)		●	●	(4.4.4.2)
	物理的安全管理措置の実施	2- 5- 1- 2- 3	Q 個人情報保護のための物理的安全管理措置を実施していますか？ (物理的安全管理措置とは、入退館(室)の管理、個人情報の盗難の防止等の措置をいいます。)		●	●	(4.4.4.2)
	技術的安全管理措置の実施	2- 5- 1- 2- 4	Q 個人情報保護のための技術的安全管理措置を実施していますか？ (技術的安全管理措置とは、個人情報およびそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人情報に対する技術的な安全管理措置をいいます。)		●	●	(4.4.4.2)
	監督の実施	2- 5- 1- 3	Q 職務権限に応じた監督責任を果たしていますか？	●	●	●	(4.4.4.1)
	従業者の監督の実施	2- 5- 1- 3- 1	Q 従業者の監督を実施していますか？ (従業者とは、正社員、契約社員、嘱託社員、パートタイマ、アルバイト、派遣社員等)および役員(取締役、執行役、監査役、理事、監事等)を指します。)		●	●	(4.4.4.1)
	委託先の監督の実施	2- 5- 1- 3- 2	Q 委託先企業の個人情報保護体制の監督を実施していますか？		●	●	(4.4.4.3)
	事故・違反への対策	2- 5- 1- 4	Q 漏えい等の事故又は取扱規程に違反した場合の対策を実施していますか？	●	●	●	4.4.4.2

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	RM	ユーザ	
個人情報保護計画	個人情報保護計画	Ⅱ. 個人情報保護に関するリスクマネジメント計画					
リスク対策	リスク対策	Ⅱ-5. 個人情報保護に関わるリスク対策					
2. 適切な取扱い	利用目的の特定の手続の実施	2- 5- 1- 5	Q 利用目的を特定するための手続を定めていますか？		●	●	4.4.2.1
	直接取得時の利用目的明示	2- 5- 1- 5- 1	Q 個人情報を本人から直接取得するにあたり、利用目的を明示していますか？		●	●	4.4.2.4
	間接取得後の利用目的明示	2- 5- 1- 5- 2	Q 個人情報を間接的に取得するにあたり、本人に通知又は公表していますか？		●	●	4.4.2.5
	利用目的の特定	2- 5- 1- 5- 3	Q 個人情報の取扱いにあたり、利用目的を特定していますか？		●	●	4.4.2.1
	利用目的特定手順の承認	2- 5- 1- 5- 4	Q 個人情報の利用目的の特定手順の承認方法を定めていますか？		●	●	(4.4.2.1)
	利用目的の変更	2- 5- 1- 5- 5	Q 利用目的の変更を本人に通知又は公表していますか？		●	●	4.4.3.2
	目的外利用	2- 5- 1- 5- 6	Q 目的外利用をする場合の本人への通知手順を定めていますか？		●	●	4.4.3.2
	適正な取得	2- 5- 1- 6	Q 個人情報は、適正な手段により取得していますか。 (適正ではない個人情報の取得の例としては、不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、詐欺等により取得したり、使用・開示することがあげられます。)		●	●	4.4.2.2
	取得の制限	2- 5- 1- 7	Q 機微情報の取得を原則禁止していますか？		●	●	4.4.2.3
3. リスクファイナンス	リスクファイナンス	2- 5- 1- 8	Q 個人情報の漏えい等に伴い発生する損害へのリスクファイナンスを実施していますか？ (リスクが発生した場合に備えて、保険、為替先物予約、デリバティブ、インパクトローン、各種準備金など、さまざまなリスクファイナンス(財務的な対応)が必要です。最近の考え方では資本金が財務における最終的なリスクヘッジと考えられています。)	●	●		－
4. 第三者提供対策	本人の同意	2- 5- 1- 9	Q 個人情報を第三者に提供する場合は、あらかじめ本人の同意を得ていますか？		●	●	4.4.3.1
	第三者提供停止(オプトアウト)	2- 5- 1- 9- 1	Q 個人情報を第三者に提供するにあたり、本人の同意を得られない場合、オプトアウトの措置を講じていますか？ (用語解説「オプトアウト」:本人の求めに応じて第三者への提供を禁止することをいいます。)		●	●	4.4.3.2
	共同利用	2- 5- 1- 9- 2	Q 共同利用を行う場合は、法定事項を本人に通知する手続を定めていますか？ (通知事項は、共同で利用される個人情報の項目、共同利用者の範囲、共同で利用する者の利用目的、および共同で利用する者のうち、個人情報の管理について責任を有する者の氏名又は名称となっています。)		●	●	－
5. 本人関与対策	周知	2- 5- 1- 10	Q 本人に対し、個人情報を保有していることを周知していますか？		●	●	4.4.5.1
	開示	2- 5- 1- 10- 1	Q 本人からの開示請求に応じる対応体制を構築していますか？		●	●	4.4.5.1
	苦情処理体制の構築	2- 5- 1- 10- 2	Q 個人情報の取扱いについて苦情処理体制を構築していますか？		●	●	4.4.7

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報セキュリティポリシー	情報セキュリティポリシー	Ⅲ-1. 情報セキュリティポリシーのリスク分析					
1. 情報セキュリティの経営からの視点	経営の視点からの分析	3- 1- 1- 1	Q 情報セキュリティポリシーを経営の視点から分析の対象としていますか？ (作成されている情報セキュリティポリシーを企業経営の視点から定期的に見直し、経営理念との齟齬の有無、ビジネス環境や商品群などの変化への対応ができているかなどの分析を行い、必要に応じて修正することが必要です。セキュリティについても経営戦略との観点で分析する必要があります。)		●		
2. 情報セキュリティポリシーの対象	リスク分析の対象	3- 1- 1- 2	Q 情報セキュリティポリシーでリスク分析の対象を定めていますか？ (情報セキュリティポリシーの中でリスク分析を行うことが定められていなければなりませんが、あわせて分析を行う対象についても明記する必要があります。)		●	●	(4.3.1)
	災害	3- 1- 1- 2- 1	Q 災害が情報セキュリティポリシーのリスク分析の対象となっていますか？ (地震、台風、火災などの災害が発生した場合の企業への影響について、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。)		●		
	障害	3- 1- 1- 2- 2	Q 障害が情報セキュリティポリシーのリスク分析の対象となっていますか？ (メインフレーム、サーバ、空調機の故障、プログラムバグ、ネットワーク切断などの障害が発生した場合の企業への影響について、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。)		●		
	不正アクセス	3- 1- 1- 2- 3	Q 不正アクセスが情報セキュリティポリシーのリスク分析の対象となっていますか？ (ハッキングや許可のない人が重要データを持ち出すなど、不正アクセスが発生した場合の企業への影響について、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。)		●		(4.3.1) (4.4.4.2)
	偽造・不正使用リスク	3- 1- 1- 2- 4	Q 情報システムを利用した偽造・不正使用がセキュリティポリシーのリスク分析の対象となっていますか？ (情報システムのアプリケーションやサービスを不正に利用した偽造、詐欺などが発生した場合の企業への影響について、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。)		●		
	コンピュータウイルス	3- 1- 1- 2- 5	Q コンピュータウイルスが情報セキュリティポリシーのリスク分析の対象となっていますか？ (コンピュータウイルスが侵入した場合や顧客にウイルスを送ってしまった場合などの企業への影響について、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。)		●		
	アウトソーシングのリスク	3- 1- 1- 2- 6	Q アウトソーシングに係わるリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ (情報システムの企画・開発・運用・保守の各局面においてアウトソーシングを行うことが一般的になりつつあります。アウトソーシングを行うことによってリスクが増減することについて、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。)		●		(4.4.4.3)
	SLA	3- 1- 1- 2- 7	Q SLAの内容がリスク分析の対象となっていますか？ (SLAの内容を守ることができなかった場合、顧客に影響を与えることになります。そのような状況が発生した場合の企業への影響について、分析の対象とすることを情報セキュリティポリシーに明記する必要があります。) (用語解説「SLA」:サービスレベルアグリーメントのことで、顧客に対して情報システムを利用したサービスの内容を約束したものです。この中には障害などが発生した場合の対応や障害などによって利用ができない時間の発生割合などについて定めることが一般的です。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報セキュリティポリシー	情報セキュリティポリシー	Ⅲ-1. 情報セキュリティポリシーのリスク分析					
2. 情報セキュリティポリシーの対象	緊急時対応	3- 1- 1- 3	Q 緊急時対応の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？ (障害や災害、コンピュータウイルスや誤作動など、さまざまな事件・事故が発生した場合の緊急時対応について、現状で問題がないかを常に分析する必要があります。)		●	●	(4.3.1)
	機密漏えい	3- 1- 1- 3- 1	Q 機密漏えい(個人情報)に対する緊急時対応は事前に備えられていますか？ (機密情報が漏えいした場合の緊急時対応が事前に検討され、実践できることが必要です。)		●	●	(4.4.4.2)
	不正アクセス	3- 1- 1- 3- 2	Q 不正アクセスに対する緊急時対応は事前に備えられていますか？ (不正アクセスが発生した場合、あるいは不正アクセスされようとした状況を把握した場合の緊急時対応が事前に検討され、実践できることが必要です。)		●	●	(4.4.4.2)
	コンピュータウイルス	3- 1- 1- 3- 3	Q コンピュータウイルスに対する緊急時対応は事前に備えられていますか？ (コンピュータウイスルが侵入した場合や企業内に蔓延した場合、あるいは顧客にウイルスを送ってしまった場合などの緊急時対応が事前に検討され、実践できることが必要です。)		●	●	
	ネットワーク障害	3- 1- 1- 3- 4	Q コンピュータウイルスや不正アクセスの結果としてネットワーク(インターネット)が障害になった場合の緊急時対応は事前に備えられていますか？ (特にネットワークが使用不能になった場合、顧客への連絡や遠隔地にある社内の利用者にどのように連絡を取り、対処してもらうかなどの緊急時対策の検討が必要です。)		●	●	
	災害	3- 1- 1- 3- 5	Q 災害(テロを含む)に対する緊急時対応は事前に備えられていますか？ (地震、洪水、テロなど重要な施設の被災や役員、従業員の被災が発生した場合などの緊急時対応が事前に検討され、実践できることが必要です。)		●	●	
	障害	3- 1- 1- 3- 6	Q 障害に対する緊急時対応は事前に備えられていますか？ (メインフレーム、サーバ、プログラムバグなどの障害によって情報システムが使用できない場合などの緊急時対応が事前に検討され、実践できることが必要です。)		●	●	
	緊急時対応	3- 1- 1- 3- 7	Q バックアップに対する緊急時対応は事前に備えられていますか？ (通常、情報システムは障害などに備えてデータやプログラムのバックアップを取得しますが、そのバックアップをいざ使用しなければならない場合などの緊急時対応が事前に検討され、実践できることが必要です。)		●	●	
	ファシリティ移動	3- 1- 1- 3- 8	Q その他ファシリティの移動が必要な事態に対する緊急時対応は事前に備えられていますか？ (主要な社屋・工場あるいは情報システムセンタなどが被災した場合など、オフィスを移転して対応しなければならない場合があります。これらのファシリティの移動が必要な場合などの緊急時対応が事前に検討され、実践できることが必要です。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報セキュリティポリシー	情報セキュリティポリシー	Ⅲ-1. 情報セキュリティポリシーのリスク分析					
2. 情報セキュリティポリシーの対象	情報セキュリティ推進組織内容	3- 1- 1- 4	Q 情報セキュリティ推進組織の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？ (情報セキュリティを推進するためには強力な推進組織が必要です。その組織の構成(参加する組織や役職員、要員など)について問題がないか常に分析・検討することが必要です。)		●		(4.3.1)
	監査内容	3- 1- 1- 4- 1	Q 監査内容が情報セキュリティポリシーのリスク分析の対象となっていますか？ (リスクマネジメントや情報セキュリティを推進するためには対策がおざなりにならないために第三者の監査が不可欠です。この監査内容について、その要員、時期、対象などが適切かを分析する必要があります。)		●		(4.5)
3. 特筆する情報リスク	基幹システム情報漏えい(情報)	3- 1- 1- 5	Q 基幹システムから機密情報が窃取されるリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ (企業の事業遂行に不可欠な重要なデータ(たとえば顧客の個人情報、特許情報、売上原価、計算ロジックなど)が搾取された場合の企業に与える影響を分析の対象とすることが必要です。)		●	●	(4.3.1)
	複次的なリスク	3- 1- 1- 6	Q 個人情報漏えいの複次的なリスクが発生する可能性が分析の対象となっていますか？ (漏えいした個人情報を利用した犯罪行為が波及していく可能性があります。)		●		
	ホームページ	3- 1- 1- 7	Q ホームページに係わる誹謗中傷リスク(被害リスク)が情報セキュリティポリシーのリスク分析の対象となっていますか？ (ホームページに誹謗中傷が掲載された場合の自社の被害程度について、分析の対象とすることが望まれます。)		●		[4.4.2.4]
	基幹システムダウン	3- 1- 1- 8	Q 基幹システムに関して不正手段による影響のリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ (さまざまなアプリケーションシステムを企業は保持していますが、少なくとも一番重要なシステムに着目してそのシステムに関して不正が行われ、架空計上、金品の搾取、いたずらによる情報改変などが発生した場合の影響度について、分析を行う必要があります。)		●		(4.3.1)
4. 時間分析	機能停止	3- 1- 1- 9	Q 機能部門別にシステムの機能停止が許される範囲を情報セキュリティポリシーにおいて設定していますか？ (情報システムが何らかの形で利用できない状況になった場合、どの程度の時間まで停止が許容されるのかについてあらかじめ分析し、許容時間を明確にすることが必要です。SLAがある場合にはそれらも考慮します。)		●		
5. 情報リスク洗出し実施基準	情報リスク洗出し実施基準	3- 1- 1- 10	Q 情報セキュリティポリシーにおいて、情報システムのリスクをもれなく洗い出す基準を定めることを明示していますか？ (リスクマネジメントの最初のステップはリスクの洗出しです。組織の現状で可能な最大限の方法でリスクを洗い出しますが、その方法と報告を記録する基準について明示することが必要です。)		●	●	(4.3.1)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	3－2－(1) 情報システムのリスク分析					
1．ＩＴ戦略のリスク分析	IT戦略のリスク分析	3－ 2－ 1－ 1	Q IT戦略(組織全体の情報システム化戦略)に係わるリスクを分析していますか？ (情報システムの活用は今後の企業の発展に欠かせません。いつ、どのような分野でIT投資を行うかについて、その成否も含めたリスクの分析を行う必要があります。)		●	●	
	情報システムの重要度測定	3－ 2－ 1－ 1－ 1	Q 情報システムの経営に関する重要度の測定を行っていますか？ (情報システムはいまや企業経営に不可欠です。情報システムが果たす経営に関する重要度、たとえば事務の効率化、開発の高速化など利益に貢献した度合いなどを測定することが望まれます。)		●		
	情報の重要度測定	3－ 2－ 1－ 1－ 2	Q 情報(コンテンツ、データ)の経営に関する重要度の測定を行っていますか？ (データやデータベースおよび各種コンテンツについて経営に関する重要度、たとえば事務の効率化、開発の高速化など、利益に貢献した度合いなどを測定することが望まれます。)		●		(4.3.1)
	業務への影響	3－ 2－ 1－ 1－ 3	Q 情報システムが業務に与える影響を分析していますか？ (情報システムが停止し利用できなかったり応答速度が遅くなったなど、業務にマイナスの影響を与えた場合、あるいは情報システムの新たなアプリケーション業務が開始されたことや応答速度や使い勝手がよくなることによって業務効率が改善される割合など、業務プラスの影響も含めて分析することが必要です。)		●	●	
	E-Commerce	3－ 2－ 1－ 1－ 4	Q E-Commerceサービスの提供やサービスの利用の両面からリスクを分析していますか？ (E-Commerceサービスについてそのサービスを提供している場合のリスク、あるいはそのサービスを利用している場合のリスクについて、誤作動、使用停止など、さまざまなリスクの分析を行う必要があります。)		●	●	
	情報リスクと経営存続	3－ 2－ 1－ 1－ 5	Q 情報システムに関し、経営の存続を左右すると考えられるリスクを明確に定義していますか？ (情報システムの停止、誤作動、使い勝手の極端な悪化などによって経営の存続が場合によっては困難なものがあれば、そのリスクを明確に認識する必要があります。情報システムの提供そのものが会社の商品である場合などが該当します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	3－2－(1) 情報システムのリスク分析					
2. 情報資産リスク	情報資産リスク	3- 2- 1- 2	Q 重要情報資産リスクを分析していますか？ (情報資産には大型コンピュータ、サーバなど有形資産のほか、顧客データベース、製法などトレードシークレットな情報などの無形資産などを含みます。これらの有形・無形資産のうち、個人情報や原価情報など重要な情報資産を選択し、それらが損なわれることによって生じるリスクを分析する必要があります。)		●	●	(4.3.1)
	重要性ランキング	3- 2- 1- 2- 1	Q 情報資産の重要性をランキングしていますか？ (有形・無形の情報資産について重要度を設定し、ランク分けを行う必要があります。)		●	●	(4.3.1)
	オーナーの明確化	3- 2- 1- 2- 2	Q 情報資産のオーナーが明確になっていますか？ (有形・無形の情報資産について、誰がその責任を持つか明確にする必要があります。特にデータベースなどの無形資産について、あるいはアプリケーションプログラムなどについてはユーザ部門が無責任になりがちなため、明確にオーナーを定めて責任体制を明確にします。)		●	●	(4.3.1)
	機密度ランク	3- 2- 1- 2- 3	Q 情報資産の機密度ランクを明確にしていますか？ (無形資産に対して情報の機密度、極秘、関係者外秘、社外秘、一般などのランクを定める必要があります。)		●	●	(4.3.1)
	可用性維持	3- 2- 1- 2- 4	Q 情報資産の可用性が維持されていますか？ (業務上必要なデータなどの情報に対し、アクセスを許可された人が必要な時間・場所においてその情報を入手できることがいつでも保障されていることが求められています。)		●	●	(4.3.1)
	複数人によるリスク分析	3- 2- 1- 2- 5	Q 情報資産への脅威(リスク)の分析は、関係する組織から視点の異なる複数人の参画を得てなされていますか？ (リスク分析は複数の立場の異なる人の視点によって行うことで、より客観的な評価ができることが期待されています。)		●	●	
	人的リスク	3- 2- 1- 3	Q 重要情報資産に係わる人的リスクを分析していますか？ (重要な情報資産が損なわれる可能性がありますが、人間が関与して損害が発生することが多いのが情報リスクの特徴です。)		●	●	(4.3.1)
	改ざんリスク	3- 2- 1- 3- 1	Q 情報資産の改ざんのリスクを分析していますか？ (情報資産、特に重要なデータベースやコンテンツなどは人為的に改ざんされることが予測されます。その発生頻度や損害の程度、発生するシナリオなどについて分析する必要があります。)		●	●	(4.3.1)
	破棄	3- 2- 1- 3- 2	Q 情報システム(ハード、ソフト、メディア)の破棄についてリスクを分析していますか？ (特にパソコンなどはそのまま破棄あるいは中古市場にリサイクルした場合、表面上データを消去しても物理的に情報が残っているため、知識がある人はその情報を復元できるので、場合によっては重要な情報が漏えいする可能性があります。また物理的な破棄の場合も、産業廃棄物処理が不適切に行われた場合、その責任を問われる場合があります。)		●		(4.3.1)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	3－2－(1) 情報システムのリスク分析					
2. 情報資産リスク	盗難	3- 2- 1- 3- 3	Q 盗難の情報システムに与える影響のリスクを分析していますか？ (職場内のパソコンやモバイル端末の盗難が増えています。盗難が発生した場合、業務を継続できなくなることに加え、その端末機に内蔵されていた情報が漏えいすることによる影響度の把握が必要です。分析にあたって、代替手段を確保している場合はその効果も考慮します。)		●		(4.3.1)
	物理的侵入	3- 2- 1- 3- 4	Q 物理的な侵入の情報システムに与える影響のリスクを分析していますか？ (盗難以外に物理的な侵入があった場合、情報をコピーして盗まれる情報漏えいのリスクや情報が改ざんされてしまうこと、あるいは機材を破壊されるなどのリスクが発生する可能性があります。)		●		(4.3.1)
	物理的攻撃	3- 2- 1- 3- 5	Q 物理的な攻撃(爆弾)の情報システムに与える影響のリスクを分析していますか？ (事務所の破壊などによる長時間の業務への影響のほか、郵便爆弾など事務所内で爆発することによるサーバ、端末機の破損などの影響などについてリスク分析を行う必要があります。)		●		(4.3.1)
	倒産	3- 2- 1- 3- 6	Q 情報システム関連のリスクが倒産に結びつくことについてリスクを分析していますか？ (情報システムサービスの提供が商品そのものの場合などが特に顕著ですが、情報システム関連のトラブルが発生した場合、最悪の場合、企業が倒産する可能性があるかについて、シナリオを作成したり分析を行う必要があります。)		●	●	
3. システム不全	機能不全	3- 2- 1- 4	Q 内的、外的理由による機能不全が情報システムに与える影響のリスクを分析していますか？ (オペレータのサポートが不十分であったり、機械の性能が著しく劣っていたりなどの内的理由、ネットワークの混雑などの外的理由など、さまざまな機能不全が発生した場合に、情報システムが被る被害について、その程度を分析する必要があります。)		●		
	ネットワーク	3- 2- 1- 4- 1	Q ネットワークの情報システムに与える影響のリスクを分析していますか？ (さまざまな一般回線、携帯回線、無線、構内LANなどネットワークの停止あるいは著しい効率の悪化などによって情報システムが被る影響について、分析する必要があります。)		●		
	誤作動	3- 2- 1- 4- 2	Q 誤作動が情報システムに与える影響のリスクを分析していますか？ (機械そのものの誤作動のほか、プログラムバグやオペレーションミスなども含め、何らかの理由で正しい動作を行わず、誤った結果が顧客に提供された場合のリスクを分析する必要があります。たとえば料金の誤請求や製品の誤発注など、さまざまなものがあります。)		●		
	犯罪	3- 2- 1- 4- 3	Q 犯罪が情報システムに与える影響のリスクを分析していますか？ (物理的な破壊、盗難のほか、プログラムの改ざん、ハッキング、架空発注など、さまざまな犯罪行為が発生するシナリオを作成し、分析する必要があります。犯罪は外部犯行と内部犯行があります。)		●		
	対応ミス	3- 2- 1- 4- 4	Q 対応ミスによるタイミングの遅れが情報システムに与える影響のリスクを分析していますか？ (オペレーションミスやプログラムミス、あるいはデータベースの不整合を発見した場合など、問題が発覚した時には一刻を争ってトラブルの拡大防止を行う必要があります。その対応が連絡遅れや手順が不適当であったために遅延した場合に発生する影響度を分析する必要があります。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	3－2－(1) 情報システムのリスク分析					
3．システム不全	質低下	3- 2- 1- 4- 5	Q システムの質の低下が情報システムに与える影響のリスクを分析していますか？ (機器の応答速度が遅く、古いプログラムを使用しつづけているためコードがあふれて特殊な計上をしなければならないなどが典型例ですが、システムの質が低下した場合に慢性的な影響が発生している度合いを分析する必要があります。)		●		
	安全性・機密保持の悪化	3- 2- 1- 4- 6	Q 安全性・機密保持の悪化が情報システムに与える影響のリスクを分析していますか？ (新たなネットワークに接続した場合、ユーザが拡大して今までの常識が通用しなくなった場合、機器の集約によって代替性や冗長性が損なわれた場合など、安全性・機密性が悪化することがあります。その場合、新たに増加したリスクの程度について分析する必要があります。)		●		(4.4.4.1)
	変化への対応性欠如	3- 2- 1- 4- 7	Q 変化(状況・環境・ニーズ・制度等)への対応性の欠如が情報システムに与える影響のリスクを分析していますか？ (ビジネス環境、端末の使用状況の変化、業務の拡大、新たな需要の発生など、常に情報システムへの要求水準や運用レベルが変化しています。これらの変化に追随できなくなった場合の影響度について分析する必要があります。)		●		
4．適用業務責任・権限	適用業務責任・権限	3- 2- 1- 5	Q システムの適用業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (システムの適用業務について、ユーザと情報システム部門、情報システム部門の中の各企画、運用などの部門(さらにその中が細分化されている場合もある)ごとの責任と権限を明確にする必要があります。)		●	●	(4.2)
	企画業務	3- 2- 1- 5- 1	Q 企画業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (システムの企画もユーザ部門と情報システム部門が協力して行いますが、それ以外にも人事部門や経理部門などが関与します。情報システム部門の中でも実際の開発担当、運用担当などが関与します。これらの協力関係を構築する一方、最終的な判断を行う責任と権限を明確にする必要があります。)		●	●	
	開発業務	3- 2- 1- 5- 2	Q 開発業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (開発について要件定義やテストへのユーザ部門の関与は不可欠です。また新たな業務のカットオーバーの判断は誰が責任を持って行うのかなど、責任と役割分担を明確にする必要があります。)		●	●	
	運用業務	3- 2- 1- 5- 3	Q 運用業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (安定しているプログラムの運用においても小規模な修正やトラブルの発生などがあります。システムのトラブル回避にはユーザの認識やユーザ部門内での教育なども不可欠です。これらの役割分担や権限などが明確になっている必要があります。また新たに開発されたプログラムを運用部門で引き継ぐ際には、十分な検証と説明を受ける義務があります。これら開発部門との責任分界点も明確にする必要があります。)		●	●	
	保守業務	3- 2- 1- 5- 4	Q 保守業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (機器の安定稼働のために企画、開発、運用部門などとの調整が必要になります。これら保守の実施については企画、開発、運用部門からの注文が多く、メンテナンスの時間の確保が困難になることも多くあります。これらの状況を踏まえて機器の稼働の最終決定権限が誰にあるのかなど、明確にする必要があります。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	3－2－(1) 情報システムのリスク分析					
4. 適用業務責任・権限	予算業務	3- 2- 1- 5- 5	Q 予算業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (情報システムの企画・開発・運用・保守にはそれぞれ人的要員に係わる人件費、機器の購入やアウトソーシングの依頼、あるいは適切なサービスの提供を受けるための費用などが発生します。費用は有限であるため、会社全体の費用負担能力との関係で調整されることは当然です。この場合どこに優先的に予算を割り当てるかによって、発生するリスクも連動します。それらを踏まえて誰が責任を持って予算の決定を行うかを明確にする必要があります。)		●	●	
	その他機能分野	3- 2- 1- 5- 6	Q その他の機能分野(　　)に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ (該当する機能分野を(　)内に記入して利用) (もしその他の機能分野がある場合は、このチェック項目にその分野を明記して判断します。)		●	●	
5. 適用業務とリスクマネジメント	情報システム適用業務	3- 2- 1- 6	Q 情報システム適用業務はリスクマネジメントを前提に構築されていますか？ (適用業務を開発する場合、その業務のプラス面のみを見て判断しがちですが、その業務の開発が遅れた場合、失敗した場合、予定された効果が現れなかった場合、その業務が事件・事故で損なわれた場合など、さまざまなリスクを判断して企画・開発される必要があります。)		●	●	(4.3.1)
	設計時の前提	3- 2- 1- 7	Q 適用業務の設計時、リスクマネジメントを前提の1つとしていますか？ (適用業務を設計する場合にはあらかじめ必要なリスクマネジメントの要件、たとえばアクセス管理を行うか否か、万一の事故発生時にバックアップシステムを持つか否かなど、さまざまな要求事項を明確にして設計する必要があります。一般に開発の最後になってセキュリティ要件が議論されることが多いのですが、それでは最悪の場合、希望するセキュリティが実現できないこともあります。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
システム開発	システム開発	3－2－(2)システム開発 (システム開発においてアウトソーシングを利用する場合は、「3-2-(4)アウトソーシング」を適用し、評価に用いること。ここでは、システム開発の各工程を対象にリスクを分析する。ただし、システム構成等の他の項目でカバーされているものを除く。)					
1．プロジェクトリスク	プロジェクトリスク	3- 2- 2- 1	Q システム開発の対象となる業務で個人情報に関するリスク分析に基づいて、セキュリティの要件が明確になっていますか？ (用語解説「セキュリティ要件」:稼働率や障害時の復旧時間目標、災害時の復旧時間と復旧時点の目標、セキュリティのレベルを指します。)		●	●	(4.4.4.2)
	企画段階	3- 2- 2- 2	Q システム開発に関して企画段階でプロジェクトリスクを分析していますか？ (企画開発段階で個人情報保護に関する要件の確認を怠った場合、後から要件の変更を余儀なくされると開発の遅延、コストの大幅な増加などのプロジェクトリスクの発生可能性が高くなるため、プロジェクトリスクを検討する際のチェックポイントに個人情報保護を加える必要があります。) (用語解説「プロジェクトリスク」:ビジネスリスク、テクノロジーリスク、組織的リスクが含まれます。)		●	●	(4.3.1)
	技術面	3- 2- 2- 2- 1	Q プロジェクト企画段階での技術面のリスクを分析していますか？ (用語解説「技術面のリスク」:企画段階で技術的に実現可能とされていたものが、実施段階で実現不可能になることをいいます。)		●	●	
	ビジネス面	3- 2- 2- 2- 2	Q プロジェクト企画段階でのビジネス面のリスクを分析していますか？ (用語解説「ビジネス面のリスク」:システム統合の前提となる企業合併が中止される等、システム化の前提条件が変化することをいいます。)		●	●	
	組織面	3- 2- 2- 2- 3	Q プロジェクト企画段階での組織面のリスクを分析していますか？ (用語解説「組織面のリスク」:完成されたシステムを組織内で予定されたユーザが使用しないことをいいます。)		●	●	
2．ライフサイクル	ライフサイクル	3- 2- 2- 3	Q 開発ライフサイクルの各工程で、開発のリスクを分析していますか？ (システム開発の各工程で、リスク分析を実施することが決められているかを確認します。) (用語解説「開発のリスク」:開発の遅れや予算超過によって生じるリスクをいいます。)		●	●	
3．開発管理	開発管理	3- 2- 2- 4	Q システム開発全般に係わるリスクを分析していますか？ (システム開発を成功させるためには、関係するリスクを包括的に見ているかを確認します。)		●	●	
	スタッフのスキルの妥当性	3- 2- 2- 4- 1	Q システム開発に関してスタッフのスキルの妥当性のリスクを分析していますか？ (スタッフに必要なスキルが定義され、満足されなかった場合のリスクを分析します。) (用語解説「妥当性のリスク」:開発の遅れや予算超過によって生じるリスクをいいます。)		●	●	
	コンプライアンス	3- 2- 2- 4- 2	Q システム開発に関してコンプライアンスの観点からリスクを分析していますか？ (法的な規制、ソフトウェアライセンスに準拠しなかった場合のリスクを分析します。)		●	●	
	開発環境	3- 2- 2- 4- 3	Q システム開発に関して開発環境のリスクを分析していますか？ (開発環境も不正アクセスリスク分析の対象とします。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
システム開発	システム開発	3－2－(2)システム開発 (システム開発においてアウトソーシングを利用する場合は、「3-2-(4)アウトソーシング」を適用し、評価に用いること。ここでは、システム開発の各工程を対象にリスクを分析する。ただし、システム構成等の他の項目でカバーされているものを除く。)					
3．開発管理	ソフトウェアのサポート切れ	3- 2- 2- 4- 4	Q システムソフトウェアのサポート切れのリスクを分析していますか？ (システムライフ期間中に、使用しているシステムソフトウェアのバージョンに対する保守が打ち切られた場合のリスクを分析します。)		●	●	
	ソフトウェアのバージョンアップ	3- 2- 2- 4- 5	Q 将来システムソフトウェアのバージョンアップが必要となるリスクを分析していますか？ (システムライフ期間中に、システムソフトウェアのバージョンアップを行う場合のテスト環境確保等のリスクを分析します。)		●	●	
4．運用テスト	運用テスト結果	3- 2- 2- 5	Q 運用テストの結果が、システム要件を満足している度合いについて、リスクを分析していますか？ (運用テスト結果が要件を満足しているかはYes/Noの判断となりますが、その満足度によって将来の環境変化に対するリスクを分析します。)		●	●	
	稼働開始による障害発生	3- 2- 2- 5- 1	Q システム稼働開始のリスクを分析していますか？ (運用テスト結果について、稼働開始後の障害発生のリスクを分析します。)		●		
	運用テスト結果	3- 2- 2- 5- 2	Q システム稼働後の処理／応答時間、処理能力のリスクを分析していますか？ (システムライフ期間中の必要能力の予測を行った上で、処理量の予期せぬ増加等によって、処理／応答時間、処理能力が不足した場合のリスクを分析します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
システム運用	システム運用	3－2－(3) システム運用 (システム運用においてアウトソーシングを利用する場合は、「3－2－(4)アウトソーシング」を適用し、評価に用いること。設備面やシステム構成面でのリスク分析は、他の項目で質問しているので、ここでは運用管理／ミスを対象にリスクを分析する。)					
1．システム運用	円滑運用	3- 2- 3- 1	Q 円滑なシステム運用を阻害する運用ミスのリスクを考慮した対応策を考えていますか？ (オペレータの過失による運用ミスによって発生する障害のリスクを分析します。)		●		
2．運用管理	ファイル管理	3- 2- 3- 2	Q 個人情報を含むファイル管理について、リスクを考慮した方針を設定していますか？ (ファイルの重要性のランクづけと対応した方針が設定されているかを確認します。)		●	●	
	ライブラリ管理	3- 2- 3- 2- 1	Q ライブラリ管理のリスクを考慮した方針を設定していますか？ (本番用のライブラリに不正なアクセスが行われたり、承認されていないバージョンアップが行われることがないような方針が設定されているかを確認します。)		●		
	バックアップ	3- 2- 3- 2- 2	Q ファイル、データの定期的なバックアップは想定されるリスク(個人情報漏えい等)を考慮して方針を設定していますか？		●		
	適用業務管理	3- 2- 3- 2- 3	Q 適用業務管理(例;入出力データの完全性)のリスクを考慮した方針を設定していますか？ (アプリケーションの障害等によってデータの完全性が壊れた時に、復旧するためのデータを保持することが方針に明記されているか、また、誤入力訂正時の手続について、正常入力時と同様の誤謬摘示手続が取られているかを確認します。)		●	●	(4.4.4.1)
3．キャパシティ管理	キャパシティ管理	3- 2- 3- 3	Q システム資源について不足するリスクの分析を実施していますか？ (個別システムではなく、サーバ等の共通インフラの資源が不足するリスクを分析します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－2. 情報システムのリスク分析					
アウトソーシング	アウトソーシング	3－2－(4)アウトソーシング					
1．アウトソーサの決定	アウトソーサの選定手続	3- 2- 4- 1	Q アウトソーサの選定手続においてリスクを分析していますか？ (アウトソーサの事業継続リスク、サービスレベル未達のリスクについて分析します。)		●		(4.4.4.3)
2．役割分担	契約内容	3- 2- 4- 2	Q アウトソーシングの契約内容についてリスクを分析していますか？ (アウトソーサが契約条件を達成できなかった場合、契約で担保するためにリスクを分析します。実損と賠償条項の関係をいいます。)		●	●	(4.4.4.3)
	責任分担	3- 2- 4- 2- 1	Q 委託者と受託者の責任分担のリスクを分析していますか？ (責任分担が不明確なリスクと、委託者の責任分担を実施できない場合のリスクを分析します。)		●	●	(4.4.4.3)
	作業内容	3- 2- 4- 2- 2	Q 受託者の作業(業務内容、範囲、スケジュール)内容のリスクを分析していますか？ (受託者の作業内容について、管理体制、要員数、要員のスキル等のリスクを分析します。)		●	●	
	変更管理	3- 2- 4- 2- 3	Q アウトソーシング契約での契約内容の変更(作業、契約、システム)のリスクを分析していますか？ (契約の条件の変更が委託者側の事情で発生するリスクを分析します。)		●	●	
3．守秘義務	守秘義務	3- 2- 4- 3	Q 受託者が守秘義務を守らなかった場合のリスクを分析していますか？ (受託者によって顧客リスト漏えい等の事故が発生した場合のリスクを分析します。)		●	●	(4.4.4.3)
	再委託時の守秘義務	3- 2- 4- 4	Q アウトソーシングの再委託が行われた場合の守秘義務のリスクを分析していますか？ (再委託が行われた場合についても、顧客リスト漏えい等の事故が発生した場合のリスクを分析します。)		●	●	(4.4.4.3)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	3－3－(1)不正アクセス・コンピュータウイルス関連					
1．コンピュータ犯罪のリスク	経営に与える影響	3- 3- 1- 1	Q コンピュータ犯罪が経営に与える影響(例:サービスの中断や重要な情報流出、企業の不名誉なうわさのひろがり等)のリスクを分析していますか？ (コンピュータ犯罪は経営に大きな影響を与えます。まず、金銭的なダメージ、これはコンピュータ犯罪が簡単にきわめて大きなダメージを与えることができるからです。さらに、企業にとってコンピュータ犯罪の事実は企業イメージを著しく傷つけます。これらの事実を情報システム部門もユーザもリスクとして認知しておくことが必要です。)		●	●	(4.3.1)
	内部犯罪による信頼への影響	3- 3- 1- 1- 1	Q 内部犯罪の場合、外部の関係者の信頼に与える影響のリスクを分析していますか？ (内部犯罪はコンピュータ犯罪よりも情報システム部門にとっては大きなリスクとなります。これによって企業の従業員のモラルを大きく傷つけることになります。さらに、犯罪は経営に大きな影響を与えることもあります。また、業界を通じて企業イメージが傷つき、その結果、企業自体の信頼度や信用度が低下することに繋がります。この事実を情報システム部門の管理職が認知することが必要です。)		●		(4.3.1)
	経営者・従業員の意識	3- 3- 1- 1- 2	Q 経営者や従業員がコンピュータ犯罪を軽視した場合のリスクを分析していますか？ (コンピュータ犯罪を軽視すると、より情報システム部門やユーザ部門の従業員のモラルが低下します。この事実は企業のつきあいの中で素早く広がり、業界での信用の低下を招きます。その結果、企業自体の信頼度や信用度が低下したり、優秀な従業員の離職にも繋がります。この事実を情報システム部門の管理職が認知することが必要です。)		●	●	(4.3.3)
	盗聴による影響	3- 3- 1- 1- 3	Q 盗聴が情報システムに与える影響のリスクを分析していますか？ (盗聴はきわめて重要な情報漏えいです。特に、盗聴によって企業の機密情報が漏れると企業の競争力や重大な経営判断が狂うことになります。さらに、盗聴は単に情報のみならず、たとえば、企業の吸収合併などが検討されているときに、その部門のトラフィックが増加したといった情報も情報漏えいとなります。これによって株価が大きく変わったりすることがあります。企業の情報漏えいに対する厳格な管理は、情報システム部門にとっては大きなリスクに繋がります。)		●		
	脅迫による影響	3- 3- 1- 1- 4	Q 脅迫が情報システムに与える影響のリスクを分析していますか？ (脅迫は企業の情報システム部門やユーザ部門など、さまざまな部門で起こりえます。特に、企業の情報システムには企業の機密情報が蓄積されているために、その情報の漏えい、情報の改ざんによって大きな利益を得る可能性があり、これらを得るために従業員を脅すことなどが起こりえます。これらのリスクについて、情報システム部門の管理職が認知することが必要です。)		●		
	改ざん	3- 3- 1- 1- 5	Q 情報システムの改ざんが経営に与える影響のリスクを分析していますか？ (改ざんは企業の情報システム部門やユーザ部門など、さまざまな部門で起こりえます。脅迫と同様に、情報の改ざんによって大きな利益を得る外部者が存在する限り、改ざんは起こりえます。これらのリスクについて、情報システム部門の管理職が認知することが必要です。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	3－3－(1)不正アクセス・コンピュータウイルス関連					
1．コンピュータ犯罪のリスク	破壊	3- 3- 1- 1- 6	Q 情報システムの破壊が情報システムに与える影響のリスクを分析していますか？ (情報システムの意図的な破壊は、情報システムに蓄積されている情報によって不利益を被る企業や個人にとって起こされる可能性が高くなります。また、テロや極端な政治的な活動に関連して情報システムの破壊が引き起こされる可能性があります。このリスクを情報システム部門は認知し、不用意に破壊されないような保護策を講じる必要があります。)		●		(4.4.4.2)
	情報漏えい	3- 3- 1- 1- 7	Q 情報漏えいが情報システムに与える影響のリスクを分析していますか？ (情報の漏えいによって企業の機密情報が漏れると企業の経営に大きな影響がでます。また、個人情報の漏えいは犯罪行為です。盗聴で述べたように、企業の情報漏えいに対する厳格な管理は、情報システム部門にとっては大きなリスクです。)		●		(4.4.4.2)
2．不正アクセスのリスク	モバイル機器盗難	3- 3- 1- 2	Q モバイル機器(パソコン、PDAなど企業外で使う情報機器)の置忘れ・盗難により重要情報が流出するリスクを分析していますか？ (パソコンには重要な企業の機密情報が蓄積されていたり、企業の情報システムにアクセスできる機能があります。PDAには、企業の機密情報や取引先を含めたアドレス、電話番号、電子メールアドレスなどの情報が蓄積されています。携帯電話も同様です。これらの機器は置き忘れると重大な企業情報の漏えいに繋がります。このリスクを考えて、企業の外部でIT機器を利用しないように情報システム部門は指導することが必要です。また、ユーザ部門ではこのリスクを考えて行動する必要があります。)		●	●	(4.4.4.2)
	インターネット経由内部犯罪	3- 3- 1- 3	Q 内部者が(社内から)インターネット経由で中継点を変え、再び社内にアクセスすることで情報窃取されるリスクを分析していますか？ (これは企業の機密漏えいの1つのパターンです。インターネットアクセスは自由度が高いため、このような不正の温床になるリスクがあります。このリスクを情報システム部門では認知して、アクセス経路にはいつも注意を払うことが要請されます。)		●		(4.4.4.2)
	ネッティングリスク	3- 3- 1- 4	Q ネッティングに関するリスクを分析していますか？ (ネッティングによって企業の重要な機密情報が外部に漏れる可能性があります。この情報漏れは避けられない場合があります。情報システム部門では、このようなリスクを考えてシステムを構築したり、運用する必要があります。)		●		
	妨害行為	3- 3- 1- 5	Q 悪意によるコンピュータなどへの妨害行為(不正アクセス、改ざん、メール爆弾、Dos攻撃など)によってサービスが中断するリスクを分析していますか？ (妨害行為は、意図された妨害と、意図されない不特定に対する妨害が存在します。特に後者については、インターネットではさまざまなものが起きると考えておく必要があります。これによって、ネットワークが利用できないことで企業の利益が減少したり、損失に繋がったりします。情報システム部門にとっては大きなリスクとして認知しておく必要があります。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	3－3－(1)不正アクセス・コンピュータウイルス関連					
3．コンピュータウイルスのリスク	コンピュータウイルス被害・復旧コスト	3- 3- 1- 6	Q コンピュータウイルス被害から全面復旧までにかかる費用を分析していますか? (コンピュータウイルスはコンピュータの機能を阻害したり、他のコンピュータを攻撃します。ウイルスに感染した場合は、企業のビジネスが停止するのみならず、ウイルスを除去するためのコストも必要になります。この間、情報システムが使えないため、その影響はきわめて大きいのです。情報システム部門は常にこのリスクを考え、ウイルスに感染しないような対策をたてる必要があります。また、万一感染した時のための緊急時対策が必要です。)		●		
	コンピュータウイルス被害による機会損失	3- 3- 1- 6- 1	Q コンピュータウイルス被害によってユーザ業務が受ける機会損失を分析していますか？ (コンピュータウイルスの被害には、情報システムが停止してビジネスが混乱したり、遂行できない場合があります。この場合のリスクについて情報システム部門が理解して対策をたてる必要があります。被害はユーザの方が大きいのです。)		●		
	感染の影響	3- 3- 1- 7	Q コンピュータウイルス感染のリスク(サービス中断など)を分析していますか？ (コンピュータウイルスの感染のリスクには、情報システムが停止してビジネスが遂行できない場合があります。この場合のリスクについて情報システム部門のみならず、ユーザ部門は理解して対策をたてる必要があります。)		●	●	
	取引先への影響	3- 3- 1- 7- 1	Q コンピュータウイルス感染によって取引先に悪影響や不安を与えるリスクを分析していますか？ (コンピュータウイルスは、取引先にウイルスを感染させて被害を与えたり、取引が中断したり、企業情報システムの運用体制の不備があることを伝えることになります。このリスクを理解して、取引先への影響を最小限にする対策が必要です。)		●		
	株価への影響	3- 3- 1- 7- 2	Q コンピュータウイルス感染による株価への影響のリスクを分析していますか？ (コンピュータウイルスの感染の事実は発表のみならず、うわさですぐに広がります。この事実は企業の信用度を著しく低下させることになります。少なくとも、情報システムの管理が十分でないこと、マネジメントの管理能力が十分でないことを伝えることになります。これはすぐに株価に影響するでしょう。ウイルス感染で情報システムが長期間停止すると株価は大きく低下することもあります。したがって、ウイルス感染は企業にとっての大きなリスクであることを意識すべきです。)		●		
	損害賠償請求	3- 3- 1- 7- 3	Q コンピュータウイルス感染によって取引先から損害賠償を請求されるリスクを分析していますか？ (最近、コンピュータウイルスの感染でコンピュータからウイルスを除外する作業や、企業がビジネスを遂行できなかったための機会損失を取引先から請求される場合があります。法律的に支払義務があるかは今後の法廷でのケースによりますが、訴えられる可能性は排除できません。このようなリスクを考慮しておく必要があります。ウイルスを他へ拡散させない対応や企業の法的な対応が必要です。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	3－3－(1)不正アクセス・コンピュータウイルス関連					
3．コンピュータウイルスのリスク	ベンダ緊急時対応の遅れ	3- 3- 1- 8	Q アンチウイルスに関するベンダのコンピュータウイルスサポート体制をチェックしなかったため、緊急時に対応できない場合のリスクを分析していますか？ (緊急時には、コンピュータウイルス対策ソフトのベンダも大変忙しい状況に陥ります。このようなときにどこまでサポートをしてもらえるかは、契約によります。緊急時に困らないためには、緊急時のことを考慮した体制を日頃から準備しておくことが望まれます。もちろん、自社で対応するという選択肢も重要です。)		●		
	アンチウイルス更新遅れ	3- 3- 1- 9	Q アンチウイルスのパラメータファイルが更新されていなかったため、コンピュータウイルスに対応できず、被害を受けるリスクを分析していますか？ (コンピュータウイルス対策ソフトはウイルスが発生しない限り、パラメータファイルを作成できません。したがって、データファイルができるまでの期間は感染する危険性があります。また、データファイルができても、十分に対応できるかは不明です。したがって、アンチウイルスソフトを使っているから安全という保証はありません。)		●		
	定期検診以上の蔓延	3- 3- 1- 10	Q 定期的なウイルスチェックだけでは間に合わず、コンピュータウイルスの蔓延を防ぐことができなかった場合のリスクを分析していますか？ (コンピュータウイルス対策ソフトはウイルスが発生しない限り、パラメータファイルを作成できません。また、パラメータファイルの更新を行っていないと無力です。そのような場合にはウイルス感染が免れません。感染を前提としたリスクを分析することが基本となります。)		●	●	
4．電子メールのリスク	コンピュータウイルス誤配	3- 3- 1- 11	Q 電子メールの利用によってコンピュータウイルスを誤って他社に送ってしまった場合のリスクを分析していますか？ (コンピュータウイルス感染が100%防ぎきれないことを前提とすると、電子メールなどで他社にウイルスを送ってしまうリスクは常に存在します。送らない対策も重要ですが、万一送ってしまった時にどうなるのか、考えておく必要があります。)		●	●	
5．ネットワークのリスク	ネットワークの大規模なダウン	3- 3- 1- 12	Q コンピュータウイルスや不正アクセスの結果としてネットワーク(インターネット)が大規模障害になり、利用できない場合のリスクを分析していますか？ (2003年1月のSlammer Wormや同年8月のMSBlasterでは、ワームが急増してネットワークが輻輳するというケースが発生しました。そのため、ウイルス対策を十分に行っていても、インターネットが使えないためにビジネスが継続できなくなりました。これは、自分だけでは対処できないものです。このようなケースが起こりうるリスクを考慮しておく必要があります。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
災害	災害	3－3－(2) 災害					
1．管理	情報システムへの影響	3- 3- 2- 1	Q 災害が情報システムに与える影響のリスクを分析していますか？ (災害(自然災害・人的災害を含む)が発生した場合、情報システム全体に与える影響度を想定しているかを確認します。) (用語解説「影響度」:情報システムの機能上どのような支障がでるのか、また支障の大きさはどの程度かを指します。)		●	●	(4.3.1)
	災害復旧手順	3- 3- 2- 2	Q 災害発生時の復旧手順について情報システムに与える影響のリスクを分析していますか？ (災害が発生した場合の復旧手順が整備されているか、また、復旧手順の内容が情報システムに対する被害を最小限に食い止めるものと考えられているかを確認します。)		●	●	(4.3.1)
2．災害	自然災害	3- 3- 2- 3	Q 自然災害が情報システムに与える影響のリスクを分析していますか？ (災害の対象を自然災害(特に以下1～8の第5階層レベルに示されている自然災害)に絞って、情報システムに与える影響度を想定しているかを確認します。)		●	●	
	地震・津波・噴火	3- 3- 2- 3- 1	Q 地震・津波・噴火が情報システムに与える影響のリスクを分析していますか？		●	●	
	台風・高潮	3- 3- 2- 3- 2	Q 台風・高潮が情報システムに与える影響のリスクを分析していますか？		●	●	
	水災・洪水	3- 3- 2- 3- 3	Q 水災・洪水が情報システムに与える影響のリスクを分析していますか？		●	●	
	竜巻・風災	3- 3- 2- 3- 4	Q 風害(竜巻・風災)が情報システムに与える影響のリスクを分析していますか？		●	●	
	落雷	3- 3- 2- 3- 5	Q 落雷が情報システムに与える影響のリスクを分析していますか？		●	●	
	雪害	3- 3- 2- 3- 6	Q 雪害が情報システムに与える影響のリスクを分析していますか？		●	●	
	雹害	3- 3- 2- 3- 7	Q 雹害が情報システムに与える影響のリスクを分析していますか？		●	●	
	天候不良・異常気象	3- 3- 2- 3- 8	Q 天候不良・異常気象(長期の日照り、冷夏、暖冬等)が情報システムに与える影響のリスクを分析していますか？		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
災害	災害	3－3－(2) 災害					
3．事故	事故	3- 3- 2- 4	Q 事故が情報システムに与える影響のリスクを分析していますか？ (突発的に発生する事件・事故(特に以下1～5までの第5階層レベルに示されている事件・事故)が、情報システムに与える影響度を想定しているかを確認します。(この場合、事件・事故の原因は問題としません。))		●	●	(4.3.1)
	火災・爆発	3- 3- 2- 4- 1	Q 火災・爆発が情報システムに与える影響のリスクを分析していますか？		●	●	
	停電	3- 3- 2- 4- 2	Q 停電が情報システムに与える影響のリスクを分析していますか？		●	●	
	人的損失	3- 3- 2- 4- 3	Q 人的損失(航空機事故・列車事故・船舶事故・交通事故)が情報システムに与える影響のリスクを分析していますか？ (情報システムに影響を与える人的損失の対象となる人の範囲(組織内・外を問わない)を明確にし、また、それらの人的損失が情報システムに与える影響度を想定しているかを確認します。)		●	●	
	漏水	3- 3- 2- 4- 4	Q 漏水が情報システムに与える影響のリスクを分析していますか？		●	●	
	動物害	3- 3- 2- 4- 5	Q 動物の害が情報システムに与える影響のリスクを分析していますか？ (用語解説「動物の害」:情報システムに何らかの害を与えると考えられるすべての動物が対象となります。)		●	●	
4．人的災害	人的災害	3- 3- 2- 5	Q 人的災害が情報システムに与える影響のリスクを分析していますか？ (人の手による災害(特に以下1、2に示す第5階層レベルの災害)が情報システムに与える影響度を想定しているかを確認します。)		●	●	(4.3.1)
	戦争・動乱・暴動による影響	3- 3- 2- 5- 1	Q 戦争・動乱・暴動が情報システムに与える影響のリスクを分析していますか？ (国内・外を問わず戦争・動乱・暴動が発生した場合の情報システムに与える影響度を想定しているかを確認します。)		●		
	人的リスクの可能性	3- 3- 2- 5- 2	Q 自然災害に乗じて起こる人的リスクの可能性を分析していますか？ (自然災害の発生によって組織体に何らかの被害を被るか混乱が起こった場合、それらの事態に便乗又は影響を受ける人の行動が、情報システムに与える影響度を想定しているかを確認します。)		●	●	
5．委託先リスクの可能性	委託先リスクの可能性	3- 3- 2- 6	Q 委託先が災害等の上記リスクを受けた場合のリスクを分析していますか？ (上記に示した災害等の影響が委託先に及ぼされた場合の、自社の情報システムに与える影響度を想定しているかを確認します。)		●		(4.4.4.3)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
障害	障害	3－3－(3) 障害					
1．管理	情報システムへの影響	3－ 3－ 3－ 1	Q 障害発生時における情報システムに与える影響のリスクを分析していますか？ (情報システムの機能に支障をきたす障害が発生した場合の影響度を想定しているかを確認します。)		●	●	(4.3.1)
	復旧手順	3－ 3－ 3－ 2	Q 障害発生時の復旧手順が情報システムに与える影響のリスクを分析していますか？ (障害が発生した場合の復旧手順が整備されているかを確認します。また、復旧手順の内容が情報システムに対する被害を最小限に食い止めるものと考えられるかについても確認します。)		●	●	
2．ハードウェア障害	ハードウェア障害	3－ 3－ 3－ 3	Q ハードウェア障害(LAN、ファイアウォール等を含む)のリスクを分析していますか？ (ハードウェア(LAN(Local Area Network)・ファイアウォール等を含むもので、特に以下1～5までの第5階層レベルに示すハードウェア)に障害が発生した場合の情報システムに与える影響度を想定しているかを確認します。)		●		(4.3.1)
	ネットワーク(WAN)障害	3－ 3－ 3－ 3－ 1	Q ネットワーク(WAN)障害のリスクを分析していますか？		●		
	サーバ障害	3－ 3－ 3－ 3－ 2	Q サーバ障害のリスクを分析していますか？		●		
	ISPサービス機能障害	3－ 3－ 3－ 3－ 3	Q インターネットサービスプロバイダのサービス機能障害のリスクを分析していますか？		●		
	端末機器障害	3－ 3－ 3－ 3－ 4	Q ユーザ又は端末、クライアント機の障害のリスクを分析していますか？		●		
	停電	3－ 3－ 3－ 3－ 5	Q 停電(UPS障害等)が情報システムに与える影響のリスクを分析していますか？ (用語解説「停電」:情報システムの運用に影響を与える停電(UPS(無停電電源装置)の障害による停電も含む)を指します。)		●		
3．ソフトウェア障害	ソフトウェア障害	3－ 3－ 3－ 4	Q ソフトウェア障害のリスクを分析していますか？ (ソフトウェア(特に以下1～5に示す第5階層レベルのソフトウェア)に障害が発生した場合の情報システムに与える影響度を想定しているかを確認します。)		●	●	(4.3.1)
	OS、ライセンスプログラム障害	3－ 3－ 3－ 4－ 1	Q サーバのOS、ライセンスプログラムの障害のリスクを分析していますか？ (用語解説「ライセンスプログラム」:許諾契約によって使用可能となるプログラムを指します。)		●		
	アプリケーションプログラム停止	3－ 3－ 3－ 4－ 2	Q サーバのアプリケーションプログラムが停止した場合のリスクを分析していますか？ (用語解説「停止」:完全停止・部分停止を指します。)		●		
	アプリケーションプログラム誤処理	3－ 3－ 3－ 4－ 3	Q アプリケーションプログラムの誤処理が情報システムに与える影響のリスクを分析していますか？ (用語解説「アプリケーションプログラム」:情報システムの運用上必要とするすべてのアプリケーションプログラムを指します。)		●		
	端末機器障害	3－ 3－ 3－ 4－ 4	Q ユーザ又は端末、クライアント機の障害のリスクを分析していますか？		●		
	その他ソフトウェア障害	3－ 3－ 3－ 4－ 5	Q その他ソフトウェアの障害のリスクを分析していますか？ (用語解説「その他のソフトウェア」:自社における情報システムの運用上、直接必要としているソフトウェア以外のソフトウェアを指します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク分析	リスク分析	Ⅲ. 情報システムのリスク分析					
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムの個別リスク分析					
障害	障害	3－3－(3) 障害					
4. 運用ミス障害	運用ミス障害	3- 3- 3- 5	Q 運用ミス障害のリスクを分析していますか？ (運用上想定されるすべてのミスが発生した場合の情報システムに与える影響度を想定しているかを確認します。ここでは、次の第5階層レベルに示されている「運用ミスとしてのバックアップの不備」以外の運用ミスも考慮に入れて判断します。).		●	●	(4.3.1)
	バックアップ不備	3- 3- 3- 5- 1	Q バックアップの不備によるリスクを分析していますか？ (運用ミスと考えられるバックアップ上の不備が発生した場合の情報システムに与える影響度を想定しているかを確認します。)		●		
	ソフトウェア更新手続ミス	3- 3- 3- 6	Q ソフトウェア更新手続ミスが情報システムに与える影響のリスクを分析していますか？ (ソフトウェアの更新のための手続にミスがあることを放置しておいた場合の、情報システムに与える影響度を想定しているかを確認します。)		●		
	人的リスクの可能性	3- 3- 3- 7	Q オペレーションミスによる消去、誤記入に乗じて起こる人的リスクの可能性を分析していますか？ (オペレーションミスによって、ソフトウェア・データ等を消去又は誤記入してしまった場合の混乱・動揺による人の行動が情報システムに与える影響度を想定しているかを確認します。)		●		(4.3.1)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
1．情報セキュリティポリシー	情報セキュリティポリシー	4- 1- 1- 1	Q リスクマネジメントポリシーに基づいて情報セキュリティポリシーを定めていますか？ (情報セキュリティポリシーとリスクマネジメントポリシーの整合性がどの程度とれていて、矛盾はどの程度かを確認します。ここではリスクマネジメントポリシーと情報セキュリティポリシーが整備されていることが前提となっています。ただし、明確にリスクマネジメントポリシー又は情報セキュリティポリシーとなっていなくても、そのような意味合いを持つ内容のものでもよく、その意味合いの明確さによって評価します。)		●	●	(4.3.1)
2．情報セキュリティポリシーに基づく実施基準	情報セキュリティポリシーに基づく実施基準	4- 1- 1- 2	Q 情報セキュリティポリシーに基づく実施基準を定めていますか？ (実施基準と情報セキュリティポリシーの整合性がどの程度とれていて、矛盾はどの程度かを確認します。ここでは情報セキュリティポリシーと実施基準が整備されていることが前提となっています。ただし、明確に情報セキュリティポリシー又は実施基準となっていなくても、そのような意味合いの内容を持つものでもよく、その意味合いの明確さによって評価します。特に以下1～15に示す第5階層レベルの内容が情報セキュリティポリシーとの整合性を考慮して、実施基準に示されているか否かを確認します。)		●	●	(4.3.1)
	情報システム総合企画	4- 1- 1- 2- 1	Q 実施基準に情報システム総合企画のリスク対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システム総合企画(情報システムに関する長期計画・情報システム戦略・開発の前提となる情報システムの事前分析も対象となる)に関して想定されるリスク対策が明確に定められているかを確認します。)		●	●	(4.4.4.2)
	システム開発	4- 1- 1- 2- 2	Q 実施基準にシステム開発のリスク対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、システム開発(システム保守・システム改善も対象となる)に関して想定されるリスク対策が明確に定められているかを確認します。)		●	●	
	システム運用	4- 1- 1- 2- 3	Q 実施基準にシステム運用のリスク対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、システム運用に関して想定されるリスク対策が明確に定められているかを確認します。)		●	●	(4.4.4.2)
	アウトソーシング	4- 1- 1- 2- 4	Q 実施基準にアウトソーシング関連のリスク対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、アウトソーシングに関して想定されるさまざまなリスク対策が明確に定められているかを確認します。)		●	●	(4.4.4.3)
	システム監査	4- 1- 1- 2- 5	Q 実施基準にシステム監査を定めていますか？ (実施基準又はそれと同等とみなされるものに、システム監査(内部・外部、定期・不定期を問わない)の実施が明確に定められているかを確認します。)		●	●	(4.5)
	コンピュータ犯罪	4- 1- 1- 2- 6	Q 実施基準にコンピュータ犯罪対策を定めていますか？ (実施基準またはそれと同等とみなされるものに、想定されるコンピュータ犯罪対策が明確に定められているかを確認します。)		●	●	(4.4.4.2)
	不正アクセス	4- 1- 1- 2- 7	Q 実施基準に不正アクセス対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、不正アクセス対策が明確に定められているかを確認します。)		●	●	(4.4.4.2)
	コンピュータウイルス	4- 1- 1- 2- 8	Q 実施基準にコンピュータウイルス対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、コンピュータウィルス対策が明確に定められているかを確認します。また、必要に応じて最新の状態に更新するように示されているかを確認します。)		●	●	(4.4.4.2)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
2．情報セキュリティポリシーに基づく実施基準	E-Commerce	4- 1- 1- 2- 9	Q 実施基準にE-Commerce対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、インターネットを利用して、受発注や決済業務など、電子商取引を行おうとする場合に想定されるリスクへの対策が明確に定められているかを確認します。)		●	●	
	電子メール	4- 1- 1- 2- 10	Q 実施基準に電子メール利用対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、社内で電子メールを利用する際に想定されるリスクへの対策が明確に定められているかを確認します。)		●	●	
	災害・障害対策	4- 1- 1- 2- 11	Q 実施基準に災害・障害対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、災害・障害が発生した場合に想定される被害を最小限に食い止める対策が明確に示されているかを確認します。)		●	●	(4.4.4.2)
	権限付与	4- 1- 1- 2- 12	Q 実施基準に個人情報にアクセスできる権限付与を定めていますか？		●	●	(4.4.1)
	その他関連項目	4- 1- 1- 2- 13	Q 実施基準にその他関連項目(経営リスク、政治・経済・社会リスク等)を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システムに係わる経営的なリスクおよび社外環境としての政治上・経済上・社会上の変化を想定されるリスクとして捉え、その対策が可能な範囲で定められているかを確認します。)		●	●	
	バックアップ	4- 1- 1- 2- 14	Q 実施基準にバックアップ対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システムの運用上必要とされるデータ・ソフトウェア等のバックアップを確実に取ることが明確に定められているかを確認します。)		●	●	
	緊急時対策	4- 1- 1- 2- 15	Q 実施基準に緊急時対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システムに対して想定される緊急事態が発生した場合の被害を最小限に食い止める対策が明確に定められているかを確認します。)		●	●	(4.3.1)
	リスクマネジメントシステム計画との整合性	4- 1- 1- 3	Q 実施基準はリスクマネジメントシステム計画と整合性をとって定めていますか？ (実施基準又はそれと同等とみなされるものと、リスクマネジメントシステム計画又はそれと同等とみなされるものとの整合性がどの程度とれていて、矛盾がどの程度かを確認します。ここでは実施基準およびリスクマネジメントシステム計画又はそれと同等のものが整備されていることが前提となっています。整備の程度・整合性の程度によって、判定基準の評価を行います。特に以下1～6までの第5階層レベルに示された内容の整合性を考慮する必要があります。)		●	●	
	企業特性	4- 1- 1- 3- 1	Q 実施基準は企業の特性を重視して作成していますか？ (実施基準又はそれと同等とみなされるものは、それぞれの企業が持つ特性を考慮して作成されているか(企業の独自性を持っているか)を確認します。)		●	●	
	論理的な構築	4- 1- 1- 3- 2	Q 実施基準の中のリスク対策は情報処理プロセスに沿って論理的に構築されていますか？ (実施基準又はそれと同等とみなされるものに示されている種々のリスク対策は、組織内の情報処理のプロセスに矛盾なく、また飛躍もなく順序正しくまとめられているかを確認します。)		●	●	
	評価リスト	4- 1- 1- 3- 3	Q 実施基準は実践的な項目配列、継続的な日常点検、点検結果の評価リストを定めていますか？ (実施基準又はそれと同等とみなされるものの項目内容は、論理的で実行しやすく配列されているべきです。また、項目内容の妥当性について定期的に点検を行い、その結果を評価リストに記録することが明確に定められているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
2．情報セキュリティポリシーに基づく実施基準	緊急事態復旧計画	4- 1- 1- 3- 4	Q 実施基準は緊急事態発生後の復旧サービスレベル等について定めていますか？ (実施基準又はそれと同等とみなされるものに、緊急事態が発生した場合の情報システムの復旧について、通常のサービスが提供できる状態になるまでの最低日数、および通常のサービスができる状態になるまでの段階的サービスレベルが明確に定められているかを確認します。)		●	●	
	JIS Q 15001との整合性	4- 1- 1- 3- 5	Q 実施基準の策定に関してJIS Q 15001との整合性を考慮していますか？		●		[4.2] [4.4]
	ISO17799との整合性	4- 1- 1- 3- 6	Q 実施基準の策定に関してISO17799(JIS X 5080、ISMS)等との国際的な整合性を考慮していますか？ (実施基準又はそれと同等とみなされるものは、ISO17799(国際規格 セキュリティ管理基準)(JIS X 5080(情報セキュリティマネジメント実践のための規範)、ISMS(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))との整合性を考慮した上で策定されているかを確認します。)		●		
	実施基準での禁止事項	4- 1- 1- 4	Q 実施基準には禁止事項を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システム管理上やってはいけない事項が禁止事項として(特に以下1～23の第5階層レベルに示された内容について)明確に定められているかを確認します。)		●	●	(4.2)
	市販ソフトのコピー使用	4- 1- 1- 4- 1	Q 市販のソフトをコピーして使う行為を禁止していますか？ (コピーが禁止されている市販ソフトを業務上使用する場合、コピーを禁止することが明確に示されているかを確認します。)		●	●	
	データ・プログラムの無断使用	4- 1- 1- 4- 2	Q 所有者のあるデータ、プログラムを無断で使う行為を禁止していますか？ (所有者が定められているデータ、又はプログラムを所有者に無断で使用することができないような措置を取っているかを確認します。(この場合、所有者が明確であることが大切です。))		●	●	
	機密情報搾取行為	4- 1- 1- 4- 3	Q イントラネットあるいはLAN情報処理環境に侵入し、機密情報を窃取する行為を禁止していますか？ (イントラネット又はLANなどのネットワークに侵入し、情報システム上の情報を窃取する行為を禁止する措置を取っているかを確認します。(この場合、機密情報は絶対的に対象になりますが、機密でないすべての情報が禁止の対象となります。))		●	●	
	覗き見	4- 1- 1- 4- 4	Q 所有者のあるデータ、プログラムを覗き見る行為を禁止していますか？ (所有者が定められているデータ、又はプログラムを所有者に無断で見ることができないような措置を取っているかを確認します。(この場合、所有者が明確であることが大切です。))		●	●	
	コンピュータ私的利用	4- 1- 1- 4- 5	Q 会社のコンピュータを私用に使う行為を禁止していますか？ (会社所有のコンピュータを用いて、私的目的に使用することを禁止する措置を取っているかを確認します。(この場合、個人貸与のコンピュータであっても、所有権が会社にあるコンピュータは対象になります。))		●	●	
	コンピュータウイルス伝染行為	4- 1- 1- 4- 6	Q コンピュータウイルスを伝染させる行為を禁止していますか？ (コンピュータウイルスを社内・外を問わず、故意に伝染させる行為を禁止する措置を取っているかを確認します。)		●	●	
	不正侵入行為	4- 1- 1- 4- 7	Q 他社のシステムへ不正侵入する行為を禁止していますか？ (理由の如何を問わず、他社の情報システムに不正に侵入する行為を禁止する措置を取っているかを確認します。)		●	●	(4.4.4.2)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
2．情報セキュリティポリシーに基づく実施基準	WWWの私的利用	4- 1- 1- 4- 8	Q WWWを仕事以外(個人目的での発注、アンケート回答等)で利用する行為を禁止していますか？ (WWW:World Wide Web(インターネットでの情報検索システムなど)を私用(個人目的での発注、アンケート回答等)で利用する行為を禁止する措置を取っているかを確認します。)		●	●	
	データ不正入力	4- 1- 1- 4- 9	Q 外部端末からインターネットを通じてデータの不正入力を行い、情報攪乱する行為を禁止していますか？ (外部の端末(端末としての機能を有するすべての端末)からインターネットを通じて不正にデータ入力を行い、情報システム内の情報をかき乱すような行為を禁止する措置を取っているかを確認します。)		●	●	
	私用電子メール使用	4- 1- 1- 4- 10	Q 私用の電子メールを受発信する行為を禁止していますか？ (勤務時間中に私用の電子メールを受発信する行為を禁止する措置を取っているかを確認します。(この場合、会社のコンピュータ、私用のコンピュータ、携帯端末などのすべての機器を対象とします。))		●	●	
	ファイルの覗き見行為	4- 1- 1- 4- 11	Q ネットワークにログインしている他者のファイルを許可なく見る行為を禁止していますか？ (ネットワークにログインしている他者のファイルを無断で見る行為を禁止する措置を取っているかを確認します。) (用語解説「ログイン」:パソコン通信サービス、FTP(File Transfer Protocol)サーバなどに接続することなどをいいます。)		●	●	
	仕事以外のファイルの覗き見行為	4- 1- 1- 4- 12	Q 共有サーバにある仕事に関係していないファイルを見る行為を禁止していますか？ (共通で使用しているサーバにあるファイルについて、業務上関係のないファイルを不必要に見る行為を禁止する措置を取っているかを確認します。)		●	●	
	他人のID無断使用	4- 1- 1- 4- 13	Q 他人のIDを無断借用する行為を禁止していますか？ (他人のIDを無断で借用(使用)する行為を禁止する措置を取っているかを確認します。) (用語解説「ID」:個人を識別するものすべてを指します。)		●	●	
	接続されたマシンの無断操作	4- 1- 1- 4- 14	Q メール、ブラウザ等接続されたままの他者の機器を操作する行為 を禁止していますか？ (電子メール、ブラウザなどが接続されたままの状態にある他人の機器を、無断で(本人の許可なく)操作する行為を禁止する措置を取っているかを確認します。) (用語解説「ブラウザ」:インターネットのWebを見るソフトウェアのことをいいます。)		●	●	
	個人情報の不正な取扱い	4- 1- 1- 4- 15	Q 個人情報の不正な取扱いを禁止していますか？		●	●	4.4.4
	顧客情報の売却	4- 1- 1- 4- 16	Q 業務上入手した顧客情報を正当な理由なしに第三者に売却する行為を禁止していますか？ (業務上又は業務以外の場で入手した顧客に関する情報を、正当な理由なしに第三者に売却もしくは無償提供する行為を禁止する措置を取っているかを確認します。)		●	●	4.4.5
	ホームページによる誹謗中傷行為	4- 1- 1- 4- 17	Q 許可なくホームページを書き換えて会社や組織に対し誹謗中傷する行為を禁止していますか？ (掲載されているホームページを無断で書き換えて、自社や自組織(他社や他組織)に対する誹謗中傷を行う行為を禁止する措置を取っているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
2．情報セキュリティポリシーに基づく実施基準	電子掲示板による誹謗中傷行為	4- 1- 1- 4- 18	Q 電子掲示板を用いて特定の組織、人間を誹謗中傷したり、名誉を傷つける行為を禁止していますか？ (電子掲示板を利用して、特定の組織(自組織・他組織)、又は個人を誹謗中傷したり、その名誉を傷つける行為を禁止する措置を取っているかを確認します。) (用語解説「電子掲示板」:ネットワークやパソコン通信などで、そこにアクセスしてくる人々と文字によるコミュニケーションを行える機能を持つすべてのものを指します。)	[redacted]	●	●	
	動作障害行為	4- 1- 1- 4- 19	Q 情報システムの動作障害を引き起こす行為を禁止していますか？ (故意に情報システムの動作を正常でない状態にするような行為を禁止する措置を取っているかを確認します。)		●	●	
	プログラム・データ改ざん	4- 1- 1- 4- 20	Q 正当な理由なくプログラム、データを改ざんする行為を禁止していますか？ (正当な理由又は正規の手続なしで、プログラムやデータを改ざんする行為を禁止する措置を取っているかを確認します。)		●	●	(4.4.4.1)
	無許可情報の開示行為	4- 1- 1- 4- 21	Q 許可なく情報をシステムを通じて開示する行為を禁止していますか？ (許可なく情報(開示されていないすべての情報)又はプログラムを情報システムを利用して開示する行為を禁止する措置を取っているかを確認します。)		●	●	
	スパムメール発信行為	4- 1- 1- 4- 22	Q スパムメールを発信する行為を禁止していますか？ (受信した人にとって迷惑になる、又は迷惑になると想定されるメールを発信する行為を禁止する措置を取っているかを確認します。)		●	●	
	社会秩序を乱す情報提供	4- 1- 1- 4- 23	Q 社会秩序の安全維持に反する情報の提供を禁止していますか？ (社会秩序の安全維持(公序良俗に違反する行為も含む)に反する情報の発信および受信の行為を禁止する措置を取っているかを確認します。)		●	●	
	コンプライアンス	4- 1- 1- 5	Q 実施基準はコンプライアンスに関する事項を定めていますか？ (実施基準又はそれと同等とみなされるものは、コンプライアンスに関する事柄が明確に定められているかを確認します。なお、コンプライアンスと共に罰則規程を定めていることが重要です。) (用語解説「コンプライアンス」:法律その他で定められた事項を遵守することです。)		●	●	4.4.8
	廃棄基準	4- 1- 1- 6	Q 実施基準に媒体の消去・廃棄について明確に定められていますか？ (個人情報の場合、消去・廃棄が十分にされていないために情報漏えい等が生じる可能性があります。)		●	●	4.4.4.2
	情報オーナーの責任	4- 1- 1- 7	Q 実施基準は機密性の高い個別情報の生成、管理、破棄に至るまでの情報のオーナーの責任と役割について定めていますか？ (実施基準又はそれと同等とみなされるものには、機密性の高い個別情報の生成、管理、廃棄に至るまでについて、情報のオーナーが明確であり、オーナーに対する責任と役割が定められているかを確認します。) (用語解説「機密性の高い個別情報」:特に高い機密度が明示されている、いないに関わらず、機密度が高いと判断される情報はすべて対象となります。)		●	●	4.3.1
	自己点検システム・監査システム	4- 1- 1- 8	Q 実施基準は内部者の情報システム利用の自己点検、監査について定めていますか？ (実施基準又はそれと同等とみなされるものには、内部の情報システム利用者の自己点検(点検項目に従った自己申告による定期的な点検)および監査の実施が定められているかを確認します。) (用語解説「監査」:継続的に自己点検が実施されており、内容に虚偽がないかを定期的に第三者が調べることです。)		●	●	(4.5)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
2．情報セキュリティポリシーに基づく実施基準	実施基準の定期的見直し	4- 1- 1- 9	Q 実施基準を定期的に見直していますか？ (実施基準又はそれと同等とみなされるものは、定期的に見直しを行うことが定められているか、また、確実に実施されているかを確認します。)		●	●	(4.6)
	企業内教育	4- 1- 1- 10	Q 実施基準は情報システムの利用に関する教育要領を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システムの利用に関する教育要領(内部、外部に係わらず何らかの形で情報システム利用者全員が対象となる)が具体的に定められているかを確認します。)		●	●	(4.4.6)
	情報セキュリティポリシーの徹底	4- 1- 1- 11	Q 情報セキュリティポリシーについての教育等を実施していますか？ (情報セキュリティポリシー又はそれと同等とみなされるものについて、関係者全員を対象とした教育訓練を定期的に実施しているか、また、結果を記録として一定期間残しているかを確認します。)		●	●	
3．情報資産インベントリ	情報資産目録	4- 1- 1- 12	Q 保護対象の情報資産は漏れなくインベントリ(目録)リストに列挙していますか？ (情報セキュリティ上、保護の対象となっている情報資産が漏れなく目録に示されているかを確認します。)		●	●	4.3.1
	劣化媒体の排除	4- 1- 1- 12- 1	Q 保護対象インベントリ(目録)から劣化した媒体を排除していますか？ (情報セキュリティ上、保護対象となった情報資産のうち、媒体が劣化したものを正規の手続の後、目録から排除して、排除した記録を一定期間保存しているかを確認します。)		●		
	重要資産の取扱いと重要装置の仕様	4- 1- 1- 12- 2	Q 実施基準は重要資産および重要装置の仕様の取扱いを定めていますか？ (実施基準又はそれと同等とみなされるものには、情報セキュリティ上重要とされる資産および重要とされる装置の仕様についての取扱方法や注意事項が明確に定められているかを確認します。特に仕様には当該資産又は装置が情報セキュリティ上重要なものに指定されていることが明示されているかを確認します。)		●		4.4.4.2
	機密度ランク	4- 1- 1- 13	Q 実施基準は情報の機密度のランクを定めていますか？ (実施基準又はそれと同等とみなされるものには、情報について規定に従った機密度のランクを明確にすることが定められているかを確認します。)		●	●	4.4.4.2
4．スタッフ	情報セキュリティ・個人情報保護管理担当者	4- 1- 1- 14	Q 情報セキュリティ管理者・個人情報保護管理者がいますか？ (情報セキュリティ管理者、個人情報保護管理者が指名されており、自他ともに存在が明確になっているかを確認します。)		●	●	4.4.1
	スタッフ	4- 1- 1- 14- 1	Q スタッフに対して強制休暇をとらせる制度がありますか？ (情報システムに係わる関係者全員に対して、定期的に一定期間強制的に交代で休暇を取らせることが制度として確立しているかを確認します。)		●	●	4.4.1
	業務ローテーション	4- 1- 1- 14- 2	Q スタッフに対してリスクの視点から定期的な業務のローテーションを組んでいますか？ (情報システムに係わる関係者全員に対して、リスクマネジメント上の理由で定期的に業務担当の入替え(交代)を制度として実施しているかを確認します。)		●	●	
	個人情報作業責任者	4- 1- 1- 14- 3	Q 個人情報を取り扱う作業責任者が明確になっていますか？		●	●	4.4.1

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
5. 情報セキュリティ個別対策	操作と業務処理手順	4- 1- 1- 15	Q 実施基準は情報システムに関して操作および業務処理方法等を具体的に示していますか？ (実施基準又はそれと同等とみなされるものに、情報システムに関する操作方法および関連業務の処理方法、緊急時対策が具体的に示されているか、また、常に最新の状態に保たれているかを確認します。)		●	●	4.4.1
	出張、移動中の実施基準	4- 1- 1- 16	Q 実施基準は出張中、移動中の個人情報の取扱いについて定めていますか？ (実施基準又はそれと同等とみなされるものに、関係者の出張中又は移動中(移動の手段は問わない)の個人情報の取扱いについて具体的に定められているかを確認します。)		●	●	
	携帯端末利用	4- 1- 1- 17	Q 携帯端末を利用している場合、実施基準は携帯端末の利用について定めていますか？ (情報システムの関係者が情報システムに対して携帯端末を用いて作業を行うケースがある場合、実施基準又はそれと同等とみなされるものに携帯端末利用上の情報セキュリティ対策が定められているかを確認します。)		●	●	
	ユーザ認証、アクセス管理	4- 1- 1- 17- 1	Q 実施基準は携帯端末からのユーザ認証、アクセス管理を定めていますか？ (実施基準又はそれと同等とみなされるものに、情報システムに対して携帯端末から作業を実施しようとする場合、利用者が間違いなく本人であることを確認する仕組み、またデータの書込みや読出しを管理する仕組みが具体的に定められているかを確認します。)		●	●	(4.3.1)
	携帯端末紛失連絡体制	4- 1- 1- 17- 2	Q 実施基準は携帯端末を紛失した場合の連絡体制、アクセス禁止等の手続を定めていますか？ (個人情報を含む携帯端末を紛失した場合は、個人情報漏えい等とみなされます。実施基準又はそれと同等とみなされるものに、情報システムで使用できる携帯端末を紛失又は盗まれた場合の緊急連絡体制が明確か、また、当該携帯端末の使用を不可能にする手続が明確に定められているかを確認します。)		●		
	授受記録	4- 1- 1- 18	Q 個人情報の授受記録を管理していますか？		●	●	4.4.3.1
	リスク管理文書化	4- 1- 1- 19	Q 実施基準はリスク管理に関する文書化について定めていますか？ (実施基準又はそれと同等とみなされるものに、リスクマネジメントの遂行に関して必要な事項がすべて文書化されているか、また、最新の状態に維持することが明確に定められているかを確認します。)		●	●	4.4.9
	データ、媒体利用	4- 1- 1- 20	Q 実施基準はデータや媒体の使用・保管の管理を定めていますか？ (実施基準又はそれと同等とみなされるものには、データやデータを保管する媒体についての使用、保管の管理事項が具体的に定められているかを確認します。また、個人情報を含む媒体の施錠管理を行うことが必要です。)		●	●	4.4.4.2

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
5. 情報セキュリティ個別対策	ログの定期的な確認・保管	4- 1- 1- 21	Q 実施基準は情報のオーナーおよびシステム管理者がアクセスログを定期的に確認し、安全に保管するよう定めていますか？ (実施基準又はそれと同等とみなされるものには、情報システムで管理されている情報のオーナーおよび情報システムの管理者が、当該情報システムのデータの書込みや読出しに関する記録を定期的に確認し、結果を記録し、その記録を安全に保管することが定められているかを確認します。)		●		(4.4.4.2)
	アクセスログ権限	4- 1- 1- 21- 1	Q 実施基準はアクセスログについてアクセスの権限、権限外の記録方法を定めていますか？ (実施基準又はそれと同等とみなされるものには、データの書込みや読出しに関する個々のケースごとに、権限内か、権限外かを明確に記録する方法が具体的に定められているかを確認します。)		●		4.3.1
	機密情報ログ	4- 1- 1- 21- 2	Q 機密度の高い個別情報に関して、生成、アクセス、その他の処理プロセスは、ログに残されていますか？ (情報システムにおいて、機密度の高い個別情報に関して、生成、情報の読出し、書込み、その他情報に関する処理の過程が漏れなく記録されるようになっているかを確認します。) (用語解説「機密度の高い個別情報」:機密度ランクが明確に定められている、いないに関わらず、機密度が高いと判断される個々の情報はすべて対象となります。)		●		(4.4.4.2)
	プログラムソースライブラリ管理	4- 1- 1- 22	Q 実施基準はプログラムソースライブラリの管理・修正・変更の記録についての方法を定めていますか？ (実施基準又はそれと同等とみなされるものには、プログラムソースライブラリ(汎用性の程度は問わない)について、その管理・修正・変更のつど確実に記録を取る方法が定められているかを確認します。)		●		
	基幹システムの国際利用	4- 1- 1- 23	Q 基幹システムを国際的に利用している場合、日本との差を把握して情報システムのセキュリティ対策を講じていますか？ (基幹システムを国際的に利用している場合、情報セキュリティに関する規制が日本と差がある場合の事業継続のため、その差を埋める情報システム上のセキュリティ対策を講じている必要があります。) (用語解説「基幹システム」:事業継続上必要とされる主要業務の遂行に欠くことのできない日常業務および決済業務の情報システムをいいます。)		●		
	情報システム利用手続	4- 1- 1- 24	Q 実施基準は情報システム利用の手続を定めていますか？ (実施基準又はそれと同等とみなされるものには、情報システムを利用する際のすべての者を対象とする手続が具体的に定められているかを確認します。)		●	●	
	プロバイダ選定基準	4- 1- 1- 25	Q 実施基準はプロバイダの選定基準を定めていますか？ (実施基準又はそれと同等とみなされるものには、組織内でプロバイダを選定する際の選定基準が具体的に定められているかを確認します。) (用語解説「プロバイダ」:インターネット接続サービスを提供する通信業者のことです。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
6．自社ホームページ承認	自社ホームページ承認	4- 1- 1- 26	Q 実施基準は自社のホームページへの掲載許可について定めていますか？ (実施基準又はそれと同等とみなされるものには、自社(自組織)で掲載しているホームページに何らかの情報を掲載しようとする場合の、掲載の許可に関する事柄が具体的に定められているか確認します。特に以下1～3の第5階層レベルに示す内容について定められているかを確認します。)		●	●	
	掲載許可	4- 1- 1- 26- 1	Q 自社のホームページへの掲載許可についてチェックしていますか？ (自社(自組織)で掲載しているホームページに掲載する際の掲載許可の内容および掲載許可の実施状況について、定期的にチェックが行われ、その結果が記録されているかを確認します。)		●	●	
	コンテンツの知的財産権	4- 1- 1- 26- 2	Q 実施基準はコンテンツの知的財産権の審査・登録の制度を定めていますか？ (実施基準又はそれと同等とみなされるものには、情報システム上で扱う情報の内容について知的財産権が妥当か否かの審査、および知的財産権を登録する制度が定められているかを確認します。)		●	●	
	ホームページ記載内容のチェック	4- 1- 1- 26- 3	Q HP記載内容の正確性、表現(差別用語等)等をチェックする部署を定めていますか？ (自社(自組織)のホームページに何らかの情報を記載する際に、その内容が間違いなく、表現方法が妥当(公序良俗に違反しておらず、差別用語を用いておらず、自社(自組織)の品位を損なうものでない)であることをチェックする部署が明確に定められているかを確認します。)		●	●	
	コンテンツ侵害への手続	4- 1- 1- 27	Q 実施基準はコンテンツへの侵害があった場合の手続を定めていますか？ (実施基準又はそれと同等とみなされるものには、情報システム上で扱う情報の内容について、自社(自組織)で持つ権利が明らかに損なわれていると判断された時の対応の手続が定められているかを確認します。)		●	●	
	営業機密漏えいチェック	4- 1- 1- 27- 1	Q コンテンツに関して、組織体の営業機密が不用意に漏えいされていないかチェックしていますか？ (情報システム上で扱う情報の内容から、自社(自組織)で持つ営業上の機密が何らかの理由で外部に漏えいされているか否かのチェックを定期的に行っているか、また、その結果を記録しているかを確認します。)		●		
7．教育内容	情報システム部門の教育内容	4- 1- 1- 28	Q 情報システム部門の教育訓練の内容に情報システムリスクおよび個人情報保護を網羅していますか？ (情報システム部門に対する教育訓練の内容に、情報システムに関するリスクマネジメントおよび個人情報保護の内容が盛り込まれているかを確認します。)		●		4.4.6
	緊急事態対応	4- 1- 1- 28- 1	Q 情報システム部門の教育訓練の内容に緊急事態対応を含んでいますか？ (情報システム部門に対する教育訓練の内容に、情報システムに関する緊急事態が発生した際の対応が盛り込まれているかを確認します。)		●		4.3.1
	誤作動対応	4- 1- 1- 28- 2	Q 情報システム部門の教育訓練の内容に誤作動対応を含んでいますか？ (情報システム部門に対する教育訓練の内容に、情報システムに誤作動があった場合の対応方法が盛り込まれているかを確認します。)		●		
	システム停止対応	4- 1- 1- 28- 3	Q 情報システム部門の教育訓練の内容にシステムの停止対応を含んでいますか？ (情報システム部門に対する教育訓練の内容に、情報システムが何らかの理由で停止した場合の対応方法が盛り込まれているかを確認します。)		●		
	システム侵入対応	4- 1- 1- 28- 4	Q 情報システム部門の教育訓練の内容にシステムへの侵入対応を含んでいますか？ (情報システム部門に対する教育訓練の内容に、何者かが情報システムに不正に侵入したと考えられる場合の対応が盛り込まれているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ					
7．教育内容	ユーザ部門の教育内容	4- 1- 1- 29	Q ユーザ部門の教育訓練の内容に情報システムリスクおよび個人情報保護を網羅していますか？ （業務上情報システムを利用する利用者に対する教育訓練に、利用の対象となる情報システムに関するリスクマネジメントおよび個人情報保護の内容が盛り込まれているかを確認します。）	[redacted]		●	4.4.6
	緊急事態対応	4- 1- 1- 29- 1	Q ユーザ部門の教育訓練に緊急事態対応を含んでいますか？ （業務上情報システムを利用する利用者に対する教育訓練に、利用の対象となる情報システムに関する緊急事態が発生した際の対応が盛り込まれているかを確認します。）			●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
情報システム総合企画	情報システム総合企画	4－2－(1) 情報システム総合企画					
1．実施基準	情報システム総合企画	4- 2- 1- 1	Q 実施基準に情報システム総合企画のリスク対策を定めていますか？ (実施基準に情報システム総合企画業務において、考慮すべきリスク対策が定められているかを確認します。)		●	●	(4.3.1)
2．ＩＴ戦略	経営戦略との整合	4- 2- 1- 2	Q 経営戦略とIT戦略の整合性(例:経営戦略での業務改革と、それを実現するシステム)がとられていますか？ (IT戦略を作成するプロセスで、経営戦略を参照することが明記され、IT戦略の内容が経営戦略策定者にフィードバックされているかを確認します。)		●		(4.3.3)
	標準ステップ	4- 2- 1- 3	Q IT戦略を作成するための標準化されたステップが存在しますか？ (IT戦略を策定する際の情報源、策定作業の内容／成果物が文書化されているかを確認します。)		●		
	外部規制	4- 2- 1- 4	Q 実施基準に法、ガイダンス、規程等の外部規制への対応が含まれていますか？ (実施基準に外部の公的な規定へのコンプライアンスを遵守することが明記されているかを確認します。)		●		
3．Ｔ計画	IT戦略とITインフラ計画	4- 2- 1- 5	Q IT戦略とITインフラストラクチャ計画の整合性がとられていますか？ (IT戦略で打ち出された施策を実現するために、適切なITインフラストラクチャの整備が計画されているかを確認します。)		●		
	ITインフラ計画	4- 2- 1- 6	Q ITインフラストラクチャ計画(例:新アプリケーションシステムに必要な技術)が文書としてまとめられていますか？ (ITインフラストラクチャとしてどの技術を導入し、現在使用しているどの技術を廃棄するかについて、文書化されているかを確認します。)		●		
	導入計画	4- 2- 1- 7	Q ITインフラストラクチャ計画に基づいて、導入計画が作成されていますか？ (特定のITインフラストラクチャを導入するプロジェクトが、ITインフラストラクチャ計画と整合性がとれているかを確認します。)		●		
4．組織体制・機能	指揮命令系統	4- 2- 1- 8	Q 情報システム組織として、適切な指揮命令系統が作られていますか？ (情報システム部門、利用部門、経営者、アウトソーサの間の役割分担が明確かつ適切に定義されているかを確認します。)		●	●	(4.4.1)
	インターナルコントロール機能	4- 2- 1- 9	Q 情報システム組織に、適切なインターナルコントロール機能が置かれていますか？ (情報システム組織に、適切な内部統制の仕組みを確保するための機能があるかを確認します。)		●	●	
	セキュリティ機能	4- 2- 1- 9- 1	Q 情報システム組織に、適切な情報セキュリティ機能が置かれていますか？ (情報システム組織に、セキュリティについて全体として見る役割が定義され、担当が明確になっているかを確認します。)		●	●	(4.4.4.2)
	品質管理機能	4- 2- 1- 9- 2	Q 情報システム組織に、適切な品質管理機能が置かれていますか？ (情報システム組織に、品質管理について全体として見る役割が定義され、担当が明確になっているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
情報システム総合企画	情報システム総合企画	4－2－(1) 情報システム総合企画					
4．組織体制・機能	決裁権限	4- 2- 1- 10	Q 決裁権限を明確に定めていますか？ (決済金額等により、適切なレベルの決裁権者を定めた決裁権限規定が文書化されているかを確認します。)		●	●	(4.3.1)
	リスク別担当部門	4- 2- 1- 11	Q リスクの種類に応じて、担当する部門が明確化されていますか？ (自然災害、不正アクセスといったリスクの種類に応じて、担当部門が明確になっているかを確認します。)		●	●	
5．スタッフ	人事計画	4- 2- 1- 12	Q IT戦略と整合のとれた人事計画が作成されていますか？ (IT戦略で必要とされるスキル・要員数を満たす採用・要員育成・アウトソーシング計画が作成されているかを確認します。)		●	●	
	スキル	4- 2- 1- 13	Q 将来必要となるスキルが識別され、人事計画や教育訓練計画に反映されていますか？ (IT戦略で必要とされるスキルが識別され、人事計画と教育訓練計画に反映されているかを確認します。)		●	●	(4.4.6)
	プロジェクト管理スキル	4- 2- 1- 14	Q スタッフのプロジェクト管理スキルは、十分ですか？ (開発プロジェクトに従事するスタッフが、PMBOK(Project Management Body Of Knowledge)等のプロジェクト管理スキルを身に付けているかを確認します。)		●	●	
	品質管理教育	4- 2- 1- 15	Q 品質管理の教育訓練が、適切に行われていますか？ (運用部門、開発部門を問わず、品質管理についての教育が適切に実施されているかを確認します。)		●	●	
6．財務	投資収益方針	4- 2- 1- 16	Q 投資収益に対する方針が文書化されていますか？ (開発プロジェクトの定量的な効果について、GO or NO GOの判断をする基準が文書化されているかを確認します。)		●	●	
	投資決定方法	4- 2- 1- 17	Q 投資決定に際して、利益実現の方法を明確にしていますか？ (IT投資が利用部門業務に貢献したり、情報システム部門のコスト削減を実現する方法が明確になっているかを確認します。)		●	●	
	短期的影響の想定	4- 2- 1- 17- 1	Q 投資決定に際して、短期的な影響を想定していますか？ (IT投資が行われた場合、定量的な効果を中心とする短期的な効果について想定しているかを確認します。)		●	●	
	長期的影響の想定	4- 2- 1- 17- 2	Q 投資決定に際して、長期的な影響を想定していますか？ (IT投資が行われた場合、定性的な効果を中心とする長期的な効果について想定しているかを確認します。)		●	●	
	他部門への影響の想定	4- 2- 1- 17- 3	Q 投資決定に際して、他部門への影響を想定していますか？ (IT投資が他部門に与えるプラス・マイナス両面の効果について想定しているかを確認します。)		●	●	
	ビジネス上の採算	4- 2- 1- 17- 4	Q 投資決定に際して、ビジネス上の採算を明確にしていますか？ (開発プロジェクトの効果算定手法が標準化され、プラス・マイナス両面の効果を考慮した採算が明確になっているかを確認します。)		●	●	
	予定利益	4- 2- 1- 18	Q 予定利益を実現するための経営的な管理が行われていますか？ (IT投資を計画した時の予定利益を実現するために、適切な事後評価と是正措置をとる仕組みが確立されているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
情報システム総合企画	情報システム総合企画	4－2－(1) 情報システム総合企画					
6. 財務	IT資産管理目録	4- 2- 1- 19	Q IT資産管理のためのインベントリ(目録)が作られていますか？ (パソコン等も含んだIT資産の全体を把握するためのインベントリが作成され、最新の状態になっているかを確認します。)		●	●	
	関連費用識別	4- 2- 1- 20	Q IT関連費用がすべて識別される仕組みがありますか？ (パソコン関連も含むすべてのIT関連費用について、識別する仕組みがあるかを確認します。)		●	●	
7. 管理（文書化を含む）	全社データ管理	4- 2- 1- 21	Q 全社的なデータ管理の機能が確立されていますか？ (全社のデータ項目について、集中的に管理する機能が作られ、担当部門が明確になっているかを確認します。)		●	●	
	全社データ標準化	4- 2- 1- 22	Q 全社的なデータの標準化が行われていますか？ (社内の各部門で横断的にデータ項目の標準化が行われているかを確認します。)		●	●	(4.3.1)
	全社データ所有者の識別	4- 2- 1- 23	Q データの所有者が識別されていますか？ (各データ項目について、その内容に責任を持つ利用部門が明確になっているかを確認します。)		●	●	
	管理工程分割	4- 2- 1- 24	Q プロジェクト計画は、成果をチェックできるまでブレークダウンした工程分割がされていますか？ (実際のプロジェクト計画が、組織のシステム開発方法論に基づいて適切な工程分割が行われているかを確認します。)		●	●	
	工程ごとの品質基準	4- 2- 1- 25	Q 品質管理基準は分割された工程ごとに定めていますか？ (組織のシステム開発方法論の工程ごとに、どのようなポイントについて品質管理を行うかが明確になっているかを確認します。)		●	●	
	ライセンス管理	4- 2- 1- 26	Q ライセンス管理を行っていますか？ (パソコンのソフトウェアについて、契約文書まで追跡可能なライセンス管理を行っているかを確認します。)		●	●	
	プロジェクト管理標準	4- 2- 1- 27	Q プロジェクト管理基準が文書化されていますか？ (プロジェクト管理として工程ごとに実施する内容、関係者の役割分担、承認権限、手法、標準値、ツールが文書化されているかを確認します。)		●	●	
	方法論	4- 2- 1- 27- 1	Q 社内で基準となるシステム開発方法論が文書化されていますか？ (開発プロジェクトの工程分割、作業内容、手法、成果物、関係者の役割分担、ツールを定義したシステム開発方法論が文書化されているかを確認します。)		●	●	
8. モニタリング	規制監視	4- 2- 1- 28	Q 法、ガイダンス、規程類等の外部規制を遵守しているかを監視する機能が存在しますか？ (社内システムの変更や外部規制の変更に伴い、外部規制を遵守しているかを監視する役割が明確にされ、担当組織が定義されているかを確認します。)		●	●	(4.3.2)
	是正措置	4- 2- 1- 29	Q 必要な是正措置の実施状況が管理されていますか？ (是正措置についてもその実施状況がプロジェクト管理の対象となっているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム開発	システム開発	4－2－(2) システム開発					
1．実施基準	システム開発	4- 2- 2- 1	Q 実施基準にシステム開発のリスク対策を定めていますか？ (システム開発業務において、考慮すべきリスク対策が定められているかを確認します。)		●	●	
	決裁実施基準	4- 2- 2- 1- 1	Q 開発プロジェクトにおける決裁権限者、決裁文書等の決裁実施基準が定められていますか？ (開発プロジェクトの各工程において、決裁すべき文書と決裁権限者が文書化されているかを確認します。)		●	●	
	開発に応じた決裁	4- 2- 2- 1- 2	Q 決裁実施基準は、プロジェクトの規模に応じて定めていますか？ (決裁権限者はすべてのプロジェクトで一律ではなく、プロジェクト規模によって適切な決裁権限者を定めているかを確認します。)		●	●	
	システム調達のライフサイクルにおけるセキュリティ	4- 2- 2- 2	Q システム調達のライフサイクルにおけるプロセスごとの処理実施基準が定められていますか？ (システムの企画、開発、導入、廃棄のライフサイクルについて、各プロセスでの実施基準が明確になっているかを確認します。)		●	●	
	調達	4- 2- 2- 2- 1	Q 情報システムの調達において、情報セキュリティ要件を満たすための明確な実施基準を設けていますか？ (外部よりパッケージを購入する場合や、SIベンダを選定する時に満足すべきセキュリティ要件が実施基準に含まれているかを確認します。)		●	●	
	不正防止・機密保護基準	4- 2- 2- 2- 2	Q 情報システムの開発／変更に関して、不正防止や機密保護の観点から明確な実施基準を設けていますか？ (情報システムの開発／変更作業において守るべき項目が明確になっているかを確認します。)		●	●	
	破棄基準	4- 2- 2- 2- 3	Q 情報システムの破棄に関して、不正防止や機密保護の観点から明確な実施基準を設けていますか？ (パソコンや記録媒体等の破棄に際して、内蔵データの完全消去等の基準が明確になっているかを確認します。)		●	●	
	品質管理	4- 2- 2- 3	Q 品質管理に関して標準的な手法を定めていますか？ (情報システムの品質管理について、社内標準が明確になっているかを確認します。)		●	●	
	要員	4- 2- 2- 4	Q 開発要員の管理の観点から明確な実施基準を設けていますか？ (開発作業とそれを実施する要員について、セキュリティを確保するための基準が明確になっているかを確認します。)		●		
	職務定義	4- 2- 2- 4- 1	Q 各職務に求められる資質や職能を明確に定義していますか？ (各職務を実行する要員について、必要とする資格、スキル、経験が明確になっているかを確認します。)		●		
	職務分離	4- 2- 2- 4- 2	Q 開発作業における職務分離－開発者・プログラマ・テストスタッフーを実施していますか？ (開発作業で、開発者・プログラマ・テストスタッフに別の要員をアサインしているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム開発	システム開発	4－2－(2) システム開発					
1．実施基準	情報セキュリティ保持の役割・責任	4－ 2－ 2－ 4－ 3	Q 各職務において情報セキュリティに関する役割や責任を明確にしていますか？ (各職務別に、たとえばセキュリティに関するプログラミングルールの遵守といった、情報セキュリティに関しての役割と責任を明確にしているかを確認します。)		●		
	機密保持合意	4－ 2－ 2－ 4－ 4	Q 開発スタッフとの契約において機密保持に関する条項が盛り込まれていますか？ (開発要員に対して、機密保持誓約書の提出等を行っているかを確認します。)		●		
2．プロジェクト管理	システム開発方法論	4－ 2－ 2－ 5	Q システム開発プロジェクトにおいて標準的なシステム開発方法論を定めていますか？ (開発プロジェクトの工程分割、作業内容、手法、成果物、関係者の役割分担、ツールを定義したシステム開発方法論が文書化されているかを確認します。)		●		
	作業内容と成果物	4－ 2－ 2－ 5－ 1	Q プロジェクト開発の各工程について、その作業内容と成果物を定めていますか？ (プロジェクトの各工程別に、実施する作業の内容と参照する情報、作成する成果物について明確になっているかを確認します。)		●		
	技法／ツール	4－ 2－ 2－ 5－ 2	Q 各工程の開発作業に関して標準的な技法／ツールを定めていますか？ (各工程で行う作業について、データ分析などの使用技法や技法支援ツールが明確になっているかを確認します。)		●		
	判定基準	4－ 2－ 2－ 5－ 3	Q 各工程が完了したかの判定基準を定めていますか？ (各工程について、完了と判断し、次工程に進むための基準が明確になっているかを確認します。)		●		
	進捗管理手続	4－ 2－ 2－ 6	Q 進捗管理に関して標準的な手続を定めていますか？ (各プロジェクトについて、その進捗をどの組織に、いつ報告するかが定められているかを確認します。)		●		
3．システム要件定義	セキュリティ基準の遵守	4－ 2－ 2－ 7	Q システム要件定義で、セキュリティに関する実施基準を遵守していますか？ (セキュリティに関するシステム要件定義ビュー等によって、セキュリティの実施基準に含まれる条項をシステム要件定義に反映させているかを確認します。)		●	●	
	要件の反映	4－ 2－ 2－ 7－ 1	Q 情報セキュリティポリシー／実施基準等で定められた要件を反映させていますか？ (パスワードの要件といったセキュリティの実施基準で定められた項目などが、システム要件定義に含まれているかを確認します。)		●	●	
	SLA合意	4－ 2－ 2－ 7－ 2	Q 管理指標に関して、SLAとして関係者の合意が取れていますか？ (システムの可用性の目標値等の管理指標が、SLAに含まれているかを確認します。)		●	●	
	システム要件の反映	4－ 2－ 2－ 7－ 3	Q 個人認証、暗号化等のシステム要件がシステム機能に反映されていますか？ (セキュリティポリシーや実施基準で個人認証手続や暗号の利用が定められている場合、それがシステム機能に適切に反映されているかを確認します。)		●	●	
	システム構成要素の入手可能性	4－ 2－ 2－ 8	Q 情報システムの開発にあたって、システム構成要素(補修部品、消耗品)の入手可能性に関して検討を行いましたか？ (システムライフとシステム構成要素の保持期限切れについて、検討しているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム開発	システム開発	4－2－(2) システム開発					
4. プログラム開発	開発環境	4- 2- 2- 9	Q 開発環境の維持、管理を適切に実施していますか？		●		
	機密保持のクラス分け	4- 2- 2- 9- 1	Q システムとデータについて、機密保持のクラス分けがなされていますか？ (厳秘、秘密、取扱注意といった機密保持のクラス分けを行っているかを確認します。)		●		
	プログラムライブラリへのアクセス管理	4- 2- 2- 9- 2	Q プログラムライブラリへのアクセス管理は適切に行われていますか？ (プログラムライブラリへのアクセスは、各要員が業務的に必要とする範囲に限定されているかを確認します。)		●		
	高機密プログラムの保管	4- 2- 2- 9- 3	Q 機密性の高いプログラムの保管に関して、適切な機密保護の対策を実施していますか？ (機密度の高いプログラムに関して、通常のプログラムと異なった特別の対策を実施しているかを確認します。)		●		
	設計文書保管	4- 2- 2- 9- 4	Q 設計文書の保管に関して、適切な機密保護の対策を実施していますか？ (設計文書等の保管についても、ソフトウェアと同様のアクセス管理が実施されているかを確認します。)		●		
	不正ソフトの混入対策	4- 2- 2- 9- 5	Q ウイルス等不正なソフトウェアの混入への対策を実施していますか？ (プログラムの製作過程で、不正なソフトウェアが混入しないために、隔離した環境にしたり、ワクチンソフトを使用しているかを確認します。)		●		
	コンプライアンス	4- 2- 2- 10	Q システム開発にあたって、関連する法規、契約等に関わる要求事項を確認していますか？ (開発されたシステムを使用するユーザ業務に関連する法規、外部規制を確認します。)		●	●	(4.4.8)
	知的財産権放棄・契約の要求事項	4- 2- 2- 10- 1	Q 知的財産権に係わる法規、契約に関わる要求事項を確認していますか？ (開発過程で産み出される知的財産の保護と、外部の知的財産の侵害防止、第三者との契約に基づく知的財産の保護について確認します。)		●	●	
	個人情報保護	4- 2- 2- 10- 2	Q 個人情報保護に係わる法規、契約等に関わる要求事項を確認していますか？ (個人情報保護法などの関連法規や情報提供主体との契約の内容と、その要求事項を確認します。)		●	●	4.2
	暗号輸出入管理	4- 2- 2- 10- 3	Q 暗号等の使用に関して、輸出入管理等関連する法規等に係わる要求事項を確認していますか？ (暗号の特定国家への輸出禁止といった、輸出入管理等関連する法規等について、その要求内容を確認します。)		●		
	各国法規遵守	4- 2- 2- 10- 4	Q 国際的な情報システムを構築する場合、各国の規制(例:ECの個人情報保護規定)に遵守すべく必要な措置を講じていますか？ (開発するシステムが国際的に使用される場合、使用される国での規制を守るために必要な措置を講じているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム開発	システム開発	4－2－(2) システム開発					
5. テストデータ	テストデータ	4- 2- 2- 11	Q テストデータの作成、保管を適切に実施していますか？ (テストデータに本番データを流用することは運用性テスト等ではよく見られる状況ですが、このデータのセキュリティを確保する手段が講じられているかを確認します。)		●	●	
	テストの機密保持規定	4- 2- 2- 11- 1	Q 本番データをテストに使用する場合の機密保持規定が明確になっていますか？ (本番データをテストに使用することの承認と、その後の機密保持規定が明確になっているかを確認します。)		●	●	
	保護データの排除	4- 2- 2- 11- 2	Q テストデータには、原則として保護すべきデータを含まないようにしていますか？ (テストデータには、個人情報の本番データといった保護すべきデータを含むことを禁止しているかを確認します。)		●		4.4.2.4
	本番データ使用時の保護対策	4- 2- 2- 11- 3	Q テストデータとして本番データを使用する場合には、適切な保護対策を実施していますか？ (テスト用に本番データを使用する場合は、暗号化等の保護対策が実施されているかを確認します。)		●		
	本番データとの分離	4- 2- 2- 11- 4	Q テストデータは、本番データと分離して保管していますか？ (テストデータと本番データの媒体を物理的に分けるといった、明確に分離した保管が行われているかを確認します。)		●		
6. 運用テスト	テスト仕様書の内容	4- 2- 2- 12	Q テスト仕様書はテストの目的に照らして適切ですか？ (テスト仕様書の内容がテストの目的に照らして適切かを判断する必要があります。)		●	●	
	運用テストの結果	4- 2- 2- 13	Q 運用テストの結果を十分確認していますか？		●	●	
	導入の妥当性	4- 2- 2- 13- 1	Q 導入の妥当性を十分確認していますか？ (運用テスト結果が、障害の発生度、機能の充足度について、本番使用に耐えるレベルに達しているかを確認します。)		●		
	システム性能	4- 2- 2- 13- 2	Q システムの性能を十分把握していますか？ (負荷テストの結果を分析し、要求性能を満たしているか、各部分の利用率はどの程度かを把握する必要があります。)		●		
	操作性確認	4- 2- 2- 13- 3	Q システム運用上の操作性について確認していますか？ (システムの操作性について利用部門が運用テストの中で確認します。)		●		
	異常時バックアップ対応	4- 2- 2- 13- 4	Q システム導入後の異常時のバックアップについて対応は十分ですか？ (システム稼働後のデータ量で、バックアップが十分な頻度で取られているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム開発	システム開発	4－2－(2) システム開発					
7．変更管理	管理責任者	4－ 2－ 2－ 14	Q プログラムライブラリの管理責任者が明確になっていますか？ (プログラムライブラリの内容として、正式に承認されたもの以外が入らないようにするため、管理責任者が明確になっているかを確認します。)		●		
	バージョンアップ手続	4－ 2－ 2－ 15	Q 本番プログラムへのバージョンアップの実施基準が明確になっていますか？ (本番プログラムについて、その一貫性を確保するための基準が明確になっているかを確認します。)		●		
	管理方針	4－ 2－ 2－ 15－ 1	Q 本番プログラムへのバージョンアップについて、全体的な管理方針が明確になっていますか？ (本番プログラムへのバージョンアップを行う時は、どのようなテストを実施し、誰が承認するかが明確になっているかを確認します。)		●		
	非常時の実施基準	4－ 2－ 2－ 15－ 2	Q 本番プログラムへのバージョンアップについて、非常時の実施基準が明確になっていますか？ (ソフトウェア障害が発生した場合の緊急復旧の手段として、プログラムのバージョンアップを実施する場合の手続が明確になっているかを確認します。)		●		
	バックアップ・他所保管の実施基準	4－ 2－ 2－ 15－ 3	Q バックアップや他所保管の実施基準が明確になっていますか？ (本番プログラムのバックアップ取得頻度や範囲、バックアップ媒体の遠隔地保管について、基準が明確になっているかを確認します。)		●		
	区分によるバージョンアップ	4－ 2－ 2－ 16	Q システムの機密保持の区分によって、特別のバージョンアップ手続が定められていますか？ (機密度の非常に高いシステムについて、独立したコードレビューを実施するといった、特別のバージョンアップ手続が定められているかを確認します。)		●		
	変更管理	4－ 2－ 2－ 17	Q プログラムライブラリの変更は記録されていますか？ (プログラムライブラリに対する変更が自動的に記録される仕組みを使っているかを確認します。)		●		
	識別のための体系	4－ 2－ 2－ 18	Q プログラムの重要度を識別するための体系を確立していますか？ (プログラムの障害がユーザ業務に与える影響を識別し、各プログラムごとに明確にしているかを確認します。)		●		
	ネーミングルール	4－ 2－ 2－ 18－ 1	Q プログラムのネーミングルールを確立していますか？ (プログラムの名前づけに関する標準が明確になっているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム開発	システム開発	4－2－(2) システム開発					
7. 変更管理	高機密プログラム保管	4- 2- 2- 19	Q 機密性の高いプログラムの変更内容は、管理責任者によって事前に承認を受けた上で実施されていますか？ (機密性の高いプログラムの変更については、その内容について管理責任者が特別の対応を行うことになっているかを確認します。)		●		
	レビュー検証	4- 2- 2- 19- 1	Q 機密性の高いプログラムの変更は、本番前および本番後で独立したレビューによって検証されていますか？ (変更作業を行ったチームとは別のチームがレビューを実施しているかを確認します。)		●		
	レビュー内容の文書化	4- 2- 2- 19- 2	Q 機密性の高いプログラム変更について、本番前および本番後のレビュー内容を文書化していますか？ (機密性の高いプログラムの変更について、行ったレビュー結果が文書として保存されているかを確認します。)		●		
	管理責任者の承認	4- 2- 2- 19- 3	Q 機密性の高いプログラム変更は管理責任者によって承認されていますか？ (機密性の高いプログラムの変更要求は、システムオーナーと情報システム部門責任者の承認を得るようになっているかを確認します。)		●		
	作業とレビューの分離	4- 2- 2- 20	Q 機密性の高いプログラムを開発する場合、開発作業とレビューの職務の分離(例：設計、プログラミング、テスト)が行われていますか？ (機密性の高いプログラムを新規に開発する時は、開発と独立したレビューチームがレビューを行っているかを確認します。)		●		
	アクセスの職務分離	4- 2- 2- 21	Q プログラムの開発／変更を行うプログラマが本番バージョンのライブラリに対するアクセスが認められないように、職務の分離が行われていますか？ (本番ライブラリが、運用部門の管理下に置かれ、開発部門からはアクセスできないようになっているかを確認します。)		●		
	配布先でのバージョン管理	4- 2- 2- 22	Q クライアントPCにソフトウェアを配布している場合、適切なバージョン管理の手続が定められていますか？ (クライアントのパソコンのソフトウェアが適切なバージョンになっているかを管理し、自動的な配布を行う手続があるかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム運用	システム運用	4－2－(3) システム運用 (基本的な流れとして、運用の基準やマニュアルがあり、各レベルの計画が作成され、それに従って運用されているかのチェックと、問題管理が行われることが対策である。)					
1. 実施基準	システム運用	4- 2- 3- 1	Q 実施基準にシステム運用のリスク対策を定めていますか？ (システム運用業務において考慮すべきリスク対策が定められているかを確認します。)		●		
	システム運用計画	4- 2- 3- 1- 1	Q システム運用計画策定に関する実施基準は、SLAに基づき明確に示されていますか？ (SLAで定められたサービスレベルが実施基準に適切に反映されているかを確認します。)		●		
2. システム運用	システム運用実施	4- 2- 3- 2	Q システムの運用はシステム運用計画どおりに行われていますか？ (システム運用計画と運用実績に乖離がないかをチェックします。個人情報の運用は利用時間を制限することが望まれています。)		●	●	(4.4.1)
	定期的見直し	4- 2- 3- 2- 1	Q システム運用計画は定期的に見直されていますか？ (新システムの追加や利用状況の変化に応じたシステム運用計画の変更が実施されているかを確認します。)		●		
	システム運用管理	4- 2- 3- 3	Q システム運用管理が適切か、定期的に確認していますか？		●	●	
	運用マニュアル	4- 2- 3- 3- 1	Q 運用マニュアルは常に最新の状態で維持されていますか？ (運用マニュアルの内容が、システム運用計画の変更やシステム構成の変化を反映しているかを確認します。)		●	●	
	スケジュール運用確認	4- 2- 3- 3- 2	Q 更新された運用マニュアルに従ってシステム運用が行われていることを確認していますか？ (更新されたマニュアルが、実際の運用で使われていることを確認します。)		●	●	
	運用手順	4- 2- 3- 3- 3	Q 運用手順は常に適切か、確認していますか？ (運用手順が要員のスキル、適用技術、障害原因からみて適切か、見直します。)		●		
	データの適切性	4- 2- 3- 3- 4	Q システム運用時の各種データは常に適切か、確認していますか？ (適切なデータが使われるように、ファイル名称やボリューム番号を使用し、運用管理部門がそれらを指定しているかを確認します。)		●	●	
	スキルの妥当性	4- 2- 3- 3- 5	Q システム運用に関するスタッフのスキルの妥当性について定期的に確認していますか？ (システム運用要員のスキルについて、現状の把握と育成計画が立てられているかを確認します。)		●		
3. モニタリング機能	記録・状況把握	4- 2- 3- 4	Q システム運用関連の記録・監視は適切に行われていますか？ (システム運用のログ取得を自動化し、その分析を定期的に行っているかを確認します。)		●	●	
	記録・監視	4- 2- 3- 4- 1	Q システムの資源の記録・監視は適切に行われていますか？ (CPU、メモリ、ストレージといったシステム資源について、その利用率を管理しているかを確認します。)		●		
	報告体制	4- 2- 3- 4- 2	Q システム運用の結果(実績)に関する報告(正常終了、異常終了など)の体制は適切ですか？ (運用指示書の作業項目に対してチェックを行い、異常時に必ず報告する体制がとられているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム運用	システム運用	4－2－(3) システム運用 (基本的な流れとして、運用の基準やマニュアルがあり、各レベルの計画が作成され、それに従って運用されているかのチェックと、問題管理が行われることが対策である。)					
3．モニタリング機能	障害監視	4－ 2－ 3－ 5	Q システム運用に関する障害監視を実施していますか？ (システム運用では、障害の発生が多大な影響を及ぼすため、どのような障害が起きているかを確認する必要があります。)		●		
	オンライン監視	4－ 2－ 3－ 5－ 1	Q システム運用に関するオンライン監視を実施していますか？ (システムの障害をオンラインで監視する必要があります。)		●		
	サーバの監視	4－ 2－ 3－ 5－ 2	Q サーバの監視を実施していますか？ (サーバの障害はシステム運用上、きわめて重要な影響を及ぼします。したがってオンライン監視が必須です。)		●		
	クライアントPCの監視	4－ 2－ 3－ 5－ 3	Q クライアントPCの監視を実施していますか？ (クライアントのパソコンの障害をオンラインで監視することが大事です。)		●		
	ネットワークの監視	4－ 2－ 3－ 5－ 4	Q ネットワーク系のオンライン監視を実施していますか？ (ネットワーク障害の検出、トラフィック等をオンラインで監視することが大事です。)		●		
4．管理機能	ファイル世代管理	4－ 2－ 3－ 6	Q ファイルの世代管理は適切に行われていますか？ (マスタファイルにトランザクションによる更新を加えていく場合、適切な世代のデータが識別され、バックアップとして必要な世代が確保されているかを確認します。)		●	●	
	ライブラリ管理	4－ 2－ 3－ 6－ 1	Q ライブラリ管理は適切に行われているか、定期的に確認していますか？ (プログラムライブラリの変更が承認された手続に従っているかを確認します。)		●		
	障害管理	4－ 2－ 3－ 6－ 2	Q 世代管理されているファイルの障害報告書に対して、原因分析、解決策をフォローしていますか？ (世代管理されているファイルの障害報告書について、根本原因の分析を行い、その原因が除去されたことを確認します。)		●		
	適用業務管理方針	4－ 2－ 3－ 6－ 3	Q 適用業務管理(たとえば入出力データの完全性)に対するリスク対策が適切に行われていることを定期的に確認していますか？ (入力時の誤謬摘示等のリスク対策がとられていることを確認します。)		●	●	
5．復旧時間	SLA	4－ 2－ 3－ 7	Q SLAで示された各アプリケーションシステム障害回復までの時間を考慮した対策を行っていますか？ (システムの冗長構成といった障害対策が、SLAで示された障害復旧時間を満足できるようになっているかを確認します(例:バックアップデータのリストア時間))。		●	●	

	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
アウトソーシング	アウトソーシング	Ⅳ－2－(4)アウトソーシング (ここでのアウトソーシングは、システム開発やデータセンタや分散環境の運用を外部に委託することをいう。アウトソーシング契約には、契約本文と作業内容を定める附属文書等を含む。)					
1．実施基準	アウトソーシング	4－ 2－ 4－ 1	Q 実施基準にアウトソーシング関連のリスク対策を定めていますか？ (システム開発・運用業務をアウトソーシングしている場合、考慮すべきリスク対策が定められているかを確認します。)		●	●	4.4.4.3
2．目的	TCC	4－ 2－ 4－ 2	Q アウトソーシングについて、TCOを認識したマネジメントコントロールが確立されていますか？ (アウトソーシング関連業務のコスト把握を行う仕組みを確立しているかを確認します。)		●	●	
	コスト削減	4－ 2－ 4－ 3	Q 情報システムに関わるコストの削減がアウトソーシングの目的となっていますか？ (アウトソーシングの目的にコスト削減が含まれている場合、実施前と実施後のコスト削減の目標が明確になっているかを確認します。)		●	●	
	スリム化	4－ 2－ 4－ 4	Q システム部門のスリム化がアウトソーシングの目的となっていますか？ (アウトソーシングの目的にシステム部門のスリム化が含まれている場合、どの業務をアウトソーシングするかの方針が明確になっているかを確認します。)		●	●	
	関連技術の安価利用	4－ 2－ 4－ 5	Q 関連技術の安価な利用がアウトソーシングの目的となっていますか？ (アウトソーシングの目的に関連技術の安価な利用が含まれている場合、対象となる技術は、社外ですでに実用化されている技術から適切に選択され、内容が明確になっているかを確認します。)		●	●	
	コスト削減	4－ 2－ 4－ 6	Q コスト削減に通じる技術の専門化、高度化がアウトソーシングの目的となっていますか？ (アウトソーシングの目的に新しい技術を導入することが含まれている場合、その技術導入の目的がビジネス上のメリットと明確に結び付けられているかを確認します。)		●	●	
3．役割分担	責任分担	4－ 2－ 4－ 7	Q アウトソーシング契約で、委託者と受託者の責任分担は明確になっていますか？ (アウトソーシング契約に両者の責任分担を明確にする仕組みが含まれているかを確認します。)		●	●	4.4.4.3
	受託者内の責任範囲	4－ 2－ 4－ 8	Q アウトソーシングの場合、受託者内の責任範囲は明確になっていますか？ (受託者内の責任範囲が不明瞭な場合、現場に混乱を与えかねないので、責任範囲を明確にする必要があります。)		●	●	4.4.4.3
	受託者の役割分担	4－ 2－ 4－ 9	Q 受託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？ (受託者が行う作業について、両者の合意した文書(仕様書等)で詳細に文書化されているかを確認します。)		●	●	4.4.4.3
	委託者の役割分担	4－ 2－ 4－ 10	Q 委託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？ (委託者が行う作業について、両者の合意した文書(仕様書)で詳細に文書化されているかを確認します。)		●	●	4.4.4.3

	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
アウトソーシング	アウトソーシング	Ⅳ－2－(4)アウトソーシング (ここでのアウトソーシングは、システム開発やデータセンタや分散環境の運用を外部に委託することをいう。アウトソーシング契約には、契約本文と作業内容を定める附属文書等を含む。)					
4．プロジェクト管理	共通開発方法論	4- 2- 4- 11	Q 開発方法論について、両者で共通のものを用いていますか？ (システム開発方法論について、両者で共通のものを作成し、文書化しているかを確認します。)		●	●	
	プロジェクト管理手法	4- 2- 4- 12	Q アウトソーシングした場合のプロジェクト管理手法が明確になっていますか？ (共通のシステム開発方法論に基づいて、合意したプロジェクト管理手法が文書化されているかを確認します。)		●	●	
	外注委託のレビュー	4- 2- 4- 13	Q 委託業務の実施内容をレビューしていますか？ (委託先の慣熟度合い等を考慮して、定期的にアウトソーシングの実施範囲を見直しているかを確認します。)		●	●	
	合意形成	4- 2- 4- 14	Q アウトソーシング契約に両者で交わす文書や会議について定められていますか？ (アウトソーシング契約で、両者間のコミュニケーションについて合意形成する仕組みが含まれているかを確認します。)		●	●	
5．アウトソーサ管理	選定評価基準	4- 2- 4- 15	Q アウトソーサの選定手続と評価基準が社内で定められていますか？ (アウトソーサの選定について、社内での標準となる手続と評価項目が定められているかを確認します。)		●	●	4.4.4.3
	SLA	4- 2- 4- 16	Q アウトソーシング契約に、SLA(サービスレベル合意)を含んでいますか？ (アウトソーシング契約に、SLAを作成することが含まれているかを確認します。)		●	●	
	ペナルティ	4- 2- 4- 17	Q SLAが守れなかった場合のペナルティが定められていますか？ (SLAに守れなかった場合のペナルティが含まれているかを確認します。)		●	●	
	事件・事故報告・連絡体制	4- 2- 4- 18	Q アウトソーシング契約にセキュリティ事件・事故が発生した場合の報告・連絡体制が定められていますか？		●	●	4.4.4.3
	ソフトウェア障害時対応	4- 2- 4- 19	Q ソフトウェア障害時の対応(体制、手続)が定められていますか？ (ソフトウェア開発のアウトソーシング契約に、ソフトウェア障害発生時の対応について含まれているかを確認します。)		●	●	
	品質管理	4- 2- 4- 20	Q 委託作業の品質管理について、体制や手続が定められていますか？ (作業品質の管理について、受託側／委託側で行う作業内容と担当が定められているかを確認します。)		●	●	
6．契約	委託契約ルール	4- 2- 4- 21	Q 社内規程には委託契約のルールが定められていますか？		●	●	4.4.4.3
	賠償上限	4- 2- 4- 22	Q アウトソーシング契約で、賠償責任の上限が定められていますか？ (受託側に過失があり、賠償責任が生じる条件と賠償の上限が明記されているかを確認します。)		●	●	4.4.4.3
	安全管理	4- 2- 4- 23	Q 委託契約には個人情報の安全管理に関する事項を明確に規定していますか？		●	●	4.4.4.3

	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
アウトソーシング	アウトソーシング	Ⅳ－2－(4)アウトソーシング (ここでのアウトソーシングは、システム開発やデータセンタや分散環境の運用を外部に委託することをいう。アウトソーシング契約には、契約本文と作業内容を定める附属文書等を含む。)					
6. 契約	開発納期延期	4- 2- 4- 24	Q 委託契約で、開発納期が遅延した場合のペナルティが定められていますか？ (開発アウトソーシングの契約で、納期が遅延した場合のペナルティについて定めているかを確認します。)		●	●	
	従事者の監督	4- 2- 4- 25	Q 委託契約で従事者の監督について明確に定められていますか？		●	●	4.4.4.3
	契約のチェック	4- 2- 4- 26	Q 委託契約が定められた委託契約ルールに基づいて締結していることをチェックしていますか？ (契約の管理部門が、個々の委託契約について、委託契約に対する方針との整合性をチェックしているかを確認します。)		●	●	4.4.4.3
	受託先監査	4- 2- 4- 27	Q 契約で受託者側に対する監査を行うことが可能となっていますか？ (委託者側が指定する第三者が、受託者に対する監査を実施できることが契約に含まれているかを確認します。)		●	●	4.4.4.3
	変更手続	4- 2- 4- 28	Q 契約内容の変更手続(作業、契約、システム)が定められていますか？ (契約に、契約内容の変更に関する定めがあり、変更の程度と関連手続が定められているかを確認します。)		●	●	4.4.4.3
7. 知的財産権	知的財産権	4- 2- 4- 29	Q 委託契約で、委託先と受託者の間で知的財産権を明確にしていますか？ (委託した作業の中で創り出された知的財産権について、契約で取扱いを明記しているかを確認します。)		●	●	
	再委託における知的財産権	4- 2- 4- 30	Q 再委託条項がある場合、受託者にとって委託者と同様に知的財産権が守られるようになっていますか？ (元請契約を受託した企業が他の企業に再委託する場合の知的財産権について、リスクの視点からみて契約で明確にする必要があります。)		●	●	
	知的財産権侵害の責任分担	4- 2- 4- 31	Q 第三者による知的財産権の侵害があった時の責任分担が事前の取決めによって明確になっていますか？ (第三者により知的財産権を侵害された時は、知的財産権の所有者が対応するのが原則となります。)		●	●	
8. セキュリティ上の留意点	委託先情報セキュリティ遵守	4- 2- 4- 32	Q 受託者に情報セキュリティポリシーがない場合、受託者が委託先の情報セキュリティポリシーや実施基準を遵守することに合意していますか？		●	●	4.4.4.3
	委託先情報セキュリティ実施状況	4- 2- 4- 33	Q 委託先における不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じていますか？ (受託側が行っている不正防止対策や機密保護対策の実施状況について、定期的に報告を受け、監査を実施し、必要な是正措置を実施しているかを確認します。)		●	●	4.4.4.3
	委託先情報セキュリティのマネジメント	4- 2- 4- 34	Q 委託先における情報セキュリティのマネジメント体制ができていますか？ (委託先においても情報セキュリティマネジメントは重要です。この中には機密保護対策、不正防止対策等が含まれます。)		●	●	4.4.4.3

	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
アウトソーシング	アウトソーシング	Ⅳ－2－(4)アウトソーシング (ここでのアウトソーシングは、システム開発やデータセンタや分散環境の運用を外部に委託することをいう。アウトソーシング契約には、契約本文と作業内容を定める附属文書等を含む。)					
8. セキュリティ上の留意点	秘密保持	4- 2- 4- 35	Q 受託者の守秘義務と秘密保持の義務が明確になっていますか？ (受託者の負う守秘義務の対象・内容と、とるべき秘密保持手段が明確になっている必要があります。) (用語解説「守秘義務と秘密保持の義務」:委託者・受託者以外の第三者に対しての情報管理義務をいいます。)	[redacted]	●	●	4.4.4.3
	再委託時の秘密保持	4- 2- 4- 36	Q アウトソーシング契約で再委託を許す場合は、委託者と同様の守秘義務と秘密保持手段が含まれるようになっていますか？ (再委託を認める場合、委託先と再委託先の契約がアウトソーシング契約に定められた守秘義務と秘密保持手段を継承しているかを確認します。)	[redacted]	●	●	4.4.4.3

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム監査	システム監査	4－2－(5) システム監査(情報セキュリティ監査を含む)					
1. 実施基準	システム監査	4- 2- 5- 1	Q 実施基準にシステム監査を定めていますか？ (リスク対策は日常業務の忙しさに埋もれて後回しになったり、所定のルールを省略したりしがちです。その歯止め策として第三者の監査が不可欠です。リスク対策の施策を定める実施基準に、明確にシステム監査を行うことを記述する必要があります。)		●	●	4.5
2. 監査	重要性の認識	4- 2- 5- 2	Q リスク対応におけるシステム監査の重要性を認識していますか？ (リスク対策はルールの逸脱や対策実施の遅れなど、定めてあるものが実施されないと効果が上がりません。そのため第三者の監査が不可欠です。ここでは監査を受ける側にとっては心理的にも負担がかかるものです。重要性を認識しているとは監査を必ず実施している状況であること、監査結果について必ず改善策を作成し、それが年間計画に優先的に反映されていることをいいます。)		●	●	4.5
	システム監査の実施	4- 2- 5- 2- 1	Q システム監査を定期的に実施していますか？ (内部監査および外部監査双方においてあらかじめ定めた間隔で監査を行うことが必要です。経営の都合などで延期したりしてはいけません。なお、追加で監査を実施することは構いません。)		●	●	(4.5)
	内部監査	4- 2- 5- 2- 2	Q 内部監査によるシステム監査を実施していますか？ (内部監査は当事者以外の第三者であれば専任部門の要員でなくても監査を行うことができます。中小の組織において専門要員を確保できない場合でも監査を行うことが必要です。)		●	●	(4.5)
	外部監査	4- 2- 5- 2- 3	Q 外部監査によるシステム監査を実施していますか？ (定期的に外部の専門家によるシステム監査を行うことが望まれます。金融検査マニュアルでは3年に一度以上の外部監査を要求しています。一般企業においても自ら定めた間隔で実施することが望まれます。)		●	●	(4.5)
	監査人の選任	4- 2- 5- 2- 4	Q システム監査人を選任していますか？ (監査は独立した第三者であれば実施が可能です。しかし、できれば専門的なシステム監査ができる要員を選任することが必要です。システム監査人は社外の者であっても構いません。)		●		
	リスクマネジメント責任者と監査人の位置づけ	4- 2- 5- 2- 5	Q リスクマネジメント責任者とシステム監査人の位置づけは明確ですか？ (リスクマネジメント全体の推進責任者は役員です。システム監査人は社内であっても公正さを確保し、適切な意見を述べることができるよう、その地位が保全されていなければなりません。)		●	●	
	報告先	4- 2- 5- 3	Q システム監査の結果は、適切なレベルの経営者に報告されていますか？ (システム監査の目的は経営の健全性に役立つ提言を行うことです。したがって現状の報告や問題点などの苦言などが経営者に対して報告されなければ意味がありません。部門の圧力により報告されないことがあってはいけません。)		●	●	(4.5)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策					
システム監査	システム監査	4－2－(5) システム監査(情報セキュリティ監査を含む)					
2. 監査	勧告のフォロー	4- 2- 5- 4	Q システム監査の勧告をフォローする体制が作られていますか？ (システム監査の結果は経営の改善に寄与するために行われますが、場合によっては改善には負荷がかかることがあります。その勧告を経営者が真摯に受け止めず無視することがあってはなりません。そのため、勧告内容の把握とその改善策が実際に実施されているかをフォローする体制がなければなりません。具体的には顧問弁護士の活用、監査役の監視も必要です。)		●	●	(4.6)
	監査未実施	4- 2- 5- 5	Q システム監査を実施していない場合、そのことによるリスクを評価していますか？ (システム監査を行わない場合、リスクを暗黙に保有していることになります。システム監査を実施しなかった場合に増加するリスクの大きさを把握し、実施しない理由を説明できるか、明確にする必要があります。)		●	●	
3. 監査基準	監査基準	4- 2- 5- 6	Q システムに関する全業務(企画、開発、運用、保守)における監査基準は、リスクマネジメントの視点から明確で確実に守られていますか？ (保守や運用などの情報セキュリティにのみ関心が集中する傾向がありますが、システム開発やシステム企画についても開発の必要性、開発工程の適切性、無理な開発ではないか、などの監査を行う必要があります。これらも含めてシステム監査を実施する監査基準を作成し、確実に実施していくことが大切です。)		●	●	(4.5)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
コンピュータ犯罪	コンピュータ犯罪	4－3－(1) コンピュータ犯罪					
1．実施基準	コンピュータ犯罪	4- 3- 1- 1	Q 実施基準にコンピュータ犯罪(ネットワークを含む)対策を定めていますか？ (コンピュータ犯罪については企業として毅然とした態度で臨むことが必要であり、そのためには実施基準にコンピュータ犯罪対策についてのマネジメントの姿勢が述べられていることが必要です。ここでは、対策についてセキュリティポリシーに触れているか、それをユーザ部門が知っているかを確認します。)		●	●	(4.4.4.2)
	内部犯罪対策	4- 3- 1- 1- 1	Q 実施基準に内部犯罪とその対策を定めていますか？ (内部犯罪についても上記のコンピュータ犯罪と同様に、企業として毅然とした態度で臨むことが必要であり、そのためには実施基準に内部犯罪対策についてのマネジメントの態度が述べられていることが必要です。対策についてセキュリティポリシーに触れているか、それをユーザ部門が知っているかを確認します。)		●		4.4.4.2
	個人利用禁止	4- 3- 1- 1- 2	Q 実施基準に情報システムの個人利用の禁止を定めていますか？ (企業や組織では、最近、コンピュータの個人利用が損害を与えるということで、犯罪と同様、企業として毅然とした態度で臨むようになってきています。そのためには、実施基準に個人利用についての企業としての方針や罰則規定などが述べられ、ユーザ部門に知らされていることが必要です。)		●		(4.4.4.2)
	不正使用対策	4- 3- 1- 1- 3	Q 実施基準に情報システムの不正使用(なりすましなど)対策を定めていますか？ (情報システムの不正使用はコンピュータ犯罪です。他人の不在時にファイルが必要だからといって、他人のパソコンを操作したり、サーバに侵入することは犯罪行為です。これには企業として毅然とした態度で臨むことが必要であり、そのためには実施基準に不正使用についてマネジメントの毅然とした態度が述べられていることが必要です。対策についても、ID・パスワードの利用と他人や許可されていないサーバやパソコンへの不正使用・侵入について実施基準に述べられ、かつ、ユーザ部門が知っているかを確認します。)		●		(4.4.4.2)
2．内部犯罪の防止	パスワードの変更	4- 3- 1- 2	Q 内部犯罪防止のためにネットワーク利用のパスワードを定期的に変更していますか？ (内部犯罪の防止対策では、安易に他人のパソコンにログインできないようにパスワードの定期的な変更が必要です。ユーザはともすれば簡単な利用のためにID・パスワードを省略したり、定期的な変更を行わないことが多いのです。これについて、企業として実施基準に定め、それをユーザ部門に周知して、遵守していることを定期的に管理者が確認する手段があることが必要です。)		●		4.4.4.2
	内部犯罪の定義	4- 3- 1- 2- 1	Q ネットワーク利用での禁止事項は検出できますか？ (内部犯罪を含め、企業の内部ネットワークではさまざまなことが想定されます。これについては、犯罪行為が実施基準に定めてあり、かつ、これらの犯罪が起きた時には的確に検出でき、不埒なユーザに対して警告したり、罰則を与えることが必要になります。また、この内容について、ユーザ部門が知っていることも重要な要素です。)		●		(4.4.4.2)
	ネットワーク機器	4- 3- 1- 3	Q 内部犯罪防止のため重要なシステム、ネットワークのパスワードを定期的に変更していますか？ (内部犯罪の防止対策のためには、ネットワークの機器やサーバなどの利用が正しく定められ、利用権限のないユーザが安易にログインできないようにする必要があります。ユーザはともすれば、間違ってログインしたり内部犯罪行為でログインすることがあります。これについて、企業として対策を行い、かつ、ネットワーク管理者が確認する手順があるかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
コンピュータ犯罪	コンピュータ犯罪	4－3－(1) コンピュータ犯罪					
2．内部犯罪の防止	個人使用システム	4- 3- 1- 4	Q 個人が日常使用するシステム(パソコンなど)はパスワードを利用していますか？ (4-3-1-2とも共通することですが、パソコンのみならず、ユーザが企業の情報を保存する機器については、安易に他人がアクセスできないようにパスワードの利用が必要です。ユーザはともすればパソコンやPDAでは簡単な利用のためにパスワードを省略することが多いのです。これについても4-3-1-2と合わせてユーザ部門に周知し、かつ、パスワードの利用を確認する手段があるかを聞いています。)		●	●	4.4.4.2
3．データ保護対策	データ保護対策	4- 3- 1- 5	Q 重要なデータの保護について、データベースに対策を講じていますか？ (企業にとって情報資産のデータを保護することは必須であり、何らかの対策が必要です。ただし、ポリシーで述べるだけでは効果がないので、データベースにこの機能が実際に実現されていることが重要です。ここでは、対策がとられているのか(IS部門)、対策について知っており、かつ、対策を活用してユーザ部門のデータを保護しているのか(ユーザ部門)を聞いています。)		●	●	(4.4.4.1)
	暗号化	4- 3- 1- 5- 1	Q 重要なデータをデータベースに記録する場合、暗号化していますか？ (サーバなどのデータを保護するためには、企業の情報について重要度が定められ、かつ、重要度に応じて暗号化するなどの対策が重要です。また、暗号化のためには、暗号方式や暗号鍵の利用について検討されていることが重要です。)		●	●	(4.4.4.2)
	デジタル署名	4- 3- 1- 5- 2	Q 重要なデータをデータベースに記録する場合、(改ざん防止のために)デジタル署名を利用していますか？ (重要なデータは単に暗号化するだけでは十分でないことがあります。すなわち、データを改ざんされないように保護することが必要です。このためには企業の情報について重要度が定められ、かつ、改ざんに対する要求の度合いに応じてデジタル署名が必要となります。どのような場合にデジタル署名を利用するのがよいかについての基準があり、かつ、デジタル署名についての利用促進がなされていることが重要です。)		●	●	
	暗合鍵	4- 3- 1- 5- 3	Q 暗号鍵の盗難、搾取、改ざんなどが行われないように管理していますか？ (データを安全に保護するための暗号化は4-3-1-5に述べられていますが、具体的には暗号化するだけでは十分ではありません。重要なのは、暗号鍵を利用者がきちんと管理することです。攻撃者は暗号鍵を狙って窃盗したり搾取することがあります。また、暗号鍵を紛失して暗号を解読できなくなる可能性もあります。このような暗号鍵の管理の仕組みが十分にできていることが重要なポイントになります。)		●	●	
	セキュリティホール対策	4- 3- 1- 5- 4	Q コンピュータウイルスに攻撃される可能性のあるセキュリティホールはタイムリーに修正していますか？ (セキュリティホールを放置していると、Slammer Wormのような攻撃で被害を受けることが増えてきます。したがって、タイムリーにセキュリティホールに関する情報を入手し、対策を打つことが必須です。大切なのは、こまめなセキュリティホール情報を入手できるための情報収集能力の向上と、迅速な対応を行える危機管理体制を持つことです。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
コンピュータ犯罪	コンピュータ犯罪	4－3－(1) コンピュータ犯罪					
4．盗聴対策	盗聴対策	4－ 3－ 1－ 6	Q 盗聴(通信回線の盗聴や室内での特殊機器による盗聴)対策を行っていますか？ (物理的な機器を利用した盗聴への対策が必要です。特に、企業機密情報が通信回線や盗聴装置などを利用して外部に漏れないような対策が必要です。)		●	●	(4.4.4.2)
	録音機器持込管理	4－ 3－ 1－ 6－ 1	Q コンピュータ室への個人のパソコンや小型デジタル録音装置(録音・記録ができる機器)の持込みの管理を行っていますか？ (昨今、デジタル機器の能力向上で、小さなデバイスやラップトップコンピュータで簡単に録音ができるようになっています。これらの機器の持込みを管理し、情報の漏えいを防ぐ必要があります。大切なのは、不要な録音を禁止することです。録音装置などを発見した時の対処策を定めておく必要があります。)		●	●	
	携帯電話持込	4－ 3－ 1－ 6－ 2	Q コンピュータ室への個人の利用の携帯電話機器の持込みを管理していますか？ (昨今の携帯電話は音声を盗聴したり、写真などで機密情報を撮影して外部に送付するなど、企業機密情報を容易に外部に露出するデバイスとして利用することができます。したがって、機密情報を扱う部門の居室にこれらの個人の機器を持ち込むことを禁じる必要があります。実施基準などに個人の携帯電話を持ち込んでもよい範囲を明記し、従わなかったり違反した場合には罰することが必要です。)		●	●	
	PDA	4－ 3－ 1－ 6－ 3	Q 個人が管理するPDAなどに会社関連の重要情報を保存しないようにしていますか(許可する場合は条件を明確に示していますか)？ (昨今のPDAは10年前のデスクトップパソコンよりも高い能力を有しています。音声を盗聴したり、写真を撮影したり、機密情報をコピーして外部に送付するなど、企業機密情報を容易に外部に露出するデバイスとして利用することができます。また、個人のスケジュールや連絡先なども企業の重要な情報であることもあります。したがって、PDAを持ち込む範囲の限定、PDAに記録して個人で利用できる情報の範囲を明確にする必要があります。実施基準などに個人のPDAの持込み、保存できる情報の範囲を明記し、従わなかったり違反した場合には罰することが必要です。)		●	●	
	無線LAN	4－ 3－ 1－ 6－ 4	Q 無線LANの利用においては盗聴、データ漏えい対策を行っていますか？ (無線LANは企業内部でネットワークの配線に依存しないことから、最近は広く利用されるようになってきています。しかし、無線LANの電波は広く伝搬し、盗聴される機会も多くなります。さらに、現在の無線LANの方式では、暗号を利用してもさまざまな制約があり、脆弱性が大きいことが指摘されています。したがって、無線LANを利用するにあたってはデータの重要度に合わせて利用できる範囲を限定することや、利用そのものを認めないなどの対策が必要です。利用について実施基準に定め、データの機密漏えいを防ぐための手順を定めておく必要があります。)		●		
	電磁波漏れ	4－ 3－ 1－ 6－ 5	Q ディスプレイの電磁波漏れなどの対策を行っていますか？ (パソコンのディスプレイはCRTや液晶を問わず、画面表示のための微弱な電波が発せられています。これらの電波を集めて解読するTempest攻撃が知られています。したがって、画面表示は至近距離から盗聴される可能性があることを考えた対策が必要です。これらの攻撃に対する注意喚起と、窓に近い席での利用制限が重要となります。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
コンピュータ犯罪	コンピュータ犯罪	4－3－(1) コンピュータ犯罪					
5. 緊急時対応	ネットワーク対策	4- 3- 1- 7	Q ウイルスの被害でネットワークが使えなくなった場合の緊急時対策(代替通信手段等)を準備していますか？ (コンピュータウイルスの被害で企業や組織のネットワークが使えなくなるケースが増えてきています。また、2003年1月のSlammer Wormでは、韓国でインターネットバックボーンネットワークが輻輳で利用できなくなるケースも発生しました。したがって、インターネットを利用する場合にネットワークの代替手段について事前に検討し、対策を用意しておく必要があります。この問題に対する認識の有無と緊急時の対策を事前に定めておくことがポイントです。)		●	●	
	外部機関への相談	4- 3- 1- 8	Q コンピュータ犯罪の被害にあたって、関係機関や警察(サイバーポリス)に相談していますか？ (現在はコンピュータ犯罪が珍しくなくなりました。また、ひとたび問題が発生すると、企業や組織が受ける被害も大きくなっています。このような状況の中で対策を行うためには、外部の専門機関を活用することが大切です。日頃から被害を受けた時にどこに相談すればよいのか、あらかじめ連絡先などの情報を準備しておくことが望まれます。)		●		
	証拠保全	4- 3- 1- 9	Q コンピュータ犯罪の証拠保全を行っていますか？ (コンピュータ犯罪は防止すること、かつ、犯罪として犯人を逮捕し、法的に罰する必要があります。日本は法治国家なので、犯罪を立証しなければ犯人の逮捕や犯罪によって受けた損害の賠償を請求することができません。犯人を想定し、犯罪を立証するためには証拠が必要となります。この証拠を被害時に適切に保存すること(＝証拠保全)が必要です。被害時にこそ、緊急時対策として証拠を残すような手順を定めておくことが必要です。)		●		(4.4.2.4) (4.4.2.5)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
1. 実施基準	不正アクセス	4- 3- 2- 1	Q 実施基準に不正アクセス対策を定めていますか？ (不正アクセスはコンピュータ犯罪です。不正アクセスが犯罪行為であることが実施基準に明記されている必要があります。また、基準には対策が定められ、かつ、ユーザ部門に周知を行うこと、ユーザ部門が正しく認識していることが重要です。)		●	●	(4.4.4.2)
	認証	4- 3- 2- 1- 1	Q 実施基準に作業担当者のID・パスワードによる認証、生体認証等による識別が定められていますか？		●		[4.4.2.4]
	物理的アクセス対策	4- 3- 2- 1- 2	Q 実施基準に物理的アクセス対策を定めていますか？ (物理的アクセス対策は、物理的に情報資産を安全に隔離する対策です。ネットワークやサーバなどのハードウェアをはじめ、ソフトウェアやデータベースなどすべてのものを安全に隔離するために必須の要素です。実施基準に記述された情報資産を保護するための対象物ごとにきちんと明記され、かつ、対策を定めていることが必要です。また、定期的に監査を行い、物理的アクセス対策が有効かを確認することが必要です。)		●		4.4.4.2
	論理的アクセス対策	4- 3- 2- 1- 3	Q 実施基準に論理的アクセス対策を定めていますか？ (論理的アクセス対策は、情報資産へのアクセスをコントロールすることで情報資産を安全に保護する対策です。ソフトウェアやデータベースなどコンピュータのシステムで保存されているすべての情報資産に対して、どのようなアクセス者がアクセスできるかを管理し、かつ、アクセスの記録を残す必要があります。実施基準には、どのような情報資産があり、誰が、いつアクセスできるかの管理や記録を行うことがきちんと明記され、かつ、対策を定めていることが必要です。また、定期的に監査を行い、論理的アクセス対策が有効かを確認することが必要です。)		●		4.4.4.2
	外部からのアクセス	4- 3- 2- 1- 4	Q 実施基準に外部からのアクセスについて定めていますか？ (情報資産へは外部のネットワークやダイヤルアップを介してアクセスする場合があります。この外部からのアクセスについて、実施基準にアクセスのポリシー(許可の基準など)やアクセスを管理し、不正アクセスを防ぐ対策が明記されていることが必要です。また、定期的に監査を行い、外部からのアクセスがコントロールされているかを確認することが必要です。)		●		4.4.4.2
	緊急時対策	4- 3- 2- 1- 5	Q 実施基準に不正アクセスがおきた場合の緊急時対策、体制を定めていますか？ (不正アクセスによって企業や組織の重要な情報資産が窃盗されたり、改ざんされたりするケースが増えてきています。したがって、インターネットなどの外部のネットワークを利用する場合、不正アクセスがおきた時、どのような緊急の対策を講じるかを事前に検討し、対策を実施基準に明記しておく必要があります。また、定期的に監査を行い、緊急時対策が有効か、実現可能かを監査する必要があります。)		●		(4.4.1)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
2. アクセス管理	アクセス管理	4- 3- 2- 2	Q. アクセス管理を行っていますか？ (アクセス管理は情報資産へのアクセスをコントロールして情報資産を安全に保護する対策です。すべての情報資産に対し、その重要度に対して誰が、いつ、アクセスできるかをコントロールできること、また、アクセスがすべて記録され、権限外のアクセスの場合は、アクセスを保留し、管理者にその事実を連絡する必要があります。また、定期的に監査を行い、アクセス管理が有効かを確認することが必要です。)		●	●	(4.4.4.2)
	不正アクセス防止	4- 3- 2- 2- 1	Q サーバ、ファイアウォール、ルータなどへの不正アクセス防止策をとっていますか？ (不正アクセスを防ぐには、サーバ、ファイアウォール、ルータなどにアクセス管理の機能を持たせ、許可された権限者のみがアクセスできるようにコントロールする必要があります。特に装置を購入した場合、誰でもアクセスできる初期パスワードのままで放置したり、パスワードを設定し忘れたりすることが多いようです。また、権限者が変わる時にパスワードをきちんと変更する必要があります。この対策がきちんと手順にまで展開されていることが重要です。)		●		(4.4.4.2)
	データ保護	4- 3- 2- 2- 2	Q 社外との通信での重要なデータを守る方法(VPNの利用、プロバイダの暗号サービス利用など)をとっていますか？ (社外との通信の場合にも公衆ネットワークを利用するケースが増えてきました。このような時にも情報資産の価値によっては適切に保護する必要があります。この保護には多くの場合、VPNやIP-VPNなど、データ保護がなされるサービスやプロバイダが提供する暗号サービスの活用が有効です。重要な情報資産の保護についてはこのようなサービスの利用をユーザに義務づけることが必要です。)		●		
	暗号利用	4- 3- 2- 2- 3	Q 重要な通信や重要なファイルについて暗号で保護していますか？ (重要な情報資産を通信ネットワークで送ったり、企業や組織の外部に持ち出す場合、情報資産の価値によっては適切に暗号で保護する必要があります。万一操作ミスなどでデータが露出しても、暗号によって内容が保護されているので情報資産そのものの露出には至りません。ユーザに情報資産の価値に応じて暗号の利用を進めることが必要です。)		●		
	ID付与・パスワード管理	4- 3- 2- 3	Q 職務の必要性に応じたアクセス権限に基づいて、情報システムへのIDが付与され、パスワードが管理されていますか？ (ユーザへのID・パスワードの付与および管理については、職務の必要性に合わせて行うことが必要です。ネットワークにアクセスするために必要となる最低限の権限を与えるのが基本です。また、申請者の部門の正式な許可を受けていることが必須です。これらについても実施基準に記述されている必要があります。また、このための申請書類なども定型化しておくことが重要です。)		●	●	(4.4.4.2)
	ID付与・パスワード管理のレビュー	4- 3- 2- 3- 1	Q ID付与・パスワード管理についてチェックやレビューを行っていますか？ (ユーザへのID・パスワードの付与については4-3-2-3に述べられているとおりです。特に、ユーザへのIDの付与については実施前に第三者によってレビューされていることが必要です。申請書類が整っていることや正しい権限者が許可を与えていることなど、レビューすることが必要です。さらに、実施された時の記録がログに保存され、正しく実施されたことをレビューする必要があります。また、申請書類やログが改ざんされたり、窃盗されないように保護する必要があります。)		●		[4.4.2.4]

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
2. アクセス管理	不正入手	4- 3- 2- 3- 2	Q ID・パスワードの不正入手があった場合、その不正入手の原因はつきとめられましたか？ (ID・パスワードが不正入手された場合、重要なのはどのような原因で不正入手されたかを検証することです。追跡して、犯人を捕捉し、再発しないようにコントロールする必要があります。そのためには不正なIDを削除するだけでは十分ではありません。)		●		
	アクセス権付与チェック・レビュー	4- 3- 2- 3- 3	Q アクセス権の付与についてチェックやレビューのシステムがありますか？ (ユーザへのアクセス権限の付与は4-3-2-3のID・パスワード付与よりも重要です。これは情報資産にアクセスできるためです。ユーザへのアクセス権限付与については、実施前に第三者によってレビューされていることが必要です。申請書類が整っていることや、正しい権限者が許可を与えていることなどをレビューする必要があります。さらに、実施された時の記録がログに保存され、正しく実施されたことをレビューする必要があります。また、申請書類やログが改ざんされたり、窃盗されないように保護する必要があります。)		●		[4.4.2.5]
	機密度・アクセス制限	4- 3- 2- 4	Q 情報システム上での、機密度のランクと対応したアクセス制限が行われていますか？ (情報システムでは、ともすれば情報資産の機密度や重要度に応じたアクセス権限が設定されていなかったり、アクセス制限機能が不十分である可能性があります。したがって、機密度や重要度に応じたアクセスコントロールが実施されていることを検証する必要があります。)		●	●	
	職務分離	4- 3- 2- 4- 1	Q データへのアクセスに対して職務の分離が行われていますか？ (データへのアクセスは、アクセス者の職務に応じた最低限のアクセス権限が付与されていることが重要です。したがって、アクセスするデータに対して職務を区別(細分化)し、職務上不必要なデータにアクセスさせないようにする必要があります。これには、実際の職位や権限とは区別して、職務遂行上最低限のデータにのみアクセスさせることが必要です。)		●	●	(4.4.1)
	インターネット利用	4- 3- 2- 5	Q インターネットの利用について利用条件が定められていますか？ (企業や組織でのインターネットの利用について、職務遂行上に必要な範囲にアクセスが限定されていることが必要です。特にWebサイトへのアクセスでは、職務以外のデータにも容易にアクセスできるため、不要なデータにアクセスする目的外利用が増えています。また、外部への不正アクセスなどの犯罪を誘発することも起こりえますので、これを防ぐことが重要です。インターネットの利用についての規則を定め、必要なアクセス以外については厳しく取り締まることが重要です。このためには、インターネットの利用についてのガイドラインをユーザに配布し、教育することが重要です。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
2. アクセス管理	教育・訓練	4- 3- 2- 6	Q ユーザにアクセス管理の実施方法や基準、概念(need to know)について教育・訓練を実施していますか？ (ユーザはネットワークが便利に使えるようになると、権限を越えてアクセスしたり、不要なWebサイトにアクセスしたりすることが増えています。これを防ぐためには、ユーザに対してネットワークの利用の基準やアクセスが職務上必要な範囲に限定されることなどを教育する必要があります。また、インターネットの利用ミスによって企業の大きな損害に繋がることなどを自覚させる必要があります。)		●	●	(4.4.6)
	不正アクセス対策教育	4- 3- 2- 6- 1	Q 情報システム部門のスタッフに対し、不正アクセス対策についての専門的な教育・訓練を実施していますか？ (不正アクセスは攻撃者側が常に企業の脆弱なところや管理の不十分なところを狙ってくるため、常に注意が必要です。すなわち、情報システムの状況を監視して不審な点がないか、OSやファイアウォールなどのソフトウェアは常に最新のバージョンか、また、脆弱性情報には常に注意を払う必要があります。これには情報システム部門のスタッフへの教育はきわめて重要です。定期的に教育や訓練を受けて常に最新の情報を得るようにすることが重要です。)		●		(4.4.6)
3. 物理的アクセス対策	不正侵入防止	4- 3- 2- 7	Q 入退館システムを通りぬけ、情報システム室、情報ネットワーク管理室に侵入されることを防ぐ仕組みがありますか？ (情報システムの物理的対策は、すべての重要な機器やデータを保護する上できわめて重要な措置です。これには施設への入退室の管理が重要です。入退室にあたり、すべてのアクセスがチェックされ、記録されている必要があります。これには、いかなる例外も認められません。すり抜けなどが起きないような対策が重要です。)		●	●	(4.4.4.2)
	ネットワーク機器の不正防止	4- 3- 2- 7- 1	Q ネットワーク機器などへの物理的アクセス対策(物理的な隔離など)がとられていますか？ (情報システムの物理的対策の中でも重要なのは、ネットワーク機器への対策です。これに細工されたりすると、重要なデータの盗難や改ざんに繋がります。したがって、ネットワーク機器を保護することは基本です。ネットワーク管理者といえども、権限外に機器に触れたりすることは認められません。機器に触る時には事前に操作が許可され、すべての操作が記録されて監視されない限り認められません。対策としては、厳しい物理的アクセス管理が必要です。)		●	●	
	入退室	4- 3- 2- 7- 2	Q 入退室に関して、パスワード、指紋・虹彩・網膜・顔形状などの確認装置等を設置していますか？ (入退室の時には本人確認を正しく行う必要があります。昨今では、技術の進歩によって本人確認の機器が市場で安価に購入できるようになっています。したがって、本人を確認できる、より高度なものを採用することが望まれます。)		●	●	(4.4.4.2)、[4.4.2.4]

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
4. 論理的アクセス対策	重要なデータ保護対策	4- 3- 2- 8	Q 機密度の高いシステムとデータについて、特別の取扱いが定められていますか？ (データなどの情報資産を保護するための論理的対策としては、重要度が定められ、かつ、重要度に応じて、特別な保護の取扱いが考慮されていることが重要です。)		●	●	(4.4.4.2)
	暗号	4- 3- 2- 8- 1	Q 通信に暗号を利用していますか？ (データなどの情報資産を保護するための論理的対策としては、重要度が定められ、かつ、重要度に応じて暗号化して保護することが重要です。また、暗号化のためには、どのような暗号方式を利用するのがよいか、また、暗号鍵について検討が行われていることが重要です。)		●		
	デジタル署名	4- 3- 2- 8- 2	Q (改ざん防止のために)デジタル署名を利用していますか？ (重要なデータは単に暗号化するだけでは十分ではないことがあります。すなわち、データを改ざんされないように保護することが必要です。このためには、企業の情報について重要度が定められ、かつ、改ざんに対する要求の度合いに応じてデジタル署名が必要となります。)		●	●	
	暗合鍵管理	4- 3- 2- 8- 3	Q 暗号鍵(公開鍵の秘密鍵や共有鍵)を適切に管理していますか？ (データを安全に保護するための暗号化は4-3-2-8-1に述べられていますが、論理的アクセスの具体的対策として暗号化するだけでは十分ではありません。大切なのは、暗号鍵を利用者がきちんと管理することです。攻撃者は暗号鍵を狙って窃盗したり、搾取することがあります。また、暗号鍵を紛失して暗号を解読できなくなる可能性もあります。このような暗号鍵の管理の仕組みが十分にできていることが重要なポイントになります。)		●		
	個人認証	4- 3- 2- 9	Q 個人認証を行っていますか？ (個人認証はネットワークを介しての情報資産へのアクセスを管理する手段です。これが機能しないと、誰が、いつ、何をしたかを正確につかめません。また、情報資産の重要度に応じたアクセス制御を行うためにも、個人を特定してその職務に見合ったアクセスを許可するためにも必要なプロセスです。具体的な技術には、パスワードによる論理的な認証に加えて、4-3-2-7-2に述べている指紋や虹彩などを利用することが望まれます。)		●	●	(4.4.4.2)
	ペネトレーションテスト	4- 3- 2- 9- 1	Q ペネトレーションテストを行っていますか？ (外部との接続でネットワークを利用する場合にはさまざまな脆弱性があります。特に、利用している機器のOSや組み込まれたプログラム、ファイアウォールの設定、ネットワーク機器のIDやパスワード、インターネットを利用する場合のプロトコルなどにはさまざまな脆弱性があります。これらをテストするためには、ペネトレーションテストと呼ばれる疑似攻撃を行い、脆弱な部分を明らかにする必要があります。脆弱性が発見された場合、ただちに対策を行うことが必須です。)		●	●	
	システム個人認証	4- 3- 2- 9- 2	Q 共通に利用するシステムやネットワークでは、ICカード、声紋、指紋等を利用していますか？ (共通に利用するシステムでは、とかく論理的アクセスが弱くなります。これは、複数の者が利用するため、サービス性を考えるとどうしてもアクセスを簡単にしてしまうからです。しかし、ネットワークでは、ひとたび破られて不正侵入を許すと全体に迷惑が及びます。そこで、個人認証として、インタフェースが比較的安易で、かつ、個人の識別能力の高いものを用いることが望まれます。この点からは、ICカード、声紋、指紋、虹彩などを利用するのが適しています。)		●	●	(4.4.2.4)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
4．論理的アクセス対策	中継地回避の実施基準	4- 3- 2- 10	Q 不正侵入や電子メールの不正中継地とされることを避けるための実施基準が定められていますか？ (通常、ハッカーなどが不正侵入を行う場合、スパムメールと呼ばれる不特定多数に多量のメールを送付する迷惑行為は、踏み台と呼ばれる不正のための中継地点を利用することが多いのです。この踏み台になると、さまざまな攻撃をこのサイトから実行され、その責任を担うことになります。中継地点とならないような対策を実施基準に盛り込んでおくことが必要です。具体的には、不正侵入対策を行う、定期的なログのチェックなどを行うことが必要です。)		●	●	
	中継地懸念とログ分析	4- 3- 2- 11	Q 知らない間にサイバーテロの中継地とされているのではないかとの疑いをもって、Eメール受信ログ、ホストごとのシステムアプリケーションログの監視を行っていますか？ (4-3-2-10で述べられている踏み台は、なかなか気づきにくいものです。これを防止するには、常に電子メールサーバやホストの状況を監視しながら、不審な動作がないか用心したり、ログの定期的なチェックで素早く異常を検知するなど、日頃の行動が必要です。)		●	●	
5．ネットワーク上のデータ保護	ネットワークの不正アクセス対策	4- 3- 2- 12	Q ネットワークを介してのアクセスではID・パスワードを利用していますか？ (ネットワークを介したアクセスの場合、正しいアクセス者になりすまされる危険性があります。これを防ぐためには、ネットワークやサーバには必ず、ID・パスワードを用いて、正しい権限者のみがアクセスできるようにすることが必須です。)		●	●	[4.4.2.4]
	暗号化転送	4- 3- 2- 12- 1	Q ネットワークを介したアクセスの場合、ID・パスワードは暗号化して転送していますか？ (ネットワークを介したアクセスの場合、なりすましを防ぐためには、ネットワークやサーバにログインする情報そのものを暗号化する必要があります。これによって、攻撃者が途中のネットワークで盗聴してもなりすまされることはありません。さらに、暗号方式の検討および暗号鍵の管理について検討されていることが重要です。)		●		
	ファイアウォール	4- 3- 2- 13	Q ファイアウォールを設けて(フィルタリングの設定を含む)いますか？ (ネットワークをインターネットや外部のネットワークと接続する場合、境界点にファイアウォールを設置することが基本です。これによって、外部からのすべてのアクセスに対してコントロールが可能になります。ただし、ファイアウォールを設置する場合、必ず初期パスワードを変更すること、OSが最新版であることを確認すること、フィルタリングを設定することが必要です。また、定期的にファイアウォールのログをチェックすることが必要です。)		●		
	DMZ	4- 3- 2- 13- 1	Q DMZ(バリアセグメント)を設け、WWW、DNSやメールサーバなどを設置していますか？ (4-3-2-13のファイアウォールと内部のネットワークの間にDMZを設けて、外部のネットワークに見せる必要のあるWebサーバやメールサーバを設置する必要があります。これは、内部のネットワークを不要なアクセスから保護するために必要です。ファイアウォールの存在がきわめて重要で、このオペレーションには専門家が必要です。)		●		
	ファイアウォールレイアウト	4- 3- 2- 13- 2	Q ファイアウォールが効果的に機能を果たすための機器構成が定められていますか？ (4-3-2-13のファイアウォールはきちんと設定して運用することが必要です。このオペレーションには、ネットワークの最新の動向を踏まえて構成を決める必要があります。特に、ファイアウォールは通過するすべてのパケットをチェックするため、高速なネットワークは能力の高いものが必要となります。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
5. ネットワーク上のデータ保護	重要データ保存管理	4- 3- 2- 13- 3	Q 重要なデータを保存管理するサーバはインターネットから直接アクセスできないようにしていますか？ (企業や組織にとって重要なデータを保存管理するサーバをインターネットに直接接続することはきわめて危険です。このサーバに侵入された場合、この重要なデータが盗難にあったり、改ざんされたりする可能性が高いからです。危険分散のためにはインターネットとの境界点にファイアウォールを設置するのが基本です。ファイアウォールで外部からのアクセスをコントロールして、正しいアクセス要求に対してのみ該当するサーバに接続させる必要があります。)		●		(4.4.4.2)
	ログ記録機能	4- 3- 2- 13- 4	Q 重要なデータを管理する情報システムやネットワークシステム(ファイアウォールやアクセスサーバ)にはログを残す機能がありますか？ (重要なデータを保存する情報システムやネットワークシステムでは、すべてのアクセスを記録し、後日、いつ、誰から、どのようなアクセスが行われたかをチェックできることが必須です。これにはログを残すことが必須です。なお、このログが第三者から不用意に改ざんされないように保護することも必要です。)		●		[4.4.2.4]
	ログ自動分析ツール	4- 3- 2- 13- 5	Q 当該ログを定期的にチェック(自動で分析するツールの利用も含む)していますか？ (4-3-2-13-4で述べられているログは、大規模なネットワーク機器の場合などは分量が膨大なものとなります。これを黙視点検するには限界があります。このような場合には、ログを自動的に分析して、疑わしいアクセス記録を抽出できることが必要です。これによって、調べる範囲を限定でき、素早く対応を行うことができます。)		●		[4.4.2.4]
	検知機能	4- 3- 2- 13- 6	Q 不審なアクセスがあった場合、検知(可能であれば追跡)機能を設けていますか？ (不審なアクセスはログファイルを分析することや、IDSなどの検知システムで検知することが必須です。検知結果はオペレータが分析し、必要があれば、不審なアクセスがどこから来ているかを追跡し、攻撃であることがわかれば、攻撃から防いだり、攻撃者を追跡できます。このような検知機能があるとよいでしょう。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
6．外部アクセスからのデータ保護	移動体内蔵データ保護	4- 3- 2- 14	Q 携帯のパソコンを使っている場合、内蔵しているデータ(会社の重要なデータ)の保護対策を行っていますか？ (携帯パソコンを仕事で利用する場合、このパソコンのデータが攻撃される可能性があります。企業内部では、情報システムや情報セキュリティポリシーで重要なデータは保護されていますが、携帯パソコンでは、管理がいい加減になるおそれがあります。したがって、このようなパソコンのデータがパソコンごと奪われたり、インターネットにダイヤルアップ接続中に不正侵入されて盗まれたりすることもあります。パソコンが奪われてもデータが読めないように暗号化などの対策が必要です。)		●	●	
	接続方式	4- 3- 2- 14- 1	Q 外部からの接続方式については、定期的に対策を見直していますか？ (ネットワークを介してアクセスしている場合、アクセス者が直接確認できないため、相手の認証をより確かなものとするためには、いろいろな方法を用いる必要があります。また、同じ接続方式を採っている場合、攻撃者に察知される可能性も高まります。そのため、接続方式については、安全性を高めるために常に対策を見直す必要があります。)		●	●	
	認証	4- 3- 2- 14- 2	Q 直接ネットワークに接続している場合、呼返し方式やワンタイムパスワードを利用していますか？ (ダイヤルアップ接続の場合、アクセスしている人間の認証をより確かなものとするためには、呼返しやワンタイムパスワードなどが必要です。ネットワークでは、接続してくる相手が必ずしも信用できないため、複数の方法を用いて、より信頼を高める必要があります。)		●	●	[4.4.2.4]
	ネットワークサービス	4- 3- 2- 14- 3	Q 直接ネットワークに接続している場合、IP-VPN等の安全なネットワークサービスを利用していますか？ (IP-VPNは、専用線と同様にIPのネットワーク上で固定接続を提供します。そのため、接続された地点以外とは接続できないため、きわめて安全性の高いネットワークサービスです。このようなサービスを利用してネットワークの安全性を高めることが必要です。)		●	●	
	ソーシャルエンジニアリング対策	4- 3- 2- 14- 4	Q 電話などでの問合せに対してソーシャルエンジニアリング対策を行っていますか？ (ソーシャルエンジニアリングは、情報システムのアウトソーシングなどによって最近増える傾向にありますが、このうち、不確かな問合せや言いがかりなど、怪しいものには回答しないことです。また、なりすましを防ぐために、必ず別のルートで相手の本人確認を行うなどの手順を確立しておくことが必要です。)		●		[4.4.2.4]

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
7．不正検出	アクセスログ確認	4- 3- 2- 15	Q アクセスログについてアクセスの権限、権限外の記録方法について定期的に分析していますか？ (不正検出を行うにはアクセスの記録をきちんとログに記録し、このログを常にチェックして、権限外のアクセスが、いつ、誰によって行われたかを確認し、その事実や理由を確認する必要があります。)		●		[4.4.2.4]
	プロトコル	4- 3- 2- 15- 1	Q ネットワーク機器は不正アクセスの対象となるプロトコルが検出できる設定になっていますか？ (不正検出を記録し、後日分析して、ネットワークで許可されていないプロトコルによる不正アクセスが、いつ、誰によって、どこから行われたかを確認し、その事実や理由を確認し、被害の最小化や現状復帰などの適切な対策を行う必要があります。)		●		
	ログ保存	4- 3- 2- 15- 2	Q 機密度の高い個別情報に関して、生成、アクセス、その他の処理プロセスは、ログに残されていますか？ (企業や組織の重要な機密度の高いデータに対しては、いつこのデータが作成され、いつ、誰がこのデータにアクセスしたか、その事実を記録してログに保存し、このデータが改ざんされないようにする必要があります。)		●		[4.4.2.4]
	ログ確認	4- 3- 2- 15- 3	Q 情報のオーナーおよびシステム管理者が上記ログを定期的に確認していますか？ (情報のオーナーがその情報にいつ、誰がアクセスしたかを定期的に確認し、アクセス権限のある人が適切にアクセスしたことがログに記録されている必要があります。また、このログを定期的に確認することで未然に犯罪を防ぎ、重要な情報資産を保護できます。これを定期的に行うことが必要です。)		●		[4.4.2.4]
8．緊急時対応	緊急対処方法	4- 3- 2- 16	Q ハッカー、ウイルス侵入、不正アクセス等による緊急事態対処のための緊急連絡、対応方法は周知され、訓練されていますか？ (現在はコンピュータウイルス侵入や不正アクセスなどのコンピュータ犯罪が珍しくなくなりました。また、ひとたびこのような問題が発生すると、企業や組織の被害も大きくなっています。このような状況の中で、日頃から、被害を受けた時にどこに相談すればよいか、どのような対処をすればよいか、あらかじめ連絡先などの情報を周到に準備しておくことが望まれます。)		●	●	
	IPAへの届出	4- 3- 2- 17	Q 不正アクセスの被害にあたって、コンピュータ不正アクセス被害届出機関である情報処理推進機構(IPA)に被害を届け出ましたか？ (現在はコンピュータ犯罪が珍しくなくなりました。また、ひとたび不正アクセスの問題が発生すると、企業や組織の信用問題など、受ける被害も大きくなっています。このような状況の中で対策を行うためには、外部の専門機関を活用することが大切です。不正アクセスについてはIPAがデータを収集しており、また、問題解決の研究を行っているので、情報を素早く連絡することが社会的にも重要です。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
不正アクセス	不正アクセス	4－3－(2)不正アクセス					
8. 緊急時対応	JPCERT／CCへの相談	4- 3- 2- 18	Q 不正アクセスの被害にあたって、JPCERT／CC(コーディネーションセンター)に相談していますか？ (現在はコンピュータ犯罪が珍しくなくなりました。また、ひとたび不正アクセスの問題が発生すると、企業や組織の信用問題など受ける被害も大きくなっています。このような状況の中で対策を行うためには、外部の専門機関を活用することが大切です。日頃から、被害を受けた時にどこに相談すればよいのか、あらかじめ連絡先などの情報を準備しておくことが望まれます。JPCERT／CCは被害報告の受付、対応支援、発生状況の把握、手口の分析、再発防止策の検討や助言などを技術的な立場から行っています。		●		
	外部機関への相談	4- 3- 2- 19	Q 不正アクセスの被害にあたって、関係機関や警察(サイバーポリス)に相談していますか？ (現在はコンピュータ犯罪が珍しくなくなりました。また、ひとたび不正アクセスが発生すると、企業や組織が受ける信用問題などの被害も大きくなってきています。このような状況の中で、対策を行ったり犯罪として訴える場合には、外部の専門機関を活用することが大切です。日頃から、被害を受けた時にどこに相談すればよいのか、あらかじめ連絡先などの情報を準備しておくことが望まれます。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
コンピュータウイルス	コンピュータウイルス	4－3－(3)コンピュータウイルス					
1．実施基準	コンピュータウイルス対策	4- 3- 3- 1	Q 実施基準にコンピュータウイルス対策(検出・駆除、教育、感染対策)を定めていますか？ (コンピュータウイルスも情報システムの大きなリスクの1つです。ウイルス対策について、実施基準で定めていないと、社内ネットワークとインターネットを遮断するといった緊急時の対応が適切に実行できなくなります。)		●		(4.4.4)
	感染時の緊急時・事後対策	4- 3- 3- 1- 1	Q 実施基準にウイルス感染の場合の緊急時対策、事後対策を定めていますか？ (実施基準に、コンピュータウイルス感染が起きた場合の緊急時対策として、緊急時の体制、感染経路の調査、感染拡大防止策、広報対応、ウイルス送付先対応等が必要です。また、事後対応として、感染した機器のウイルス駆除、データの復旧、セキュリティホール対策、ワクチンソフトの更新等が必要です。)		●		
2．事前対策	ウイルス防止ソフト	4- 3- 3- 2	Q コンピュータウイルスを防ぐソフトウェアを用意していますか？ (ワクチンソフトをクライアントのパソコン、ファイルサーバ、メールサーバ等に導入する必要があります。)		●	●	
	ウイルス検出・駆除	4- 3- 3- 2- 1	Q コンピュータウイルスの検出・駆除のためにソフトウェアのバージョンアップを定期的に行っていますか？ (コンピュータウイルス感染を防止するためにはOSに対する最新のパッチや、ワクチンパターンファイルにアップグレードする必要があります。)		●	●	
3．教育・訓練	教育・訓練体制	4- 3- 3- 3	Q コンピュータウイルス対策に関して組織的に教育・訓練を実施する体制がありますか？ (コンピュータウイルス対策について、システム管理者やユーザに対し、教育・訓練を行う体制を持つ必要があります。特にシステム管理者については、高度な教育を実施する必要があります。)		●	●	(4.4.6)
	社員の教育・訓練	4- 3- 3- 3- 1	Q 社員にコンピュータウイルス対策に関して定期的に教育・訓練を実施していますか？ (コンピュータウイルスは、新種が発生するたびにその感染メカニズムが変り、たとえばメールの添付書類を開かなければ感染しないといった、過去の対策が安全ではなくなります。全社員に対しても、定期的な教育が必要です。)		●	●	(4.4.6)
	システム管理者の教育・訓練	4- 3- 3- 4	Q システム管理者に対し、コンピュータウイルス対策、緊急時対策、感染防止の方法に関して最新の教育・訓練を実施していますか？ (システム管理者に対しては外部の専門機関を使って、コンピュータウイルスの予防、検出、駆除、システムの復旧について、最新の内容で、定期的な教育を実施する必要があります。)		●	●	(4.4.6)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ−3. 不正アクセス・コンピュータウイルス関連					
コンピュータウイルス	コンピュータウイルス	4−3−(3)コンピュータウイルス					
4．ウイルス対策	緊急連絡体制	4− 3− 3− 5	Q コンピュータウイルスに感染した場合の緊急連絡体制ができていますか？ (ユーザがコンピュータウイルスに感染した疑いを抱いた時に、連絡すべき窓口が明確になっていたり、情報システム部門内の緊急時連絡網が明確になっていることが必要です。)		●	●	
	影響判断	4− 3− 3− 5− 1	Q 仕事への影響をすぐに判断できるようになっていますか？ (連絡を受けた窓口が、仕事への影響を判断するために、システム構成等の必要な情報を整備しておくことが必要です。)		●		
	情報収集	4− 3− 3− 5− 2	Q すぐに情報を集め、ウイルスの感染防止や復旧など対処できるようになっていますか？ (感染拡大の防止や、感染した機器からのコンピュータウイルスの駆除のために、IPA等の公的機関やワクチンベンダから情報を収集する体制が必要です。)		●		
	感染ルート	4− 3− 3− 5− 3	Q 感染ルートを突き止めることができますか？ (感染ルートを突き止めるために、電子メールのメッセージログ等を保存しておく必要があります。)		●		
	感染の緊急時対策	4− 3− 3− 6	Q ウイルスに感染した場合に備えた緊急時の対策(システムの再インストール、バックアップデータからの早急な回復など)を有していますか？ (コンピュータウイルスに感染した場合、ディスクをフォーマットしてから、システムを再インストールするために、システムイメージやデータのバックアップを定期的に取得する必要があります。)		●	●	
	感染防止対策	4− 3− 3− 7	Q ウイルスの感染を防ぐための対策がありますか？ (ワクチンソフトの導入といった、コンピュータウイルス感染を防ぐ対策の実施が必要です。)		●	●	
	伝染防止	4− 3− 3− 8	Q 感染したウイルスを伝染させないための対策(ソフトでの対策、感染したパソコンをネットワークから除去するなど)を行っていますか？ (外部に感染を拡大しないために、メールサーバでのウイルスチェックや、感染したパソコンの切離し、インターネットとの接続の切離し等を行う必要があります。) (用語解説「伝染」:他にウイルスをうつすことをいいます。)		●	●	
5．事後対策	事後対策	4− 3− 3− 9	Q ウイルス感染した場合、事後対策を講じていますか？ (コンピュータウイルスに感染した場合、回線経路の解明、感染原因の分析、感染対策の実施といった事後対策を行う必要があります。)		●	●	
	感染情報	4− 3− 3− 9− 1	Q ウイルス感染に関する情報を共有していますか？ (システム管理とセキュリティ管理のチームの中で、コンピュータウイルス感染に関する情報を共有する必要があります。)		●	●	
	通知	4− 3− 3− 9− 2	Q ウイルス感染の通知を作成し、周知していますか？ (コンピュータウイルス感染の経路や対策の概要をユーザに周知する必要があります。)		●	●	
	体制強化	4− 3− 3− 9− 3	Q ウイルス対策の体制を強化(ウイルス対策担当者を置くなど)していますか？ (コンピュータウイルス感染の対策として、発見された感染原因を抑止できる新たな対策が必要です。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
コンピュータウイルス	コンピュータウイルス	4－3－(3)コンピュータウイルス					
5．事後対策	復旧対策	4- 3- 3- 9- 4	Q ウイルス駆除後のシステムの復旧対策がありますか？ (システムイメージの定期的な保存、データのバックアップ取得、システムにインストールしたソフトウェアの集中管理といった、復旧対策が必要です。)		●		
	再発防止対策	4- 3- 3- 9- 5	Q ウイルス駆除後、再発防止対策がありますか？ (サーバへのワクチンソフトの導入、OSに対するパッチの適用、ワクチンパターンファイルの更新を定期的に行う必要があります。)		●		
	経験の共有化	4- 3- 3- 9- 6	Q ウイルス感染、駆除の経験は組織で共有化されていますか？ (コンピュータウイルス感染の対応改善について、システム管理者やユーザに対して周知する必要があります。この内容は、最終的に教育内容に反映します。)		●	●	
	IPAへの届出	4- 3- 3- 10	Q コンピュータウイルスの被害にあたって、コンピュータウイルス被害届出機関である情報処理推進機構(IPA)に被害を届け出ましたか。 (コンピュータウイルスの被害にあった時は、届出機関に被害を届けることが、経済産業省の告示で定められています。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
E-Commerce	E-Commerce	4－3－(4)E-Commerce					
1．実施基準	E-Commerce	4- 3- 4- 1	Q E-Commerceサービスを提供している場合、実施基準にE-Commerce対策を定めていますか？ (ネットワークを使って一般消費者を含む取引先と金銭の授受を伴う商取引を行っている場合には、人手により行っていた時とは異なるリスクが発生します。安定的なE-Commerceの基盤には、これらのリスクへの対策が必要です。)		●		
	個人情報保護対策	4- 3- 4- 1- 1	Q 実施基準に個人情報保護対策を定めていますか？ (一般消費者を含むE-Commerceを行っている場合は、個人情報保護対策を実施基準で定める必要があります。)		●		4.2
	データ保護対策	4- 3- 4- 1- 2	Q 実施基準にデータ保護対策を定めていますか？ (E-commerceに関連するデータについて、重要なデータとして特別な保護対策をとることを実施基準で定める必要があります。)		●		4.4.4.2
	インターネット利用対策	4- 3- 4- 1- 3	Q 実施基準にインターネット利用に関する対策を定めていますか？ (インターネットを利用する場合には、DDoS攻撃といった専用ネットワークにないリスクがありますが、これへの対策を実施基準で定める必要があります。)		●		
	電子商取引規定	4- 3- 4- 1- 4	Q 実施基準に電子商取引に関する規定を定めていますか？ (電子的な取引固有のリスクに対して、実施基準で対応を定める必要があります。)		●		
2．プライバシー保護	プライバシー保護対策	4- 3- 4- 2	Q インターネットでの電子商取引において、利用者情報の収集についてはプライバシー保護対策を行っていますか？ (個人情報保護法に準拠した、利用者情報収集時の情報主体の承諾とともに、情報保護の対策が必要です。)		●	●	4.2
	コンプライアンスプログラム	4- 3- 4- 2- 1	Q 個人情報保護コンプライアンスプログラムを実施していますか？ (JIS Q 15001に基づくコンプライアンスプログラムを実施する必要があります。)		●	●	
	プライバシーマーク取得	4- 3- 4- 2- 2	Q プライバシーマークの取得(や同等な認証)を受けていますか？ (個人情報保護を適切に行っていることを外部に実証するためには、認証の取得が有効です。)		●	●	
	クッキー対策	4- 3- 4- 2- 3	Q クッキーを利用する場合(セッション間で個人を識別するために情報を共有する目的で利用する)の指針を定めていますか？ (自社Webについてのガイドラインの中で、クッキーの使用について、利用者情報の取得等で個人情報保護の規定を遵守するための制限が必要です。)		●		[4.4.2.5]
3．不良客情報管理	不払い、不良客情報管理	4- 3- 4- 3	Q インターネットでの電子商取引での不払いなどの不良客に対する情報の管理を行っていますか？ (インターネットでは、取引先数の増大や、取引サイクルの短縮を考慮した、迅速な顧客管理が必要となります。)		●	●	4.2 4.4.3
	不良客情報入手	4- 3- 4- 3- 1	Q 外部からの不良客などの情報を入手していますか？ (顧客管理の一環として、外部からの信用情報を活用する必要があります。ただし、個人情報保護法の遵守も必要です。)		●	●	[4.4.2.4]

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
E-Commerce	E-Commerce	4－3－(4)E-Commerce					
4．データ保護対策	電子商取引時のデータ保護対策	4- 3- 4- 4	Q インターネットでの電子商取引の増加に伴う情報量の増加にあたって、情報の集積とともにデータの保護対策をより強化していますか？ (インターネットでの一般消費者向けの電子商取引では、取引のピークが非常に高くなることがあります。データの保護対策においても、これへの配慮が必要です。)		●	●	4.4.4.2
	インターネットからの攻撃	4- 3- 4- 5	Q Webサーバに対し、インターネットからの攻撃を想定して対策を行っていますか？ (インターネットに接続されるWebサーバは、不正アクセスやDDoS攻撃に対する対策を実施する必要があります。)		●		
	Dos攻撃対策	4- 3- 4- 5- 1	Q Dos攻撃対策を行っていますか？ (Dos攻撃の対策として、ISPと連携して攻撃を遮断する体制が必要です。)		●		
	アタック対策	4- 3- 4- 5- 2	Q 不正侵入のアタックへの対策を行っていますか？ (不正侵入を防ぐ対策として、ファイアウォール、アクセス管理、セキュリティホール対策、パスワード管理といった対策が必要です。)		●		
	セキュリティホール対策	4- 3- 4- 5- 3	Q 迅速なセキュリティホール対策(CERT／CC等の情報に基づき早急なパッチ当てなど)を行っていますか？ (サーバやクライアントについて、OSやミドルウェアのセキュリティホールへの対策を行うために、ソフトウェアベンダやCERT／CC等から出されるセキュリティホール対策を実施する必要があります。)		●		
	コンピュータウイルス対策	4- 3- 4- 5- 4	Q コンピュータウイルス対策を行っていますか？ (コンピュータウイルス対策として、利用者の教育、ワクチンの利用といった対策を実施する必要があります。)		●		
	スパムメール対策	4- 3- 4- 5- 5	Q スパムメール対策を行っていますか？ (社員の教育とともに、スパムメールを送付したアドレスからのメールをフィルタリングするといった対策が必要です。)		●		
	改ざん対策	4- 3- 4- 5- 6	Q クロスサイトサブスクリプション対策(信用のできない他サイトへリンクしない)を行っていますか？ (自社のホームページからリンクを張るURLについて、その信用度等を調査する仕組みが必要です。)		●		
5．ネットワーク機器対応	ネットワーク機器、サーバの信頼性	4- 3- 4- 6	Q 電子商取引に利用するネットワーク機器、サーバなどの信頼性(二重化や負荷分散)は十分ですか？ (ハードウェア障害に対する対策としての二重化等が必要です。)		●		
	ネットワーク機器、サーバの性能	4- 3- 4- 7	Q 電子商取引に利用するネットワーク機器、サーバなどの性能(能力)は十分ですか？ (電子商取引では、利用トランザクションに大きなピークを持つ場合があり、これに対する対策としての負荷分散や十分な容量を持たせることが必要です。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
E-Commerce	E-Commerce	4－3－(4)E-Commerce					
6．インターネット接続管理	インターネット接続の規制	4- 3- 4- 8	Q インターネットの利用について規制していますか？ (社内からのインターネットの利用について、不適切サイトの閲覧禁止等を規定する必要があります。)		●		
	インターネット接続機器管理	4- 3- 4- 9	Q インターネットと接続する機器の管理を行っていますか？ (インターネットに接続する機器の管理を適切に行い、インターネット経由での不正アクセス等を防止する必要があります。)		●		
	ファイアウォール管理	4- 3- 4- 9- 1	Q ファイアウォールの管理(性能、情報セキュリティ、ログ)を行っていますか？ (ファイアウォールについて、アクセス数と処理能力、セキュリティホールのパッチ、ログ分析といった管理を適切に実施する必要があります。)		●		
	IDS	4- 3- 4- 9- 2	Q IDS(設置されている場合)の管理を行っていますか？ (侵入検知システムを設置している場合、検知対象の設定や、アラームへの対応を適切に管理する必要があります。)		●		
	DNS管理	4- 3- 4- 9- 3	Q DNS(設置されている場合)の管理を行っていますか？ (DNSを設置している場合、セキュリテイホールのパッチ、稼働率の監視、アドレス設定の変更といった管理を適切に行う必要があります。)		●		
	暗号	4- 3- 4- 9- 4	Q ユーザ情報や購入情報などの転送にあたって、暗号を利用し、その暗号鍵の管理、デジタル署名を管理していますか？ (ユーザの個人情報やカード番号等を伝送する時には、暗号を利用し、情報の漏えいを防止する必要があります。また、暗号を利用している場合は、暗号鍵の管理や個人認証機能を適切に管理する必要があります。)		●		
	暗号利用に関する通知	4- 3- 4- 9- 5	Q ユーザに暗号利用に関して通知していますか？ (暗号を利用しているか否かについて、利用者に通知することが必要です。)		●		
	不正行為監視	4- 3- 4- 9- 6	Q 利用者への詐欺行為を監視(チェック)していますか？ (利用者が不正な取引を行った場合、その情報が適切に収集される仕組みが必要です。)		●		[4.4.2.4]
7．電子的証拠	デジタル署名	4- 3- 4- 10	Q 改ざん防止が必要な場合、デジタル署名や電子認証サービスを利用していますか？ (改ざん防止や否認防止が必要な場合には、デジタル署名や電子認証サービスを適切に利用することが必要です。)		●		
	時刻証明	4- 3- 4- 11	Q 時刻などの証明が必要な場合、時刻証明を利用していますか？ (取引の時刻を証明することが必要な場合は、タイムスタンプサービスを利用する必要があります。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
電子メール	電子メール	4－3－(5)電子メール					
1．実施基準	電子メール利用対策	4－ 3－ 5－ 1	Q 実施基準に電子メール利用対策を定めていますか？ (電子メールの利用について、業務上の必要性に基づいた適切な管理を行う必要があります。)		●	●	(4.4.3)
	ユーザ利用	4－ 3－ 5－ 1－ 1	Q 実施基準に電子メールのユーザの利用を定めていますか？ (実施基準で、電子メールのユーザIDの管理、パスワードの管理、使用目的等を規定する必要があります。)		●	●	[4.4.2.4]
	サーバ管理	4－ 3－ 5－ 1－ 2	Q 実施基準に電子メールサーバの管理を定めていますか？ (電子メールサーバの構成管理、変更管理、運用管理等について、実施基準で定める必要があります。)		●		(4.4.1)
	インターネット利用	4－ 3－ 5－ 1－ 3	Q 実施基準にインターネット利用に関する対策を定めていますか？ (電子メールをインターネットを通じてやり取りする場合、盗聴防止、改ざん防止、到達確認等について、メールの重要度に応じた対策が必要です。)		●	●	
2．メールサーバ管理	メールサーバのデータ保護対策	4－ 3－ 5－ 2	Q メールサーバはデータの改ざんから保護されていますか？ (メールサーバは、不正アクセス防止対策を徹底する必要があります。)		●		(4.4.4.2)
	メールサーバへの攻撃	4－ 3－ 5－ 3	Q メールサーバに対しスパム攻撃を想定して対策を行っていますか？ (メールの発信アドレスで、スパムメールをフィルタリングする等の対策が必要です。)		●		
	Dos攻撃対策	4－ 3－ 5－ 3－ 1	Q Dos攻撃対策を行っていますか？ (Dos攻撃を受けた場合、ISPとの連絡を含めた対策をあらかじめ用意しておくことが必要です。)		●		
	不正アクセス対策	4－ 3－ 5－ 3－ 2	Q 不正アクセス対策を行っていますか？ (不正なアクセスを防ぐ対策として、ファイアウォール、アクセス管理、セキュリティホール対策、パスワード管理といった対策が必要です。)		●		
	セキュリティホール対策	4－ 3－ 5－ 3－ 3	Q セキュリティホール対策を行っていますか？ (サーバやクライアントについて、OSやミドルウェアのセキュリティホールへの対策を行うために、ソフトウェアベンダやCERT／CC等から出されるセキュリティホール対策を実施する必要があります。)		●		
	コンピュータウイルス対策	4－ 3－ 5－ 3－ 4	Q コンピュータウイルス対策を行っていますか？ (コンピュータウイルス対策として、利用者の教育、ワクチンの利用などを実施する必要があります。)		●		
	不正メール転送	4－ 3－ 5－ 3－ 5	Q 不正を招くおそれのあるメール転送を禁止していますか(例：社外経由で自社メールを転送するなど)？ (社外のアドレスから発信されたメールを社外に転送する、メーリングリストのアドレスは特定のユーザのみの使用に制限する、といった対策が必要です。)		●		[4.4.2.4]

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	Ⅳ－3. 不正アクセス・コンピュータウイルス関連					
電子メール	電子メール	4－3－(5)電子メール					
3．ネットワーク機器管理	ネットワーク機器、サーバの信頼性	4－ 3－ 5－ 4	Q 電子メールのネットワーク機器、サーバの信頼性は十分にありますか？ (電子メールも普及すると、仕事に欠かせないミッションクリティカルなシステムになります。この重要度に見合った信頼性を確保する必要があります。)		●		
	ネットワーク機器、サーバの性能	4－ 3－ 5－ 5	Q 電子メールのネットワーク機器、サーバなどの性能(能力、記憶容量)は十分にありますか？ (電子メールも使用量に高いピークが出ることがあるので、それに耐える処理能力と記憶容量を備える必要があります。)		●		
	インターネット接続機器管理	4－ 3－ 5－ 6	Q インターネットと接続する機器の管理を行っていますか？ (インターネットに接続する機器の管理を適切に行い、インターネット経由での不正アクセス等を防止する必要があります。)		●		
	ファイアウォール管理	4－ 3－ 5－ 6－ 1	Q ファイアウォールの管理(性能、情報セキュリティ、ログ)を行っていますか？ (ファイアウォールについて、アクセス数と処理能力、セキュリティホールのパッチ、ログ分析といった管理を適切に実施する必要があります。)		●		
	DNS管理	4－ 3－ 5－ 6－ 2	Q DNS(設置している場合)の管理を行っていますか？ (DNSを設置している場合、セキュリティホールのパッチ、稼働率の監視、アドレス設定の変更といった管理を適切に行う必要があります。)		●		
	暗号	4－ 3－ 5－ 6－ 3	Q 暗号の利用と暗号鍵の管理、デジタル署名の管理を行っていますか？ (機密度の高い情報を電子メールでやり取りする時には、暗号を利用し、情報の漏えいを防止する必要があります。また、暗号を利用している場合は、暗号鍵の管理や個人認証機能を適切に管理する必要があります。)		●		
	不正行為監視	4－ 3－ 5－ 6－ 4	Q 利用者の不正行為を監視(チェック)していますか？ (利用者が業務以外の不正な目的で電子メールを使った場合、その情報が適切に収集される仕組みが必要です。)		●		[4.4.2.4]
4．デジタル署名	デジタル署名	4－ 3－ 5－ 7	Q 改ざん防止が必要な場合、デジタル署名や電子認証サービスを利用していますか？ (改ざん防止や否認防止が必要な場合には、デジタル署名や電子認証サービスを適切に利用することが必要です。)		●		
5．悪質メール対策	添付ファイル	4－ 3－ 5－ 8	Q 添付ファイルによる悪意のあるプログラムを阻止する対策がありますか？ (受信した電子メールの添付ファイルについて、不正プログラムの検出と駆除を実施する必要があります。)		●		
	スクリプト	4－ 3－ 5－ 9	Q メールとともに送られてくる不正スクリプトを防止する対策がありますか？ (テキスト以外の形式で送られた電子メールについて、不正スクリプトの検出と駆除を実施する必要があります。)		●		
	不正メール対策	4－ 3－ 5－ 10	Q 送信元のないメールや悪意のあるメールを防止する対策がありますか？ (メールヘッダのアドレスがなかったり、ブラックリストに載っている電子メールをブロックすることが必要です。)		●		
6．転送エラー対策	転送エラー	4－ 3－ 5－ 11	Q 電子メールの不用意な転送エラーによる重要な情報の漏えい対策を行っていますか？ (重要な情報を送る時の手続として、複数の人間がチェックを行うといった対策が必要です。特に、多数のアドレスを含んだメーリングリストを取り扱う時は注意が必要で、BccとCcを間違えると、全メンバーにアドレスを公開したと同じことになります。)		●	●	4.4.4.2

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
災害対策	災害対策	Ⅳ－4. 災害対策					
1．実施基準	災害対策	4- 4- 1- 1	Q 実施基準に災害対策を定めていますか？ (実施基準またはそれと同等とみなされるものに、災害対策(特に以下1～3の第5階層レベルに示す対象)を定めていますか？)		●	●	4.4.4.2
	自然災害対策	4- 4- 1- 1- 1	Q 実施基準に自然災害対策を定めていますか？ (用語解説「自然災害対策」:地震・津波・噴火、台風・高潮、水災・洪水、竜巻・風災、落雷、雪害、雹害、天候不良・異常気象のうち、必要と思われる災害を対象とした対策をいいます。)		●	●	
	事故災害対策	4- 4- 1- 1- 2	Q 実施基準に事故災害対策を定めていますか？ (用語解説「事故災害対策」:火災・爆発、停電、人的損失(航空機事故・列車事故・交通事故等)、漏水、動物害のうち、必要と思われる災害を対象とした対策をいいます。)		●	●	
	人的災害対策	4- 4- 1- 1- 3	Q 実施基準に人的災害対策を定めていますか？ (用語解説「人的災害対策」:戦争、動乱、暴動、テロなど、および自然災害、事故災害に便乗又は影響を受けて行動する人の災害についての対策をいいます。)		●	●	[4.4.2.4]
2．管理	経営者の決定	4- 4- 1- 2	Q 災害リスク対策の採用の可否について経営者によって決定されていますか？ (災害リスクの対策を採用するにあたっては、責任ある経営者の承認を受けているかを確認します。)		●	●	
	災害復旧レベル	4- 4- 1- 3	Q 災害復旧のレベルに関してあらかじめ段階的に決められていますか？ (災害復旧のレベル(特に以下1～3の第5階層レベルに示す内容の水準)に関して、無理、無駄のない復旧計画を定めているかを確認します。)		●	●	
	事業再開	4- 4- 1- 3- 1	Q 事業再開のための最低限のレベルを決めていますか？ (事業の継続性を確保できる最低限の必要事項とその条件を決めているかを確認します。)		●		
	災害復旧レベル	4- 4- 1- 3- 2	Q 災害復旧にあたって、平常時に必要な水準レベルを決めていますか？ (災害復旧にあたって、平常な状態にするための必要項目と条件を決めているかを確認します。)		●		
	改善レベル	4- 4- 1- 3- 3	Q 復旧にあたって、災害以前以上の改善レベルを決めていますか？ (災害復旧にあたって、復旧作業の過程で災害発生以前の状態をさらに改善する項目と、その条件を決めているかを確認します。)		●		
	是正措置	4- 4- 1- 4	Q 復旧手順について不具合があった場合、是正処置をとっていますか？ (復旧手順は定期的に見直しを行い、必要な是正処置を取ることが明確に定められ、実行されているかを確認します。)		●		
	避難対策	4- 4- 1- 5	Q 経営者、スタッフの避難対策を実施していますか？ (経営者およびスタッフの災害発生時の避難対策が明確に示されているか、また、関係者がそれを理解しているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
災害対策	災害対策	Ⅳ－4. 災害対策					
3．防火対策	防火壁	4－ 4－ 1－ 6	Q 防火壁を採用していますか？ (以下1～4の第5階層レベルに示す箇所の壁が防火壁になっているかを確認します。)		●		
	コンピュータ室	4－ 4－ 1－ 6－ 1	Q コンピュータ室に防火壁を採用していますか？ (用語解説「コンピュータ室」:コンピュータ室にはサーバ設置場所を含みます。)		●		
	データ保管場所	4－ 4－ 1－ 6－ 2	Q データ保管場所に防火壁を採用していますか？ (用語解説「ネットワーク保管場所」:データ保管場所として独立しているか否かに関係なく、事業の継続性を確保するために必要なデータを保管している場所を指します。)		●		
	ネットワーク設備室	4－ 4－ 1－ 6－ 3	Q ネットワーク設備室に防火壁を採用していますか？ (用語解説「ネットワーク設備室」:ネットワーク設備室にはサーバ設置場所を含みます。)		●		
	コンピュータ設置場所	4－ 4－ 1－ 6－ 4	Q コンピュータ設置場所に防火壁を採用していますか？ (用語解説「コンピュータ設置場所」:コンピュータ(パソコンを除く)設置場所にはサーバ設置場所を含みます。)		●		
	自動消火装置	4－ 4－ 1－ 7	Q 自動消火装置を設置していますか？ (以下1～4の第5階層レベルに示す箇所に自動消火装置を設置し、定期的に機能確認を行っているかを確認します。)		●		
	コンピュータ室	4－ 4－ 1－ 7－ 1	Q コンピュータ室に自動消火装置を設置していますか？		●		
	データ保管場所	4－ 4－ 1－ 7－ 2	Q データ保管場所に自動消火装置を設置していますか？		●		
	ネットワーク設備室	4－ 4－ 1－ 7－ 3	Q ネットワーク設備室に自動消火装置を設置していますか？		●		
	コンピュータ設置場所	4－ 4－ 1－ 7－ 4	Q コンピュータ設置場所に自動消火装置を設置していますか？		●		
	区画放出対応消火システム	4－ 4－ 1－ 8	Q 区画放出対応消火システムを採用していますか？ (以下1～3の第5階層レベルに示す場所に該当区間のみに対応する区画放出対応の消火システムを採用し、定期的に機能確認を行っているかを確認します。)		●		
	コンピュータ室	4－ 4－ 1－ 8－ 1	Q コンピュータ室に区画放出対応消火システムを採用していますか？		●		
	データ保管場所	4－ 4－ 1－ 8－ 2	Q データ保管場所に区画放出対応消火システムを採用していますか？		●		
	ネットワーク設備室	4－ 4－ 1－ 8－ 3	Q ネットワーク設備室に区画放出対応消火システムを採用していますか？		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
災害対策	災害対策	Ⅳ－4. 災害対策					
3．防火対策	消火器	4- 4- 1- 9	Q 消火器を設置していますか？ (以下1～4の第5階層レベルに示す箇所に消火器を設置し、定期的に機能確認を行っているかを確認します。)		●	●	
	コンピュータ室	4- 4- 1- 9- 1	Q コンピュータ室に消火器を設置していますか？		●		
	データ保管場所	4- 4- 1- 9- 2	Q データ保管場所に消火器を設置していますか？		●		
	ネットワーク設備室	4- 4- 1- 9- 3	Q ネットワーク設備室に消火器を設置していますか？		●		
	コンピュータ設置場所	4- 4- 1- 9- 4	Q コンピュータ設置場所に消火器を設置していますか？		●		
	消火栓	4- 4- 1- 10	Q 消火栓を設置していますか？ (以下1～4の第5階層レベルに示す箇所に消火栓を設置しているかを確認します。)		●		
	コンピュータ室	4- 4- 1- 10- 1	Q コンピュータ室設置フロアに消火栓を設置していますか？		●		
	データ保管場所	4- 4- 1- 10- 2	Q データ保管場所設置フロアに消火栓を設置していますか？		●		
	ネットワーク設備室	4- 4- 1- 10- 3	Q ネットワーク設備室設置フロアに消火栓を設置していますか？		●		
	コンピュータ設置場所	4- 4- 1- 10- 4	Q コンピュータ設置フロアに消火栓を設置していますか？		●		
	遮断装置	4- 4- 1- 11	Q 遮断装置を設置していますか？ (以下1～4の第5階層レベルに示す箇所に、炎、煙、有毒ガス等の拡散を防ぐ遮断装置を設置し、定期的に機能確認を行っているかを確認します。)		●		
	コンピュータ室	4- 4- 1- 11- 1	Q コンピュータ室に遮断装置を設置していますか？		●		
	データ保管場所	4- 4- 1- 11- 2	Q データ保管場所に遮断装置を設置していますか？		●		
	ネットワーク設備室	4- 4- 1- 11- 3	Q ネットワーク設備室に遮断装置を設置していますか？		●		
	コンピュータ設置場所	4- 4- 1- 11- 4	Q コンピュータ設置場所に遮断装置を設置していますか？		●		
	2方向非常口	4- 4- 1- 12	Q 経営者、スタッフの避難対策として2方向非常口を設置していますか？ (経営者、スタッフの緊急時の避難対策として、常に2方向以上の非常口を設置し、常時使用可能な状態で維持されているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
災害対策	災害対策	Ⅳ－4. 災害対策					
4．耐震対策	フリーアクセス耐震補強	4- 4- 1- 13	Q コンピュータ室ではフリーアクセスの耐震補強を実施していますか？ (コンピュータ室(サーバ設置場所を含む)では、フリーアクセスの耐震補強として支柱の補強を行っているかを確認します。)		●		
	コンピュータ機器の固定	4- 4- 1- 14	Q コンピュータ室では耐震対策としてコンピュータ機器を固定していますか？		●		
	転倒防止	4- 4- 1- 15	Q コンピュータ室では耐震対策としてコンピュータ機器の転倒防止策をとっていますか？		●		
	機器・ラックの固定	4- 4- 1- 16	Q データ保管場所では耐震対策として機器およびラックを固定していますか？		●		
	テープ落下防止策	4- 4- 1- 17	Q データ保管場所では耐震対策としてテープ等の落下防止策をとっていますか？		●		
	機器の落下防止策	4- 4- 1- 18	Q コンピュータ設置場所では耐震対策として機器の落下防止策をとっていますか？		●		
	電源設備	4- 4- 1- 19	Q 電源設備の耐震対策として機器の転倒防止、固定をしていますか？ (用語解説：主として情報システムへ電気を供給する設備に対する耐震対策をいいます。)		●		
5．水害対策	コンピュータ室	4- 4- 1- 20	Q コンピュータ室の浸水対策として浸水のおそれのない場所に設置していますか？		●		
	上げ床	4- 4- 1- 21	Q コンピュータ室の浸水対策として上げ床にしていますか？		●		
	防水堤・ピット	4- 4- 1- 22	Q コンピュータ室の浸水対策として防水堤およびピットを設置していますか？		●		
	漏水検知機	4- 4- 1- 23	Q コンピュータ室の浸水対策として漏水検知機を設置していますか？		●		
	排水口	4- 4- 1- 24	Q コンピュータ室の浸水対策として排水口を設置していますか？		●		
	水落下防止策	4- 4- 1- 25	Q 基幹システムに対する漏水対策として、天井配管から水落下のおそれのない場所に設置していますか？		●		
	吹込み対策	4- 4- 1- 26	Q 基幹システムに対する漏水対策として、窓からの雨水の吹込みのおそれのない場所に機器を設置していますか？		●		
	防水シート	4- 4- 1- 27	Q 基幹システムに対する漏水対策として防水シートの準備をしていますか？		●		
	電源設備	4- 4- 1- 28	Q 電源設備の水害対策として防水堤を設置していますか？ (用語解説「水害対策」：主として情報システムへ電気を供給する設備に対する水害対策をいいます。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
障害対策	障害対策	Ⅳ－5. 障害対策					
1．実施基準	障害対策	4- 5- 1- 1	Q 実施基準に障害対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、以下1～3の第5階層レベルに示す対象の障害対策を定めているかを確認します。)		●	●	(4.4.4)
	ハードウェア障害対策	4- 5- 1- 1- 1	Q 実施基準にハードウェア障害対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、ハードウェアの正常機能に支障をきたす障害が発生した場合の対策を定めているかを確認します。)		●	●	
	ソフトウェア障害対策	4- 5- 1- 1- 2	Q 実施基準にソフトウェア障害対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、ソフトウェアの正常機能に支障をきたす障害が発生した場合の対策を定めているかを確認します。)		●	●	
	運用ミス障害	4- 5- 1- 1- 3	Q 実施基準に運用ミス障害対策を定めていますか？ (実施基準又はそれと同等とみなされるものに、運用ミスによって情報システムの正常運用に支障をきたす障害が発生した場合の対策を定めているかを確認します。)		●	●	
2．管理	障害対策	4- 5- 1- 2	Q 情報システムの障害対策を実施していますか？ (情報システムの機能に支障をきたす障害の対策として、以下1～5の第5階層レベルに示す対策を実施しているかを確認します。)		●		
	運用監視機能	4- 5- 1- 2- 1	Q 運用監視機能を設置していますか？		●		
	障害検出機能	4- 5- 1- 2- 2	Q 障害検出機能を設置していますか？ (情報システムの機能に支障をきたす障害が発生した場合、その障害を検出する機能を有しているかを確認します。)		●		
	縮退運転機能	4- 5- 1- 2- 3	Q 縮退運転機能を設置していますか？ (情報システムの機能に支障をきたす障害が発生した場合、通常の運転の一部を制限し、その障害の影響を受けない機能についてのみ運転を継続させる機能を有しているかを確認します。)		●		
	代替運転機能	4- 5- 1- 2- 4	Q 代替運転機能を設置していますか？ (情報システムの機能に支障をきたす障害が発生した場合、他の情報システムに運転を代えることのできる機能を有しているかを確認します。)		●		
	回復機能	4- 5- 1- 2- 5	Q 回復機能を設置していますか？ (情報システムの機能に支障をきたす障害が発生した場合、障害発生の状況によって情報システムの機能を正常に回復させる機能を有しているかを確認します。)		●		
	サービスレベル	4- 5- 1- 3	Q 障害対策に関してサービスレベルを取り決めていますか？ (特に、アウトソーシングの場合、以下1～4の第5階層レベルに示すサービスのレベルを明確にし、両者の合意を得ているかを確認します。)		●	●	
	ポリシーとの整合性	4- 5- 1- 3- 1	Q SLA(サービスレベル合意)で取り決めた内容は、情報セキュリティポリシーの要件を満たしていますか？ (SLA(Service Leve Agreement)で取り決めた内容が、情報セキュリティポリシー又はそれと同等とみなされるものと整合がとれているかを確認します。)		●	●	
	管理責任者の承認	4- 5- 1- 3- 2	Q SLAで示された内容に関して、アプリケーションの管理責任者の承認を得ていますか？ (SLAで示された内容に関して、アプリケーションの管理責任者の承認を得ていることが第三者にわかるようになっているかを確認します。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
障害対策	障害対策	Ⅳ－5. 障害対策					
3．手続	トランザクション量	4- 5- 1- 3- 3	Q SLAでシステムへ入力するトランザクション量が示されていますか？ (用語解説「トランザクション量」:データの更新処理・ファイルの検索処理などの量を指します。)		●	●	
	トランザクション量の測定	4- 5- 1- 3- 4	Q SLAで示されたシステムへ入力するトランザクション量は、定期的に測定を行い、結果を記録していますか？ (SLAで示された該当システムへ入力するトランザクション量は定期的に測定し、結果を記録しているか、又測定結果のトランザクション量が当初SLAで示した内容と大幅に差があった場合、必要に応じてSLAの内容を見直しているかを確認します。)		●		
4．情報システム	ソフトウェア更新手続	4- 5- 1- 4	Q ソフトウェアの更新手続について明確になっていますか？ (ソフトウェアの更新手続について、特に以下の1～3の第5階層レベルに示す内容について明確に示されているかを確認します。)		●	●	
	最終テスト結果確認	4- 5- 1- 4- 1	Q アプリケーションの管理責任者が最終テスト結果を確認していますか？ (アプリケーションの管理責任者が最終テスト結果を確認し、記録に残しているかを確認します。)		●	●	
	更新記録整備	4- 5- 1- 4- 2	Q すべての更新記録を整備していますか？ (ソフトウェアの更新に関するすべての記録が整備され、閲覧可能な状態になっているかを確認します。)		●		
	記録内容	4- 5- 1- 4- 3	Q 更新記録と許可内容を一致させる手順を明確にしていますか？ (ソフトウェアの更新記録と許可内容を一致させる手順が示され、定期的に見直されているかを確認します。)		●		
	更新確認	4- 5- 1- 5	Q ソフトウェアの更新について、手続どおりに実施されているか、定期的な確認が行われていますか？ (ソフトウェアの更新について、手続どおりに実施されていることを責任ある管理者が定期的に確認しているか、又、確認結果を記録しているかを確認します。)		●		
	ソフトウェア更新	4- 5- 1- 6	Q ソフトウェアの更新手続についての各項目は、その妥当性について定期的に評価し、不具合の是正処置をとっていますか？ (ソフトウェアの更新手続についての各項目を定期的に評価し、不具合があった場合は是正処置をとり、責任ある管理者の承認を得ているかを確認します。)		●		
	障害管理票	4- 5- 1- 7	Q すべての障害についての障害管理票の作成要領を定めていますか？ (情報システムに関する障害について、情報システムの機能に与える影響の大小に関わらず、すべて記録する障害管理票の作成要領を定め、定期的に見直されているかを確認します。)		●		
	変更後障害	4- 5- 1- 8	Q プログラム変更後に障害が発生した時に、変更前のプログラムに戻す手続が文書化されていますか？ (プログラム変更後に障害が発生した場合、ただちに変更前のプログラムに戻す手続が示されているかを確認します。)		●		
5．ユーティリティ	ディスク障害対策	4- 5- 1- 9	Q ディスク障害対策として、重要なディスクドライブは冗長な構成がとられていますか？ (ディスク障害対策として、重要なディスクドライブは余裕のある構成をとっているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
障害対策	障害対策	Ⅳ－5. 障害対策					
5．ユーティリティ	施設障害対策	4- 5- 1- 10	Q 施設の障害対策を講じていますか？ (障害対策として、以下1～6の第5階層レベルに示す内容を講じているかを確認します。)		●		(4.4.4.2)
	適用業務優先順位	4- 5- 1- 10- 1	Q 機器障害発生時における縮退・再編成の際の適用業務の優先順位を決めていますか？ (機器障害が発生した場合、当該機器の運転を一部制限、または機器の構成を再編成して運転を継続する際の適用業務の優先順位を決めているかを確認します。)		●		
	無停電装置	4- 5- 1- 10- 2	Q 主要な機器の電源は無停電装置(自家発電装置を含む)から供給されていますか？ (事業の継続性から見て、主要な機器と主要でない機器が明確に区分され、特に主要な機器についての電源が無停電装置から供給されているかを確認します。)		●		
	無停電装置テスト	4- 5- 1- 10- 3	Q 設置した無停電装置(自家発電装置を含む)は定期的にテストが行われていますか？ (設置した無停電装置は定期的にテストを行い、結果を記録しているかを確認します。)		●		
	供給能力	4- 5- 1- 10- 4	Q 無停電装置の供給能力は、計画された拡張も含む機器構成に対して十分ですか？ (無停電装置(自家発電装置を含む)の供給能力は、計画が承認されている拡張も含む機器構成に対して十分か否かを確認し、十分でない場合は供給能力向上の処置を講じているかを確認します。)		●		
	空調設備の多重化	4- 5- 1- 10 5	Q 空調設備は、室内設備および屋外設備ともに多重化されていますか？ (空調設備はその種類に係わらず多重化され、不測の事態でも機能を維持することができるかを確認します。)		●		
	水冷	4- 5- 1- 10- 6	Q 空調設備が水冷の場合、水冷用の予備水を確保していますか？ (空調設備(室外機にクーリングタワーを使っているなど)が水冷の場合、水冷用の予備水を確保しているかを確認します。)		●		
6．ネットワーク対策	回線障害対策	4- 5- 1- 11	Q 回線障害対策を実施していますか？ (回線障害対策として、以下1～2の第5階層レベルに示す内容を実施しているかを確認します。)		●		
	避雷針	4- 5- 1- 11- 1	Q 交換機に避雷針を設置していますか？ (情報システムの運用に関わる交換機に避雷針を設置しているかを確認します。)		●		
	ネットワーク障害対策	4- 5- 1- 11- 2	Q ネットワーク障害対策を実施していますか？ (ネットワークに障害が発生した場合、情報システムの運用に与える影響を最小限にする対策を講じているかを確認します。)		●		
7．復旧	復旧レベル	4- 5- 1- 12	Q 障害復旧のレベルを定めていますか？ (情報システムに係わる障害が発生した場合の復旧レベルを段階的に定めているかを確認します。)		●	●	
	代替手段	4- 5- 1- 12- 1	Q 必要な場合の代替手段を講じていますか？ (情報システムに係わる障害が発生した場合、必要に応じて代替手段(ハードウェア、機器、設備、回線、要員など情報システムの運用に関するすべて)を講じることができるかを確認します。)		●	●	
	是正措置	4- 5- 1- 12- 2	Q 復旧手順について不具合があった場合、是正処置をとっていますか？ (復旧手順を定期的に見直し、必要な是正処置を取ることが明確に定められ、実行されているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
その他	その他	Ⅳ－6. その他関連項目					
1．実施基準	その他関連項目	4- 6- 1- 1	Q 実施基準にその他関連項目を定めていますか？ (リスク対策は主要なリスクについて実施することが一般的ですが、その場合、主要なものと定めたもの以外のリスクが発生することもあります。そのため、その他の関連するリスクについても対応を定める必要があります。)		●	●	4.2
	経営リスク	4- 6- 1- 1- 1	Q 実施基準に経営リスクに関する対策を定めていますか？ (経営リスクは事業運営によって発生するリスク(法務リスク、事務リスクなど)のほかに、経営者の判断による事業戦略リスク(価格戦略、商品戦略、設備投資など)もあります。これらのリスクのうち、主要なリスクとして選定されなかったリスクに対する対策を実施基準に定める必要があります。)		●	●	
	政治・経済・社会リスク	4- 6- 1- 1- 2	Q 実施基準に政治・経済・社会リスクに関する対策を定めていますか？ (政治・経済・社会リスクには戦争、通商問題、税務問題、為替変動、消費者運動などさまざまなリスクがあります。これらのうち、主要なリスクとして選定されなかったリスクに対する対策を実施基準に定める必要があります。)		●	●	
	テロ対策	4- 6- 1- 1- 3	Q 実施基準にテロに対する対策を定めていますか？ (テロリスクは日本では比較的リスクが少ないとされています。リスク評価により対策が不要と判断された場合にはその他のリスクが万一発生した場合の対策で対応できるか、確認が必要です。)		●	●	
2．サービス提供	会員規約	4- 6- 1- 2	Q サービス提供にあたって利用者の会員規約を定めていますか？ (会員制のサービス、たとえば電子掲示板などのサービスの場合、サービスの安定的な供給に資するために利用者に対して実施してはならないこと(誹謗中傷の禁止、著作権違反の禁止など)について明確に定めた会員規約を定めるべきです。)		●	●	(4.4.3) [4.4.2.4]
	規約違反	4- 6- 1- 3	Q サービス提供の停止となる規約違反事項を明確にし、会員に説明していますか？ (サービスの安定供給に資するため、違反した場合は会員資格の停止や契約の解除などの処置の対象となる規約違反事項を明確にし、会員に説明し、そのような違反がないようにする必要があります。当然違反が発生した場合は規約に従って厳正に対処する必要があります。)		●	●	
	通信の秘密保護教育	4- 6- 1- 4	Q サービス提供の実務に携わっている管理者に対し、「通信の秘密保護(電気通信事業法第4条)」について教育を行っていますか？ (メールサービスなどを行っている場合、管理者として場合によってメールを読む機会があります。その場合でもそこで得た情報については守秘義務があり、他人にみだりに漏らした場合処罰されることを教育し、不祥事発生を防ぐ必要があります。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
その他	その他	Ⅳ－6. その他関連項目					
3．ユーザ間トラブル	ユーザ間トラブル対策の決定	4- 6- 1- 5	Q ユーザとの間のサービス、契約等に関するトラブルリスクの対策を採用するか否かについて、経営者が決定していますか？ (企業が提供しているメールサービス、掲示板サービスなどを利用してユーザ同士が誹謗中傷や著作権争いなどを起こした場合、その対応策をどこまで実施するかについて経営者が判断する必要があります。)		●	●	
	ユーザ間トラブル対策	4- 6- 1- 5- 1	Q ユーザ間トラブルリスクについて、分析の結果、対策を講じていますか？ (企業が提供しているメールサービス、掲示板サービスなどを利用してユーザ同士が誹謗中傷や著作権争いなどを起こすリスクの発生頻度と企業の被る影響度を分析し、対応策を実施するか否かも含め、対策を検討・実施する必要があります。)		●	●	
	法的責任・事後対応	4- 6- 1- 5- 2	Q 会員が提供しているサービスを利用して違法行為を行った場合について事前にシナリオを作成し、サービス提供企業(自社)の法的責任および事後対応について検討していますか？ (リスクの発生が十分予想されるものに対してはあらかじめ事件が起きることを想定した対応計画(コンティンジェンシープラン)が必要です。このような従来にはなかった新たなリスクについては事件や事故が実際に起こる前に事前に十分な検討が必要です。このケースは会員が違法行為を行った場合を想定しています。)		●	●	
	法的責任・事後対応対象	4- 6- 1- 5- 3	Q 会員間で提供しているサービスの利用の結果トラブルが発生した場合について事前にシナリオを作成し、サービス提供企業(自社)の法的責任および事後対応について対象を定めていますか？ (このケースは会員同士のトラブルの発生を想定しています。たとえばネットオークションや掲示板の運営などがあげられます。)		●	●	
4．苦情処理対応	苦情処理対応の決定	4- 6- 1- 6	Q 苦情処理対応トラブルリスクの対策を採用するか否かについて、経営者および責任者が決定していますか？ (製品サービスは不良がないよう万全な対応を講じていくことは当然ですが、それでも人間が行うためにミスや事故を皆無にすることはできません。その場合の苦情の受付方法如何によっては不誠実であるという風評の拡大など、新たなリスクが生じる可能性があります。そのため苦情対応の対応策の採用の可否は経営者と責任者が関与する必要があります。)		●	●	4.4.7
	苦情処理対応策	4- 6- 1- 6- 1	Q 苦情処理対応におけるトラブルリスクについて対策を講じていますか？ (苦情対応処理の失敗によるトラブルのリスク対応が必要であると判断された場合、その対策を実施する必要があります。)		●	●	4.4.7
	苦情処理対応マネジメントシステム	4- 6- 1- 6- 2	Q サービス提供に対する苦情処理対応マネジメントシステムを導入していますか？ (サービス提供に対する苦情は一定程度発生するものとして、その対応を組織的に実施するためJIS Z 9920(苦情対応マネジメントシステムの指針)に則った対応を構築することが必要です。)		●	●	4.4.7

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
その他	その他	Ⅳ－6. その他関連項目					
5．危機管理計画徹底	危機管理計画の内外関係者への徹底	4- 6- 1- 7	Q 危機管理計画は、資産の喪失・破壊に関してユーザ、アウトソーサも含め関係者に周知徹底されていますか？ (資産の喪失破壊など物理的な被害が発生した場合の危機管理計画について、自社(ユーザ部門を含む)はもちろんのこと、ユーザ(顧客)や関連企業、委託企業などアウトソーサに対しても十分説明し、万一の場合には協力して行動してもらうよう徹底することが必要です。)		●	●	
	物的資産喪失・破壊	4- 6- 1- 7- 1	Q 物的資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？ (用語解説「物的資産の喪失・破壊」:社屋、生産設備、什器備品、メインフレーム、サーバ、モデム、ルータ、ディスク、テープ、FD、MO、CD-R、パソコンなどすべての資産が火災や洪水、地震、破壊行為などにより使用できなくなることをいいます。)		●	●	
	情報資産喪失・破壊	4- 6- 1- 7- 2	Q 情報資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？ (用語解説「情報資産の喪失・破壊」:サーバ、ディスク、FD、パソコンなど情報機器に存在するデータおよびプログラム、コンテンツなどが物理的な破壊や電子的な消去などで使用不能になることです。なお、広く考える場合は紙に打ち出したデータや稟議書、計画書などの情報、ノウハウなど個人の頭の中にある情報などを含めることもあります。)		●	●	
	その他資産喪失・破壊	4- 6- 1- 7- 3	Q その他の資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？ (用語解説「その他の資産」:物的資産、情報資産以外には、人員の損失など人的資産、ブランド価値などの無形資産などがあります。)		●	●	

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
バックアップ	バックアップ	Ⅳ－7. バックアップ					
1．実施基準	バックアップ対策	4- 7- 1- 1	Q 実施基準にバックアップ対策を定めていますか？ (実施基準又はそれと同等とみなされるものには、情報システム上、必要とされるデータ又はプログラムのファイルのバックアップ対策が定められているかを確認します。) (用語解説「バックアップ対策」:別の記録媒体に同じものをコピーして保存する措置をとることをいいます。)		●	●	(4.2)
2．二重化対策	二重化対策	4- 7- 1- 2	Q 情報システムのバックアップ対策(二世代保存を含む)を実施していますか？ (情報システム上、必要なもの(特に以下1～4の第5階層レベルに示す内容のもの)についてバックアップ対策(二世代保存を含む)を実施しているかを確認します。) (用語解説「二世代保存」:現在の状態と、現在の状態に更新する1つ前の状態を保存することをいいます。)		●		(4.4.4.2)
	交換機、チャネル	4- 7- 1- 2- 1	Q 交換機、チャネルの二重化を行っていますか？		●		
	機器	4- 7- 1- 2- 2	Q 機器の二重化を行っていますか？		●		
	LAN	4- 7- 1- 2- 3	Q LANの二重化を行っていますか？		●		
	WAN	4- 7- 1- 2- 4	Q WANの二重化を行っていますか？		●		
	切替テスト	4- 7- 1- 3	Q バックアップ機器への切替テストが実施され、その結果の評価が行われていますか？ (情報システムのバックアップ用として準備した機器に通常使用している機器からの切替えを行った場合、正常な処理機能が維持されるか否かのテストが定期的に実施されているか、又、その結果を評価して記録しているかを確認します。)		●		
3．ファイルのバックアップ	プログラムバックアップ	4- 7- 1- 4	Q プログラムのバックアップを行っていますか？ (情報システム上必要な各種のプログラムすべてのバックアップ(特に以下1～3の第5階層レベルに示す内容)が確実に行われているかを確認します。)		●		
	実施方法	4- 7- 1- 4- 1	Q プログラムファイルバックアップの実施方法は明確ですか？ (情報システム上必要なプログラムを保存するファイルのバックアップ実施の方法(特にバックアップ頻度・バックアップ取得方法・保管場所)が文書化され、明確に示されているかを確認します。)		●		
	遠隔地保管	4- 7- 1- 4- 2	Q プログラムファイルバックアップの遠隔地保管を行っていますか？ (情報システム上必要なプログラムのバックアップファイルが、通常使用しているコンピュータが設置されている場所から離れた場所で保管されているかを確認します。)		●		
	同一サイト内保管	4- 7- 1- 4- 3	Q プログラムファイルバックアップの同一サイト内保管を行っていますか？ (情報システム上必要なプログラムのバックアップファイルが、通常使用しているコンピュータが設置してある場所と同じ場所に保管されているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
バックアップ	バックアップ	Ⅳ－7. バックアップ					
3．ファイルのバックアップ	OSファイルバックアップ	4- 7- 1- 5	Q OSファイルのバックアップを行っていますか？ (情報システム上必要なOSファイルのバックアップ(特に以下1～3の第5階層レベルに示す内容)が、確実に行われているかを確認します。)		●		
	実施方法	4- 7- 1- 5- 1	Q OSファイルバックアップの実施方法は明確ですか？ (情報システム上必要なOSファイルバックアップの実施の方法(特にバックアップ頻度・バックアップ取得方法・保管場所)が、文書化され明確に示されているかを確認します。)		●		
	遠隔地保管	4- 7- 1- 5- 2	Q OSファイルバックアップの遠隔地保管を行っていますか？ (バックアップされたOSファイルが、通常使用しているコンピュータが設置してある場所から離れた場所で保管されているかを確認します。)		●		
	同一サイト内保管	4- 7- 1- 5- 3	Q OSファイルバックアップの同一サイト内保管を行っていますか？ (バックアップされたOSファイルが、通常使用しているコンピュータが設置してある場所と同じ場所で保管されているかを確認します。)		●		
	データファイルバックアップ	4- 7- 1- 6	Q データファイルのバックアップを行っていますか？ (情報システム上必要なすべてのデータファイルのバックアップ(特に以下1～6の第5階層レベルに示す内容)が確実に行われているかを確認します。)		●	●	
	実施方法	4- 7- 1- 6- 1	Q データファイルバックアップの実施方法は明確ですか？ (情報システム上必要なデータを保存するファイルのバックアップ実施の方法(特にバックアップ頻度・バックアップ取得方法・保管場所)が、文書化され明確に示されているかを確認します。)		●		
	遠隔地ミラーデータ	4- 7- 1- 6- 2	Q データファイルはリアルタイムで遠隔地ミラーデータを作成していますか？ (情報システム上必要なデータが、更新・書込みのつど、データ更新・書込みの行われている場所から離れた場所で、即時に別のデータファイルに同じ内容のものが更新・書込みが行われているかを確認します。)		●		
	遠隔地保管	4- 7- 1- 6- 3	Q データファイルバックアップの遠隔地保管を行っていますか？ (バックアップされたデータファイルが通常使用しているコンピュータが設置してある場所から離れた場所で保管されているかを確認します。)		●		
	同一サイト内保管	4- 7- 1- 6- 4	Q データファイルバックアップの同一サイト内保管を行っていますか？ (バックアップされたデータファイルが通常使用しているコンピュータが設置してある場所と同じ場所で保管されているかを確認します。)		●		
	保存期間	4- 7- 1- 6- 5	Q データの保存期間は示されていますか？ (情報システム上必要なデータの保存期限が明確に文書で示され、確実に実行されているかを確認します。)		●		
	バックアップ頻度	4- 7- 1- 6- 6	Q 機能停止許容時間内に復旧ができる頻度でバックアップを実施していますか？ (特にデータのバックアップが、情報システムの機能が何らかの理由で正常に働かなくなった場合、機能が正常な状態に復旧するまでに許される最短時間の範囲で機能が復旧できるような頻度で行われているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
バックアップ	バックアップ	Ⅳ－7. バックアップ					
3．ファイルのバックアップ	DBファイルバックアップ	4- 7- 1- 7	Q DBファイルのバックアップを行っていますか？ (情報システム上必要なDB(データベース)ファイルのバックアップ(特に以下1～8の第5階層レベルに示す内容)が、確実に行われているかを確認します。)		●		
	実施方法	4- 7- 1- 7- 1	Q DBファイルバックアップの実施方法(バックアップ頻度、バックアップ取得方法、保管場所)は明確ですか？ (情報システム上必要なDBファイルバックアップの実施の方法が文書化され、明確に示されているかを確認します。)		●		
	遠隔地ミラーDB	4- 7- 1- 7- 2	Q DBファイルはリアルタイムで遠隔地ミラーDBを作成していますか？ (情報システム上必要なDBファイルが、更新・書込みのつど、DBファイル更新・書込みの行われている場所から離れている場所で、即時に別のDBファイルに同じ内容のものが更新・書込みが行われているかを確認します。)		●		
	遠隔地保管	4- 7- 1- 7- 3	Q DBファイルバックアップの遠隔地保管を行っていますか？ (バックアップされたDBファイルが、通常使用しているコンピュータが設置してある場所から離れた場所で保管されているかを確認します。)		●		
	同一サイト内保管	4- 7- 1- 7- 4	Q DBファイルバックアップの同一サイト内保存を行っていますか？ (バックアップされたDBファイルが、通常使用しているコンピュータが設置してある場所と同じ場所で保管されているかを確認します。)		●		
	ボリューム	4- 7- 1- 7- 5	Q ボリューム単位でバックアップを取得している場合、必要なボリュームはすべて対象となっていますか？ (バックアップの単位がボリューム単位の場合、情報システム上必要なボリュームが、すべてバックアップの対象になっているかを確認します。)		●		
	災害時用同一ディスク保有	4- 7- 1- 7- 6	Q ボリューム単位でバックアップを取得している場合、災害時用に同一モデルのディスクを確保していますか？ (バックアップの単位がボリューム単位の場合、災害時の対策用に通常使用されているDBファイルのディスクと同一のモデルのディスクを用いてバックアップしているかを確認します。)		●		
	ログバックアップ	4- 7- 1- 7- 7	Q DBMSのログは、定期的にバックアップされていますか？ (DBMS(データベースマネジメントシステム)の記録が、定期的にバックアップすることが文書化され、また、実施されているかを確認します。)		●		
	ログの分別化	4- 7- 1- 7- 8	Q DBMSのログは、データベース本体と別のディスクを使用していますか？ (DBMSの記録が、データベース本体とは別のディスクを使用しているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
バックアップ	バックアップ	Ⅳ－7. バックアップ					
4．ネットワーク対策	代替回線	4- 7- 1- 8	Q 代替回線を確保していますか？ (情報システムで使用する回線が単一のみでなく、万一回線にトラブルが発生しても情報システムに支障をきたさないように、代わりの回線が確保されているかを確認します。)		●		
	代替機	4- 7- 1- 9	Q 代替機を準備していますか？ (情報システムで使用する機器類が、万一機器類にトラブルが発生しても情報システムに支障をきたさないように、代わりの機器類が準備されているかを確認します。)		●		
	手作業による代替手段	4- 7- 1- 9- 1	Q 手作業による代替手段を準備していますか？ (情報システム上通常は自動化されている場合でも、自動化された一部又は全体にトラブルが発生した場合を考慮して、情報システムに対する被害が大きくならないように人力作業による運用ができるような手順書が準備されているか、又、関係者の教育訓練が適宜行われているかを確認します。)		●		
5．予備サイト	予備サイト設置	4- 7- 1- 10	Q 情報システムの予備サイトを設置していますか？ (情報システムの関連設備にトラブルが発生しても情報システムの運用に支障をきたさないよう、同等の機能を維持できる予備の関連設備が他の場所に設置されているかを確認します。)		●		
	同一室内のバックアップ用コンピュータ	4- 7- 1- 10- 1	Q 同一コンピュータ室内にバックアップ用のコンピュータを設置していますか？ (情報システムで使用するコンピュータが設置されている同じ室内に、同等の機能を持つコンピュータがバックアップ用として設置されているかを確認します。)		●		
	同一建物内のバックアップ用コンピュータ	4- 7- 1- 10- 2	Q 同一建物内の別室にバックアップ用のコンピュータを設置していますか？ (情報システムで使用するコンピュータが設置されている建物と同じ建物内の別の部屋に、同等の機能を持つコンピュータがバックアップ用として設置されているかを確認します。)		●		
	バックアップセンタ	4- 7- 1- 10- 3	Q 情報喪失に備えて、平時からのバックアップセンタが準備されていますか？ (情報システム上の情報が何らかの理由により喪失した場合に備え、通常の情報システムを運用する場合と同じ機能を持つバックアップセンタがいつも準備されているかを確認します。)		●		
	遠隔地バックアップセンタ	4- 7- 1- 10- 4	Q 遠隔地にバックアップセンタを設置していますか？ (通常の情報システムと同じ機能を持つバックアップセンタが、情報システムが運用されている場所から離れた場所に設置されているかを確認します。)		●		
	バックアップサービス業者	4- 7- 1- 10- 5	Q バックアップサービス業者と契約していますか？ (情報システムのバックアップ対策として、バックアップサービスを営業目的とする業者とバックアップに関する何らかの契約を行っているかを確認します。)		●		
	相互バックアップ契約	4- 7- 1- 10- 6	Q 同種コンピュータのユーザと相互バックアップ契約を締結していますか？ (情報システムのバックアップ対策として、自社(自組織)で使用するものと同種のコンピュータを持つ別のユーザと、万一の場合を考慮して相互のバックアップ契約を締結しているかを確認します。)		●		

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
緊急時対策	緊急時対策	Ⅳ－8. 緊急時対策					
1. 実施基準	緊急時対策	4- 8- 1- 1	Q 実施基準に緊急時対策を定めていますか？ (緊急時対策について実施基準に定める必要があります。) (用語解説「緊急時対策」:万一の事件や事故が発生した場合に、誰が、どのように、何をするのかについて、あらかじめ定めた対策をいいます。)		●		(4.2)
	障害発生	4- 8- 1- 1- 1	Q 実施基準に障害発生時の緊急時対策を定めていますか？ (ハードウェアの故障などによって情報システムが正常に稼働しない場合の緊急時対策について、実施基準に定める必要があります。)		●		
	機密・個人情報漏えい対策	4- 8- 1- 1- 2	Q 実施基準に機密・個人情報漏えいに対する緊急時対策を定められていますか？ (重要な情報が漏えいした場合の緊急時対策について、実施基準に定める必要があります。)		●		4.2
	不正アクセス	4- 8- 1- 1- 3	Q 実施基準に不正アクセスに対する緊急時対策を定めていますか？ (ハッカーや社内、外の許可を得ない者によって重要な情報が参照や利用などされた場合の緊急時対策について、実施基準に定める必要があります。)		●		
	マクロウイルス	4- 8- 1- 1- 4	Q 実施基準にマクロウイルスに対する緊急時対策を定めていますか？ (コンピュータウイルスに感染した場合や他人にウイルスメールを発信した場合などの緊急時対策について、実施基準に定める必要があります。)		●		
	自然災害	4- 8- 1- 1- 5	Q 実施基準に自然災害に対する緊急時対策を定めていますか？ (地震や台風・洪水、雷などの自然災害の被災を受けた場合の緊急時対策について、実施基準に定める必要があります。)		●		
	倒産	4- 8- 1- 1- 6	Q 実施基準にアウトソース先の倒産による緊急時対策を定めていますか？ (運用や開発業務をアウトソースしている場合は、万一アウトソース先が倒産し、委託業務を続行できなくなった場合について、緊急時対策を実施基準に定める必要があります。)		●		
	法令侵害	4- 8- 1- 1- 7	Q 実施基準に各種法令侵害に対する緊急時対策を定めていますか？ (著作権法違反などの各種法令に違反してしまった場合の緊急時対策について、実施基準に定める必要があります。)		●		4.4.8
	バックアップ	4- 8- 1- 1- 8	Q 実施基準にバックアップに対する緊急時対策を定めていますか？ (緊急時にはバックアップシステムの稼働やバックアップテープなどを利用する場合がありますが、その対策について実施基準に定める必要があります。)		●		
	ファシリティ移動	4- 8- 1- 1- 9	Q 実施基準にその他ファシリティの移動が必要な事態に対する緊急時対策を定めていますか？ (伝染病の蔓延、テロ、長期間のインフラの停止など、事務所や機器の移動が必要な事態が発生した場合の緊急時対策について、実施基準に定める必要があります。)		●		
2. 事前対応	緊急時対応の訓練	4- 8- 1- 2	Q 緊急事態発生時の対応について情報セキュリティの面からスタッフに対して定期的に訓練を行っていますか？ (緊急事態が発生した場合に、実施基準や各種手順書に定められている行動が実際に取れるようにするため、定期的にスタッフに訓練を実施する必要があります。)		●		(4.4.6)

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
緊急時対策	緊急時対策	Ⅳ－8. 緊急時対策					
3．緊急時対応手続	緊急時対応手続の明確化	4- 8- 1- 3	Q 緊急時対策における手続は明確ですか？ （緊急事態が発生し、緊急時対策を実施する場合の権限者の許可や承認を得るなどの手続が明確に定められている必要があります。緊急時には時間との戦いになります。そのため初期対応においては現場の最上位者に対して権限委譲を行い、実施した内容を事後報告し、承認するなどの手続をあらかじめ定めておき、初動の速度を確保する必要があります。）		●	●	(4.4.1)
	緊急連絡網	4- 8- 1- 3- 1	Q 緊急連絡網を整備していますか？ （最終責任者、現場責任者、管理者、実務担当者の緊急連絡網を整備し、365日24時間必要に応じて連絡が取れる体制を作る必要があります。）		●	●	4.4.1
	緊急時対応体制	4- 8- 1- 3- 2	Q 緊急時対応体制を明確にしていますか？ （緊急時対応を行う場合の現場の対応チーム体制および組織としての災害事故対策本部体制などを明確にする必要があります。）		●	●	
	代替対応手順	4- 8- 1- 3- 3	Q 緊急時の代替対応手順を明確にしていますか？ （緊急事態が発生し、そのままでは業務を継続できない場合に備えて、業務を継続するための代替対応手順を明確にする必要があります。） （用語解説：代替対応手順は必ずしも自社の情報システムを用いるものでなくても構いません。手作業や同業者への協力要請なども含みます。）		●	●	
	障害解決のフローチャート化	4- 8- 1- 3- 4	Q 発生した障害について、解決までの業務をフローチャート化していますか？ （障害事故が発生した場合、その解決にあたって原因追求や現場連絡などを含めて、さまざまな業務をフローチャートにまとめておく必要があります。）		●	●	
	教育訓練計画	4- 8- 1- 3- 5	Q 緊急事態を想定した教育訓練計画を作成していますか？ （緊急事態が発生した場合の対応を情報システム部門だけではなくユーザも含めて身に付けるためには、教育訓練を実施する必要があります。その教育訓練計画を年間計画として作成する必要があります。）		●	●	4.4.6
	対策本部	4- 8- 1- 3- 6	Q 緊急時対策本部の組織と物理的な設定基準はあらかじめ定められていますか？ （緊急時対策本部の組織を定める必要がありますが、その対策本部を設置するための条件を明確に定める必要があります。） （用語解説「物理的な設定基準」：地震でいえば震度6弱を超える大地震が発生した場合、システム障害ではシステムが3時間以上停止した場合などの明確な基準のことを指します。また被害程度によって社長、情報システム担当役員、情報システム部長が対策本部長になるなど、段階をつけることも一般的です。）		●	●	
	判定基準	4- 8- 1- 3- 7	Q 情報資産に関する緊急事態の判定基準は明確ですか？ （情報資産が損なわれた場合を緊急事態と判定しますが、その判定基準を明確にする必要があります。） （用語解説「緊急事態」：たとえばデータベースが破損し復旧不可能な場合、1件では緊急事態とはいえないものの全体の1％が破損した場合は緊急事態とするなど、あらかじめ明確にできる場合は基準を作成しておきます。）		●		
	緊急事態宣言	4- 8- 1- 3- 8	Q 緊急事態宣言（シナリオ）と通知方法は事前に決められていますか？ （緊急事態と判定された場合は組織をあげて対策本部を設置します。その場合、緊急事態を宣言し、職務権限の切替えなどを行います。そのための文章や従業員への通知方法について事前に定めておく必要があります。）		●	●	4.2

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
緊急時対策	緊急時対策	Ⅳ－8. 緊急時対策					
3．緊急時対応手続	情報資産	4- 8- 1- 3- 9	Q 情報資産固有の緊急事態対応手順はあらかじめ定められていますか？ (個人情報など情報資産それぞれについて特別な緊急時対応が必要な場合は、その特殊な対応についてあらかじめ対応手順を定めておく必要があります。)		●		4.4.1
	情報漏えい等の発見時の通報・究明手順	4- 8- 1- 3- 10	Q 情報漏えい等の発見とシステム管理者への通報・究明手順があらかじめ定められていますか？ (事件や事故を把握し、被害の拡大を防止するためには早期発見が不可欠です。そのためおかしいと感じた時に一刻も早くシステム管理者に対し通報し、原因を究明する仕組みを構築しておく必要があります。)		●		
	バックアップ手順	4- 8- 1- 3- 11	Q システム遮断、ユーザへの緊急サービス停止などを実施した後のバックアップ手順があらかじめ定められていますか？ (システムの誤作動、コンピュータウイルスやハッカーの侵入、不正利用の発覚など、被害の拡大防止のためにシステムを停止しなければならない場合があります。その場合にそのシステムの利用者に対して代替サービスを提供することが必要で、そのための手順を定める必要があります。)		●		
	危機障害発生時の適用業務優先順位	4- 8- 1- 3- 12	Q 機器障害発生時における縮退・再編成の際の適用業務の優先順位を決めていますか？ (ホスト機、サーバ、ディスクなどの一部が破損などにより使用できない場合、残りの機器で縮退運転を実施することがあります。その場合、どの業務を優先して実施し、どの業務は停止するかについて事前に優先順位を定めておく必要があります。)		●		
	障害切分け	4- 8- 1- 3- 13	Q 障害切分けのために必要な設備を整備していますか？ (ネットワーク障害などが発生した場合、どの機器やどの通信業者のサービスが障害を起こしているかを早期に発見する必要があります。そのための障害切分けを実施するための機器を用意する必要があります。)		●		
	障害発生アラーム	4- 8- 1- 3- 14	Q ネットワークを含むシステム全体の運用監視で、障害発生時に運用スタッフに知らせることのできるアラーム等を整備していますか？ (ネットワークを含め、システムを自動監視するケースが増えています。その場合、異常が発生した時にすぐにスタッフに連絡できるための仕組みが必要です。)		●		
	障害管理票	4- 8- 1- 3- 15	Q すべての障害についての障害管理票の作成要領を定めていますか？ (システム障害が発生した場合はそのすべてについて障害管理票を作成し、今後の分析のための資料とする必要があります。その管理票の作成要領について定める必要があります。)		●		
	定期的評価、是正改善	4- 8- 1- 4	Q 緊急時対策について不具合があった場合、是正処置をとっていますか？ (緊急時対策を実際に実施した場合、事前の計画どおりではうまくいかない場合もあります。その場合、その不具合を緊急時対策終了後、すぐ是正しておく必要があります。)		●		4.6

キーワード	キーワード	識別コード	質問項目	回答者			JIS Q 15001
				経営者	IS	ユーザ	
リスク対策	リスク対策	Ⅳ. 情報システムにおけるリスク対策					
緊急時対策	緊急時対策	Ⅳ－8. 緊急時対策					
4．復旧計画	復旧計画	4- 8- 1- 5	Q 復旧計画は、詳細な手続が定められていますか？ (緊急時対策を行い、場合によってはバックアップシステムを稼働したり縮退運転を稼働させる場合があります。その場合、元の状態にシステムや情報資産を復旧させる必要があります。その復旧にあたっての手順や管理権限、承認などの手続を定める必要があります。)		●	●	(4.2)
	復旧オーナー、管理者の選定	4- 8- 1- 5- 1	Q 主幹システム、重要ビジネスプロセスごとの、復旧のオーナー、支援のためのシステム管理者、その他の支援スタッフを決めていますか？ (組織にとって主要な主幹システムや重要なビジネスについては、復旧にあたってユーザ部門を含め、誰が責任者であり、誰が復旧のための予算や費用、要員の手配を行うかなどについて、事前に明確に定めておく必要があります。)		●		
	代替手段	4- 8- 1- 5- 2	Q 代替手段によるバックアップ実施を決定していますか？ (リラン(Rerun)やリトライを行うなどの一般的な復旧がうまくいかない場合に備えて、あらかじめ手作業による再入力や緊急システムの臨時作成などによる復旧を行う、などの方法を定めておく必要があります。)		●		
	計画維持・テストのスケジュール化	4- 8- 1- 5- 3	Q 復旧計画の維持、テストのためのスケジュールを決定していますか？ (復旧計画を維持するため、あるいは維持ができていることを確認するためにはテストが必要です。そのテストを行うため、あらかじめ年間の機械稼働スケジュールにテストのための時間を確保しておくことが必要です。 (用語解説：当然ながらスケジュールを確保するのみならず、実際にテストを実施しておかなければならないことは言うまでもありません。)		●		

参考資料

●個人情報の保護に関する法律（平成十五年法律第五十七号）

目　　次

第一章　総則

（目的）

第一条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

（定義）

第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

2　この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるものをいう。

一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

3　この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

一　国の機関

二　地方公共団体

三　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。）

四　地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。）

五　その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者

4　この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。

5　この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。

6　この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

（基本理念）

第三条　個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。

第二章　国及び地方公共団体の責務等

（国の責務）

第四条　国は、この法律の趣旨にのっとり、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定し、及びこれを実施する責務を有する。

（地方公共団体の責務）

第五条　地方公共団体は、この法律の趣旨にのっとり、その地方公共団体の区域の特性に応じて、個人情報の適正な取扱いを確保するために必要な施策を策定し、及びこれを実施する責務を有する。

（法制上の措置等）

第六条　政府は、国の行政機関について、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

2　政府は、独立行政法人等について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

3　政府は、前二項に定めるもののほか、個人情報の性質及び利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする。

第三章　個人情報の保護に関する施策等

第一節　個人情報の保護に関する基本方針

第七条　政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針（以下「基本方針」という。）を定めなければならない。

2　基本方針は、次に掲げる事項について定めるものとする。

一　個人情報の保護に関する施策の推進に関する基本的な方向

二　国が講ずべき個人情報の保護のための措置に関する事項

三　地方公共団体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

四　独立行政法人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

五　地方独立行政法人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

六　個人情報取扱事業者及び第四十条第一項に規定する認定個人情報保護団体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

七　個人情報の取扱いに関する苦情の円滑な処理に関する事項

八　その他個人情報の保護に関する施策の推進に関する重要事項

3　内閣総理大臣は、国民生活審議会の意見を聴いて、基本方針の案を作成し、閣議の決定を求めなければならない。

4　内閣総理大臣は、前項の規定による閣議の決定があったときは、遅滞なく、基本方針を公表しなければならない。

5　前二項の規定は、基本方針の変更について準用する。

第二節　国の施策

（地方公共団体等への支援）

第八条　国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずるものとする。

（苦情処理のための措置）

第九条　国は、個人情報の取扱いに関し事業者と本人との間に生じた苦情の適切かつ迅速な処理を図るために必要な措置を講ずるものとする。

（個人情報の適正な取扱いを確保するための措置）

第十条　国は、地方公共団体との適切な役割分担を通じ、次章に規定する個人情報取扱事業者による個人情報の適正な取扱いを確保するために必要な措置を講ずるものとする。

第三節　地方公共団体の施策

（地方公共団体等が保有する個人情報の保護）

第十一条　地方公共団体は、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

2　地方公共団体は、その設立に係る地方独立行政法人について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

（区域内の事業者等への支援）

第十二条　地方公共団体は、個人情報の適正な取扱いを確保するため、その区域内の事業者及び住民に対する支援に必要な措置を講ずるよう努めなければならない。

（苦情の処理のあっせん等）

第十三条　地方公共団体は、個人情報の取扱いに関し事業者と本人との間に生じた苦情が適切かつ迅速に処理されるようにするため、苦情の処理のあっせんその他必要な措置を講ずるよう努めなければならない。

第四節　国及び地方公共団体の協力

第十四条　国及び地方公共団体は、個人情報の保護に関する施策を講ずるにつき、相協力するものとする。

第四章　個人情報取扱事業者の義務等

第一節　個人情報取扱事業者の義務

（利用目的の特定）

第十五条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（利用目的による制限）

第十六条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

2　個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3　前二項の規定は、次に掲げる場合については、適用しない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（適正な取得）

第十七条　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

（取得に際しての利用目的の通知等）

第十八条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

2　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

3　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

4　前三項の規定は、次に掲げる場合については、適用しない。

一　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

三　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

四　取得の状況からみて利用目的が明らかであると認められる場合

（データ内容の正確性の確保）

第十九条　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らない。

（安全管理措置）

第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の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じなければならない。

（従業者の監督）

第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

（委託先の監督）

第二十二条　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は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（第三者提供の制限）

第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、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らない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

2　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

3　個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

4　次に掲げる場合において、当該個人データの提供を受ける者は、前三項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

5　個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

（保有個人データに関する事項の公表等）

第二十四条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

一　当該個人情報取扱事業者の氏名又は名称

二　すべての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く。）

三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

2　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。

ただし、次の各号のいずれかに該当する場合は、この限りでない。

一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合

二　第十八条第四項第一号から第三号までに該当する場合

3　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

（開示）

第二十五条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

三　他の法令に違反することとなる場合

2　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの全部又は一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

3　他の法令の規定により、本人に対し第一項本文に規定する方法に相当する方法により当該本人が識別される保有個人データの全部又は一部を開示することとされている場合には、当該全部又は一部の保有個人データについては、同項の規定は、適用しない。

（訂正等）

第二十六条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

2　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知しなければならない。

（利用停止等）

第二十七条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第十六条の規定に違反して取り扱われているという理由又は第十七条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

2　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第二十三条第一項の規定に違反して第三者に提供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

3　個人情報取扱事業者は、第一項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

（理由の説明）
第二十八条　個人情報取扱事業者は、第二十四条第三項、第二十五条第二項、第二十六条第二項又は前条第三項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。
（開示等の求めに応じる手続）
第二十九条　個人情報取扱事業者は、第二十四条第二項、第二十五条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求め（以下この条において「開示等の求め」という。）に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。
2　個人情報取扱事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、個人情報取扱事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。
3　開示等の求めは、政令で定めるところにより、代理人によってすることができる。
4　個人情報取扱事業者は、前三項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。
（手数料）
第三十条　個人情報取扱事業者は、第二十四条第二項の規定による利用目的の通知又は第二十五条第一項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。
2　個人情報取扱事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。
（個人情報取扱事業者による苦情の処理）
第三十一条　個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。
2　個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。
（報告の徴収）
第三十二条　主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができる。
（助言）
第三十三条　主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し必要な助言をすることができる。
（勧告及び命令）
第三十四条　主務大臣は、個人情報取扱事業者が第十六条から第十八条まで、第二十条から第二十七条まで又は第三十条第二項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行
為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

2　主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる。

3　主務大臣は、前二項の規定にかかわらず、個人情報取扱事業者が第十六条、第十七条、第二十条から第二十二条まで又は第二十三条第一項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

（主務大臣の権限の行使の制限）

第三十五条　主務大臣は、前三条の規定により個人情報取扱事業者に対し報告の徴収、助言、勧告又は命令を行うに当たっては、表現の自由、学問の自由、信教の自由及び政治活動の自由を妨げてはならない。

2　前項の規定の趣旨に照らし、主務大臣は、個人情報取扱事業者が第五十条第一項各号に掲げる者（それぞれ当該各号に定める目的で個人情報を取り扱う場合に限る。）に対して個人情報を提供する行為については、その権限を行使しないものとする。

（主務大臣）

第三十六条　この節の規定における主務大臣は、次のとおりとする。ただし、内閣総理大臣は、この節の規定の円滑な実施のため必要があると認める場合は、個人情報取扱事業者が行う個人情報の取扱いのうち特定のものについて、特定の大臣又は国家公安委員会（以下「大臣等」という。）を主務大臣に指定することができる。

一　個人情報取扱事業者が行う個人情報の取扱いのうち雇用管理に関するものについては、厚生労働大臣（船員の雇用管理に関するものについては、国土交通大臣）及び当該個人情報取扱事業者が行う事業を所管する大臣等

二　個人情報取扱事業者が行う個人情報の取扱いのうち前号に掲げるもの以外のものについては、当該個人情報取扱事業者が行う事業を所管する大臣等

2　内閣総理大臣は、前項ただし書の規定により主務大臣を指定したときは、その旨を公示しなければならない。

3　各主務大臣は、この節の規定の施行に当たっては、相互に緊密に連絡し、及び協力しなければならない。

第二節　民間団体による個人情報の保護の推進

（認定）

第三十七条　個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第三号ロにおいて同じ。）は、主務大臣の認定を受けることができる。

一　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。）の個人情報の取扱いに関する　第四十二条の規定による苦情の処理

二　個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供
三　前二号に掲げるもののほか、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

2　前項の認定を受けようとする者は、政令で定めるところにより、主務大臣に申請しなければならない。

3　主務大臣は、第一項の認定をしたときは、その旨を公示しなければならない。

（欠格条項）

第三十八条　次の各号のいずれかに該当する者は、前条第一項の認定を受けることができない。

一　この法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者
二　第四十八条第一項の規定により認定を取り消され、その取消しの日から二年を経過しない者
三　その業務を行う役員（法人でない団体で代表者又は管理人の定めのあるものの代表者又は管理人を含む。以下この条において同じ。）のうちに、次のいずれかに該当する者があるもの
イ　禁錮以上の刑に処せられ、又はこの法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者
ロ　第四十八条第一項の規定により認定を取り消された法人において、その取消しの日前三十日以内にその役員であった者でその取消しの日から二年を経過しない者

（認定の基準）

第三十九条　主務大臣は、第三十七条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。

一　第三十七条第一項各号に掲げる業務を適正かつ確実に行うに必要な業務の実施の方法が定められているものであること。
二　第三十七条第一項各号に掲げる業務を適正かつ確実に行うに足りる知識及び能力並びに経理的基礎を有するものであること。
三　第三十七条第一項各号に掲げる業務以外の業務を行っている場合には、その業務を行うことによって同項各号に掲げる業務が不公正になるおそれがないものであること。

（廃止の届出）

第四十条　第三十七条第一項の認定を受けた者（以下「認定個人情報保護団体」という。）は、その認定に係る業務（以下「認定業務」という。）を廃止しようとするときは、政令で定めるところにより、あらかじめ、その旨を主務大臣に届け出なければならない。

2　主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

（対象事業者）

第四十一条　認定個人情報保護団体は、当該認定個人情報保護団体の構成員である個人情報取扱事業者又は認定業務の対象となることについて同意を得た個人情報取扱事業者を対象事業者としなければならない。

2　認定個人情報保護団体は、対象事業者の氏名又は名称を公表しなければならない。

（苦情の処理）

第四十二条　認定個人情報保護団体は、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。

2　認定個人情報保護団体は、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができる。

3　対象事業者は、認定個人情報保護団体から前項の規定による求めがあったときは、正当な理由がないのに、これを拒んではならない。

（個人情報保護指針）

第四十三条　認定個人情報保護団体は、対象事業者の個人情報の適正な取扱いの確保のために、利用目的の特定、安全管理のための措置、本人の求めに応じる手続その他の事項に関し、この法律の規定の趣旨に沿った指針（以下「個人情報保護指針」という。）を作成し、公表するよう努めなければならない。

2　認定個人情報保護団体は、前項の規定により個人情報保護指針を公表したときは、対象事業者に対し、当該個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとるよう努めなければならない。

（目的外利用の禁止）

第四十四条　認定個人情報保護団体は、認定業務の実施に際して知り得た情報を認定業務の用に供する目的以外に利用してはならない。

（名称の使用制限）

第四十五条　認定個人情報保護団体でない者は、認定個人情報保護団体という名称又はこれに紛らわしい名称を用いてはならない。

（報告の徴収）

第四十六条　主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に対し、認定業務に関し報告をさせることができる。

（命令）

第四十七条　主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に対し、認定業務の実施の方法の改善、個人情報保護指針の変更その他の必要な措置をとるべき旨を命ずることができる。

（認定の取消し）

第四十八条　主務大臣は、認定個人情報保護団体が次の各号のいずれかに該当するときは、その認定を取り消すことができる。

一　第三十八条第一号又は第三号に該当するに至ったとき。

二　第三十九条各号のいずれかに適合しなくなったとき。

三　第四十四条の規定に違反したとき。

四　前条の命令に従わないとき。

五　不正の手段により第三十七条第一項の認定を受けたとき。

2　主務大臣は、前項の規定により認定を取り消したときは、その旨を公示しなければならない。

（主務大臣）

第四十九条　この節の規定における主務大臣は、次のとおりとする。ただし、内閣総理大臣は、この節の規定の円滑な実施のため必要があると認める場合は、第三十七条第一項の認定を受けようとする者のうち特定のものについて、特定の大臣等を主務大臣に指定することができる。

一　設立について許可又は認可を受けている認定個人情報保護団体（第三十七条第一項の認定を受けようとする者を含む。次号において同じ。）については、その設立の許可又は認可をした大臣等

二　前号に掲げるもの以外の認定個人情報保護団体については、当該認定個人情報保護団体の対象事業者が行う事業を所管する大臣等

2　内閣総理大臣は、前項ただし書の規定により主務大臣を指定したときは、その旨を公示しなければならない。

第五章　雑則

（適用除外）

第五十条　個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。

一　放送機関、新聞社、通信社その他の報道機関（報道を業として行う個人を含む。）報道の用に供する目的

二　著述を業として行う者　著述の用に供する目的

三　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的

四　宗教団体　宗教活動（これに付随する活動を含む。）の用に供する目的

五　政治団体　政治活動（これに付随する活動を含む。）の用に供する目的

2　前項第一号に規定する「報道」とは、不特定かつ多数の者に対して客観的事実を事実として知らせること（これに基づいて意見又は見解を述べることを含む。）をいう。

3　第一項各号に掲げる個人情報取扱事業者は、個人データの安全管理のために必要かつ適切な措置、個人情報の取扱いに関する苦情の処理その他の個人情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

（地方公共団体が処理する事務）

第五十一条　この法律に規定する主務大臣の権限に属する事務は、政令で定めるところにより、地方公共団体の長その他の執行機関が行うこととすることができる。

（権限又は事務の委任）

第五十二条　この法律により主務大臣の権限又は事務に属する事項は、政令で定めるところにより、その所属の職員に委任することができる。

（施行の状況の公表）
第五十三条　内閣総理大臣は、関係する行政機関（法律の規定に基づき内閣に置かれる機関（内閣府を除く。）及び内閣の所轄の下に置かれる機関、内閣府、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関並びに国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関をいう。次条において同じ。）の長に対し、この法律の施行の状況について報告を求めることができる。
２　内閣総理大臣は、毎年度、前項の報告を取りまとめ、その概要を公表するものとする。
（連絡及び協力）
第五十四条　内閣総理大臣及びこの法律の施行に関係する行政機関の長は、相互に緊密に連絡し、及び協力しなければならない。
（政令への委任）
第五十五条　この法律に定めるもののほか、この法律の実施のため必要な事項は、政令で定める。

第六章　罰則
第五十六条　第三十四条第二項又は第三項の規定による命令に違反した者は、六月以下の懲役又は三十万円以下の罰金に処する。
第五十七条　第三十二条又は第四十六条の規定による報告をせず、又は虚偽の報告をした者は、三十万円以下の罰金に処する。
第五十八条　法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。）の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、前二条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。
２　法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。
第五十九条　次の各号のいずれかに該当する者は、十万円以下の過料に処する。
一　第四十条第一項の規定による届出をせず、又は虚偽の届出をした者
二　第四十五条の規定に違反した者

附　則
（施行期日）
第一条　この法律は、公布の日から施行する。ただし、第四章から第六章まで及び附則第二条から第六条までの規定は、公布の日から起算して二年を超えない範囲内において政令で定める日から施行する。
（本人の同意に関する経過措置）
第二条　この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第十五条第一項の規定により特定される利用目的以外の目的で個人情報を取り扱うこ

とを認める旨の同意に相当するものであるときは、第十六条第一項又は第二項の同意があったものとみなす。

第三条　この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第二十三条第一項の規定による個人データの第三者への提供を認める旨の同意に相当するものであるときは、同項の同意があったものとみなす。

（通知に関する経過措置）

第四条　第二十三条第二項の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。

第五条　第二十三条第四項第三号の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同号の規定により行われたものとみなす。

（名称の使用制限に関する経過措置）

第六条　この法律の施行の際現に認定個人情報保護団体という名称又はこれに紛らわしい名称を用いている者については、第四十五条の規定は、同条の規定の施行後六月間は、適用しない。

附則（平成十五年法律第百十九号）抄

（施行期日）

第一条　この法律は、地方独立行政法人法（平成十五年法律第百十八号）の施行の日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

一　第六条の規定　個人情報の保護に関する法律の施行の日又はこの法律の施行の日のいずれか遅い日

（その他の経過措置の政令への委任）

第六条　この附則に規定するもののほか、この法律の施行に伴い必要な経過措置は、政令で定める。

政令第五百六号

個人情報の保護に関する法律の一部の施行期日を定める政令

内閣は、個人情報の保護に関する法律（平成十五年法律第五十七号）附則第一条ただし書の規定に基づき、この政令を制定する。

個人情報の保護に関する法律附則第一条ただし書に規定する規定の施行期日は、平成十七年四月一日とする。

政令第五百七号

個人情報の保護に関する法律施行令

内閣は、個人情報の保護に関する法律（平成十五年法律第五十七号）第二条第二項第二号、第三項第四号及び第五項、第二十四条第一項第四号、第二十五条第一項、第二十九条第一項及び第三項、第三十七条第二項、第四十条第一項、第五十一条、第五十二条並びに第五十五条の規定に基づき、この政令を制定する。

（個人情報データベース等）

第一条　個人情報の保護に関する法律（以下「法」という。）第二条第二項第二号の政令で定めるものは、これに含まれる個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。

（個人情報取扱事業者から除外される者）

第二条　法第二条第三項第五号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等で個人情報として氏名又は住所若しくは居所（地図上又は電子計算機の映像面上において住所又は居所の所在の場所を示す表示を含む。）若しくは電話番号のみが含まれる場合であって、これを編集し、又は加工することなくその事業の用に供するときは、当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。）の合計が過去六月以内のいずれの日においても五千を超えない者とする。

（保有個人データから除外されるもの）

第三条　法第二条第五項の政令で定めるものは、次に掲げるものとする。

一　当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

二　当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

三　当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

四　当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

（保有個人データから除外されるものの消去までの期間）

第四条　法第二条第五項の政令で定める期間は、六月とする。

（保有個人データの適正な取扱いの確保に関し必要な事項）

第五条　法第二十四条第一項第四号の政令で定めるものは、次に掲げるものとする。

一　当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先

二　当該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ある場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

（個人情報取扱事業者が保有個人データを開示する方法）

第六条　法第二十五条第一項の政令で定める方法は、書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）とする。

（開示等の求めを受け付ける方法）

第七条　法第二十九条第一項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる事項は、次に掲げるとおりとする。

一　開示等の求めの申出先

二　開示等の求めに際して提出すべき書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

三　開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

四　法第三十条第一項の手数料の徴収方法

（開示等の求めをすることができる代理人）

第八条　法第二十九条第三項の規定により開示等の求めをすることができる代理人は、次に掲げる代理人とする。

一　未成年者又は成年被後見人の法定代理人

二　開示等の求めをすることにつき本人が委任した代理人

（認定個人情報保護団体の認定の申請）

第九条　法第三十七条第二項の規定による申請は、次に掲げる事項を記載した申請書を主務大臣に提出してしなければならない。

一　名称及び住所並びに代表者又は管理人の氏名

二　認定の申請に係る業務を行おうとする事務所の所在地

三　認定の申請に係る業務の概要

2　前項の申請書には、次に掲げる書類を添付しなければならない。

一　定款、寄附行為その他の基本約款

二　認定を受けようとする者が法第三十八条各号の規定に該当しないことを誓約する書面

三　認定の申請に係る業務の実施の方法を記載した書類

四　認定の申請に係る業務を適正かつ確実に行うに足りる知識及び能力を有することを明らかにする書類

五　最近の事業年度における事業報告書、貸借対照表、収支決算書、財産目録その他の経理的基礎を有することを明らかにする書類（申請の日の属する事業年度に設立された法人にあっては、その設立時における財産目録）

六　役員の氏名、住所及び略歴を記載した書類

七　対象事業者の氏名又は名称を記載した書類及び当該対象事業者が認定を受けようとする者の構成員であること又は認定の申請に係る業務の対象となることについて同意した者であることを証する書類

八　認定の申請に係る業務以外の業務を行っている場合は、その業務の種類及び概要を記載した書類

九　その他参考となる事項を記載した書類

3　認定個人情報保護団体は、第一項第一号若しくは第二号に掲げる事項又は前項第二号から第四号まで、第六号若しくは第八号に掲げる書類に記載した事項に変更があったときは、遅滞なく、その旨（同項第三号に掲げる書類に記載した事項に変更があったときは、その理由を含む。）を記載した届出書を主務大臣に提出しなければならない。

（認定業務の廃止の届出）

第十条　認定個人情報保護団体は、認定業務を廃止しようとするときは、廃止しようとする日の三月前までに、次に掲げる事項を記載した届出書を主務大臣に提出しなければならない。

一　名称及び住所並びに代表者又は管理人の氏名

二　法第四十二条第一項の申出の受付を終了しようとする日

三　認定業務を廃止しようとする日

四　認定業務を廃止する理由

（地方公共団体の長等が処理する事務）

第十一条　法第三十二条から第三十四条までに規定する主務大臣の権限に属する事務は、個人情報取扱事業者が行う事業であって当該主務大臣が所管するものについての報告の徴収、検査、勧告その他の監督に係る権限に属する事務の全部又は一部が他の法令の規定により地方公共団体の長その他の執行機関（以下この条において「地方公共団体の長等」という。）が行うこととされているときは、当該地方公共団体の長等が行う。この場合において、当該事務を行うこととなる地方公共団体の長等が二以上あるときは、法第三十二条及び第三十三条に規定する主務大臣の権限に属する事務は、各地方公共団体の長等がそれぞれ単独に行うことを妨げない。

2　法第三十七条、第四十条及び第四十六条から第四十八条までに規定する主務大臣の権限に属する事務は、認定個人情報保護団体（法第三十七条第一項の認定を受けようとする者を含む。）であってその設立の許可又は認可に係る主務大臣の権限に属する事務が他の法令の規定により地方公共団体の長等が行うこととされているときは、当該地方公共団体の長等が行う。

3　第一項の規定は、主務大臣が自ら同項に規定する事務を行うことを妨げない。

4　第一項の規定により同項に規定する主務大臣の権限に属する事務を行った地方公共団体の長等は、速やかに、その結果を主務大臣に報告しなければならない。

5　第一項及び第二項に規定する場合においては、法及びこの政令中これらの規定に規定する事務に係る主務大臣に関する規定は、地方公共団体の長等に関する規定として地方公共団体の長等に適用があるものとする。

（権限又は事務の委任）

第十二条　主務大臣は、法第五十二条の規定により、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項の庁の長、国家行政組織法（昭和二十三年法律第百二十号）第三条第二

項の庁の長又は警察庁長官に法第三十二条から第三十四条まで、第三十七条、第三十九条、第四十条及び第四十六条から第四十八条までに規定する権限又は事務のうちその所掌に係るものを委任することができる。

2　主務大臣（前項の規定によりその権限又は事務が内閣府設置法第四十九条第一項の庁の長又は国家行政組織法第三条第二項の庁の長に委任された場合にあっては、その庁の長）は、法第五十二条の規定により、内閣府設置法第十七条若しくは第五十三条の官房、局若しくは部の長、同法第十七条第一項若しくは第六十二条第一項若しくは第二項の職、同法第四十三条若しくは第五十七条の地方支分部局の長又は国家行政組織法第七条の官房、局若しくは部の長、同法第九条の地方支分部局の長若しくは同法第二十条第一項若しくは第二項の職に法第三十二条から第三十四条まで、第三十七条、第三十九条、第四十条及び第四十六条から第四十八条までに規定する権限又は事務のうちその所掌に係るものを委任することができる。

3　警察庁長官は、法第五十二条の規定により、警察法（昭和二十九年法律第百六十二号）第十九条第一項の長官官房若しくは局、同条第二項の部又は同法第三十条第一項の地方機関の長に第一項の規定により委任された権限又は事務を委任することができる。

4　主務大臣、内閣府設置法第四十九条第一項の庁の長、国家行政組織法第三条第二項の庁の長又は警察庁長官は、前三項の規定により権限又は事務を委任しようとするときは、委任を受ける職員の官職、委任する権限又は事務及び委任の効力の発生する日を公示しなければならない。

（主務大臣による権限の行使）

第十三条　個人情報取扱事業者が行う個人情報の取扱いについて、法第三十六条第一項の規定による主務大臣が二以上あるときは、法第三十二条及び第三十三条に規定する主務大臣の権限は、各主務大臣がそれぞれ単独に行使することを妨げない。

2　前項の規定によりその権限を単独に行使した主務大臣は、速やかに、その結果を他の主務大臣に通知するものとする。

附則

この政令は、公布の日から施行する。ただし、第五条から第十三条までの規定は、平成十七年四月一日から施行する。

附則（平成十六年政令第三百八十九号）

この政令は、公布の日から施行し、この政令による改正後の個人情報の保護に関する法律施行令第二条の規定は、平成十六年十月一日から適用する。

●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

経済産業省　平成１６年１０月

目　　次

Ⅰ．目的及び適用範囲

このガイドラインは、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第７条第１項に基づき平成１６年４月２日に閣議決定された「個人情報の保護に関する基本方針」を踏まえ、また、法第８条に基づき法に定める事項に関して必要な事項を定め、経済産業省が所管する分野及び法第３６条第１項により経済産業大臣が主務大臣に指定された特定の分野（以下「経済産業分野」という。）における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として定めるものである。

本ガイドラインは、経済産業大臣が法を執行する際の基準となるものであるが、従業員の個人情報（雇用管理に関するもの）に関する部分については、雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（平成１６年厚生労働省告示第２５９号）との整合性に留意した。このため、本ガイドラインのうちこれらの部分については、厚生労働大臣及び経済産業大臣の共同で作成し、両大臣が共同して法を執行する。

本ガイドライン中、「しなければならない」と記載されている規定については、それに従わなかった場合は、経済産業大臣により、法の規定違反と判断され得る。一方、「望ましい」と記載されている規定については、それに従わなかった場合でも、法の規定違反と判断されることはない（Ⅲ．参照）。しかし、「望ましい」と記載されている規定についても、個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに配慮して適正な取扱いが図られるべきとする法の基本理念（法第３条）を踏まえ、個人情報保護の推進の観点から、できるだけ取り組むことが望まれるものである。もっとも、個人情報の保護に当たって個人情報の有用性に配慮することとしている法の目的（法第１条）の趣旨に照らし、公益上必要な活動や正当な事業活動等までも制限するものではない。

なお、本ガイドライン中に事例として記述した部分は、理解を助けることを目的として、該当する事例及び該当しない事例のそれぞれにつき、典型的な例を示すものであり、すべての事案を網羅することを目的とするものではない。実際には個別事案ごとに検討が必要となる。また、幾つかの業種の例を取り上げたもので、すべての業種の例を網羅しているわけではないことを付記しておく。

このほか、経済産業分野に該当するもののうち、個人情報の性質及び利用方法又は事業実態の特殊性等にかんがみ、特別に個人情報の適正な取扱いを確保する必要がある場合には、経済産業大臣が、別途更なる措置を講ずることもあり得る。また、認定個人情報保護団体（法第３７条第１項の認定を受けた団体をいう。以下同じ。）が、法第４３条第１項に規定する個人情報保護指針を策定することもあり得る。これらの場合、それらに該当する個人情報を扱うに当たっては、当該更なる措置及び個人情報保護指針に沿った対応を行う必要がある。

また、事業者団体等が、当該事業の実態を踏まえ、当該団体傘下企業を対象とした自主的ルールである、事業者団体ガイドラインを策定又は改正することもあり得る。

Ⅱ．法令解釈指針・事例

１．定義（法第２条関連）

(1)「個人情報」（法第２条第１項関連）

法第２条第１項
この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

「個人情報」※1とは、生存する「個人に関する情報」であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができる※2ものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているかどうかを問わない。

なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。

また、「生存する個人」には日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体そのものに関する情報は含まれない（ただし、役員、従業員等に関する情報は個人情報）。

※１法は、「個人情報」、「（４）個人データ」及び「（５）保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

※２「他の情報と容易に照合することができ、…」とは、例えば通常の作業範囲において、個人情報データベース等にアクセスし、照合することができる状態をいい、他の事業者への照会を要する場合、当該事業者内部でも取扱部門が異なる場合等であって照合が困難な状態を除く。

【個人情報に該当する事例】

事例１）　本人の氏名

事例２）　生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報

事例３）　防犯カメラに記録された情報等本人が判別できる映像情報

事例４）　特定の個人を識別できるメールアドレス情報(keizai_ichiro@meti.go.jp等のようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等)

事例５）　特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識する

ことにより特定の個人を識別できる情報

事例６） 雇用管理情報（会社が従業員を評価した情報を含む。）

事例７） 個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となる。）

事例８） 官報、電話帳、職員録等で公にされている情報（本人の氏名等）

【個人情報に該当しない事例】

事例１）企業の財務情報等、法人等の団体そのものに関する情報（団体情報）

事例２）記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば、abc012345@ispisp.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。）

事例３）特定の個人を識別することができない統計情報

(2) 「個人情報データベース等」（法第２条第２項関連）

法第２条第２項

この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるものをいう。

１ 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

２ 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

個人情報の保護に関する法律施行令（平成１５年政令第５０７号。以下「政令」という。）第１条

法第２条第２項第２号の政令で定めるものは、これに含まれる個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。

「個人情報データベース等」とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した、個人情報を含む情報の集合物、又はコンピュータを用いていない場合であっても、カルテや指導要録等、紙面で処理した個人情報を一定の規則（例えば、五十音順、年月日順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものをいう。

【個人情報データベース等に該当する事例】

事例１）電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組

み合わせた情報を入力している場合）

事例２）ユーザーＩＤとユーザーが利用した取引についてのログ情報が保管されている電子ファイル（ユーザーIDを個人情報と関連付けて管理している場合）

事例３）従業員が、名刺の情報を業務用パソコン（所有者を問わない。）の表計算ソフト等を用いて入力・整理し、他の従業員等によっても検索できる状態にしている場合

事例４）人材派遣会社が登録カードを、氏名の五十音順に整理し、五十音順のインデックスを付してファイルしている場合

事例５）氏名、住所、企業別に分類整理されている市販の人名録

【個人情報データベース等に該当しない事例】

事例１）従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いていても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合

事例２）アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

(3)「個人情報取扱事業者」（法第２条第３項関連）

法第２条第３項

この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

1 国の機関

2 地方公共団体

3 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成１５年法律第５９号）第２条第１項に規定する独立行政法人等をいう。以下同じ。）

4 地方独立行政法人（地方独立行政法人法（平成１５年法律第１１８号）第２条第１項に規定する地方独立行政法人をいう。以下同じ。）

5 その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者

政令第２条

法第２条第３項第５号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等で個人情報として氏名又は住所若しくは居所（地図上又は電子計算機の映像面上において住所又は居所の所在の場所を示す表示を含む。）若しくは電話番号のみが含まれる場合であって、これを編集し、又は加工することなくその事業の用に供するときは、当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。）の合計が過去６月以内のいずれの日においても５０００を超えない者とする。

「個人情報取扱事業者」とは、国の機関、地方公共団体、独立行政法人等の保有する個人情

報の保護に関する法律（平成１５年法律第５９号）で定める独立行政法人等、地方独立行政法人法（平成１５年法律第１１８号）で定める地方独立行政法人並びにその取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ない者を除いた、個人情報データベース等を事業の用に供している者をいう。

ここでいう「取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ない者」とは、政令第２条では、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数※の合計が過去６か月以内のいずれの日においても５０００人を超えない者とする。５０００人を超えるか否かは、当該事業者の管理するすべての個人情報データベース等を構成する個人情報によって識別される特定の個人の数の総和により判断する。ただし、同一個人の重複分は除くものとする。

ここでいう「事業の用に供している」の「事業」とは、一定の目的を持って反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいい、営利事業のみを対象とするものではない。

法人格のない、権利能力のない社団（任意団体）又は個人であっても個人情報取扱事業者に該当し得る。

※「特定の個人の数」について

個人情報データベース等が、以下の要件のすべてに該当する場合は、その個人情報データベース等を構成する個人情報によって識別される特定の個人の数は、上記の「特定の個人の数」には算入しない。

① 個人情報データベース等の全部又は一部が他人の作成によるものである。

② その個人情報データベース等を構成する個人情報として氏名、住所（居所を含み、地図上又はコンピュータの映像面上において住所又は居所の所在場所を示す表示を含む。）又は電話番号のみを含んでいる。

③ その個人情報データベース等を事業の用に供するに当たり、新たに個人情報を加え、識別される特定の個人を増やしたり、他の個人情報を付加したりして、個人情報データベース等そのものを変更するようなことをしていない。

【特定の個人の数に算入しない事例】

事例１）電話会社から提供された電話帳及び市販の電話帳CD-ROM等に掲載されている氏名及び電話番号

事例２）市販のカーナビゲーションシステム等のナビゲーションシステムに格納されている氏名、住所又は居所の所在場所を示すデータ（ナビゲーションシステム等が当初から備えている機能を用いて、運行経路等新たな情報等を記録する場合があったとしても、「特定の個人の数」には算入しないものとする。）

事例３）氏名又は住所から検索できるよう体系的に構成された、市販の住所地図上の氏名及び住所又は居所の所在場所を示す情報

【事業の用に供しないため特定の個人の数に算入しない事例】

事例） 倉庫業、データセンター（ハウジング、ホスティング）等の事業において、当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に、その情報中に含まれる個人情報

【個人情報取扱事業者に該当する事例】

事例） 電子媒体及び紙媒体（以下「媒体」という。）の個人情報データベース等を構成する個人情報によって識別される特定の個人の数の総和が５０００人を超えている事業者

(4) 「個人データ」（法第２条第４項関連）

法第２条第４項 この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。

「個人データ」※とは、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう。

※法は、「（１）個人情報」、「個人データ」及び「（５）保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

【個人データに該当する事例】

事例１）個人情報データベース等から他の媒体に格納したバックアップ用の個人情報

事例２）コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

【個人データに該当しない事例】

事例）個人情報データベース等を構成する前の入力帳票に記載されている個人情報

※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

個人情報データベース等が、以下の要件のすべてに該当する場合であっても、その個人情報データベース等を構成する個人情報については、個人データとなる可能性も否定できない。しかしながら、その利用方法からみて個人の権利利益を侵害するおそれが少ないことから、個人情報取扱事業者の義務（２．個人情報取扱事業者の義務等）を課されないものと解釈する。

①個人情報データベース等の全部又は一部が他人の作成によるものである。

②その個人情報データベース等を構成する個人情報として氏名、住所（居所を含み、地図上又はコンピュータの映像面上において住所又は居所の所在場所を示す表示を含む。）又は電話番号のみを含んでいる。

③その個人情報データベース等を事業の用に供するに当たり、新たに個人情報を加え、識別される

特定の個人を増やしたり、他の個人情報を付加したりして、個人情報データベース等そのものを変更するようなことをしていない。

(5) 「保有個人データ」(法第２条第５項関連)

法第２条第５項

この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は１年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。

政令第３条

法第２条第５項の政令で定めるものは、次に掲げるものとする。

1 当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

2 当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

3 当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

4 当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

政令第４条

法第２条第５項の政令で定める期間は、６月とする。

「保有個人データ」※1とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する※2「個人データ」をいう。

※１法は、「(１) 個人情報」、「(４) 個人データ」及び「保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

※２個人情報取扱事業者が個人データを受託処理している場合で、その個人データについて、何ら取決めがなく、自らの判断では本人に開示等をすることができないときは、本人に開示等の権限を有しているのは委託者であって、受託者ではない。

ただし、次の①又は②の場合は、「保有個人データ」ではない。

① その存否が明らかになることにより、公益その他の利益が害されるもの※3。

② ６か月以内に消去する（更新することは除く。）こととなるもの。

※３「その存否が明らかになることにより、公益その他の利益が害されるもの」とは、以下の場合を指す。

ⅰ．その個人データの存否が明らかになることで、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの。

事例）家庭内暴力、児童虐待の被害者の支援団体が、加害者（配偶者又は親権者）及び被害者(配偶者又は子)を本人とする個人データを持っている場合

ⅱ．その個人データの存否が明らかになることで、違法又は不当な行為を助長し、又は誘発するおそれがあるもの。

事例１）いわゆる総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人データを持っている場合

事例２）いわゆる不審者、悪質なクレーマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人データを保有している場合

ⅲ．その個人データの存否が明らかになることで、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの。

事例１）製造業者、情報サービス事業者等が、防衛に関連する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人データを保有している場合

事例２）要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合

ⅳ．その個人データの存否が明らかになることで、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの。

事例）警察からの捜査関係事項照会や捜索差押令状の対象となった事業者がその対応の過程で捜査対象者又は被疑者を本人とする個人データを保有している場合

(6)「本人」（法第２条第６項関連）

法第２条第６項 この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

(7) 「本人に通知」

法第１８条第１項
個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

その他、法第１８条第３項・第４項第１号～第３号等に記述がある。

「本人に通知」とは、本人に直接知らしめることをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【本人への通知に該当する事例】

事例１）面談においては、口頭又はちらし等の文書を渡すこと。
事例２）電話においては、口頭又は自動応答装置等で知らせること。
事例３）隔地者間においては、電子メール、ファックス等により送信すること、又は文書を郵便等で送付すること。
事例４）電話勧誘販売において、勧誘の電話において口頭の方法によること。
事例５）電子商取引において、取引の確認を行うための自動応答の電子メールに記載して送信すること。

(8) 「公表」

法第１８条第１項
個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

その他、法第１８条第３項・第４項第１号～第３号等に記述がある。

「公表」とは、広く一般に自己の意思を知らせること（国民一般その他不特定多数の人々が知ることができるように発表すること）をいう。ただし、公表に当たっては、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければならない。

【公表に該当する事例】

事例１）自社のウェブ画面中のトップページから１回程度の操作で到達できる場所への掲載、自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備置き・配布等
事例２）店舗販売においては、店舗の見やすい場所への掲示によること。
事例３）通信販売においては、通信販売用のパンフレット等への記載によること。

(9) 「本人に対し、その利用目的を明示」

法第１８条第２項

個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

「本人に対し、その利用目的を明示」とは、本人に対し、その利用目的を明確に示すことをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【利用目的の明示に該当する事例】

事例１）利用目的を明記した契約書その他の書面を相手方である本人に手渡し、又は送付すること（契約約款又は利用条件等の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）中に利用目的条項を記載する場合は、例えば、裏面約款に利用目的が記載されていることを伝える、又は裏面約款等に記載されている利用目的条項を表面にも記述する等本人が実際に利用目的を目にできるよう留意する必要がある。）

事例２）ネットワーク上においては、本人がアクセスした自社のウェブ画面上、又は本人の端末装置上にその利用目的を明記すること（ネットワーク上において個人情報を取得する場合は、本人が送信ボタン等をクリックする前等にその利用目的（利用目的の内容が示された画面に１回程度の操作でページ遷移するよう設定したリンクやボタンを含む。）が本人の目にとまるようその配置に留意する必要がある。）

(10) 「本人の同意」

法第１６条第１項

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

法第２３条第１項

個人情報取扱事業者は、次に掲げる場合を除くほか、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らない。

1 法令に基づく場合
2 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
3 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって本人の同意を得ることが困難であるとき。
4 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

その他、法第１６条第２項・第３項第２号～第４号等に記述がある。

「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提。）。

また「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。

【本人の同意を得ている事例】

事例１）同意する旨を本人から口頭又は書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）で確認すること。
事例２）本人が署名又は記名押印した同意する旨の申込書等文書を受領し確認すること。
事例３）本人からの同意する旨のメールを受信すること。
事例４）本人による同意する旨の確認欄へのチェック
事例５）本人による同意する旨のウェブ画面上のボタンのクリック
事例６）本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

(11) 「本人が容易に知り得る状態」

法第２３条第２項

個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

3 個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

その他法第２３条第３項等に記述がある。

「本人が容易に知り得る状態」とは、本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いていることをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【本人が容易に知り得る状態に該当する事例】

事例１） ウェブ画面中のトップページから１回程度の操作で到達できる場所への掲載等が継続的に行われていること。
事例２）事務所の窓口等への掲示、備付け等が継続的に行われていること。
事例３）広く頒布されている定期刊行物への定期的掲載を行っていること。
事例４）電子商取引において、商品を紹介するウェブ画面にリンク先を継続的に掲示すること。

(12) 「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」

法第２４条第１項
個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」とは、ウェブ画面への掲載、パンフレットの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうとすれば、知ることができる状態に置くことをいい、常にその時点での正確な内容を本人の知り得る状態に置かなければならない。必ずしもウェブ画面への掲載、又は事務所等の窓口等へ掲示すること等が継続的に行われることまでを必要とするものではないが、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

なお、ふだんから問い合わせ対応が多い事業者等において、ウェブ画面へ継続的に掲載する方法は、(11)「本人が容易に知り得る状態」及び(12)「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」の両者の趣旨に合致する方法である。

【本人の知り得る状態に該当する事例】
事例１）問い合わせ窓口を設け、問い合わせがあれば、口頭又は文章で回答できるよう体制を構築して

おくこと。

事例２）店舗販売において、店舗にパンフレットを備え置くこと。

事例３）電子商取引において、問い合わせ先のメールアドレスを明記すること。

(13) 「提供」

法第２３条第１項

個人情報取扱事業者は、次に掲げる場合を除くほか、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らない。

その他、法第２３条第２項等に記述がある。

「提供」とは、個人データを利用可能な状態に置くことをいう。個人データが、物理的に提供されていない場合であっても、ネットワーク等を利用することにより、個人データを利用できる状態にあれば（利用する権限が与えられていれば）、「提供」に当たる。

２．個人情報取扱事業者の義務等

(1) 個人情報の利用目的関係（法第１５条～第１６条関連）

①① 利用目的の特定（法第１５条第１項関連）

法第１５条第１項

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

個人情報取扱事業者は、利用目的をできる限り特定しなければならない。

利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報取扱事業者において最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定する必要がある（１．(4)※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。）。利用する個人情報の種類及び入手先の事業者名等を特定することまで求めているわけではない。

具体的には、「○○事業※における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられるが、定款や寄附行為等に想定されている事業の内容に照らして、個人情報によって識別される本人からみて、自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範囲が想定される場合には、これで足りるとされることもあり得る。しかしながら、単に「事業活動」、「お客様のサービスの向上」等を利用目的とすることは、できる限り特定したこ

とにはならない。

なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨特定しなければならない。

雇用管理情報の利用目的の特定に当たっても、単に抽象的、一般的に特定するのではなく、労働者等（個人情報取扱事業者に使用されている労働者、個人情報取扱事業者に使用される労働者になろうとする者及びなろうとした者並びに過去において個人情報取扱事業者に使用されていた者。以下同じ。）本人が、取得された当該本人の個人情報が利用された結果が合理的に想定できる程度に、具体的、個別的に特定しなければならない。

※○○事業の特定に当たっては、社会通念上、本人から見てその特定に資すると認められる範囲に特定することが望ましい。例えば、日本標準産業分類の中分類から小分類程度の分類が参考になる場合がある。

【具体的に利用目的を特定している事例】

事例１）「○○事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします。」

事例２）「ご記入いただいた氏名、住所、電話番号は、名簿として販売することがあります。」

事例３）例えば、情報処理サービスを行っている事業者の場合であれば、「給与計算処理サービス、あて名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために、委託された個人情報を取り扱います。」のようにすれば利用目的を特定したことになる。

【具体的に利用目的を特定していない事例】

事例１）「事業活動に用いるため」

事例２）「提供するサービスの向上のため」

事例３）「マーケティング活動に用いるため」

② 利用目的の変更（法第１５条第２項、法第１８条第３項関連）

法第１５条第２項

個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

法第１８条第３項

個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

上記①により特定した利用目的は、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することは可能である。変更された利用目的は、本人に通知※1するか、又は公表※2しなければならない。

※１「本人に通知」については、１．(7)参照。
※２「公表」については、１．(8)参照。

＊ 本人が想定することが困難でないと認められる範囲内の基準

利用目的で示した個人情報を取り扱う事業の範囲を超えての変更は、あらかじめ本人の同意なく行うことはできない。

利用目的において、一連の個人情報の取扱いの典型を具体性をもって示していた場合は、その典型例から推測できる範囲内で変更することができる。

【本人が想定することが困難でないと認められる範囲内に該当する事例】

事例）「当社の行う○○事業における新商品・サービスに関する情報を電子メールにより送信することがあります。」とした利用目的において、「郵便によりお知らせすることがある」旨追加することは、許容される。

③ 利用目的による制限（法第１６条第１項関連）

法第１６条第１項

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

個人情報取扱事業者は、利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意※を得なければならない。

同意を得るために個人情報を利用すること（メールの送付や電話をかけること等）は、当初の利用目的として記載されていない場合でも、目的外利用には該当しない。

※「本人の同意」については、１．(10)参照。

【同意が必要な事例】

事例） 就職のための履歴書情報をもとに、自社の商品の販売促進のために自社取扱商品のカタログと商品購入申込書を送る場合

④ 事業の承継（法第１６条第２項関連）

法第１６条第２項

個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

個人情報取扱事業者が、合併、分社化、営業譲渡等により他の個人情報取扱事業者から事業の承継をすることに伴って個人情報を取得した場合であって、当該個人情報に係る承継前の利用目的の達成に必要な範囲内で取り扱う場合は目的外利用にはならず、本人の同意を得る必要はない。

⑤ 適用除外（法第１６条第３項関連）

以下のような場合には、上記③及び④において本人による同意を得ることが求められる場合でも、その適用を受けない。

ｉ．法令に基づく場合（法第１６条第３項第１号関連）

法第１６条第３項第１号
前２項の規定は、次に掲げる場合については、適用しない。 １　法令に基づく場合

法令に基づいて個人情報を取り扱う場合は、その適用を受けない。

上記の根拠となる法令の規定としては、刑事訴訟法第２１８条（令状による捜査）、地方税法第７２条の６３（事業税に係る質問検査権、各種税法に類似の規定あり。）等が考えられる。これらについては、強制力を伴っており、回答が義務づけられているため、一律これに該当する。

事例）所得税法第２２５条第１項等による税務署長に対する支払調書等の提出

一方、刑事訴訟法第１９７条第２項（捜査と必要な取調べ）等のような、個人情報の提供が任意協力の場合についても対象となり得ると考えられるが、個別の判断が必要とされる。

事例１）　商法第２７４条の３による親会社の監査役の子会社に対する調査への対応
事例２）　株式会社の監査等に関する商法の特例に関する法律第２条及び証券取引法第１９３条の２の規定に基づく財務諸表監査への対応

ⅱ．人の生命、身体又は財産の保護（法第１６条第３項第２号関連）

法第１６条第３項第２号
前２項の規定は、次に掲げる場合については、適用しない。 ２　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

人（法人を含む。）の生命又は財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人情報の利用が必要であり、かつ、本人の同意を得ることが困難である場合（他の方法により、当該権利利益の保護が十分可能である場合を除く。）は、その適用を受けない。

事例１） 急病その他の事態時に、本人について、その血液型や家族の連絡先等を医師や看護師に提供する場合

事例２） 私企業間において、意図的に業務妨害を行う者の情報について情報交換される場合

ⅲ．公衆衛生の向上等（法第１６条第３項第３号関連）

法第１６条第３項第３号
前２項の規定は、次に掲げる場合については、適用しない。 3 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）は、その適用を受けない。

事例１） 健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究又は統計調査のために、個人名を伏せて研究者等に提供する場合

事例２） 不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

ⅳ． 国の機関等への協力（法第１６条第３項第４号関連）

法第１６条第３項第４号
前２項の規定は、次に掲げる場合については、適用しない。 4 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が目的外利用を行うことについて、本人の同意を得ることが当

該事務の遂行に支障を及ぼすおそれがあると認められる場合は、その適用を受けない。

事例１）　事業者等が、税務署の職員等の任意調査に対し、個人情報を提出する場合
事例２）　事業者等が警察の任意の求めに応じて個人情報を提出する場合

(2) 個人情報の取得関係（法第１７条～第１８条関連）

① 適正取得（法第１７条関連）

法第１７条
個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。
なお、不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、詐欺等により取得したり、使用・開示した者には不正競争防止法（平成５年法律第４７号）第１４条により刑事罰（３年以下の懲役又は３００万円以下の罰金）が科され得る。

【不正の手段により個人情報を取得している事例】
事例１）　親の同意がなく、十分な判断能力を有していない子供から、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合
事例２）　法第２３条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合
事例３）　他の事業者に指示して上記事例１）又は事例２）などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

② 利用目的の通知又は公表（法第１８条第１項関連）

法第１８条第１項
個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

個人情報取扱事業者は、個人情報を取得する場合は、あらかじめその利用目的を公表※1していることが望ましい。公表していない場合は、取得後速やかに、その利用目的を、本人に通知※2するか、又は公表しなければならない（１．(4)※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。）。
法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第１８条の規定は適用されない。ただし、保有個人データに関する事項の本人への周知につ

いては、法施行時に法第２４条第１項の措置を講ずる必要がある（２．(5)１）①参照）。

※１「公表」については、１．(8)参照。
※２「本人に通知」については、１．(7)参照。

【本人に通知又は公表が必要な事例】
事例１）インターネット上で本人が自発的に公にしている個人情報を取得する場合
事例２）インターネット、官報、職員録等から個人情報を取得する場合
事例３）電話による問い合わせやクレームのように本人により自発的に提供される個人情報を取得する場合（本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除く。）
事例４）個人情報の第三者提供を受ける場合

③ 直接書面等による取得（法第１８条第２項関連）

法第１８条第２項
個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

個人情報取扱事業者は、書面等による記載、ユーザー入力画面への打ち込み等により、直接本人から個人情報を取得する場合には、あらかじめ、本人に対し、その利用目的を明示※しなければならない。なお、口頭による個人情報の取得にまで、当該義務を課すものではない。

※「本人に対して、その利用目的を明示」については、１．(9)参照。

【あらかじめ、本人に対し、その利用目的を明示しなければならない場合】
事例１） 申込書・契約書に記載された個人情報を本人から直接取得する場合
事例２） アンケートに記載された個人情報を直接本人から取得する場合
事例３） 懸賞の応募はがきに記載された個人情報を直接本人から取得する場合

④ 利用目的の変更（法第１８条第３項関連）

法第１８条第３項

個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

個人情報取扱事業者は、社会通念上、本人が想定することが困難でないと認められる範囲内で利用目的を変更した場合は、変更された利用目的について、本人に通知※1するか、又は公表※2しなければならない（(1)②参照）。

※１「本人に通知」については、１．(7)参照。
※２「公表」については、１．(8)参照。

⑤ 適用除外（法第１８条第４項関連）

以下の場合においては、上記②、③及び④はその適用を受けない。

ｉ．本人又は第三者の権利利益を害するおそれ（法第１８条第４項第１号関連）

法第１８条第４項第１号

前３項の規定は、次に掲げる場合については、適用しない。

１ 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合は、その適用を受けない。

事例）いわゆる総会屋等による不当要求等の被害を防止するため、当該総会屋担当者個人に関する情報を取得し、相互に情報交換を行っている場合で、利用目的を通知又は公表することにより、当該総会屋等の逆恨みにより、第三者たる情報提供者が被害を被る恐れがある場合

ⅱ．当該個人情報取扱事業者の権利等を害するおそれ（法第１８条第４項第２号関連）

法第１８条第４項第２号

前３項の規定は、次に掲げる場合については、適用しない。

２ 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

利用目的を本人に通知し、又は公表することにより企業秘密に関すること等が他社に明ら

かになり、当該個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合は、その適用を受けない。

事例）通知又は公表される利用目的の内容により、当該個人情報取扱事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密にかかわるようなものが明らかになる場合

iii．国の機関等への協力（法第１８条第４項第３号関連）

法第１８条第４項第３号
前３項の規定は、次に掲げる場合については、適用しない。 3　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が国の機関等から受け取った個人情報の利用目的を本人に通知し、又は公表することにより、当該事務の遂行に支障を及ぼすおそれがある場合は、その適用を受けない。

事例）公開手配を行わないで、被疑者に関する個人情報を、警察から被疑者の立ち回りが予想される個人情報取扱事業者に限って提供する場合、警察から受け取った当該個人情報取扱事業者が、利用目的を本人に通知し、又は公表することにより、捜査活動に重大な支障を及ぼすおそれがある場合

iv．利用目的が自明（法第１８条第４項第４号関連）

法第１８条第４項第４号
前３項の規定は、次に掲げる場合については、適用しない。 4　取得の状況からみて利用目的が明らかであると認められる場合

個人情報が取得される状況から見て利用目的が自明であると認められる場合は、その適用を受けない。

事例１）商品・サービス等を販売・提供する場合、住所・電話番号等の個人情報を取得する場合があるが、その利用目的が当該商品・サービス等の販売・提供のみを確実に行うためという利用目的であるような場合

事例２）一般の慣行として名刺を交換する場合、書面により、直接本人から、氏名・所属・肩書・連絡先等の個人情報を取得することとなるが、その利用目的が今後の連絡の

ためという利用目的であるような場合（ただし、ダイレクトメール等の目的に名刺を用いることは自明の利用目的に該当しない場合があるので注意を要する。）

(3) 個人データの管理（法第１９条～第２２条関連）

1) データ内容の正確性の確保（法第１９条関連）

法第１９条
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らない。

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、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、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らない（１．(4)※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る。

2) 安全管理措置（法第２０条関連）

法第２０条
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の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じなければならない。

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき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、物理的及び技術的な安全管理措置を講じなければならない（１．(4)※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。）。その際、本人の個人データが漏えい、滅失又はき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状況等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する。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。

【必要かつ適切な安全管理措置を講じているとはいえない場合】
事例１） 公開されることを前提としていない個人データが事業者のウェブ画面上で不特定多数に公開されている状態を個人情報取扱事業者が放置している場合
事例２） 組織変更が行われ、個人データにアクセスする必要がなくなった従事者が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従事者が個人データを漏えいした場合

事例３） 本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失又はき損し、本人がサービスの提供を受けられなくなった場合

事例４） 個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合

事例５） 個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

①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
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データの取扱い状況を一覧できる手段の整備
④個人データの安全管理措置の評価、見直し及び改善
⑤事故又は違反への対処

【各項目について講じることが望まれる事項】

①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をする上で望まれる事項

- 従業者の役割・責任の明確化
  ※個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。
- 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
- 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
- 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
- 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
- 監査責任者の設置
- 監査実施体制の整備
- 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
- 個人データの漏えい等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

※個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第３１条を参照）。

- 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
- 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

②個人データの安全管理措置を定める規程等の整備と規程等に従った運用をする上で望まれる事項

- 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
- 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

  ※なお、これらについてのより詳細な記載事項については、下記の【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】を参照。
- 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
- 個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
- 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

  ※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

③個人データの取扱い状況を一覧できる手段の整備をする上で望まれる事項

- 個人データについて、取得する項目、通知した利用目的、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
- 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

④個人データの安全管理措置の評価、見直し及び改善をする上で望まれる事項

- 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
- 監査実施結果の取りまとめと、代表者への報告
- 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

⑤事故又は違反への対処をする上で望まれる事項

- 事実関係、再発防止策等の公表

- その他、以下の項目等の実施
  ア）事実調査、イ）影響範囲の特定、ウ）影響を受ける可能性のある本人及び主務大臣等への報告、エ）原因の究明、オ）再発防止策の検討・実施

【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】

以下、（ⅰ）取得・入力、（ⅱ）移送・送信、（ⅲ）利用・加工、（ⅳ）保管・バックアップ、（ⅴ）消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

（ⅰ）取得・入力

ⅰ）作業責任者の明確化

- 個人データを取得する際の作業責任者の明確化
- 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。）

ⅱ）手続の明確化と手続に従った実施

- 取得・入力する際の手続の明確化
- 定められた手続による取得・入力の実施
- 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
- 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
- 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。)

ⅲ）作業担当者の識別、認証、権限付与

- 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
- 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
- 作業担当者に付与する権限の限定
- 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

ⅳ）作業担当者及びその権限の確認

- 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
- アクセスの記録、保管と、権限外作業の有無の確認

（ⅱ）移送・送信

ⅰ）作業責任者の明確化

- 個人データを移送・送信する際の作業責任者の明確化

ⅱ）手続の明確化と手続に従った実施

- 個人データを移送・送信する際の手続の明確化

- 定められた手続による移送・送信の実施
- 個人データを移送・送信する場合の個人データの暗号化（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）
- ＦＡＸ等におけるあて先番号確認と受領確認
- 個人データを記した文書をＦＡＸ等に放置することの禁止
- 暗号鍵やパスワードの適切な管理

ⅲ）作業担当者の識別、認証、権限付与
- 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
- 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
- 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。）
- 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

ⅳ）作業担当者及びその権限の確認
- 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
- アクセスの記録、保管と、権限外作業の有無の確認

（ⅲ）利用・加工

ⅰ）作業責任者の明確化
- 個人データを利用・加工する際の作業責任者の明確化

ⅱ）手続の明確化と手続に従った実施
- 個人データを利用・加工する際の手続の明確化
- 定められた手続による利用・加工の実施
- 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
- 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
- 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。）

ⅲ）作業担当者の識別、認証、権限付与
- 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
- 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
- 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。）
- 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

iv）作業担当者及びその権限の確認

- 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
- アクセスの記録、保管と権限外作業の有無の確認

（iv）保管・バックアップ

i）作業責任者の明確化

- 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

ii）手続の明確化と手続に従った実施

- 個人データを保管・バックアップする際の手続※の明確化

※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム(ＯＳ)やアプリケーションのバックアップも必要となる場合がある。

- 定められた手続による保管・バックアップの実施
- 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
- 暗号鍵やパスワードの適切な管理
- 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
- 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
- 個人データを記録している媒体の遠隔地保管
- 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
- 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

iii）作業担当者の識別、認証、権限付与

- 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
- 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
- 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。）
- 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

iv）作業担当者及びその権限の確認

- 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
- アクセスの記録、保管と権限外作業の有無の確認

（v）消去・廃棄

i）作業責任者の明確化

- 個人データを消去する際の作業責任者の明確化
- 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

ii）手続の明確化と手続に従った実施

- 消去・廃棄する際の手続の明確化

- 定められた手続による消去・廃棄の実施
- 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
- 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
- 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。)
- 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。)

iii) 作業担当者の識別、認証、権限付与
- 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
- 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
- 作業担当者に付与する権限の限定
- 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

iv) 作業担当者及びその権限の確認
- 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
- アクセスの記録、保管、権限外作業の有無の確認

人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】
①雇用契約時及び委託契約時における非開示契約の締結
②従業者に対する教育・訓練の実施
なお、管理者が定めた規程等を守るように監督することについては、法第２１条を参照。

【各項目について講じることが望まれる事項】
①雇用契約時及び委託契約時における非開示契約の締結をする上で望まれる事項
- 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
  用契約又は委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。
- 非開示契約に違反した場合の措置に関する規程の整備
  ※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

②従業者に対する周知・教育・訓練を実施する上で望まれる事項

- 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
- 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
- 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

物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

【物理的安全管理措置として講じなければならない事項】

①入退館（室）管理の実施

②盗難等の防止

③機器・装置等の物理的な保護

【各項目について講じることが望まれる事項】

①入退館（室）管理を実施する上で望まれる事項

- 個人データを取り扱う業務上の、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
- 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

②盗難等を防止する上で望まれる事項

- 離席時の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等への放置の禁止
- 離席時のパスワード付きスクリーンセイバ等の起動
- 個人データを含む媒体の施錠保管
- 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
- 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

③機器・装置等を物理的に保護する上で望まれる事項

- 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

技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】

①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
⑥個人データの移送・送信時の対策
⑦個人データを取り扱う情報システムの動作確認時の対策
⑧個人データを取り扱う情報システムの監視

【各項目について講じることが望まれる事項】

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項 ・・・・

- 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アクセス権限を有する従業者本人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
- IDとパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDを停止する等の措置を講じることが望ましい。
- 個人データへのアクセス権限を有する各従業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

②個人データへのアクセス制御を行う上で望まれる事項

- 個人データへのアクセス権限を付与すべき従業者数の最小化
- 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。）
- 従業者に付与するアクセス権限の最小化
- 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
- 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）
- 個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）
- 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、業務上必要となる従業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）

情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。
特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。

- 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）

③個人データへのアクセス権限の管理を行う上で望まれる事項

- 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。）
- 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

④個人データへのアクセスの記録を行う上で望まれる事項

- 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）
- 採取した記録の漏えい、滅失及びき損からの適切な保護
  個人データを取り扱う情報システムの記録が個人情報に該当する場合 があることに留意する。

⑤個人データを取り扱う情報システムについて不正ソフトウェア対策を実施する上で望まれる事項

- ウイルス対策ソフトウェアの導入
- 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
- 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）

⑥個人データの移送（運搬、郵送、宅配便等）・送信時の対策の上で望まれる事項

- 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）
- 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

⑦個人データを取り扱う情報システムの動作確認時の対策の上で望まれる事項

- 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

- 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

⑧個人データを取り扱う情報システムの監視を行う上で望まれる事項

- 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
- 個人データへのアクセス状況（操作内容も含む。）の監視

  個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。

3）従業者の監督（法第２１条関連）

法第２１条 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

個人情報取扱事業者は、法第２０条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない（１．(4)※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。）。その際、本人の個人データが漏えい、滅失又はき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状況等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する。
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、派遣社員等も含まれる。

【従業者に対して必要かつ適切な監督を行っていない場合】

事例１）従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合

事例２）内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】

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（以下「モニタリング」という。）を実施する場合は、次の点に留意する。
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。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。
なお、本ガイドライン及び雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（平成１６年厚生労働省告示第２５９号）第三 九 （一）に規定する雇用管理に関する個人情報の取扱いに関する重要事項とは、モニタリングに関する事項等をいう。

- モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
- モニタリングの実施に関する責任者とその権限を定めること。
- モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。
- モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。

4）委託先の監督（法第２２条関連）

法第２２条
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は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

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、法第２０条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない（１．(4)※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。）。その際、本人の個人データが漏えい、滅失又はき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状況等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する。

「必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。

なお、優越的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはならない。

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する。

【受託者に必要かつ適切な監督を行っていない場合】

事例１） 個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外

部の事業者に委託した場合で、受託者が個人データを漏えいした場合

事例２）個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合

事例３）再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】・・・

- 委託者及び受託者の責任の明確化
- 個人データの安全管理に関する事項
  - 個人データの漏えい防止、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
  - 委託契約期間
  - 委託契約終了後の個人データの返還・消去・廃棄に関する事項
- 再委託に関する事項
  - 再委託を行うに当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
- 契約内容が遵守されていることの確認(例えば、情報セキュリティ監査なども含まれる。)
- 契約内容が遵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

(4) 第三者への提供（法第２３条関連）

① 原則（法第２３条第１項関連）

法第２３条第１項

個人情報取扱事業者は、次に掲げる場合を除くほか、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らない。

1 法令に基づく場合

2 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

3 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって本人の同意を得ることが困難であるとき。

4 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

個人情報取扱事業者は、あらかじめ※1、本人の同意を得※2ないで、個人データを第三者に提供してはならない（１．(4)※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。）。同意の取得に当たっては、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

※１「あらかじめ」とは、「個人データの第三者への提供に当たりあらかじめ」をいう。
※２「本人の同意を得（る）」については、１．(10)参照。

【第三者提供とされる事例】（ただし、法第２３条第４項各号の場合を除く。）
事例１） 親子兄弟会社、グループ会社の間で個人データを交換する場合
事例２） フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
事例３） 同業者間で、特定の個人データを交換する場合
事例４） 外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】（ただし、利用目的による制限がある。）
事例）同一事業者内で他部門へ個人データを提供すること。

ただし、以下の場合は本人の同意なく第三者への提供を行うことができる。

ⅰ．法令に基づいた個人データを提供する場合

（事例は、(1)⑤ⅰ．と同様。）

【追加事例】
事例）法第４２条第２項に基づき認定個人情報保護団体が対象事業者に資料提出等を求め、対象事業者がそれに応じて資料提出をする場合

ⅱ．人（法人を含む。）の生命又は財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人データの提供が必要であり、かつ、本人の同意を得ることが困難である場合（他の方法により、当該権利利益の保護が十分可能である場合を除く。）

（事例は、(1)⑤ⅱ．と同様。）

ⅲ．公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）

（事例は、(1)⑤ⅲ．と同様。）

ⅳ．国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であって、協力する民間企業等が当該国の機関等に個人データを提供することについて、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがある場合

（事例は、(1)⑤ⅳ．と同様。）

② オプトアウト（法第２３条第２項関連）

個人情報取扱事業者は、第三者提供におけるオプトアウト※1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る。

※1「第三者提供におけるオプトアウト」とは、提供に当たりあらかじめ、以下のｉ．～ⅳ．の情報を、本人に通知※2し、又は本人が容易に知り得る状態※2に置いておくとともに、本人の求めに応じて第三者への提供を停止することをいう。

※2「本人に通知」については、１．(7)参照。
※3「本人が容易に知り得る状態」については、１．(11)参照。

【オプトアウトの事例】
事例１）住宅地図業者（表札や郵便受けを調べて住宅地図を作成し、販売（不特定多数への第三者提供））
事例２）データベース事業者（ダイレクトメール用の名簿等を作成し、販売）

法第２３条第２項
個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
1 第三者への提供を利用目的とすること。
2 第三者に提供される個人データの項目
3 第三者への提供の手段又は方法
4 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

以下のｉ．～ⅳ．の事項すべてをあらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

ⅰ．第三者への提供を利用目的とすること。

ⅱ．第三者に提供される個人データの項目

事例１） 氏名、住所、電話番号
事例２） 氏名、商品購入履歴

ⅲ．第三者への提供の手段又は方法

事例１） 書籍として出版
事例２） インターネットに掲載
事例３） プリントアウトして交付等

ⅳ．本人の求めに応じて第三者への提供を停止すること。

③ 第三者に該当しないもの（法第２３条第４項関連）

以下のⅰ．～ⅲ．の場合は、第三者には該当しないため、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。

ⅰ．委託（法第２３条第４項第１号関連）

法第２３条第４項第１号
次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。 １ 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合。

個人データの取扱いに関する業務の全部又は一部を委託する場合は、第三者に該当しない。
個人情報取扱事業者には、委託先に対する監督責任が課される（法第２２条関連）。

事例１） データの打ち込み等、情報処理を委託するために個人データを渡す場合
事例２） 百貨店が注文を受けた商品の配送のために、宅配業者に個人データを渡す場合

ⅱ．事業の承継（法第２３条第４項第２号関連）

法第２３条第４項第２号

次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。

２ 合併その他の事由による事業の承継に伴って個人データが提供される場合

合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合は、第三者に該当しない。

事業の承継後も、個人データが譲渡される前の利用目的の範囲内で利用しなければならない。

事業の承継のための契約を締結するより前の交渉段階で、相手会社から自社の調査を受け、自社の個人データを相手会社へ提供する場合は、第三者提供となり得るため、注意する必要がある。

事例１） 合併、分社化により、新会社に個人データを渡す場合
事例２） 営業譲渡により、譲渡先企業に個人データを渡す場合

ⅲ．共同利用（法第２３条第４項第３号関連）

法第２３条第４項第３号

次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。

３ 個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

個人データを特定の者との間で共同して利用する場合、以下のア）～エ）の情報をあらかじめ※1本人に通知※2し、又は本人が容易に知り得る状態※3に置いておくとともに、共同して利用することを明らかにしている場合は、第三者に該当しない。

※１「あらかじめ」とは、「個人データの共同利用に当たりあらかじめ」をいう。
※２「本人に通知」については、１．(7)参照。
※３「本人が容易に知り得る状態」については、１．(11)参照。

【共同利用を行うことがある事例】

事例１） グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合
事例２） 親子兄弟会社の間で利用目的の範囲内で個人データを共同利用する場合
事例３） 外国の会社と利用目的の範囲内で個人データを共同利用する場合

ア） 共同して利用される個人データの項目

事例１） 氏名、住所、電話番号
事例２） 氏名、商品購入履歴

イ） 共同利用者の範囲（本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。）

ウ） 利用する者の利用目的（共同して利用する個人データのすべての利用目的）

エ） 開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称（共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者を、「責任を有する者」といい、共同利用者の内部の担当責任者をいうのではない。）

法第２３条第５項
個人情報取扱事業者は、前項第３号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

上記ア）イ）については、変更することができないが、ウ）エ）については、社会通念上、本人が想定することが困難でないと認められる範囲内※1で変更することができ、変更する前に、本人に通知※2又は本人が容易に知り得る状態※3に置かなければならない。

※１「本人が想定することが困難でないと認められる範囲内」については、(1)②参照。
※２「本人に通知」については、１．(7)参照。
※３「本人が容易に知り得る状態」については、１．(11)参照。

④ 雇用管理に関する個人データ関連

個人データの第三者への提供（法第２３条第１項第１号から第４号までに該当する場合を除く。）のうち、雇用管理に関するものについては、次に掲げる事項に留意することが望ましい。その際、事業の性質及び雇用管理に関する個人データの取扱状況等に応じ、必要かつ適切な措置を講じるものとする。

ここでいう雇用管理に関する個人データの第三者への提供とは、従業員の子会社への出向に際して、出向先に当該従業員の人事考課情報等の雇用管理に関する個人データを提供する場合や、労働者を派遣する際に技術者の能力に関する情報等の雇用管理に関する個人データ

を提供する場合を指すものである。

したがって、企業から、その従業員の氏名、役職等の個人データの提供を受け、当該情報をデータベース化し、公開、販売することを目的とする者への提供のような場合はこの限りではない。

・提供先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこととされていること。
・当該個人データの再提供を行うに当たっては、あらかじめ文書をもって事業者の了承を得ること。
・提供先における保管期間等を明確化すること。
・利用目的達成後の個人データを返却し、又は破棄し若しくは削除し、これと併せてその処理が適切かつ確実になされていることを事業者において確認すること。
・提供先における個人データの複写及び複製（安全管理上必要なバックアップを目的とするものを除く。）を禁止すること。

(5) 保有個人データに関する事項の公表、保有個人データの開示・訂正・利用停止等 （法第２４条～第３０条関連）

1) 保有個人データに関する事項の公表等（法第２４条関連）

① 保有個人データに関する事項の本人への周知（法第２４条第１項関連）

法第２４条第１項

個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

1 当該個人情報取扱事業者の氏名又は名称

2 すべての保有個人データの利用目的（第１８条第４項第１号から第３号までに該当する場合を除く。）

3 次項、次条第１項、第２６条第１項又は第２７条第１項若しくは第２項の規定による求めに応じる手続（第３０条第２項の規定により手数料の額を定めたときは、その手数料の額を含む。）

4 前３号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

政令第５条

法第２４条第１項第４号の政令で定めるものは、次に掲げるものとする。

1 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先

2 当該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ある場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

個人情報取扱事業者は、保有個人データについて、以下のⅰ．～ⅳ．の情報を本人の知り得

る状態(本人の求めに応じて遅滞なく回答する場合を含む。)※1に置かなければならない(1.(4)※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。)。
法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第18条の規定が適用されないので、法施行時に法第24条第1項の措置を講ずる必要がある。

※1「本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)」については、1.(12)参照。

i. 個人情報取扱事業者の氏名又は名称

ii. すべての保有個人データの利用目的(ただし、一定の場合※2を除く。法第15条以下で用いられる個人情報に関する「利用目的」に同じ。)

※2「一定の場合」とは、以下をいう。
ア) 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合(事例は(2)⑤iと同様。)
イ) 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合(事例は(2)⑤iiと同様。)
ウ) 国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が国の機関等から受け取った個人情報の利用目的を本人に通知し、又は公表することにより、当該事務の遂行に支障を及ぼすおそれがある場合(事例は(2)⑤iiiと同様。)

iii. 保有個人データの利用目的の通知及び保有個人データの開示に係る手数料の額(定めた場合に限る)※3並びに開示等の求め※4の手続

※3行政機関の保有する情報の公開に関する法律(平成11年法律第42号)第16条及び同法施行令(平成12年政令第41号)第13条第1項第1号に基づく開示請求に係る手数料は300円である(開示実施手数料は別途発生)。

※4「開示等の求め」とは、保有個人データの利用目的の通知、保有個人データの開示、保有個人データの内容の訂正、追加又は削除、保有個人データの利用の停止又は消去、保有個人データの第三者への提供の停止の求めをいう。

iv. 保有個人データの取扱いに関する苦情及び問い合わせの申出先(個人情報取扱事業者が認定個人情報保護団体※5に所属している場合は、その団体の名称及び申出先も含む。)

※5「認定個人情報保護団体」制度について
苦情処理業務等、個人情報の適正な取扱いの確保を目的として業務を行う民間団体に対し、主務大臣が認定する制度であり、この制度の設置により、当該業務の信頼性を確保し、民間

団体による個人情報の保護の推進を図ろうとするものである（法第３７条以下参照）。

（参考）

法第３７条第１項

個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第３号ロにおいて同じ。）は、主務大臣の認定を受けることができる。

１ 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。）の個人情報の取扱いに関する第４２条の規定による苦情の処理

２ 個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供

３ 前２号に掲げるもののほか、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

法第３７条第２項

前項の認定を受けようとする者は、政令で定めるところにより、主務大臣に申請しなければならない。

法第３７条第３項

主務大臣は、第１項の認定をしたときは、その旨を公示しなければならない。

法第４２条第１項

認定個人情報保護団体は、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。

法第４２条第２項

認定個人情報保護団体は、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができる。

法第４２条第３項

対象事業者は、認定個人情報保護団体から前項の規定による求めがあったときは、正当な理由がないのに、これを拒んではならない。

② 保有個人データの利用目的の通知（法第２４条第２項、第３項関連）

法第２４条第２項

個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次の各号のいずれかに該当する場合は、この限りでない。

1 前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合

2 第１８条第４項第１号から第３号までに該当する場合

法第２４条第３項

個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

個人情報取扱事業者は、以下のｉ．～ⅳ．の場合を除いて、本人から、自己が識別される保有個人データの利用目的の通知を求められたときは、遅滞なく、本人に通知※しなければならない。なお、通知しない旨を決定したときも、遅滞なく、本人に通知しなければならない（１．(4)※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。）。

※ 「本人に通知」については、１．(7)参照。

ｉ． 上記①の措置により、自己が識別される保有個人データの利用目的が明らかである場合

ⅱ． 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

（事例は(2)⑤ｉと同様。）

ⅲ． 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合

（事例は(2)⑤ⅱと同様。）

ⅳ． 国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が国の機関等から受け取った保有個人データの利用目的を本人に通知し、又は公表することにより、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがある場合

（事例は(2)⑤ⅲと同様。）

2) 保有個人データの開示（法第２５条関連）

法第２５条第１項

個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

1 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
2 当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
3 他の法令に違反することとなる場合

政令第６条

法第２５条第１項の政令で定める方法は、書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）とする。

個人情報取扱事業者は、本人から、自己が識別される保有個人データの開示（存在しないときにはその旨を知らせることを含む。）を求められたときは、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときはその方法※１）により、遅滞なく、当該保有個人データを開示しなければならない（１．(4)※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。）。

なお、他の法令の規定により、別途開示の手続が定められている場合には、当該別途の開示の手続が優先されることとなる。

雇用管理情報の開示の求めに応じる手続については、個人情報取扱事業者は、あらかじめ、労働組合等と必要に応じ協議した上で、本人から開示を求められた保有個人データについて、その全部又は一部を開示することによりその業務の適正な実施に著しい支障を及ぼすおそれがある場合に該当するとして非開示とすることが想定される保有個人データの開示に関する事項を定め、労働者等に周知させるための措置を講ずるよう努めなければならない。

※１「開示の求めを行った者が同意した方法があるときはその方法」について

開示の方法としては、求めを行った者が同意している場合には電子メール、電話等様々な方法が可能であり、書面の交付による方法は同意がなくても可能との意味である。

また、開示の求めを行った者から開示の方法について特に指定がなく、個人情報取扱事業者が提示した方法に対して異議を述べなかった場合（電話での開示の求めがあり、必要な本人確認等の後、そのまま電話で問い合わせに回答する場合を含む。）は、当該方法について同意があったものとみなすことができる。開示の求めがあった者からの同意の取り方として、個人情報取扱事業者が開示方法を提示して、その者が希望する複数の方法の中から当該事業者が選択することも考えられる。

ただし、開示することにより下記のｉ．～ⅲ．のいずれかに該当する場合は、その全部又は一部を開示しないことができるが、この場合は、その旨を本人に通知※２しなければならない。

※２「本人に通知」については、１．(7)参照。

ｉ．　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

事例）　医療機関等において、病名等を開示することにより、本人の心身状況を悪化させるおそれがある場合

ⅱ．　個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

事例１）試験実施機関において、採点情報のすべてを開示することにより、試験制度の維持に著しい支障を及ぼすおそれがある場合

事例２）同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼすおそれがある場合

ⅲ．他の法令に違反することとなる場合

事例）　金融機関が「組織的な犯罪の処罰及び犯罪収益の規制等に関する法律」第５４条第１項に基づいて、主務大臣に取引の届出を行っていたときに、当該届出を行ったことが記録されている保有個人データを開示することが同条第２項の規定に違反する場合

3）保有個人データの訂正等（法第２６条関連）

法第２６条第１項
個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。
法第２６条第２項
個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知しなければならない。

個人情報取扱事業者は、本人から、保有個人データに誤りがあり、事実でないという理由によって訂正等を求められた場合には、原則※１として、訂正等※２を行い、訂正等を行った場合には、その内容を本人に対し、遅滞なく通知しなければならない（１．(4)※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。)。

なお、他の法令の規定により特別の手続が定められている場合には、当該特別の手続が優先されることとなる。

※1「原則」…利用目的から見て訂正等が必要ではない場合や誤りである旨の指摘が正しくない場合には、訂正等を行う必要はない。ただし、その場合には、遅滞なく、訂正等を行わない旨を本人に通知※3しなければならない。
※2「訂正等」とは、保有個人データの内容の訂正、追加又は削除をいう。
※3「本人に通知」については、1．(7)参照。

【訂正を行う必要がない事例】
事例）訂正等の対象が事実でなく評価に関する情報である場合

4）保有個人データの利用停止等（法第27条関連）

法第27条第1項

個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第16条の規定に違反して取り扱われているという理由又は第17条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

法第27条第2項

個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第23条第1項の規定に違反して第三者に提供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

法第27条第3項

個人情報取扱事業者は、第1項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

個人情報取扱事業者は、本人から、手続違反※1の理由により保有個人データの利用停止等※2が求められた場合には、原則※3として、当該措置を行わなければならない。なお、利用の停止等を行った場合には、遅滞なく、その旨を本人に通知※4しなければならない（１．(4)※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。）。

※１「手続違反」とは、同意のない目的外利用、不正な取得、又は同意のない第三者提供をいう。
※２「利用の停止等」とは、保有個人データの利用の停止、消去又は第三者への提供の停止をいう。
※３「原則」…違反を是正するための必要な限度を超えている場合や手続違反である旨の指摘が正しくない場合には、利用の停止等を行う必要はない。ただし、その場合には、遅滞なく、利用の停止等を行わない旨を本人に通知しなければならない。
※４「本人に通知」については、１．(7)参照。

5) 理由の説明（法第２８条関連）

法第２８条
個人情報取扱事業者は、第２４条第３項、第２５条第２項、第２６条第２項又は前条第３項の規定により、本人から求められた措置の全部又は一部についてその措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。

個人情報取扱事業者は、保有個人データの公表・開示・訂正・利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨を本人に通知※する場合は、併せて、本人に対して、その理由を説明するように努めなければならない。

※「本人に通知」については、１．(7)参照。

6) 開示等の求めに応じる手続（法第２９条関連）

法第２９条第１項

個人情報取扱事業者は、第２４条第２項、第２５条第１項、第２６条第１項又は第２７条第１項若しくは第２項の規定による求め（以下この条において「開示等の求め」という。）に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。

法第２９条第２項

個人情報取扱事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、個人情報取扱事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。

法第２９条第３項

開示等の求めは、政令で定めるところにより、代理人によってすることができる。

法第２９条第４項

個人情報取扱事業者は、前３項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

政令第７条

法第２９条第１項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる事項は、次に掲げるとおりとする。

1 開示等の求めの申出先

2 開示等の求めに際して提出すべき書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

3 開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

4 法第３０条第１項の手数料の徴収方法

政令第８条

法第２９条第３項の規定により開示等の求めをすることができる代理人は、次に掲げる代理人とする。

1 未成年者又は成年被後見人の法定代理人

2 開示等の求めをすることにつき本人が委任した代理人

① 個人情報取扱事業者は、開示等の求め※1において、その求めを受け付ける方法として下記のｉ．～ⅳ．の事項を定めることができる。また、その求めを受け付ける方法を定めた場合には、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）※2に置いておかなければならない（上記(5) 1）参照）。なお、個人情報取扱事業者が、開示等の求めを受け付ける方法を合理的な範囲で定めたときで、求めを行った者がそれに従

わなかった場合は、開示等を拒否することができる。

※１「開示等の求め」とは、保有個人データの利用目的の通知、保有個人データの開示、保有個人データの内容の訂正、追加又は削除、保有個人データの利用の停止又は消去、保有個人データの第三者への提供の停止の求めをいう。
※２「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」については、１．(12)参照。

ⅰ．開示等の求めの受付先

ⅱ．開示等の求めに際して提出すべき書面（電子的方式、磁気的方式その他、人の知覚によっては認識することができない方式で作られる記録を含む。）の様式、その他の開示等の求めの受付方法（郵送、ＦＡＸで受け付ける等）

ⅲ．開示等の求めをする者が本人又はその代理人（(ア)未成年者又は成年被後見人の法定代理人、(イ)開示等の求めをすることにつき本人が委任した代理人）であることの確認の方法（ただし、確認の方法は、事業の性質、保有個人データの取扱状況、開示等の求めの受付方法等に応じ、適切なものでなければならない。）

事例１）　本人の場合（来所）：運転免許証、健康保険の被保険者証、写真付き住民基本台帳カード、旅券（パスポート）、外国人登録証明書、年金手帳、印鑑証明書と実印
事例２）　本人の場合（オンライン）：IDとパスワード
事例３）　本人の場合（電話）：一定の登録情報（生年月日等）、コールバック
事例４）　本人の場合（送付（郵送、ＦＡＸ等））：運転免許証のコピーと住民票の写し
事例５）　本人の場合（送付（郵送、ＦＡＸ等））：運転免許証や健康保険の被保険者証等の公的証明書のコピーの送付を顧客等から受け、当該公的証明書のコピーに記載された顧客等の住所にあてて文書を書留郵便により送付
事例６）　代理人の場合（来所）：本人及び代理人ついて、運転免許証、健康保険の被保険者証、旅券（パスポート）、外国人登録証明書、年金手帳、弁護士の場合は登録番号、代理を示す旨の委任状

ⅳ．保有個人データの利用目的の通知、又は保有個人データの開示をする際に徴収する手数料の徴収方法

なお、開示等の求めを受け付ける方法を定めない場合には、自由な申請を認めることとなる。

②　個人情報取扱事業者は、円滑に開示等の手続が行えるよう、本人に対し、自己のデータの特定に必要な事項（住所、ID、パスワード、会員番号等）の提示を求めることができ

る。なお、本人が容易に自己のデータを特定できるよう、自己の保有個人データの特定に資する情報の提供その他本人の利便性を考慮しなければならない。

③ 個人情報取扱事業者は、開示等の求めに応じる手続を定めるに当たっては、必要以上に煩雑な書類を求めることや、求めを受け付ける窓口を他の業務を行う拠点とは別にいたずらに不便な場所に限定すること等して、本人に過重な負担を課することのないよう配慮しなければならない。

7) 手数料（法第３０条関連）

法第３０条第１項 個人情報取扱事業者は、第２４条第２項の規定による利用目的の通知又は第２５条第１項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。 法第３０条第２項 個人情報取扱事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

個人情報取扱事業者は、保有個人データの利用目的の通知、又は保有個人データの開示を求められたときは、当該措置の実施に関し、手数料の額を定めることができる。また、手数料の額を定めた場合には、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）※に置いておかなければならない（上記(5) 1）参照）。なお、手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない（(5)1）①iii．参照）。

※「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」については、１．(12)参照。

(6) 苦情の処理（法第３１条関連）

法第３１条第１項 個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。 法第３１条第２項 個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。また、苦情の適切かつ迅速な処理を行うに当たり、苦情処理窓口の設置や苦

情処理の手順を定める等必要な体制の整備に努めなければならない。もっとも、無理な要求にまで応じなければならないものではない。
なお、必要な体制の整備に当たっては、日本工業規格 JISZ9920「苦情対応マネジメントシステムの指針」を参考にすることができる。

(7) 経過措置（法附則第２条～第５条関連）

（本人の同意に関する経過措置）
法附則第２条
この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第１５条第１項の規定により特定される利用目的以外の目的で個人情報を取り扱うことを認める旨の同意に相当するものであるときは、第１６条第１項又は第２項の同意があったものとみなす。
法附則第３条
この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第２３条第１項の規定による個人データの第三者への提供を認める旨の同意に相当するものであるときは、同項の同意があったものとみなす。
（通知に関する経過措置）
法附則第４条
第２３条第２項の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。
法附則第５条
第２３条第４項第３号の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同号の規定により行われたものとみなす。

(1)③、(1)④及び(4)①の「本人の同意」については、法施行前に得たものであっても、法に基づく同意があったものとみなされる。

また、(4)②及び(4)③ⅲ．の「本人に通知」については、法施行前に本人に通知していても、法に基づき、本人に通知したものとみなされる。

なお、法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第１８条（取得に際しての利用目的の通知等）の規定は適用されない（(2)②参照）。ただし、保有個人データに関する事項の本人への周知については、法施行時に法第２４条第１項の措置を講ずる必要がある（(5)１）①参照）。

３．民間団体付属の研究機関等における個人情報の取扱いについて

法第５０条第１項第３号 個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。 ３ 大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者 学術研究の用に供する目的

民間団体付属の研究機関等における研究活動についても、個人情報を取り扱う場面があるが、当該機関が学術研究を主たる目的とするものであって、当該活動が学術研究の用に供する目的である場合には、法第５０条第１項第３号により、法の適用除外となる。そのため、個人情報の取扱いを含む研究活動を行う、経済産業分野における民間団体付属の研究機関等について、法第５０条第１項第３号の考え方を整理する。

民間企業の研究機関等、「○○研究所」との名称を有している機関であっても、単に製品開発を目的としているものについては、学術研究を主たる目的として活動しているものとはいえないことから、本法の「学術研究を目的とする機関又は団体」には該当しない。

※法第５０条第１項第３号の考え方

法第５０条第１項第３号に規定する「大学その他の学術研究を目的とする機関」とは、学術研究（新しい法則や原理の発見、分析や方法論の確立、新しい知識やその応用方法の体系化、先端的な学問領域の開拓等）を主たる目的とする機関である。

そのような機関において、個人情報を取り扱う目的の全部又は一部が、学術研究の用に供する目的である場合には、個人情報取扱事業者としての義務を課されない。

【適用除外となる場合】

事例）学術研究を主たる目的とする団体付属の研究機関において、個人情報を利用する目的の全部又は一部が学術研究である場合

【適用除外とならない場合】

事例１） 学術研究を主たる目的とする団体付属の研究機関において、個人情報を利用する目的が商品開発情報の分析のみ（学術研究目的を含まない。）である場合

事例２） 学術研究を主たる目的としない団体付属の研究機関

Ⅲ．「勧告」、「命令」及び「緊急命令」についての考え方

法第３４条第１項

主務大臣は、個人情報取扱事業者が第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

法第３４条第２項

主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる。

法第３４条第３項

主務大臣は、前２項の規定にかかわらず、個人情報取扱事業者が第１６条、第１７条、第２０条から第２２条まで又は第２３条第１項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

法第５６条

第３４条第２項又は第３項の規定による命令に違反した者は、６月以下の懲役又は３０万円以下の罰金に処する。

法第５８条第１項

法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。）の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、前２条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。

法第５８条第２項

法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

法第３４条に規定される経済産業大臣の「勧告（第１項）」「命令（第２項）」及び「緊急命令（第３項）」については、個人情報取扱事業者が本ガイドラインに沿って必要な措置等を講じたか否かにつき判断して行うものとする。

すなわち、本ガイドライン中、「しなければならない」と記載されている規定について、それに従わなかった場合は、法第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定違反と判断され得る。違反と判断された際、実際、「勧告」を行うこととなるのは、個人の権利利益を保護するため必要があると認めるときである。一方、本ガイドライン中、「望ましい」と記載されている規定については、それに従わなかった場合でも、法第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定違反と判断されることはないが、個人情報保護の推進の観点か

ら個人情報取扱事業者においては、できるだけ取り組むことが望まれる。

「命令」は、単に「勧告」に従わないことをもって発することはなく、正当な理由なくその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときに限られる。なお、「勧告」に従わなかったか否かを明確にするため、経済産業大臣は、「勧告」に係る措置を講ずべき期間を設定して「勧告」を行うこととする。

「緊急命令」は、個人情報取扱事業者が法第１６条、第１７条、第２０条から第２２条まで又は第２３条第１項の規定に違反した場合において、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときに、「勧告」を前置せずに行う。

なお、「命令」及び「緊急命令」に従わなかったか否かを明確にするため、経済産業大臣は、「命令」及び「緊急命令」に係る措置を講ずべき期間を設定して「命令」及び「緊急命令」を行い、当該期間中に措置が講じられない場合は、「罰則（法第５６条、第５８条）」を適用される。

Ⅳ．ガイドラインの見直し

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて毎年見直しを行うよう努めるものとする。

Ⅴ．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

個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのコンプライアンス・プログラムを策定し、実施し、維持し及び改善を行うことが望ましい。

なお、その体制の整備に当たっては、日本工業規格 JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 JISX5070「セキュリティ技術 － 情報技術セキュリティの評価基準」及び日本工業規格 JISX5080「情報セキュリティマネジメントの実践のための規範」等を参考にすることができる。

また、個人情報取扱事業者は、以下の事項を参考として「個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）」を策定し、ウェブ画面への掲載等により公表することが望ましい。

① 事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。

ⅰ．取得する個人情報の利用目的（法第１８条関係）

ⅱ．＜本人の同意なく第三者提供する場合＞（法第２３条第２項及び第３項関係）

・ 利用目的に第三者提供が含まれていること。

・ 第三者に提供される個人データの項目
・ 第三者への提供の手段又は方法
・ 本人の求めに応じて第三者への提供を停止すること。

iii．＜共同利用する場合＞（法第２３条第４項及び第５項）
・ 特定の者との間で共同利用すること。
・ 共同して利用される個人データの項目
・ 共同利用者の範囲
・ 共同して利用する者の利用目的
・ 共同して利用する者のうち、個人データの管理について責任を有する者の氏名又は名称

iv．以下の保有個人データに関すること（法第２４条関係）。
・ 自己の氏名又は名称
・ すべての保有個人データの利用目的
・ 「開示等の求め」に応じる手続（定めた場合に限る。）
・ 保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る。）
・ 苦情の申出先（認定個人情報保護団体の対象事業者※である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先を含む。）ｖ．開示等の求めに応じる手続に関すること（法第２９条関係）。
・ 申請書の様式（定めた場合に限る。）
・ 受け付ける方法（定めた場合に限る。）
・ 保有個人データの特定に役立つ情報の提供

vi．問い合わせ及び苦情の受付窓口に関すること（法第２３条第５項、第２４条第１項、第２９条第１項及び第３１条関係）。

② 個人情報の保護に関する法律を遵守すること。

③ 個人情報の安全管理措置に関すること。

④ コンプライアンス・プログラムの継続的改善に関すること。

※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等

●個人情報の保護に係る関係省庁のガイドライン等一覧

（出典：内閣府国民生活局企画課個人情報保護推進室　ホームページより抜粋）
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

分野		所管省庁	ガイドライン・指針等の名称	告示年月日等
医療	医療一般	厚生労働省	「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」 http://www.mhlw.go.jp/houdou/2004/12/dl/h1227-6a.pdf	H16.12.24 告示
			「健康保険組合等における個人情報の適切な取扱いのためのガイドライン」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/kenkou.pdf	H16.12.27 告示
	研究	文部科学省 厚生労働省 経済産業省	「ヒトゲノム・遺伝子解析研究に関する倫理指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/genomu.pdf	H16.12.28 告示 (H13.3.29 指針の全部改正)
			「遺伝子治療臨床研究に関する指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/iden.pdf	H16.12.28 告示 (H14.3.27 指針全部改正)
			「疫学研究に関する倫理指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/ekigaku.pdf	H16.12.28 告示 (H14.6.17 指針全部改正)
			「臨床研究に関する倫理指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/rinshou.pdf	H16.12.28 告示 (H15.7.30 指針全部改正)
金融・信用	金融	金融庁	「金融分野における個人情報保護に関するガイドライン」 http://www.fsa.go.jp/siryou/siryou/kj-hogo/01.pdf	H16.12.6 告示
	信用	経済産業省	「経済産業分野のうち信用分野における個人情報保護ガイドライン」 http://www.meti.go.jp/feedback/downloadfiles/i41202ij.pdf	H16.12.17 告示
情報通信	電気通信	総務省	「電気通信事業における個人情報保護に関するガイドライン」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/denki.pdf	H16.8.31 告示 (H10.12.2.2 ガイドラインの改訂)
	放送	総務省	「放送受信者等の個人情報の保護に関する指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/housou.pdf	H16.8.31 告示
事業全般		経済産業省	「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」 http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf	H16.10.22 告示
			「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」 http://www.meti.go.jp/press/20041217010/041217iden.pdf	H16.12.17 告示

分野		所管省庁	ガイドライン・指針等の名称	告示年月日等
雇用管理	一般	厚生労働省	「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/koyou.pdf	H16.7.1 告示
			「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/tsuutatsu.pdf	H16.10.29 局長通達
	船員	国土交通省	「船員の雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/senin.pdf	H16.9.29 告示
警察		警察庁	「国家公安委員会が所管する事業を行う者等が講ずべき個人情報の保護のための措置に関する指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/kouan.pdf	H16.10.29 告示
法務		法務省	「法務省が所管する事業を行う事業者等が取り扱う個人情報の保護に関するガイドライン」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/houmu.pdf	H16.10.29 告示
			債権管理回収業分野ガイドライン案の公表	パブリックコメント募集終了
財務		財務省	「財務省所管分野における事業者が講ずべき個人情報の保護に関する指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/zaimu.pdf	H16.11.25 告示
教育		文部科学省	「学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/seito.pdf	H16.11.11 告示
福祉		厚生労働省	「福祉関係事業者における個人情報の適正な取扱いのためのガイドライン」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/fukushi.pdf	H16.11.30 策定
職業紹介等		厚生労働省	「職業紹介事業者、労働者の募集を行う者、募集受託者、労働者供給事業者等が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、職業紹介事業者の責務、募集内容の的確な表示等に関して適切に対処するための指針の一部を改正する告示」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/shokugyou.pdf	H16.11.4 告示（H11 指針の改定）
労働者派遣		厚生労働省	「派遣元事業主が講ずべき措置に関する指針の一部を改正する告示」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/haken.pdf	H16.11.4（H11 指針の改定）
国土交通		国土交通省	「国土交通省所管分野における個人情報保護に関するガイドライン」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/kokudo.pdf	H16.12.2 告示
農林水産		農林水産省	「個人情報の適正な取扱いを確保するために農林水産分野における事業者が講ずべき措置に関するガイドライン」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/nousui.pdf	H16.11.9 告示

●参考 JIS 規格

「JIS Q 15001：1999 個人情報保護に関するコンプライアンス・プログラムの要求事項」

「JIS Q 2001：2001 リスクマネジメントシステム構築のための指針」

平成１７年３月発行

発行所　財団法人 日本情報処理開発協会
東京都港区芝公園３丁目５番８号
機械振興会館内
ＴＥＬ　０３（３４３２）９３８７

印刷所　株式会社 美 行 企 画
東京都千代田区神田錦町２丁目５番地
鈴木第２ビル
ＴＥＬ　０３（３２１９）２９７１

16－H002