

目 次

	ページ
0.1 序文	1
0.2 ISMS の採用	1
0.2.1 概要	1
0.2.2 プロセスアプローチ	1
0.2.3 他のマネジメントシステムとの両立性	3
1 適用範囲	3
1.1 一般	3
1.2 適用	4
2 引用規格	4
3 用語及び定義	4
4 情報セキュリティマネジメントシステム	6
4.1 一般要求事項	6
4.2 ISMS の確立及び運営管理	6
4.2.1 ISMS の確立	6
4.2.2 ISMS の導入及び運用	8
4.2.3 ISMS の監視及びレビュー	8
4.2.4 ISMS の維持及び改善	9
4.3 文書化に関する要求事項	9
4.3.1 一般	9
4.3.2 文書管理	10
4.3.3 記録の管理	10
5 経営陣の責任	10
5.1 経営陣のコミットメント	10
5.2 経営資源の運用管理	11
5.2.1 経営資源の提供	11
5.2.2 教育・訓練, 意識向上及び力量	11
6 ISMS 内部監査	11
7 ISMS のマネジメントレビュー	12
7.1 一般	12
7.2 レビューへのインプット	12
7.3 レビューからのアウトプット	12
8 ISMS の改善	13
8.1 継続的改善	13
8.2 是正処置	13
8.3 予防処置	13

	ページ
附属書 A (規定) 管理目的及び管理策	14
附属書 B (参考) OECD 原則及びこの規格	26
附属書 C (参考) JIS Q 9001:2000, JIS Q 14001:2004, 及びこの規格の比較	27
参考文献	29

まえがき

この規格は、工業標準化法に基づき、日本工業標準調査会の審議を経て、経済産業大臣が制定した日本工業規格である。

この規格は、著作権法で保護対象となっている著作物である。

この規格の一部が、技術的性質をもつ特許権、出願公開後の特許出願、実用新案権、又は出願公開後の実用新案登録出願に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本工業標準調査会は、このような技術的性質をもつ特許権、出願公開後の特許出願、実用新案権、又は出願公開後の実用新案登録出願にかかわる確認について、責任をもたない。

白 紙

情報技術—セキュリティ技術— 情報セキュリティマネジメントシステム—要求事項

Information technology—Security techniques— Information security management systems—Requirements

0.1 序文

この規格は、2005年に第1版として発行された **ISO/IEC 27001**, Information technology—Security techniques—Information security management systems—Requirements を基に、技術的内容及び対応国際規格の構成を変更することなく作成した日本工業規格である。

なお、この規格で点線の下線を施してある“注記”及び“注”は、対応国際規格にはない事項である。

0.2 ISMS の採用

0.2.1 概要

この規格は、情報セキュリティマネジメントシステム（以下、ISMS という。）を確立、導入、運用、監視、レビュー、維持及び改善するためのモデルを提供するために作成された。ISMS の採用は、その組織の戦略的決定とすることが望ましい。ISMS の設計及び実施は、その組織のニーズ及び目的、セキュリティ全般への要求、採用しているプロセス、並びに組織の規模及び構造によって影響を受ける。これらの状況及びこれらを支えるシステムは時間とともに変化するであろう。したがって、ISMS の導入に際しては、その組織のニーズに従って規模の調整を図る（例えば、単純な状況には単純な ISMS をもってこたえる。）ことが期待される。この規格は、組織内・外の利害関係者が適合性のアセスメントを行うために使用することができる。

0.2.2 プロセスアプローチ

この規格は、組織の ISMS の確立、導入、運用、監視、レビュー、維持及び改善のために、プロセスアプローチを採用する。

組織が有効に機能するためには、多くの活動を明確にし、また、それらを運営管理する必要がある。インプットをアウトプットに変換することを可能にするために経営資源を使用して運営管理するあらゆる活動は、プロセスとみなすことができる。多くの場合、一つのプロセスからのアウトプットは、次のプロセスへの直接のインプットとなる。

そのようなプロセスを明確にし、かつ、相互作用させることと合わせて、それらのプロセスをシステムとして組織内に適用し、かつ、運営管理することを“プロセスアプローチ”と呼ぶ。

この規格が規定する情報セキュリティマネジメントのためのプロセスアプローチでは、利用者が次の点を重視することを期待する。

a) 組織の情報セキュリティ要求事項を理解し、かつ、情報セキュリティのための基本方針及び目的を確

立する必要性を理解する。

- b) その組織の事業リスク全般に対する考慮のもとで、組織の情報セキュリティリスクを運営管理するための管理策を導入し、運用する。
- c) その ISMS のパフォーマンス及び有効性を監視し、レビューする。
- d) 客観的な測定に基づいて継続的に改善する。

この規格は、“Plan-Do-Check-Act（計画－実行－点検－処置）”（PDCA）モデルを採用し、これを ISMS プロセスすべての構築に適用する。図 1 は、ISMS が、利害関係者からの情報セキュリティ要求事項及び期待をインプットとしてどう取り入れ、必要となる活動及びプロセスを経て、その要求事項及び期待を満たした情報セキュリティの成果をどう生み出すかを表している。また、図 1 は、箇条 4、5、6、7 及び 8 に規定するプロセス間のつながりも表している。

この PDCA モデルを採用することは、2002 年版の OECD ガイドライン¹⁾によって設定された、情報システム及びネットワークのセキュリティを律する諸原則を反映することでもある。この規格は、リスクアセスメント、セキュリティの設計及び実施、セキュリティマネジメント、並びに再評価について律するガイドラインの諸原則を実施するための強固なモデルを提供する。

注¹⁾ OECD Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

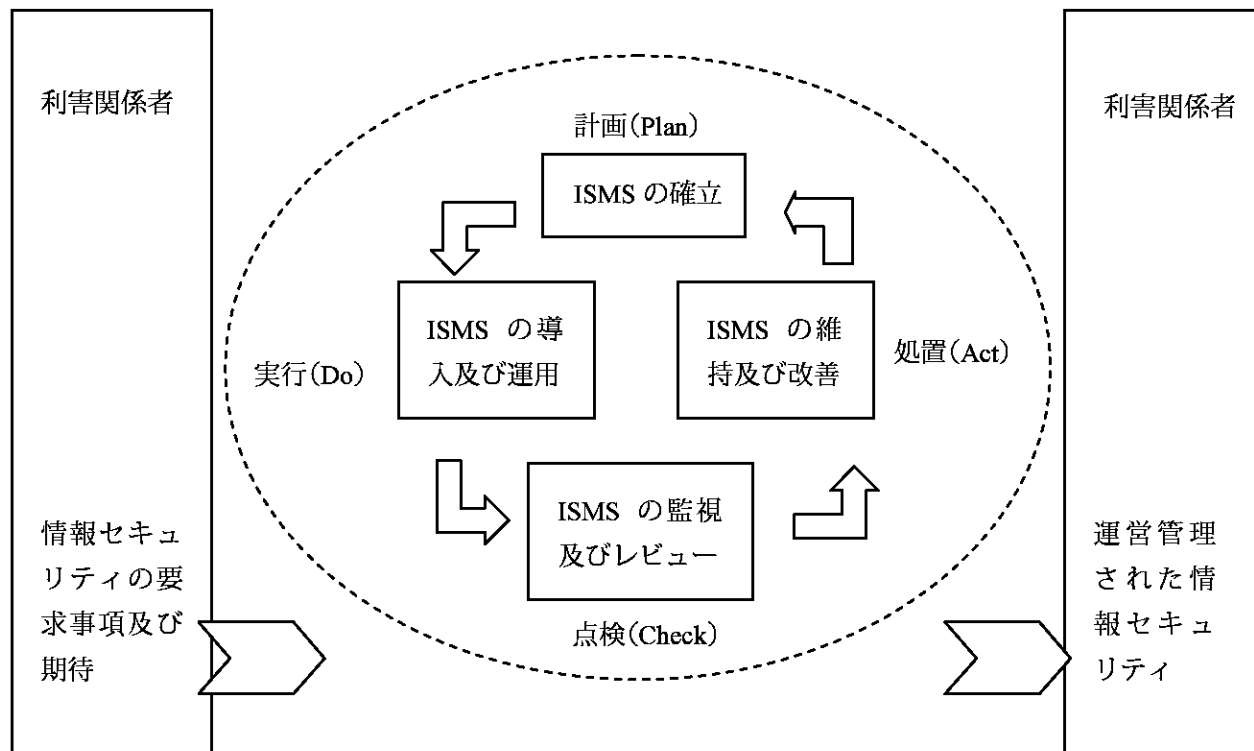
例 1 （情報セキュリティ要求事項の例）

- 1) 情報セキュリティ違反が、組織に重大な資金的損害を与えない。
- 2) 情報セキュリティ違反が、組織の存続を脅かさない。

例 2 （利害関係者の期待の例）

重大なインシデント[例えば、組織が電子商取引に使用しているウェブサイトのハッキング²⁾]が発生しても、その影響を最小限に抑える適切な手順について十分に教育・訓練を受けた要員が存在する。

注²⁾ ハッキングとは、コンピュータシステムの動作を解析したりプログラムを改造したりすること。転じて、他人のシステムを不正な手段で操作すること。



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

図 1-ISMS プロセスに適用される PDCA モデル

0.2.3 他のマネジメントシステムとの両立性

この規格は、関係するマネジメント規格と矛盾なく統合して導入及び運用することができるように、JIS Q 9001:2000 及び JIS Q 14001:2004 との調和がとられている。したがって、適切に設計した一つのマネジメントシステムは、これらすべての規格の要求事項を満たすことができる。附属書 C の表 C.1 は、この規格、JIS Q 9001:2000 及び JIS Q 14001:2004 の各箇条の間の関係を表している。

この規格は、組織が自らの ISMS を、関係する他のマネジメントシステムの要求事項に調和させること又は統合することが可能なように設計されている。

1 適用範囲

1.1 一般

この規格は、あらゆる形態の組織（例えば、営利企業、政府機関、非営利団体）を対象にする。この規格は、その組織の事業リスク全般に対する考慮のもとで、文書化した ISMS (Information security management

system) を確立、導入、運用、監視、レビュー、維持及び改善するための要求事項について規定する。この規格は、それぞれの組織又はその組織の一部が、そのニーズに応じて調整したセキュリティ管理策を導入する際の要求事項について規定する。

この ISMS は、情報資産を保護し、また、利害関係者に信頼を与える、十分で、かつ、均整のとれたセキュリティ管理策の選択を確実にするために設計される。

注記 1 この規格における“事業”又は“業務”という用語は、組織の形態にかかわらず、その組織が存立するための核となる活動を意味する。

注記 2 管理策の設計に際して利用できる“実施の手引”については、**JIS Q 27002** による。

注記 3 この規格の対応国際規格及びその対応の程度を表す記号を、次に示す。

ISO/IEC 27001 : 2005, Information technology – Security techniques – Information security management systems – Requirements (IDT)

なお、対応の程度を表す記号 (IDT) は、**ISO/IEC Guide 21** に基づき、一致していることを示す。

1.2 適用

この規格が規定する要求事項は、はん（汎）用的であり、形態、規模及び事業の性質を問わず、すべての組織に適用できることを意図している。組織がこの規格への適合を宣言する場合には、箇条 4, 5, 6, 7 及び 8 に規定するいかなる要求事項の除外も認められない。

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

注記 組織が業務プロセスについてのマネジメントシステム（例えば、**JIS Q 9001** 又は **JIS Q 14001** に関連したもの）を既に運用しているならば、多くの場合、その既存システムのなかでこの規格の要求事項を満たすことが好ましい。

2 引用規格

次に掲げる規格は、この規格に引用されることによって、この規格の規定の一部を構成する。これらの引用規格のうちで、西暦年を付記してあるものは、記載の年の版を適用し、その後の改正版（追補を含む。）には適用しない。

JIS Q 27002:2006 情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範

注記 対応国際規格：**ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management (IDT)**

3 用語及び定義

この規格で用いる主な用語及び定義は、次による。

3.1

資産 (asset)

組織にとって価値をもつもの (**JIS Q 13335-1:2006**)。

3.2

可用性 (availability)

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性 (JIS Q 13335-1:2006)。

3.3

機密性 (confidentiality)

認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性 (JIS Q 13335-1:2006)。

3.4

情報セキュリティ (information security)

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい (JIS Q 27002:2006)。

3.5

情報セキュリティ事象 (information security event)

システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示しているものをいう (ISO/IEC TR 18044:2004)。

3.6

情報セキュリティインシデント (information security incident)

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの (ISO/IEC TR 18044:2004)。

3.7

情報セキュリティマネジメントシステム, ISMS (information security management system)

マネジメントシステム全体の中で、事業リスクに対する取組み方に基づいて、情報セキュリティの確立、導入、運用、監視、レビュー、維持及び改善を担う部分。

注記 マネジメントシステムには、組織の構造、方針、計画作成活動、責任、実践、手順、プロセス及び経営資源が含まれる。

3.8

完全性 (integrity)

資産の正確さ及び完全さを保護する特性 (JIS Q 13335-1:2006)。

3.9

残留リスク (residual risk)

リスク対応の後に残っているリスク (TR Q 0008:2003)。

3.10

リスクの受容 (risk acceptance)

リスクを受容する意思決定 (TR Q 0008:2003)。

3.11

リスク分析 (risk analysis)

リスク因子を特定するための、及びリスクを算定するための情報の系統的使用 (TR Q 0008:2003)。

3.12**リスクアセスメント (risk assessment)**

リスク分析からリスク評価までのすべてのプロセス (TR Q 0008:2003)。

3.13**リスク評価 (risk evaluation)**

リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセス (TR Q 0008:2003)。

3.14**リスクマネジメント (risk management)**

リスクに関して組織を指揮し管理する調整された活動 (TR Q 0008:2003)。

3.15**リスク対応 (risk treatment)**

リスクを変更させるための方策を、選択及び実施するプロセス (TR Q 0008:2003)。

注記 この規格では、“管理策”という用語を“方策”の類義語として使用する。

3.16**適用宣言書 (statement of applicability)**

その組織の ISMS に関連して適用する管理目的及び管理策を記述した文書。

注記 管理目的及び管理策は、組織の情報セキュリティに対する、次のものに基づく。

- リスクアセスメント及びリスク対応のプロセスの結果及び結論
- 法令又は規制の要求事項
- 契約上の義務
- 事業上の要求事項

4 情報セキュリティマネジメントシステム**4.1 一般要求事項**

組織は、その組織の事業活動全般及び直面するリスクに対する考慮のもとで、文書化した ISMS を確立、導入、運用、監視、レビュー、維持及び改善しなければならない。この規格の目的のために、ここで用いるプロセスは、図 1 に示す PDCA モデルに基づいている。

4.2 ISMS の確立及び運営管理**4.2.1 ISMS の確立**

組織は、次の事項を実行しなければならない。

- a) 事業・組織・所在地・資産・技術の特徴の見地から、ISMS の適用範囲及び境界を定義する。この定義には、適用範囲からの除外について、その詳細及びそれが正当である理由も含めるものとする (1.2 参照)。
- b) ISMS 基本方針を、事業・組織・所在地・資産・技術の特徴の見地から、次を満たすように定義する。
 - 1) 目的を設定するための枠組みを含め、また、情報セキュリティに関係する活動の方向性の全般的認識及び原則を確立する。
 - 2) 事業上及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮する。
 - 3) それのもとで ISMS の確立及び維持をする、組織の戦略的なリスクマネジメントの状況と調和をとる。

4) リスクを評価するに当たっての基軸を確立する [4.2.1 c) 参照]。

5) 経営陣による承認を得る。

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

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

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

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

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

注記 リスクアセスメントの方法には、幾つか異なるものがある。

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

d) リスクを、次のように特定する。

1) ISMS の適用範囲の中にある資産及びそれらの資産の管理責任者を特定する。

2) それらの資産に対する脅威を特定する。

3) それらの脅威がつけ込むかもしれないぜい弱性を特定する。

4) 機密性、完全性及び可用性の喪失がそれらの資産に及ぼす影響を特定する。

e) それらのリスクを次のように分析し、評価する。

1) セキュリティ障害に起因すると予想される、組織における事業的影響のアセスメントを行う。このアセスメントでは、その資産の機密性、完全性又は可用性の喪失の結果を考慮する。

2) 認識されている脅威及びぜい弱性並びに情報資産に関連する影響の観点から、起こり得るセキュリティ障害などの現実的な発生可能性についてアセスメントを行う。その際に、現在実施されている管理策を考慮する。

3) そのリスクのレベルを算定する。

4) そのリスクが受容できるか、又は対応が必要であるかを判断する。この判断には、4.2.1 c) 2) によって確立したリスク受容基準を用いる。

f) リスク対応のための選択肢を特定し、評価する。選択肢には、次がある。

1) 適切な管理策の適用

2) 組織の方針及びリスク受容基準を明確に満たすリスクの、意識的、かつ、客観的な受容 [4.2.1 c) 参照]

3) リスクの回避

4) 関連する事業上のリスクの、他者（例えば、保険業者、供給者）への移転

g) リスク対応のための、管理目的及び管理策を選択する。

管理目的及び管理策は、リスクアセスメント及びリスク対応のプロセスにおいて特定した要求事項を満たすために選択し、導入しなければならない。

この選択には、法令、規制及び契約上の要求事項と同じく、リスク受容基準 [4.2.1 c) 2) 参照] も考慮しなければならない。

このプロセスの一部として、附属書 A の中から、特定した要求事項を満たすために適切のように、管理目的及び管理策を選択しなければならない。

附属書 A に規定した管理目的及び管理策は、すべてを網羅してはいないので、追加の管理目的及び

管理策を選択してもよい。

注記 附属書 A は、様々な組織が共通的に関連する管理目的及び管理策を幅広く集めたリストである。
この規格の利用者には、**附属書 A** を、重要な管理策の選択に見落としがないことを確実にする、
管理策選択の出発点として示す。

- h) その結果としての残留リスクについて経営陣の承認を得る。
- i) その ISMS を導入し、運用することについて経営陣の許可を得る。
- j) 適用宣言書を作成する。

適用宣言書は、次を含むように作成しなければならない。

- 1) **4.2.1 g)**によって選択した管理目的及び管理策、並びにそれらを選択した理由
- 2) 現在実施している管理目的及び管理策 [**4.2.1 e) 2)** 参照]
- 3) **附属書 A** に規定された管理策の中で適用除外とした管理目的及び管理策、並びにそれらを適用除外とすることが正当である理由

注記 適用宣言書は、リスク対応に関する決定の概要を提供する。適用除外に対する理由付けは、不注意による管理策の抜けを起こさないための点検手段を提供する。

4.2.2 ISMS の導入及び運用

組織は、次の事項を実行しなければならない。

- a) リスク対応計画を策定する。この計画では、情報セキュリティリスクを運営管理するための、経営陣の適切な活動、経営資源、責任体制及び優先順位を特定する。
- b) 特定した管理目的を達成するためにリスク対応計画を実施する。この計画には、必要資金の手当て並びに役割及び責任の割当てへの考慮を含む。
- c) **4.2.1 g)** によって選択した管理策を、その管理目的を満たすために実施する。
- d) 選択した管理策又は一群の管理策の有効性をどのように測定するかを定義し、また、比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために、それらの測定をどのように利用するかを規定する [**4.2.3 c)** 参照]。

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

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

4.2.3 ISMS の監視及びレビュー

組織は、次の事項を実行しなければならない。

- a) 監視及びレビューの手順並びにその他の管理策を、次のために実施する。
 - 1) 処理結果の中の誤りを迅速に検知する。
 - 2) 未遂であるか既遂であるかを問わず、セキュリティの違反及びインシデントを迅速に特定する。
 - 3) 人力にゆだねて又は情報技術を導入して実施しているセキュリティ活動が期待どおりかどうかを経営陣が判断することを可能にする。
 - 4) セキュリティ事象の検知を補助し、その結果の表示を利用してセキュリティインシデントを防止する。

- 5) セキュリティ違反を解決するためにとった処置が有効であるかどうかを判断する。
- b) ISMS の有効性について定期的にレビューする。これには、ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは、セキュリティ監査の結果、インシデント、有効性測定の結果、提案、及びすべての利害関係者からのフィードバックを考慮する。
- c) セキュリティ要求事項を満たしていることを検証するために、管理策の有効性を測定する。
- d) リスクアセスメントをあらかじめ定めた間隔でレビューする。残留リスク及び特定したリスク受容可能レベルをレビューする。これらのレビューでは、次に起きた変化を考慮する。
- 1) 組織
 - 2) 技術
 - 3) 事業の目的及びプロセス
 - 4) 特定した脅威
 - 5) 導入した管理策の有効性
 - 6) 外部事情（例えば、法令又は規制の状況、契約上の義務、社会的風潮）
- e) あらかじめ定めた間隔で ISMS 内部監査を実施する。
- 注記 第一者監査と呼ばれる内部監査は、内部目的のために、その組織自身又はその組織に代わる者が実施するものである。
- f) 適用範囲が引き続き適切であること、及び ISMS のプロセスにおける改善策を特定（7.1 参照）することを確認するために、ISMS のマネジメントレビューを定期的実施する。
- g) 監視及びレビューの活動から見出された事項を考慮に入れるために、セキュリティ計画を更新する。
- h) ISMS の有効性又はパフォーマンスに影響を及ぼす可能性のある活動及び事象を記録する（4.3.3 参照）。

4.2.4 ISMS の維持及び改善

組織は、常に次の事項を実行しなければならない。

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

4.3 文書化に関する要求事項

4.3.1 一般

文書には、経営陣の決定に関する記録も含めなければならない。文書は、とった処置から、経営陣の決定及び方針へたどれること、並びに記録した結果が再現可能であることを確実にしなければならない。

選択した管理策からリスクアセスメント及びリスク対応のプロセスまで、更には ISMS 基本方針及び目的のまでにつながる関係を説明できることが重要である。

ISMS 文書には、次を含めなければならない。

- a) 文書化した ISMS 基本方針 [4.2.1 b) 参照] 及び目的
- b) ISMS の適用範囲 [4.2.1 a) 参照]
- c) ISMS を支えている手順及び管理策

- d) リスクアセスメントの方法 [4.2.1 c) 参照] の記述
- e) リスクアセスメント報告 [4.2.1 c)～4.2.1 g) 参照]
- f) リスク対応計画 [4.2.2 b) 参照]
- g) 情報セキュリティのプロセスを有効に計画、運用及び管理することを確実にするために、組織が必要とする文書化した手順。管理策の有効性をどう測定するか [4.2.2 d) 参照] を記述するために、組織が必要とする文書化した手順。
- h) この規格が要求する記録 (4.3.3 参照)
- i) 適用宣言書

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

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

- 組織の規模及び活動の種類
- 適用範囲、並びにセキュリティの要求事項及び運営管理するシステムの複雑さ

注記 3 文書・記録の様式及び媒体の種類は、どのようなものでもよい。

4.3.2 文書管理

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

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

4.3.3 記録の管理

記録は、要求事項への適合性及び ISMS の有効な運用の証拠を提供するために、作成し、維持しなければならない。記録は、関連する法令又は規制の要求事項及び契約上の義務を考慮して保護し、管理しなければならない。記録は、読みやすく、容易に識別可能で、検索可能にしておかなければならない。記録の識別、保管、保護、検索、保管期間及び廃棄のために必要な管理策を文書化し、実施しなければならない。

4.2 に規定したプロセスのパフォーマンスの記録、及び ISMS に関係する重大なセキュリティインシデントすべての発生記録を保持しなければならない。

例 記録の例として、来訪者記録帳、監査報告書、記入済みのアクセス認可の書式などがある。

5 経営陣の責任

5.1 経営陣のコミットメント

経営陣は、ISMS の確立、導入、運用、監視、レビュー、維持、及び改善に対する自らのコミットメン

トの証拠を、次によって提供しなければならない。

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

5.2 経営資源の運用管理

5.2.1 経営資源の提供

組織は、次の事項を行うのに必要な経営資源を決定し、提供しなければならない。

- a) ISMS を確立、導入、運用、監視、レビュー、維持及び改善する。
- b) 事業上の要求事項を満たすことに、情報セキュリティの手順が寄与することを確実にする。
- c) 法令及び規制の要求事項並びに契約上のセキュリティ義務を明確にし、これを扱う。
- d) 導入したすべての管理策を正確に適用することによって、十分なセキュリティを維持する。
- e) 必要に応じてレビューし、レビューの結果に対して適切に対応する。
- f) 必要な場合には、ISMS の有効性を改善する。

5.2.2 教育・訓練、意識向上及び力量

組織は、ISMS に定義された責任を割り当てた要員すべてが、要求された職務を実施する力量をもつことを、次の事項によって確実にしなければならない。

- a) ISMS に影響がある業務に従事する要員に必要な力量を決定する。
- b) 必要な力量がもてるように教育・訓練するか、又は他の処置（例えば、適格な要員の雇用）をとる。
- c) とった処置の有効性を評価する。
- d) 教育、訓練、技能、経験及び資格についての記録を維持する (4.3.3 参照)。

組織は、また、関連する要員すべてが、自らの情報セキュリティについての活動がもつ意味と重要性とを認識し、ISMS の目的の達成に向けて、自分はどのように貢献できるか認識することを確実にしなければならない。

6 ISMS 内部監査

組織は、その ISMS の管理目的、管理策、プロセス及び手順について、次の事項を判断するために、あらかじめ定めた間隔で ISMS 内部監査を実施しなければならない。

- a) この規格及び関連する法令又は規制の要求事項に適合しているかどうか。
- b) 特定された情報セキュリティ要求事項に適合しているかどうか。
- c) 有効に実施され、維持されているかどうか。

d) 期待したように実施されているかどうか。

組織は、監査の対象となるプロセス及び領域の状況及び重要性、並びに前回までの監査結果を考慮して、監査プログラムを策定しなければならない。監査の基準、範囲、頻度及び方法を定義しなければならない。監査員の選定及び監査の実施においては、監査プロセスの客観性及び公平性を確実にしなければならない。監査員は、自らの仕事を監査してはならない。

監査の計画・実施に関する責任及び要求事項、並びに結果報告・記録維持（4.3.3 参照）に関する責任及び要求事項を、文書化した手順の中で定義しなければならない。

監査された領域に責任をもつ管理者は、発見された不適合及びその原因を除去するために遅滞なく処置がとられることを確実にしなければならない。フォローアップには、とった処置の検証及び検証結果の報告を含めなければならない（箇条 8 参照）。

注記 JIS Q 19011:2003 は、ISMS 内部監査の実施のための有益な手引となる場合がある。

7 ISMS のマネジメントレビュー

7.1 一般

経営陣は、組織の ISMS が引き続き適切であり、妥当であり、かつ、有効であることを確実にするために、あらかじめ定めた間隔（少なくとも年 1 回）で、ISMS をレビューしなければならない。このレビューでは、情報セキュリティの基本方針及び目的を含め、ISMS に対する改善の機会及び変更の必要性のアセスメントも行わなければならない。レビューの結果は、明確に文書化し、記録を維持しなければならない（4.3.3 参照）。

7.2 レビューへのインプット

次の情報を、マネジメントレビューに対して提供しなければならない。

- a) ISMS 監査及びレビューの結果
- b) 利害関係者からのフィードバック
- c) ISMS のパフォーマンス及び有効性を改善するために組織の中で利用可能な技術、製品又は手順
- d) 予防処置及び是正処置の状況
- e) 前回までのリスクアセスメントが十分に取り上げていなかったぜい弱性又は脅威
- f) 有効性測定の結果
- g) 前回までのマネジメントレビューの結果に対するフォローアップ
- h) ISMS に影響を及ぼす可能性がある、あらゆる変化
- i) 改善のための提案

7.3 レビューからのアウトプット

マネジメントレビューからのアウトプットには、次に関係する決定及び処置を含めなければならない。

- a) ISMS の有効性の改善
- b) リスクアセスメント及びリスク対応計画の更新
- c) ISMS に影響を与える可能性がある内外の事象に対応するために、必要に応じた、情報セキュリティを実現する手順及び管理策の修正。そのような事象には、次について起きた変化が含まれる。
 - 1) 事業上の要求事項
 - 2) セキュリティ要求事項
 - 3) 現在の事業上の要求事項を実現する業務プロセス
 - 4) 法令又は規制の要求事項

- 5) 契約上の義務
- 6) リスクのレベル及び／又はリスク受容基準
- d) 必要となる経営資源
- e) 管理策の有効性測定方法の改善

8 ISMS の改善

8.1 継続的改善

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

8.2 是正処置

組織は、ISMS の要求事項に対する不適合の原因を除去する処置を、その再発防止のためにとらなければならない。是正処置のために文書化された手順の中で、次のための要求事項を定義しなければならない。

- a) 不適合の特定
- b) 不適合の原因の決定
- c) 不適合の再発防止を確実にするための処置の必要性の評価
- d) 必要な是正処置の決定及び実施
- e) とった処置の結果の記録（4.3.3 参照）
- f) とった是正処置のレビュー

8.3 予防処置

組織は、ISMS の要求事項に対する不適合の発生を防止するために、起こり得る不適合の原因を除去する処置を決定しなければならない。とられる予防処置は、起こり得る問題の影響に見合ったものでなければならない。予防処置のために文書化された手順の中で、次のための要求事項を定義しなければならない。

- a) 起こり得る不適合及びその原因の特定
- b) 不適合の発生を予防するための処置の必要性の評価
- c) 必要な予防処置の決定及び実施
- d) とった処置の結果の記録（4.3.3 参照）
- e) とった予防処置のレビュー

組織は、変化したリスクを特定し、大きく変化したリスクに注意を向けて、予防処置についての要求事項を特定しなければならない。

予防処置の優先順位は、リスクアセスメントの結果に基づいて決定しなければならない。

注記 不適合を予防するための処置は、多くの場合、是正処置よりも費用対効果が大きい。

附属書 A (規定) 管理目的及び管理策

表 A.1 に規定した管理目的及び管理策は、JIS Q 27002:2006 の箇条 5～15 までに掲げられているものをそのまま取り入れて配列したものである。この表は、管理目的及び管理策のすべてを網羅してはいないので、組織は、管理目的及び管理策の追加が必要であると考えてよい。この表の中の管理目的及び管理策は、本体の 4.2.1 に規定する ISMS のプロセスの一部として、選択しなければならない。

JIS Q 27002:2006 の箇条 5～15 までは、A.5～A.15 までに規定した管理策を支える、導入への助言及び最適な実施のための手引を提供している。

表 A.1—管理目的及び管理策

A.5 セキュリティ基本方針		
A.5.1 情報セキュリティ基本方針		
目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規制に従って規定するため。		
A.5.1.1	情報セキュリティ基本方針文書	管理策 情報セキュリティ基本方針文書は、経営陣によって承認されなければならない。また、全従業員及び関連する外部関係者に公表し、通知しなければならない。
A.5.1.2	情報セキュリティ基本方針のレビュー	管理策 情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当及び有効であることを確実にするためにレビューしなければならない。
A.6 情報セキュリティのための組織		
A.6.1 内部組織		
目的：組織内の情報セキュリティを管理するため。		
A.6.1.1	情報セキュリティに対する経営陣の責任	管理策 経営陣は、情報セキュリティの責任に関する明りょうな方向付け、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持しなければならない。
A.6.1.2	情報セキュリティの調整	管理策 情報セキュリティ活動は、組織の中の、関連する役割及び職務機能をもつ様々な部署の代表が、調整しなければならない。
A.6.1.3	情報セキュリティ責任の割当て	管理策 すべての情報セキュリティ責任を、明確に定めなければならない。
A.6.1.4	情報処理設備の認可プロセス	管理策 新しい情報処理設備に対する経営陣による認可プロセスを定め、実施しなければならない。
A.6.1.5	秘密保持契約	管理策 情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューしなければならない。
A.6.1.6	関係当局との連絡	管理策 関係当局との適切な連絡体制を維持しなければならない。

A.6.1.7	専門組織との連絡	管理策 情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。
A.6.1.8	情報セキュリティの独立したレビュー	管理策 情報セキュリティ及びその実施のマネジメントに対する組織の取組み（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）について、あらかじめ計画した間隔で、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビューを実施しなければならない。
A.6.2 外部組織 目的：外部組織によってアクセス、処理、通信、又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。		
A.6.2.1	外部組織に関係したリスクの識別	管理策 外部組織がかかわる業務プロセスからの、組織の情報及び情報処理施設に対するリスクを識別しなければならない。また、外部組織にアクセスを許可する前に適切な管理策を実施しなければならない。
A.6.2.2	顧客対応におけるセキュリティ	管理策 顧客に組織の情報又は資産へのアクセスを許す前に、明確にしたすべてのセキュリティ要求事項を満たすように対処しなければならない。
A.6.2.3	第三者との契約におけるセキュリティ	管理策 組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約、又は情報処理施設に製品・サービスを追加する第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げなければならない。
A.7 資産の管理		
A.7.1 資産に対する責任 目的：組織の資産を適切に保護し、維持するため。		
A.7.1.1	資産目録	管理策 すべての資産は、明確に識別しなければならない。また、重要な資産すべての目録を、作成し、維持しなければならない。
A.7.1.2	資産の管理責任者	管理策 情報及び情報処理施設と関連する資産のすべてについて、組織の中に、その管理責任者を指定しなければならない。
A.7.1.3	資産利用の許容範囲	管理策 情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。
A.7.2 情報の分類 目的：情報の適切なレベルでの保護を確実にするため。		
A.7.2.1	分類の指針	管理策 情報は、組織に対しての価値、法的要求事項、取扱いに慎重を要する度合い及び重要性の観点から、分類しなければならない。
A.7.2.2	情報のラベル付け及び取扱い	管理策 情報に対するラベル付け及び取扱いに関する適切な一連の手順は、組織が採用した分類体系に従って策定し、実施しなければならない。

A.8 人的資源のセキュリティ

注記 A.8 では、組織の情報セキュリティに影響を与え得る者を、従業員、契約相手及び第三者の利用者の三群に大別し、また、組織とそれらの者とのかかわりの経過を、関係の開始、継続及び終了の三段階に大別して、人的資源のセキュリティを取り扱う。

このことから A.8 では、従業員、契約相手又は第三者の利用者のいずれに関しても、組織が関係を開始することを雇用 (A.8.1 参照)、この関係が継続している期間を雇用期間 (A.8.2 参照)、この関係が終了することを雇用の終了と総称する (A.8.3 参照)。また、雇用期間中における職務内容の変更を、旧職務の雇用が終了し、新職務の雇用が開始するととらえ、これを雇用の変更と総称する (A.8.3 参照)。

また、A.8 では、組織と従業員、契約相手及び第三者の利用者との情報セキュリティ側面での関係を規定したもの (文書化しているかどうかを問わない) を、職務定義書、雇用条件又は雇用契約書と総称し (A.8.1、A.8.2 参照)、必要に応じて、組織と従業員、契約相手又は第三者の利用者との雇用の関係を、それぞれ、雇用、契約又は合意と称する (A.8.3 参照)。このことから、例えば、雇用の終了を、従業員については雇用の終了、契約相手については契約の終了、また第三者の利用者については合意の終了として、それぞれを区別することがある。

A.8 において従業員とは、常勤・非常勤、常用・臨時、又は長期・短期などの雇用の形態を問わない。契約相手には、組織が契約を締結したサービス提供者、下請負業者、人材派遣業者などのほかに、これら業者の従業員であって、組織と締結した契約の履行のために組織に派遣された者なども含む (派遣された者が、組織とは直接に契約を締結していないことに留意)。第三者の利用者には、組織への一般来訪者、組織が開設するウェブサイト (ネットバンキングなど) の閲覧者などが含まれる。ただし、ウェブサイトの完全公開情報の閲覧については、除外する。

A.8.1 雇用前

目的：従業員、契約相手及び第三者の利用者がその責任を理解し、求められている役割にふさわしいことを確実にするとともに、盗難、不正行為、又は施設の不正使用のリスクを低減するため。

A.8.1.1	役割及び責任	管理策 従業員、契約相手及び第三者の利用者のセキュリティの役割及び責任は、組織の情報セキュリティ基本方針に従って定め、文書化しなければならない。
A.8.1.2	選考	管理策 従業員、契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は、関連のある法令、規制及び倫理に従って行わなければならない。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。
A.8.1.3	雇用条件	管理策 従業員、契約相手及び第三者の利用者は、契約上の義務の一部として、情報セキュリティに関する、これらの者の責任及び組織の責任を記載した雇用契約書に同意し、署名しなければならない。

A.8.2 雇用期間中

目的：従業員、契約相手及び第三者の利用者の、情報セキュリティの脅威及び諸問題、並びに責任及び義務に対する認識を確実なものとし、通常の業務の中で組織の情報セキュリティ基本方針を維持し、人による誤りのリスクを低減できるようにすることを確実にするため。

A.8.2.1	経営陣の責任	管理策 経営陣は、組織の確立された方針及び手順に従ったセキュリティの適用を従業員、契約相手及び第三者の利用者に要求しなければならない。
A.8.2.2	情報セキュリティの意識向上、教育及び訓練	管理策 組織のすべての従業員、並びに、関係するならば、契約相手及び第三者の利用者は、職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受けなければならない。また、定めに従ってそれを更新しなければならない。
A.8.2.3	懲戒手続	管理策 セキュリティ違反を犯した従業員に対する正式な懲戒手続を備えなければならない。

A.8.3 雇用の終了又は変更 目的：従業員、契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。		
A.8.3.1	雇用の終了又は変更に関する責任	管理策 雇用の終了又は変更の実施に対する責任は、明確に定め、割り当てなければならない。
A.8.3.2	資産の返却	管理策 すべての従業員、契約相手及び第三者の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産すべてを返却しなければならない。
A.8.3.3	アクセス権の削除	管理策 すべての従業員、契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除しなければならず、また、変更に合わせて修正しなければならない。
A.9 物理的及び環境的セキュリティ		
A.9.1 セキュリティを保つべき領域 目的：組織の施設及び情報に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。		
A.9.1.1	物理的セキュリティ境界	管理策 情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いなければならない。
A.9.1.2	物理的入退管理策	管理策 セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護しなければならない。
A.9.1.3	オフィス、部屋及び施設のセキュリティ	管理策 オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用しなければならない。
A.9.1.4	外部及び環境の脅威からの保護	管理策 火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害による被害からの物理的な保護を設計し、適用しなければならない。
A.9.1.5	セキュリティを保つべき領域での作業	管理策 セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し、適用しなければならない。
A.9.1.6	一般の人の立ち寄り場所及び受渡場所	管理策 一般の人が立ち寄る場所（例えば、荷物などの受渡場所）、及び敷地内の、認可されていない者が立ち入ることもある場所は、管理しなければならない。また、可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離さなければならない。
A.9.2 装置のセキュリティ 目的：資産の損失、損傷、盗難又は劣化、及び組織の活動に対する妨害を防止するため。		
A.9.2.1	装置の設置及び保護	管理策 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、又は保護しなければならない。
A.9.2.2	サポートユーティリティ	管理策 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護しなければならない。
A.9.2.3	ケーブル配線のセキュリティ	管理策 データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受又は損傷から保護しなければならない。
A.9.2.4	装置の保守	管理策 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守しなければならない。

A.9.2.5	構外にある装置のセキュリティ	管理策 構外にある装置に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用しなければならない。
A.9.2.6	装置の安全な処分又は再利用	管理策 記憶媒体を内蔵した装置は、処分する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又は問題が起きないように上書きしていることを確実にするために、すべてを点検しなければならない。
A.9.2.7	資産の移動	管理策 装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出してはならない。
A.10 通信及び運用管理		
A.10.1 運用の手順及び責任		
目的：情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため。		
A.10.1.1	操作手順書	管理策 操作手順は、文書化し、維持しなければならない。また、その手順は、必要とするすべての利用者に対して利用可能にしなければならない。
A.10.1.2	変更管理	管理策 情報処理設備及びシステムの変更は、管理しなければならない。
A.10.1.3	職務の分割	管理策 職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分割しなければならない。
A.10.1.4	開発施設、試験施設及び運用施設の分離	管理策 開発施設、試験施設及び運用施設は、運用システムへの認可されていないアクセス又は変更によるリスクを低減するために、分離しなければならない。
A.10.2 第三者が提供するサービスの管理		
目的：第三者の提供するサービスに関する合意に沿った、情報セキュリティ及びサービスの適切なレベルを実現し、維持するため。		
A.10.2.1	第三者が提供するサービス	管理策 第三者が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義、及び提供サービスレベルが、第三者によって実施、運用、及び維持されることを確実にしなければならない。
A.10.2.2	第三者が提供するサービスの監視及びレビュー	管理策 第三者が提供するサービス、報告及び記録は、常に監視し、レビューしなければならない。また、監査も定期的に実施しなければならない。
A.10.2.3	第三者が提供するサービスの変更に対する管理	管理策 関連する業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、サービス提供の変更（現行の情報セキュリティ方針、手順及び管理策の保守・改善を含む。）を管理しなければならない。
A.10.3 システムの計画作成及び受入れ		
目的：システム故障のリスクを最小限に抑えるため。		
A.10.3.1	容量・能力の管理	管理策 要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならない。また、将来必要とする容量・能力を予測しなければならない。
A.10.3.2	システムの受入れ	管理策 新しい情報システム、及びその改訂版・更新版の受入れ基準を確立しなければならない。また、開発中及びその受入れ前に適切なシステム試験を実施しなければならない。

A.10.4 悪意のあるコード及びモバイルコード³⁾からの保護 目的： ソフトウェア及び情報の完全性を保護するため。 注³⁾ モバイルコードとは、あるコンピュータから別のコンピュータへ移動するソフトウェアであって、利用者とのやり取りがほとんどない、又はまったくない状態で自動的に起動し、特定の機能を実行するものをいう。		
A.10.4.1	悪意のあるコードに対する管理策	管理策 悪意のあるコードから保護するために、検出、予防及び回復のための管理策、並びに利用者に適切に意識させるための手順を実施しなければならない。
A.10.4.2	モバイルコードに対する管理策	管理策 モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行わなければならない。また、認可されていないモバイルコードを実行できないようにしなければならない。
A.10.5 バックアップ 目的： 情報及び情報処理設備の完全性及び可用性を維持するため。		
A.10.5.1	情報のバックアップ	管理策 情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査しなければならない。
A.10.6 ネットワークセキュリティ管理 目的： ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため。		
A.10.6.1	ネットワーク管理策	管理策 ネットワークを脅威から保護するために、また、ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理し、制御しなければならない。
A.10.6.2	ネットワークサービスのセキュリティ	管理策 すべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について、セキュリティ特性、サービスレベル及び管理上の要求事項を特定しなければならない。また、いかなるネットワークサービス合意書にもこれらを盛り込まなければならない。
A.10.7 媒体の取扱い 目的： 資産の認可されていない開示、改ざん、除去又は破壊、及びビジネス活動の中断を防止するため。		
A.10.7.1	取外し可能な媒体の管理	管理策 取外し可能な媒体の管理のための手順は、備えなければならない。
A.10.7.2	媒体の処分	管理策 媒体が不要になった場合は、正式な手順を用いて、セキュリティを保ち、かつ、安全に処分しなければならない。
A.10.7.3	情報の取扱手順	管理策 情報の取扱い及び保管についての手順は、その情報を認可されていない開示又は不正使用から保護するために、確立しなければならない。
A.10.7.4	システム文書のセキュリティ	管理策 システム文書は、認可されていないアクセスから保護しなければならない。
A.10.8 情報の交換 目的： 組織内部で交換した及び外部と交換した、情報及びソフトウェアのセキュリティを維持するため。		
A.10.8.1	情報交換の方針及び手順	管理策 あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備えなければならない。
A.10.8.2	情報交換に関する合意	管理策 組織と外部組織との間の情報及びソフトウェアの交換について、両者間での合意が成立しなければならない。

A.10.8.3	配送中の物理的媒体	管理策 情報を格納した媒体は、組織の物理的境界を越えた配送の途中における、認可されていないアクセス、不正使用又は破損から保護しなければならない。
A.10.8.4	電子的メッセージ通信	管理策 電子的メッセージ通信に含まれた情報は、適切に保護しなければならない。
A.10.8.5	業務用情報システム	管理策 業務用情報システムの相互接続と関連がある情報を保護するために、個別方針及び手順を策定し、実施しなければならない。
A.10.9 電子商取引サービス		
目的：電子商取引サービスのセキュリティ、及びそれらサービスのセキュリティを保った利用を確実にするため。		
A.10.9.1	電子商取引	管理策 公衆ネットワークを経由する電子商取引に含まれる情報は、不正行為、契約紛争、認可されていない開示及び改ざんから保護しなければならない。
A.10.9.2	オンライン取引	管理策 オンライン取引に含まれる情報は、次の事項を未然に防止するために、保護しなければならない。 － 不完全な通信 － 誤った通信経路設定 － 認可されていないメッセージの変更 － 認可されていない開示 － 認可されていない複製又は再生
A.10.9.3	公開情報	管理策 認可されていない変更を防止するために、公開システム上で利用可能な情報の完全性を保護しなければならない。
A.10.10 監視		
目的：認可されていない情報処理活動を検知するため。		
A.10.10.1	監査ログ取得	管理策 利用者の活動、例外処理及びセキュリティ事象を記録した監査ログを取得しなければならない。また、将来の調査及びアクセス制御の監視を補うために、合意された期間、保持しなければならない。
A.10.10.2	システム使用状況の監視	管理策 情報処理設備の使用状況を監視する手順を確立しなければならない。また、監視活動の結果を定めに従ってレビューしなければならない。
A.10.10.3	ログ情報の保護	管理策 ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護しなければならない。
A.10.10.4	実務管理者及び運用担当者の作業ログ	管理策 システムの実務管理者及び運用担当者の作業は、記録しなければならない。
A.10.10.5	障害のログ取得	管理策 障害のログを取得し、分析し、また、障害に対する適切な処置をとらなければならない。
A.10.10.6	クロックの同期	管理策 組織又はセキュリティ領域内のすべての情報処理システム内のクロックは、合意された正確な時刻源と同期させなければならない。
A.11 アクセス制御		
A.11.1 アクセス制御に対する業務上の要求事項		
目的：情報へのアクセスを制御するため。		
A.11.1.1	アクセス制御方針	管理策 アクセス制御方針は、アクセスについての業務上及びセキュリティの要求事項に基づいて確立し、文書化し、レビューしなければならない。

A.11.2 利用者アクセスの管理		
目的：情報システムへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。		
A.11.2.1	利用者登録	管理策 すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備えなければならない。
A.11.2.2	特権管理	管理策 特権の割当て及び利用は、制限し、管理しなければならない。
A.11.2.3	利用者パスワードの管理	管理策 パスワードの割当ては、正式な管理プロセスによって管理しなければならない。
A.11.2.4	利用者アクセス権のレビュー	管理策 管理者は、正式なプロセスを使用して、利用者のアクセス権を定められた間隔でレビューしなければならない。
A.11.3 利用者の責任		
目的：認可されていない利用者のアクセス、並びに情報及び情報処理設備の損傷又は盗難を防止するため。		
A.11.3.1	パスワードの利用	管理策 パスワードの選択及び利用時に、正しいセキュリティ慣行に従うことを、利用者に要求しなければならない。
A.11.3.2	無人状態にある利用者装置	管理策 利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。
A.11.3.3	クリアデスク・クリアスクリーン ⁴⁾ 方針	管理策 書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない。 注 ⁴⁾ クリアデスクは、机上に書類を放置しないことである。また、クリアスクリーンは、情報をスクリーンに残したまま離席しないことである。
A.11.4 ネットワークのアクセス制御		
目的： ネットワークを利用したサービスへの認可されていないアクセスを防止するため。		
A.11.4.1	ネットワークサービスの利用についての方針	管理策 利用することを特別に認可したサービスへのアクセスだけを、利用者に提供しなければならない。
A.11.4.2	外部から接続する利用者の認証	管理策 遠隔利用者のアクセスを管理するために、適切な認証方法を利用しなければならない。
A.11.4.3	ネットワークにおける装置の識別	管理策 特定の場所及び装置からの接続を認証するための手段として、自動の装置識別を考慮しなければならない。
A.11.4.4	遠隔診断用及び環境設定用ポートの保護	管理策 診断用及び環境設定用ポートへの物理的及び論理的なアクセスは、制御しなければならない。
A.11.4.5	ネットワークの領域分割	管理策 情報サービス、利用者及び情報システムは、ネットワーク上、グループごとに分割しなければならない。
A.11.4.6	ネットワークの接続制御	管理策 共有ネットワーク、特に、組織の境界を越えて広がっているネットワークについて、アクセス制御方針及び業務用ソフトウェアの要求事項に沿って、利用者のネットワーク接続能力を制限しなければならない (A.11.1 参照)。
A.11.4.7	ネットワークルーティング制御	管理策 コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、ルーティング制御の管理策をネットワークに対して実施しなければならない。

A.11.5 オペレーティングシステムのアクセス制御		
目的：オペレーティングシステムへの、認可されていないアクセスを防止するため。		
A.11.5.1	セキュリティに配慮したログオン手順	管理策 オペレーティングシステムへのアクセスは、セキュリティに配慮したログオン手順によって制御しなければならない。
A.11.5.2	利用者の識別及び認証	管理策 すべての利用者は、各個人の利用ごとに一意な識別子（利用者 ID）を保有しなければならない。また、利用者が主張する同一性を検証するために、適切な認証技術を選択しなければならない。
A.11.5.3	パスワード管理システム	管理策 パスワードを管理するシステムは、対話式でなければならない。また、良質なパスワードを確実とするものでなければならない。
A.11.5.4	システムユーティリティの使用	管理策 システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。
A.11.5.5	セッションのタイムアウト	管理策 一定の使用中断時間が経過したときは、使用が中断しているセッションを遮断しなければならない。
A.11.5.6	接続時間の制限	管理策 リスクの高い業務用ソフトウェアに対しては、更なるセキュリティを提供するために、接続時間の制限を利用しなければならない。
A.11.6 業務用ソフトウェア及び情報のアクセス制御		
目的：業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。		
A.11.6.1	情報へのアクセス制限	管理策 利用者及びサポート要員による情報及び業務用ソフトウェアシステム機能へのアクセスは、既定のアクセス制御方針に従って、制限しなければならない。
A.11.6.2	取扱いに慎重を要するシステムの隔離	管理策 取扱いに慎重を要するシステムは、専用の（隔離された）コンピュータ環境をもたなければならない。
A.11.7 モバイルコンピューティング及びテレワーキング⁵⁾		
目的：モバイルコンピューティング及びテレワーキングの設備を用いるときの情報セキュリティを確実にするため。		
注 ⁵⁾ モバイルコンピューティングとは、移動中又は外出先でコンピュータを利用することであり、テレワーキングとは、要員が、自分の所属する組織の外の決まった場所で、通信技術を用いて作業することである。		
A.11.7.1	モバイルのコンピューティング及び通信	管理策 モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するために、正式な方針を備えなければならない。また、適切なセキュリティ対策を採用しなければならない。
A.11.7.2	テレワーキング	管理策 テレワーキングのための方針、運用計画及び手順を策定し、実施しなければならない。
A.12 情報システムの取得、開発及び保守		
A.12.1 情報システムのセキュリティ要求事項		
目的：セキュリティは情報システムの欠くことのできない部分であることを確実にするため。		
A.12.1.1	セキュリティ要求事項の分析及び仕様化	管理策 新しい情報システム又は既存の情報システムの改善に関する業務上の要求事項を記述した文書では、セキュリティの管理策についての要求事項を仕様化しなければならない。
A.12.2 業務用ソフトウェアでの正確な処理		
目的：業務用ソフトウェアにおける情報の誤り、消失、認可されていない変更又は不正使用を防止するため。		

A.12.2.1	入力データの妥当性確認	管理策 業務用ソフトウェアに入力するデータは、正確で適切であることを確実にするために、その妥当性を確認しなければならない。
A.12.2.2	内部処理の管理	管理策 処理の誤り又は故意の行為によって発生する情報の破壊を検出するために、妥当性確認の機能を業務用ソフトウェアに組み込まなければならない。
A.12.2.3	メッセージの完全性	管理策 業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定しなければならず、また、適切な管理策を特定し、実施しなければならない。
A.12.2.4	出力データの妥当性確認	管理策 業務用ソフトウェアからの出力データは、保存する情報の処理が正しく、かつ、状況に対して適切であることを確実にするために、その妥当性を確認しなければならない。
A.12.3 暗号による管理策 目的：暗号手段によって、情報の機密性、真正性又は完全性を保護するため。		
A.12.3.1	暗号による管理策の利用方針	管理策 情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施しなければならない。
A.12.3.2	かぎ（鍵）管理	管理策 組織における暗号技術の利用を支持するために、かぎ管理を実施しなければならない。
A.12.4 システムファイルのセキュリティ 目的：システムファイルのセキュリティを確実にするため。		
A.12.4.1	運用ソフトウェアの管理	管理策 運用システムにかかわるソフトウェアの導入を管理する手順を備えなければならない。
A.12.4.2	システム試験データの保護	管理策 試験データは、注意深く選択し、保護し、管理しなければならない。
A.12.4.3	プログラムソースコードへのアクセス制御	管理策 プログラムソースコードへのアクセスは、制限しなければならない。
A.12.5 開発及びサポートプロセスにおけるセキュリティ 目的：業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。		
A.12.5.1	変更管理手順	管理策 変更の実施は、正式な変更管理手順の使用によって、管理しなければならない。
A.12.5.2	オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー	管理策 オペレーティングシステムを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要な業務用ソフトウェアをレビューし、試験しなければならない。
A.12.5.3	パッケージソフトウェアの変更に対する制限	管理策 パッケージソフトウェアの変更は、抑止しなければならず、必要な変更だけに限らなければならない。また、すべての変更は、厳重に管理しなければならない。
A.12.5.4	情報の漏えい	管理策 情報漏えいの可能性を抑止しなければならない。
A.12.5.5	外部委託によるソフトウェア開発	管理策 組織は、外部委託したソフトウェア開発を監督し、監視しなければならない。
A.12.6 技術的ぜい弱性管理 目的：公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。		

A.12.6.1	技術的ぜい弱性の管理	管理策 利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずを獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価しなければならない。さらに、それらと関連するリスクに対処するために、適切な手段をとらなければならない。
A.13 情報セキュリティインシデントの管理		
A.13.1 情報セキュリティの事象及び弱点の報告		
目的：情報システムに関連する情報セキュリティの事象及び弱点を、時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。		
A.13.1.1	情報セキュリティ事象の報告	管理策 情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけすみやかに報告しなければならない。
A.13.1.2	セキュリティ弱点の報告	管理策 すべての従業員、契約相手並びに第三者の情報システム及びサービスの利用者に、システム又はサービスの中で発見した又は疑いをもったセキュリティ弱点は、どのようなものでも記録し、また、報告するように要求しなければならない。
A.13.2 情報セキュリティインシデントの管理及びその改善		
目的：情報セキュリティインシデントの管理に、一貫性のある効果的な取り組み方法を用いることを確実にするため。		
A.13.2.1	責任及び手順	管理策 情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするために、責任体制及び手順を確立しなければならない。
A.13.2.2	情報セキュリティインシデントからの学習	管理策 情報セキュリティインシデントの形態、規模及び費用を定量化し監視できるようにする仕組みを備えなければならない。
A.13.2.3	証拠の収集	管理策 情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には、関係する法域で定めている証拠に関する規則に従うために、証拠を収集、保全及び提出しなければならない。
A.14 事業継続管理		
A.14.1 事業継続管理における情報セキュリティの側面		
目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、また、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。		
A.14.1.1	事業継続管理手続への情報セキュリティの組込み	管理策 組織全体を通じた事業継続のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う、管理された手続を策定し、維持しなければならない。
A.14.1.2	事業継続及びリスクアセスメント	管理策 業務プロセスの中断を引き起こし得る事象は、そのような中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに、特定しなければならない。
A.14.1.3	情報セキュリティを組み込んだ事業継続計画の策定及び実施	管理策 重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し、実施しなければならない。
A.14.1.4	事業継続計画策定の枠組み	管理策 すべての計画が整合したものになることを確実にするため、情報セキュリティ上の要求事項を矛盾なく取り扱うため、また、試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持しなければならない。

A.14.1.5	事業継続計画の試験、維持及び再評価	管理策 事業継続計画は、最新で効果的なものであることを確実にするために、定めに従って試験・更新しなければならない。
A.15 順守		
A.15.1 法的要求事項の順守		
目的：法令、規制又は契約上のあらゆる義務、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 注記：法的順守は、しばしば、コンプライアンスといわれることがある。		
A.15.1.1	適用法令の識別	管理策 各情報システム及び組織について、すべての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組み方を、明確に定め、文書化し、また、最新に保たなければならない。
A.15.1.2	知的財産権（IPR）	管理策： 知的財産権が存在する可能性があるものを利用するとき、及び権利関係のあるソフトウェア製品を利用するときは、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を導入しなければならない。
A.15.1.3	組織の記録の保護	管理策 重要な記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊及び改ざんから保護しなければならない。
A.15.1.4	個人データ及び個人情報保護	管理策 個人データ及び個人情報の保護は、関連する法令、規制、及び適用がある場合には、契約条項の中の要求に従って確実にしなければならない。
A.15.1.5	情報処理施設の不正使用防止	管理策 認可されていない目的のための情報処理施設の利用は、阻止しなければならない。
A.15.1.6	暗号化機能に対する規制	管理策 暗号化機能は、関連するすべての協定、法令及び規制を順守して用いなければならない。
A.15.2 セキュリティ方針及び標準の順守、並びに技術的順守		
目的：組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。		
A.15.2.1	セキュリティ方針及び標準の順守	管理策 管理者は、セキュリティ方針及び標準類への順守を達成するために、自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にしなければならない。
A.15.2.2	技術的順守の点検	管理策 情報システムを、セキュリティ実施標準の順守に関して、定めに従って点検しなければならない。
A.15.3 情報システムの監査に対する考慮事項		
目的：情報システムに対する監査手続の有効性を最大限にするため、及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。		
A.15.3.1	情報システムの監査に対する管理策	管理策 運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画され、合意されなければならない。
A.15.3.2	情報システムの監査ツールの保護	管理策 情報システムを監査するツールの不正使用又は悪用を防止するために、それらのツールへのアクセスは、抑制しなければならない。

附属書 B (参考) OECD 原則及びこの規格

OECD の“情報システム及びネットワークのセキュリティガイドライン”に掲げられた原則は、情報システム及びネットワークのセキュリティを律するあらゆる方針及び運用のレベルに通用する。この規格は、OECD 原則の中の幾つかを履行するための、PDCA モデル及びこの規格本体の箇条 4, 5, 6, 7 及び 8 に規定されたプロセスを用いた、情報セキュリティマネジメントシステムの枠組みを提供する。

表 B.1—OECD 原則及び PDCA モデル

OECD 原則	対応する ISMS プロセス及び PDCA
認識 (Awareness) 参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分たちにできることについて認識すべきである。	この活動は、Do の段階（本体の 4.2.2 及び 5.2.2 参照）に含まれている。
責任 (Responsibility) すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。	この活動は、Do の段階（本体の 4.2.2 及び 5.1 参照）に含まれている。
対応 (Response) 参加者は、セキュリティの事件・事故に対する予防、検出及び対応のために、時宜を得た、かつ、協力的な方法で行動すべきである。	これは、Check の段階での監視の活動（本体の 4.2.3 及び箇条 6～7.3 参照）、及び Act の段階での対処の活動（本体の 4.2.4 及び 8.1～8.3 参照）に含まれている。また、Plan 及び Check の段階の幾つかの側面も、この活動をカバーしている。
リスクアセスメント (Risk assessment) 参加者は、リスクアセスメントを行うべきである。	この活動は、Plan の段階（本体の 4.2.1 参照）に含まれており、また、再アセスメントの活動が、Check の段階（本体の 4.2.3 及び箇条 6～7.3 参照）に含まれている。
セキュリティの設計及び実装 (Security design and implementation) 参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。	リスクアセスメントが完了すると、リスクに対応するために管理策を選択するが、これは Plan の段階に含まれている（本体の 4.2.1 参照）。続く Do の段階は、これら管理策の導入及び運用を取り上げている（本体の 4.2.2 及び 5.2 参照）。
セキュリティマネジメント (Security management) 参加者は、セキュリティマネジメントへの包括的アプローチを採用すべきである。	リスクマネジメントは、予防、セキュリティ事件・事故の検出と対処、継続的な維持、見直しと監査を含むプロセスである。これら側面のすべてが、Plan, Do, Check, Act の段階にまたがって取り込まれている。
再評価 (Reassessment) 参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。	情報セキュリティのアセスメントを繰り返すことは、ISMS の有効性の点検のために見直しを行う Check の段階（本体の 4.2.3 及び箇条 6～7.3 参照）に含まれており、セキュリティの改善は Act の段階（本体の 4.2.4 及び 8.1～8.3 参照）に含まれている。

附属書 C (参考)

JIS Q 9001:2000, JIS Q 14001:2004, 及びこの規格の比較

表 C.1 は、JIS Q 9001:2000, JIS Q 14001:2004, 及びこの規格の比較を示す。

表 C.1—JIS Q 9001:2000, JIS Q 14001:2004, 及びこの規格の比較

この規格	JIS Q 9001: 2000	JIS Q 14001: 2004
0.1 序文	序文	序文
0.2 ISMS の採用	0.1 一般	
0.2.1 概要		
0.2.2 プロセスアプローチ	0.2 プロセスアプローチ	
	0.3 JIS Q 9004 との関係	
0.2.3 他のマネジメントシステムとの両立性	0.4 他のマネジメントシステムとの両立性	
1 適用範囲	1 適用範囲	1 適用範囲
1.1 一般	1.1 一般	
1.2 適用	1.2 適用	
2 引用規格	2 引用規格	2 引用規格
3 用語及び定義	3 定義	3 用語及び定義
4 情報セキュリティマネジメントシステム	4 品質マネジメントシステム	4 環境マネジメントシステム要求事項
4.1 一般要求事項	4.1 一般要求事項	4.1 一般要求事項
4.2 ISMS の確立及び運営管理		
4.2.1 ISMS の確立		
4.2.2 ISMS の導入及び運用		4.4 実施及び運用
4.2.3 ISMS の監視及びレビュー	8.2.3 プロセスの監視及び測定	4.5.1 監視及び測定
4.2.4 ISMS の維持及び改善	8.2.4 製品の監視及び測定	
4.3 文書化に関する要求事項	4.2 文書化に関する要求事項	
4.3.1 一般	4.2.1 一般	
4.3.2 文書管理	4.2.2 品質マニュアル	
4.3.3 記録の管理	4.2.3 文書管理	4.4.5 文書管理
	4.2.4 記録の管理	4.5.4 記録の管理
5 経営陣の責任	5 経営者の責任	
5.1 経営陣のコミットメント	5.1 経営者のコミットメント	
	5.2 顧客重視	
	5.3 品質方針	4.2 環境方針
	5.4 計画	4.3 計画
	5.5 責任、権限及びコミュニケーション	
5.2 経営資源の運用管理	6 資源の運用管理	
5.2.1 経営資源の提供	6.1 資源の提供	
	6.2 人的資源	
5.2.2 教育・訓練、意識向上及び力量	6.2.2 力量、認識及び教育・訓練	4.4.2 力量、教育訓練及び自覚
	6.3 インフラストラクチャー	
	6.4 作業環境	
6 ISMS 内部監査	8.2.2 内部監査	4.5.5 内部監査

表 C.1－JIS Q 9001:2000, JIS Q 14001:2004, 及びこの規格の比較（続き）

この規格	JIS Q 9001: 2000	JIS Q 14001: 2004
7 ISMS のマネジメントレビュー 7.1 一般 7.2 レビューへのインプット 7.3 レビューからのアウトプット	5.6 マネジメントレビュー 5.6.1 一般 5.6.2 マネジメントレビューへのインプット 5.6.3 マネジメントレビューからのアウトプット	4.6 マネジメントレビュー
8 ISMS の改善 8.1 継続的改善 8.2 是正処置 8.3 予防処置	8.5 改善 8.5.1 継続的改善 8.5.2 是正処置 8.5.3 予防処置	4.5.3 不適合並びに是正処置及び予防処置
附属書 A（規定） 管理目的及び管理策 附属書 B（参考） OECD 原則及びこの規格 附属書 C（参考） JIS Q 9001:2000, JIS Q 14001:2004 及びこの規格の比較	 附属書 A（参考） JIS Q 9001:2000 と JIS Q 14001:1996 との比較	附属書 A（参考） この規格の利用の手引 附属書 B（参考） JIS Q 14001:2004 と JIS Q 9001:2000 との対応

参考文献

規格

- 1) **JIS Q 9001:2000** 品質マネジメントシステム—要求事項
(ISO 9001:2000, Quality management systems—Requirements)
- 2) **JIS Q 13335-1:2006** 情報技術—セキュリティ技術—情報通信技術セキュリティマネジメント—第1部：情報通信技術セキュリティマネジメントの概念及びモデル
(ISO/IEC 13335-1:2004, Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management)
- 3) **JIS Q 14001:2004** 環境マネジメントシステム—要求事項及び利用の手引
(ISO 14001:2004, Environmental management systems—Requirements with guidance for use)
- 4) **JIS Q 19011:2003** 品質及び／又は環境マネジメントシステム監査のための指針
(ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing)
- 5) **JIS Z 9362:1996** 品質システム審査登録機関に対する一般要求事項
(ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems)
- 6) **TR Q 0008:2003** リスクマネジメント—用語—規格において使用するための指針
(ISO/IEC Guide 73:2002, Risk management—Vocabulary—Guidelines for use in standards)
- 7) **TR X 0036-3:2001** ITセキュリティマネジメントのガイドライン—第3部：ITセキュリティマネジメントのための手法
(ISO/IEC TR 13335-3:1998, Information technology—Guidelines for the management of IT Security—Part 3: Techniques for the management of IT security)
- 8) **TR X 0036-4:2001** ITセキュリティマネジメントのガイドライン—第4部：セーフガードの選択
(ISO/IEC TR 13335-4:2000, Information technology—Guidelines for the management of IT Security—Part 4: Selection of safeguards)
- 9) **ISO/IEC TR 18044:2004** Information technology—Security techniques—Information security incident management

その他の出版物

- 1) OECD, Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org
- 2) NIST SP 800-30, Risk Management Guide for Information Technology systems
- 3) Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering study, 1986