****

**ISO/IEC FDIS 27001:2013**

**改訂解説資料**

**改訂：2013年9月23日**

**資料提供**

**日本シーエスアール認証登録機構**

**はじめに**

この文書は、2013年9月13日に**国際マネジメントシステム認証機構株式会社**が主催したISO/IEC FDIS 27001:2013改訂解説セミナーの資料としてお配りしたものを皆様からのご意見を参考に改訂版として掲載しています。

この文書は、ダウンロードされた方が、自由に意見を記載し、ご自身で利用できるようWord文書として公開しています。多くの人の手で改良を加えていくことで、ISO/IEC 27001:2013について共通に認識を育てる目的が有ります。文書に修正を加えた際は、下記メールアドレスに修正箇所を明記し、ご連絡ください。今後の改訂の参考とさせていただきます。

この取り組みは、試験的に実施しているものですが、好評であれば、今後（2015年頃）発行を予定しているISO9001やISO14001についても、検討したいと考えています。

e-mail：JCSR.Info@jcsr.co.jp

尚、この文書は、ISO/IEC 27001:2013規格書の代わりになるものではありません。4章からの要求事項についても、規格要求事項の理解を助けるために、“意訳”を掲載していますが、正確な訳文については規格の英文、又は正式な翻訳文を参照ください。

また、利用に際しては、各個人の責任でお願いいたします。利用者同士、もしくは利用者によるトラブルについては、当方では一切の責任は負いかね ます。

日本シーエスアール認証登録機構

代表取締役　　　土屋慶三

**１章 改訂の背景**

ISOのマネジメント規格を制定・改訂する際のガイドとして使用されてきたISO Guide 83が、2012年4月30日にISO/IEC Directives（指針）の付属書SL‐Appendix 3に包含されたこと受けて、今後、新たに制定される、または改訂されるすべてのマネジメントシステム規格は、この付属書 SL‐Appendix 3に従い再構築されることになります。

今回公開されたISO/IEC FDIS 27001:2013は、その指針に基づき改訂された最初のマネジメントシステム規格です。

ISO/IEC Directivesとは、ISOのマネジメントシステム規格を開発するためのルールを包括的に規定したものであり、規格同士の両立性があるように、一貫した上位構造、共通の中核となるテキスト、共通用語及び中核となる定義を定めたものです。付属書 SLは、その指針本文を補足するもので、その第8項（SL.8）に記されたAppendix 3は、具体的なマネジメントシステム規格のテンプレートが示されたものです。

参考）ISO/IEC Directivesの目次

|  |
| --- |
| 統合版 ISO 補足指針の序文 |
| まえがき |
| 1 | 専門業務に関する組織構成及び責任 |
| 2 | IS（国際規格）の開発 |
| 3 | その他の規格類（TS、PAS、TR）の開発 |
| 4 | 会議 |
| 5 | 異議申立て |
| 附属書A | ガイド |
| ・・・ |
| 附属書 SL | マネジメントシステム規格の提案 |
| SL.1 | 一般 |
| SL.2 | 妥当性評価を提出する義務 |
| SL.3 | 妥当性評価が提出されていない場合 |
| SL.4 | 附属書 SLの適用性 |
| SL.5 | 用語及び定義 |
| SL.6 | 一般原則 |
| SL.7 | 妥当性評価プロセス及び規準 |
| SL.8 | MSS の開発プロセス及び構成に関する手引 |
| Appendix 1 | 妥当性の判断基準となる質問事項 |
| Appendix 2 | マネジメントシステム規格における利用のための上位構造、共通の中核となるテキストや共通用語及び中核となる定義 |
| Appendix 3 | 上位構造、共通の中核となる共通テキスト、共通用語及び中核となる定義 ↑ ISO Guide 83を包含 |
| Appendix 4 | 上位構造、共通の中核となる共通テキストや共通用語及び中核となる定義に関する手引 |
| ・・・ |

ISO/IEC Directives の日本語訳は、以下のサイトで公開しています。

 http://www.jsa.or.jp/itn/pdf/shiryo/iso\_supplement\_sl234.pdf

ISO/IEC FDIS 27001:2013の改訂作業は、下記表の項目が一致していることを見てもわかるように、付属書 SL‐Appendix 3をテンプレートとして、その原則に従って開発されています。原則の一つ目は、規格の上位構造と呼ばれる箇所（オレンジ色で示す箇所）については、全く同じ条項の名称を採用することです。二つ目は、マネジメントシステムを構成する中核となる84の要求事項、45の“Shall”について、マネジメントシステム規格間の違いが生じないように同じテキスト（文章）を採用することです。表のピンクの網掛け部分は、多少の要求の追加はあるものの、ほぼ付属書 SL‐Appendix 3と同じ内容になっています。

付属書 SL‐Appendix 3とISO/IEC FDIS 27001:2013の比較　【規格の全体像をとらえる】

|  |  |  |
| --- | --- | --- |
| 付属書 SL‐Appendix 3 | ISO/IEC FDIS 27001:2013 | 備考 |
| 序文 | 序文 | 序文、適用範囲、引用規格の項については同一の上位構造（条項）を採用。但し、内容はISMS特有の記述。 |
| 1. 適用範囲 | 1 適用範囲 |
| 2. 引用規格 | 2 引用規格 |
| 3. 用語及び定義 | 3 用語及び定義 | 同一の上位構造（条項）。ISO/IEC 27000を引用（改訂版は現在DIS） |
| 4. 組織の状況 | 4 組織の状況 | 同一の上位構造（条項）。要求事項を構成。4章が求めている事組織は、何のためにISMSを導入するかを自らに問い、その目的のために適当なISMSを構築する5章が求めている事経営者の積極的な関与は、最重要6章が求めている事4章で明らかになった目的の達成と課題解決のために情報セキュリティリスクをどのように扱うかを計画PDCA7章が求めている事マネジメントシステムを支援する基本要素。業務遂行上、当たり前のこと。ISMSに特化したものではない。支援8章が求めている事6章の計画を実践。リスクを特定し、対応策（管理策）を実施。PDCA9章が求めている事成果を確認。デミングサイクルの基本。ISMSに特化したものではない。PDCA10章が求めている事上手く行かない所を正す。デミングサイクルの基本。ISMSに特化したものではない。PDCA |
| 4.1 組織及びその状況の理解 | 4.1 組織及びその状況の理解 |
| 4.2 利害関係者のニーズ及び期待の理解 | 4.2 利害関係者のニーズ及び期待の理解 |
| 4.3 XXX マネジメントシステムの適用範囲の決定 | 4.3 情報セキュリティマネジメントシステムの適用範囲の決定 |
| 4.4 XXX マネジメントシステム | 4.4 情報セキュリティマネジメントシステム |
| 5. リーダシップ | 5 リーダシップ |
| 5.1 リーダシップ及びコミットメント | 5.1 リーダシップ及びコミットメント |
| 5.2 方針 | 5.2 方針 |
| 5.3 組織の役割、責任及び権限 | 5.3 組織の役割、責任及び権限 |
| 6. 計画 | 6 計画 |
| 6.1 リスク及び機会への取り組み | 6.1 リスク及び機会への取り組み |
| 6.1.1 一般 |
|  | 6.1.2情報セキュリティリスクアセスメント |
|  | 6.1.3情報セキュリティリスク対応 |
| 6.2 XXX 目的及びそれを達成するための計画策定 | 6.2 情報セキュリティ目的及びそれを達成するための計画 |
| 7. 支援 | 7 支援 |
| 7.1 資源 | 7.1 資源 |
| 7.2 力量 | 7.2 力量 |
| 7.3 認識 | 7.3 認識 |
| 7.4 コミュニケーション | 7.4 コミュニケーション |
| 7.5 文書化された情報 | 7.5 文書化された情報 |
| 7.5.1 一般 | 7.5.1 一般 |
| 7.5.2 作成及び更新 | 7.5.2 作成及び更新 |
| 7.5.3 文書化された情報の管理 | 7.5.3文書化された情報の管理 |
| 8. 運用 | 8 運用 |
| 8.1 運用の計画及び管理 | 8.1 運用の計画及び管理 |
|  | 8.2 情報セキュリティリスクアセスメント |
|  | 8.3 情報セキュリティリスク対応 |
| 9. パフォーマンス評価 | 9 パフォーマンス評価 |
| 9.1 監視、測定、分析及び評価 | 9.1 監視、測定、分析及び評価 |
| 9.2 内部監査 | 9.2 内部監査 |
| 9.3 マネジメントレビュー | 9.3 マネジメントレビュー |
| 10. 改善 | 10 改善 |
| 10.1 不適合及び是正措置 | 10.1 不適合及び是正処置 |
| 10.2 継続的改善 | 10.2 継続的改善 |

**２章　何が変わったか**

|  |
| --- |
| **規格の構造の変化・・・①** |
| 今回の改訂は、付属書 SL‐Appendix 3の適用を受けて規格同士の両立性を高めることが主な狙いです。しかし、あらかじめ定められた枠の中に、2005年度版の要求事項をあてがう作業には、かなり苦労された跡が伺えます。特に、6章や8章については、理解しにくい部分や、違和感がのこる要求も見受けられます。ISMSの要求事項については、特に目新しいものはなく、変化は限定的です。但し、ISMSが、解決すべき課題を明確にできていない場合は、後出の**②**に示すことが重要な変化に映るでしょう。（**②**参照）本質的には変わらないものの、見た目の変更点として目立つところは、予防処置の要求事項の削除です。予防処置は、リスクマネジメントそのものであることから、『6.1項　リスク及び機会に対処する行動』の「望ましくない影響を防止・・・」という表現の中に含みを持たせています。今まで是正処置と予防処置については、その処置方法（原因の特定、処置の決定・実施や有効性のレビュー）が似ている個々の要求事項としてまとめられていましたが、時系列的に見ると、是正処置は不具合が起こってから行うもの、一方、予防処置は不具合が起きる前に行うものであることから、不具合を起こさないようにするマネジメントシステムの計画（PDCA）の段階で扱われるのは当然のことかもしれません。 |
| **【組織は何をすべきか】**ISMSの概要（マネジメントプロセス）を記述した文書については、対比し易くするため構成を見直す余地があります。内部監査その他組織の活動を回す中で誤解が生じない程度の修正が求められます。 |

|  |
| --- |
| **ISMSの目的がより鮮明に・・・②** |
| 今回の改訂は、2005年度版の4.1の要求をより鮮明にしたことが大きな成果であり、2013年度版の4章の構成は、ISMSを課題や目的ベースに構築する上で反映すべきことを明確に記しています。「組織は、ISMSを何故導入したのか（するのか）」、それは、組織が置かれた状況を考えればわかることで、**組織の目的に関連した内外の課題を解決することや、さまざまな期待、ニーズに応じること**が、その答えの一つであると言うことが要求事項から読み取れます。組織がさらされている競争関係、お客様の期待、ニーズ、取り巻く社会環境、組織の処理能力、規制など、内外の課題の中に機密性、完全性、可用性の要求が見え隠れしているものです。『4.1　組織及びその状況の理解』、『4.2　利害関係者のニーズ及び期待の理解』によってそのことが鮮明になり、それらを考慮し、効果的な範囲を定め、ISMSを構築、実施、維持、改善することが、『4.3　情報セキュリティマメントシステムの適用範囲の決定』及び『4.4　情報セキュリティマネジメントシステム』に記されています。機密性、完全性、可用性の要求は、6.1項でリスクとして捉え、8章から10章、さらに7章の支援を活用しPDCAを完結します（・・・Aの流れ）。「組織は、ISMSを何故導入したのか（するのか）」について、2013年度版では、もう一つの答えを用意しています。それは、**情報セキュリティ目的**です。こちらも、組織の目的から発し、5章のリーダシップを発揮するために、情報セキュリティ方針を確立し、戦略的な方向に組織を向けるために、情報セキュリティ目的を設定し、組織内に展開して、6.2項で計画、8章から10章、さらに7章の支援を活用しPDCAを完結します（・・・Bの流れ）。Bの流れは、組織の目的を達成するための情報戦略と捉えられ、情報セキュリティ目的の達成を管理するための要求（6.2項）はあるものの、情報セキュリティ目的の設定に関しては、組織戦略と合致していれば、比較的自由に選択でき、使い方次第で組織の強味をより強固にすることが出来る要求です。企業の目的を、「（ISMSを使い）リスクを減らし、それによって事業機会を最大にすること」と考えると、その達成は、リスクベースでAの流れに一致してしまうため、情報セキュリティ目的から始まるBの流れの必要性を感じないと考える方も多いことと思います。しかし、上記目的を達成するための戦略を「リスクマネジメントに長けた人材の育成」と考えれば、情報セキュリティ目的は、Aの流れと別の意味をなすものになるでしょう。少し極端かもしれませんが、事業機会を最大にするために、「ISMSの有効性を市場にアピールすること」や「情報の安全性について市場からのフィードバックを活用すること」など、リスクに直接かかわりを持たないテーマを、戦略的な事業活動に展開するきっかけとして、Bの流れに落とし込むことも可能です。（6.2項の解説も参照ください）情報セキュリティを活用してプラス（＋）に転じるというのが、これからの情報セキュリティの在り方なのかもしれません。用語の解説の3.08目的の注記4にある通り、情報セキュリティ目的が**特定の結果を達成するために設定するものである**と言うことを強く意識されると良いでしょう。2005年度版の4.1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・・・」と表現された中に課題や利害関係者の期待、ニーズ、情報セキュリティ戦略を含めて考えていた組織にとっては大きな変化ではないかもしれませんが、そうでない組織にとっては、ISMS導入の原点に立ち返る良い機会になることでしょう。 |
| **【組織は何をすべきか】**改めてISMS導入の趣旨を考えて見ましょう。（・・・わからないままISMSを構築していませんか？）* お客様はISMSの認証取得を要求しているが、達成を期待される成果とは？
* 情報セキュリティに関わるどんな課題が生じているか？

－　納期に影響する情報のボトルネック－　作業ミスを誘発する情報の問題－　情報の間違った伝達－　情報の悪用－　情報の停滞* 情報セキュリティで事業を変えられるか？
* 情報セキュリティで何を、マーケットに伝えられるか？
* 情報セキュリティで企業文化を変えられるか？

我々は、何をしたいのか？　　　　　　　　　　　　　　　 どんな戦略が考えられるか？* 情報の流通スピードを高めたい。
* 情報の安全性を高めたい。
* 情報の正確性を高めたい。
* 情報の安定性（継続性）を高めたい。

（自身の言葉で目的を説明できることが重要）6.1　リスク及び機会に対処する活動　　　　　6.2　情報セキュリティ目的及びそれを達成するための計画ここから、ISMSの設計がスタートし、上記決定事項を達成するためのリスク分析、管理策の採用の見直しが必要になります。 |

|  |
| --- |
| **管理策（付属書A）の変更・・・③** |
| 多くの管理策は、2005年版の管理策を継承し、標題と管理策については、ほぼ同じ内容と言えます。他方で、2005年以後の新しい動向や概念を取り入れている箇所がいくつか有ります。箇条、目的や管理策の配置変換については、2005年の改訂でも有りましたが、今回の改訂でも見直され、整理されています。旧2005年版と2013年版の管理策の構成の違いは、以下の表に記します。管理策の数は、2005年度版が133項目であったのに対し、2013年度版では、114項目と少なくなっています。技術的な指針は削られ、例えば、2005年版の「A.11.4 ネットワークのアクセス制御」の項については、いくつかの管理策が削除されています。また、ICTの変化に伴い陳腐化した内容については、書き換え、又は削除されています。• 2005年版「A.10.9 電子商取引サービス」（・・・書き換え）• 2005年版「A.12.5.4 情報の漏えい」（・・・削除）

|  |  |
| --- | --- |
| 旧2005年版 | 2013年版 |
| A5 情報セキュリティ基本方針 | A5 情報セキュリティのための方針群 |
| A6 情報セキュリティのための組織 | A6 情報セキュリティのための組織 |
| A7 資産の管理 | A8 資産の管理 |
| A8 人的資源のセキュリティ | A7 人的資源のセキュリティ |
| A9 物理的及び環境的セキュリティ | A11 物理的及び環境的セキュリティ |
| A10 通信及び運用管理 | A12 運用のセキュリティ |
| A13 通信のセキュリティ |
| A15 供給者関係 |
| A11 アクセス制御 | A 9 アクセス制御 |
| A12 情報システムの取得、開発及び保守 | A10 暗号 |
| A14 システムの取得、開発及び保守 |
| A13 情報セキュリティインシデントの管理 | A16 情報セキュリティインシデントの管理 |
| A14 事業継続管理 | A17 事業継続管理における情報セキュリティの側面 |
| A15 順守 | A18 順守 |
| 目的 39項目　管理策133項目 | **目的 31項目　管理策114項目** |

 |
| **【組織は何をすべきか】**2013年度版で新たに加わった管理策と内容が強化されている管理策について、リスクに影響する可能性を探り、リスクを下げる効果が認められるものであれば、適用宣言書の採用理由に記載し、宣言することが望まれます。2005年度版から削除された管理策について、リスクを下げる効果が引き続きあるものについては、除外する必要はありません。但し、適用宣言書には、2005年度版から引き続き採用したなどの理由を記載することが要求されます。また、管理目的の変更とそれに伴う管理策の位置付けが変わったことについては、その影響について検討が望まれます。それらの結果をリスク評価にフィードバックし、全体的な矛盾を無くすことが重要です。 |

**３章 用語の解説**

用語については正しくマネジメントシステムを理解するための基本であり、規格を読むための前提でなければなりません。ISO/IEC 27000の発行が間に合わないからといって、規格を読まないわけにはいかないため、Annex SL‐Appendix 3「3. 用語及び定義」のXXXを「情報セキュリティ」に置き換え、用語の解説を以下に記します。

3.01　組織

自らの目的を達成するため、責任、権限、相互関係を伴い独自機能をもつ、個人又は集団。

注記 1 組織という概念には、法人か否か、公的か私的かを問わず、自営業者、会社、法人、事務所、企業、

当局、共同経営会社、非営利団体若しくは協会、又はこれらの一部若しくは組合せが含まれる。

（ただし、これらに限定されるものではない。）

3.02　利害関係者（interested party）（推奨用語）、ステークホルダー（stakeholder）（許容用語）

ある決定事項又は活動に影響を与え得る又は影響を受ける（影響を受けると認識している）個人又は組織。

3.03　要求事項（requirement）

明示されている、通常暗黙のうちに了解されている又は義務として要求されている、ニーズ又は期待。

注記 1 “通常暗黙のうちに了解されている”とは、組織及び利害関係者にとって、慣習又は慣行であることを意味する。

注記 2 規定要求事項とは、例えば、文書化された情報の中で、明示されている要求事項をいう。

3.04　マネジメントシステム（management system）

方針及び目的やそれらの目的を達成するためのプロセスを確立するための、組織の要素。

注記 1 一つのマネジメントシステムは、単一又は複数の分野を取り扱うことができる。

注記 2 システムの要素には、組織の構造、役割、責任、計画、運用などが含まれる。

注記 3 マネジメントシステムの適用範囲は、組織全体、組織内の固有の機能・部門、組織横断的な一つ又は複数の機能などがある。

3.05　トップマネジメント（top management）

最高位で組織を指揮し、管理する個人又は複数の個人。

注記 1 トップマネジメントは、組織内で、権限を委譲し、資源を提供する力をもっている。

注記 2 マネジメントシステムの適用範囲が組織の一部だけの場合は、トップマネジメントとは、組織内のその

一部を指揮し、管理する人をいう。

3.06　有効性（effectiveness）

計画した活動が実行され、計画した結果が達成された程度。

3.07　方針（policy）

トップマネジメントによって正式に表明された、組織の意図と方向付け。

3.08　目的（objective）

達成すべき結果。

注記 1 目的は、戦略的、戦術的又は運用的である。

注記 2 目的は、例えば、財務、安全衛生、環境の到達点（goal）のように様々な領域に関連し、様々な階層（戦略的レベル、組織全体、プロジェクト単位、製品単位、プロセス単位）で適用できる。

注記 3 目的は、例えば、意図する成果、Purpose、運用基準など、別の形で表現することもできる。

同じような意味をもつ別の用語、例えば、狙い（aim）、到達点（goal）、目標（target）で表すことも

できる。

**注記 4 情報セキュリティマネジメントシステムの場合、組織は、特定の結果を達成するため、情報セキュリティ方針と整合のとれた情報セキュリティ目的を設定する。**

3.09　リスク（risk）

不確かさの影響。

注記 1 影響とは、期待されていることから、好ましい方向又は好ましくない方向に乖離すること。

注記 2 不確かさとは、事象、その結果又はその起こりやすさに関する、情報、理解又は知識に、部分的にでも

不備がある状態。

注記 3 リスクは、起こり得る事象及び結果、又はこれらの組合せについて述べることによって、特徴を示す。

注記 4 リスクは、ある事象とそれによって生じる周辺状況の変化が及ぼす結果と、その事象の発生しやすさとの組合せとして表現される。

3.10　力量（competence）

意図した結果を達成するために、知識及び技能を適用する能力。

3.11　文書化された情報（documented information）

組織が管理し、維持するよう要求されている情報、及びそれが含まれている媒体。

注記 1 文書化された情報は、あらゆる形式及び媒体の形をとることができ、あらゆる情報源から得られる。

注記 2 文書化された情報には、次に示すものがある。

- 　関連するプロセスを含む、マネジメントシステムの情報

- 　組織の運用のために作成された情報（文書類）

- 　達成された結果の証拠（記録）

3.12　プロセス（process）

インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動。

3.13　パフォーマンス（performance）

測定可能な結果。

注記 1 パフォーマンスは、定量的又は定性的な所見のいずれにも関連する。

注記 2 パフォーマンスは、活動、プロセス、製品、サービス、システム、又は組織の運営管理に関係する。

3.14　外部委託する（outsource）（動詞）

ある組織の機能又はプロセスの一部を外部の組織が実施すること。

注記 1 外部委託された機能又はプロセスはマネジメントシステムの適用範囲内にあるが、外部の組織はマネジメントシステムの適用範囲の外にある。

3.15　監視（monitoring）

システム、プロセス又は活動の状況を明確にすること。

状況を明確にするために、点検、監督、又は、注意深い観察が必要な場合もある。

3.16　測定（measurement）

値を決定するプロセス。

3.17　監査（audit）

監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための体系的で、独立し、文書化されたプロセス。

注記 1 監査は、内部監査（第一者）外部監査（第二者・第三者）のいずれでも、又は複合監査（複数の分野の組合せ）もある。

注記 2 “監査証拠”及び“監査基準”は、JIS Q 19011 に定義。

3.18　適合（conformity）

要求事項を満たしていること。

3.19　不適合（nonconformity）

要求事項を満たしていないこと。

3.20　修正（correction）

検出された不適合を除去するための処置。

3.21　是正処置（corrective action）

不適合の原因を除去し、再発を防止するための処置。

3.22　継続的改善（continual improvement）

パフォーマンスを向上するために繰り返し行われる活動。

**４章　要求事項の解説**

4章からの要求事項について解説します。規格要求事項の理解を助けるために、【意訳】と書かれた欄に、要求事項の意訳を掲載しています。正確に規格要求事項を理解する際は、規格の英文又は正式な翻訳文を参照ください。

**○４－１　要求事項**

|  |
| --- |
| **4.組織の状況** |
| 4.1　組織及びその状況の理解 | 旧項番：4.1 | 改訂の影響：やや大 |
| 【意訳】組織の目的に関連し、ISMSの意図を達成することに影響する、外部、内部の課題を決めなければならない。注記：“課題の決定”とは、ISO31000:2009（リスクマネジメント-原則及び指針）の5.3に記載されている組織の外部状況、内部状況を確定すること。 |
| 【解説】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。注記にあるISO 31000:2009の外部状況、内部状況の確定について、以下に補足をします。外部状況とは、組織が自ら目的を達成しようとする状態を取り巻く外部の環境の事で、内部状況とは、同じく内部の環境の事です。外部、内部の課題を決定するために、そこからどの様な影響を受けるかに注目しなければなりません。【外部状況】次の様な事が外部状況として含まれます。－　社会環境、文化、政治の影響、法律・規制、金融・経済環境、自然環境、競争関係－　組織の目的に影響を与える原動力、傾向－　外部の利害関係者との関係、認知、価値観【内部状況】次の様な事が内部状況として含まれます。－　統制、体制、役割、アカウンタビリティ－　方針、目的、戦略－　資源、知識、能力－　内部の利害関係者との関係、認知、価値観－　組織文化－　情報システム、情報の流れ、意思決定プロセス－　組織の決め事－　契約 |
| 【期待される対応】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。 |
| 4.2　利害関係者のニーズ及び期待の理解 | 旧項番：0.2.2、4.1 | 改訂の影響：やや大 |
| 【意訳】組織は、次の事を決めなければならない。a） ISMSの利害関係者b） 利害関係者の情報セキュリティに関する要求事項注記：利害関係者の要求事項は、法的及び規制の要求事項や契約上の義務を含めてもよい。 |
| 【解説】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。 |
| 【期待される対応】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。 |
| 4.3　情報セキュリティマネジメントシステムの適用範囲の決定 | 旧項番：4.2.1 a） | 改訂の影響：小 |
| 【意訳】組織は、 ISMSの適用範囲を決めるために、その境界と適用の根拠を示さなければならない。適用範囲を決める際、組織は、次の事を考慮しなければならない。a） 4.1項の外部、内部の課題b） 4.2項の要求事項c） 組織の活動と他の組織の活動間の、インタフェースと依存関係ISMSの適用範囲は、”文書化された情報”として利用可能な状態になっていなければならない。 |
| 【解説】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。適用範囲については、対象となる建物、システム、設備などを何処から何処まで含めるかと言うような物理的境界や、情報がやり取りされる論理的な境界、業務プロセスにおけるサプライチェーンなどの管理義務の及ぶ境界を考慮し、適用しなければ課題やニーズ、期待を解決又は満足させることが出来ない範囲として直接管理可能な対象を含む必要があります。また、直接管理できない範囲については、その範囲において組織の管理義務を果たす為に、組織の活動と他の組織の活動間の、インタフェースと依存関係を考慮することが要求されています。 |
| 【期待される対応】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。 |
| 4.4　情報セキュリティマネジメントシステム | 旧項番：4.1 | 改訂の影響：小 |
| 【意訳】組織は、この国際規格の要求事項に従って、 ISMSを確立、実施、維持、及び、継続的に改善しなければならない。 |
| 【解説】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。 |
| 【期待される対応】2章の「ISMSの目的がより鮮明に・・・②」の解説を参照ください。 |

|  |
| --- |
| **5.リーダシップ** |
| 5.1　リーダシップ及びコミットメント | 旧項番：5.1 | 改訂の影響：小 |
| 【意訳】トップマネジメントは、次に示す事によって、 ISMSに関するリーダシップとコミットメントを実証しなければならない。a）情報セキュリティ方針と情報セキュリティ目的を戦略的な方向性と矛盾なく確立するb）ISMSの要求事項を組織のプロセスに統合するc）ISMSに必要な資源を利用可能にするd）情報セキュリティマネジメントが効果的であることISMSの数ある要求事項に適合する重要性を伝えるe）ISMSが意図した成果を達成することを確実にするf） ISMSの有効性に貢献するように、人を指揮して支援するg）継続的改善を促進するh）関連する管理層がその責任の下、リーダシップを発揮できるよう管理層の役割を支援する |
| 【解説】ISMSを確立、実施、維持、改善を成功させるためには、トップマネジメントの関与が必須条件であることが記されています。大切なのは、組織の戦略との一致と必要な資源の提供、管理層を含めた社内への支援をリーダシップの下に実施することです。情報セキュリティが独り歩きし、事業と乖離しないように、a）の戦略的な方向性との両立やb）の組織のプロセスとの統合が強調されています。また、d）のISMSの要求事項は、ISO207001の要求事項のみならず、法律や事業要求など、組織の活動に関わる様々なISMS上の要求事項への適合の重要性を含んで考えなければなりません。見過ごしやすいところなので注意が必要です。d）やg）の項目は、5.2項の方針に含めることによって、コミットメントされるものと考えます。情報セキュリティ目的については、2章の「ISMSの目的がより鮮明に・・・②」の解説及び3章の「用語の解説3.08　目的」を参照し、リスクアプローチとの違いを理解してください。 |
| 【期待される対応】トップマネジメントのリーダシップが期待されます。 |
| 5.2　方針 | 旧項番：4.2.1、5,1 | 改訂の影響：小 |
| 【意訳】トップマネジメントは、次の事を満たした情報セキュリティ方針を制定しなければならない。a）組織の目的に相応しいb）情報セキュリティ目的（6.2参照）を含むか、又は情報セキュリティ目的を設定するための枠組みを示すc）情報セキュリティに関する適用可能な要求事項を満たすことへのコミットメント（誓い）を含むd）ISMSの継続的改善へのコミットメント（誓い）を含む情報セキュリティ方針は、次に示す事を満たさなければならないe）”文書化された情報”として利用可能であるf） 組織内に伝達するg）利害関係者が必要に応じて入手できる |
| 【解説】情報セキュリティ目的については、2章の「ISMSの目的がより鮮明に・・・②」の解説及び3章の「用語の解説3.08　目的」を参照し、リスクアプローチとの違いを理解してください。 |
| 【期待される対応】情報セキュリティ方針文書の作成、社内周知が期待されます。 |
| 5.3　組織の役割、責任及び権限 | 旧項番：5.1、7.2 | 改訂の影響：小 |
| 【意訳】トップマネジメントは、情報セキュリティの役割について、その責任・権限を割り当て、確実に伝えなければならない。トップマネジメントは、次の役割について、責任・権限を割り当てなければならない。a） ISMSが、この国際規格の要求事項に適合することを確実にするb） ISMSのパフォーマンスをトップマネジメントに報告する注記：トップマネジメントは、ISMSのパフォーマンスを組織内に報告する責任・権限を割り当ててもよい。 |
| 【解説】5.3　組織の役割、責任及び権限では、以下の2つの役割が扱われています。1. 情報セキュリティに関連する役割・・・情報のオーナー、情報セキュリティプロセスオーナー等
2. ISMS（マネジメントシステム）に関連する役割・・・文書管理、リスクアセスメント、教育、内部監査、

各種ISMS会議の開催等 |
| 【期待される対応】職務分掌、各種手順、計画への役割、責任及び権限の記載が期待されます。 |

|  |
| --- |
| **6．計画** |
| 6.1　リスク及び機会への取組み |
| 6.1.1　一般 | 旧項番：New | 改訂の影響：やや大 |
| 【意訳】ISMSの計画を策定する際、組織は、 4.1項で特定した課題や4.2項で特定した要求事項を考慮し、次の事のために取り組むべきリスクと改善の機会を特定しなければならない。a） ISMSが意図した効果を達成するb） 望ましくない影響を防止又は低減するc） 継続的改善を達成する組織は、次の事への構想を練らなければならない。d） これらのリスクと改善の機会に取り組むための活動e） 次の事を行う方法　1）これらの活動をISMSのプロセスの中に統合し、実施する　2）これらの活動の有効性を評価する |
| 【解説】6.1.1項では、4.1項と4.2項の決定事項を、リスクアセスメントや計画、実施、監視、改善などのISMSのプロセスにどのようにつなげていくかについて記載されています。前半は、ISMSの意図した効果の達成と、それを阻む影響を排除するために、リスクと改善の機会（改善の可能性がある分野）を決定しなければならないという原則を述べ、後半には、これらのリスクと改善の機会に対する取り組み方や評価方法をどうするかについて、ISMSに統合されたプロセスの構想を練るよう要求されています。原文はPlanと書かれていますが、この項は、計画書の作成を求めている内容ではないため、意訳では“構想を練らなければならない”としました。 |
| 【期待される対応】4.1項と4.2項での決定事項を、どのようにISMSプロセスにつなげていくかについて、考え方の整理が期待されます。 |
| 6.1.2　情報セキュリティリスクアセスメント | 旧項番：4.2.1 | 改訂の影響：小 |
| 【意訳】組織は、次の情報セキュリティリスクアセスメントのプロセスを明確にし、適用しなければならない。a）次の基準を含む情報セキュリティリスク基準を制定し、維持するプロセス　1） リスクを受容する基準　2） 情報セキュリティリスクをアセスメントするための基準b） 繰り返し行われる情報セキュリティリスクアセスメントが一貫性、妥当性を有し、比較可能な結果を生み出すことを確実にするプロセスc）次の事を有する情報セキュリティリスクを特定するプロセス　1） ISMSの適用範囲内の情報の、機密性、完全性、可用性の喪失に結びつくリスクを特定する　2） リスクのオーナーを特定するd）次の事によって情報セキュリティリスクを分析するプロセス　1） 6.1.2 c）1）で特定されたリスクが顕在化した場合に起こり得る結果をアセスメントする　2） 6.1.2 c）1）で特定されたリスクの現実的な起こりやすさをアセスメントする　3） リスクレベルを決定するe）次の事によって情報セキュリティリスクを評価するプロセス　1） リスク分析の結果と6.1.2 a）で制定したリスク基準を比較する　2） リスク対応のために、分析したリスクに優先順位を付ける組織は、情報セキュリティリスクアセスメントプロセスを”文書化された情報”として保持しなければならない。 |
| 【解説】2005年度版の要求事項では、資産ベースに細かいアプローチの規制があったものが、簡素化されたことによって、より自由度のあるリスク評価の展開が許容されたと考えてよいでしょう。会議体（個人）による形式にとらわれない情報セキュリティリスクアセスメントのアプローチも採用しやすい要求になりました。 |
| 【期待される対応】リスクアセスメントを実施するための基準の見直しが期待されます。2013年度版への対応として、リスクアセスメントのアプローチを見直す必要が有るか／無いかについては、既存の評価方法が効果的且つ成熟しているか否かによります。上手く行っている組織については、変える必要はないかもしれません。 |
| 6.1.3　情報セキュリティリスク対応 | 旧項番：4.2.1 | 改訂の影響：やや大 |
| 【意訳】組織は、次の情報セキュリティリスク対応プロセスを定め、適用しなければならない。a） リスクアセスメントの結果を踏まえ、適切な情報セキュリティリスク対応の選択肢を決めるプロセスb） 決定した情報セキュリティリスク対応の選択肢として必要な管理策を決めるプロセス注記：組織は、必要な管理策を立案するか、又は任意の情報源の中から管理策を特定することができる。c） 6.1.3 b）で決めた管理策を附属書Aに示す管理策と比較し、必要な管理策の見落しが無いことを検証するプロセス注記1： 附属書Aは、管理目的及び管理策の包括的なリストである。この国際規格の利用者は、必要な管理策を見落とさないために、附属書Aを参照することを意図している。注記2 ：管理目的は、選択した管理策に暗に含まれているものである。附属書Aに規定した管理目的及び管理策は、全てを網羅しているわけではないため、追加の管理目的、管理策が必要な場合もある。d） 適用宣言書を作成するプロセス。適用宣言書には、必要とした管理策〔6.1.3のb）及びc）参照〕、それらの管理策を必要とした理由、それらの管理策を実施しているか否か、附属書Aに規定する管理策を除外した理由の記載を含むe） 情報セキュリティリスク対応計画を策定するプロセスf） 情報セキュリティリスク対応計画、及び、残留している情報セキュリティリスクの受容について、 リスクのオーナーの承認を得るプロセス組織は、情報セキュリティリスク対応のプロセスを”文書化された情報”として保持しなければならない。注記：この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは、 ISO 31000に規定する原則及び一般的な指針と整合している。 |
| 【解説】2005年度版の要求事項では、「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なように、管理目的及び管理策を選択しなければならない」と記されていた部分が、「管理策の見落としが無いことを検証する」と表現が変わっています。管理策の採用は附属書Aに留まることなく、さまざまなソースの活用を意図したための変化です。事業分野に特化したガイドライン（分野別指針）や他の規格の参照も意図しておくと良いでしょう。分野別指針：ISO/IEC 27010 Information security management for inter-sector and inter-organizational communicationsISO/IEC 27011 Information security management guidelines for telecommunications based on ISO/IEC 27002ISO/IEC 27017 Code of practice for information security controls for cloud computing services based on ISO/IEC 27002等適用宣言書への記載は、附属書Aに留まらず、採用したすべての管理策を採用理由も含め記載することになります。採用理由については、リスク低減に他なりませんが、以前より実施している管理策は、「それらの管理策を実施しているか否か」の記載と併せて参照手順などの引用で伝わります。附属書Aに規定する管理策を除外した際はその理由が必要です。リスク対応計画や残留リスクの受容承認については、「経営陣の承認」からリスクオーナーに改まっています。経営に関わるリスクについては、引き続き経営陣がリスク所有者になりますが、部門プロセスのリスク改善については、リスク所有者の責任を部門長が保有しているものと考えます。 |
| 【期待される対応】適用宣言書の改訂付属書Aについては、今回の改訂で管理目的、管理策の編成や追加がされているため、2013年度版への対応時に、管理策の見落としが無いことを検証することと、項番の並べ替えが期待されます。2章の「管理策（付属書A）の変更・・・③」の解説を参照ください。リスク対応プロセスに関わる文書化された情報（基準、手順）の作成も忘れてはなりません。 |
| **6．計画** |
| 6.2　情報セキュリティ目的及びそれを達成するための計画策定 | 旧項番：New | 改訂の影響：やや大 |
| 【意訳】組織は、関係する組織の機能や階層で、情報セキュリティ目的を定めなければならない。情報セキュリティ目的は、次の事を満たさなければならない。a） 情報セキュリティ方針と一致しているb） 測定可能である（但し、実行可能な場合）c） 適用可能な情報セキュリティの要求事項、リスクアセスメント及びリスク対応の結果を考慮しているd） 適切に（必要に応じて）伝達するe） 適切に（必要に応じて）更新する組織は、情報セキュリティ目的を”文書化された情報”として保持しなければならない。組織は、情報セキュリティ目的の達成方法を計画する際、次の事を決めなければならない。f） 実施すべき事g） 必要な資源h） 責任者i） 達成期限j） 結果の評価方法 |
| 【解説】トップマネジメントのリーダシップの下、推進される計画です。組織の戦略に情報セキュリティを組み込み、方針展開させ、PDCAを完結する流れになります。2章の「ISMSの目的がより鮮明に・・・②」の解説及び3章の「用語の解説3.08　目的」を参照し、リスクアプローチとの違いを理解してください。 |
| 【期待される対応】情報セキュリティ戦略との両立が期待されます。情報セキュリティ目的については、3章の「用語の解説3.08　目的」に記載されている通り、**特定の結果を達成するため**のものです。例えば、「セキュリティインシデントを3件以下」と言うように情報セキュリティ目的を設定しても規格適合と言う観点からは、成立しますが、セキュリティインシデントを削減するアプローチが6.1項で特定されたリスクと被ってしまうため、6.2項で扱う意味が薄れてしまいます。「○○プロセスにおける情報のボトルネック解消」や「開発環境のクラウド化推進」などの情報セキュリティ目的は、事業に結びついた情報セキュリティ戦略であることと、リスクについては、戦略によって生じるものであるため、6.1項のリスクアプローチと被ることはありません。6.2項の計画を推進する過程で、6.1項のリスクアプローチを利用することはありますが、これは情報セキュリティ目的を達成するためにf） 実施事項として必要なリスクアプローチが採用されたと考えれば納得いくものと思われます。情報セキュリティ目的に関わる文書化された情報（目的、計画、測定（フォローアップ）、伝達、更新）の作成も忘れてはなりません。 |

|  |
| --- |
| **７．支援** |
| 7.1　資源 | 旧項番：5.2.1 | 改訂の影響：小 |
| 【意訳】組織は、 ISMSの確立、 実施、維持及び継続的改善に必要な資源を決定し、提供しなければならない。 |
| 【解説】資源の決定、提供については、リーダシップ（5.1項　c, e, f, g, h）の要求事項を念頭に、進めなければなりません。資源は、ただ導入し、提供し、あとは良きに計らえ、では効果を生みません。導入計画はあるが先に進まないケースをよく目にします。利用可能な状態に整え、関係するリスクのオーナーに意図した成果を伝え、指揮し、管理層がリーダシップを発揮するなど、それを生かす計画が重要です。以下に、5.1項のc）, e）, f）, g）, h）の要求事項を記します。c）ISMSに必要な資源を利用可能にするe）ISMSが意図した成果を達成することを確実にするf） ISMSの有効性に貢献するように、人を指揮して支援するg）継続的改善を促進するh）関連する管理層がその責任の下、リーダシップを発揮できるよう管理層の役割を支援する |
| 【期待される対応】リーダシップの発揮に期待します。 |
| 7.2　力量 | 旧項番：5.2.2 | 改訂の影響：小 |
| 【意訳】組織は、次の事を行わなければならない。a） 情報セキュリティパフォーマンスに影響を与える業務を行う管理下の人に必要な力量を、決定するb） 教育、訓練、経験に基づいて、これらの人に力量が有ることを、確実にするc） 該当する場合には、必要な力量を身につけるための手段を講じ（注記）、その有効性を評価するd） 力量の証拠として適切なものを、”文書化された情報”として保持する注記：講じる手段には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、 配置転換の実施などがあり、また、力量を備えた人々の雇用、そうした人々との契約締結などもある |
| 【解説】力量と言う言葉は、日常あまり使わない言葉だと思います。3章の「用語の解説3.10　力量（competence）」では、「意図した結果を達成するために、知識及び技能を適用する能力」と記載されていますが、情報セキュリティパフォーマンスに影響を与える業務、即ち、管理策の実施やリスクアセスメント、内部監査やその他監視などを確実に遂行できる人を育成するために、知識を得る教育と能力を伸ばす訓練（トレーニング）、実体験を活用しなければなりません。a）で必要な力量を決定し、b）でこれまでの教育訓練経験に基づいて力量が備わっている（又はいない）を見極め、c）で必要に応じた教育訓練の提供、指導の実施、 配置転換の実施などの処置を講じ、d）で力量が備わっていることを裏付ける証拠を保持することが要求されています。 |
| 【期待される対応】必要な力量を決定、教育、訓練をプランニング、その際、パフォーマンスの影響が力量への依存度が高い場合、必要な力量を身につけたことを“確信する手段方法”（有効性評価）をあらかじめ考えておくとよいでしょう。力量を決定、教育、訓練、処置及びその有効性の評価を立証する証拠（記録）の作成も忘れてはなりません。 |
| 7.3　認識 | 旧項番：5.2.2 | 改訂の影響：小 |
| 【意訳】組織の管理下で働く人々は、次の事に関して知覚していなければならない。a） 情報セキュリティ方針b） 情報セキュリティパフォーマンスの向上によって得られる効果やISMSの有効性に対する自らの貢献c） ISMSの数ある要求事項に適合しないことが、何を意味するか |
| 【解説】最近では、eラーニングを活用しISMSの基礎教育を実施している組織を多く見かけます。認識をもたせる手段として基礎教育は欠かせない存在になっているものと思われます。併せてその責任の所在を考え、リーダシップの発揮に期待します。（5.1項　d, e, f, h）を考え、進めなければなりません。以下に、5.1項のd）, e）, f）, h）の要求事項を記します。d）情報セキュリティマネジメントが効果的であることISMSの数ある要求事項に適合する重要性を伝えるe）ISMSが意図した成果を達成することを確実にするf） ISMSの有効性に貢献するように、人を指揮して支援するh）関連する管理層がその責任の下、リーダシップを発揮できるよう管理層の役割を支援する |
| 【期待される対応】リーダシップの発揮に期待します。 |
| 7.4　コミュニケーション | 旧項番：New | 改訂の影響：中 |
| 【意訳】組織は、次の事を含み、ISMSに関する内部、外部のコミュニケーションのために必要な事項を決めなければならない。a） 何をコミュニケーションするのかb） 何時コミュニケーションするのかc） 誰とコミュニケーションするのかd） 誰がコミュニケーションするのかe） コミュニケーションを実施するプロセス |
| 【解説】2005年度版では、トップマネジメントの「 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」の伝達に関わる責任と「A.6.1.2 情報セキュリティの調整」の管理策が7.4項に包含されたものと考えます。コミュニケーションの不備・不足は、情報のリスクであるという考えから管理策としての重要性も感じますが、 2013年の改訂では、管理策から除外されています。多くのリスク対応に「A.6.1.2 情報セキュリティの調整」を採用している組織は、管理策として残すことも含め2章の「管理策（付属書A）の変更・・・③」の解説を参照ください。要求事項では、「ISMSに関連する内部及び外部のコミュニケーションを実施する必要性を決定すること」が要求されています。外部のコミュニケーションとしては、お客様、サプライヤー、その他外部の利害関係者との事業推進上の報告や情報交換、法律上の届け出や情報公開などが考えられます。内部のコミュニケーションについては経営会議や部門長会議、セキュリティ委員会、朝礼など階層（戦略的レベル、組織全体、プロジェクト単位、製品単位、プロセス単位）ごとにコミュニケーションの場が存在します。 |
| 【期待される対応】ISMSに関連する内部及び外部のコミュニケーションを実施する必要性を決定することが求められます。 |
| 7.5　文書化された情報 |
| 7.5.1　一般 | 旧項番：4.3 | 改訂の影響：小 |
| 【意訳】ISMSには、次の”文書化された情報”を含まなければならない。a） この規格が要求する”文書化された情報”b） ISMSの有効性のために必要であると組織が決定した、”文書化された情報”注記：”文書化された情報”の程度は、次のような理由で、組織毎に異なる。a） 組織の規模、活動、プロセス、製品・サービスの種類b） プロセス及びプロセス相互の複雑さc） 人々が有する力量 |
| 【解説】文書化された情報として本文中に記載があるものを示します。5.2　　情報セキュリティ方針6.1.2　リスクアセスメントプロセスに関わる文書化された情報（基準、手順）6.1.3　リスク対応プロセスに関わる文書化された情報（基準、手順）6.2　　情報セキュリティ目的に関わる文書化された情報（目的、計画、測定（フォローアップ）、伝達、更新）7.2　　力量の証拠（記録）7.5.1　組織が決めた文書化された情報8.1　　プロセス実施に関わる文書化された情報（運用計画、運用の記録）8.2　　リスクアセスメントの結果（運用の記録）8.3　　リスク対応の結果（運用の記録）9.1　　監視・測定の結果（運用の記録）9.2　　監査プログラムの実施、結果に関わる文書化された情報（監査計画、チェックリスト、報告書）9.3　　マネジメントレビューの結果（指示事項）10.1　 不適合の内容と処置、処置の結果（記録） |
| 【期待される対応】文書化の適切性は、その文書が意図した目的を達成するに十分なものであるか否かです。指示文書であるならば、指示を受ける人が、参照し、正確に指示に従う状況が無ければなりません。作成しただけで、事実上お蔵入りしている文書（誰も見ない）は文書化の適切性に疑問が残ります。また、証拠となる記録類は、裏付け情報がしっかり記されていなければなりません。承認欄ばかりが並び、肝心なことが記されていない記録をよく目にしますが、見直しの機会として利用されるとよいでしょう。 |
| 7.5.2　作成及び更新 | 旧項番：4.3 | 改訂の影響：小 |
| 【意訳】“文書化された情報”を作成及び、更新する際、組織は、次の事を確実にしなければならない。a） 適切な識別と記述（タイトル、 日付、作成者、参照番号等）b） 適切な書式（言語、ソフトウェアの版、図表）と媒体（紙、電子媒体等）c） 適切性と妥当性を、レビューし、承認する |
| 【解説】文書の識別や、承認など基本中の基本が書かれています。理解できない内容ではありませんが、等閑にならないよう注意が必要です。 |
| 【期待される対応】承認については、”文書化された情報”を展開することによって生ずる影響に見合った責任及び権限を有していることを確実にしなければなりません。その責任及び権限がトップマネジメントによって割り当てられるものであることが、「5.3　組織の役割、責任及び権限」に記載されています。 |
| 7.5.3　文書化された情報の管理 | 旧項番：4.3 | 改訂の影響：小 |
| 【意訳】“文書化された情報”は、次の事を確実にするために、管理しなければならない。a） “文書化された情報”が必要なときに、必要な場所で、適切に利用できるb） “文書化された情報”が十分に保護されている（機密性の喪失、不適切な使用、完全'性の喪失からの保護等）“文書化された情報”の管理のために、次の事を実施しなければならない（該当する場合）。c） 配付、アクセス、検索、利用d） 読み取れる状態に保つことを含む、保管と保護e） 変更の管理（版の管理等）f） （必要期間）保持する事と廃棄ISMSの計画及び運用時に欠くことの出来ない外部の”文書化された情報”は、適切なものを特定して、管理しなければならない。注記：アクセスとは、”文書化された情報”の閲覧許可又は、閲覧及び変更の許可、権限に関する決定などを意味する。 |
| 【解説】文書化された情報の利用や、アクセス権による情報の保護など文書管理の基本が書かれています。理解できない内容ではありませんが、等閑にならないよう注意が必要です。 |
| 【期待される対応】文書化された情報に関する要求全体（7.5.1～7.5.3）を通じて、情報の価値に見合った保護の重要性の理解を深め、バランスの良いISMSを推進されることに期待します。 |

|  |
| --- |
| **8．運用** |
| 8.1　運用の計画及び管理 | 旧項番：4.2.1、4.2.2 | 改訂の影響：小 |
| 【意訳】組織は、情報セキュリティの要求事項を満たすため、及び6.1項で決めた活動を行うために、必要なプロセスを計画し、実施し、管理しなければならない。また、6.2項で決めた情報セキュリティ目的を達成するための計画も実施しなければならない。組織は、プロセスが計画通りに実施されたことの確信を持つために、必要なものを”文書化された情報”として保持しなければならない。組織は、計画した変更を管理し、予期せぬ変更の結果をレビューし、必要に応じて、負の影響を軽減する処置をとらなければならない。組織は、外部委託するプロセスを決定し、管理を確実にしなければならない。 |
| 【解説】「6　計画」を実施に移すさいの要求事項です。計画された情報セキュリティ目的やリスクアセスメント、それらを管理する手順に関わる実作業で遵守すべきことが要求されています。 |
| 【期待される対応】実践あるのみです。運用に関わる文書化された情報（運用計画、運用の記録）の作成も忘れてはなりません。 |
| 8.2　情報セキュリティリスクアセスメント | 旧項番：4.2.1、4.2.2 | 改訂の影響：小 |
| 【意訳】組織は、あらかじめ定められた間隔で、又は、重要な変更、若しくは重大な変化が生じた場合に、 6.1.2 項のa）で制定した基準を考慮し、情報セキュリティリスクアセスメントを実施しなければならない。組織は、情報セキュリティリスクアセスメント結果を”文書化された情報”として保持しなければならない。 |
| 【解説】情報セキュリティリスクアセスメントの実施時期についての要求が8.2項に記載されています。PDCAのサイクルに乗せるために付属書SL‐Appendix 3に無い項目をISO/IEC 27001で独自に追加したものです。この要求事項で注意しなければならないポイントが一つあります。それは、下記に記す6.1.2 項のa）で制定した基準については、「・・・考慮する事」と要求されている点です。情報セキュリティリスクは、必ずしも計算式だけで測れるものではないことが、ここから伺えます。6.1.2項のリスクアセスメントの要求が今回の改訂で自由度のあるものに改められたことにも関係する内容です。基準と異なる結果を採用した場合は、その正当性を”文書化された情報”として保持する必要は有るものの、禁止事項ではないということがわかります。以下に、6.1.2項のa）の要求事項を記します。次の基準を含む情報セキュリティリスク基準を制定し、維持するプロセス　1） リスクを受容する基準　2） 情報セキュリティリスクをアセスメントするための基準 |
| 【期待される対応】6.1.2項の情報セキュリティリスクアセスメントを実践するのみです。リスクアセスメントの結果（運用の記録）の作成も忘れてはなりません。 |
| 8.3　情報セキュリティリスク対応 | 旧項番：4.2.2 | 改訂の影響：小 |
| 【意訳】情報セキュリティリスク対応計画を実施しなければならない。情報セキュリティリスク対応結果を”文書化された情報”として保持しなければならない |
| 【解説】6.1.3項の情報セキュリティリスク対応を実施するための要求事項です。PDCAのサイクルに乗せるために付属書SL‐Appendix 3に無い項目をISO/IEC 27001で独自に追加したものです。 |
| 【期待される対応】6.1.3項の情報セキュリティリスク対応を実践するのみです。リスク対応の結果（運用の記録）の作成も忘れてはなりません。 |

|  |
| --- |
| **9.パフォーマンス評価** |
| 9.1　監視、測定、分析及び評価 | 旧項番：4.2.3 | 改訂の影響：小 |
| 【意訳】組織は、情報セキュリティのパフォーマンスと、ISMSの有効性を評価しなければならない。組織は、次の事を決めなければならない。a） 必要な監視・測定の対象を決定する。これには、情報セキュリティプロセスと管理策を対象として含むb） 実施結果の正当性（効果）を保証するための、監視、測定、分析、評価の方法を決定する。（該当する場合）注記：方法は、正当な根拠となるよう、比較可能で再現可能な結果を生み出すことが望ましいc） 何時、監視・測定するのかd） 誰が、監視・測定するのかe） 何時、監視・測定結果の分析・評価するのか誰が、監視・測定結果の分析・評価するのか組織は、監視・測定結果の証拠を”文書化された情報”として保持しなければならない。 |
| 【解説】情報セキュリティパフォーマンスとISMS（マネジメントシステム）の有効性を扱っています。ISMSの有効性は、「9.2　内部監査」によって情報を収集し「9.3　マネジメントレビュー」で確認することが基本的な要求事項の対応と言えるでしょう。内部監査結果から分るISMSの各種要求事項の順守状況から結論付けられる有効性や、内部監査の調査そのものの有効性など、さまざまな見方が出来ます。また、情報セキュリティパフォーマンスの向上がISMSの有効性と強い相関があるものと考えれば、情報セキュリティパフォーマンスの評価も、ISMSの有効性を測ることに通じます。情報セキュリティパフォーマンスについては、「A.12.4　ログ取得及び監視」や「15.2.1 供給者が提供するサービスの監視及びレビュー」などの管理策が、情報セキュリティパフォーマンスの監視に当たるものもあれば、情報セキュリティ目的の達成状況、外部、内部の課題の状況変化を評価するなど、ISMSの意図した効果を測る方法もあります。個別に重要な管理策のパフォーマンスチェックを計画するのも一つの方法ですが、それなりに手間がかかる作業であり、監視・測定のターゲットを絞り込む必要が有ります。リスクアセスメントも、網羅的且つ継続的に情報セキュリティパフォーマンスを測定する手段と考えてもよいでしょう。 |
| 【期待される対応】監視・測定の意図を明確にし、情報セキュリティパフォーマンスを測定した結果が、「10．改善」につながるように評価を心がけてください。監視及び測定の結果の証拠（記録）の作成も忘れてはなりません。 |
| 9.2　内部監査 | 旧項番：6 | 改訂の影響：小 |
| 【意訳】組織は、 ISMSが次の状況にあるか否かについて情報提供を行うために、あらかじめ定められた間隔で、内部監査を実施しなければならない。a） 次の事に適合しているか否か　1） ISMSについて、組織が認めた要求事項　　2） この国際規格の要求事項b） 有効に実施され、維持されているか否か組織は、次に示す事を行わなければならない。c） 頻度、方法、責任、計画に要求している事、報告を含む監査プログラムを計画し、確立し、実施し、維持しなければならない監査プログラムは、関連する（監査対象となる）プロセスの重要性及び前回までの監査結果を考慮しなければならないd） 監査基準及び監査範囲を明確にする。e） 監査プロセスの客観性及び公平性を確保した上で、監査員を選定し、監査を実施するf） 監査結果を関連する管理層に報告するg） 監査プログラム及び監査結果の証拠を”文書化された情報”として保持する |
| 【解説】内部監査では、次の2つの観点で評価することが求められています。①決めたルールが守られている（適合している）こと②有効に実施され、維持されていること上記二つの評価の内、①についてはチェックリストが効果的です。②については、内部監査員の実力の見せ所です。有効なISMSとは、「4.1　組織及びその状況の理解」、「4.2　利害関係者のニーズ及び期待の理解」によって特定された課題や期待、ニーズ、更に情報セキュリティ目的に対処し、意図した成果を達成するためにISMSが活用されている様を表し、リスクアセスメントから各種計画、実施、監視、改善の全ての効果を総合的に測る活動です。 |
| 【期待される対応】内部監査員の実践的なトレーニングにも期待します。監査プログラムの実施、結果に関わる文書化された情報（監査計画、チェックリスト、報告書）の作成も忘れてはなりません。 |
| 9.3　マネジメントレビュー | 旧項番：7 | 改訂の影響：小 |
| 【意訳】トップマネジメントは、ISMSが、適切で、妥当で、且つ有効であることを継続するために、あらかじめ定められた間隔で、 ISMSをレビューしなければならない。マネジメントレビューは、次の事を考慮しなければならない。a） 以前のマネジメントレビューから引きずっている活動の状況b） ISMSに関連する外部、内部の課題の変化c） 次への動向を含めた、情報セキュリティパフォーマンスに関するフィードバック　　1） 不適合及び是正処置　2） 監視及び測定の結果　3） 監査結果　　4） 情報セキュリティ目的の達成d） 利害関係者からのフィードバックe） リスクアセスメント結果及びリスク対応計画の状況f） 継続的改善の機会マネジメントレビューからのアウトプットには、継続的改善の機会、及びISMSのあらゆる変更の必要性に関する決定を含めなければならない。組織は、マネジメントレビュー結果を”文書化された情報”として保持しなければならない。 |
| 【解説】2005年度版では、「7.2 レビューへのインプット」の記載の中で“提供しなければならない”となっていた項目が“考慮しなければならない”に改められています。インプットの項目は、トップマネジメントが5章のリーダシップを発揮し、情報セキュリティ方針及び情報セキュリティ目的の設定、戦略との両立、資源の利用状況、ISMSの意図した成果の達成、支援すべきこと、継続的改善の促進を考える上で、判断材料となる情報を列挙したものです。“考慮すしなければならない”と改まったことは、判断材料のISMS事務局任せでの提示の網羅性を求めるのでなく、トップマネジメント主導で考慮する事を重んじたものと思われます。9.3項でもう一つ重要なことは、マネジメントレビュープロセスの中で、継続的改善の機会や、ISMSのあらゆる変更の必要性に関する決定がなされ、その結果を”文書化された情報”として保持することです。 |
| 【期待される対応】リーダシップの発揮に期待します。マネジメントレビューの結果の証拠（記録）の作成も忘れてはなりません。 |

|  |
| --- |
| **10．改善** |
| 10.1　不適合及び是正処置 | 旧項番：8.2 | 改訂の影響：中 |
| 【意訳】不適合が生じた場合、次の事を行わなければならない。a） 不適合に対応し、次の事を行う（該当する場合）　　1） 不適合を管理し、適合に直すための処置をとる　　2） 不適合が起こした結果（影響）に対処するb） 不適合を再発又は、他で発生させないために、次の事によって、不適合の原因を除去する必要が有るか／無いかを評価する　　1） 不適合をレビューする　　2） 不適合の原因を解明する　3） 類似の不適合の存在、又はそれが発生する可能性を特定するc） 原因除去に必要な処置を取るd） 全ての是正処置について、有効性をレビューする。e） ISMSの変更を行う（必要な場合）是正処置は、不適合によって引き起こされる影響に沿ったものでなければならない。組織は、次に示す証拠として、”文書化された情報”を保持しなければならない。f） 不適合の内容とそれに続く一連の処置g） 是正処置の結果 |
| 【解説】先ず、不適合について考えて見ましょう。不適合とは、法律、規格、社内規定のような明示されている要求や、暗黙のうちに了解されている又は義務として要求されているニーズ、期待も含め、組織が遵守すべき要求を満たしていない様を言います。「リスクアセスメントを実施していない」、「作成を意図した”文書化された情報”が作成されていない」、などと言うISMSの不適合から、「要求された情報の開示範囲を守っていない」、「暗号のルールを守っていない」と言うような、情報セキュリティパフォーマンスに関係する不適合も有ります。不適合が発見される場面は、内部監査の結果やインシデントの原因を特定する過程、日常の監視活動の中でも基準を満たしていないことが発覚します。その際、とるべき処置は、不適合の影響を緩和し、適合状態に戻すことを第一に考えなければなりません。不適合の原因を除去する、いわゆる是正処置は、そのあとです。“文書化された情報”（記録）は、その内容と一連の処置及び結果を留めるものでなければなりません。予防処置の要求事項の削除については、2章の「規格の構造の変化・・・①」の解説を参照ください。 |
| 【期待される対応】不適合の内容と処置、処置の結果に関わる証拠（記録）の作成も忘れてはなりません。 |
| 10.2　継続的改善 | 旧項番：8.1 | 改訂の影響：小 |
| 【意訳】組織は、 ISMSが適切で、妥当で、且つ有効で有り続けるよう、継続的に改善しなければならない。 |
| 【解説】継続的改善を表す英語表現は二つあり混同されることが多いので解説を加えます。マネジメント規格で扱う継続的改善は、”Continual improvement”で、これは断続的に改善のチャンスがあるたびに行うものです。これに対し、”Continuous improvement”は、連続的に改善をし続けるような場合に使われるものです。原価低減などはこのような類かもしれません。情報セキュリティについては、確かにリスクは絶え間なく変わります。しかしマネジメント（ISMS）は、その影響に応じてアクションをとる即ち”Continual improvement”でなければなりません。さて、10.1項の不適合及び是正処置は、不適合の影響を緩和したり、適合状態に戻したり、不適合の原因を除去したり、ISMSの改善に至らないケースの方が多いのかもしれません。それは、10.1項のe）「必要な場合には、 ISMSの変更を行う」と言う表現からもうかがえます。しかし、その中から、リスクアセスメントのリスク特定方法の改善を行ったり、各種計画の見直しを行ったり、ISMSの適合性、妥当性及び、有効性を継続的に改善につなげるチャンスを見逃さないようにしなければなりません。ISMSの継続的改善は、必ずしもリスクを低減する活動ばかりでなく、組織の戦略や情報セキュリティ目的に関わる内容や、インシデントや事象の報告を通じて透明性を確保するなど、さまざまな改善の可能性が存在します。 |
| 【期待される対応】”Continual improvement”のチャンスの逃さないことが大切です。 |

**○４－２　附属書A　管理目的及び管理策**

|  |
| --- |
| **A.5　情報セキュリティのための方針群** |
| A.5.1 情報セキュリティのための管理の方向性 | 改訂の影響：小 |
| 目的：情報セキュリティに関する管理の方向性と支持を、事業上の要求事項、関連する法令・規制に従って提示するため。 |
| A.5.1.1旧：A.5.1.1 | 情報セキュリティのための方針群 | 【管理策意訳】情報セキュリティのための方針群を定義し、管理者の承認をもって発行し、従業員及び関連する外部関係者に伝える。 | 【解説】情報セキュリティ基本方針文書でなく、方針（群）と複数形に変わりました。その意図は、固有のパフォーマンスについて情報セキュリティのマネジメントの方向性を定められた方針文書をA.5.1の管理策として定めたからです。従って、承認についても、各方針に責任を有する管理者が行うこととされています。以下に付属書に書かれている方針群を例示します。例）「モバイル機器の方針」、「暗号による管理策の利用方針」、「クリアデスク・クリアスクリーン方針」、「情報転送の方針」、「セキュリティに配慮した開発のための方針」、「供給者関係のための情報セキュリティの方針」等 |
| A.5.1.2旧：A.5.1.2 | 情報セキュリティのための方針群のレビュー | 【管理策意訳】情報セキュリティのための方針群は、あらかじめ定められた間隔で、又は重大な変化が生じた場合に、それが適切で、妥当で且つ有効であることを継続するためにレビューする。 |

|  |
| --- |
| **A.6　情報セキュリティのための組織** |
| A.6.1 内部組織  | 改訂の影響：中 |
| 目的：情報セキュリティの実施、運用を開始し、管理するための管理上の枠組みを組織内に確立するため。 |
| A.6.1.1旧：A.6.1.3 | 情報セキュリティの役割及び責任 | 【管理策意訳】全ての情報セキュリティの責任を定め、割り当てること。 | 【解説】2005年版からの構成の変化：* 旧「A.6.1.1 情報セキュリティに対する経営陣の責任」→**削除**
* **「A.6.1.1 情報セキュリティの役割と責任」**←旧「A.8.1.1 役割及び責任」と旧「A.6.1.3　情報セキュリティ責任の割当て」を統合
* 旧「A.6.1.2 情報セキュリティの調整」→**削除**
* A.6.2（特に「A.6.2.3 第三者との契約におけるセキュリティ」）→「A.15 供給者関係」へ移動
* **「A.6.1.2　職務の分離」**←旧「A.10.1.3　職務の分離」から移動
* **「A.6.1.5　プロジェクトマネジメトにおける情報セキュリティ」新規追加**

改訂版の「A.6　情報セキュリティのための組織」は、組織のマネジメントが及ぶ範囲の管理策として、A.6.1の内部組織のみとし、2005年版のA.6.2に有った外部組織に当たる部分は改訂版のA.15に移動されています。内容については、改訂版の「A.6.1.1 情報セキュリティの役割と責任」に、2005年版の「A.6.1.3 情報セキュリティ責任の割当て」と「A.8.1.1 役割及び責任」が統合され“組織”に関わる管理としてまとまりました。改訂版では、「A.6.1.2　職務の分離」が2005年版のA.10.1.3から移動になりました。また、改訂版では、新たに内部組織の対象としてプロジェクト活動を含め、「A.6.1.5　プロジェクトマネジメトにおける情報セキュリティ」を新たに加え再構成されています。【理解のポイント】「A.6.1.2　職務の分離」では、例えば、情報セキュリティリスクを保有している立場の方とそのリスクを監視する立場の方と言うように、役割を分離することによってリスクやリスクの顕在化の早期発見などの効果を期待したものです。 |
| A.6.1.2旧：A.10.1.3 | 職務の分離 | 【管理策意訳】立場が異なる職務や責任範囲は、組織の資産に対する許可されていない、又は、意図していない変更や不正使用される危険性があるため、職務を分離する。 |
| A.6.1.3旧：A.6.1.6 | 関係当局との連絡 | 【管理策意訳】関係当局との適切な連絡体制を維持する。 |
| A.6.1.4旧：A.6.1.7 | 専門組織との連絡 | 【管理策意訳】情報セキュリティに関する研究会又は専門的なセキュリティ会議、協会・団体との適切な連絡体制を維持する。 |
| A.6.1.5旧：N/A | プロジェクトマネジメトにおける情報セキュリティ | 【管理策意訳】プロジェク卜の種類にかかわらず、プロジェクトマネジメントにおいて、情報セキュリティに取り組む。 |
| A.6.2 モバイル機器及びテレワーキング | 改訂の影響：小 |
| 目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。 |
| A.6.2.1旧：A.11.7.1 | モバイル機器の方針 | 【管理策意訳】モバイル機器を使用することによって生じるリスクを管理するために、方針及び方針を支援するセキュリティ対策を取る。 | 【解説】2005年版からの構成の変化：* **「A.6.2　モバイル機器及びテレワーキング」**←旧「A.11.7　モバイルコンピューティング及びテレワーキン」から移動

【理解のポイント】A.6.2.1のモバイル機器の利用とは、移動中又は外出先でモバイル機器を利用することであり、ノートPCのみならず、スマートフォン、その他携帯端末の利用を意図されています。また、A.6.2.2のテレワーキングとは、要員が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り、組織が事業上許可したSOHO（small office home office）や臨時事務所なども含まれます。PCを自宅に持ち帰り作業をする際は、自宅も外出先の一つととらえ「A.6.2.1　モバイル機器の利用」を適用します。 |
| A.6.2.2旧：A.11.7.2 | テレワーキング | 【管理策意訳】テレワーキングの現場でアクセスされ、処理され、保存される情報を保護するために、方針及び方針を支援するセキュリティ対策を取る。 |

|  |
| --- |
| **A.7　人的資源のセキュリティ** |
| A.7.1 雇用前 | 改訂の影響：小 |
| 目的：従業員及び契約相手がその責任を理解し、役割を確実にするため。 |
| A.7.1.1旧：A.8.1.2 | 選考 | 【管理策意訳】全ての従業員の選考対象者について、経歴などの確認は、関連する法規制及び倫理を踏まえて行うこと。また、この確認は、事業上の要求事項、アクセスさせる情報の分類、認識されたリスクに応じて行うこと。 | 【解説】2005年版からの構成の変化：* 旧A.8→**A.7に項番変更**
* 旧「A.8.1.1 役割及び責任」→「A.6.1.1 情報セキュリティの役割と責任」に移動し統合
* 旧「第三者の利用者」→**人的資源から除外（下記参照）**

改訂版の「A.7 人的資源のセキュリティ」は、従業員等の個人について雇用前、雇用期間中、雇用の終了又は変更における管理策を示し、2005年版のA.8.1.1に有った内部組織の役割と責任は、改訂版のA.6に整理されています。また、2005年版では、人的資源のセキュリティの人的資源を、人間として扱い「第三者の利用者」※を含めていましたが、「第三者の利用者」は、組織が管理可能な人的資源ではなく、「雇用前」「雇用期間中」「雇用の終了又は変更」の概念も適用できないため、除外され従業員と契約相手（派遣社員、業務委託）に限定されています。※）第三者の利用者：組織への一般来訪者、組織が開設するウェブサイトを利用する個人 |
| A.7.1.2旧：A.8.1.3 | 雇用条件 | 【管理策意訳】従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任と組織の責任を記載する。 |
| A.7.2 雇用期間中 | 改訂の影響：小 |
| 目的：従業員及び契約相手が、情報セキュリティの責任を認識し、且つ、その責任を全うすることを確実にするため。 |
| A.7.2.1旧：A.8.2.1 | 経営陣の責任 | 【管理策意訳】経営陣は、組織が確立した方針及び手順に従った情報セキュリティを適用させることを、全従業員及び契約相手に要求する。 | 【解説】2005年版からの構成の変化：* 旧A.8→**A.7に項番変更**
* 「第三者の利用者」→**人的資源から除外（A.7.1参照）**
 |
| A.7.2.2旧：A.8.2.2 | 情報セキュリティの自覚、教育及び訓練 | 【管理策意訳】組織の全従業員及び、関係する場合は、契約相手も、職務に関連する組織の方針及び手順についての自覚を即す教育・訓練を受け、定期的な啓発を即す。 |
| A.7.2.3旧：A.8.2.3 | 懲戒手続 | 【管理策意訳】情報セキュリティ違反を犯した従業員に対して、処置を行うための正式、且つ周知された懲戒手続を備える。 |
| A.7.3 雇用の終了及び変更 | 改訂の影響：小 |
| 目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。 |
| A.7.3.1旧：A.8.3.1 | 雇用の終了又は変更に関する責任 | 【管理策意訳】雇用の終了又は変更に際しては、引き続き、有効な情報セキュリティに関する責任と義務を定め、対象者となる従業員又は契約相手に伝達し、適用する。 | 【解説】2005年版からの構成の変化：* 旧A.8→**A.7に項番変更**
* 旧「A.8.3.2　資産の返却」→「A.8.1.4　資産の返却」に移動
* 旧「A.8.3.3 アクセス権の削除」→「A.9.2.6 アクセス権の削除又は修正」に移動

2005年版の「A.8.3.2　資産の返却」は、雇用の終了又は変更時の管理策として構成されていましたが、改訂版では、資産に関わる管理を優先し、「A.8　資産の管理」の「A.8.1　資産に対する責任」に移されています。また、「A.8.3.3 アクセス権の削除」も同様の考え方で「9 アクセス制御」の「A.9.2 利用者アクセスの管理」に移されています。 |

|  |
| --- |
| **A.8　資産の管理** |
| A.8.1 資産に対する責任 | 改訂の影響：小 |
| 目的：組織の資産を特定し、適切な保護の責任を定めるため。 |
| A.8.1.1旧：A.7.1.1 | 資産目録 | 【管理策意訳】情報及び情報処理施設に関連する資産を特定する。また、これらの資産の目録を作成し、維持する。 | 【解説】2005年版からの構成の変化：* 旧A.7＆旧A.10→**A.8に項番変更**
* **「A.8.1.4　資産の返却」**←旧「A.8.3.2　資産の返却」から移動

2005年版の「A.8.3.2　資産の返却」は、雇用の終了又は変更時の管理策として構成されていましたが、改訂版では、資産に関わる管理を優先し、「A.8　資産の管理」の「A.8.1　資産に対する責任」に移され「A.8.1.4　資産の返却」として再構築されています。【理解のポイント】改訂版では、情報セキュリティリスクアセスメントの際に、資産ベースに細かいアプローチの規制が簡素化されたこと（規格本文6.1.2項参照）をお伝えしましたが、情報セキュリティの対策を施す対象を知るために不可欠な管理策として、資産（情報資産）を把握することは、必要です。特に、A.8.1.2で資産の“オーナーシップを持たせること”は、114項の管理策の中でも5本の指に入るくらい重要な管理策です。 |
| A.8.1.2旧：A.7.1.2 | 資産の管理責任（オーナーシップ） | 【管理策意訳】目録で維持される資産は、オーナーシップを持たせる。 |
| A.8.1.3旧：A.7.1.3 | 資産利用の許容範囲 | 【管理策意訳】情報や情報処理施設及びそれらに関わる資産の利用を許可する範囲を特定し、規則を文書化し、実施する。 |
| A.8.1.4旧：A.8.3.2 | 資産の返却 | 【管理策意訳】全従業員及び外部の利用者は、雇用、契約又は合意が終了した時点で、自らが所有する組織の資産を全て返却する。 |
| A.8.2 情報の分類 | 改訂の影響：小 |
| 目的：組織に対する情報の重要性に応じて、情報を適切なレベル分けの下で保護を確実にするため。 |
| A.8.2.1旧：A.7.2.1 | 情報の分類 | 【管理策意訳】法的要求事項、情報の価値、重要性、及び許可されていない開示や変更に対して、取扱いを慎重にする必要性の観点から情報を分類する。 | 【解説】2005年版からの構成の変化：* 旧A.7＆旧A.10→**A.8に項番変更**
* **「A.8.2.2 情報のラベル付け」、「A.8.2.3 資産の取扱い」**←旧「A.7.2.2　情報のラベル付け及び取扱い」を分割

【理解のポイント】2005年度版「A.7.2.2　情報のラベル付け及び取扱い」を二つに分割し、「A.8.2.2 情報のラベル付け」「A.8.2.3 資産の取扱い」とされています。これは、A.8.2.1で分類された情報の次の管理の行き先が、“ラベル付け”になるものと、“ラベル付け”を経ずに“取扱いに関する手順”を定めるものとに分かれることを示唆しています。 |
| A.8.2.2旧：A.7.2.2 | 情報のラベル付け | 【管理策意訳】情報のラベル付けに関する一連の手順は、組織が採用した“情報の分類”の体系に従って策定し、実施する。 |
| A.8.2.3旧：A.7.2.2 | 資産の取扱い | 【管理策意訳】資産の取扱いに関する手順は、組織が採用した“情報の分類”の体系に従って策定し、実施する。 |
| A.8.3 媒体の取扱い | 改訂の影響：小 |
| 目的：媒体に保存された情報の許可されていない開示、変更、除去又は破壊を防止するため。 |
| A.8.3.1旧：A.10.7.1 | 取り外し可能な媒体の管理 | 【管理策意訳】組織が採用した情報の分類体系に従って、取り外し可能な媒体の管理手順を実施する。 | 【解説】2005年版からの構成の変化：* 旧A.7＆旧A.10→**A.8に項番変更**
* **「A.8.3.3　物理的媒体の輸送」新規追加**

2005年版の「A.10.7.1　取出し可能な媒体の管理」と「A.10.7.2　媒体の処分」に「A.8.3.3　物理的媒体の輸送」の管理策を新たに加え、「A.8.3　媒体の取扱い」として再構築されています。 |
| A.8.3.2旧：A.10.7.2 | 媒体の処分 | 【管理策意訳】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、処分する。 |
| A.8.3.3旧：N/A | 物理的媒体の輸送 | 【管理策意訳】情報を格納した媒体は、輸送の途中の、不正アクセス、不正使用、破損から保護する。 |

|  |
| --- |
| **A.9　アクセス制御** |
| A.9.1 アクセス制御に対する業務上の要求事項 | 改訂の影響：やや大 |
| 目的：情報及び情報処理施設へのアクセスを制限するため。 |
| A.9.1.1旧：A.11.1.1 | アクセス制御方針 | 【管理策意訳】アクセス制御方針は、業務上、及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。 | 【解説】2005年版からの構成の変化：* 旧A.11→**A.9に項番変更**
* 旧「A.11.4.2 外部から接続する利用者の認証」→**削除**
* 旧「A.11.4.3 ネットワークにおける装置の識別」→**削除**
* 旧「A.11.4.4 遠隔診断用及び環境設定用ポートの保護」→**削除**
* 旧「A.11.4.6 ネットワークの接続制御」→**削除**
* 旧「A.11.4.7 ネットワークのルーティング制御」→**削除**

2005年版の「A.11.4.1　ネットワークサービスの利用についての方針」を改訂版の「A.9.1　アクセス制御に対する業務上の要求事項」に統合し再構築されています。その際、2005年版の「A.11.4.2 外部から接続する利用者の認証」、「A.11.4.3 ネットワークにおける装置の識別」、「A.11.4.4 遠隔診断用及び環境設定用ポートの保護」、「A.11.4.6 ネットワークの接続制御」、「A.11.4.7 ネットワークのルーティング制御」の詳細な管理策は、技術的事項を減らす改訂方針のため、削除されました。 |
| A.9.1.2旧：A.11.4.1 | ネットワーク及びネットワークサービスへのアクセス | 【管理策意訳】ネットワーク及びネットワークサービスへのアクセスは、利用することを特別に許可した利用者にのみ提供する。 |

|  |  |
| --- | --- |
| A.9.2 利用者アクセスの管理 | 改訂の影響：小 |
| 目的：システム及びサービスへの許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.9.2.1旧：A.11.2.1 | 利用者登録及び登録抹消 | 【管理策意訳】アクセス権を付与するために、正式な利用者登録と登録抹消のプロセスを実施する。 | 【解説】2005年版からの構成の変化：* 旧A.11→**A.9に項番変更**
* 「**秘密認証情報」（A.9.2.4）**←旧「パスワード」から用語変更
* **「A.9.2.6 アクセス権の削除又は修正」**←旧「A.8.3.3 アクセス権の削除」から移動
* **「A.9.2.2　利用者アクセスの提供（プロビジョニング）」新規追加**

2005年版の「A.11.2.3 利用者パスワードの管理」は、「パスワード」と言う単語を秘密鍵、ワンタイム・パスワードなどの、パスワード以外の手段も含まれるように一般化し、改訂版では「A.9.2.4 利用者の秘密認証情報の管理」とされています。※パスワード→秘密認証情報（secret authentication information）2005年版の「A.8.3.3 アクセス権の削除」は、改訂版の「9 アクセス制御」の「A.9.2 利用者アクセスの管理」に移され、「A.9.2.6 アクセス権の削除又は修正」として再構築されています。【理解のポイント】「A.9.2.2　利用者アクセスの提供（プロビジョニング）」は、改訂版で新たに追加された項目ですが、クラウドなど昨今のIT技術やユーザのニーズの変化を考慮したものと思われます。プロビジョニングと記されていることから、ユーザのニーズに応じたサービス提供を考え、需要予想を立てることや、ユーザからの申し込みを受け付けた後、即座にサービス提供ができるよう、リソースを計画的に調達し、アクセス権について、割り当てや無効化の迅速化を図るために備えることで、システムの可用性を高めることを意図していることが伺えます。「A.9.2.5　利用者アクセス権のレビュー」では、資産の管理責任者（オーナー）と言う表現をしていますが、ここで言う資産は、目的に記されている通り、“システム及びサービス”を示すものと考えてよいでしょう。 |
| A.9.2.2旧：N/A | 利用者アクセスの提供（プロビジョニング） | 【管理策意訳】全ての利用者のタイプについて、利用者の要求に迅速に対応するために、全てのシステム・サービスへのアクセス権を割り当て又は無効化するための、正式な利用者アクセスの提供（プロビジョニング）プロセスを実施する。 |
| A.9.2.3旧：A.11.2.2 | 特権的なアクセス権の管理 | 【管理策意訳】特権的な利用者のアクセス権の付与及び利用は、制限し、管理する。 |
| A.9.2.4旧：A.11.2.3 | 利用者の秘密認証情報の管理 | 【管理策意訳】秘密認証情報の付与は、正式な管理プロセスによって管理する。 |
| A.9.2.5旧：A.11.2.4 | 利用者アクセス権のレビュー | 【管理策意訳】資産の管理責任者（オーナー）は、利用者のアクセス権を定められた間隔でレビューする。 |
| A.9.2.6旧：A.8.3.3 | アクセス権の削除又は修正 | 【管理策意訳】全従業員及び外部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、契約又は合意が終了した時に、削除し、または、変更に合わせて修正する。 |

|  |  |
| --- | --- |
| A.9.3 利用者の責任 | 改訂の影響：小 |
| 目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。 |
| A.9.3.1旧：A.11.3.1 | 秘密認証情報の利用 | 【管理策意訳】秘密認証情報の利用に際しては、組織の慣行に従うことを、利用者に要求する。 | 【解説】2005年版からの構成の変化：* 旧A.11→**A.9に項番変更**
* 「**秘密認証情報」（A.9.3.1）**←旧「パスワード」から用語変更

2005年版の「A.11.3.1 パスワードの利用」は、「パスワード」と言う単語を秘密鍵、ワンタイム・パスワードなどの、パスワード以外の手段も含まれるように一般化し、改訂版では「A.9.3.1 秘密認証情報の利用」とされています。※パスワード→秘密認証情報（secret authentication information） |

|  |  |
| --- | --- |
| A.9.4 システム及び業務用ソフトウェアのアクセス制御 | 改訂の影響：小 |
| 目的：システム及びアプリケーションへの、許可されていないアクセスを防止するため。 |
| A.9.4.1旧：A.11.6.1 | 情報へのアクセス制限 | 【管理策意訳】情報及びアプリケーションシステムへのアクセスは、アクセス制御方針に従って、制限する。 | 【解説】2005年版からの構成の変化：* 旧A.11→**A.9に項番変更**
* **A.9.4 システム及び業務用ソフトウェアのアクセス制御**←旧「A.11.5 オペレーティングシステムのアクセス制御」と旧「A.11.6 業務用ソフトウェア及び情報のアクセス制御」を統合
* 旧「A.11.5.5 セッションのタイムアウト」→**削除**
* 旧「A.11.5.6 接続時間の制限」→**削除**
* **「A.9.4.5　プログラムソースコードへのアクセス制御」**←旧「A.12.4.3　プログラムソースコードへのアクセス制御」から移動

2005年版の「A.11.5 オペレーティングシステムのアクセス制御」の「A.11.5.1 セキュリティに配慮したログオン手順」と「A.11.5.3 パスワード管理システム」及び「A.11.6 業務用ソフトウェア及び情報のアクセス制御」の「A.11.6.1 情報へのアクセス制限」は、システムとアプリケーションに共通に適用すべきものであることから、改訂版では統合し、さらに、「A.12.4.3　プログラムソースコードへのアクセス制御」を加え、「9.4 システム及びアプリケーションのアクセス制御」として再構築されています。「A.11.5.5 セッションのタイムアウト」と「A.11.5.6 接続時間の制限」は、分類から削除されています。 |
| A.9.4.2旧：A.11.5.1 | セキュリティに配慮したログオン手順 | 【管理策意訳】アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。 |
| A.9.4.3旧：A.11.5.3 | パスワード管理システム | 【管理策意訳】パスワード管理システムは、インタラクティブ（対話式）で且つ、良質なパスワードを確実にする。 |
| A.9.4.4旧：A.11.5.4 | 特権的なユーティリティプログラムの使用 | 【管理策意訳】システム及びアプリケーションによる制御を無効にすることができるユーティリティプログラムは、使用を制限し、厳しく管理する。 |
| A.9.4.5旧：A.12.4.3 | プログラムソースコードへのアクセス制御 | 【管理策意訳】プログラムソースコードへのアクセスは、制限する。 |

|  |
| --- |
| **A.10　暗号** |
| A.10.1 暗号による管理策 | 改訂の影響：小 |
| 目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切且つ有効な利用を確実にするため。 |
| A.10.1.1旧：A.12.3.1 | 暗号による管理策の利用方針 | 【管理策意訳】情報を保護するための暗号利用に関する方針を策定し、実施する。 | 【解説】2005年版からの構成の変化：* **「A.10　暗号」**←旧「A.12.3 暗号による管理策」から独立項目に昇格

2005年版の「A.12.3 暗号による管理策」は、情報システムの運用と開発の両面に関係することから、一つの独立した箇条とされています。 |
| A.10.1.2旧：A.12.3.2 | 鍵管理 | 【管理策意訳】暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全般にわたって実施する。 |

|  |
| --- |
| **A.11　物理的及び環境的セキュリティ** |
| A.11.1 セキュリティを保つべき領域 | 改訂の影響：小 |
| 目的：組織の情報及び情報処理施設に対する許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.11.1.1旧：A.9.1.1 | 物理的セキュリティ境界 | 【管理策意訳】物理的なセキュリティの境界を定め、取扱いが慎重な、又は重要な情報や情報処理施設を有する領域を保護するために用いること。 | 【解説】2005年版からの構成の変化：* 旧A.9→**A.11に項番変更**

内容については、2005年版から大きな変更はありません。 |
| A.11.1.2旧：A.9.1.2 | 物理的入退管理策 | 【管理策意訳】セキュリティを保つべき領域は、許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、適切な入退管理によって保護する。 |
| A.11.1.3旧：A.9.1.3 | オフィス、部屋及び施設のセキュリティ | 【管理策意訳】オフィス、部屋及び施設に対する物理的なセキュリティを設計し、適用する。 |
| A.11.1.4旧：A.9.1.4 | 外部及び環境の脅威からの保護 | 【管理策意訳】自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。 |
| A.11.1.5旧：A.9.1.5 | セキュリティを保つべき領域での作業 | 【管理策意訳】セキュリティを保つべき領域での作業に関する手順を設計し、適用する。 |
| A.11.1.6旧：A.9.1.6 | 受渡場所 | 【管理策意訳】荷物の受渡場所のように、立寄り場所や、許可されていない者が施設に立ち入る場所は、管理する。また、可能な場合には、許可されていないアクセスを避けるために、情報処理施設をそれらの場所から隔離する。 |
| A.11.2 装置 | 改訂の影響：小 |
| 目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。 |
| A.11.2.1旧：A.9.2.1 | 装置の設置及び保護 | 【管理策意訳】装置は、環境上の脅威や、災害のリスク、許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、保護する。 | 【解説】2005年版からの構成の変化：* 旧A.9→**A.11に項番変更**
* **「A.11.2.8 無人状態にある装置」**←旧「A.11.3.2 無人状態にある装置」から移動
* **「A.11.2.9 クリアデスク・クリアスクリーン方針」**←旧「A.11.3.3　クリアデスク・クリアスクリーン方針」から移動

2005年版のアクセス制御の利用者の責任に位置付けられていた「A.11.3.2　 無人状態にある装置」と「A.11.3.3　クリアデスク・クリアスクリーン方針」は、改訂版では物理的管理とされ、「A.11　物理的及び環境的セキュリティ」として再構築されています。【理解のポイント】A.11.2.2のサポートユーティリティとは、例えば、電気、給水、排水、換気、空調などの情報システムや装置、設備の適性稼働を支えるものを指すと考えてよいでしょう。 |
| A.11.2.2旧：A.9.2.2 | サポートユーティリティ | 【管理策意訳】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する。 |
| A.11.2.3旧：A.9.2.3 | ケーブル配線のセキュリティ | 【管理策意訳】データを転送する又は情報サービスをサポートする通信ケーブルや電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 |
| A.11.2.4旧：A.9.2.4 | 装置の保守 | 【管理策意訳】装置は、可用性や完全性を継続的に維持することを確実にするために、正しく保守する。 |
| A.11.2.5旧：A.9.2.7 | 資産の移動 | 【管理策意訳】装置、情報又はソフトウェアは、事前の許可なしに構外へ持ち出さないこと。 |
| A.11.2.6旧：A.9.2.5 | 構外にある装置及び資産のセキュリティ | 【管理策意訳】構外にある資産に対しては、構内での作業とは異なる、構外での作業に伴うリスクを考慮に入れて、セキュリティを適用する。 |
| A.11.2.7旧：A.9.2.6 | 装置のセキュリティを保った処分又は再利用 | 【管理策意訳】記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての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、又はセキュリティを保って上書きしていることを確実にするために、検証する。 |
| A.11.2.8旧：A.11.3.2 | 無人状態にある装置 | 【管理策意訳】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する。 |
| A.11.2.9旧：A.11.3.3 | クリアデスク・クリアスクリーン方針 | 【管理策意訳】書類や取外し可能な記憶媒体に対するクリアデスク方針や情報処理設備に対するクリアスクリーン方針を適用する。 |

|  |
| --- |
| **A.12　運用のセキュリティ** |
| A.12.1 運用の手順及び責任 | 改訂の影響：小 |
| 目的：情報処理設備の正確且つセキュリティを保った運用を確実にするため。 |
| A.12.1.1旧：A.10.1.1 | 操作手順書 | 【管理策意訳】（情報処理設備の）操作手順は、文書化し、必要とする全ての利用者が利用可能にする。 | 【解説】2005年版からの構成の変化：* 旧A.10→**A.12に項番変更**
* 旧「A.10.2 第三者が提供するサービスの管理」→「15 供給者管理」に移動

2005年版の「A.10 通信及び運用管理」から、運用に関する管理策を取り出し、「A.12　運用のセキュリティ」として一つの箇条に再構築されています。「A.10.2 第三者が提供するサービスの管理」は、委託の管理策として「15 供給者管理」にまとめられ、再構築されています。 |
| A.12.1.2旧：A.10.1.2 | 変更管理 | 【管理策意訳】情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を、管理する。 |
| A12.1.3旧：A.10.3.1 | 容量・能力の管理 | 【管理策意訳】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、また、将来必要となる容量・能力を予測する。 |
| A.12.1.4旧：A.10.1.4 | 開発環境、試験環境及び運用環境の分離 | 【管理策意訳】開発環境、試験環境及び運用環境は、運用環境への許可されていないアクセスや変更によるリスクを低減するために、分離する。 |
| A.12.2 悪意のあるソフトウェア（malware）からの保護 | 改訂の影響：小 |
| 目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。 |
| A.12.2.1旧：A.10.4.1 | マルウェアに対する管理策 | 【管理策意訳】マルウェアから保護するために、利用者に自覚させることと併せて、検出、予防、回復のための管理を実施する。 | 【解説】2005年版からの構成の変化：* 旧A.10→**A.12に項番変更**
* **「マルウェア（malware）」（A.12.2.1）**←旧「malicious code」から用語変更
* 「A.10.4.2 モバイルコードに対する管理策」→**削除**

2005年版の「A.10.4.2 モバイルコードに対する管理策」が削除され「A.12.2.1　マルウェアに対する管理策」として再構築されています。マルウェア：コンピューターの動作をおかしくしたり、データを破壊したりといった不正な目的のために作成されたプログラム。 |
| A.12.3 バックアップ | 改訂の影響：小 |
| 目的：データの消失から保護するため。 |
| A.12.3.1旧：A.10.5.1 | 情報のバックアップ | 【管理策意訳】情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。 | 【解説】2005年版からの構成の変化：* 旧A.10→**A.12に項番変更**

内容については、2005年版から大きな変更はありません。 |
| A.12.4 ログ取得及び監視 | 改訂の影響：小 |
| 目的：イベントを記録し、証拠を作成するため。 |
| A.12.4.1旧：A.10.10.1 | イベントログ取得 | 【管理策意訳】利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。 | 【解説】2005年版からの構成の変化：* 旧A.10→**A.12に項番変更**
* 旧「A.10.10.2 システム使用状況の監視」→**削除**
* 旧「A.10.10.5 障害のログ取得」→**削除**

2005年版の「A.10.10.2 システム使用状況の監視」と「A.10.10.5 障害のログ取得」は削除され、改訂版では「A.12.4.1　イベントログ取得」に含めて再構築されています。 |
| A.12.4.2旧：A.10.10.3 | ログ情報の保護 | 【管理策意訳】ログ機能及びログ情報は、改ざん及び許可されていないアクセスから保護する。 |
| A.12.4.3旧：A.10.10.4 | 実務管理者及び運用担当者の作業ログ | 【管理策意訳】システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。 |
| A.12.4.4旧：A.10.10.6 | クロックの同期 | 【管理策意訳】組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、基となる単一の時刻に同期させる。 |
| A.12.5 運用ソフトウェアの管理 | 改訂の影響：小 |
| 目的：運用システムの完全性を確実にするため。 |
| A.12.5.1旧：A.12.4.1 | 運用システムに関わるソフトウェアの導入 | 【管理策意訳】運用システムに関わるソフトウェアの導入を管理するための手順を実施する。 | 【解説】2005年版からの構成の変化：* **「A.12.5.1　運用システムに関わるソフトウェアの導入」**←旧「A.12.4.1 運用ソフトウェアの管理」から移動

2005年版の「A.12　情報システムの取得，開発及び保守」に有った「A.12.4.1 運用ソフトウェアの管理」は、目的を“運用システムの完全性”に変え、改訂版では「A.12.5 運用ソフトウェアの管理」に移動され、再構築されています。【理解のポイント】A.12.5.1の“運用システムに関わるソフトウェアの導入を管理するための手順”については、漠然としていて、ピンとこない内容ですが、変更管理やリリース管理、構成管理をイメージすると解りやすいでしょう。 |
| A.12.6 技術的な脆弱性の管理 | 改訂の影響：中 |
| 目的：技術的な脆弱性の悪用を防止するため。 |
| A.12.6.1旧：A.12.6.1 | 技術的な脆弱性の管理 | 【管理策意訳】利用中の情報システムの技術的な脆弱性に関する情報は、時機を失せずに獲得する。また、そのような脆弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。 | 【解説】2005年版からの構成の変化：* **「A.12.6.1 技術的脆弱性の管理」**←旧「A.12.6.1 技術的脆弱性の管理」から移動
* **「A.12.6.2　ソフトウェアのインストールの制限」新規追加**

2005年版の「A.12.6.1 技術的脆弱性の管理」は、目的を運用時のリスクとして技術的脆弱性の悪用をとらえ、「A.12　運用のセキュリティ」の「A.12.6 技術的脆弱性管理」の項目として再構築されています。また、「A.12.6.2　ソフトウェアのインストールの制限」を新たに加え、再構築されています。ソフトウェアを制限なしにインストールされるリスクは、これまで、ピッタリでは無いにしても、比較的近い管理策として「A.12.4.1 運用ソフトウェアの管理」に含めていた組織は多いと思います。改訂版では、「A.12.6　技術的脆弱性管理」の目的の中で、安全なソフトウェアのみインストールする管理策として「A.12.6.2　ソフトウェアのインストールの制限」を運用の管理策に加えました。 |
| A.12.6.2旧：N/A | ソフトウェアのインストールの制限 | 【管理策意訳】利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。 |
| A.12.7 情報システムの監査に対する管理策 | 改訂の影響：小 |
| 目的：運用システムに対する監査活動の影響を最小限にするため。 |
| A.12.7.1旧：A.15.3.1 | 情報システムの監査に対する管理策 | 【管理策意訳】運用システムの検証に必要な監査は、その要求事項及び監査活動が業務プロセスの中断を最小限に抑えるように慎重に計画し、合意する。 | 【解説】2005年版からの構成の変化：* **「A.12.7.1 情報システムの監査に対する管理策」**←旧「A.15.3.1 情報システムの監査に対する管理策」から移動

2005年版の順守の中で扱われていた「A.15.3.1 情報システムの監査に対する管理策」は、監査活動の影響が運用システムの停止を招くなど、業務プロセスの可用性リスクを取り扱うものとして「A.15 順守」から「A.12　運用のセキュリティ」に移動されています。 |

|  |
| --- |
| **A.13　通信のセキュリティ** |
| A.13.1 ネットワークセキュリティ管理 | 改訂の影響：小 |
| 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情報処理施設の保護を確実にするため。 |
| A.13.1.1旧：A.10.6.1 | ネットワーク管理策 | 【管理策意訳】システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。 | 【解説】2005年版からの構成の変化：* 旧A.10→**A.13に項番変更**

2005年版の「A.10 通信及び運用管理」から、通信に関する管理策を取り出し、「A.13　通信のセキュリティ」として一つの箇条に再構築されています。 |
| A.13.1.2旧：A.10.6.2 | ネットワークサービスのセキュリティ | 【管理策意訳】全てのネットワークサービスについて、組織が提供しているか、外部委託しているかに関わらず、セキュリティ機能、サービスレベル及び管理上の要求事項を決定し、ネットワークサービス・アグリメント（合意書）に盛り込む。 |
| A.13.1.3旧：A.11.4.5 | ネットワークの領域分割 | 【管理策意訳】情報サービス、利用者、情報システムは、ネットワーク上でグループ毎に分割する。 |
| A.13.2 情報の転送 | 改訂の影響：小 |
| 目的：組織の内部で、或いは外部との間で転送された情報のセキュリティを維持するため。 |
| A.13.2.1旧：A.10.8.1 | 情報転送の方針及び手順 | 【管理策意訳】通信設備のタイプに関わらず、転送した情報を保護するために、正式な転送方針、手順及び管理を備える。 | 【解説】2005年版からの構成の変化：* 旧A.10→**A.13に項番変更**
* **「A.13.2.4　秘密保持契約又は守秘義務契約」**←旧「A.6.1.5 秘密保持契約」から移動

2005年版の「A.10.8 情報の交換」は、「情報の交換（exchange）」を、改訂版で「情報の転送（transfer）」に変え、通信上の管理策の色を濃くする意図が伺えます。ここで使われている転送（transfer）の意味は、情報を信号として一方の装置から他の装置へ移動させることを意味し、組織内での情報の移動や、組織外との情報の移動を考慮しセキュリティを維持することが意図されています。2005年版の内部組織の中で扱われていた「A.6.1.5 秘密保持契約」は、通信を保護するための規約として取り扱うものとして「A.6.1 内部組織」から「A.13　通信のセキュリティ」に目的を変え再構築されています。 |
| A.13.2.2旧：A.10.8.2 | 情報転送に関する合意 | 【管理策意訳】（情報の転送に関する）合意では、組織と外部関係者間のビジネス情報の安全な転送について取り扱う。 |
| A.13.2.3旧：A.10.8.3 | 電子的メッセージ通信 | 【管理策意訳】電子的なメッセージを発信する場合、そこに含まれた情報は、適切に保護する。 |
| A.13.2.4旧：A.6.1.5 | 秘密保持契約又は守秘義務契約 | 【管理策意訳】情報保護のために組織のニーズを反映した秘密保持契約又は守秘義務契約の要件を特定し、定期的にレビューし、文書化する。 |

|  |
| --- |
| **A.14　システムの取得、開発及び保守** |
| A.14.1 情報システムのセキュリティ要求事項 | 改訂の影響：小 |
| 目的：ライフサイクル全体にわたって、情報セキュリティが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。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。 |
| A.14.1.1旧：A.12.1.1 | 情報セキュリティ要求事項の分析及び仕様化 | 【管理策意訳】新しい情報システムの仕様や既存の情報システムの改善要求事項には、情報セキュリティに関する要求事項を含める。 | 【解説】2005年版からの構成の変化：* 旧A.12→**A.14に項番変更**
* **「A.14.1.2 公共ネットワーク上のアプリケーションサービスのセキュリティの考慮」**←旧「A.10.9.1 電子商取引」から移動
* **「A.14.1.3 アプリケーションサービスのトランザクションの保護」**←旧「A.10.9.2 オンライン取引」から移動

2005年版の「A.10.9 電子商取引サービス」の「A.10.9.1 電子商取引」と「A.10.9.2 オンライン取引」は、「電子商取引」という概念を、“公衆ネットワーク上のアプリケーションサービス”として一般化し「A.14.1.2 公共ネットワーク上のアプリケーションサービスのセキュリティの考慮」、「A.14.1.3 アプリケーションサービスのトランザクションの保護」の構成とされています。【理解のポイント】「A.14.1.2 公共ネットワーク上のアプリケーションサービスのセキュリティの考慮」と「A.14.1.3 アプリケーションサービスのトランザクションの保護」の管理策は、「A.14　システムの取得、開発及び保守」の項として扱うため、Webショップを利用し物品購買をする作業は対象にはなりません。社内の例えば財務サービスの開発の際に、他社が運営するASPサービスを組み込む場合には、「A.14.1.2 公共ネットワーク上のアプリケーションサービスのセキュリティの考慮」、「A.14.1.3 アプリケーションサービスのトランザクションの保護」と「A.15　供給者関係」とを併せて活用するとよいでしょう。 |
| A.14.1.2旧：A.10.9.1 | 公衆ネットワーク上のアプリケーションサービスのセキュリティ考慮 | 【管理策意訳】公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、や許可されていない開示・変更から保護する。 |
| A.14.1.3旧：A.10.9.2 | アプリケーションサービスのトランザクションの保護 | 【管理策意訳】アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。不完全な通信、誤った通信経路設定、許可されていないメッセージの変更、許可されていない開示、許可されていないメッセージの複製又は再生。 |
| A.14.2 開発及びサポートプロセスにおけるセキュリティ | 改訂の影響：中 |
| 目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。 |
| A.14.2.1旧：N/A | セキュリティに配慮した開発のための方針 | 【管理策意訳】ソフトウェアやシステムの開発規則は、組織内で確立し、開発に適用する。 | 【解説】2005年版からの構成の変化：* 旧A.12→**A.14に項番変更**
* **「A.14.2.1 セキュリティに配慮した開発の方針」新規追加**
* **「A.14.2.6 セキュリティに配慮した開発環境」新規追加**
* **「A.14.2.8 システムのセキュリティ試験」新規追加**
* **「A. 14.2.5 セキュリティに配慮したシステム開発の原則」**←旧「A. 12.2 業務用ソフトウェアでの正確な処理」から移動

システムの開発について、ライフサイクルの観点から管理策を整備・拡充し新たな管理策が追加されています。追加管理策：「A.14.2.1 セキュリティに配慮した開発の方針」、「A.14.2.6 セキュリティに配慮した開発環境」、「A.14.2.8 システムのセキュリティ試験」2005年版の「A. 12.2 業務用ソフトウェアでの正確な処理」は、セキュリティに配慮したシステムを構築するための原則として「A. 14.2.5 セキュリティに配慮したシステム開発の原則」に含めて、確立し、文書化し、維持し、適用することが意図されています。 |
| A.14.2.2旧：A.12.5.1 | システムの変更管理手順 | 【管理策意訳】開発のライフサイクルの中で発生するシステム変更は、正式な変更管理手順を用いて管理する。 |
| A.14.2.3旧：A.12.5.2 | オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー | 【管理策意訳】オペレーティングプラットフォー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、重要なアプリケーションについてレビューし、試験する。 |
| A.14.2.4旧：A.12.5.3 | パッケージソフトウェアの変更に対する制限 | 【管理策意訳】パッケージソフトウェアの改良は、極力避け、必要な変更だけに留める。又、全ての変更は、厳重に管理する。 |
| A.14.2.5旧：A. 12.2 | セキュリティに配慮したシステム構築の原則 | 【管理策意訳】安全なシステムを設計するための原則を定め、文書化し、維持し、全ての情報システムの実装に対して適用する。 |
| A.14.2.6旧：N/A | セキュリティに配慮した開発環境 | 【管理策意訳】組織は、全ての開発のライフサイクルをカバーするシステム開発とシステムインテグレーションの活動のために、安全な開発環境を構築して、適切に保護する。 |
| A.14.2.7旧：A.12.5.5 | 外部委託による開発 | 【管理策意訳】組織は、外部委託したシステム開発の活動を監督し、監視する。 |
| A.14.2.8旧：N/A | システムセキュリティの試験 | 【管理策意訳】セキュリティ機能の試験は、開発期間中に実施する。 |
| A.14.2.9旧：A.10.3.2 | システムの受入れ試験 | 【管理策意訳】新しい情報システム、アップグレード及び新しいバージョンのために、受入れ試験のプログラム及び関連する受け入れ基準を確立する。 |
| A.14.3 試験データ | 改訂の影響：小 |
| 目的：試験に用いるデータの保護を確実にするため。 |
| A.14.3.1旧：A.12.4.2 | 試験データの保護 | 【管理策意訳】試験データは、注意して選び、保護し、管理する。 | 【解説】2005年版からの構成の変化：* 旧A.12→**A.14に項番変更**

内容については、2005年版から大きな変更はありません。 |

|  |
| --- |
| **A.15　供給者関係** |
| A.15.1 供給者管理におけるセキュリティ | 改訂の影響：中 |
| 目的：供給者がアクセスできる組織の資産の保護を確実にするため。 |
| A.15.1.1旧：A.6.2.3 | 供給者関係のための情報セキュリティの方針 | 【管理策意訳】組織の資産に供給者がアクセスするリスクを軽減するために、情報セキュリティの要求事項について、供給者と合意し、文書化する。 | 【解説】2005年版からの構成の変化：* **「A.15.1　供給者管理におけるセキュリティ」**←旧「A.6.2.3 供給者との契約におけるセキュリティの考慮」を統合
* **「A.15.1.3　ICTサプライチェーン」新規追加**
* 旧「A.6.2.1　外部組織に関係したリスクの識別」→**削除**
* 旧「A.6.2.2　顧客対応におけるセキュリティ」→**削除**

2005年版の「A.6.2 外部組織」に含まれる「6.2.3 供給者との契約におけるセキュリティの考慮」は、「A.15 供給者管理」に統合され、「A.15.1　供給者管理におけるセキュリティ」として再構築されています。その過程で、「A.6.2.1　外部組織に関係したリスクの識別」と「A.6.2.2　顧客対応におけるセキュリティ」は、削除されています。また、「A.15.1.3　ICTサプライチェーン」では、情報通信技術（lCT）サービスに関わる供給者だけでなく製品のサプライチェーンに関わる内容が追加されています。 |
| A.15.1.2旧：A.6.2.3 | 供給者との合意に含まれるセキュリティの取り組み | 【管理策意訳】関連する全ての情報セキュリティ要求事項を確立し、組織の情報にアクセスし、処理し、それを保存し、通信を行う、又は組織の情報のためにITインフラを提供するなどの可能性を有する供給者と合意する。 |
| A.15.1.3旧：N/A | ICTサプライチェーン | 【管理策意訳】供給者との合意には、情報通信技術（lCT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めること。 |
| A.15.2 供給者が提供するサービスの管理 | 改訂の影響：小 |
| 目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。 |
| A.15.2.1旧：A.10.2.2 | 供給者のサービス提供の監視及びレビュー | 【管理策意訳】組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。 | 【解説】2005年版からの構成の変化：* **「A.15.2　供給者が提供するサービスの管理」**←旧「A.10.2　第三者が提供するサービスの管理」を統合

2005年版の「A.10 通信及び運用管理」に含まれる「A.10.2 第三者が提供するサービスの管理」は、「A.15 供給者管理」に統合され、「A.15.2　供給者が提供するサービスの管理」として再構築されています。その過程で、「A.10.2.1　第三者が提供するサービス」は、削除されています。 |
| A.15.2.2旧：A.10.2.3 | 供給者のサービス提供の変更に対する管理 | 【管理策意訳】現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む供給者によるサービス提供の変更は、ビジネス情報、システム及び関連プロセスの重要性やリスクの再評価の結果を考慮して、管理する。 |

|  |
| --- |
| **A.16　情報セキュリティインシデントの管理** |
| A.16.1 情報セキュリティインシデントの管理及びその改善 | 改訂の影響：小 |
| 目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。 |
| A.16.1.1旧：A.13.2.1 | 責任及び手順 | 【管理策意訳】情報セキュリティインシデントに対し、迅速で、効果的で整然とした対応を確実にするために、管理層の責任及び手順を確立する。 | 【解説】2005年版からの構成の変化：* 旧A.13→**A.16に項番変更**

2005年版の「A.13 情報セキュリティインシデントの管理」5個の管理策を継承し、さらに、1つの管理策「A.16.1.4　情報セキュリティ事象の評価及び決定」を加え情報セキュリティインシデントからの学習への過程が強化されています。 |
| A.16.1.2旧：A.13.1.1 | 情報セキュリティ事象の報告 | 【管理策意訳】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、できるだけ速やかに報告する。 |
| A.16.1.3旧：A.13.1.2 | 情報セキュリティ弱点の報告 | 【管理策意訳】システム又はサービスの中で発見した又は疑いがある情報セキュリティ上の弱点は、どのようなものでも記録し、報告するよう、組織の情報システム、サービスを利用する従業員、契約相手に要求する。 |
| A.16.1.4旧：N/A | 情報セキュリティ事象の評価及び決定 | 【管理策意訳】情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。 |
| A.16.1.5旧：A.13.2.1 | 情報セキュリティインシデントへの対応 | 【管理策意訳】情報セキュリティインシデントは、文書化した手順に従って対応する。 |
| A.16.1.6旧：A.13.2.2 | 情報セキュリティインシデントからの学習 | 【管理策意訳】情報セキュリティインシデントの分析や解決から得られた知識は、インシデントが将来起こる可能性又は、その影響を低減するために用いる。 |
| A.16.1.7旧：A.13.2.3 | 証拠の収集 | 【管理策意訳】組織は、証拠となり得る情報の特定、収集、取得、保存のための手順を定め、適用する。 |

|  |
| --- |
| **A.17　事業継続マネジメントにおける情報セキュリティの側面** |
| A.17.1 情報セキュリティ継続 | 改訂の影響：小 |
| 目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。 |
| A.17.1.1旧：A.14.1 | 情報セキュリティ継続の計画 | 【管理策意訳】組織は、困難な状況の下で（adverse situation） （例えば、危機又は災害）情報セキュリティ及び情報セキュリティマネジメントを継続するための要求事項を決定する。 | 【解説】2005年版からの構成の変化：* 旧A.14→**A.17に項番変更**

2005年版は、事業プロセスの保護と再開に重点が置かれ、これを支えるものとして、情報システムの継続的運用と回復がテーマになっていました。改訂版の「A.17.1 情報セキュリティ継続」では、 情報セキュリティ及び情報セキュリティマネジメントの継続と回復に主題が置かれ再構築されています。情報セキュリティリスクに対する管理策としてわかりやすくなり、事業とのかかわり合いは、本文の4章、5章、6章に譲った形になっています。 |
| A.17.1.2旧：A.14.1 | 情報セキュリティ継続の実施 | 【管理策意訳】組織は、困難な状況の下で情報セキュリティ継続に関する要求レベルを確実にするために、プロセス、手順及び管理策を定め、文書化し、実施し、維持する。 |
| A.17.1.3旧：A.14.1 | 情報セキュリティ継続の検証、レビュー及び評価 | 【管理策意訳】確立及び実施した情報セキュリティ継続のための管理が、困難な状況の下で妥当且つ有効であることを確実にするために、組織は、定められた間隔でこれらの管理を検証する。 |
| A.17.2 冗長性 | 改訂の影響：やや大 |
| 目的：情報処理施設の可用性を確実にするため。 |
| A.17.2.1旧：N/A | 情報処理施設の可用性 | 【管理策意訳】情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。 | 【解説】2005年版からの構成の変化：* **「A.17.2.1　情報処理施設の可用性」新規追加**

2005年版は、情報および情報処理施設の可用性に関係する管理策が体系的に見えにくいものでした。改訂版に新たに追加された「A.17.2.1　情報処理施設の可用性」によって、情報処理施設の可用性確保の対応を包括的に示しているものと思われます。情報処理施設の可用性確保は事業継続管理の一部でもあるため、本管理策をA.17に置いたものと思われます。 |

|  |
| --- |
| **A.18　順守** |
| A.18.1 情報セキュリティのレビュー | 改訂の影響：小 |
| 目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、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。 |
| A.18.1.1旧：A.15.1.1 | 適用法令及び契約上の要求事項の特定 | 【管理策意訳】各情報システム及び組織に関する法令、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を明確に定め、文書化し、最新に保つ。 | 【解説】2005年版からの構成の変化：* 旧A.15→**A.18に項番変更**
* 旧「A.15.1.5 情報処理施設の誤用防止」→**削除**

2005年版の「A.15.1.5 情報処理施設の誤用防止」が削除されているが、内容については、2005年版から大きな変更はありません。【理解のポイント】法規制違反が事業に及ぼす影響は計り知れないものがあります。情報セキュリティに関しては、インターネットにおける詐欺、プライパシーの保護、知的財産権の保護など、法律に抵触するリスクはきわめて重要です。また、法律に違反していると疑いをかけられたり、不正を受けたことで相手を訴えたりすることもあり、法律違反が訴訟に発展するリスクに対処する方法も考えておかなければなりません。いざ訴訟が起きた場合は、自らの正当性を立証する証拠が必要です。訴訟の原因が事象やインシデントの場合、その証拠を「A.16.1.7　証拠の収集」に基づいて収集し、「A.18.1.3　記録の保護」で記録を維持すると言うような管理目的同士の関係をうまく利用することが重要です。 |
| A.18.1.2旧：A.15.1.2 | 知的財産権 | 【管理策意訳】知的財産権及び登録商標が存在するソフトウェア製品の利用する場合、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実施する。 |
| A.18.1.3旧：A.15.1.3 | 記録の保護 | 【管理策意訳】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、改ざん、許可されていないアクセス及び公開から保護する。 |
| A.18.1.4旧：A.15.1.4 | プライパシー及び個人を特定できる情報の保護 | 【管理策意訳】プライパシー及び個人を特定できる情報の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にする。 |
| A.18.1.5旧：A.15.1.6 | 暗号化機能に対する規制 | 【管理策意訳】暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。 |
| A.18.2 法的及び契約上の要求事項の識別 | 改訂の影響：小 |
| 目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。 |
| A.18.2.1旧：A.6.1.8 | 情報セキュリティの独立したレビュー | 【管理策意訳】情報セキュリティ及びその実施の管理（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）に関する組織の取組みは、あらかじめ定められた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。 | 【解説】2005年版からの構成の変化：* 旧A.15→**A.18に項番変更**
* **「A.18.2.1　情報セキュリティの独立したレビュー」**←旧「A.6.1.8 情報セキュリティの独立したレビュー」から移動

2005年版では「A.6.1 内部組織」にあった「A.6.1.8 情報セキュリティの独立したレビュー」を、18.2.1に移動し、分かりやすくなりました。 |
| A.18.2.2旧：A.15.2.1 | 情報セキュリティのための方針群及び標準の順守 | 【管理策意訳】管理者（マネジャー）は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。 |
| A.18.2.3旧：A.15.2.2 | 技術的順守のレビュー | 【管理策意訳】情報システムは、組織の情報セキュリティのための方針群や基準の順守について、定期的にレビューする。 |

**2005年度版から削除された項目**

A.6.1.1　情報セキュリティに対する経営陣の責任

A.6.2.1　外部組織に関係したリスクの識別

A.6.2.2　顧客対応におけるセキュリティ

A.10.2.1　第三者が提供するサービス

A.10.4.2 モバイルコードに対する管理策

A.10.7.4 システム文書のセキュリティ

A.10.8.5 業務用情報システム

A.10.9.3 公開情報

A.10.10.2 システム使用状況の監視

A.10.10.5 障害のログ取得

A.11.4.2 外部から接続する利用者の認証

A.11.4.3 ネットワークにおける装置の識別

A.11.4.4 遠隔診断用及び環境設定用ポートの保護

A.11.4.6 ネットワークの接続制御

A.11.4.7 ネットワークのルーティング制御

A.11.5.2 利用者の識別及び認証

A.11.5.5 セッションのタイムアウト

A.11.5.6 接続時間の制限

A.12.2.1 入力データの妥当性

A.12.2.2 内部処理の管理

A.12.2.3 メッセージの完全性

A.12.2.4 出力データの妥当性確認

A.15.1.5 情報処理施設の不正使用防止

A.15.3.2 情報システムの監査ツールの保護

**５章　審査はどう変わる**

これまでの審査と大きく変わる要素は無いものの、管理策を網羅的に当たることを多少なりとも重視してきた審査アプローチについては、組織の目的に関連する課題や利害関係者の期待、ニーズを起点とした、リスクアプローチに変わることが予想されます。