

ISMS

情報セキュリティマネジメントシステム適合性評価制度

ISMS 認証基準 (Ver.2.0) (案)



平成 15 年 1 月 15 日



財団法人 日本情報処理開発協会

JIPDECの許可なく転載することを禁じます

本基準（ISMS 認証基準）は、情報セキュリティマネジメントシステム適合性評価制度において、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価するための認証基準である。本基準は、JIS X 5080:2002(国際規格 ISO/IEC 17799:2000 (Information technology -- Code of practice for information security management: 情報技術 - 情報セキュリティマネジメントの実践のための規範))及び英国規格 BS 7799-2:2002 (Information security management systems - Specification with guidance for use: 情報セキュリティマネジメントシステム - 仕様及び利用の手引)を参照し作成したものである。

また本基準は、時代に適合したものであり続けるために、情報セキュリティに関する国際標準のJIS 化の動向やJIS 化後の周知状況等を踏まえ、適宜見直し及び改訂されるものである。

(財)日本情報処理開発協会

目次

第0 序文	4
1 . 一般.....	4
2 . プロセスアプローチ	4
3 . 他のマネジメントシステムとの両立性	6
第1 適用範囲	7
1 . 一般.....	7
2 . 適用.....	7
第2 引用規格等	8
第3 定義	9
1 . 可用性 (availability)	9
2 . 機密性 (confidentiality)	9
3 . 情報セキュリティ (information security)	9
4 . 情報セキュリティマネジメントシステム ISMS (information security management system)	9
5 . 完全性 (integrity)	9
6 . リスク受容 (risk acceptance)	9
7 . リスク分析 (risk analysis)	9
8 . リスクアセスメント (risk assessment)	10
9 . リスク評価 (risk evaluation)	10
10 . リスクマネジメント (risk management)	10
11 . リスク対応 (risk treatment)	10
12 . 適用宣言書 (statement of applicability)	10
第4 情報セキュリティマネジメントシステム	11
1 . 一般要求事項	11
2 . ISMS の確立及び運営管理	11
3 . 文書化に関する要求事項	14
第5 経営陣の責任	17
1 . 経営陣のコミットメント	17
2 . 経営資源の運用管理	17

第6 マネジメントレビュー	19
1 . 一般.....	19
2 . マネジメントレビューへのインプット.....	19
3 . マネジメントレビューからのアウトプット.....	19
4 . 内部監査.....	20
第7 改善	21
1 . 継続的改善.....	21
2 . 是正処置.....	21
3 . 予防処置.....	21
附属書「詳細管理策」	22
1 . はじめに.....	22
2 . 実践規範への手引き.....	22
3 . 情報セキュリティポリシー.....	22
4 . セキュリティ組織.....	23
5 . 情報資産の分類及び管理.....	24
6 . 人的セキュリティ.....	25
7 . 物理的及び環境的セキュリティ.....	26
8 . 通信及び運用管理.....	27
9 . アクセス制御.....	30
10 . システムの開発及びメンテナンス.....	34
11 . 事業継続管理.....	36
12 . 準拠.....	37
参考資料 ISMS 認証基準(Ver.1.0)との対応表	38

第0 序文

1. 一般

本基準は、経営陣及び要員が、効果的な情報セキュリティマネジメントシステム（以下、ISMS という。）を構築し、運営管理していくためのモデルを提供することを目的として作成されたものである。ISMS を採用するかどうかは、組織における戦略上の決定とすべきである。組織における ISMS の設計及び導入は、事業上のニーズ及び目標、その結果生じる情報セキュリティ要求事項、用いられるプロセス、並びに組織の規模及び構造によって影響を受ける。これらの事項及びこれらを支えるシステムは、時とともに変化すると考えられる。

本基準は、あらゆる顧客からの要求又は規制上の要求と同様に、組織固有の要求事項を満たす組織の能力を、内部の者及び認証機関を含む外部の者が評価するためにも使用することができる。

2. プロセスアプローチ

本基準では、組織において ISMS を確立、導入、運用、監視、維持し、かつその ISMS の有効性を改善する際に、プロセスアプローチを採用することを奨励している。

組織は、有効に機能するために、多くの活動を明確にし、運営管理しなければならない。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されるあらゆる活動は、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、後に続くプロセスへの直接のインプットとなる。

組織内においてプロセスを明確にし、その相互関係を把握し、運営管理することとあわせて、一連のプロセスをシステムとして適用することを「プロセスアプローチ」と呼ぶ。

プロセスアプローチによって、その利用者は次の事項の重要性を強調するようになる。

事業上の情報セキュリティ要求事項、並びに情報セキュリティポリシー及び目標を確立する必要性を理解すること。

組織における全般的な事業上のリスク管理を考慮に入れて、管理策を導入し、運用すること。

ISMS の実施状況及び有効性を監視し、見直すこと。

客観的な測定結果に基づいて継続的に改善すること。

本基準で採用されているモデルは、「Plan-Do-Check-Act」(PDCA) モデルとして知られており、あらゆる ISMS プロセスに適用できるものである。図 1 は、ISMS が情報セキュリティ要求事項及び利害関係者の期待をインプットとし、必要な活動及びプロセスを経て、これらの要求事項及び期待を満たす情報セキュリティの成果（すなわち運営管理された情報セキュ

リティ)を生み出すことを表したものである。図1は、また、第4、第5、第6、第7に記述するプロセスのつながりも表している。

情報セキュリティ要求事項の例示

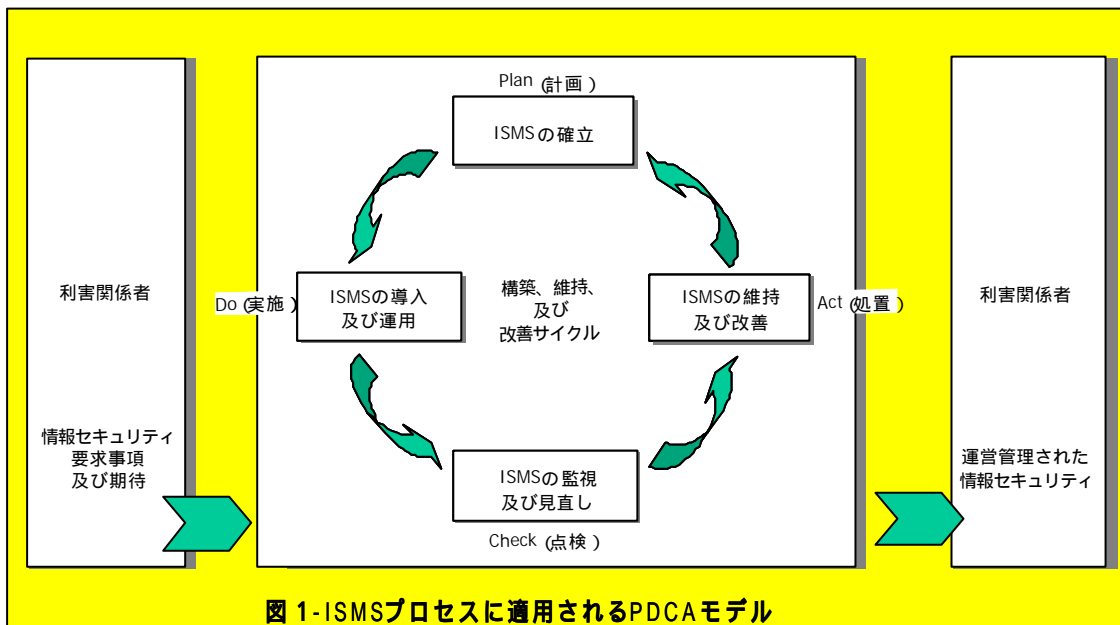
情報セキュリティ違反によって組織が深刻な財務上の損害を受けないようにすること。

情報セキュリティ違反によって組織の存続が脅かされないようにすること。

利害関係者の期待の例示

電子商取引に使用しているウェブサイトに対し不正侵入のような重大な事件・事故が起こった場合、その影響を最小限に抑えるための適切な手順に対する十分な訓練を受けた要員がいること

参考 情報セキュリティでは、「手順」という語は、慣習的に、コンピュータや他の電子的手段ではなく、人によって実施される「プロセス」という意味で使用される。



Plan - 計画 (ISMS の確立)	組織の全般的なポリシー及び目標に沿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する情報セキュリティポリシー、目標、対象、プロセス及び手順を確立する。
Do - 実施 (ISMS の導入及び運用)	その情報セキュリティポリシー、管理策、プロセス及び手順を実施し運用する。
Check - 点検 (ISMS の監視及び見直し)	情報セキュリティポリシー、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。
Act - 処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。

3. 他のマネジメントシステムとの両立性

本基準は、関連するマネジメント規格と矛盾なく統合して実施・運用することができるように、JIS Q 9001:2000 及び JIS Q 14001:1996 との整合がとられている。

本基準は、組織自らの ISMS を、関連する他のマネジメントシステムの要求事項に整合したり、統合したりすることができるように設計されている。

第1 適用範囲

1. 一般

本基準は、組織の事業上のリスク全般に対して、文書化された ISMS の確立、導入、運用、監視、見直し、維持及び改善に関する要求事項を規定するものである。また本基準は、個々の組織又は組織の一部が、その必要性に応じて情報セキュリティ管理策を適切に実施できるように要求事項を規定している。

ISMS は、情報資産を保護するため、十分でバランスのとれた適切な情報セキュリティ管理策を確保し、顧客及び他の利害関係者に対して信頼を与えるように設計されるものである。このように設計された ISMS は、競争力、キャッシュフロー、収益性、法令等の遵守及び企業イメージを維持し、改善することにつながる。

2. 適用

本基準の要求事項は汎用性があり、業種及び事業形態、規模及び事業の性質を問わず、あらゆる組織に適用できることを意図している。組織やその事業の性質によって、本基準の要求事項のいずれかが適用できない場合には、その要求事項の除外を考慮することができる。

このような除外を行う場合、その除外が、リスクアセスメント及び該当する規制上の要求事項によって決定されるセキュリティ要求事項を満たす情報セキュリティを提供する組織の能力、責任などに影響を及ぼさないと判断されない限り、本基準への適合の宣言は受け入れられない。リスク受容の基準を満たすために必要と考えられる管理策を適用除外とする場合には、その理由及び関連するリスクが責任者によって正式に受容されたことを示す証拠が必要である。本基準の第 4、第 5、第 6 及び第 7 に定める要求事項を除外することは、いかなる場合であっても認められない。

第2 引用規格等

次に掲げる規格等は、本基準の適用にあたり不可欠なものである。発行年の付いている規格等については、記載の年の版だけが本基準に適用される。発行年のない規格等については、その引用規格等の最新版が適用となる。

JIS X 5080:2002 情報技術 – 情報セキュリティマネジメントの実践のための規範

ISO Guide 73:2002 リスクマネジメント – 用語集 – 規格において使用するための指針(TR Q 0008 として平成 15 年 2 月発行予定。)

第3 定義

本基準の目的のために、次に掲げる定義を適用する。

1. 可用性 (availability)

許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

[JIS X 5080:2002 を参考]

2. 機密性 (confidentiality)

アクセスを許可された者だけが情報にアクセスできることを確実にすること。

[JIS X 5080:2002 を参考]

3. 情報セキュリティ (information security)

情報の機密性、完全性及び可用性のセキュリティの維持。

[JIS X 5080:2002 を参考]

4. 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なかで、事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善をになう部分。

参考 マネジメントシステムには、組織の構造、ポリシー、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。

5. 完全性 (integrity)

情報及び処理方法の正確性及び完全性を保持すること。

[JIS X 5080:2002 を参考]

6. リスク受容 (risk acceptance)

リスクを受容する意思決定。

[ISO Guide 73 を参照]

7. リスク分析 (risk analysis)

リスク因子を特定し、リスクを算定するために、情報を体系的に利用すること。

[ISO Guide 73 を参考]

参考 リスク因子(risk source)：結果をもたらす可能性が潜在する物事や行動。

[ISO Guide 73 を参照]

8．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全てのプロセス。

[ISO Guide 73 を参照]

9．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評価基準と比較するプロセス。

[ISO Guide 73 を参照]

10．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。

[ISO Guide 73 を参照]

11．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対応プロセス。

[ISO Guide 73 を参照]

12．適用宣言書 (statement of applicability)

組織のリスクアセスメント及びリスク対応プロセスの結果及び結論に基づいて、本基準の附属書「詳細管理策」の管理目的及び管理策の選択可否と選択しない場合の理由並びに必要な応じ追加した管理目的及び管理策とその理由について記述した文書。

第4 情報セキュリティマネジメントシステム

1. 一般要求事項

組織は、自らの事業の活動全般及びリスク全般を考慮して、文書化された ISMS を構築、導入、維持し、かつこれを継続的に改善すること。本基準で使われるプロセスは、図1に示す PDCA モデルに基づいている。

2. ISMS の確立及び運営管理

(1) ISMS の確立

組織は次の事項を実施すること。

事業の特徴、組織、その所在地、資産及び技術の観点から、ISMS の適用範囲を定義する。

事業の特徴、組織、その所在地、資産及び技術の観点から、次の事項を満たす ISMS の基本方針を策定する。

- (ア) ISMS の目標を設定するための枠組みを含み、情報セキュリティに関する全般的な方向性及び行動指針を確立する。
- (イ) 事業上の要求事項及び法的又は規制要求事項、並びに契約上のセキュリティ義務を考慮する。
- (ウ) ISMS を確立し、維持するために必要な戦略上の視点からみた組織環境、並びにリスクマネジメントのための環境を整備する。
- (エ) リスクを評価するための基準を確立し、定義されたリスクアセスメントの構造を確立する(第4.2.(1) 参照)。
- (オ) 経営陣による承認を得る。

リスクアセスメントについての体系的な取組方法を策定する。

当該 ISMS に適しており、また、明確にされた事業上の情報セキュリティ要求事項、並びに識別された法的及び規制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。リスクを受容可能な水準にまで軽減するために、ISMS の基本方針及び目標を設定する。また、リスクを受容するための基準を定め、受容可能なリスクの水準を特定する(第5.1. 参照)。

リスクを識別する。

- (ア) 当該 ISMS の範囲内の情報資産及び情報資産の責任者を特定する。
- (イ) それらの情報資産に対する脅威を明確にする。
- (ウ) 脅威によって利用されるおそれのある脆弱性を明確にする。
- (エ) 機密性、完全性及び可用性の喪失が情報資産に及ぼすかもしれない影響を明確にする。

リスクアセスメントを実施する。

- (ア) セキュリティ障害に起因して想定される事業上の損害を評価する。その際に、当該情報資産の機密性、完全性又は可用性の喪失による潜在的な影響を考慮する。
- (イ) 一般に認識されている脅威及び脆弱性の観点から起こりうるセキュリティ障害などの現実的な発生可能性、情報資産に関連する影響、並びに現在実施されている管理策を考慮してアセスメントを実施する。
- (ウ) リスクの度合いを算定する。
- (エ) 第 4 2.(1) で確立した評価基準を使用して、当該リスクについて、受容できるか、対応が必要かを定める。

リスク対応についての選択肢を明確にし、評価する。

考えられるリスク対応に関する選択肢として、次のような事項が含まれる。

- (ア) 適切な管理策を採用する。
- (イ) リスクを保有する。リスクが組織の基本方針及びリスク受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容する（第 4 2.(1) 参照）。

参考 リスクの保有(risk retention): あるリスクからの損失の負担又は利得の恩恵の受容

[ISO Guide 73 を参照]

- (ウ) リスクを回避する。
- (エ) リスクを移転する。関連する事業上のリスクを、例えば、保険会社又は供給者という他者に移転する。

リスク対応に関する管理目的及び管理策を選択する。

本基準の附属書「詳細管理策」から、適切な管理目的及び管理策を選択する。また、この選択については、リスクアセスメント及びリスク対応プロセスの結果に基づいてその妥当性を示すこと。

参考 附属書「詳細管理策」の管理目的及び管理策は網羅的なものではなく、追加の管理目的及び管理策を選択することができる。

適用宣言書を作成する。

第 4 2.(1) で選択した管理目的及び管理策、並びにこれらを選択した理由を文書化し、適用宣言書に含めなければならない。また、附属書「詳細管理策」に記載する管

理目的及び管理策を選択しない場合についても、その理由を記述しなければならない。

残留リスクに対する経営陣の承認及び当該 ISMS を導入し、運用するための許可を得る。

(2) ISMS の導入及び運用

組織は次の事項を実施すること。

情報セキュリティについてのリスクを管理するための、適切な管理活動、責任及び優先順位が明確にされたリスク対応計画を策定する（第 5 参照）。

識別され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。これには、必要な資金の拠出を考慮し、役割及び責任を割り当てることを含む。

当該管理目的を達成するために第 4 2.(1) で選択した管理策を実施する。

教育・訓練及び周知のためのプログラムを実施する（第 5 2.(2)参照）。

運用を管理する。

経営資源を管理する（第 5 2.参照）。

セキュリティ事件・事故を迅速に検出し、それらに対して迅速な対応を行うことのできる手順及びその他の管理策を実施する。

(3) ISMS の監視及び見直し

組織は次の事項を実施すること。

次の事項を行うため、監視のための手順及び他の管理策を実施する。

- (ア) 処理結果から誤りを速やかに検出する。
- (イ) セキュリティ上の違反行為及び事件・事故は未遂であっても、迅速に識別する。
- (ウ) 人又は情報技術によって実施されるセキュリティ活動が意図した通りに実施されているかどうかを、経営陣や管理者が判断できるようにする。
- (エ) セキュリティ違反の再発防止のためにとるべき処置を、事業上の優先順位を踏まえて判断する。

当該 ISMS の有効性に関して定期的な見直しを実施する（情報セキュリティポリシー及び目標を満たすこと、並びにセキュリティ管理策の見直しを含む）。その際、セキュリティ監査の結果、事件・事故、提案及び全ての利害関係者からのフィードバックを考慮に入

れる。

残留リスク及び受容可能なリスク水準の見直しを行う。その際、次の事項に生じる変化を考慮に入れる。

- (ア) 組織
- (イ) 技術
- (ウ) 事業の目標及びプロセス
- (エ) 識別された脅威
- (オ) 外部の事象。例えば、法的又は規制環境や社会環境の変化など

あらかじめ定められた間隔で ISMS の内部監査を実施する。

適用範囲が引き続き適切であり、ISMS のプロセスにおける改善策が明確にされていることを確実にするために、定期的に（少なくとも年1回）ISMS のマネジメントレビューを実施する（第6 参照）。

ISMS の有効性又は実施状況に影響を与える可能性のある活動及び事象を記録する（第4 3.(3)参照）。

(4) ISMS の維持及び改善

組織は定期的に次の事項を実施すること。

識別された ISMS の改善策を実施する。

第7 2.及び第7 3.に従って適切な是正処置及び予防処置を実施する。自らの組織及び他の組織の情報セキュリティに関する経験から学んだ教訓を活用する。

利害関係者全てに結果及び講じた処置を伝達し、合意を得る。

改善が、その意図した目標を確実に達成するようにする。

3. 文書化に関する要求事項

(1) 一般

ISMS 文書には、次の事項を含めること。

情報セキュリティポリシー（第4 2.(1) 参照）及び管理目的の表明。

当該 ISMS の適用範囲（第4 2.(1) 参照）並びに ISMS を支える手順及び管理策。

リスクアセスメントの結果報告(第4.2.(1) から第4.2.(1) 参照)。

リスク対応計画(第4.2.(2) 参照)。

情報セキュリティに関するプロセスの効果的な計画、運用及び管理を確実に実施するために、組織が必要と判断した、文書化された手順(第6.1.参照)。

本基準が要求する記録(第4.3.(3)参照)。

適用宣言書。

文書は全て、ISMS ポリシーの要求に応じて利用できるようにしておくこと。

参考 1 本基準で「文書化された手順」という用語を使う場合には、その手順が確立され、文書化され、実施され、かつ、維持されていることを意味する。

参考 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、セキュリティ要求事項及び運営管理するシステムの複雑さ

参考 3 文書及び記録の様式及び媒体の種類はどのようなものでもよい。

(2) 文書管理

ISMS で必要とされる文書は、保護し管理すること。次の事項を行うのに必要な管理活動を規定する文書化された手順を確立すること。

発行前に、適切かどうかの観点から文書を承認する。

文書の見直しを行う。また、必要に応じて更新し、再承認する。

文書の変更の識別及び現在の改訂版の識別を確実にする。

該当する文書の最新版が、必要なときに、必要なところで使用可能な状態にあることを確実にする。

文書が読みやすく、容易に識別可能な状態であることを確実にする。

どれが外部で作成された文書かが識別されていることを確実にする。

文書の配付が適切に管理されていることを確実にする。

廃止文書が誤って使用されないようにする。

廃止文書を何らかの目的で保持する場合には、適切な識別をする。

(3) 記録の管理

記録は、要求事項への適合及び ISMS の効果的運用の証拠を示すために、作成され、維持されること。また、これらの記録は管理されること。その際、当該 ISMS は該当する法的要求事項を考慮に入れること。記録は、読みやすく、容易に識別可能で、検索可能な状態であること。記録の識別、保管、保護、検索、保管期間及び廃棄に関して必要な管理を文書化すること。運営管理プロセスで、記録の必要性及び記録の範囲を定めること。

第 4.2. に記述されているプロセスの実施状況に関する記録及び ISMS に関連する全てのセキュリティ事件・事故の発生に関する記録を維持すること。

記録の例

訪問者台帳、監査記録及びアクセスの承認記録など。

第5 経営陣の責任

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、見直し、維持及び改善に対するコミットメントの証拠を、次の事項によって示すこと。

情報セキュリティポリシーを確立する。

情報セキュリティ目標が設定され、計画が立案されることを確実にする。

情報セキュリティに対する役割及び責任を定める。

情報セキュリティ目標を達成すること及び情報セキュリティポリシーに適合することの重要性、当該組織の法的責任、並びに継続的改善の必要性を組織内に周知する。

ISMS の構築、導入、運用及び維持に十分な経営資源を提供する（第5.2.(1)参照）。

リスクの受容可能な水準を決める。

ISMS のマネジメントレビューを実施する（第6参照）。

2. 経営資源の運用管理

(1) 経営資源の提供

組織は、次の事項を実施するために必要な経営資源を決定し、提供すること。

ISMS を確立、導入、運用及び維持する。

情報セキュリティの手順が事業上の要求事項を満たすものであることを確実にする。

法的及び規制要求事項と契約上のセキュリティに関する義務を識別し、取扱う。

実施される全ての管理策を的確に適用することにより、十分なセキュリティを維持する。

必要な場合には見直しを行い、その結果に対して適切に対応する。

必要な場合には、ISMS の有効性を改善する。

(2) 教育・訓練、認識及び力量

ISMS において、明確にされた責任を割り当てられた要員全てが要求される業務を実施す

る力量をもつことを、次の事項を実施することによって組織は確実にすること。

ISMS に影響がある業務に従事する要員に必要な力量を明確にする。

必要な力量がもてるように適切な教育・訓練を実施し、必要な場合には、適格な要員を雇用する。

実施した教育・訓練及びその他の講じた処置の有効性を評価する。

教育・訓練、技能、経験及び資格についての記録を維持する（第 4 3.(3)参照）。

組織はまた、該当する要員全てが、自らの情報セキュリティについての活動のもつ意味とその重要性を認識し、ISMS の目標の達成に向けて自らが、どのように貢献できるかを認識することを確実にしなければならない。

第6 マネジメントレビュー

1. 一般

経営陣は、組織の ISMS が、引き続き適切で、妥当で、かつ、有効であることを確実にするために、あらかじめ定められた間隔で ISMS をレビューすること。このレビューでは、ISMS に対する改善の機会の評価、情報セキュリティポリシー及び情報セキュリティ目標を含む ISMS の変更の必要性の評価も行うこと。また、このレビューの結果を明確に文書化しなければならず、その記録を維持すること(第4.3.(3)参照)。

2. マネジメントレビューへのインプット

マネジメントレビューへのインプットには次の情報を含めること。

監査及びレビューの結果

利害関係者からのフィードバック

ISMS の実施状況及び有効性を改善するために組織において利用可能な技術、製品又は手順

予防処置及び是正処置の状況

過去のリスクアセスメントで適切に取り扱われなかった脆弱性又は脅威

過去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

ISMS に影響を及ぼす可能性のある全ての変更

改善のための提案

3. マネジメント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、次の事項に関する決定及び処置を含めること。

ISMS の有効性の改善

ISMS に影響を与える可能性のある内部又は外部の事象に対応するために必要に応じて加えられる、情報セキュリティを実現する手順の修正。それら事象には、次の事項に対する変更が含まれる

(ア) 事業上の要求事項

(イ) 情報セキュリティ要求事項

- (ウ) 既存の事業上の要求事項を満たす業務プロセス
- (エ) 規制環境又は法的環境
- (オ) リスクの度合い及びリスク受容の水準

必要となる経営資源

4. 内部監査

組織は、当該 ISMS の管理目的、管理策、プロセス及び手順が次の事項を満たしているか否かを明確にするために、あらかじめ定められた間隔で ISMS の内部監査を実施すること。

本基準の要求事項に適合していること。また、関連する法令又は規制に適合していること。

識別した情報セキュリティ要求事項に適合していること。

有効に実施され維持されていること。

期待通りに実施されていること。

組織は、監査の対象となるプロセス及び領域の状況と重要性、並びにこれまでの監査結果を考慮して、監査プログラムを策定すること。監査の評価基準、対象範囲、頻度及び方法を規定すること。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保すること。監査員は自らの仕事は監査しないこと。

監査の計画及び実施、結果の報告、記録の維持（第 4.3.(3)参照）に関する責任、並びに要求事項を文書化された手順の中で規定すること。

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確実に講じられるようにすること。改善活動には、講じた処置の検証及び検証結果の報告を含めること(第7 参照)。

第7 改善

1. 継続的改善

組織は、情報セキュリティポリシー、情報セキュリティ目標、監査結果、監視した事象の分析、是正処置、予防処置及びマネジメントレビューを通じて、ISMS の有効性を継続的に改善すること。

2. 是正処置

組織は、再発防止のため、ISMS の導入及び運用に関連する不適合の原因を除去するための処置を講ずること。是正処置に関する文書化された手順では、次の事項に関する要求事項を規定すること。

ISMS の導入及び運用についての不適合の識別

不適合の原因の特定

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

必要な是正処置の決定及び実施

実施した処置の結果の記録（第 4 3.(3)参照）

実施した是正処置のレビュー

3. 予防処置

組織は、不適合の発生を未然に防ぐための処置を決めること。予防処置は、起こり得る問題の影響に見合ったものであること。予防処置に関する文書化された手順では、次の事項に関する要求事項を規定すること。

起こり得る不適合及び原因の識別

必要な予防処置の決定及び実施

実施した処置の結果の記録（第 4 3.(3)参照）

実施した予防処置のレビュー

変化したリスクの識別及び大きく変化したリスクに対して確実に注意が払われるようにすること

予防処置の優先順位については、リスクアセスメントの結果に基づいて決定すること。

参考 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高い。

附属書「詳細管理策」

1. はじめに

3.から 12.に記載する管理目的及び管理策は、JIS X 5080:2002 を参照している。この一覧表は網羅的なものではなく、組織は追加の管理目的及び管理策の必要性を検討することができる。第4 2.(1)で規定された ISMS のプロセスの一部として、この一覧表から管理目的及び管理策を選択すること。

2. 実践規範への手引き

附属書の 3.から 12.は JIS X 5080:2002 の 3.から 12.に規定する管理策を基にした最良な実践の導入についての助言及び手引きを提供するものである。

3. 情報セキュリティポリシー

3(1) 情報セキュリティポリシー	
管理目的: 情報セキュリティのための経営陣の指針及び支持を規定するため。	
管理策	
3(1)	情報セキュリティポリシー文書は、経営陣により承認及び制定されること。
3(1)	情報セキュリティポリシー文書は、必要な関係者全員に公表され、通知されること。
3(1)	情報セキュリティポリシーは、定期的に見直され、必要に応じて変更されること。また、変更された場合にはその変更内容の妥当性が確認されること。

4. セキュリティ組織

4(1) 情報セキュリティ・インフラストラクチャ 管理目的: 組織内の情報セキュリティを管理するため。	
管理策	
4(1)	情報セキュリティを主導するための明瞭な方向付け及び経営陣による目に見える形での支持を確実にするため、委員会等を設置すること。 この委員会は適切にコミットメントされ、経営資源が割り当てられることにより、情報セキュリティの促進をすること。
4(1)	大きな組織では、組織内の情報セキュリティの管理策を調整するため、関連する部門の管理者の代表を集めた委員会を利用すること。
4(1)	個々の情報資産に対する保護責任及び特定のセキュリティ手順に関する実施責任を明確にすること。
4(1)	情報処理施設及び設備の新規導入に対する経営陣・管理者による承認プロセスを定めること。
4(1)	情報セキュリティに関して、適宜社内又は社外の専門家から助言を受け、組織全体を調整すること。
4(1)	行政機関、規制当局、情報サービス提供者（ISP）及び通信事業者等との適切な連絡体制を維持すること。
4(1)	情報セキュリティポリシーの実施を独立して見直すこと。
4(2) 第三者アクセスのセキュリティ 管理目的: 第三者によってアクセスされる組織の情報処理設備及び情報資産のセキュリティを維持するため。	
管理策	
4(2)	第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、評価されたリスクに基づき必要な措置を講ずること。
4(2)	第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、必要なセキュリティ要求事項を全て明記した正式な契約を締結すること。
4(3) 第三者への委託（アウトソーシングや外部委託） 管理目的: 情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため。	
管理策	
4(3)	情報システムの管理や制御を委託する場合、セキュリティ要求事項を明記した正式な契約を締結すること。

5. 情報資産の分類及び管理

5(1) 情報資産に対する責任 管理目的: 組織の資産の適切な保護を維持するため。	
管理策	
5(1)	情報資産を適切に管理するため、情報システムに関連づけて全ての重要な情報資産について資産台帳を作成し、維持すること。
5(2) 情報の分類 管理目的: 情報資産の適切なレベルでの保護を確実にするため。	
管理策	
5(2)	事業における必要性や問題が生じた場合の影響度に応じた情報資産の分類基準を設けること。
5(2)	情報資産を分類基準に従い分類し、その取扱いに関する手順を定めること。

6. 人的セキュリティ

6(1) 職務定義及び採用におけるセキュリティ	
管理目的: 人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため。	
管理策	
6(1)	情報セキュリティポリシーに定義した情報セキュリティに関する役割及び責任を職務定義書に明記すること。
6(1)	採用する人員、請負業者及び臨時職員に求める資質や職能を明確にすること。
6(1)	人員の採用条件の一部として、被雇用者から機密保持合意書への署名を得ること。
6(1)	雇用条件には、被雇用者に対し情報セキュリティに関する責任を明示すること。
6(2) 利用者の教育・訓練	
管理目的: 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティポリシーを維持していくことを確実にするため。	
管理策	
6(2)	情報セキュリティポリシーの対象者に対し、情報セキュリティポリシー及び関連する手順等に関する教育・訓練を定期的実施すること。
6(3) セキュリティ事件・事故及び誤動作への対処	
管理目的: 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティポリシーを維持していくことを確実にするため。	
管理策	
6(3)	セキュリティ事件・事故は、経営陣を含めた連絡網を通じてできるだけ早く報告すること。
6(3)	セキュリティ事件・事故やそれに準ずる出来事を発見した場合の報告義務を、その義務を有する者に対し周知徹底すること。
6(3)	ソフトウェアが誤動作した場合の報告手順を定めること。
6(3)	発見したセキュリティ事件・事故や誤動作の種類や規模、事業への影響度の大きさ、復旧のための関連費用等を明確にすること。また、その結果を組織の情報セキュリティに反映させる態勢を整えること。
6(3)	情報セキュリティポリシー及び関連する手順に違反した場合の処置は、正式な懲戒プロセスに従うこと。

7. 物理的及び環境的セキュリティ

7(1) セキュリティ区画	
管理目的: 業務施設及び情報に対する許可されていないアクセス、損傷及び妨害を防止するため。	
管理策	
7(1)	情報処理施設及び設備を含む領域の保護のために、セキュリティ境界を導入すること。
7(1)	セキュリティ区画は、許可されない者がアクセスできないよう入退管理されること。
7(1)	セキュリティ区画は、特別な管理を要求される作業場所や施設を保護する目的で設置されること。
7(1)	セキュリティ区画において作業をするために必要な措置を講じ、作業ガイドライン等を整備すること。
7(1)	納品及び積荷場所は、許可されないアクセスを避けるため管理され、情報処理施設及び設備から分離されること。
7(2) 装置のセキュリティ	
管理目的: 資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため。	
管理策	
7(2)	装置の設置場所における環境上の脅威を軽減するための措置を講ずること。
7(2)	装置を許可されないアクセスから保護すること。
7(2)	装置を停電やその他の電源異常から保護すること。
7(2)	データ伝送や情報サービスに使用する電源及び通信ケーブルの配線に対し、傍受や損傷等を防止するための措置を講ずること。
7(2)	装置の可用性及び完全性を確実に維持するために、装置の保守を正しく実施すること。
7(2)	組織の敷地外で情報処理装置を利用する場合は、管理者による承認を受けること。
7(2)	装置を処分あるいは再利用する際、装置に格納された情報を事前に消去すること。
7(3) 一般的な管理策	
管理目的: 情報及び情報処理設備の損傷又は盗難を防止するため。	
管理策	
7(3)	離席時や帰宅時における、机上やその他の場所への情報の放置を禁止すること。
7(3)	離席時や帰宅時には、パスワードで保護されたスクリーンセーバの使用やログオフを徹底し、他人による情報システムへのアクセスを防止するための措置を講ずること。
7(3)	組織が所有する装置や情報、ソフトウェア等を管理者による承認なしに移動させないこと。

8. 通信及び運用管理

8(1) 運用手順及び責任	
管理目的: 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。	
管理策	
8(1)	セキュリティポリシーに従い特定した操作手順を文書化し、維持すること。
8(1)	情報システムや情報処理施設等に対する変更を管理すること。
8(1)	セキュリティ事件・事故の対応を迅速、効果的、整然と行うために、また関連するデータ（監査証跡、監査ログなど）の収集を行うために、セキュリティ事件・事故を管理する責任体制及び手順を定めること。
8(1)	情報やサービスへの許可されない変更や誤用の機会を低減するため、職務の分離及び責任の範囲を明確にすること。
8(1)	情報システムの開発及びテストの環境を運用施設及び設備から分離すること。 また、運用ソフトウェアについて、開発段階から運用段階へ移行の手順を定めること。
8(1)	外部の施設管理サービスを利用する場合、評価されたリスクに基づき、適切な措置を定め、内容を明記した正式な契約を締結すること。
8(2) システム計画の作成及び受け入れ	
管理目的: システム障害によるリスクを最小限に抑えるため。	
管理策	
8(2)	情報システムの処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。
8(2)	情報システムを新規導入あるいは変更する際の受け入れ基準を確立し、情報システムの本番利用を容認する前に適切なテストを実施すること。
8(3) 不正ソフトウェアからの保護	
管理目的: ソフトウェア及び情報の完全性を保護するため。	
管理策	
8(3)	情報や情報システムを不正ソフトウェアから保護するための検出及び防止策を講じ、適宜利用者の教育・訓練を実施すること。

8(4) 情報システムの管理	
管理目的: 情報処理及び通信サービスの完全性及び可用性を維持するため。	
管理策	
8(4)	重要な情報及びソフトウェアのバックアップコピーを定期的を取得し、定期的にテストすること。
8(4)	情報システムの操作担当者の作業履歴を記録すること。 また、操作担当者以外の者が作業履歴を定期的にチェックすること。
8(4)	障害が報告された情報システムを確実に修正すること。
8(5) ネットワークの管理	
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。	
管理策	
8(5)	ネットワークにおけるセキュリティを確保し維持するための措置を講ずること。
8(6) 媒体の取扱い及びセキュリティ	
管理目的: 情報資産に対する損害及び事業活動の中断を回避するため。	
管理策	
8(6)	テープ、ディスク、カセット等の移動可能な記憶媒体や書類等を適切に管理すること。
8(6)	不要になった媒体を処分する際、情報漏洩を防止するための措置を講ずること。
8(6)	情報の、許可されない開示及び改ざん、誤用等を防止するため、媒体の取扱い及び保管に関する手順を定めること。
8(6)	情報システムに関する文書を許可されないアクセスから保護すること。

8(7) 組織間における情報及びソフトウェアの交換	
管理目的: 組織間で交換される情報の紛失、改ざん又は誤用を防止するため。	
管理策	
8(7)	取引先や協業相手等と情報やソフトウェアを交換（電子的、人手にかかわらず）する場合、必要に応じて情報交換の実施に関する正式な契約を締結すること。
8(7)	移送中の媒体を許可されないアクセス、誤用及び破損から保護すること。
8(7)	電子取引を行う場合、不正行為、契約紛争、情報の許可されない開示及び改ざんを防止するための措置を講ずること。
8(7)	電子メールの使用に関するポリシーを定め、電子メールの使用により発生しうるリスクを軽減するための措置を講ずること。
8(7)	電子オフィスシステムの使用に関するポリシー及びガイドラインを定め、電子オフィスシステムの使用に関連したリスクを抑制すること。
8(7)	組織の情報を一般に公開し利用可能にする場合の正式な承認プロセスを定めること。
8(7)	組織の情報を一般に公開し利用可能にする場合、その情報を許可されない変更から保護すること。
8(7)	電話やファクシミリ、ビデオ通信等を使用して情報を交換する場合、そのポリシーと手順を定め、必要な措置を講ずること。

9. アクセス制御

9(1) アクセス制御に関する事業上の要求事項 管理目的: 情報へのアクセスを制御するため。	
管理策	
9(1)	情報へのアクセス制御に関する事業上及びセキュリティ上の必要性を明確にし、それに従いアクセス制御ポリシーを定めること。
9(1)	情報へのアクセスは、アクセス制御ポリシーに従い制限されること。
9(2) 利用者アクセス管理 管理目的: 情報システムへの許可されていないアクセスを防止するため。	
管理策	
9(2)	情報システム利用者の登録及び登録抹消の手順を定めること。
9(2)	特権の割当て及び使用を制限し管理すること。
9(2)	情報システム利用者に対するパスワードの割当ては、確立された管理プロセスに従い実施されること。
9(2)	経営陣・管理者は情報システム利用者のアクセス権を定期的に見直すように指示すること。
9(3) 利用者の責任 管理目的: 許可されていない利用者のアクセスを防止するため。	
管理策	
9(3)	パスワードの選択及び使用に際して、正しい情報セキュリティ慣行を参考に、利用者に情報セキュリティ上の問題を考慮することを要求すること。
9(3)	利用者の領域にある装置を常時監視することが不可能な場合、当該装置を適切に保護するよう利用者に要求すること。

9(4) ネットワークのアクセス制御	
管理目的: ネットワークを利用したサービスの保護のため。	
管理策	
9(4)	利用者に、明確に許可された以外のサービスへのアクセスを防止するための措置を講ずること。
9(4)	情報システムの利用者がコンピュータにアクセスする場合のネットワークの経路を制御すること。
9(4)	情報システムに対する遠隔地からのアクセスを許可する場合、利用者認証を行うこと。
9(4)	遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。
9(4)	診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。
9(4)	情報システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。
9(4)	共有ネットワークへのアクセス権限は、アクセス制御ポリシーに従い付与されること。
9(4)	共有ネットワークへのアクセスを許可する場合、アクセス制御ポリシーに基づき、可能な限り経路を制御すること。
9(4)	ネットワークに関連するサービスを使用する場合、そのサービスに施されたセキュリティに関する情報について、明確な説明をうけること。

9(5) オペレーティングシステムのアクセス制御	
管理目的: 許可されていないコンピュータアクセスを防止するため。	
管理策	
9(5)	接続が許可された特定の場所や携帯装置に対する認証を行うため、端末を自動的に識別する機能を備えること。
9(5)	情報サービスへのアクセスは、安全なログオンプロセスを使用すること。
9(5)	情報システム利用者は、個人を特定できる一意の識別子（利用者 ID）を有すること。 また、正当な利用者であることを認証するための適切な技術を選択すること。
9(5)	パスワード管理システムは、情報システム利用者に有効なパスワードを設定させるための対話式の機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を管理すること。
9(5)	システムユーティリティプログラムの使用を制限し管理すること。
9(5)	情報へのアクセスに際して、脅迫の対象となり得る利用者のため、脅迫に対して警報を発信する機能を備えること。
9(5)	取扱いに慎重を要する情報システムに接続された端末が活動停止状態にある場合、その端末を一定の活動停止時間の経過後、システムから遮断すること。
9(5)	リスクの高いアプリケーションシステムへの接続時間は、制限されること。
9(6) アプリケーションシステムのアクセス制御	
管理目的: 情報システムが保有する情報への許可されていないアクセスを防止するため。	
管理策	
9(6)	情報及びアプリケーションシステムへのアクセスは、アクセス制御ポリシーに従い制限されること。
9(6)	取扱いに慎重を要する情報システムは、隔離した環境に設置されること。

9(7) システムアクセス及びシステム使用の監視	
管理目的: 許可されていない活動を検出するため。	
管理策	
9(7)	例外事項やその他のセキュリティ関連イベント等の監査ログを記録し、定められた期間において保存すること。
9(7)	情報処理施設及び設備の使用を監視するための手順を定めること。
9(7)	情報処理施設及び設備の監視活動の結果を定期的に検証すること。
9(7)	正確に記録をするために、コンピュータ内のクロックを同期化すること。
9(8) モバイルコンピューティング及び遠隔地勤務	
管理目的: 移動型計算処理及び遠隔作業の設備を用いるとき、情報セキュリティを確実にするため。	
管理策	
9(8)	モバイルコンピュータを用いる場合、評価されたリスクに基づき、モバイルコンピュータ使用の方針を定めた上で必要な措置を講ずること。
9(8)	遠隔作業を許可し、管理するためのポリシー、手順及び基準を策定すること。

10. システムの開発及びメンテナンス

10(1) システムのセキュリティ要求事項	
管理目的: 情報システムへのセキュリティの組み込みを確実にするため。	
管理策	
10(1)	情報システムを新規導入あるいは変更する際、事業の要求事項に基づいたセキュリティ要求事項を明確にすること。
10(2) アプリケーションシステムのセキュリティ	
管理目的: 業務用システムにおける利用者データの消失、変更又は誤用を防止するため。	
管理策	
10(2)	アプリケーションシステムに入力されるデータが妥当なものであることを確認するための機能を整備すること。
10(2)	アプリケーションシステムで処理されたデータに対する改変を検出する機能を備えること。
10(2)	メッセージの完全性を保護する必要がある場合、メッセージ認証機能を備えること。
10(2)	アプリケーションシステムから出力されるデータが妥当なものであることを確認するための機能や手順を整備すること。
10(3) 暗号による管理策	
管理目的: 情報の機密性、真正性又は完全性を保護するため。	
管理策	
10(3)	情報を保護するために、評価されたリスクに基づき、暗号の使用についての方針を定めること。
10(3)	取扱いに慎重を要する情報や重要な情報については、機密性を保護するため暗号化すること。
10(3)	電子情報の真正性および完全性を保護するため、デジタル署名を用いること。
10(3)	取引に関わる紛争を解決するため、電子情報による取引事実の否認を防止するための措置を講ずること。
10(3)	情報を保護するために暗号を用いる場合、関連する対策基準類や手順等に準拠し、適切に鍵管理を行うこと。

10(4) システムファイルのセキュリティ	
管理目的: IT プロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため。	
管理策	
10(4)	稼働中の情報システムへのソフトウェアの導入は適切に管理されること。
10(4)	テスト用のデータは適切に保護され管理されること。
10(4)	プログラムソースライブラリへのアクセスを厳格に管理すること。
10(5) 開発及びサポートプロセスにおけるセキュリティ	
管理目的: アプリケーションシステムソフトウェア及び情報のセキュリティを維持するため。	
管理策	
10(5)	情報システムの正式な変更管理の手順を定め、変更を厳格に管理すること。
10(5)	オペレーティングシステムを変更する場合、アプリケーションシステムの見直し及びテストを実施すること。
10(5)	パッケージソフトウェアの変更は原則として行わないこと。
10(5)	やむを得ずパッケージソフトウェアの変更が必要になった場合、変更を厳格に管理すること。
10(5)	ソフトウェアの購入の際、プログラムにトロイの木馬やコバート通信路等が懸念される場合、事前に検査し、また使用及び変更を厳格に管理すること。
10(5)	ソフトウェア開発をアウトソーシングする場合、評価されたリスクに基づいた正式な契約を締結すること。

11. 事業継続管理

11(1) 事業継続管理 管理目的: 事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務プロセスを保護するため。	
管理策	
11(1)	ISMS 適用範囲全体を含む組織の事業継続を検討し策定、維持するための管理プロセスを整備すること。
11(1)	事業継続に取り組むため、リスクアセスメントに基づいた戦略計画を策定すること。
11(1)	重要な業務プロセスに関連した中断又は障害の際、事業の運営を維持し、許容時間内に復旧させるため、必要な計画を立案すること。
11(1)	全ての計画の整合性を保証し、また、試験や保守の優先順位を明確にするため、事業継続計画全体を統括する枠組みを維持すること。
11(1)	事業継続計画は定期的に試験され、常時有効であることを確実にするために内容の見直しにより維持されること。

12. 準拠

12(1) 法的要求事項への準拠	
管理目的: 刑法及び民法、制定法、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため。	
管理策	
12(1)	個別の情報システム毎に関連する全ての法令、規制及び契約上の要求事項を明確にし、これを文書化すること。
12(1)	知的財産権に関わる法的制限事項を遵守した手順を整備すること。
12(1)	組織の重要な記録を紛失、消失、破壊、改ざん等から保護すること。
12(1)	個人情報保護に関する法令に従い、個人の情報を保護すること。
12(1)	情報処理施設及び設備の悪用を防止するための措置を講ずること。
12(1)	暗号の使用に関する法令を遵守すること。
12(1)	訴訟に提示する証拠は、関連する法令に定められた規則に準拠すること。
12(2) セキュリティポリシーと技術標準への準拠性のレビュー	
管理目的: 組織のセキュリティポリシー及び関連する対策基準や手順書等へのシステムの準拠を確実にするため。	
管理策	
12(2)	組織の経営者・管理者は、責任範囲における全てのセキュリティ手続きが正しく実行されていること確実にする措置を講じ、組織内のすべての範囲においてセキュリティポリシー及び関連する対策基準や手順書等への準拠を定期的に見直すこと。
12(2)	情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的を確認すること。
12(3) システム監査の考慮事項	
管理目的: システム監査プロセスの有効性を最大に、また監査プロセスと業務の間でおよぼしあう影響を最小にするため。	
管理策	
12(3)	稼働中の情報システムに対する監査を実施する場合、業務が中断するリスクを最小限に抑えるよう計画し、被監査部門と合意すること。
12(3)	システム監査ツールに対する誤用又は悪用等を防止するための措置を講ずること。

参考資料 ISMS 認証基準(Ver.1.0)との対応表