

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)

JIP-ISMS100-2.0



平成 15 年 4 月 21 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(Ver.2.0)）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、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)に基づき作成したもので、本基準で使用する用語、表現については、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))との互換性を確保した。

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化の動向、JIS 化の動向、さらに 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。

なお、ISMS 認証基準(Ver.1.0)は、本基準に置き換えられるものであり、2004 年 9 月 30 日に廃止される。

(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 用語及び定義	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. リスクの受容 (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
(1) ISMSの確立	11
(2) ISMSの導入及び運用	13
(3) ISMSの監視及び見直し	13
(4) ISMSの維持及び改善	14
3. 文書化に関する要求事項	14

(1) 一般	14
(2) 文書管理	15
(3) 記録の管理	16
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
(1) 経営資源の提供	17
(2) 教育・訓練、認識及び力量	18
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. 情報セキュリティ基本方針	22
4. 組織のセキュリティ	23
5. 資産の分類及び管理	25
6. 人的セキュリティ	26
7. 物理的及び環境的セキュリティ	28
8. 通信及び運用管理	30
9. アクセス制御	33
10. システムの開発及び保守	37
11. 事業継続管理	39
12. 適合性	40
参考資料 ISMS 認証基準(Ver.1.0)との対応表	42

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。従って、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ことが期待される。

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、内部の者及び審査登録機関を含む外部の者が評価するために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明確に認識するようになる。

事業上の情報セキュリティ要求事項を理解し、情報セキュリティ基本方針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（計画-実施-点検-処置）」

(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、利害関係者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、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。

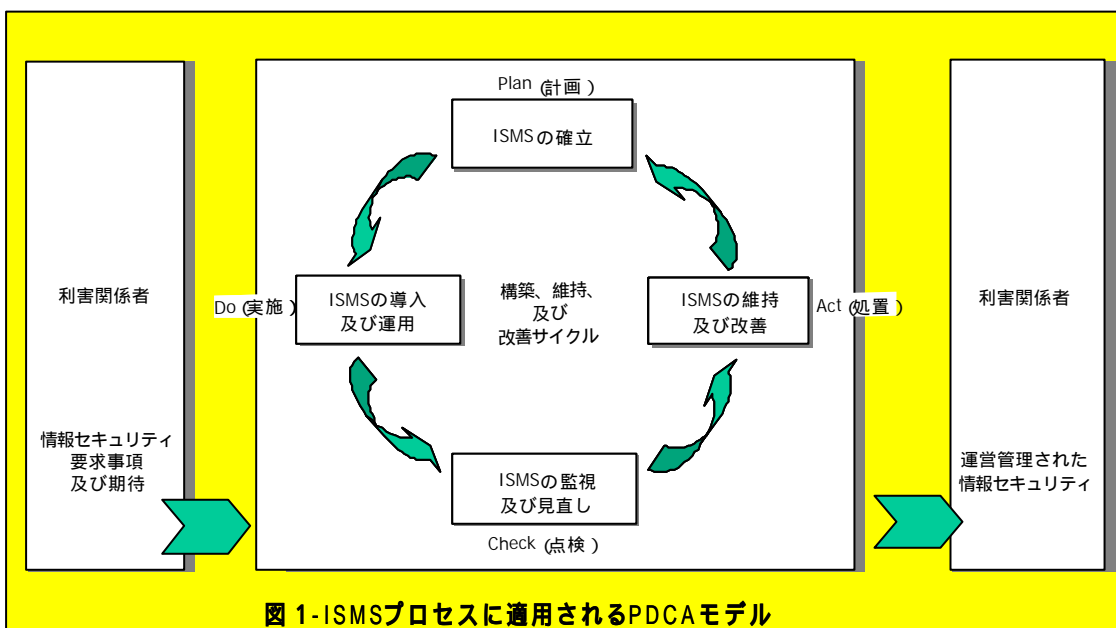
情報セキュリティ要求事項の例示

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」という用語は、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)	組織の全般的な基本方針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基本方針、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基本方針、管理策、プロセス及び手順を導入し運用する。
Check - 点検 (ISMS の監視及び見直し)	情報セキュリティ基本方針、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導入・運用することができるように、JIS Q 9001 : 2000 及び JIS Q 14001 : 1996 との統合がとられている。

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。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。また、組織やその事業の性質によって、本基準の附属書「詳細管理策」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。

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

JIS Q 9001:2000 品質マネジメントシステム - 要求事項

TR Q 0008:2003 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

第3 用語及び定義

本基準の目的のために、次に掲げる用語及び定義を適用する。

1. 可用性 (availability)

認可された利用者が、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 を参照]

2. 機密性 (confidentiality)

アクセスを認可された(authorized)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 を参照]

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維持。

[JIS X 5080:2002 を参照]

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、及び方針、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。

5. 完全性 (integrity)

情報及び処理方法が、正確であること及び完全であることを保護すること。

[JIS X 5080:2002 を参照]

6. リスクの受容 (risk acceptance)

リスクを受容する意思決定。

[TR Q 0008:2003 を参照]

7. 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 を参照]

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

[TR Q 0008:2003 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すべてのプロセス。

[TR Q 0008:2003 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基準と比較するプロセス。

[TR Q 0008:2003 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。

[TR Q 0008:2003 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、選択及び実施するプロセス。

[TR Q 0008:2003 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き、組織のISMS に適切で当てはまる管理目的及び管理策を記述した文書。

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の受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容する（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。

[TR Q 0008:2003 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」のリストは組織が必要とする管理目的及び管理策の全てとは限らないので、組織は必要に応じて追加の管理目的及び管理策を選択してもよい。

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、適用宣言書に含めること。また、附属書「詳細管理策」に記載する管理目的及び管理策の中から適用除外としたものは記録すること。

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、経営陣の適切な活動、責任及び優先順位が明確にされたり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・訓練及び認識させる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導入された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) セキュリティ違反を解決するためにとるべき処置を、事業上の優先順位を踏まえて決定する。

当該 ISMS の有効性に関して定期的な見直しを実施する（情報セキュリティ基本方針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

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、可能な限り合意を得る。

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。

情報セキュリティ基本方針（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。

本基準が要求する記録（第 4 3.(3)参照）。

適用宣言書(第 4 2.(1) 参照)。

文書は全て、ISMS の基本方針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策を文書化すること。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

訪問者の記録、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。

情報セキュリティ基本方針を確立する。

情報セキュリティ目標が設定され、計画が策定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の重要性及び情報セキュリティ基本方針に適合することの重要性、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 の確立、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情報セキュリティに関する義務を識別し、適切に対処する。

実施される全ての管理策を的確に適用することにより、十分な情報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

組織は、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すること。

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、情報セキュリティ基本方針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、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。それらの事象には、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。

(I) 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。

識別され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を監査しないこと。

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、情報セキュリティ基本方針、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の導入及び運用における不適合の識別。

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のリストは、JIS X 5080:2002 を参照している。本基準の第 4 2.(1)で規定された ISMS のプロセスの一部として、下記のリストから管理目的及び管理策を選択すること。ただし、このリストは組織が必要とする管理目的及び管理策の全てとは限らないので、組織は必要に応じて追加の管理目的及び管理策を選択してもよい。

2. 実践規範への手引き

JIS X 5080:2002 の 3.から 12.は、附属書の 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. 情報セキュリティ基本方針

3.(1) 情報セキュリティ基本方針		
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 基本方針文書	基本方針文書は、経営陣によって承認され、適当な手段で、全従業員に公表し、通知すること。
3.(1)	見直し及び評価	基本方針は、依然として適切であることを確実にするために、定期的に、また影響を及ぼす変化があった場合に、見直すこと。

4. 組織のセキュリティ

4.(1) 情報セキュリティ基盤 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 運営委員会	セキュリティを主導するための明りょう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に、運営委員会を設置すること。運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること。
4.(1)	情報セキュリティ の調整	大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を利用すること。
4.(1)	情報セキュリティ責 任の割当て	個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を、明確に定めること。
4.(1)	情報処理設備の認可 手続	新しい情報処理設備に対する経営陣による認可手続を確立すること。
4.(1)	専門家による情報セ キュリティの助言	専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること。
4.(1)	組織間の協力	行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること。
4.(1)	情報セキュリティの 他者によるレビュー	情報セキュリティ基本方針の実施を、他者がレビューすること。
4.(2) 第三者による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)	第三者のアクセスか ら生じるリスクの識 別	組織の情報処理施設への第三者のアクセスに関連づけてリスクアセスメントを実施し、適切なセキュリティ管理策を実施すること。
4.(2)	第三者との契約書に 記載するセキュリテ ィ要求事項	組織の情報処理施設への第三者アクセスにかかわる取決めは、必要なセキュリティ要求事項すべてを含んだ正式な契約に基づくこと。

4.(3) 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)	外部委託契約におけるセキュリティ要求事項	情報システム、ネットワーク及び/又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述されること。

5. 資産の分類及び管理

5.(1) 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)	資産目録	情報システムそれぞれに関連づけてすべての重要な資産について目録を作成し、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)	分類の指針	情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮に入れておくこと。
5.(2)	情報のラベル付け及び取扱い	組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること。

6. 人的セキュリティ

6.(1) 職務定義及び雇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)	セキュリティを職責に含めること	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で定められたとおりに、職務定義のなかに文書化すること。
6.(1)	要員審査及びその個別方針	常勤職員、請負業者及び臨時職員を採用するときは、提出された応募資料の内容を検査すること。
6.(1)	機密保持契約	従業員は、入社時の雇用条件の一部として、機密保持契約書に署名すること。
6.(1)	雇用条件	雇用条件には、情報セキュリティに対する従業員の責任について記述してあること。
6.(2) 利用者の訓練 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、通常の仕事の中で利用者が組織のセキュリティ基本方針を維持していくことを確実にするため。		
管理策		
6.(2)	情報セキュリティの教育及び訓練	組織の基本方針及び手順について、組織のすべての従業員及び関係するならば外部利用者を適切に教育すること、並びに定期的に更新教育を行うこと。

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：セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため。		
管理策		
6.(3)	セキュリティ事件・事故の報告	セキュリティ事件・事故は、適切な連絡経路をとおして、できるだけ速やかに報告すること。
6.(3)	セキュリティの弱点の報告	システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合に、情報サービスの利用者に対して、注意を払い、かつ、報告するよう要求すること。
6.(3)	ソフトウェアの誤動作の報告	ソフトウェア誤動作を報告する手順を確立すること。
6.(3)	事件・事故からの学習	事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを備えていること。
6.(3)	懲戒手続	従業員による組織のセキュリティ基本方針及び手順への違反は、正式な懲戒手続によって処理すること。

7. 物理的及び環境的セキュリティ

7.(1) セキュリティが保たれた領域 管理目的：業務施設及び業務情報に対する認可されていない物理的なアクセス、損傷及び妨害を防止するため。		
管理策		
7.(1)	物理的セキュリティ境界	組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること。
7.(1)	物理的入退管理策	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セキュリティの保たれた領域を保護すること。
7.(1)	オフィス、部屋及び施設のセキュリティ	特別なセキュリティ要求事項のあるオフィス、部屋及び施設を保護するために、セキュリティの保たれた領域を設定すること。
7.(1)	セキュリティが保たれた領域での作業	セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加すること。
7.(1)	受渡し場所の隔離	品物を受渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること。
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)	装置の設置及び保護	装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置又は保護すること。
7.(2)	電源	装置は、停電、その他の電源異常から保護すること。
7.(2)	ケーブル配線のセキュリティ	データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること。
7.(2)	装置の保守	装置についての継続的な可用性及び完全性の維持を可能とするために、装置を正しく保守すること。
7.(2)	事業敷地外における装置のセキュリティ	組織の敷地外で情報処理のために装置を使用するいかなる場合も、管理者による認可を要求すること。
7.(2)	装置の安全な処分又は再使用	装置を処分又は再使用する前に、情報を装置から消去すること。

7.(3) その他の管理策		
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)	クリアデスク及びクリアスクリーンの個別方針	組織は、情報への認可されていないアクセス、情報の消失及び損傷のリスクを軽減するための、クリアデスク方針及びクリアスクリーン方針を持つこと。
7.(3)	資産の移動	組織に属する装置、情報又はソフトウェアは、管理者による認可なしでもち出しできないこと。

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)	操作手順書	セキュリティ個別方針によって明確化した操作手順は、文書化して維持すること。
8.(1)	運用変更管理	情報処理設備及びシステムの変更について管理すること。
8.(1)	事件・事故管理手順	セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うために、および監査証跡及び記録といった事件・事故に関連するデータを収集するために、事件・事故管理の責任及び手順を確立すること。
8.(1)	職務の分離	情報若しくはサービスの無許可の変更又は誤用の可能性を小さくするために、職務及び責任領域を分離すること。
8.(1)	開発施設及び運用施設との分離	開発施設及び試験施設は、運用施設から分離すること。ソフトウェアの開発から運用の段階への移行についての規則は、明確に定め、文書化すること。
8.(1)	外部委託による施設管理	外部委託による施設管理サービスを利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること。
8.(2) システムの計画作成及び受入れ 管理目的：システム故障のリスクを最小限に抑えるため。		
管理策		
8.(2)	容量・能力の計画作成	十分な処理能力及び記憶容量の利用を可能にするために、容量・能力の需要を監視し、将来必要とされる容量・能力を予測すること。
8.(2)	システムの受入れ	新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること。
8.(3) 悪意のある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、悪意のあるソフトウェアによる被害から保護するため。		
管理策		
8.(3)	悪意のあるソフトウェアに対する管理策	悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること。

8.(4) システムの維持管理		
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)	情報のバックアップ	極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること。
8.(4)	運用の記録	運用担当者は、自分の作業の記録を継続すること。 運用担当者の記録は、定期的に独立した検査を受けること。
8.(4)	障害記録	障害については報告を行い、是正処置をとること。
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)	ネットワーク管理策	ネットワークにおけるセキュリティを実現し、かつ、維持するために一連の管理策を実施すること。
8.(6) 媒体の取扱い及びセキュリティ		
管理目的：財産に対する損害及び事業活動に対する妨害を回避するため。		
管理策		
8.(6)	コンピュータの取外し可能な付属媒体の管理	コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書を管理すること。
8.(6)	媒体の処分	媒体が不要となった場合は、安全、かつ、確実に処分すること。
8.(6)	情報の取扱手順	認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること。
8.(6)	システムに関する文書のセキュリティ	認可されていないアクセスからシステムに関する文書を保護すること。

8.(7) 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)	情報及びソフトウェアの交換契約	組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと。
8.(7)	配送中の媒体のセキュリティ	配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること。
8.(7)	電子商取引のセキュリティ	電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること。
8.(7)	電子メールのセキュリティ	電子メールの使用に関する個別方針を作成し、電子メールがもたらすセキュリティ上のリスクを軽減するための管理策を実施すること。
8.(7)	電子オフィスシステムのセキュリティ	オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること。
8.(7)	公開されているシステム	情報を公開する前に正式な認可の手続がとられ、また、情報の改ざんを防止するために公開した情報の完全性を保護すること。
8.(7)	情報交換のその他の方式	音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、個別方針、手順及び管理策をもつこと。

9. アクセス制御

9.(1) アクセス制御に関する業務上の要求事項 管理目的：情報へのアクセスを制御するため。		
管理策		
9.(1)	アクセス制御方針	アクセス制御についての業務上の要求事項を定義して文書化し、アクセスをアクセス制御方針で定義されたものに限定すること。
9.(2) 利用者のアクセス管理 管理目的：情報システムへのアクセス権が、適切に認可され、割り当てられ、維持されていることを確実にするため。		
管理策		
9.(2)	利用者登録	複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること。
9.(2)	特権管理	特権の割当て及び使用は、制限し、管理すること。
9.(2)	利用者のパスワードの管理	パスワードの割当ては、正規の管理手続によって統制すること。
9.(2)	利用者アクセス権の見直し	経営陣は、利用者のアクセス権を見直す正規の手順を、定期的の実施すること。
9.(3) 利用者の責任 管理目的：認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)	パスワードの使用	パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うことを、利用者に要求すること。
9.(3)	利用者領域にある無人運転の装置	無人運転の装置に適切な保護対策を備えていることを確実にするように、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：ネットワークを介したサービスの保護のため。		
管理策		
9.(4)	ネットワークサービスの使用についての個別方針	利用者には、使用することが特別に認可されたサービスへの直接のアクセスだけを提供すること。
9.(4)	指定された接続経路	利用者端末からコンピュータサービスまでの経路は、管理すること。
9.(4)	外部から接続する利用者の認証	遠隔地からの利用者のアクセスには、認証を行うこと。
9.(4)	ノードの認証	遠隔コンピュータシステムへの接続は、認証されること。
9.(4)	遠隔診断用ポートの保護	診断ポートへのアクセスは、セキュリティを保つように制御されること。
9.(4)	ネットワークの領域分割	情報サービス、利用者及び情報システムのグループを分割するための制御を、ネットワーク内に導入すること。
9.(4)	ネットワークの接続制御	共有ネットワークにおける利用者の接続の可能性は、アクセス制御方針に従って制限すること。
9.(4)	ネットワーク経路を指定した制御	共有ネットワークは、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、経路指定の制御策を組み込むこと。
9.(4)	ネットワークサービスのセキュリティ	ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けること。

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：認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)	自動の端末識別	特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること。
9.(5)	端末のログオン手順	情報サービスへのアクセスは、安全なログオン手順を使用すること。
9.(5)	利用者の識別及び認証	すべての利用者は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者 ID）を保有すること。利用者が主張する ID を確認するための適切な認証技術を選択すること。
9.(5)	パスワード管理システム	パスワード管理システムは、質のよいパスワードであることを確実にするための、有効な対話的機能を提供すること。
9.(5)	システムユーティリティの使用	システムユーティリティプログラムの使用を制限し、厳しく管理すること。
9.(5)	利用者を保護するための脅迫に対する警報	脅迫の標的となり得る利用者のために、脅迫に対する警報を備えること。
9.(5)	端末のタイムアウト機能	リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、認可されていない者によるアクセスを防止するために、一定の活動停止時間の経過後、その端末は遮断されること。
9.(5)	接続時間の制限	リスクの高い業務用ソフトウェアに対して、追加のセキュリティを提供するために、接続時間に制限を設けること。
9.(6) 業務用ソフトウェアのアクセス制御		
管理目的：情報システムが保有する情報への認可されていないアクセスを防止するため。		
管理策		
9.(6)	情報へのアクセス制限	情報及び業務用システム機能へのアクセスは、アクセス制御方針に従い、制限されること。
9.(6)	取扱いに慎重を要するシステムの隔離	取扱いに慎重を要するシステムは、専用の（隔離された）コンピュータ環境にあること。

9.(7) システムアクセス及びシステム使用状況の監視		
管理目的：認可されていない活動を検出するため。		
管理策		
9.(7)	事象の記録	例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること。
9.(7)	システム使用状況の監視	情報処理設備の使用状況を監視する手順を確立し、監視の結果を、定期的に見直すこと。
9.(7)	コンピュータ内の時計の同期	正確な記録のために、コンピュータ内の時計を同期させておくこと。
9.(8) 移動型計算処理及び遠隔作業		
管理目的：移動型計算処理（mobile computing）及び遠隔作業（teleworking）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。		
管理策		
9.(8)	移動型計算処理	移動型計算処理の設備（ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話等）を用いた作業、特に保護されていない環境における作業のリスクから保護するために、正式な個別方針を持ち、適切な管理策を採用すること。
9.(8)	遠隔作業	遠隔作業を認可し及び管理するための個別方針、手順及び標準類を策定すること。

10. システムの開発及び保守

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)	セキュリティ要求事項の分析及び明示	新しいシステム又は既存のシステムの改善に関する業務上の要求事項では、管理策についての要求事項を明記すること。
10.(2) 業務用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)	入力データの妥当性確認	業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること。
10.(2)	内部処理の管理	処理したデータの改ざんを検出するために、システムに妥当性の検査を組み込むこと。
10.(2)	メッセージ認証	重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合は、メッセージ認証を使用すること。
10.(2)	出力データの妥当性確認	業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること。
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)	暗号による管理策の使用に関する個別方針	情報を保護するための暗号による管理策の使用について、個別方針を定めること。
10.(3)	暗号化	取扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化を用いること。
10.(3)	デジタル署名	電子的な情報（電子文書等）の真正性及び完全性を保護するために、デジタル署名を用いること。
10.(3)	否認防止サービス	事象又は動作が起こったか、起こらなかったかについての紛争の解決には、否認防止サービスを用いること。
10.(3)	かぎ管理	一連の合意された標準類、手順及び方法に基づくかぎ管理システムを、暗号技術の利用を支援するために用いること。

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)	運用ソフトウェアの管理	運用システムでのソフトウェアの実行を管理する手順を持つこと。
10.(4)	システム試験データの保護	試験データは保護され、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制御	プログラムソースライブラリへのアクセス全体にわたって、厳しい管理を維持すること。
10.(5) 開発及び支援過程におけるセキュリティ		
管理目的：業務用システム及び情報のセキュリティを維持するため。		
管理策		
10.(5)	変更管理手順	正式な変更管理手順によって、情報システムの変更の実施を厳しく管理すること。
10.(5)	オペレーティングシステムの変更の技術的レビュー	オペレーティングシステムを変更する場合は、業務用システムをレビューし、試験すること。
10.(5)	パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は極力行わないようにし、絶対に必要な変更は厳しく管理すること。
10.(5)	隠れチャンネル及びトロイの木馬	隠れチャンネル (Covert channels) 又はトロイの木馬 (Trojan code) の危険性から保護するために、ソフトウェアの購入、使用及び修正を管理し、検査すること。
10.(5)	外部委託によるソフトウェア開発	外部委託によるソフトウェア開発をセキュリティの保たれたものとするための管理策を適用すること。

11. 事業継続管理

<p>11.(1) 事業継続管理の種々の面</p> <p>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手続を保護するため。</p>		
<p>管理策</p>		
11.(1)	事業継続管理手続	組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること。
11.(1)	事業継続及び影響分析	事業継続に対する全般的取組方法のために、適切なリスクアセスメントに基づいた戦略計画を立てること。
11.(1)	継続計画の作成及び実施	事業運営を、重要な業務手続の中断又は障害の後、適切な時間内で維持又は復旧させるための計画を立てること。
11.(1)	事業継続計画作成のための枠組み	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、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること。
11.(1)	事業継続計画の試験、維持及び再評価	事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために定期的に試験をし、定期的な見直しをすること。

12. 適合性

12.(1) 法的要求事項への適合 管理目的：刑法及び民法、その他の法令、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)	適用法令の識別	各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること。
12.(1)	知的所有権（IPR）	知的所有権がある物件及びソフトウェア製品を使用する場合は、法的制限事項に適合するように、適切な手続を実行すること。
12.(1)	組織の記録の保護	組織の重要な記録は、消失、破壊及び改ざんから保護されること。
12.(1)	データの保護及び個人情報保護	関連法令に従って個人情報を保護するために、管理策を適用すること。
12.(1)	情報処理施設の誤用の防止	情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐための管理策を用いること。
12.(1)	暗号による管理策の規制	暗号による管理策へのアクセス又はその使用を統制することを目的とした、国による協定、法律、規制、又はその他の手段に、適合することを可能にするために、管理策を用いること。
12.(1)	証拠の収集	人又は組織に対する措置が、民事であれ刑事であれ、法律にかかわるものである場合、提示する証拠は、関連法令又は事件の審理が行われる特定の法廷の規則に定められた証拠に関する規定に適合させること。また、容認される証拠を作成するために、公表されている標準類又は実践規範に適合すること。
12.(2) セキュリティ基本方針及び技術適合のレビュー 管理目的：組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため。		
管理策		
12.(2)	セキュリティ基本方針との適合	管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること。組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的に見直すこと。
12.(2)	技術適合の検査	情報システムは、セキュリティ実行標準と適合していることを定期的に検査すること。

12.(3) システム監査の考慮事項

管理目的：システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため。

管理策

12.(3)	システム監査管理策	運用システムの監査は業務手続の中断のリスクを最小限に抑えるように慎重に計画を立て、合意されること。
12.(3)	システム監査ツールの保護	システム監査ツールは、誤用又は悪用を防止するために、保護されること。

参考資料 ISMS 認証基準(Ver.1.0)との対応表

ISMS認証基準(Ver2.0)		ISMS認証基準(Ver1.0)	
項番	条文	項番	条文
第0	序文	-	
第0.1.	<p>一般</p> <p>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。従って、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ことが期待される。</p> <p>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、内部の者及び審査登録機関を含む外部の者が評価するために使用することができる。</p>		
第0.2.	<p>プロセスアプローチ</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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明確に認識するようになる。</p>		
第0.2.	事業上の情報セキュリティ要求事項を理解し、情報セキュリティ基本方針及び目標を確立する必要性を理解すること。		
第0.2.	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。		
第0.2.	ISMSの実施状況及び有効性を監視し、見直すこと。		
第0.2.	客観的な測定結果に基づいて継続的に改善すること。		
	<p>本基準で採用されているモデルは、「Plan-Do-Check-Act(計画-実施-点検-処置)」（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、利害関係者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、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。</p> <p>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。</p> <p>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。</p> <p>参考 情報セキュリティでは、「手順」という用語は、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。</p>		
	<p>図1-ISMSプロセスに適用されるPDCAモデル</p>		

ISMS認証基準(Ver2.0)		ISMS認証基準(Ver1.0)									
項番	条文	項番	条文								
	<table border="1"> <tr> <td>Plan・計画 (ISMSの確立)</td> <td>組織の全般的な基本方針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訂に関する情報セキュリティ基本方針、目標、対策、プロセス及び手順を確立する。</td> </tr> <tr> <td>Do・実施 (ISMSの導入及び運用)</td> <td>その情報セキュリティ基本方針、目標、対策、プロセス及び手順を確立し運用する。</td> </tr> <tr> <td>Check・点検 (ISMSの監視及び見直し)</td> <td>情報セキュリティ基本方針、目標及び対策の達成に照らしてプロセスの達成状況を評価し、可能な場合にこれを測定し、その結果を見直しのために改善案に報告する。</td> </tr> <tr> <td>Act・処置 (ISMSの維持及び改訂)</td> <td>ISMSの継続的改善を遂行するために、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。</td> </tr> </table>	Plan・計画 (ISMSの確立)	組織の全般的な基本方針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訂に関する情報セキュリティ基本方針、目標、対策、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基本方針、目標、対策、プロセス及び手順を確立し運用する。	Check・点検 (ISMSの監視及び見直し)	情報セキュリティ基本方針、目標及び対策の達成に照らしてプロセスの達成状況を評価し、可能な場合にこれを測定し、その結果を見直しのために改善案に報告する。	Act・処置 (ISMSの維持及び改訂)	ISMSの継続的改善を遂行するために、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。		
Plan・計画 (ISMSの確立)	組織の全般的な基本方針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訂に関する情報セキュリティ基本方針、目標、対策、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基本方針、目標、対策、プロセス及び手順を確立し運用する。										
Check・点検 (ISMSの監視及び見直し)	情報セキュリティ基本方針、目標及び対策の達成に照らしてプロセスの達成状況を評価し、可能な場合にこれを測定し、その結果を見直しのために改善案に報告する。										
Act・処置 (ISMSの維持及び改訂)	ISMSの継続的改善を遂行するために、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。										
第03.	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導入・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	第1	適用範囲								
第11.	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、十分に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。		本基準は、情報セキュリティマネジメントシステム（以下、「ISMS」という）の確立、実施及び文書化についての要求事項を明記する。 <参考> 本基準（ISMS認証基準）の第4に規定する詳細管理策は、JIS X 5080（ISO/IEC 17799）を参照しており、これと整合するものとなっている。JIS X 5080（ISO/IEC 17799）は、本基準の要求事項の実施を支援する最良な実践（Best Practice）を推奨するものである。								
第12.	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。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。また、組織やその事業の性質によって、本基準の附属書「詳細管理策」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。										
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 JIS Q 9001:2000 品質マネジメントシステム - 要求事項 TR Q 0008:2003 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										
第3	用語及び定義	第2	用語及び定義								
	本基準の目的のために、次に掲げる用語及び定義を適用する。										
第31.	可用性 (availability) 認可された利用者が、必要ときに、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を参照]										
第32.	機密性 (confidentiality) アクセスを認可された(authorized)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を参照]										
第33.	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維持。 [JIS X 5080:2002を参照]	第2(1)	情報セキュリティ 情報の機密性、完全性及び可用性を確保し維持すること。 機密性：アクセスを認可された者だけが、情報にアクセスできることを確実にすること。 完全性：情報及び処理方法が正確であること及び完全であることを保護すること。 可用性：認可された利用者が、必要ときに、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。								

ISMS認証基準(Ver.20)		ISMS認証基準(Ver.10)	
項番	条文	項番	条文
第3.4.	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、及び方針、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。		
第3.5.	完全性 (integrity) 情報及び処理方法が、正確であること及び完全であることを保護すること。 [JIS X 5080:2002を参照]		
第3.6.	リスクの受容 (risk acceptance) リスクを受容する意思決定。 [TR Q 0008:2003を参照]		
第3.7.	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を参照] 参考 リスク因子(source) : 結果をもたらす可能性が潜在する物事や行動。 [TR Q 0008:2003を参照]		
第3.8.	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すべてのプロセス。 [TR Q 0008:2003を参照]	第2(2)	リスク評価 情報や情報処理施設等に対する脅威及びその脅威への脆弱性を分析し、その結果からリスクが顕在化する可能性及び顕在化した場合の事業への影響度を検証すること。
第3.9.	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基準と比較するプロセス。 [TR Q 0008:2003を参照]		
第3.10.	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。 [TR Q 0008:2003を参照]		
第3.11.	リスク対応 (risk treatment) リスクを変更させるための方策を、選択及び実施するプロセス。 [TR Q 0008:2003を参照]		
第3.12.	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き、組織のISMSに適切で当てはまる管理目的及び管理策を記述した文書。	第2(3)	適用宣言書 組織の必要性に基づき、本基準の第4詳細管理策の選択可否と選択しない場合の理由、並びに必要に応じ追加した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	第3	ISMSの要求事項
第4.1.	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。	第3(1)	一般
		第3(1)	組織は以下の項目を明確にしたISMSを確立し維持すること。
		第3(1) (ア)	保護すべき情報資産
		第3(1) (イ)	リスクマネジメントに対する組織の取組方法
		第3(1) (ウ)	管理目的及び管理策の内容
第3(1) (エ)	保護すべき情報資産に要求される保証の度合い		
第4.2.	ISMSの確立及び運営管理	第3(2)	マネジメント枠組みの確立
第4.2(1)	ISMSの確立 組織は次の事項を実施すること。	第3(2)	組織の必要性に基づき、管理目的及び管理策の内容を明確にすること。
		第3(2)	の目的及び内容を文書化するために以下の作業を実施すること。
		第3(2) (イ)	ISMSの適用範囲の決定
第4.2(1)	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。	第3(2) (ア)	情報セキュリティポリシーの策定
第4.2(1) (フ)	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。		
第4.2(1) (ク)	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。		
第4.2(1) (ケ)	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。		
第4.2(1) (コ)	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) 。		
第4.2(1) (カ)	経営陣による承認を得る。		

ISMS認証基準(Ver2.0)		ISMS認証基準(Ver1.0)	
項番	条文	項番	条文
第4.2.(1)	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）。	第3(2) (ウ)	リスク評価
第4.2.(1)	リスクを識別する。		
第4.2.(1) (F)	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。		
第4.2.(1) (I)	それらの情報資産に対する脅威を明確にする。		
第4.2.(1) (Q)	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。		
第4.2.(1) (I)	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。		
第4.2.(1)	リスクアセスメントを実施する。		
第4.2.(1) (F)	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、完全性及び可用性の喪失による潜在的な影響を考慮する。		
第4.2.(1) (I)	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。		
第4.2.(1) (Q)	リスクの度合いを算定する。		
第4.2.(1) (I)	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。	第3(2) (エ)	リスクマネジメントの対象範囲の決定
第4.2.(1)	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。		
第4.2.(1) (F)	適切な管理策を採用する。		
第4.2.(1) (I)	リスクを保有する。リスクが組織の基本方針及びリスクの受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容する（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。 [TR Q 0008:2003を参照]		
第4.2.(1) (Q)	リスクを回避する。		
第4.2.(1) (I)	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。	第3(2) (オ)	本基準の第4 詳細管理策及び必要に応じ追加した管理策の選択
第4.2.(1)	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」のリストは組織が必要とする管理目的及び管理策の全てとは限らないので、組織は必要に応じて追加の管理目的及び管理策を選択してもよい。		
第4.2.(1)	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、適用宣言書に含めること。また、附属書「詳細管理策」に記載する管理目的及び管理策の中から適用除外としたものは記録すること。		
第4.2.(1)	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。	第3(2) (カ)	適用宣言書の作成
第4.2.(2)	ISMSの導入及び運用 組織は次の事項を実施すること。	第3(3)	管理策の実施
第4.2.(2)	情報セキュリティについてのリスクを管理するための、経営陣の適切な活動、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）。	第3(3)	第3(2) (ウ)で選択した管理策を実施すること。
第4.2.(2)	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。		
第4.2.(2)	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。		
第4.2.(2)	教育・訓練及び認識させるためのプログラムを実施する（第5.2.(2)参照）。		
第4.2.(2)	運用を管理する。		
第4.2.(2)	経営資源を管理する（第5.2参照）。		

ISMS認証基準(Ver2.0)		ISMS認証基準(Ver1.0)	
項番	条文	項番	条文
第4.2.(2)	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。		
第4.2.(3)	ISMSの監視及び見直し 組織は次の事項を実施すること。	第3(3)	管理策を実施するために採用した手順について、第4.10(2)に従いその有効性を確認すること。
第4.2.(3)	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。		
第4.2.(3) (7)	処理結果から誤りを速やかに検出する。		
第4.2.(3) (4)	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。		
第4.2.(3) (9)	人又は情報技術によって導入された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。		
第4.2.(3) (I)	セキュリティ違反を解決するためにとるべき処置を、事業上の優先順位を踏まえて決定する。		
第4.2.(3)	当該ISMSの有効性に関して定期的な見直しを実施する（情報セキュリティ基本方針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。		
第4.2.(3)	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。		
第4.2.(3) (7)	組織。		
第4.2.(3) (4)	技術。		
第4.2.(3) (9)	事業の目標及びプロセス。		
第4.2.(3) (I)	識別された脅威。		
第4.2.(3) (オ)	外部の事象。例えば、法的又は規制環境や社会環境など。		
第4.2.(3)	あらかじめ定められた間隔でISMSの内部監査を実施する。		
第4.2.(3)	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）。		
第4.2.(3)	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）。		
第4.2.(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。	第3(2)	マネジメント枠組みを維持・改善するため、の各項目について、定期的及び必要に応じて見直すこと。
第4.2.(4)	識別されたISMSの改善策を実施する。		
第4.2.(4)	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。		
第4.2.(4)	利害関係者全てに結果及び講じた処置を伝達し、可能な限り合意を得る。		
第4.2.(4)	改善が、その意図した目標を確実に達成するようにする。		
第4.3.	文書化に関する要求事項	第3(4)	文書化
第4.3.(1)	一般 ISMS文書には、次の事項を含めること。	第3(4)	以下の内容を包含するものを文書化し、ISMS文書として維持すること。
第4.3.(1)	情報セキュリティ基本方針（第4.2.(1) 参照）及び管理目的の表明。	第3(4) (イ)	第3(2)で確立したマネジメント枠組みの要約
第4.3.(1)	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。	第3(4) (ウ)	第3(3)の管理策を実施するために採用した手順及びその実施責任と関連する作業内容
第4.3.(1)	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）。		
第4.3.(1)	リスク対応計画（第4.2.(2) 参照）。		
第4.3.(1)	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3(4) (エ)	ISMSを運用するための手順とそれらの実施責任及び関連する作業内容
第4.3.(1)	本基準が要求する記録（第4.3.(3)参照）。	第3(4) (ア)	第3(2)の作業の証拠
第4.3.(1)	適用宣言書(第4.2.(1) 参照)。 文書は全て、ISMSの基本方針の要求に応じて利用できるようにしておくこと。		

ISMS認証基準(Ver.20)		ISMS認証基準(Ver.10)	
項番	条文	項番	条文
	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p>		
第4.3(2)	<p>文書管理</p> <p>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。</p>	第3(5)	文書管理
		第3(5)	第3(4)のISMS文書を管理するため、以下の条件を満たす手順を定め、維持すること。
第4.3(2)	発行前に、適切かどうかの観点から文書を承認する。		
第4.3(2)	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。	第3(5) (イ)	ISMS文書の定期的な見直しを行い、情報セキュリティポリシーに対する準拠性を維持しながら必要に応じて改訂する
第4.3(2)	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。	第3(5) (ウ)	ISMS文書の更新履歴を管理する
第4.3(2)	該当する文書の最新版が、必要ときに、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。	第3(5) (エ)	ISMSの運用に関わる全ての事業所等において、必要なISMS文書が閲覧可能である
第4.3(2)	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。	第3(5) (ア)	ISMS文書の利用者が文書を容易に利用することができる
第4.3(2)	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。		
第4.3(2)	文書の配付が適切に管理されていることを確実にする。		
第4.3(2)	廃止文書が誤って使用されないようにする。	第3(5) (オ)	ISMS文書の一部について、その必要性がなくなったり、別途新たな文書が作成された場合に、当該ISMS文書が速やかに廃止される
第4.3(2)	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。	第3(5) (カ)	(オ)の廃止にかかわらず、法規制等による要請がある場合や専門知識を蓄積するために、必要に応じてISMS文書が保管される
第4.3(3)	<p>記録の管理</p> <p>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策を文書化すること。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。</p> <p>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。</p> <p>記録の例 訪問者の記録、監査記録及びアクセスの承認記録など。</p>	第3(6)	記録
		第3(6)	第3(1)から(5)の内容に対する準拠状況を保証するために必要な記録を特定すること。
		第3(6)	で特定した記録を管理する手順を定め、必要に応じて見直すこと。
		第3(6)	で特定した記録に対し、損傷、劣化、紛失、消失を防止するための措置を講ずること。
第5	経営陣の責任	-	
第5.1.	<p>経営陣のコミットメント</p> <p>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。</p>		
第5.1.	情報セキュリティ基本方針を確立する。		
第5.1.	情報セキュリティ目標が設定され、計画が策定されることを確実にする。		
第5.1.	情報セキュリティに対する役割及び責任を定める。		
第5.1.	情報セキュリティ目標を達成することの重要性及び情報セキュリティ基本方針に適合することの重要性、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。		
第5.1.	ISMSの確立、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）。		
第5.1.	リスクの受容可能な水準を決める。		
第5.1.	ISMSのマネジメントレビューを実施する（第6参照）。		
第5.2.	経営資源の運用管理		
第5.2(1)	<p>経営資源の提供</p> <p>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。</p>		
第5.2(1)	ISMSを確立、導入、運用及び維持する。		

ISMS認証基準(Ver.20)		ISMS認証基準(Ver.10)	
項番	条文	項番	条文
第5.2.(1)	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。		
第5.2.(1)	法的及び規制要求事項と契約上の情報セキュリティに関する義務を識別し、適切に対処する。		
第5.2.(1)	実施される全ての管理策を的確に適用することにより、十分な情報セキュリティを維持する。		
第5.2.(1)	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。		
第5.2.(1)	必要な場合には、ISMSの有効性を改善する。		
第5.2.(2)	教育・訓練、認識及び力量 組織は、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確実にすること。		
第5.2.(2)	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。		
第5.2.(2)	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。		
第5.2.(2)	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。		
第5.2.(2)	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すること。		
第6	マネジメントレビュー	-	
第6.1.	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、情報セキュリティ基本方針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、その記録を維持すること(第4.3.(3)参照)。		
第6.2.	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。		
第6.2.	監査及びレビューの結果。		
第6.2.	利害関係者からのフィードバック。		
第6.2.	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。		
第6.2.	予防処置及び是正処置の状況。		
第6.2.	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。		
第6.2.	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。		
第6.2.	ISMSに影響を及ぼす可能性のある全ての変更。		
第6.2.	改善のための提案。		
第6.3.	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。		
第6.3.	ISMSの有効性の改善。		
第6.3.	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。それらの事象には、次の事項に対する変更が含まれる。		
第6.3.(7)	事業上の要求事項。		
第6.3.(1)	情報セキュリティ要求事項。		
第6.3.(9)	既存の事業上の要求事項を満たす業務プロセス。		
第6.3.(I)	規制環境又は法的環境。		
第6.3.(オ)	リスクの度合い及びリスク受容の水準。		
第6.3.	必要となる経営資源。		

ISMS認証基準/Ver.20		ISMS認証基準/Ver.10	
項番	条文	項番	条文
第6.4.	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。		
第6.4.	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。		
第6.4.	識別された情報セキュリティ要求事項に適合していること。		
第6.4.	有効に実施され維持されていること。		
第6.4.	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を監査しないこと。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	-	
第7.1.	継続的改善 組織は、情報セキュリティ基本方針、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。		
第7.2.	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。		
第7.2.	ISMSの導入及び運用における不適合の識別。		
第7.2.	不適合の原因の特定。		
第7.2.	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。		
第7.2.	必要な是正処置の決定及び実施。		
第7.2.	実施した処置の結果の記録（第4.3.(3)参照）。		
第7.2.	実施した是正処置のレビュー。		
第7.3.	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。		
第7.3.	起こり得る不適合及び原因の識別。		
第7.3.	必要な予防処置の決定及び実施。		
第7.3.	実施した処置の結果の記録（第4.3.(3)参照）。		
第7.3.	実施した予防処置のレビュー。		
第7.3.	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。		

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
1.	はじめに	-	
	3.から12.に記載する管理目的及び管理策のリストは、JIS X 5080:2002を参照している。本基準の第4 2.(1)で規定されたISMSのプロセスの一部として、下記のリストから管理目的及び管理策を選択すること。ただし、このリストは組織が必要とする管理目的及び管理策の全てとは限らないので、組織は必要に応じて追加の管理目的及び管理策を選択してもよい。		
2.	実践規範への手引き	-	
	JIS X 5080:2002の3.から12.は、附属書の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.	情報セキュリティ基本方針	1.	セキュリティポリシー
3.(1)	情報セキュリティ基本方針 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。	1.(1)	情報セキュリティポリシー
3.(1)	情報セキュリティ基本方針文書 基本方針文書は、経営陣によって承認され、適当な手段で、全従業員に公表し、通知すること。	1.(1)	情報セキュリティポリシーは、経営陣により承認及び制定されること。
		1.(1)	情報セキュリティポリシーは、必要な関係者全員に公表されること。
3.(1)	見直し及び評価 基本方針は、依然として適切であることを確実にするために、定期的に、また影響を及ぼす変化があった場合に、見直すこと。	1.(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.	組織のセキュリティ	2.	セキュリティ組織
4.(1)	情報セキュリティ基盤 管理目的：組織内の情報セキュリティを管理するため。	2.(1)	情報セキュリティ・インフラストラクチャ
4.(1)	情報セキュリティ運営委員会 セキュリティを主導するための明りょう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に、運営委員会を設置すること。運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること。	2.(1)	経営陣が情報セキュリティについて討論する委員会を設置すること。
4.(1)	情報セキュリティの調整 大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を利用すること。	2.(1)	組織内の情報セキュリティを管理するため、関連する部門を横断的に調整する部門等を設けること。
4.(1)	情報セキュリティ責任の割当て 個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を、明確に定めること。	2.(1)	個々の情報資産に対する保護責任及び特定の業務に関する実施責任を明確にすること。
4.(1)	情報処理設備の認可手続 新しい情報処理設備に対する経営陣による認可手続を確立すること。	2.(1)	情報処理施設及び設備の新規導入に対する経営陣による承認プロセスを定めること。
4.(1)	専門家による情報セキュリティの助言 専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること。	2.(1)	情報セキュリティに関して、適宜社内または社外の専門家から助言を受け、その内容を組織内に公表すること。
4.(1)	組織間の協力 行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること。	2.(1)	監督官庁、規制当局及びセキュリティ上重要な役割を担う外部組織への連絡体制を維持すること。
4.(1)	情報セキュリティの他者によるレビュー 情報セキュリティ基本方針の実施を、他者がレビューすること。	2.(1)	情報セキュリティポリシーの導入や運用の状況を客観的視点で見直すこと。
4.(2)	第三者による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。	2.(2)	第三者アクセスのセキュリティ
4.(2)	第三者のアクセスから生じるリスクの識別 組織の情報処理施設への第三者のアクセスに関連づけてリスクアセスメントを実施し、適切なセキュリティ管理策を実施すること。	2.(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)	第三者との契約書に記載するセキュリティ要求事項 組織の情報処理施設への第三者アクセスにかかわる取決めは、必要なセキュリティ要求事項すべてを含んだ正式な契約に基づくこと。	2.(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、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。
4.(3)	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。	2.(3)	第三者への委託（アウトソーシングや外部委託）

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
4.(3)	外部委託契約におけるセキュリティ要求事項 情報システム、ネットワーク及び/又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述されること。	2.(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.	資産の分類及び管理	3.	情報資産の分類及び管理
5.(1)	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。	3.(1)	情報資産に対する責任
5.(1)	資産目録 情報システムそれぞれに関連づけてすべての重要な資産について目録を作成し、維持すること。	3.(1)	情報資産を適切に管理するため資産台帳を作成し、重要な情報資産のすべてを登録すること。
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。	3.(2)	情報の分類
5.(2)	分類の指針 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮に入れておくこと。	3.(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)	情報のラベル付け及び取扱い 組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること。	3.(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	4.	人的セキュリティ
6.(1)	職務定義及び雇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。	4.(1)	職務定義および採用におけるセキュリティ
6.(1)	セキュリティを職責に含めること 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で定められたとおりに、職務定義のなかに文書化すること。	4.(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)	要員審査及びその個別方針 常勤職員、請負業者及び臨時職員を採用するときは、提出された応募資料の内容を検査すること。	4.(1)	採用する人員に求める資質や職能を明確にすること。
6.(1)	機密保持契約 従業員は、入社時の雇用条件の一部として、機密保持契約書に署名すること。	4.(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 雇用条件には、情報セキュリティに対する従業員の責任について記述してあること。	4.(1)	人員を採用する際、被雇用者に対し情報セキュリティに関する役割及び責任を明示すること。
6.(2)	利用者の訓練 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かなものとし、通常の仕事の中で利用者が組織のセキュリティ基本方針を維持していくことを確実にするため。	4.(2)	ユーザの教育・訓練
6.(2)	情報セキュリティの教育及び訓練 組織の基本方針及び手順について、組織のすべての従業員及び関係するならば外部利用者を適切に教育すること、並びに定期的に更新教育を行うこと。	4.(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：セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため。	4.(3)	セキュリティ事故及び誤動作への対処
6.(3)	セキュリティ事件・事故の報告 セキュリティ事件・事故は、適切な連絡経路をとおして、できるだけ速やかに報告すること。	4.(3)	発見したセキュリティ事故を迅速に報告するため、経営陣を含めた連絡網を設置すること。
6.(3)	セキュリティの弱点の報告 システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合に、情報サービスの利用者に対して、注意を払い、かつ、報告するよう要求すること。	4.(3)	セキュリティ事故やそれに準ずる出来事を見つけ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)	ソフトウェアの誤動作の報告 ソフトウェア誤動作を報告する手順を確立すること。	4.(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)	事件・事故からの学習 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを備えていること。	4.(3)	発見したセキュリティ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)	懲戒手続 従業員による組織のセキュリティ基本方針及び手順への違反は、正式な懲戒手続によって処理すること。	4.(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。

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
7.	物理的及び環境的セキュリティ	5.	物理的及び環境的セキュリティ
7.(1)	セキュリティが保たれた領域 管理目的：業務施設及び業務情報に対する認可されていない物理的なアクセス、損傷及び妨害を防止するため。	5.(1)	セキュリティ区画
7.(1)	物理的セキュリティ境界 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること。	5.(1)	情報処理施設及び設備は、他の区画と明確に分離したセキュリティ区画に設置され、適切に保護されること。
7.(1)	物理的入退管理策 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セキュリティの保たれた領域を保護すること。	5.(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)	オフィス、部屋及び施設のセキュリティ 特別なセキュリティ要求事項のあるオフィス、部屋及び施設を保護するために、セキュリティの保たれた領域を設定すること。	5.(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建設されること。
7.(1)	セキュリティが保たれた領域での作業 セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加すること。	5.(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、ガイドラインを整備すること。
7.(1)	受渡し場所の隔離 品物を受渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること。	5.(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。	5.(2)	装置のセキュリティ
7.(2)	装置の設置及び保護 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置又は保護すること。	5.(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)	電源 装置は、停電、その他の電源異常から保護すること。	5.(2)	装置を許可されないアクセスから保護すること。
7.(2)	ケーブル配線のセキュリティ データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること。	5.(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)	装置の保守 装置についての継続的な可用性及び完全性の維持を可能とするために、装置を正しく保守すること。	5.(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)	事業敷地外における装置のセキュリティ 組織の敷地外で情報処理のために装置を使用するいかなる場合も、管理者による認可を要求すること。	5.(2)	装置を使用する際、装置製造業者が提供する取扱い説明書や手順書に従い、装置の可用性及び完全性を確実に維持すること。
7.(2)	装置の安全な処分又は再利用 装置を処分又は再利用する前に、情報を装置から消去すること。	5.(2)	装置を組織の敷地外で利用する際、適切に保護するための手順を定め、必要な措置を講ずること。
7.(2)	装置の安全な処分又は再利用 装置を処分又は再利用する前に、情報を装置から消去すること。	5.(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)	その他の管理策 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。	5.(3)	一般管理策
7.(3)	クリアデスク及びクリアスクリーンの個別方針 組織は、情報への認可されていないアクセス、情報の消失及び損傷のリスクを軽減するための、クリアデスク方針及びクリアスクリーン方針を持つこと。	5.(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)	資産の移動 組織に属する装置、情報又はソフトウェアは、管理者による認可なしでもち出さないこと。	5.(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)	資産の移動 組織に属する装置、情報又はソフトウェアは、管理者による認可なしでもち出さないこと。	5.(3)	組織が所有する装置や情報、ソフトウェア等を承認なしに組織外へ持ち出さないこと。
8.	通信及び運用管理	6.	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。	6.(1)	運用手順及び責任
8.(1)	操作手順書 セキュリティ個別方針によって明確化した操作手順は、文書化して維持すること。	6.(1)	第3(1)(ウ)にある管理目的及び管理策に従い特定した操作手順を文書化し維持すること。
8.(1)	運用変更管理 情報処理設備及びシステムの変更について管理すること。	6.(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。

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
8.(1)	事件・事故管理手順 セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うために、および監査証跡及び記録といった事件・事故に関連するデータを収集するために、事件・事故管理の責任及び手順を確立すること。	6.(1)	セキュリティ事故を管理する責任体制及び手順を定めること。
8.(1)	職務の分離 情報若しくはサービスの無許可の変更又は誤用の可能性を小さくするために、職務及び責任領域を分離すること。	6.(1)	情報や情報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)	開発施設と運用施設との分離 開発施設及び試験施設は、運用施設から分離すること。ソフトウェアの開発から運用の段階への移行についての規則は、明確に定め、文書化すること。	6.(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。
8.(1)	外部委託による施設管理 外部委託による施設管理サービスを利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること。	6.(1)	外部の施設管理サービスを利用する場合、リスクを考慮し適切な措置を決定した上で、この内容を明記した正式な契約を締結すること。
8.(2)	システムの計画作成及び受け入れ 管理目的：システム故障のリスクを最小限に抑えるため。	6.(2)	システム計画の作成及び受け入れ
8.(2)	容量・能力の計画作成 十分な処理能力及び記憶容量の利用を可能にするために、容量・能力の需要を監視し、将来必要とされる容量・能力を予測すること。	6.(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)	システムの受け入れ 新しい情報システム、改訂版及び更新版の受け入れ基準を確立し、その受け入れ前に適切な試験を実施すること。	6.(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)	悪意のある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、悪意のあるソフトウェアによる被害から保護するため。	6.(3)	不正ソフトウェアからの保護
8.(3)	悪意のあるソフトウェアに対する管理策 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること。	6.(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、適宜ユーザの教育・訓練を実施すること。
8.(4)	システムの維持管理 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。	6.(4)	情報システム管理
8.(4)	情報のバックアップ 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること。	6.(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に取得すること。
8.(4)	運用の記録 運用担当者は、自分の作業の記録を継続すること。運用担当者の記録は、定期的に独立した検査を受けること。	6.(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。
8.(4)	障害記録 障害については報告を行い、是正処置をとること。	6.(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。	6.(5)	ネットワークの管理
8.(5)	ネットワーク管理策 ネットワークにおけるセキュリティを実現し、かつ、維持するために一連の管理策を実施すること。	6.(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：財産に対する損害及び事業活動に対する妨害を回避するため。	6.(6)	媒体の取扱い及びセキュリティ
8.(6)	コンピュータの取外し可能な付属媒体の管理 コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書を管理すること。	6.(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)	媒体の処分 媒体が不要となった場合は、安全、かつ、確実に処分すること。	6.(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)	情報の取扱手順 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管に関する手順を確立すること。	6.(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)	システムに関する文書のセキュリティ 認可されていないアクセスからシステムに関する文書を保護すること。	6.(6)	情報システムに関するドキュメントを許可されないアクセスから保護すること。
8.(7)	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。	6.(7)	組織間における情報及びソフトウェアの交換

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
8.(7)	情報及びソフトウェアの交換契約 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと。	6.(7)	取引先や協業相手等と情報を交換する場合、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)	配送中の媒体のセキュリティ 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること。	6.(7)	移送中の媒体を許可されないアクセス、誤用及び改ざんから保護すること。
8.(7)	電子商取引のセキュリティ 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること。	6.(7)	電子取引を行う場合、詐欺行為、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)	電子メールのセキュリティ 電子メールの使用に関する個別方針を作成し、電子メールがもたらすセキュリティ上のリスクを軽減するための管理策を実施すること。	6.(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セキュリティ オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること。	6.(7)	電子機器の使用に関するポリシー及びガイドラインを定め、電子機器の使用に関連したリスクを抑制すること。
8.(7)	公開されているシステム 情報を公開する前に正式な認可の手続がとられ、また、情報の改ざんを防止するために公開した情報の完全性を保護すること。	6.(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許可の手順を定めること。
8.(7)	情報交換のその他の方式 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、個別方針、手順及び管理策をもつこと。	6.(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、その手順を定め、必要な措置を講ずること。
9.	アクセス制御	7.	アクセス制御
9.(1)	アクセス制御に関する業務上の要求事項 管理目的：情報へのアクセスを制御するため。	7.(1)	アクセス制御に関する事業の要求事項
9.(1)	アクセス制御方針 アクセス制御についての業務上の要求事項を定義して文書化し、アクセスをアクセス制御方針で定義されたものに限定すること。	7.(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。
		7.(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)	利用者のアクセス管理 管理目的：情報システムへのアクセス権が、適切に認可され、割り当てられ、維持されていることを確実にするため。	7.(2)	ユーザアクセス管理
9.(2)	利用者登録 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること。	7.(2)	情報システムユーザの登録及び登録抹消の手順を定めること。
9.(2)	特権管理 特権の割当て及び使用は、制限し、管理すること。	7.(2)	特権の割当て及び使用を制限し管理すること。
9.(2)	利用者のパスワードの管理 パスワードの割当ては、正規の管理手続によって統制すること。	7.(2)	情報システムユーザ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)	利用者アクセス権の見直し 経営陣は、利用者のアクセス権を見直す正規の手順を、定期的実施すること。	7.(2)	情報システムユーザのアクセス権を定期的に見直すこと。
9.(3)	利用者の責任 管理目的：認可されていない利用者のアクセスを防止するため。	7.(3)	ユーザの責任
9.(3)	パスワードの使用 パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うことを、利用者に要求すること。	7.(3)	パスワードを設定及び使用する際、情報セキュリティ上の問題を考慮すること。
9.(3)	利用者領域にある無人運転の装置 無人運転の装置に適切な保護対策を備えていることを確実にするように、利用者に要求すること。	7.(3)	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ための措置を講ずること。
9.(4)	ネットワークのアクセス制御 管理目的：ネットワークを介したサービスの保護のため。	7.(4)	ネットワークのアクセス制御
9.(4)	ネットワークサービスの使用についての個別方針 利用者には、使用することが特別に認可されたサービスへの直接のアクセスだけを提供すること。	7.(4)	明確に許可されたサービス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。

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
9.(4)	指定された接続経路 利用者端末からコンピュータサービスまでの経路は、管理すること。	7.(4)	情報システムの利用者がコンピュータの各サービス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)	外部から接続する利用者の認証 遠隔地からの利用者のアクセスには、認証を行うこと。	7.(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、ユーザ認証を行うこと。
9.(4)	ノードの認証 遠隔コンピュータシステムへの接続は、認証されること。	7.(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)	遠隔診断用ポートの保護 診断ポートへのアクセスは、セキュリティを保つように制御されること。	7.(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)	ネットワークの領域分割 情報サービス、利用者及び情報システムのグループを分割するための制御を、ネットワーク内に導入すること。	7.(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)	ネットワークの接続制御 共有ネットワークにおける利用者の接続の可能性は、アクセス制御方針に従って制限すること。	7.(4)	共有ネットワークへのアクセス権限は、第4 7(1)のアクセス制御ポリシーに従い付与されること。
9.(4)	ネットワーク経路を指定した制御 共有ネットワークは、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、経路指定の制御策を組み込むこと。	7.(4)	共有ネットワークへのアクセスを許可する場合、第4 7(1)の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)	ネットワークサービスのセキュリティ ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けること。	7.(4)	ネットワークに関連する外部のサービスを受ける場合、そのサービスに施されたセキュリティに関する情報入手し、これを文書化すること。
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：認可されていないコンピュータアクセスを防止するため。	7.(5)	オペレーティングシステムのアクセス制御
9.(5)	自動の端末識別 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること。	7.(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)	端末のログオン手順 情報サービスへのアクセスは、安全なログオン手順を使用すること。	7.(5)	情報サービスへのログオンプロセスを明確にすること。
9.(5)	利用者の識別及び認証 すべての利用者は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ID）を保有すること。利用者が主張するIDを確認するための適切な認証技術を選択すること。	7.(5)	情報システムユーザは、個人専用の識別子（ユーザID）を有すること。
9.(5)	パスワード管理システム パスワード管理システムは、質のよいパスワードであることを確実にするための、有効な対話的機能を提供すること。	7.(5)	パスワード管理システムは、情報システムユーザに有効なパスワードを設定させるための対話式的機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を制限すること。
9.(5)	システムユーティリティの使用 システムユーティリティプログラムの使用を制限し、厳しく管理すること。	7.(5)	システム設定プログラムの使用を制限し管理すること。
9.(5)	利用者を保護するための脅迫に対する警報 脅迫の標的となり得る利用者のために、脅迫に対する警報を備えること。	7.(5)	情報へのアクセスに際して、脅迫の対象となり得るユーザを保護するため、脅迫に対して警報を発信する機能を備えること。
9.(5)	端末のタイムアウト機能 リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、認可されていない者によるアクセスを防止するために、一定の活動停止時間の経過後、その端末は遮断されること。	7.(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、その端末をシャットダウンすること。
9.(5)	接続時間の制限 リスクの高い業務用ソフトウェアに対して、追加のセキュリティを提供するために、接続時間に制限を設けること。	7.(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)	業務用ソフトウェアのアクセス制御 管理目的：情報システムが保有する情報への認可されていないアクセスを防止するため。	7.(6)	アプリケーションシステムのアクセス制御
9.(6)	情報へのアクセス制限 情報及び業務用システム機能へのアクセスは、アクセス制御方針に従い、制限されること。	7.(6)	情報及びアプリケーションシステムへのアクセスは、第4 7(1)の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システムの隔離 取扱いに慎重を要するシステムは、専用の（隔離された）コンピュータ環境にあること。	7.(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状況の監視 管理目的：認可されていない活動を検出するため。	7.(7)	システムアクセス及びシステム使用の監視

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
9.(7)	事象の記録 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること。	7.(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)	システム使用状況の監視 情報処理設備の使用状況を監視する手順を確立し、監視の結果を、定期的に見直すこと。	7.(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。
		7.(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)	コンピュータ内の時計の同期 正確な記録のために、コンピュータ内の時計を同期させておくこと。	7.(7)	すべての重要なコンピュータにおいて時刻設定を同期化すること。
9.(8)	移動型計算処理及び遠隔作業 管理目的：移動型計算処理（mobile computing）及び遠隔作業（teleworking）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。	7.(8)	モバイルコンピューティング及び遠隔地勤務
9.(8)	移動型計算処理 移動型計算処理の設備（ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話等）を用いた作業、特に保護されていない環境における作業のリスクから保護するために、正式な個別方針を持ち、適切な管理策を採用すること。	7.(8)	モバイルコンピュータを用いる場合、リスクを考慮し、モバイルコンピュータ使用ポリシーを定めた上で必要な措置を講ずること。
9.(8)	遠隔作業 遠隔作業を認可し及び管理するための個別方針、手順及び標準類を策定すること。	7.(8)	遠隔地勤務を許可する場合、評価されたリスクに基づき、遠隔地勤務ポリシー及び手順を定めること。
10.	システムの開発及び保守	8.	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。	8.(1)	システムのセキュリティ要求事項
10.(1)	セキュリティ要求事項の分析及び明示 新しいシステム又は既存のシステムの改善に関する業務上の要求事項では、管理策についての要求事項を明記すること。	8.(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)	業務用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。	8.(2)	アプリケーションシステムのセキュリティ
10.(2)	入力データの妥当性確認 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること。	8.(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)	内部処理の管理 処理したデータの改ざんを検出するために、システムに妥当性の検査を組み込むこと。	8.(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ざんを検出する機能を備えること。
10.(2)	メッセージ認証 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合は、メッセージ認証を使用すること。	8.(2)	メッセージの完全性を保護する必要がある場合、メッセージが改ざんされていないことを確認する機能を備えること。
10.(2)	出力データの妥当性確認 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること。	8.(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。	8.(3)	暗号による管理策
10.(3)	暗号による管理策の使用に関する個別方針 情報を保護するための暗号による管理策の使用について、個別方針を定めること。	8.(3)	情報を保護するために暗号を用いる場合、リスクを考慮し、暗号使用ポリシーを定めること。
10.(3)	暗号化 取扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化を用いること。	8.(3)	取扱いに慎重を要する情報や重大な情報については、機密性を保護するため暗号化すること。
10.(3)	デジタル署名 電子的な情報（電子文書等）の真正性及び完全性を保護するために、デジタル署名を用いること。	8.(3)	電子情報の真正性及び完全性を保護するため、デジタル署名を適用すること。
10.(3)	否認防止サービス 事象又は動作が起こったか、起こらなかったかについての紛争の解決には、否認防止サービスを用いること。	8.(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)	かぎ管理 一連の合意された標準類、手順及び方法に基づくかぎ管理システムを、暗号技術の利用を支援するために用いること。	8.(3)	情報を保護するために暗号を用いる場合、関連する対策標準類や手順等に準拠し、適切に鍵管理を行うこと。

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
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。	8.(4)	システムファイルのセキュリティ
10.(4)	運用ソフトウェアの管理 運用システムでのソフトウェアの実行を管理する手順を持つこと。	8.(4)	稼働中の情報システムへのアプリケーションソフトウェアの導入は適切に管理されること。
10.(4)	システム試験データの保護 試験データは保護され、管理されること。	8.(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制御 プログラムソースライブラリへのアクセス全体にわたって、厳しい管理を維持すること。	8.(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)	開発及び支援過程におけるセキュリティ 管理目的：業務用システム及び情報のセキュリティを維持するため。	8.(5)	開発及びサポートプロセスにおけるセキュリティ
10.(5)	変更管理手順 正式な変更管理手順によって、情報システムの変更の実施を厳しく管理すること。	8.(5)	情報システムの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の変更の技術的レビュー オペレーティングシステムを変更する場合は、業務用システムをレビューし、試験すること。	8.(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に対する制限 パッケージソフトウェアの変更は極力行わないようにし、絶対に必要な変更は厳しく管理すること。	8.(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)	隠れチャネル及びトロイの木馬 隠れチャネル（Covert channels）又はトロイの木馬（Trojan code）の危険性から保護するために、ソフトウェアの購入、使用及び修正を管理し、検査すること。	8.(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)	外部委託によるソフトウェア開発 外部委託によるソフトウェア開発をセキュリティの保たれたものとするための管理策を適用すること。	8.(5)	ソフトウェア開発をアウトソーシングする場合、リスクを考慮し、それに基づいた正式な契約を締結すること。
11.	事業継続管理	9.	事業継続管理
11.(1)	事業継続管理の種々の面 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手続を保護するため。	9.(1)	事業継続管理
11.(1)	事業継続管理手続 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること。	9.(1)	ISMS適用範囲全体を含む組織の事業継続計画を検討し策定、維持するための管理プロセスを整備すること。
11.(1)	事業継続及び影響分析 事業継続に対する全般的取組方法のために、適切なリスクアセスメントに基づいた戦略計画を立てること。	9.(1)	事業継続に取り組むため、リスク評価に基づいた戦略計画を策定すること。
11.(1)	継続計画の作成及び実施 事業運営を、重要な業務手続の中断又は障害の後、適切な時間内で維持又は復旧させるための計画を立てること。	9.(1)	重要な業務に障害または故障が発生した際に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)	事業継続計画作成のための枠組み 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、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること。	9.(1)	すべての計画の整合性を保証し、また、試験や整備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)	事業継続計画の試験、維持及び再評価 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために定期的に試験をし、定期的な見直しをすること。	9.(1)	事業継続計画を定期的に試験し見直すこと。
12.	適合性	10.	準拠
12.(1)	法的要求事項への適合 管理目的：刑法及び民法、その他の法令、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。	10.(1)	法的要求事項への準拠
12.(1)	適用法令の識別 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること。	10.(1)	個別の情報システム毎に関連するすべての法規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)	知的所有権（IPR） 知的所有権がある物件及びソフトウェア製品を使用する場合は、法的制限事項に適合するように、適切な手続を実行すること。	10.(1)	知的財産権に関わる法的制限事項を遵守した手続を整備すること。
12.(1)	組織の記録の保護 組織の重要な記録は、消失、破壊及び改ざんから保護されること。	10.(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。

ISMS認証基準Ver.2.0 附属書「詳細管理策」		ISMS認証基準Ver.1.0 第4 詳細管理策	
項番	条文	項番	条文
12.(1)	データの保護及び個人情報の保護 関連法令に従って個人情報を保護するために、管理策を適用すること。	10.(1)	個人情報保護に関する法規に従い、個人の情報を保護すること。
12.(1)	情報処理施設の誤用の防止 情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐための管理策を用いること。	10.(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)	暗号による管理策の規制 暗号による管理策へのアクセス又はその使用を統制することを目的とした、国による協定、法律、規制、又はその他の手段に、適合することを可能にするために、管理策を用いること。	10.(1)	暗号の使用に関する法規を遵守すること。
12.(1)	証拠の収集 人又は組織に対する措置が、民事であれ刑事であれ、法律にかかわるものである場合、提示する証拠は、関連法令又は事件の審理が行われる特定の法廷の規則に定められた証拠に関する規定に適合させること。また、容認される証拠を作成するために、公表されている標準類又は実践規範に適合すること。	10.(1)	訴訟に提示する証拠は、関連する法規に定められた規則に適合すること。
12.(2)	セキュリティ基本方針及び技術適合のレビュー 管理目的：組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため。	10.(2)	セキュリティポリシーへの準拠
12.(2)	セキュリティ基本方針との適合 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること。組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的に見直すこと。	10.(2)	すべての手続が情報セキュリティポリシーに準拠して実行されていることを定期的に見直すこと。
12.(2)	技術適合の検査 情報システムは、セキュリティ実行標準と適合していることを定期的に検査すること。	10.(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に確認すること。
12.(3)	システム監査の考慮事項 管理目的：システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため。	10.(3)	システム監査の考慮事項
12.(3)	システム監査管理策 運用システムの監査は業務手続の中断のリスクを最小限に抑えるように慎重に計画を立て、合意されること。	10.(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すること。
12.(3)	システム監査ツールの保護 システム監査ツールは、誤用又は悪用を防止するために、保護されること。	10.(3)	システム監査ツールに対する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。