# 情報セキュリティ管理基準活用ガイドライン

Ver1.0

# Ⅰ．はじめに

## １．本ガイドラインの位置付け

本ガイドラインは、「情報セキュリティ管理基準」（令和 7 年改正版）の活用を促進する観点から、同基準をもとに組織体における情報セキュリティリスクに関するリスク対応のための方針の決定や、その管理体制の構築及び管理策の検討を担う者と、当該組織体を対象とする情報セキュリティ監査を行う監査人（外部監査、内部監査とも）を対象に、それぞれの観点において考慮すべき事項について解説するものである。なお、検討にあたっては双方の観点に配慮する必要があることから、いずれの立場においてもすべての内容について参照することが望ましい。

## ２．個別管理基準と業種・業態別管理基準

情報セキュリティ管理基準は、組織体における情報セキュリティマネジメントの円滑で効果的な確立のための、マネジメントサイクル構築の出発点から具体的な管理策に至るまで、包括的な適用範囲を有する参照基準である。同基準は包括的な基準であるがゆえに、組織体における個別の事情への対応に最適化したものではない。また、情報セキュリティ監査を実施するにあたっては、判断の尺度をより具体的に規定する必要も生じ得る。

そこで、組織体に適した情報セキュリティマネジメントシステムを構築・運用するためには、組織体が属する業界又は事業活動の特性等に加えて、契約など組織体固有の要求事項を考慮し、必要に応じて同基準の項目等を取捨選択、追加又は統合することにより、組織体独自の管理基準体系（個別管理策体系）を策定する必要がある。個別管理策体系に基づいた対策の実施により、情報セキュリティインシデントの低減や、投資効率の向上等を期待できる。

一方で、個別管理策体系を策定するためには、情報セキュリティに関する専門的な知見や詳細な業務分析が必要となるなど、組織体の負担は大きい。そこで、同じ業種や業態であれば経営や事業を通じた情報セキュリティリスクの態様は類似していることを踏まえ、業界団体等により特定の業種・業態を対象とした業種・業態別管理基準を策定し、業界内で共有する活動が行われている。これらの活動成果を活用することで、各組織体は個別管理基準の策定に関する負荷を減らしつつ、効果的な情報セキュリティ対策を実現することができる。

監査人は、情報セキュリティ管理基準又は業種・業態別管理基準及び組織体固有の要求事項に基づく、個別管理基準を作成し、組織体の管理策が体系的に整備されているかを監査する整備状況評価を行う。整備状況評価の結果、組織体が策定した個別管理策体系が個別管理基準と整合する場合には、個別管理策体系が適正であるとすることができる。個別管理策体系が有効である場合には、個別管理基準に基づき適正な運用がなされているかの運用状況評価を行い、管理策の有効性を評価する。

## ３．個別管理基準をリスクベースで活用するには

前節に示した個別管理基準の策定にあたっては、組織体における情報セキュリティリスクの態様を把握した上で、それらのリスクを組織体で許容できる水準以下に抑制する観点から行うこと（リスクベースによるアプローチ）が適切である。具体的にはまずリスクアセスメントを行った上で、情報セキュリティガバナンスの取組みとしてトップマネジメントが組織体としてのリスク対応のための方針を定める。

このうち、リスク対応のための方針には、次のような内容が含まれる。

1) リスク認識[1]をどのように共有するか
2) 共有されたリスク認識に基づき、どのような方法で目標（許容できるリスク水準）を立てるのか（例えば、リスク「高」は半年以内に「中」以下に低減すること）
3) 目標の達成状況をどのようにトップマネジメントが把握（モニタ）するか
4) 達成状況の評価及びフィードバックをどのように行うか

リスク対応のための方針を定めた上で、次に上記 2)における目標達成の方法として、情報セキュリティマネジメントシステムで用いる管理策のうち、リスクの低減に有効と判断されるものについて取捨選択及び優先順位付けを行う[2]。

---

[1] 本ガイドラインでは、リスク（目的に対する不確かさの影響）の存在を単に知るだけでなく、より一歩進めて組織体としてリスクに対してどのような対策をしなければならないかまで含めて認識することを「リスク認識」と定義して用いる。

[2] リスク対応のための方針に基づくリスクマネジメントが行われていると、リスクベース監査がより効果的に実施できる。リスクマネジメントの基準として、JIS Q 31000、COBIT、NIST RMF (Risk Management Framework)などの例が挙げられる。また、業界で固有の基準を定めている例もある。

## Ⅱ．個別管理基準の策定手順

個別管理基準の策定にあたっては、①情報セキュリティ管理基準の参照・項目の抽出、②関連法規制及び考慮すべき事項の明確化、③他の規定等の参照、④当該組織体に必要と思われる項目の追加、⑤組織内規定との整合性を図る、⑥管理策の選定、⑦技術的検証項目の追加といった手順を踏むことが適当である。

上記①から⑦の手順は、組織体において管理すべき情報等の洗い出しとリスクアセスメントに基づいて行わなければならない。なお、組織体が個別管理策体系を作成する場合の手順は、監査人が個別管理基準を作成するための手順と同一である。本手順は、情報セキュリティ管理基準のうちマネジメント基準 4.4.8（情報セキュリティリスク対応）において規定している次の２つの管理策を具体化したものである。

4.4.8.1　組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。

4.4.8.2　組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。

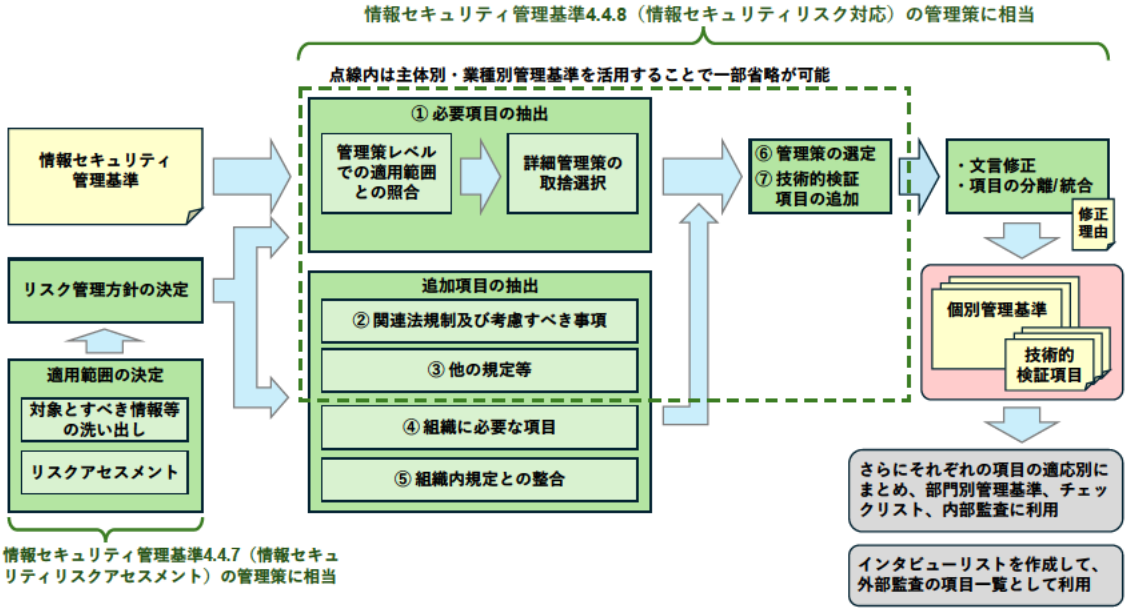


図　個別管理基準策定の流れ

### １．情報セキュリティ管理基準の参照・項目の抽出

個別管理基準を策定するにあたって、情報セキュリティ管理基準又は当該業種・業態向けに提供されているセキュリティ管理基準やガイドライン等を参照し、当該組織体にとって必要とされる項目を抽出する。

項目の抽出後、項目中の文言を当該組織体にとって適切な表現に修正を行う。また、必要に応じて、項目を分割又は、統合を図る。

それぞれの作業の後には、監査人への説明、あるいは後任の担当者への引継のため、修正理由を記述しておく。

例）5a-5.4 管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。

＜適切な表現に修正＞

例）5a-5.4 最高情報セキュリティ責任者は、規定された情報セキュリティ方針、情報セキュリティスタンダード及び関連手順に従った情報セキュリティの適用を、全ての要員に要求する。

（修正理由）わかりやすさを高めるため、自組織で定められた役職及び規定名称に置換。

**２．関連法規制及び考慮すべき事項の明確化**

関連する法令及び各種の規制が要求する事項のうち、個別管理基準として考慮が必要な事項について追加する。

法令の遵守については、記載の有無に関わらず当然守るべき内容であり、情報セキュリティ管理基準の中にも記述されているが、その内容について個別管理基準に記述されることによって、情報セキュリティ関連の他の規定との関係を整理することが可能となる。

**３．他の規定の参照**

情報セキュリティ管理基準は主として組織体で扱う情報を守るためのセキュリティ対策を整理した基準である。一方、IoT 製品や産業用制御機器などが備えるべきセキュリティ対策は網羅されていない。

よって、組織体が IoT 製品や産業用制御機器などを対象にセキュリティ対策を強化したい場合は、情報セキュリティ管理基準以外の参照基準から管理策を選択することが考えられる。

経済産業省の「サイバー・フィジカル・セキュリティ対策フレームワーク」（CPSF）[3]は IoT 機器・システムにおけるリスクへの対策のための管理策を検討するための参考資料として有用である。

その他、業種別のセキュリティガイドライン等を適宜参照して、適切な管理策の下位に必要に応じて詳細管理策として項目を追加又は修正を行う。

**４．当該組織体に必要とされる項目の追加**

[3] https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

情報セキュリティ管理基準から項目を抽出した後、当該組織体にとって必要と考えられる項目を追加する。特に、個別管理基準の適用範囲内において非常に重要な情報が存在し、脅威の発生頻度が高く、発生し得る被害が大きなものとなる場合、情報セキュリティ管理基準に記載の情報セキュリティ対策を修正若しくは追加することで、より強化した対策を追加することが想定される。

項目を修正又は追加する際は、他の項目における表現の抽象度を参照しつつ、表現を検討し、対策の詳細については、技術的検証項目（後述）、実施手順書などに記述するなど、適切な表現で項目を追加する。以下に修正又は追加の例を示す。

注）情報セキュリティ管理基準のそれぞれの項目は、必ずしも同等の抽象度（レベル）で記述されていない。また、全く同じ抽象度とすることには意味がなく、リスク評価の結果として、項目ごとの抽象度を決定すべきである。ある項目が当該組織体にとって非常に重要である場合、これを詳細化して個別管理基準とすることが適当な場合もある。しかし、項目を追加する際はおおよその表現ぶりを検討し、項目の文章が非常に長くなりそうな場合は、詳細を実施手順書に記述するなどして、全体のバランスを図ることが必要である。

例１）4.8.2.2　組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。 [27001-7.5.3]

・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。
・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用又は完全性の喪失からの保護）。
・文書化した情報の配付、アクセス、検索及び利用
・文書化した情報の読みやすさが保たれることを含む、保管及び保存
・文書化した情報の変更の管理（例えば、版の管理）
・<u>文書化した情報の保持及び廃棄</u>

＜上記の項目に対して修正・追加＞（下線項を下記のように変更）

・文書化した情報の保持
・文書化した情報を破棄及び廃棄状況の確認

（修正・追加理由）過去に情報の廃棄を委託した事業者からの情報漏えい事案が発生しており、単に廃棄扱いとするだけでなく、破棄を外部委託した場合の委託先における契約遵守状況の確認が必要と考えられるため

例２）5b-5.9.2　文書は、必要に応じて専用の目録又は既存の目録として維持する。

＜上記の項目に対して追加＞

5b-5.9.2.1　個人情報を含む重要な情報が記録された文書は、専用の目録として維持する。

（追加理由）個人情報については、通常よりも高い情報セキュリティ対策が必要とされると考えられるため

例３）7a-7.2.3　物理的入退の管理策の実施については、次の事項を考慮する。

f)　全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容易に区別できるバッジの使用を検討する。

＜上記の項目に対して修正＞

f)　全ての要員及び期間を問わず一時的に入退室するすべての者に電子的に確認可能な身分証の着用を要求する。常勤の従業員、供給者及び訪問者を識別しやすくするために、供給者及び訪問者の立入の場合は容易に区別できるストラップを使用する。

（修正理由）物理的入退の制限方法について、自組織で用いている方法に修正

例４）7a-7.5.5　リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の採用を考慮する。

a)　火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知し、警報を送信する又は消火システムを起動することができるシステムを設置し、構成する。消火は、周囲の環境に対して最も適切な物質を使用して実施する。

b)　洪水：記憶媒体又は情報処理システムを含む領域の床の下に、洪水を早期に検知できるシステムを設置する。洪水が発生した場合に水ポンプ又は同等の手段をすぐに利用できるようにする。

c)　電気サージ：サーバ及びクライアントの両方の情報システムを電気サージ又は同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。

d)　爆発物及び武器：取扱いに慎重を要する情報処理施設に入る要員、

車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する。

＜上記の項目に対して追加＞

e) 地震：記憶媒体及び関連する情報処理システムの地震による損傷を防ぐために、振動による影響を緩和し得る設置場所での保管、及び地震発生時に安全に停止させるための設備を設置する。

（修正理由）組織として認識しているリスクを追加

**５．組織内規定との整合性を図る**

個別管理基準の策定以前に策定された組織内規定が存在し、情報セキュリティ管理基準中には記述されていない組織内規定の項目について、個別管理基準に追加又はその組織内規定との関連が理解できるように記述する。

組織内規定と個別管理基準との整合性を図り両者に矛盾が生じないようにそれぞれを修正する。

**６．管理策の選定**

個別管理基準の各管理策について、当該組織体のリスク管理目標への影響度に応じて「必ず遵守すべき必須項目」と「可能であれば実行すべき推奨項目」に分けることが可能である。

そのような項目に対して、文末表現等で書き分けることで「必須項目」と「推奨項目」を識別し、対策リソースが限られている場合であれば必須項目を中心に管理策を実践する等により、情報セキュリティ対策の有効性を高めることが可能となる。

**７．技術的検証項目の策定**

追加・修正すべき項目の中には、管理策の実践に際して技術的に高度な内容が求められる項目が含まれる可能性がある（例：ペネトレーションテストの実施）。これらについては、外部の専門家への委託により実施するなどの対応が必要となるため、技術的検証項目として識別可能にすることが考えられる。

また、技術的検証項目についてはそれ以外の項目と比較して情報技術の変化の影響を受けやすいため、比較的頻繁に見直しを行う必要がある。

## Ⅲ．管理基準のさらなる活用

### １．ガバナンスの評価（有効性評価）の考え方

情報セキュリティ管理基準の「Ⅲ．ガバナンス基準」ではガバナンスの目的とプロセスに関する管理策を示しているが、これらの有効性は組織体の情報セキュリティ目標の達成状況を次の３点の測定結果をもとに評価することが考えられる。

【トップマネジメントにおける役割の遂行】

適切な指示等が実施されていることの前提として、トップマネジメントが自ら最新の動向を認識することに努めているか、最新の情報をトップマネジメントに伝達する仕組みが機能しているかどうかを確認することが考えられる。

【リスク認識の共有の程度】

組織体の構成員（例：すべての役職員）において情報セキュリティに関する重要なリスク（例：個人情報の漏えい）について認識がなされていれば、共有がなされていると考えられる。

【目標の達成状況】

全社目標が部署ごとにブレークダウンされているとき、各部署がそれぞれの目標を達成しているかどうかを測定する。

なお、情報セキュリティガバナンスを対象とする監査を実施する場合には、その前提として組織体における IT ガバナンスの状況を把握しておくことが有用である。

### ２．管理策に関する属性情報の活用

JIS Q 27002:2024 では個々の管理策について、新たに下表で定義される属性が記載されるようになった。表内の記号は情報セキュリティ管理基準の「Ⅶ．属性一覧」に記載した凡例に対応している。

**表１　属性の一覧**

| | | |
|---|---|---|
| 管理策タイプ | P<br>D<br>C | #予防<br>#検知（Detective）<br>#是正 |
| 情報セキュリティ特性 | C<br>I<br>A | #機密性<br>#完全性<br>#可用性 |
| サイバーセキュリティ概念 | I<br>P<br>D<br>Rs<br>Rc | #識別<br>#防御（Protect）<br>#検知（Detect）<br>#対応<br>#復旧 |
| 運用機能 | G<br>As | #ガバナンス<br>#資産管理 |

| | | |
|---|---|---|
| | IP | #情報保護 |
| | H | #人的資源のセキュリティ |
| | P | #物理的セキュリティ |
| | Sy | #システム及びネットワークのセキュリティ |
| | Ap | #アプリケーションセキュリティ |
| | Se | #セキュリティを保った構成 |
| | Id | #識別情報及びアクセスの管理 |
| | T | #脅威及びぜい弱性の管理 |
| | C | #継続 |
| | Su | #供給者関係のセキュリティ |
| | L | #法令及び順守 |
| | IE | #情報セキュリティ事象管理 |
| | IA | #情報セキュリティ保証 |
| セキュリティドメイン | G | #ガバナンス及びエコシステム |
| | P | #保護 |
| | D | #防御（Defence） |
| | R | #レジリエンス |

属性の活用例を以下に示す。

**① 個別管理基準を策定する際の活用方法**

属性は、リスクベースで管理策を選定する際に活用することができる。属性の種類としては、上記の表の属性を活用することもでき、また、各組織体にて独自の属性を作ることもできる。上記の表の属性は、ISO/IEC 27002:2022 で初めて導入されたものであるため、その活用方法は今後さらに具体化が進むこととなるが、例えば以下の２つのような活用方法が考えられる。

【属性による管理策の分類】属性により、管理策を分類することができる。例えば、表の「管理策タイプ」では、管理策が情報セキュリティインシデントの発生を「予防」「検知」「是正」のいずれを意図した管理策であるかという観点により、管理策を分類することができる。また、「情報セキュリティ特性」では、管理策が情報の「機密性」「完全性」「可用性」のどの特性を維持するのに寄与するのかという観点により、管理策を分類することができる。このように属性によって管理策を分類することにより、リスクベースで管理策を選定する際、「予防」「検知」「是正」に関連する管理策がバランスよく配備・選定されているか、対策を強化したい部分の管理タイプや情報セキュリティ特性を明確化することにより、それらに対応した適切な管理策が十分に選別されているか、などの観点からの評価や見直しができる。次ページ表２に、運用機能「#資産管理（As)」に該当する管理策を抽出した例を示す。

【他の規定とのマッピング】属性により、他の規定の管理策や要件とのマッピングを行うことができる。例えば、「サイバーセキュリティ概念」は、米国 NIST による“The NIST

Cybersecurity Framework 2.0”[4]が定義する 6 つの機能のうち、“Govern”を除く 5 つを属性としており、情報セキュリティ管理基準の各管理策とのマッピングを行うことが可能である。

**表２　運用機能「#資産管理（As)」に該当する管理策の抽出例**

| | |
|---|---|
| 5b-5.9 | 情報及びその他の関連資産の目録 |
| 5b-5.10 | 情報及びその他の関連資産の許容される利用 |
| 5b-5.11 | 資産の返却 |
| 5b-5.14 | 情報の転送 |
| 5g-5.33 | 記録の保護 |
| 5g-5.37 | 操作手順書 |
| 6a-6.5 | 雇用の終了又は変更後の責任 |
| 6a-6.7 | リモートワーク |
| 7a-7.3 | オフィス、部屋及び施設のセキュリティ |
| 7b-7.8 | 装置の設置及び保護 |
| 7b-7.9 | 構外にある資産のセキュリティ |
| 7b-7.10 | 記憶媒体 |
| 7b-7.13 | 装置の保守 |
| 7b-7.14 | 装置のセキュリティを保った処分又は再利用 |
| 8a-8.1 | 利用者エンドポイント機器 |
| 8b-8.14 | 情報処理施設・設備の冗長性 |

### ② 監査を実施する際の活用方法

監査目的によっては、属性を用いて目的に適合する管理策を抽出することで、監査を効率的に行うことができる。例えば、サイバーセキュリティ対策に係る事項が適切に実施されているかを監査目的とした場合には、「サイバーセキュリティ概念」の項目をまず抽出し、それらの項目に、情報セキュリティ管理基準に含まれない、組織が定めたサイバーセキュリティ対策に対応する項目を追加して監査項目を作成し、適用することが考えられる。次ページ表３に、運用機能とサイバーセキュリティ概念の２つの属性について管理策を整理した例を示す。

[4] https://www.nist.gov/cyberframework

## 表３　属性を用いた管理策の抽出例

| | | 運用機能（抜粋） | | |
|---|---|---|---|---|
| | | ガバナンス(G) | 情報保護(IP) | アプリケーションセキュリティ(Ap) |
| サイバーセキュリティ概念 | 識別(I) | 5.1　情報セキュリティのための方針群<br>5.2　情報セキュリティの役割及び責任<br>5.4　管理層の責任<br>5.5　関係当局との連絡<br>5.8　プロジェクトマネジメントにおける情報セキュリティ | 5.12 情報の分類<br>5.33 記録の保護<br>5.34 プライバシー及び PII の保護 | 8.29 開発及び受入れにおけるセキュリティテスト<br>8.30 外部委託による開発 |
| | 防御(P)<br>(Protect) | 5.3　職務の分離<br>5.5　関係当局との連絡<br>5.6　専門組織との連絡<br>5.8　プロジェクトマネジメントにおける情報セキュリティ | 5.10 情報及びその関連資産の許容される利用<br>5.13 情報のラベル付け<br>5.14 情報の転送<br>5.33 記録の保護<br>5.34 プライバシー及び PII の保護<br>6.6　秘密保持契約又は守秘義務契約<br>6.7　リモートワーク<br>8.1　利用者エンドポイント機器<br>8.7　マルウェアに対する保護<br>8.10 情報の削除<br>8.11 データマスキング<br>8.12 データ漏えい防止<br>8.33 テスト用情報<br>8.34 監査におけるテスト中の情報システムの保護 | 5.37 操作手順書<br>8.4　ソースコードへのアクセス<br>8.18 特権的なユーティリティプログラムの使用<br>8.19 運用システムへのソフトウェアの導入<br>8.25 セキュリティに配慮した開発のライフサイクル<br>8.26 アプリケーションセキュリティの要求事項<br>8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則<br>8.28 セキュリティに配慮したコーディング<br>8.30 外部委託による開発<br>8.31 開発環境、テスト環境及び本番環境の分離<br>8.32 変更管理 |
| | 検知(D)<br>(Detect) | － | 8.7　マルウェアに対する保護<br>8.12 データ漏えい防止 | 8.30 外部委託による開発 |
| | 対応(Rs) | 5.5　関係当局との連絡<br>5.6　専門組織との連絡<br>5.24 情報セキュリティインシデント管理の計画策定及び準備 | － | － |
| | 復旧(Rc) | 5.5　関係当局との連絡<br>5.6　専門組織との連絡<br>5.24 情報セキュリティインシデント管理の計画策定及び準備 | － | 5.37 操作手順書 |