個別管理基準（監査項目）策定ガイドライン

Ver1.0

本ガイドラインは、「情報セキュリティ管理基準」に従って、組織体ごとに具体的な管理基準（以下、「個別管理基準」という。）を策定する際の手順について示したものである。「情報セキュリティ管理基準」を各組織体の実状に見合ったものとする際のガイドラインであるから、情報セキュリティ監査において監査人が監査項目（「監査要点」ともいう。）を選択する際のガイドラインとしても有用なものである。

組織体が個別管理基準を策定する場合であっても、また情報セキュリティ監査人が監査項目を選定する場合であっても、基本的に同様の手順を踏むと考えられる。

なお、本ガイドラインを用い、サンプルとして「電子政府における一般的な庁内ネットワークシステム」を対象として、個別管理基準（監査項目）の策定を行ったものが、「電子政府情報セキュリティ管理基準モデル（庁内ネットワークシステム）」である。

Ⅰ．個別管理基準（監査項目）の策定手順

０．　個別管理基準（監査項目）策定の流れ

0.1　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当該組織体に必要と思われる項目の追加、③組織内規定との整合性をはかる、④関連法令の参照、⑤他の規定の参照、⑥必須項目と推奨項目の選別、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。

0.2　上記①から⑦の手順は、組織体の情報資産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。

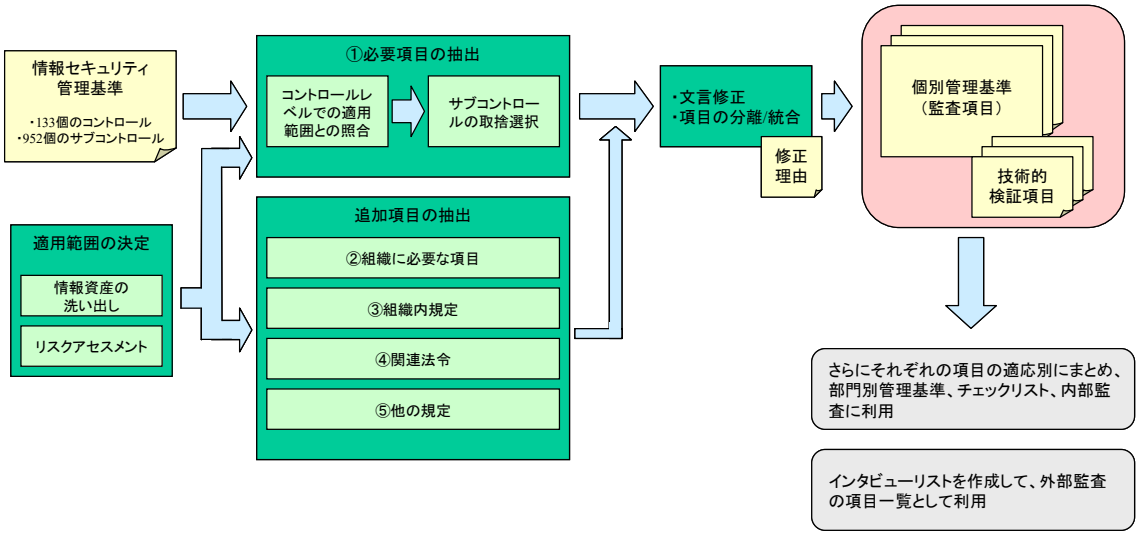

図　個別管理基準（監査項目）策定の流れ

１.「情報セキュリティ管理基準」の参照・項目の抽出

1.1　個別管理基準（監査項目）を策定するにあたって、「情報セキュリティ管理基準」を参照し、当該組織にとって必要とされる項目を抽出する。

1.2　項目の抽出後、項目中の文言を当該組織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。

1.3　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ことが望ましい。

例）8.1.1.5　適切であれば管理者は、独立に評価され、認定された製品の利用を考慮すること。

＜適切な表現に修正＞

8.1.1.5　情報システム担当者は、「IT セキュリティ評価・認証制度」において認証された製品の利用を考慮すること。

（修正理由）わかりにくい部分を具体化。「認定された製品」とは、我が国においては「IT セキュリティ評価・認証制度において認証された製品」を示すため分かりやすい表現とした。

２．当該組織に必要とされる項目の追加

2.1　「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（監査項目）の適用範囲内において非常に重要な情報資産が存在し、脅威の発生頻度が高く、発生しうる被害が大きなものとなる場合、通常の情報セキュリティ対策に加えて、厳重な対策を追加することが想定される。

2.2　項目を追加する際は、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、適切な表現での項目を追加する。

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、項目毎の抽象度を決定すべきである。ある項目が当該組織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（監査項目）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、全体のバランスをはかることが必要である。

例１）3.1.1.2　情報システムに関連づけて重要な資産について目録を作成すること

＜上記の項目に対して追加＞

3.1.1.3　情報システムそれぞれに関連づけて個人情報を含む重要な情報について目録を作成すること

（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２）5.2.1.2　取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は，使用中に盗み見されるリスクを軽減するように設置すること

5.1.2.14　組織自ら管理する情報処理設備は、第三者が管理するものから物理的に分離しておくこと

＜上記２つの項目に対して追加＞

5.1.3.19　特に重要とされる情報資産について、第三者が管理するものから物理的に分離しておくことが困難な場合において、電磁的情報漏洩への対策（テンペスト対策）を施すこと

（追加理由）国家機密等、極めて重要な情報については、通常よりも高い情報セキュリティ対策が必要とされ、電磁的漏洩に対する対策（テンペスト対策）を特別に講ずる必要があるため。

注）なお、上記は事例であり、テンペスト対策については、コストとセキュリティ向上とのバランスを検討し、適用する必要がある。

３．組織内規定との整合性をはかる

3.1　個別管理基準（監査項目）の策定以前に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（監査項目）に追加または、その組織内規定との関連が理解できるように記述する。

3.2　組織内規定と個別管理基準（監査項目）との整合性をはかり両者に矛盾が生じないようにそれぞれを修正する。

４．関連法令の参照

4.1　関連する法令の要求する事項の中で特に重要と考えられる事項について追加する。

4.2　法令の遵守については、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（監査項目）に記述されることによって、情報セキュリティ関連の規定を整理することが可能となる。

例）10.1.1.2　国家公務員法第 100 条「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。」を遵守すること

（追加理由）遵守すべき法令の中で特に重要なものであり、かつ、従前より、情報セキュリティ確保上、運用されてきた条文であるため。

５．他の規定の参照

5.1　その他、ウイルス対策基準、不正アクセス対策基準、ISO/IEC TR13335（GMITS）等情報セキュリティ管理を行う上で参考になる基準が存在する。これらを適宜参照して、適切なコントロールの下位にサブコントロールとして項目を追加あるいは、修正を行う。

5.2　これまでに当該組織が利用してきたセルフチェックリスト、当該組織が属する業種において利用されている基準を追加・修正する。

６．必須項目と推奨項目の選定

6.1　個別管理基準（監査項目）においては、当該組織が必ず遵守すべき必須項目とともに、可能であれば実行すべき項目が存在する。その様な項目に対して、それぞれ「必須項目」と「推奨項目」とにそれぞれ「○」、「△」を付し、区別を行うことによって、経済的で効率の良い情報セキュリティ対策を行うことが可能となる。

７．技術的検証項目の策定

7.1　追加・修正すべき項目の中には、技術的に高度な内容のため、管理項目として記述することが、適当でない場合がある。特にＩＴ製品・システムの設定を行うといった専門的で、技術的に高度なコントロールの場合には、サブコントロールとは別途、技術的検証項目として策定することが適当である。技術的な設定・手続きについて、それぞれのサブコントロールの下位に、技術的な検証項目を策定しておくことが適当である。

また、この様な技術的コントロールは陳腐化が激しい場合があり、サブコントロール以上の項目とは別に、比較的頻繁にメンテナンスを図っていく必要がある。

Ⅱ．その他

１．個別管理基準（監査項目）の利用方法等

1.1　策定される個別管理基準（監査項目）については、項目毎に責任の所在を明らかにすることができる場合がある。この場合、それぞれの項目を責任者毎に振り分け、それぞれが守るべきものを明確にすることは、効率的な管理につながる。また、監査主体が監査を行う際に、項目毎に被監査主体を設定し、対象者毎に監査を行うことも想定される。

1.2　策定される個別管理基準（監査項目）は、一度の策定に留まらず、組織の態様の変化及び外部要因によって、徐々に評価・改善をしていくべきものである。また、その際、必要に応じて、情報セキュリティ監査の専門家に評価・改善の提案を求めることが有用である。

２．主体別・業種別管理基準の策定

2.1　主体別・業種別の情報セキュリティ管理基準の策定に当たっても、上記の手順を経て策定することができる。

2.2　電子政府の一般的な庁内ネットワークシステムを想定し、上記の手順を経て策定したものが、「電子政府情報セキュリティ管理基準モデル（庁内ネットワークシステム）」である。