DM4-01-061

別紙１：雛形

情報システムにおける情報セキュリティ対策実施規程

雛形

2006 年 3 月

内閣官房情報セキュリティセンター

本書の位置付け

本書は、情報システムにおける情報セキュリティ対策実施規程を作成する場合の雛形であり、「情報システムにおける情報セキュリティ対策実施規程 策定手引書」２に示す実施手順に記載すべき事項を、同 3 に示す文書構成例の枠組みの中に盛り込み作成したものである。

本書の利用方法

本書において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 統括情報セキュリティ責任者又は情報セキュリティ責任者が規程を策定することを想定している。
- 情報システムセキュリティ責任者が規程を利用することを想定している。
- 大規模な情報システム等であり、情報システムのライフサイクルにおける業務を外部委託する場合、「外部委託におけるセキュリティ対策実施規程」に記載された事項を考慮する必要がある。
- 個別の情報セキュリティ対策の適用に関する詳細については、別途情報セキュリティ関係規程を定め、これを遵守することを要求する必要がある。

手直しポイント

「情報システムにおける情報セキュリティ対策実施規程」を策定するに当たり、以下の点について手直しをする必要がある。

(1) 雛形において*[・・・]*形式で示す設定値（担当者名、手順書名等）については、各府省庁内の定めに合わせる。

(2) 雛形において【・・・の場合】形式で示す記述については、想定される案を記したものであり、各府省庁の判断により適宜、選択又は修正する。

(3) 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。

(4) 雛形に情報セキュリティ対策の観点以外の一般的な記述について不足がある場合には、適宜、補う。

改訂履歴

改訂日	改訂理由
2006/3/31	初版
2006/6/16	仮称を記載していた参照先資料の名称を、確定した名称に変更。 「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」 「情報システムの構築等における ST 評価・ST 確認の実施に関する解説書」

目次

1　本手順の目的

情報システムは、目的業務を円滑に遂行するため、情報システムのライフサイクルを通じて様々な要件を満たすことが必要となる。その要件の中には、情報システムのライフサイクルで発生する様々な脅威に対応するための情報セキュリティの観点からの要件も含まれる。そして、セキュリティの要件を満足するためには、情報システムのライフサイクルを通じて適切な情報セキュリティ対策を実施し、実施した情報セキュリティ対策を PDCA サイクルによって、見直ししていかなければならない。

本手順は、情報システムのライフサイクルの視点に立ち、情報システムのセキュリティ要件に基づいて、各段階において考慮すべき情報セキュリティ対策について定めることを目的とする。

2　本手順の対象

2.1　対象者

本規程は、情報システムセキュリティ責任者を対象とする。

3　用語の定義

本手順において使用する用語の定義は次のとおりである。

(1) 「情報システム」とは、情報処理及び通信に係るシステムをいう。

(2) 「機器等」とは、情報機器及びソフトウェアをいう。

(3) 「情報システムのライフサイクル」とは、情報システムの「計画／設計／構築／運用／移行／廃棄」の過程をいう。

(4) 「情報セキュリティ対策の PDCA サイクル」とは、情報セキュリティ対策の「計画（PLAN）／実施（DO）／点検（CHECK）／見直し（ACTION）」の過程をいう。

4　情報システムの計画

4.1　体制の確保

規程策定者への解説

情報システムのライフサイクル全般にわたってセキュリティを維持していく体制を確保するためには、十分な資源が必要となる。資源としては、一般的に下記のようなものが想定できる。

- セキュリティを維持するための人員（＝ヒト）
- セキュリティを維持するための予算（＝カネ）
- セキュリティを維持するための機器（＝モノ）

(1)　*[情報システムセキュリティ責任者]*は、セキュリティを維持するために人員、予算、機器等を必要とする場合は、*[情報システムを統括する責任者]*に申請すること。

規程利用者への補足説明

情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたってセキュリティを維持するために必要な措置に対して、情報システムを統括する責任者より十分な資源の提供を受けるべきである。

なお、情報システムのライフサイクルを通じてセキュリティを維持するために必要な措置とは、すなわち本項以降で説明されるすべての事項にほかならない。

【情報システムの分析を求める場合】

4.2　情報システムの分析

規程策定者への解説

情報システムのライフサイクル全般にわたってセキュリティを維持するためには、情報システムの状況に関する正確な調査・認識が必要であり、これは、稼動中のシステムであっても、開発中のシステムであっても同様である。

【システム構成図の作成を求める場合】

(1)　*[情報システムセキュリティ責任者]*は、システムが提供するサービス、システムの構成、システムの関与者をまとめ、*[システム構成図]*を作成すること。

規程利用者への補足説明

情報システムのライフサイクル全般にわたってセキュリティを維持する

作業を実施しやすくするために、情報システムの概要、情報システムの関与者、ネットワーク環境等について調査し、把握しておくべきである。
なお、大規模な組織においては、今後の作業を軽減するために、セキュリティ要件を判断する上で類似している情報システム、すなわち類似する構成、関与者、ネットワーク接続等、同一のセキュリティの条件を持った情報システムをグループ化しておくことが望ましい。
まとめた内容は、「システム構成図」等として整理しておくと脅威の洗い出し等の今後の作業が実施しやすい。
一般的に調査・把握しておくべき事項を以下に例示する。

(a) 情報システムの概要

- 適用業務
- 機能
- 設置場所
- *[その他各府省庁が情報セキュリティ関係規程で定める事項]*

(b) 情報システムの関与者

- サーバ担当者
- ネットワーク担当者
- ソフトウェア開発者
- 機器等の購入者
- 利用者
- 保守管理者
- *[その他各府省庁が情報セキュリティ関係規程で定める者]*

(c) ネットワーク環境

- ネットワーク接続
- インターネット等の外的環境との接続
- 外部システムとの連携
- *[その他各府省庁が情報セキュリティ関係規程で定める事項]*

【情報システムの構成要素の調査・把握を求める場合】

(2) *[情報システムセキュリティ責任者]*は、情報セキュリティ対策の観点から情報システムの構成要素を調査し、把握すること。

規程利用者への補足説明

政府機関統一基準において、情報システムとは「情報処理及び通信に係るシステム」と定義され、具体的には、サーバ装置やクライアント PC 等の

ハードウェア、個別に開発した行政事務用アプリケーション、商用 OS や DBMS 等の製品ソフトウェア、通信回線及び通信回線装置等の複数の要素から構成される。この場合、情報システム全体のセキュリティ強度は、最も弱い部分のセキュリティ強度の影響を受ける。例えば、ウェブアプリケーションが極めて強固に作られていても、セキュリティホールを抱えるウェブサーバソフトウェアを使用していれば、情報システム全体としては脆弱となる。

情報システム全体のセキュリティ水準を高めるためには、各構成要素における情報セキュリティ対策を実施する必要があり、その前提として、情報システムの構成要素を調査し、把握しておくべきである。

一般的に調査・把握しておくべき事項を以下に例示する。

- アプリケーションソフトウェア（行政事務用アプリケーション等）
- OS、ミドルウェア（UNIX系OS、Linux系OS、Windows系OS、DBMS等）
- サーバ装置（サーバ、ワークステーション等）
- 端末、周辺機器（デスクトップPC、ノートPC、プリンタ、外部記録媒体等）
- 通信回線及び通信回線装置（LAN、インターネット、ルータ、モデム等）
- *［その他各府省庁が情報セキュリティ関係規程で定める事項］*

【情報システムの台帳の作成を求める場合】

(3) *［情報システムセキュリティ責任者］*は、情報システムの台帳を作成すること。

規程利用者への補足説明

情報システムの分析の結果を府省庁の共通する様式の台帳等にまとめておくと、組織全体の情報セキュリティを管理する面で役立つ資料となる。

一般的に管理すべき項目を以下に例示する。

- 情報システムの一意的な名称
- 主管課
- 用途の概要
- 用途の種別
- システムの種別
- サーバの有無
- 端末の有無
- アカウント数、インターネット接続
- 国民端末からの利用者
- *［その他各府省庁が情報セキュリティ関係規程で定める事項］*

4.3　情報システムのセキュリティ要件

規程策定者への解説

セキュリティ要件とは、情報セキュリティに関する要求事項である。情報システムのセキュリティ要件を決定し、セキュリティ要件の重要性を判断する必要がある。

例えば、郵便を送る場合、その内容が秘匿すべきもので、かつ途中で盗み読まれる危険があるのであれば、封入封緘し、書留等の方法を用いるべきであるが、その内容が誰に読まれても構わない内容であるか、または盗み読まれる危険性がそもそもないのであれば、普通郵便で送るなど特に対策を採る必要がない。

なお、政府機関統一基準では、各府省庁において共通して対応を図るべき脅威として以下の対策を定めている。

- セキュリティホール対策[統一基準4.2.1]
- 不正プログラム対策　[統一基準4.2.2]
- サービス不能攻撃対策　[統一基準4.2.3]

【セキュリティ要件の決定に当たって、情報システムが取り扱う情報の抽出と格付けを要求する場合】

(1) *[情報システムセキュリティ責任者]*は、情報システムが取り扱う情報のうち保護すべき情報を抽出し、抽出した情報資産に対して、機密性、完全性及び可用性の観点から情報の格付けを実施すること。

規程利用者への補足説明

情報システムのセキュリティ要件を決定するために、情報システムが取り扱う情報のうち保護すべきものを抽出し、当該情報について、そのセキュリティ上の重要度を識別しておくため、情報の機密性、完全性、可用性の格付けを行う必要がある。

なお、情報の抽出に当たっては、例えば、情報システムで取り扱う情報を以下のように大別して作業を行うと効率的である。

- 一次情報資産（行政管理文書等）
- 二次情報資産（システム構成情報等）

一次情報資産とは、情報システムにて取り扱う行政事務情報そのものである。二次情報資産は、例えば、ソースコードやセッション ID 等の情報システムの構成情報であり、一次情報資産を保護するために、間接的に重要な情報といえる。二次情報資産にどのようなものが含まれるかは、システ

ムの仕様に左右されるが、新規開発の案件であれば、基本設計等の工程を経ることで明確化される。この分類は情報システムの開発が外部に委託される場合は、一次情報資産の洗い出しが発注者側の責務となり、二次情報資産の洗い出しが受注者側の責務となることが多いことから有効である。

【セキュリティ要件の決定に当たって、情報システムが取り扱う脅威の洗い出しを要求する場合】

(2) *[情報システムセキュリティ責任者]*は、どのような攻撃者が、どの情報に対して、どのような攻撃を行う可能性があるかを検討し、情報システムに対する脅威を洗い出すこと。

規程利用者への補足説明

情報システムに対する情報セキュリティの脅威とは、情報の機密性、完全性、可用性の侵害であり、例えば、機密性の侵害であれば、アカウントのない者によるデータへのアクセス、アカウントのある者によるアクセス、又は通信の盗聴等、様々な事由によって情報漏えいという事象として表面化する。

このため、脅威を検討するに当たっては、「どのような攻撃者が、どのデータに対して、どのような行いをする可能性があるか」を検討し、明確にする必要がある。

(3) *[情報システムセキュリティ責任者]*は、情報システムのセキュリティ要件を決定すること。

【情報システムのセキュリティ要件定義書の作成を要求する場合】

(4) *[情報システムセキュリティ責任者]*は、決定したセキュリティ要件に基づいて、セキュリティ要件定義書を作成すること。

規程利用者への補足説明

セキュリティ要件は、今後の作業のために「セキュリティ要件定義書」として文書化しておくことが望ましい。また、決定した情報システムのセキュリティ要件を各構成要素のセキュリティ要件として具体化するべきである。

なお、セキュリティ要件を決定する具体的な手順は、*[情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書]*を参考とできる。

4.4　情報システムにおける情報セキュリティ対策の選択

規程策定者への解説

情報システムにおける情報セキュリティ対策は、認証や暗号化等の情報セキュリティの機能についての対策、不正プログラムやサービス不能攻撃等の脅威への対策、情報システムの開発や購入等において必要な対策、ハードウェアや通信回線等の情報システムの構成要素についての対策等、情報システムのセキュリティ要件に応じて極めて多様な形態を取り得る。

このため、必要となるセキュリティ対策を各府省庁が独自に検討するのは困難を伴うことから、政府機関として最低限必要となる情報セキュリティ対策については、政府機関統一基準において、

「第４部　情報セキュリティ要件の明確化に基づく対策」

「第５部　情報システムの構成要素についての対策

「第６部　個別事項についての対策]

にて、遵守事項として定めている。

したがって情報システムにおける情報セキュリティ対策については、政府機関統一基準を反映した省庁基準が要求している遵守事項から、セキュリティ要件を満足する有効かつ網羅的な情報セキュリティ対策を選択し、これを実施するべきである。

(1) *[情報システムセキュリティ責任者]*は、情報システムのセキュリティ要件に基づいて、情報セキュリティ対策を*[省庁基準]*より選択し、これを実施すること。

規程利用者への補足説明

情報システムのセキュリティ要件に基づいて必要となるセキュリティ対策を*[○○省]*が遵守すべきセキュリティの遵守事項を定めた*[省庁基準]より選択し*、これを実施するべきである。

なお、 情報システムのセキュリティ要件を満足できない場合は、セキュリティ要件に基づいて、追加のセキュリティ対策を選択し、実施するべきである。

(2) *[情報システムセキュリティ責任者]*は、情報システムのセキュリティ要件に基づいて、情報システムにおける脅威に適切に対抗する情報セキュリティ対策を漏れなく選択すること。

規程利用者への補足説明

情報セキュリティ対策とは、「資産を脅威からどのように守るのか」とい

う方法論である。脅威に対抗するための情報セキュリティ対策そのものに誤りや抜けがある場合、情報システムのセキュリティは維持できない。

例えば、「なりすまし」の脅威があるサーバに冗長化という対策を行ったとしても「なりすまし」を防ぐことはできない。また、外部の人間に厳重な認証を行っていながら、開発者が自由にアクセスできてしまう情報システムは、「開発者の悪意」という脅威に対しては無防備である。

したがって、情報システムのセキュリティ要件に基づいて、脅威に適切に対応した情報セキュリティ対策を漏れなく選択すべきである。

(3) *[情報システムセキュリティ責任者]*は、情報システムのセキュリティ要件に基づいて、情報システムのライフサイクルを網羅する情報セキュリティ対策を選択すること。

規程利用者への補足説明

情報システムに対する脅威は、情報システムのライフサイクルを通して存在している。

例えば、不正プログラムに対抗するために最新のアンチウイルスソフトウェアを購入しインストールしても、運用時の定義ファイルの更新に不備があれば、新たな不正プログラムに対して無防備となる。また、情報システムの厳格な運用を行っていても、機器等が安易に廃棄されれば、機密情報が漏えいすることも考えられる。

したがって、情報システムのセキュリティ要件に基づいて、情報システムのライフサイクルを通して、網羅的な情報セキュリティ対策を実施するべきである。

5　情報システムの設計・構築

5.1　設計・構築における情報セキュリティ対策

規程策定者への解説

情報システムのライフサイクルにおける設計・構築においては、情報システムのセキュリティ要件に基づいて、脅威に適切に対抗するセキュリティ機能を実装した情報システムを設計・構築し、設計・構築時におけるセキュリティ要件を満足していることを検証・確認した上で、運用環境に安全に導入する必要がある。

なお、重要なセキュリティ要件があると認めた情報システムについては、ST 評価、ST 確認と IT セキュリティ評価・認証制度を利用して、設計・構築を行うことが可能であり、これについては、本雛形の 9 章で示している。

(1) *[情報システムセキュリティ責任者]*は、脅威に対抗する情報システムのセキュリティ機能の設計と構成要素の構築を行うこと。

規程利用者への補足説明

情報システムの設計段階において、脅威に確実に対抗するために必要なセキュリティ機能を適切に選択すべきである。また、構成要素を適切に構築して、情報システムのセキュリティ機能を有効に動作させなければならない。

なお、情報システムの構築に際しては、機器等を購入したり、ソフトウェアを独自に開発したりする場合が想定される。

例えば、情報システムの構成要素の内、サーバ装置、端末等のハードウェア及び OS、ミドルウェア等のソフトウェアは、市販されている製品の購入、また、業務プログラム等は、業務仕様にあわせて開発することが想定される。

機器等の購入における情報セキュリティ対策については、*[機器等の購入におけるセキュリティ対策実施規程]*を、ソフトウェア開発における情報セキュリティ対策については、*[ソフトウェア開発におけるセキュリティ対策実施規程]*をあわせて参照されたい。

(2) *[情報システムセキュリティ責任者]*は、セキュリティ要件を満足する情報システムが設計・構築されたことを検証・確認すること。

規程利用者への補足説明

設計・構築時において、セキュリティ要件を満足する情報システムが設計・構築されたことを検証・確認するための情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 設計・構築時におけるセキュリティのレビューとテスト
- セキュリティを考慮した設計・構築体制及び環境
- 評価・認証等を受けた製品

(3) *[情報システムセキュリティ責任者]*は、誤った情報システムの導入及び運用環境と開発用資産へのセキュリティ侵害を防止するため、情報システムを運用環境に導入する手順及び環境に関するセキュリティの管理を行うこと。

規程利用者への補足説明

脆弱性を発生させるような誤った情報システムの導入及び運用環境や開発用資産へのセキュリティ侵害を防止するため、導入のための手順及び環境を管理するための情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 運用の誤りを低減するためのガイダンスと教育（機能、設計、操作、保守、事故対応手順等）
- 脆弱性の混入を排除するための安全な導入の手順（配付・移送の保護、セキュリティを意識した設定等）
- セキュリティの保たれた運用環境への導入
- 運用環境へのセキュリティ侵害を防止する安全な移行の手順
- 開発に利用した機密性を有する情報資産の廃棄

(4) *[その他府省庁が必要と認めるセキュリティ対策]*

6　情報システムの運用

6.1　運用における情報セキュリティ対策

規程策定者への解説

情報システムのライフサイクルにおける運用においては、情報システムのセキュリティ要件に基づいて、設計・構築したセキュリティ機能を適切に運用、維持することでセキュリティレベルの低下を慎重に防止することに加えて、運用時に発生するセキュリティの問題を想定し、これに適切に対処するための手順を整備しておく必要がある。

(1) *[情報システムセキュリティ責任者]*は、情報資産へのセキュリティ侵害を防止するために、セキュリティ機能の適切な利用を行うこと。

規程利用者への補足説明

強固なセキュリティ機能が実装されたとしても、その後適切な利用が行われなければ情報システムのセキュリティは維持できない。例えば、ソフトウェアにマクロの自動実行を禁止する機能が実装されていたとしても、行政事務従事者がその機能を使用していない状態では、不正プログラムに感染する危険性は低減しない。

セキュリティ機能の誤った利用による情報資産へのセキュリティ侵害を防止するため、セキュリティ機能の適切な利用という観点からの情報セキュリティ対策を選択すべきである。

(2) *[情報システムセキュリティ責任者]*は、法令や規制等の要求を満足するため、将来発生するかもしれない障害等の調査のため、又は情報セキュリティ対策の点検と改善に資するために、情報システムの運用を記録すること。

規程利用者への補足説明

法令及び規制等の要請に応えるため、将来発生し得る障害等の調査のため、又は情報セキュリティ対策の点検と改善に資するため、情報システムの運用の記録という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 情報システムへのセキュリティ侵害に関する記録（適正な取得内容、時期、項目等）
- 記録へのセキュリティ侵害に対応するための保護（アクセス制御、暗号化、保存、廃棄等）

(3) *[情報システムセキュリティ責任者]*は、セキュリティの侵害を検知するために、情報システムの運用を監視すること。

規程利用者への補足説明

セキュリティの侵害を検知するため、情報システムの運用の監視という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 不正な変更やセキュリティレベルの低下を防止する情報システムの構成変更の監視
- 不正行為、不正利用に対する監視
- 性能、故障等の監視

(4) *[情報システムセキュリティ責任者]*は、情報システムの障害等及び作業時における機密性、完全性の侵害から保護するために保守作業におけるセキュリティの管理を行うこと。

規程利用者への補足説明

情報システムの障害等及び作業時における機密性、完全性の侵害から保護するために保守作業における情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 障害等を低減する適切な保守（適正な時期、回数、方法等）
- 障害等から情報システムを復旧させるための情報のバックアップ（適正な時期、回数、媒体、復元等）

- バックアップ情報への機密性、完全性侵害を防止するための保護（アクセス制御、暗号化等）
- 情報システムへの機密性、完全性の侵害を防止するための保守作業の管理（許可された担当者、暗号化された作業、機器等を敷地外に持ち出す場合の保護等）

(5) *[情報システムセキュリティ責任者]*は、新たに発生する脅威から情報システムを保護するための脆弱性への対応を行うこと。

規程利用者への補足説明

新たに発生するセキュリティホールや不正プログラムから情報システムを保護するため、脆弱性への対応という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 新たに発生する脆弱性に迅速かつ安全な対応を行うための手順（脆弱性情報の収集、対応計画、暫定対応、修正の試験，修正の配布方法等）

(6) *[情報システムセキュリティ責任者]*は、障害等による被害拡大の防止と情報システムを迅速に回復するための対応を行うこと。

規程利用者への補足説明

障害等による被害拡大を防止し、情報システムを迅速に回復するため、障害等に関する対応という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 障害等による被害拡大防止及び早期復旧のための手順（事故の定義、報告、対処、復旧、原因検証、再発防止、訓練等）

(7) *[その他府省庁が必要と認めるセキュリティ対策]*

7　情報システムの移行・廃棄

7.1　移行・廃棄における情報セキュリティ対策

規程策定者への解説

情報システムのライフサイクルにおける移行・廃棄においては、情報システムのセキュリティ要件に基づいて、情報システムの記憶媒体に含まれる情報の適切な消去を行う必要がある。

(1) *[情報システムセキュリティ責任者]*は、法令、規制等の要求を遵守し、かつ情報の漏えいを防止するために、記憶媒体に含まれる情報を消去すること。

規程利用者への補足説明

情報システムの記憶媒体に保存されている情報について、法令、規制等の要求を遵守し、かつ情報の漏えいを防止するために情報の消去という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 記憶媒体に保存された情報への機密性の侵害を防止するための情報の消去

(2) *[その他府省庁が必要と認めるセキュリティ対策]*

8 情報セキュリティ対策の見直し

8.1 情報セキュリティ対策の見直し

規程策定者への解説

実施すべき情報セキュリティ対策は、状況や環境の変化によって影響を受ける。例えば、ある時点で有効とされる情報セキュリティ対策が、新たな脅威の発生によって無効化されるおそれがあり、また組織が新たに重要な業務を受け持つようになったり、法令が改正される等の環境の変化があったりした場合は、既存の対策の十分性が失われる可能性がある。

こうしたことから、情報システムにおける情報セキュリティ対策は PDCA サイクルに基づいて、常に見直して、有効かつ効率的に機能しているかを検証し、最適な状態に維持し続けなければならない。

(1) *[情報システムセキュリティ責任者]*は、情報システムの情報セキュリティ対策を必要に応じて見直すこと。

規程利用者への補足説明

情報セキュリティ対策は下記の要因を踏まえて定期的又は必要に応じて見直し、最適化を進めていくべきである。

(a) 定期的な要因

- 自己点検の結果
- 監査の結果

- 情報システムの記録、監視の結果

(b) 非定期的な要因

- 組織の変更
- 技術の変化
- 情報セキュリティ関係規程の変更
- 脅威の変化
- 法的規制又は社会環境の変化

9 ST 評価・ST 確認と IT セキュリティ評価及び認証制度の活用

9.1 ST 評価・ST 確認の手続

規程策定者への解説

ST 評価・ST 確認は、情報システム及び製品のセキュリティ設計仕様書（ST：Security Target）が ISO/IEC15408 に適合していることを、第三者評価機関を使い評価・確認する制度である。セキュリティ機能の実装に当たって客観性の高い評価・確認を行いたい場合には、ST 評価・ST 確認を受けることを求めることができる。

(1) *[情報システムセキュリティ責任者]*は、*[情報システムの構築等における ST 評価・ST 確認の実施に関する解説書]* に準じて、重要なセキュリティ要件がある情報システムについて、ST を作成し、評価機関・認証機関に申請を行い、ST 評価・ST 確認を受けたことを示す確認書を入手すること。なお、ST 評価・ST 確認は開発が終了するまでに終了すること。

規程利用者への補足説明

セキュリティ機能の実装に当たって客観性の高い評価・確認を行いたい場合には、セキュリティ設計仕様書（ST：Security Target）に関する ST 評価・ST 確認を受けるべきである。

府省庁が自ら情報システムの構築又はソフトウェアの開発を行う場合には、府省庁が第三者機関に依頼して ST 評価・ST 確認を受けることを想定している。

情報システムの基本設計がまとまった時点で、ST の作成を開始し、ST 評価・ST 確認の申請を評価機関・認証機関に行い、ST 確認を実施する必要がある。また、ST 評価・ST 確認は、開発が終了するまでに終了している必要がある。

なお、手続の詳細については、*[情報システムの構築等における ST 評価・ST 確認の実施に関する解説書]*を参考とできる。

(2) *[情報システムセキュリティ責任者]*は、ST 評価・ST 確認を行う場合、ST 評価・確認制度を運用する IPA（独立法人情報処理推進機構）の策定する要領に沿って ST を作成すること。
[http://www.ipa.go.jp/security/jisec/apdx0504.html]

規程利用者への補足説明

ST に関する詳細は、ST 評価・確認制度を運用する IPA（独立法人情報処理推進機構）のホームページに記載されており、これに準じて作成する必要がある。

【ITセキュリティ評価・認証制度を利用する場合】

9.2 ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度の利用

規程策定者への解説

構築する情報システムの構成要素として調達する機器及びソフトウェアの選択に当たり、採用候補製品が複数ある場合に、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度に基づく認証を取得している製品を選択する。IT セキュリティ評価・認証制度とは、IT 製品あるいはシステムのセキュリティ機能が、正確に実装され、想定されている脅威に有効に動作することを、認定された中立性の高い第三者（評価機関）が評価する制度である。

なお、本事項は政府機関統一基準における強化遵守事項であって、採否は府省庁が判断する。

(1) *[情報システムセキュリティ責任者]*は、重要なセキュリティ要件がある情報システムについて、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能について、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合には、その中から当該セキュリティ機能に関して IT セキュリティ評価及び認証制度に基づく認証を取得している製品を情報システムの構成要素として選択すること。

規程利用者への補足説明

情報システムの構築を行う場合には、*[外部委託における情報セキュリティ対策実施規程 策定手引書及び同雛形(DM6-02-061)]*も参照されたい。

なお、手続の詳細については、*「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」*を参考とできる。