情報セキュリティ管理規程

第１４版

令和７年１月３０日改正

独立行政法人 製品評価技術基盤機構

目　次

第１章　総則

（目的）

第１条　この規程は、独立行政法人製品評価技術基盤機構（以下「機構」という。）における情報セキュリティの適正な管理を行うために必要な事項を定め、もって機構の保有する情報に係る安全性及び信頼性の向上に資することを目的とする。

（定義）

第２条　この規程において使用する用語は、次の各号による。

一　サイバーセキュリティ戦略本部　サイバーセキュリティに関する施策を総合的かつ効果的に推進するためのサイバーセキュリティ基本法（平成二十六年法律第百四号）に基づく体制として内閣に設置された組織をいう。

二　統一基準　サイバーセキュリティ戦略本部が定める政府機関等のサイバーセキュリティ対策のための統一基準をいう。

三　業務従事者　機構の業務に従事している役職員その他指揮命令に服している者のうち、機構の管理対象である情報及び情報システムを取り扱う者をいう。

四　情報　業務従事者が職務上取り扱う、システム又は記録媒体（書面を含む。）に記録された情報及び機構が所有するシステムの設計又は運用管理に関する情報をいう。

五　情報システム　ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機構が調達又は開発するもの（管理を外部委託しているシステムや政府共通利用型システムを含む。）をいう。

六　政府共通利用型システム　他の機関等含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、他の機関等が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報システム及び他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システムをいう。

　なお、政府共通利用型システムを構築・運用する機関等を「政府共通利用型システム管理機関」といい、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築・運用する機関等及び政府共通利用型システムが提供する機器等を利用する機関等を「政府共通利用型システム利用機関」という。

七　機関等　国の行政機関、独立行政法人及び指定法人をいう。

八　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九

条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。

九　要管理対策区域　機構内で取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。

十　機構外　組織規程（企画－法Ａ－組織規程）第５条に規定する主たる事務所及び第５条の２に規定する従たる事務所以外の場所をいう。

十一　情報セキュリティ対策推進体制　機関等の情報セキュリティ対策の推進に係る事務を遂行するため、当該機関等に設置された体制をいう。

十二　リスク　目的に対する不確かさの影響をいう。

十三　情報セキュリティ関係規程　管理規程、対策基準、運用規程及び実施手順を総称したものをいう。

十四　対策基準　機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。

十五　対策推進計画　情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。

十六　運用規程　対策基準に定められた対策内容を個別の情報システムや業務において運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。

十七　実施手順　対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順や手続をいう。

十八　機密性　情報に関して、アクセスを認可された者だけがこれにアクセスできる特性をいう。

十九　完全性　情報が破壊、改ざん又は消去されていない特性をいう。

二十　可用性　情報及び関連資産へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる特性をいう。

二十一　取扱制限　情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを業務従事者に確実に行わせるための手段をいう。

二十二　明示等　情報を取り扱う全ての者が当該情報の格付について共通の認識となるよう、措置を講ずることをいう。

二十三　情報セキュリティインシデント　JIS Q 27000:2019 における情報セキュリティインシデント（望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの）をいう。

二十四　情報セキュリティ事象　情報セキュリティ方針への違反若しくは管理策の不具合の可能性又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象

二十五　本部監査　サイバーセキュリティ基本法第二十六条第１項第二号に基づきサイバーセキュリティ戦略本部が実施する監査をいう。

二十六　CSIRT(シーサート)　機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制をいう。Computer Security Incident Response Team の略

二十七　CYMAT　サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略

第２章　組織及び体制の整備

（最高情報セキュリティ責任者）

第３条　機構に最高情報セキュリティ責任者を置く。

２　最高情報セキュリティ責任者は、機構における情報セキュリティ対策に関する事務を統括する。

３　最高情報セキュリティ責任者は、理事長とする。

（情報セキュリティ委員会）

第４条　機構に情報セキュリティ委員会を置く。

２　情報セキュリティ委員会の委員は、理事、第８条に規定する統括情報セキュリティ責任者、デジタル監、各部門（組織規程第２条に規定する「部門」をいう。）の長、各支所(組織規程第５条の２第六号から第十二号まで)の長、デジタル監情報統括課長、企画管理部経営企画課長及び企画管理部人事企画課長とする。

３　情報セキュリティ委員会の委員長（以下「委員長」という。）は、最高情報セキュリティ責任者が兼務する。委員長は、統括情報セキュリティ責任者を委員長代理として指名することができる。

４　委員長が必要と認める場合は、情報セキュリティ委員会の審議は書面によって行うことができる。

５　情報セキュリティ委員会の庶務は、リスクマネジメント推進室が行う。

６　情報セキュリティ委員会は、次に掲げる事項を審議する。

一　情報セキュリティ管理規程及び情報セキュリティ対策基準の改正等

二　対策推進計画の策定及び見直し

三　前各号に掲げるもののほか、情報セキュリティに関し必要な事項

７　委員長は、必要があると認めるときは、情報セキュリティ委員会の委員以外の情報

セキュリティに関する専門家等を情報セキュリティ委員会に出席させ、意見の開陳又は説明を求めることができる。

８　情報セキュリティ委員会は、委員の過半数の出席をもって成立する。

９　委員長が必要と認める場合は、情報セキュリティ委員会にワーキンググループを置くことができる。

１０　第７項に規定する専門家等が委員会又はワーキンググループに出席した場合には、専門家等に委員会運営規程（管理－法Ｂ－委員会運営）に規定する専門委員と同額の謝金を支給する。ただし、専門家等が謝金の受領を辞退した場合はこの限りでない。

１１　第７項に規定する専門家等には、委員会運営規程（管理－法Ｂ－委員会運営）に基づき旅費を支払うものとする。ただし、専門家等が旅費の受領を辞退した場合はこの限りでない。

（最高情報セキュリティアドバイザー）

第５条　最高情報セキュリティ責任者は、最高情報セキュリティアドバイザー（この規程において情報セキュリティについて専門的な知識及び経験を有する者をいう。）として、組織規程（企画－法Ａ－組織規程）第３０条に規定する最高情報セキュリティアドバイザーを指名する。

２　最高情報セキュリティアドバイザーは、最高情報セキュリティ責任者に対し、情報セキュリティに関する専門的な助言及び業務の支援を行う。

（情報セキュリティ監査責任者）

第６条　最高情報セキュリティ責任者は、情報セキュリティ監査責任者として、組織規程第７条に規定する監査室の長を指名する。

２　情報セキュリティ監査責任者は、最高情報セキュリティ責任者の指示に基づき、情報セキュリティ監査に関する事務を統括する。

（情報セキュリティ責任者）

第７条　最高情報セキュリティ責任者は、部等（組織規程第７条に規定する部・センター及び第５条の２第六号から第一二号までに規定する支所をいう。以下同じ。）ごとの情報セキュリティ責任者として、当該部等における組織規程に規定する当該部等の長を指名する。この場合において、監査室は企画管理部に置かれるものとして取り扱う。

２　情報セキュリティ責任者は、部等内の情報セキュリティ対策に関する事務を統括する。

（統括情報セキュリティ責任者）

第８条　最高情報セキュリティ責任者は、機構に統括情報セキュリティ責任者として、組織規程第７条に規定するリスクマネジメント推進統括官（組織）の長を指名する。

２　統括情報セキュリティ責任者は、最高情報セキュリティ責任者の補佐を行う者として、情報セキュリティ責任者を統括する。

（区域情報セキュリティ責任者）

第９条　統括情報セキュリティ責任者は、情報セキュリティ対策の運用に係る管理を行う区域の単位を定め、単位ごとに区域情報セキュリティ責任者を指名する。

２　区域情報セキュリティ責任者は、所管する単位における区域ごとの情報セキュリティ対策に関する事務を統括する。

（課室情報セキュリティ責任者）

第１０条　情報セキュリティ責任者は、各課室に課室情報セキュリティ責任者として、組織規程第５条の２第六号から第一二号までに規定する支所、第７条に規定する監査室、第１４条に規定するセンター及び課、第１５条に規定する室、（以下「課室」という。）の長を指名する。

２　課室情報セキュリティ責任者は、課室における情報セキュリティ対策に関する事務を統括する。

３　情報セキュリティ責任者は、課室情報セキュリティ責任者を指名したとき、及び変更したときは、統括情報セキュリティ責任者にその旨を報告する。

（情報システムセキュリティ責任者）

第１１条　情報セキュリティ責任者は、自らが統括する部署で所管する情報システムごとに、当該情報システムの計画段階までに情報システムセキュリティ責任者を指名する。

２　情報システムセキュリティ責任者は、所管する情報システムに対する情報セキュリティの対策に関する事務を統括する。

３　情報システムセキュリティ責任者は、情報セキュリティ責任者が別に指名する場合を除き、情報システムを所管する課室の長とする。

４　情報セキュリティ責任者は、情報システムセキュリティ責任者を指名したとき、及び変更したときは、統括情報セキュリティ責任者にその旨を報告する。

（情報システムセキュリティ管理者）

第１２条　情報システムセキュリティ責任者は、所管する情報システムの管理業務にお

いて必要な単位ごとに情報システムセキュリティ管理者を指名する。
２　情報システムセキュリティ管理者は、所管する管理業務における情報セキュリティ対策を実施する。
３　情報システムセキュリティ責任者は、情報システムセキュリティ管理者を指名したとき、及び変更したときは、統括情報セキュリティ責任者にその旨を報告する。

（情報セキュリティ対策推進体制の整備）
第１３条　最高情報セキュリティ責任者は、機構内の情報セキュリティ対策推進体制を整備する。
２　情報セキュリティ対策推進体制の役割は、次の各号に掲げるものとする。
一　情報セキュリティ関係規程及び対策推進計画の策定に係る事務
二　情報セキュリティ関係規程の運用に係る事務
三　例外措置に係る事務
四　情報セキュリティ対策の教育の実施に係る事務
五　情報セキュリティ対策の自己点検に係る事務
六　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務
３　情報セキュリティ対策推進体制の責任者は、統括情報セキュリティ責任者とする。

（兼務の禁止）
第１４条　情報セキュリティ対策の運用において、次の各号に掲げる者は、兼務することができない。
一　承認又は許可（以下「承認等」という。）の申請者及び当該承認等を行う許可権限者（以下「許可権限者」という。）
二　監査を受ける者及びその監査を実施する者

（上司による承認・許可）
第１５条　業務従事者は、承認等を申請する場合において、自らが許可権限者であるとき、その他許可権限者が承認等の可否を判断することが不適切と認められるときは、当該許可権限者の上司又は適切な者に承認等を申請する。この場合において、当該許可権限者の上司等の承認等を得たときは、当該許可権限者の承認等を得ることを要しない。

第３章　資産管理

（情報システム台帳の整備）
第１６条　統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報シ

ステムのセキュリティ要件に係る事項について、情報システム台帳に整備する。

第４章　情報セキュリティ関連規程の整備

（リスク評価の実施）

第１７条　最高情報セキュリティ責任者は、機構の目的等を踏まえ、自己点検の結果、情報セキュリティ監査の結果、本部監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価する。

（情報セキュリティ対策基準等の策定）

第１８条　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠し、これと同等以上の情報セキュリティ対策が可能となるように、機構における情報セキュリティ対策に関して遵守すべき事項を定めた対策基準を定める。また、対策基準は、機構における業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果及び対策基準や対策推進計画の見直し結果を踏まえた上で定める。

（運用規程及び実施手順の策定）

第１９条　統括情報セキュリティ責任者は、機構における情報セキュリティ対策に関する運用規程及び実施手順を整備し、運用規程及び実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告する。

２　統括情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の規定運用規程を整備する。

（情報セキュリティ対策推進計画の策定）

第２０条　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、対策推進計画を定める。

２　最高情報セキュリティ責任者は、対策推進計画には、機構の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえ、全体方針並びに次の各号に掲げる取組の方針・重点及びその実施時期を含めるものとする。

一　情報セキュリティに関する教育

二　情報セキュリティ対策の自己点検

三　情報セキュリティ監査及び過年度の監査結果（本部監査の結果を含む。）を踏まえた取組

四　情報システムに関する技術的な対策を推進するための取組

五　前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

第５章　情報の取扱いの原則

（情報の格付及び取扱制限）

第２１条　統括情報セキュリティ責任者は、機構の業務で取り扱う情報について、電磁的記録については、機密性、完全性及び可用性の観点から、書面については機密性の観点から、次を全て含む情報の取扱いに関する運用規程を整備する。

一　情報の格付及び取扱制限についての定義

二　情報の格付及び取扱制限の明示等についての手続

三　情報の格付及び取扱制限の継承、見直しに関する手続

第６章　情報セキュリティ関係規程の運用

（情報セキュリティ対策の運用）

第２２条　情報セキュリティ対策推進体制は、第１３条第２項に規定する役割に応じて必要な事務を遂行する。

２　情報セキュリティ責任者又は課室情報セキュリティ責任者は、業務従事者から情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告する。

３　統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告する。

（違反に対する措置）

第２３条　業務従事者は、情報セキュリティ関係規程等への重大な違反を知った場合には、各規程の実施に責任を持つ情報セキュリティ責任者にその旨を報告する。

２　情報セキュリティ責任者は、情報セキュリティ関係規程等への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの確保に必要な措置を講じさせる。

３　情報セキュリティ責任者は、情報セキュリティ関係規程等への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、統括情報セキュリティ責任者及び最高情報セキュリティ責任者に当該違反の内容及びその講じた措置を報告する。

（例外措置）

第２４条　最高情報セキュリティ責任者は、例外措置の適用申請についての審査手続を

定める。
２　例外措置の適用の申請を審査し、許可する者（以下この条において「例外許可権限者」という。）は、統括情報セキュリティ責任者とする。
３　業務従事者は、定められた審査手続に従い、例外許可権限者に例外措置の適用を申請する。ただし、業務の遂行に緊急を要し、当該規定の趣旨を十分尊重した扱いをとることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出る。
４　例外許可権限者は、業務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定する。
５　統括情報セキュリティ責任者は、例外措置の申請状況を踏まえて必要に応じ、情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告する。

第７章　情報セキュリティインシデントへの対応

（情報セキュリティインシデントの発生に備えた体制の整備）
第２５条　最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化する。
２　最高情報セキュリティ責任者は、業務従事者のうちから CSIRT に属する実務担当者等として専門的な知識又は適性を有すると認められる者を選任する。そのうち、機構における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を指名する。また、CSIRT 内の業務統括及び外部との連携等を行う実務担当者等を指名する。
３　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

（情報セキュリティインシデントの発生に備えた事前準備）
第２６条　統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機構関係者への報告手順を整備し、報告が必要な具体例を含め、業務従事者に周知する。
２　統括情報セキュリティ責任者は、、情報セキュリティインシデントの可能性を認知した際の機構外との情報共有を含む対処手順を整備する。
３　統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。
４　統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の

必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備する。

５　統括情報セキュリティ責任者は、情報セキュリティインシデントについて機構外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を機構外の者に明示する。

６　統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認する。

（情報セキュリティインシデントの発生時の対応）

第２７条　業務従事者は、情報セキュリティインシデントの可能性を認知した場合には、機構の報告窓口に報告し、指示に従う。

２　CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。

３　CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告する。

４　CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行う。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システムセキュリティ責任者へ確認を指示する。

５　情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処する。

６　CSIRT は、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、警察への通報・連絡等を行う。

７　CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、対処全般に関する指示、勧告又は助言を行う。

８　CSIRT は、情報セキュリティインシデントに関する対処の内容を記録する。

９　CSIRT は、CYMAT の支援を受ける場合には、支援を受けるに当たって必要な情報提供を行う。

（情報セキュリティインシデントに係る情報共有）

第２８条　CSIRT は、機構の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、経済産業省に連絡する。

２　CSIRT は、情報セキュリティインシデントに関して、機構を含む関係機関と情報共有を行う。

３　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告を行う。

（情報セキュリティインシデントの再発防止策）

第２９条　情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告する。

２　最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示する。

３　第２５条第１項に定める体制は、情報セキュリティインシデントの対処の結果から得られた教訓を、関係する情報セキュリティ責任者等に共有する。

第８章　教育

（情報セキュリティ教育の実施体制の整備・教育実施計画の策定）

第３０条　統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。

２　統括情報セキュリティ責任者は、業務従事者の役割に応じて教育すべき内容を検討し、教育のための資料を整備する。

３　統括情報セキュリティ責任者は、原則として業務従事者が毎年度１回以上は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備する。

４　統括情報セキュリティ責任者は、業務従事者の着任時、異動時（ただし、機構内の異動は除く。）に当該着任又は異動の時から３か月以内に受講できるように、その実施体制を整備する。

５　統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、業務従事者に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直す。

（情報セキュリティ教育の実施）

第３１条　課室情報セキュリティ責任者は、教育実施計画に基づき、業務従事者に対して、情報セキュリティ関係規程に係る教育を適切に受講させる。

２　業務従事者は、教育実施計画に従って、適切な時期に教育を受講する。

３　課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及び CSIRT に属する業務従事者に教育を適切に受講させる。

４　課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任

者及び統括情報セキュリティ責任者に報告する。
５　統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告する。

第９章　評価及び見直し

（自己点検の実施に関する準備）
第３２条　統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定する。
２　情報セキュリティ責任者は、年度自己点検計画に基づき、業務従事者ごとの自己点検票及び自己点検の実施手順を整備する。
３　統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、業務従事者に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直す。

（自己点検の実施）
第３３条　情報セキュリティ責任者は、年度自己点検計画に基づき、業務従事者に自己点検の実施を指示する。
２　業務従事者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施する。

（自己点検結果の評価・改善）
第３４条　情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を統括情報セキュリティ責任者に報告する。
２　統括情報セキュリティ責任者は、機構に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を最高情報セキュリティ責任者に報告する。
３　最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受ける。

第１０章　情報セキュリティ監査

（監査実施計画の策定）
第３５条　情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定める。

２　情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定める。

（監査の実施）

第３６条　情報セキュリティ監査責任者は、監査実施計画に基づき、監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告する。

（監査結果に応じた対処）

第３７条　最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示する。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示する。

２　統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、機構内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

３　情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告する。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告する。

第１１章　情報セキュリティ対策の見直し

（情報セキュリティ対策の見直し）

第３８条　最高情報セキュリティ責任者は、リスク評価に変化が生じた場合には、情報セキュリティ委員会による審議を経て、対策基準や対策推進計画の必要な見直しを行う。

（情報セキュリティ関係規程等の見直し）

第３９条　最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・、情報セキュリティ監査、本部監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策基準について必要な見直しを行う。

２　統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキ

ュリティ監査、本部監査等の結果等を踏まえて情報セキュリティ対策に関する運用規程及び実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告する。

３　統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を踏まえて機構内で横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、機構内の職制及び職務に応じた措置の実施又は指示し、措置の結果について最高情報セキュリティ責任者に報告する。

（対策推進計画の見直し）

第４０条　最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査、本部監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行う。

第１２章　雑則

（本規程の管理部署）

第４１条　この規程を管理する担当課等はリスクマネジメント推進室とする。

附則

（施行期日）

第１条　この規程は、平成２０年２月１５日から施行する。

附則

（施行期日）

第１条　この規程は、平成２２年４月１日から施行する。

附則

（施行期日）

第１条　この規程は、平成２３年４月１日から施行する。

附則

（施行期日）

第１条　この規程は、平成２４年１０月１６日から施行する。

附則

（施行期日）
第１条　この規程は、平成２６年３月３１日から施行する。

附則
（施行期日）
第１条　この規程は、平成２７年４月１日から施行する。

附則
（施行期日）
第１条　この規程は、平成３０年４月１日から施行する。

附則
（施行期日）
第１条　この規程は、令和元年１０月１５日から施行する。

附則
（施行期日）
第１条　この規程は、令和２年２月２８日から施行する。

附則
（施行期日）
第１条　この規程は、令和２年３月２６日から施行する。

附則
（施行期日）
第１条　この規程は、令和２年５月１５日から施行する。

附則
（施行期日）
第１条　この規程は、令和４年１０月２１日から施行する。

附則
（施行期日）
第１条　この規程は、令和５年４月１日から施行する。

附則

（施行期日）

第１条　この規程は、令和７年１月３０日から施行する。