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対策を確実に行うための基本的な枠組みに必要な事項を定め、もって機構の保有する情報資産の安全性の確保及び信頼性の向上に資することを目的として制定する。

（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　業務従事者　役職員等（機構の役員、職員、非常勤職員、客員研究員、認定審査員、製品事故調査員、客員調査員、電力安全技術調査員及び各種委員会委員（ただし、委嘱状が交付された者に限る。））、派遣職員、共同研究従事者及び共同事業従事者のうち、機構の指揮命令に服し、かつ機構の管理対象である情報資産を取り扱う者をいう。

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

三　政府統一基準　内閣府が定める政府機関の情報セキュリティ対策のための統一基準をいう。

四　取扱制限　情報資産の取扱いに関する制限をいう。

五　明示等　情報を取り扱う全ての者が当該情報の格付け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。

六　例外措置　業務従事者がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

七　記録媒体　情報が記録され、又は記載されたものをいう。

八　要保護情報　要機密情報、要保全情報、要安定情報をいう。

九　要機密情報　機構の業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成２３年４月１日内閣総理大臣決定。）に定める秘密文書に相当する機密性を要する情報を含む情報及び独立行政法人等の保有する情報の公開に関する法律（平成１３年法律第１４０号）（以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報をいう。

十　要保全情報　機構の業務で取り扱う情報のうち、その改ざん、誤謬又は破損により、国民の権利が侵害され又は機構の業務の的確な遂行に支障（ただし、軽微なものを除く。）を及ぼすおそれがある情報をいう。

十一　要安定情報　機構の業務で取り扱う情報のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は機構の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

十二　委託先等　情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を請け負った者をいう。

十三　外部委託等　情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を機構外の者に請け負わせることをいう。

十四　機器等　情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

十五　情報システム　情報処理及び通信に係るシステムをいう。

十六　機構外での情報処理　機構外において機構が管理する場所以外にて業務の遂行のための情報処理を行うことをいう。

なお、オンラインで機構外から機構の情報システムに接続して、情報処理を行う場合だけでなく、オフラインで行う場合も含むものとする。

十七　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。

第２章　組織と体制の整備

（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は、機構の情報セキュリティに関する対策基準及び機構における情報セキュリティに関する他の重要な事項について審議を行うとともに、機構における情報セキュリティに関する認識の統一を図り、情報セキュリティに関する経営的な判断を行う。ただし、最高情報セキュリティ責任者が必要と認める場合は、一部の技術的な事項について、最高情報セキュリティ責任者が指定した者にその審議を委任することができる。

３　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、デジタル統括官、各部門（組織規程第２条に定める「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）の長、企画管理部経営企画課長、

企画管理部人事企画課長及び企画管理部情報システム課長とする。

４　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。委員長代理を置く場合は、統括情報セキュリティ責任者が兼務する。

５　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。

６　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。

７　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。

８　情報セキュリティ委員会の庶務は、情報統括官室が行う。

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　本条第５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）で定め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　本条第５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　機構に最高情報セキュリティアドバイザーを置く。

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を行う。

３　最高情報セキュリティアドバイザーは、組織規程第３０条に定める情報統括責任者補佐官とする。

（情報セキュリティ監査責任者）

第６条　機構に情報セキュリティ監査責任者を置く。

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。

３　情報セキュリティ監査責任者は、監査室長とする。

（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

一及び第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。）ごとに情報セキュリティ責任者を置く。ただし、監査室及びデジタル統括官は企画管理部に置かれるものとして取り扱うこととする。

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。

３　情報セキュリティ責任者は、第１項に定める部等の長とする。

（統括情報セキュリティ責任者）

第８条　機構に統括情報セキュリティ責任者を置く。

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。

３　統括情報セキュリティ責任者は、情報統括官とする。

４　統括情報セキュリティ責任者は、全ての情報セキュリティ責任者に対する連絡網を整備しなければならない。

（区域情報セキュリティ責任者）

第８条の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置く。

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。

３ 統括情報セキュリティ責任者は、要管理対策区域の範囲を定め、区域情報セキュリティ責任者を指定しなければならない。

（情報システムセキュリティ責任者）

第９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組織規程第７条に規定する監査室及びデジタル統括官、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。

５　統括情報セキュリティ責任者は、全ての情報システムセキュリティ責任者に対する連絡網を整備しなければならない。

（情報システムセキュリティ管理者）

第１０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。

４　統括情報セキュリティ責任者は、全ての情報システムセキュリティ管理者に対する連絡網を整備しなければならない。

（課室情報セキュリティ責任者）

第１１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　課室情報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、課室の長とする。

４　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。

５　統括情報セキュリティ責任者は、全ての課室情報セキュリティ責任者に対する連絡網を整備しなければならない。

（兼務の禁止）

第１２条　次に掲げる者は、相兼ねることができない。

一　この規程において定める承認又は許可を求める者と当該承認又は当該許可を行う者（以下「承認権限者等」という。）

二　監査を受ける者と当該監査を実施する者

（上司による承認・許可）

第１３条　業務従事者は、承認等を申請する場合において、自らが承認権限者等であるとき、その他承認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、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得なければならない。

（情報セキュリティの適切な管理のための連絡及び調整）

第１４条　統括情報セキュリティ責任者は、重要事項の決定のためその他必要があると認めるときは、運営会議において、各部等と連絡及び調整を行わなければならない。

第３章　情報の取扱いの原則

（情報の作成と入手、利用）

第１５条　業務従事者は、機構の業務の遂行以外の目的で、情報を作成し、又は入手してはならない。

２　業務従事者は、機構の業務の遂行以外の目的で、情報を利用してはならない。

（重要度に応じた取扱い）

第１６条　情報の取扱いに当っては、その情報の重要度に応じた適切な措置を講じなければならない。

２　前項の重要度は第２０条の情報の格付けにより分類する。

第４章　対策基準及び対策推進計画の策定

（情報セキュリティ対策基準の策定）

第１７条　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して遵守すべき事項を定めた情報セキュリティ対策基準（以下「対策基準」という。）を定めなければならない。

（情報セキュリティ対策推進計画の策定）

第１８条　最高情報セキュリティ責任者は、機構の情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めなければならない。

２　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なければならない。

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

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

３　最高情報セキュリティ責任者は、対策推進計画の実施状況の評価を行い、必要に応じて対策推進計画の見直しを行わなければならない。

第５章　情報セキュリティ関係規程の整備

（実施手順等の整備）

第１９条　統括情報セキュリティ責任者は、機関等における情報セキュリティ対策に関する実施手順を整備し、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しなければならない。

２　情報セキュリティ責任者は、自らが統括する部等で所管する情報システムについて、この規程及び対策基準で定める事項のほか、必要がある場合は、情報セキュリティ対策に関する事項を独自に定めることができる。

（情報の格付け）

第２０条　最高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、当該情報の格付け及び取扱制限の指定並びに取扱制限の明示等の規定を定めなければならない。

（機器等の購入）

第２１条　最高情報セキュリティ責任者は、機器等の選定基準を定めなければならない。

２　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視点を加味して、機器等の購入時の確認・検査手続きを定めなければならない。

３　機器等の購入の実施における手続については、別に定める。

（外部委託等）

第２２条　最高情報セキュリティ責任者は、外部委託等（ソフトウェア開発、情報処理、賃貸借、調査・研究等をいい、その詳細は統括情報セキュリティ責任者が別に示すものとする。）の対象としてよい情報システム及び委託先等によるアクセスを認める情報資産を判断する基準を定めなければならない。

２　最高情報セキュリティ責任者は、委託先等の選定手続及び選定基準を定めなければならない。

（機構外での情報処理の制限）

第２３条　最高情報セキュリティ責任者は、要保護情報について機構外での情報処理を行う場合の安全管理措置についての規定を定めなければならない。

２　最高情報セキュリティ責任者は、要保護情報を取り扱う情報システムを機構外に持ち出す場合の安全管理措置についての規定を定めなければならない。

３　最高情報セキュリティ責任者は、要保護情報について機構支給以外の情報システム

により情報処理を行う場合に講ずる安全管理措置についての規定を定めなければならない。

（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規定を定めなければならない。

２　例外措置の適用の申請を審査する者（以下「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、例外措置の適用を受けようとする場合には、第１項に定めた審査手続に従い、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する等の場合であって、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を実施しないことが不可避のときは、事後速やかに申請を行う。業務従事者は、申請の際に次の事項を含む項目を明確にし、申請しなければならない。

一　申請者の情報（氏名、所属、連絡先）

二　例外措置の適用を申請する情報セキュリティ関係規程の適用箇所（規程名と条項等）

三　例外措置の適用を申請する期間

四　例外措置の適用を申請する措置内容（講ずる代替手段等）

五　例外措置の適用を終了したときの報告方法

六　例外措置の適用を申請する理由

４　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しなければならない。

（違反に対する措置）

第２５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、各規定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しなければならない。

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なければならない。

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しなければならない。

第６章　障害･事故等への対応

（障害･事故等の発生に備えた事前準備）

第２６条　最高情報セキュリティ責任者は、情報セキュリティに関する障害･事故等（インシデント及び故障を含む。以下「障害･事故等」という。）が発生した場合に対処の一元管理を行い、被害の拡大を防ぐとともに、障害･事故等から復旧するため、実務担当者等を含めた体制を整備しなければならない。

２　前項に定める体制の責任者は、統括情報セキュリティ責任者とし、業務統括を行うとともに外部との連携等を行う際の窓口とする。

３　統括情報セキュリティ責任者は、第１項に定める体制に属する職員等に教育を適切に受講させなければならない。

４　統括情報セキュリティ責任者は、障害･事故等について業務従事者から情報セキュリティ責任者への報告手順を整備し、当該報告手順を全ての業務従事者に周知しなければならない。

５　統括情報セキュリティ責任者は、障害･事故等が発生した際の対処手順を整備しなければならない。

６　統括情報セキュリティ責任者は、障害･事故等について機構外からの報告を受けるための窓口を設置しなければならない。

（障害･事故等の発生時の対応）

第２７条　業務従事者は、障害・事故等を発見したときは、前条第４項に定める手順に従い、障害・事故等の内容を直ちに所属の長に報告しなければならない。

２　所属の長は、必要に応じて前条第４項に定める手順に従い、障害・事故等の内容を連絡しなければならない。

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であると評価した場合は、前条第４項に定める手順に従い、関係部署等に速やかに連絡するとともに最高情報セキュリティ責任者に報告しなければならない。また、情報セキュリティインシデントではないと評価した場合であっても、注意喚起等が必要と考えられるものについては、関係する者に情報共有を行わなければならない。

４　第２項により連絡を受けた情報システム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、障害・事故等への対処が必要と判断した場合は、統括情報セキュリティ責任者の指示又は勧告の下、被害の拡大防止等を図るための応急措置を実施するとともに、障害・事故等の対処を実施する者（以下「対処実施者」という。）を選定し、対処すべき旨の指示を与えなければならない。

５　対処実施者は、対処方針を決定し情報システムセキュリティ責任者又は課室情報セ

キュリティ責任者の承認を得なければならない。ただし、前条第５項に定めた手順において、対処方針が規定されている場合には、この限りではない。

６　対処実施者は、その承認された対処方針に従い障害・事故等に対処する。

７　対処実施者は、対処の実施結果について情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告し、対処が確実に実施されたことの確認を受けなければならない。

８　情報システム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、情報セキュリティ責任者、統括情報セキュリティ責任者及び関係部署等に報告しなければならない。

（障害･事故等の再発防止策）

第２８条　情報セキュリティ責任者は、障害･事故等が発生した場合には、障害･事故等の原因を調査し、必要な場合は情報システムセキュリティ責任者若しくは課室情報セキュリティ責任者及び対処実施者に指示し、再発防止策を策定させなければならない。また、策定した再発防止策を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報告しなければならない。

２　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は、策定された再発防止策について、その実施に必要となる措置があれば当該措置を実施しなければならない。

３　統括情報セキュリティ責任者は、障害･事故等の対処及び再発防止策から得られた対処手順等の改善や情報セキュリティ水準の改善につなげられるような事項を関係する情報セキュリティ責任者等に共有しなければならない。

第７章　教育

（情報セキュリティ対策の教育の実施）

第２９条　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等について、業務従事者に対し、その啓発をしなければならない。

２　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等について、業務従事者に教育すべき内容を検討し、教育のための資料を整備しなければならない。

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回以上受講できるように、情報セキュリティ対策の教育に係る計画を企画及び立案するとともに、その実施体制を整備しなければならない。

４　統括情報セキュリティ責任者は、原則として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、情報セキュリティ対策の教育に係る計画を企画し、及び立案するとともに、その実施

体制を整備しなければならない。
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、情報セキュリティ対策の教育に係る計画を見直さなければならない。
６　統括情報セキュリティ責任者は、業務従事者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備しなければならない。
７　課室情報セキュリティ責任者は、情報セキュリティ対策の教育の受講状況を記録し、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しなければならない。
８　課室情報セキュリティ責任者は、業務従事者の情報セキュリティ対策の教育の受講が達成されていないと認識した場合には、その未受講者に対して、受講を勧告する。業務従事者が当該勧告に従わない場合には、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その旨を報告するとともに、統括情報セキュリティ責任者の指示に従いその未受講者に対して必要な措置を講じさせなければならない。
９　統括情報セキュリティ責任者は、毎年度１回、最高情報セキュリティ責任者に業務従事者の情報セキュリティ対策の教育の受講状況について分析、評価し、報告しなければならない。

（情報セキュリティ対策の教育の受講）
第３０条　業務従事者は、原則として毎年度１回以上、情報セキュリティ対策の教育に係る計画に従って当該教育を受講しなければならない。
２　業務従事者は、着任時又は異動時（ただし、機構内の異動は除く。）に新しい職場等で、情報セキュリティ対策の教育の受講方法について課室情報セキュリティ責任者に確認しなければならない。
３　業務従事者は、情報セキュリティ対策の教育を受講できない場合には、その理由について、課室情報セキュリティ責任者に報告しなければならない。報告を受けた課室情報セキュリティ責任者は、その理由を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しなければならない。

第８章　評価及び見直し

（自己点検に関する年度計画の策定）
第３１条　統括情報セキュリティ責任者は、年度自己点検計画を策定しなければならない。

（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、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しなければならない。
２　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さなければならない。

（自己点検の実施）
第３３条　統括情報セキュリティ責任者は、年度自己点検計画に基づき、業務従事者に対して、自己点検の実施を指示しなければならない。
２　業務従事者は、統括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し、その結果を報告しなければならない。

（自己点検の結果の評価）
第３４条　情報セキュリティ責任者は、業務従事者による自己点検の結果について、自らが担当する組織のまとまり、取り扱う情報等の特性に応じた課題や、改善すべき点があるか否かを確認するなどの観点から自己点検結果を分析し、点検項目の履行状況を評価しなければならない。また、評価結果を統括情報セキュリティ責任者に報告しなければならない。
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、評価しなければならない。また、評価結果を最高情報セキュリティ責任者に報告しなければならない。

（自己点検に基づく改善）
第３５条　業務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲内で改善できると判断したことは改善しなければならない。
２　最高情報セキュリティ責任者は、自己点検の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なければならない。

（年度監査計画の策定）
第３６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年度監査計画を策定しなければならない。

（監査の実施に関する指示）
第３７条　最高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て必要と判断した場合、情報セキュリティ監査責任者に対して、対策推進計画又は年度監

査計画で計画されたこと以外の監査の実施を指示しなければならない。

（個別の監査業務における監査実施計画の策定）

第３８条　情報セキュリティ監査責任者は、対策推進計画、年度監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定しなければならない。

（監査の実施に係る準備）

第３９条　情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者として指名しなければならない。

２　情報セキュリティ監査責任者は、必要に応じ、機構外の者に監査の一部を請け負わせることができるものとする。

（監査の実施）

第４０条　情報セキュリティ監査実施者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施しなければならない。

２　情報セキュリティ監査実施者は、この規程及び対策基準が政府統一基準に準じていることを確認し、準じていない場合は監査調書に指摘しなければならない。

３　情報セキュリティ監査実施者は、実施手順がこの規程及び対策基準に準じていることを確認し、準じていない場合は監査調書に指摘しなければならない。

４　情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、被監査部門における実際の運用が情報セキュリティ関係規程等に準じていることを確認し、準じていない場合は監査調書に指摘しなければならない。

５　情報セキュリティ監査実施者は、監査調書を作成し、情報セキュリティ監査責任者に報告しなければならない。

６　情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、最高情報セキュリティ責任者へ報告しなければならない。

（監査結果への対処）

第４１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対して、指摘されたことに対する対処の実施を指示しなければならない。

２　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、監査を受けた部門以外の部門等においても同種の課題及び問題点がある可能性が高く、かつ、緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部門等

の情報セキュリティ責任者に対しても、同種の課題及び問題点の有無を確認するように指示しなければならない。

３　統括情報セキュリティ責任者は、監査報告書等に基づく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しなければならない。

４　情報セキュリティ責任者は、監査報告書等に基づく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しなければならない。

５　最高情報セキュリティ責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程等の妥当性を評価し、必要に応じて当該規程等の見直しを指示しなければならない。

（情報セキュリティ対策の見直し）

第４２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・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、情報セキュリティ関係規程等について必要な見直しを行わなければならない。

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・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しなければならない。

３　業務従事者は、情報セキュリティ関係規程等に課題及び問題点が認められる場合には、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に当該課題又は問題点について指摘しなければならない。

４　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、情報セキュリティ関係規程等に課題及び問題点が認められる旨の指摘を受けた場合は、統括情報セキュリティ責任者に報告するとともに、必要に応じてその措置を講じなければならない。

５　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こと。

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。