○奈良教育大学情報セキュリティポリシー

（平成 19 年３月 23 日規則第 40 号）

改正 平成 23 年３月 24 日規則第 22 号　平成 26 年３月 20 日規則第 15 号
平成 27 年 10 月 23 日規則第 49 号　平成 28 年９月 14 日規則第 31 号
平成 30 年７月 18 日規則第 26 号　令和４年４月１日

１　情報システム運用基本方針

(情報システムの目的)

１．１　奈良教育大学（以下「本学」という。）情報システムは、本学の理念である「学芸の理論とその応用とを教授研究し、高い知性と豊かな教養とを備えた人材、特に有能な教育者を育てるとともに、この地方に特色のある文化の向上を図る」ことの実現のため、本学のすべての教育・研究活動及び運営の基盤として設置され、運営されるものである。

(運営の基本方針)

１．２　前条の目的を達成するため、本学情報システムは、円滑で効果的な情報流通を図るために、情報システム運用基準により、秩序と安全性をもって安定的かつ効率的に運用され、全学に供用される。

(利用者の義務)

１．３　本学情報システムを利用する者は、奈良国立大学機構情報セキュリティポリシー（令和４年度機構規程第 23 号）（以下「機構ポリシー」という。）及び奈良国立大学機構情報システム運用・管理規程（令和４年度機構規程第 25 号）（以下「運用・管理規程」という。）、並びに、本方針及び運用基準に沿って利用し、別に定める運用と利用に関する実施規則を遵守しなければならない。

(罰則)

１．４　本方針に基づく規定等に違反した場合の利用の制限及び罰則は、それぞれの規則に別に定めることができる。

２　情報システム運用基準

２．１　本学情報システムの運用については、この運用基準の定めるところによる。

(適用範囲)

２．２　この運用基準は、本学情報システムを運用・管理・利用するすべての者に適用する。

(定義)

２．３　この運用基準において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　情報システム

情報処理及び情報ネットワークに係わるシステムで、次のものをいう。

(1)　大学により所有又は管理されているもの

(2)　大学との契約あるいは他の協定に従って提供されるもの

(3)　前記(1)、(2)以外で大学の情報ネットワークに接続を許可されたもの

なお、本方針においては事務処理に供され、事務局が運用責任を持つ情報システムを、研究・教育用の情報システムと区別するため、事務情報システムという。

二　情報ネットワーク

情報ネットワークは次のものをいう。

(1)本学により、所有又は管理されているすべての情報ネットワーク

(2)本学との契約あるいは他の協定に従って提供されるすべての情報ネットワーク

三　情報

情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

四　情報資産（電子・電磁的なもの）

本学の情報システム、情報ネットワークに接続された情報機器並びにそこで取り扱われる情報をいう。

五　実施規則

本学が定める奈良教育大学情報セキュリティポリシー（以下「ポリシー」という。）に基づいて策定される規則や手順及び計画をいう。

六　手順

実施規則に基づいて策定される具体的な手順、マニュアル及びガイドラインを指す。なお、情報資産管理の具体的なマニュアルを情報資産管理手順という。

七　情報セキュリティインシデント対応手順

奈良教育大学の最高情報セキュリティ責任者補佐（以下「CISOA」という。）が策定する本学の情報セキュリティインシデント対応手順を指す。

八　利用者

職員等及び学生等で、利用許可を受けて本学情報システムを利用するものをいう。

九　職員等

本学に勤務する国立大学法人奈良国立大学機構（以下「機構」という。）の常勤又は非常勤の役員及び職員(派遣職員を含む)をいう。

十　学生等

本学学部学生、大学院学生、研究生、科目等履修生、留学生、附属学校園生徒・児童・幼児、及び研究者等をいう。

十一　臨時利用者

職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

十二　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

十三　電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

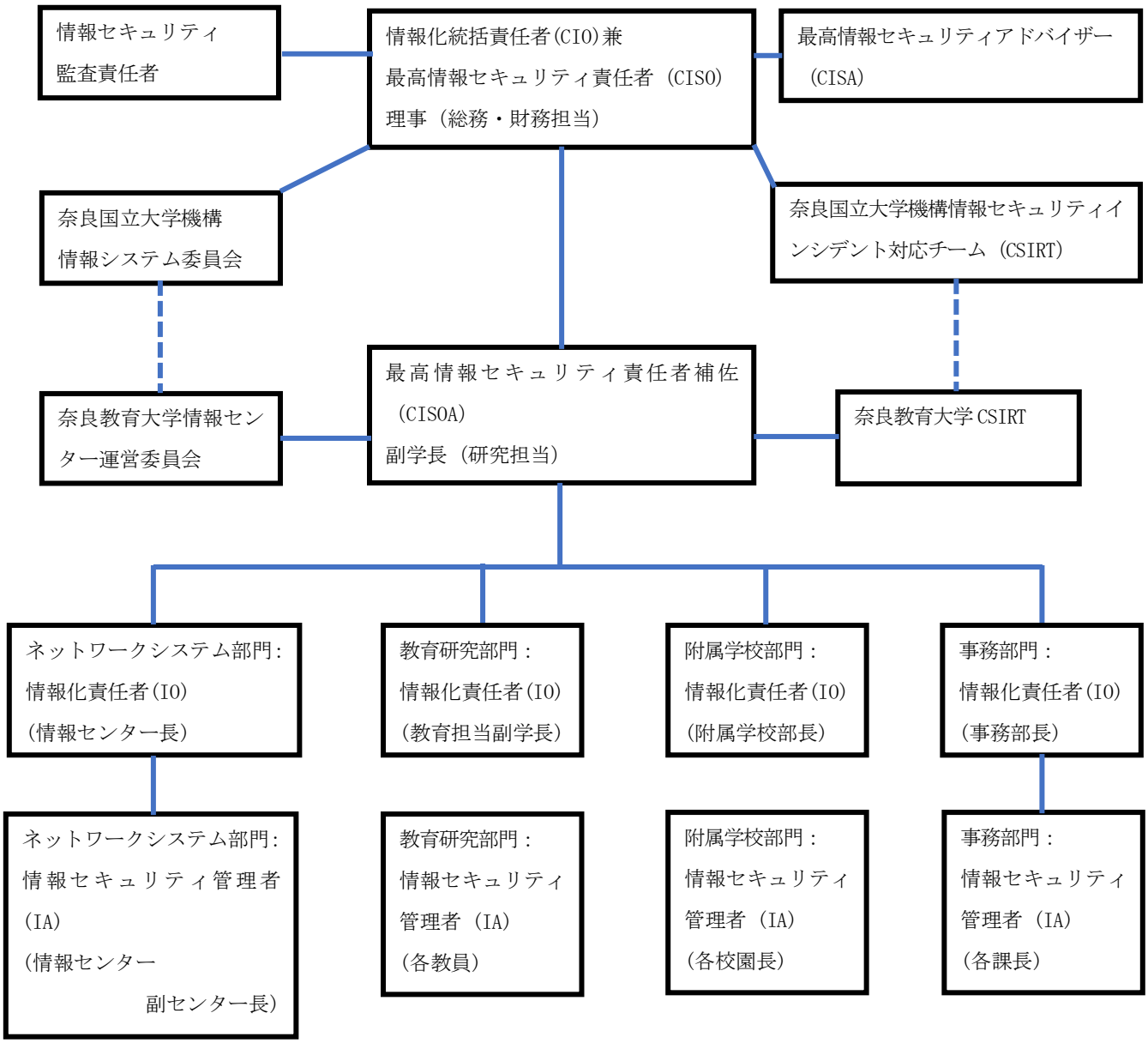
十四　その他の定義については、基本規程の定めるところによる。

３　組織と体制

(管理・運用組織の構成)

３．１　情報セキュリティを確保するための組織を図１に示す。

図１　組織の構成図



３．１．１　情報化統括責任者（CIO)

機構ポリシー第７条に基づく、機構及び機構の設置する国立大学（以下「各大学」という。）の情報システムの運用責任者をいう（以下「CIO」という)。

３．１．２　最高情報セキュリティ責任者（CISO)

機構ポリシー第７条に基づく、機構及び各大学の情報セキュリティ対策の円滑な運用についての統括的な役割を担う者をいう（以下「CISO」という)。

３．１．３　最高情報セキュリティアドバイザー（CISA)

機構ポリシー第７条に基づく、情報セキュリティに関する専門的知識及び経験を有した専門家をいう（以下「CISA」という)。

３．１．４　副情報化統括責任者（副CIO)

機構ポリシー第８条に基づく、各大学の情報システムのポリシー及び関連規程並びに手順等の整備と情報セキュリティに関する教育を企画・実施する者いう（以下「副 CIO」という)。

３．１．５　最高情報セキュリティ責任者補佐（CISOA）

機構ポリシー第８条及び第９条に基づく、最高情報セキュリティ責任者を補佐する者として、機構及び各大学の情報システムのセキュリティ関する連絡と通報において各大学を代表する者をいう（以下本学の CISOA を「CISOA」という)。

３．１．６　情報化統括責任者補佐（CIO 補佐）

機構ポリシー第９条に基づく、機構の各大学の情報システムのポリシー及び関連規程並びに手順等の整備と情報セキュリティに関する教育を企画・実施する者いう。

３．１．７　奈良国立大学機構情報システム委員会

機構ポリシー第１３条に基づく、情報システムの円滑な運用のための最終意思決定機関をいう（以下「情報システム委員会」という)。

３．１．８　奈良教育大学情報センター運営委員会

情報システム委員会の下に設置される奈良教育大学情報システム部会の業務として本学セキュリティポリシーの策定及び情報セキュリティに関する事項の企画立案を行う（以下「委員会」という)。

３．１．９　情報セキュリティ監査責任者

機構ポリシー第１１条に基づき、機構に置かれる、機構の情報セキュリティの監査に関する業務を統括する者をいう。

３．１．１０　情報化責任者（IO)

機構ポリシー第１０条に基づき機構及び各大学に置かれる、各部局における情報システム上での各種問題に対する処置を担当する者をいう（以下「IO」という。）本学においては、ネットワークシステム部門、教育研究部門、附属学校部門及び事務部門の所管するシステムの情報セキュリティに関する業務を統括するため、各々に IO を置く。

３．１．１１　情報セキュリティ責任者（IA)

情報セキュリティ対策を実施するため、各部門の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セキュリティ管理者(IA)を置く。

３．１．１２　奈良国立大学機構情報セキュリティインシデント対応チーム（CSIRT)

機構ポリシー第１２条に基づく、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るための組織をいう（以下「機構 CSIRT」という)。

３．１．１３　奈良教育大学 CSIRT

機構 CSIRT の下に設置される、本学の情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るためのチームをいう（以下「CSIRT」という)。CSIRT の運用に関して必要な事項は別に定める。

３．２　役割の分離及び例外措置

３．２．１　機構ポリシー第１４条に基づき、情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないものとする。

(1) 承認又は許可事案の申請者とその承認又は許可を行う者(以下「承認権限者等」という。)

(2) 監査を受ける者とその監査を実施する者

３．２．２　前項の定めに係わらず，職員は，承認権限者等が有する職務上の権限等から，当該承認権限者等が承認又は許可(以下「承認等」という。)の可否の判断を行うことが不適当と認められる場合には，当該承認権限者等の上司に承認等の申請をする。この場合において，当該承認権限者等の上司の承認等を得たときは，当該承認権限者等の承認等を得ることを要しない。

３．２．３　職員は，前項の場合において承認等を与えたときは，承認権限者等に係る遵守事項に準じて，措置を講ずる。

４　情報資産の管理

４．１　機構ポリシー第１５条に基づき、情報システム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当該情報の格付け及び取り扱い制限の基準並びに格付け及び取り扱い制限を明示する手順を整備する。

４．２　職員等は、業務の遂行以外の目的で、情報システムに係る情報を作成し又は入手しないこと。

４．３ 情報システムには、アクセス可能な担当者・利用者を定め、適切なアクセス制限を行う。

４．４　IA は、管理する情報システムの内容について変更があった場合、速やかに IO に報告しなければならない。

なお、IO は、上記報告を受けた場合、速やかに委員会に報告しなければならない。

４．５　IA は、必要に応じバックアップをとり、滅失・改ざん等があった場合は、速やかに復旧できるようにしておかなければならない。

４．６　情報機器及び記憶媒体の処分にあたり、情報の消去を行い、特に重要な情報については物理的処分を行わなければならない。

また、レンタル機器の撤去に際しても記憶媒体の処理については、データの復元ができないようにしなければならない。

５　情報機器の管理・運用

５．１　クライアント機器

クライアント機器とは、常時もしくは一時的に情報ネットワークに接続し、主として個人的な業務で用いられ、情報システムへアクセスすることで処理を行う機器をいう。VPN(Virtual Private Network)接続によって、情報ネットワークに接続する学外のコン

ピュータも含まれる。

(クライアント機器のセキュリティ)

５．１．１　IA は、当該システムに接続する(一時的なものも含め)すべてのクライアント機器(以下「機器」という)を把握しておかなければならない。

５．１．２　各機器の IA は、その設置場所も含め、適宜施錠するなど機器の盗難対策を施さねばならない。

５．１．３　情報ネットワークへの機器等の接続については、ネットワークシステム部門の IA の許可を必要とし、一時的であっても許可無しに接続することはできない。

また、許可された IP アドレス以外を使用することはできない。

５．２　サーバ機器

サーバ機器とは、情報ネットワークに常時接続し、複数のクライアント機器からアクセスされ、共同で利用される情報機器をいう。また、情報ネットワークに接続されない情報資産であっても、職員等が業務遂行のために作成した情報を継続的に記録する情報機器を含む。

(サーバ機器のセキュリティ)

５．２．１　委員会はすべてのサーバ機器に関し、設置場所を把握すること。また、IO 及び IA は、設置場所の入退出管理を徹底しなければならない。

なお、特に機構ポリシー第７条第３項で CIO が指定する情報システム及び重要度の高い機能・情報を有するサーバにあっては別途これを定め、その設置場所を情報管理区域として十分な管理を行わなければならない。

５．２．２　特に重要度の高い情報を有するサーバの電源供給に対しては無停電電源装置などを経由し、常に安定な稼働を保証しなければならない。

５．２．３　情報ネットワークへのサーバの接続については、ネットワークシステム部門の IA の許可を必要とし、一時的であっても許可無しに接続することはできない。また、許可された IP アドレス以外を使用することはできない。

５．２．４　サーバ機器に記録されるデータは必要に応じバックアップし、バックアップしたメディアは管理が徹底した場所に保管しなければならない。

５．２．５　サーバ障害により著しく業務等に影響を及ぼすものについては、多重化を図らなければならない。

５．２．６　特に重要度の高い情報を有するサーバにあっては、耐震を考慮した措置を施し、情報管理区域には火災の一次消火手段を整備しなければならない。

５．３　ネットワーク機器のセキュリティ

５．３．１　情報ネットワークの基幹部におかれたルータや、各棟において情報ネットワークを分岐する主要なスイッチングハブは、許可された IA 以外は使用できないように対策を施さなければならない。

５．３．２　基幹部におかれたネットワーク機器や、棟毎にネットワークを分岐する主要な

スイッチングハブは、その設置場所をできる限り秘匿しなければならない。

５．３．３　情報ネットワークには、情報ネットワーク接続承認を得たコンピュータ以外は接続してはならない。

学生及びその他の利用者のための共同利用コンピュータを接続する際、職員等が利用するネットワークとはサブネットや無線 LAN を利用するなどして極力分離しなければならない。

６　セキュリティに関わる役割と責任

(役割と責任)

６．１奈良教育大学最高情報セキュリティ責任者補佐（CISOA）

６．１．１　CISOA は、ポリシーに基づき、学内のすべての情報セキュリティに関する総括的な権限と責任を有する。

６．１．２　CISOA は、各部門の IO を通じ、すべての部門にポリシーの遵守を励行させる。

６．１．３　CISOA、情報システムの円滑な運用に必要な措置を各部門の IO に指示する。

６．１．４　CISOA は、情報システム委員会、教育研究評議会、執行役会、教授会等に情報セキュリティに関する重要事項の報告もしくは勧告を行う。

(外部委託事業者の管理)

６．１．５　CISOA は、機構ポリシー第１７条により、本学情報システムの運用業務のすべてまたはその一部を第三者に委託する場合は、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

６．２　情報化責任者(IO)

６．２．１　IO は、当該部門の情報システムのセキュリティが円滑に運用されるように情報セキュリティの保持と強化のための技術的な調査検討と対策の実施にあたる。

６．２．２　IO は、当該部門において情報セキュリティを守るため必要と判断した場合は、緊急避難措置をとることができる。

６．３　情報セキュリティ管理者(IA)

IA は、個々の情報システムを維持・管理する者で、セキュリティを維持するための実質的な責任をもつ。情報システムの管理は、本学職員等に限り、学生等にその管理を任せてはならない。

６．４　教育・研修

６．４．１　CISOA は、情報システム委員会が制定する教育の年度計画に従い、各部門の利用者向けの教育・研修の実施しなければならない。

６．４．２　委員会は、CISOA が行う研修プログラムの実施に必要な措置及び支援を行わなければならない。

６．４．３　利用者は、CISOA が行う教育・研修に参加し、機構ポリシー、運用・管理規程並びに本学ポリシー及び実施規則を理解し、遵守しなければならない。

６．５　事故・障害の報告

６．５．１　利用者は、情報セキュリティに関する事故、情報システムの不審な動作、公開情報の改ざん、情報システム上の障害及び誤動作を発見した場合は、職員等又は、奈良国立大学機構が設置する情報セキュリティインシデント対応窓口（以下「対応窓口」という）に直ちに報告しなければならない。また、職員等は報告のあった事故・障害に対し情報セキュリティインシデント対応手順に従い適切に対応する。

６．５．２　職員等は報告のあった事故・障害に対し情報セキュリティインシデント対応手順に従い適切に対応するとともに、IO または IA 並び対応窓口に直ちに報告しなければならない。

６．５．３　IA は、報告のあった事故等について IO に報告するとともに情報セキュリティインシデント対応手順に従い適切に対応する等必要な措置を講じなければならない。

６．５．４　IO は報告のあった事故等について情報セキュリティインシデント対応手順に従い適切に対応する等必要な措置を講じなければならない。

６．５．５　利用者に対する情報セキュリティの事故・障害の通知は、問題の程度に応じた適切な表現に配慮し、速やかに行わなければならない。

６．５．６　学内からの不正アクセスによって学外に被害を及ぼし、その事実関係の説明を被害者または第三者から求められた場合は、実施規則に従い適切に対応する。

６．６　ID の発行・パスワード管理・アクセス記録管理

６．６．１　IO は、情報システムの利用資格者の規定を定め、その規定に基づく利用資格者以外に ID・パスワードを発行してはならない。また、利用資格を失った利用者の ID･パスワードは直ちに削除されなければならない。

６．６．２　利用者は自己のパスワードを他に示してはならない。また、容易に解読できるパスワードを設定してはならない。

６．６．３　利用者は、他の利用者の ID・パスワードを使用してはならない。

６．６．４　利用者は、いかなる場合も他の利用者のパスワードを聞き出してはならない。

６．６．５　IA がパスワードの変更を求めた場合、利用者はその指示に従わなければならない。

６．６．６　IA は、必要に応じアクセス記録を一定の期間保存しなければならない。

６．７　本学外の情報セキュリティ水準の低下を招く行為の防止

６．７．１　CISOA は、機構ポリシー第１６条の規程に基づき、本学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規程を整備する。

６．７．２　本学情報システムを運用・管理・利用する者は、原則として、本学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

(不正アクセス等への対応)

６．８　IO 及び IA は、外部または内部からの不正アクセスを検出した場合、実施規則に従い、関連する通信の遮断または該当する情報機器の切り離しを実施するとともに、不正ア

クセスが継続する場合、当該情報機器またはそれを接続するネットワークについて定常的な利用の停止などの抑止措置をとることができる。

(臨時利用者)

６．９　臨時利用者に本学の情報システムを一時的に使用させる場合においては、本学の担当者の責任においてポリシーを厳守させる適切な措置を施さなければならない。

７　ネットワーク接続

(学外接続)

７．１　端末は原則として情報ネットワークに接続し、学外との直接接続は禁止する(PPP サーバ、外部ネットワークへの物理的接続、VPN 装置及びソフトウェア等を含む)。

(ネットワーク設計)

７．２　委員会の許可なしに情報ネットワークの改変を行ってはならない。

７．３　学生及びその他の利用者が、共通で利用できるネットワークは、可能な限り職員等が利用するネットワークと分離しなければならない。

７．４　ネットワーク機器は、不正アクセス、機器障害が起きないよう常に十分な管理が行われなければならない。

７．５　委員会は、適宜適切なセキュリティ機器等を導入し、外部からの不正アクセスに対処しなければならない。

(端末機器)

７．６　情報ネットワークに接続する端末は原則としてウィルス防止ソフトを備えていなければならない。また、セキュリティホールを有するソフトウェアの使用に際しては適宜改善しなければならない。なお、管理が不適切な場合は、IA が適切な指示を行う。

８　法令の遵守と違反への対応

(法令の遵守)

８．１　利用者は、使用する情報資産について次の法令を遵守し、これに従わなければならない。

(1) 不正アクセス行為の禁止等に関する法律

(2) 著作権法

(3) 独立行政法人等の保有する電子計算機処理に係る個人情報の保護に関する法律等

(情報セキュリティに関する違反に対する対応)

８．２　CISOA は、ポリシーに違反した者について、利用者を管理する関係委員会等に対し違反行為の報告を行う。

９　評価と見直し

９．１　委員会は、利用者のポリシーの遵守状況を把握し、定期的に評価し、見直しを行わ

なければならない。

９．２　IO は、委員会の下、情報システムに対する情報セキュリティ診断を実施し、委員会に報告しなければならない。

　なお、セキュリティの脆弱性が発見された場合、委員会は緊急避難措置をとるとともに改善策を講じなければならない。

９．３　委員会は、情報セキュリティを維持するための予算措置を含め適切な措置を講じなければならない。

９．４　委員会は、情報システム委員会、執行役会にその評価・見直しの結果を報告しなければならない。

１０　監査

(情報セキュリティ対策の監査)

１０．１　CISOA は、機構ポリシー第１８条に基づく情報セキュリティ監査の他に、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、情報セキュリティ監査計画で計画された事案以外の監査の実施を依頼することができる。

１０．２　CISOA は、前項による監査を依頼する場合は、対象となる監査業務ごとの監査計画案を策定し、情報セキュリティ監査責任者に提出する。

１０．３　CISOA は、監査報告書に基づいて CIO から適切な対応の実施を指示された事案について、被監査部門の IO に対して、適切な対応の実施及び対応計画の作成し、報告を指示する。

１０．４　CISOA 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、他の部門の IO 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する。

１０．５　CISOA は、監査の結果を踏まえ、既存の実施規則及び手順並びに関係規程の妥当性を評価し、必要に応じてその見直しを行う。

１１　雑則

この規定に定めのない事項は、委員会の議を経て別途定めることができる。

附　則

このポリシーは、平成１９年３月２３日から施行する。

附　則

このポリシーは、平成２３年３月２４日から施行する。

附　則（平成２６年規則第１５号）

このポリシーは、平成２６年４月１日から施行する。

附　則（平成２７年規則第４９号）

このポリシーは、平成２７年１０月２３日から施行する。

附　則（平成２８年規則第３１号）

このポリシーは、平成２８年９月１４日から施行する。

附　則（平成３０年規則第２６号）

このポリシーは、平成３０年７月１８日から施行する。

附　則（令和４年４月１日）

このポリシーは、令和４年４月１日から施行する。