公立大学法人前橋工科大学情報セキュリティ対策基準に基づく運用方針

公立大学法人前橋工科大学情報セキュリティ対策基準に基づく運用方針（以下「本方針」という。）は、公立大学法人前橋工科大学情報セキュリティポリシーに基づき、公立大学法人前橋工科大学（以下「本学」という。）における情報資産のセキュリティ対策に関する具体的な運用方針を定めることとする。

なお、本方針において「情報セキュリティ」とは、サイバーセキュリティを含む情報資産の機密性、完全性及び可用性の確保に関する事項をいう。

1　組織・体制

(1) 情報セキュリティ最高責任者（CISO）

情報セキュリティ最高責任者は、理事（副学長）をもって充てる。情報セキュリティ最高責任者は、本学における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

(2) 情報セキュリティ管理責任者

情報セキュリティ管理責任者は、図書・情報センター長をもって充てる。情報セキュリティ管理責任者は、情報セキュリティ最高責任者を補佐するとともに、次に掲げる権限及び責任を有する。

① 本学の全てのネットワーク、情報システムにおける開発、設定の変更、運用、見直し及びこれらの調整等を行う統括的な権限及び責任

② 本学の全てのネットワーク、情報システムにおける情報セキュリティ対策に関する統括的な権限及び責任

③ 情報セキュリティ管理者 、ネットワーク管理者及び情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限

④ 本学の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、情報セキュリティ最高責任者の指示に従い、情報セキュリティ最高責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任

(3) 情報セキュリティ管理者

情報セキュリティ管理者は、事務局長をもって充てる。情報セキュリティ管理者は、情報セキュリティ管理責任者を補佐するとともに、情報セキュリティ管理責任者に事故ある時は、その職務を全て代行することができる。情報セキュリティ管理者は、次に掲げる権限及び責任を有する。

① 事務局の情報セキュリティ対策に関する権限及び責任

② 事務局のネットワーク、情報システムにおける開発、設定の変更、運用、見

直し等を行う権限及び責任

③　事務局のネットワーク、情報システムについて、緊急時等における連絡体制の整備

(4) ネットワーク管理者

ネットワーク管理者は、本学の職員の中から図書・情報センター長が指名した者をもって充てる。ネットワーク管理者は、次に掲げる事務を所掌する。

①　その所管するネットワークにおける開発、設定の変更、運用、見直し等の実務

②　情報システム管理者に対して、情報システムにおける開発、設定の変更、運用、見直し等に関する指導及び助言

③　その所管する情報セキュリティ対策の実務の統括

④　情報セキュリティ管理者に対する情報セキュリティに関する指導及び助言

(5) 情報システム管理者

情報システム管理者は、各情報システムの担当課長をもって充てる。情報システム管理者は、次に掲げる事務を所掌する。

①　その所管する情報システムにおける開発、設定の変更、運用、見直し等の実務

②　その所管する情報システムにおける情報セキュリティに関する実務

③　その所管する情報システムに関する情報セキュリティ実施手順の作成及び維持・管理

(6) 情報セキュリティ委員会

本学における情報セキュリティ対策を統一的・計画的に推進するため、情報セキュリティ委員会を設置する。

情報セキュリティ委員会は、次に掲げる事項を所掌する。

・方針及び情報セキュリティポリシーの実施状況の評価

・監査・自己点検結果の審議

・方針及び情報セキュリティポリシーの見直し案の検討

・重大インシデント発生時の助言

2　情報資産の分類と管理

本章に定める情報資産の分類及び管理は、地方自治法第 244 条の 6 第 1 項に基づく措置として実施するものとする。

(1) 情報資産の管理責任等

①　管理責任

情報セキュリティ管理者は、その所管する情報資産について管理責任を有す

る。

② 複製又は伝送された情報資産の管理

情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も管理しなければならない。

(2) 情報資産の重要性分類と管理方法

① 情報資産の重要性分類

本学における情報資産は、機密性、完全性及び可用性を踏まえ、次に掲げる情報資産の区分に応じ、それぞれに定める重要性分類に分類する。

(ｱ) 個人情報及び業務上必要とする最小限の者のみが扱う情報資産（極秘の情報を含む。） 重要性分類Ⅰ

(ｲ) 公開することを予定していない情報資産（極秘の情報を含む。） 重要性分類Ⅱ

(ｳ) 外部に公開する情報資産のうち業務上重要な情報資産 重要性分類Ⅲ

(ｴ) 上記以外の情報資産 重要性分類Ⅳ

② 情報の作成

(ｱ) 情報資産に係る業務に携わる職員（非常勤及び臨時の職員を含む。以下「職員等」という。）は、業務上必要のない情報を作成してはならない。

(ｲ) 職員等は、作成途上の情報についても、紛失や流出等の防止に努め、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③ 情報資産の利用

(ｱ) 職員等は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 職員等は、情報資産の重要性分類に応じ、適切な取扱いをしなければならない。

(ｳ) 職員等は、記録媒体に情報資産の重要性分類が異なる情報が複数記録されている場合は、最高度の重要性分類に従って、当該記録媒体を取り扱わなければならない。

④ 情報資産の保管

(ｱ) 情報セキュリティ管理者、ネットワーク管理者及び情報システム管理者は、情報資産の重要性分類に従って、情報資産を適切に保管しなければならない。

(ｲ) 情報セキュリティ管理者、ネットワーク管理者及び情報システム管理者は、情報資産を記録した外部記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

(ｳ) 情報セキュリティ管理者、ネットワーク管理者及び情報システム管理者は、重要性分類Ⅱ以上の情報（以下「重要な情報資産」という。）を記録した記録媒体を、耐火、耐熱、耐水及び耐湿策を講じた施錠可能な場所に保管しなけ

ればならない。

⑤　情報の送信

職員等は、電子メールにより重要な情報資産を外部に送信する場合は、暗号化を行わなければならない。

⑥　情報資産の持ち出し

職員等は重要な情報資産を外部に持ち出してはならない。ただし、業務上の必要性により、やむを得ず持ち出す場合は、鍵付きのケース等に格納し、又は暗号化を行う等、情報資産の不正利用を防止するための必要な措置を講じなければならない。

⑦　情報資産の提供及び公表

(ｱ) 職員等は、重要な情報資産を外部に提供する場合は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

(ｲ) 職員等は、重要な情報資産を外部に提供する場合は、情報セキュリティ管理者に許可を得なければならない。

(ｳ) 情報セキュリティ管理者､情報システム管理者及びネットワーク管理者は、外部に公開する情報資産について、完全性を確保しなければならない。

⑧　情報資産の廃棄

(ｱ) 職員等は、重要な情報資産が不要になった場合は、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

(ｲ) 職員等は、重要な情報資産の廃棄を行う場合は、廃棄を行った日時、担当者及び廃棄方法等を記録しなければならない。

(ｳ) 職員等は、重要な情報資産の廃棄を行う場合は、当該情報資産を所管する情報セキュリティ管理者、ネットワーク管理者及び情報システム管理者の許可を得なければならない。

3　物理的セキュリティ

(1) 装置の設置

①　基幹装置の取付け等

情報ネットワーク・システムを構成する重要な基幹装置は、施錠などによって物理的に隔離された区域で、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置するものとする。

②　情報システム機器の盗難対策

据付型パソコン端末機器又はサーバ及びネットワーク機器などの情報システム機器は、盗難などの対策を施さなければならない。

③　電源

情報ネットワーク・システムを構成する重要な基幹装置の電源には、十分な電力を供給する容量の予備電源を備え付けなければならない。また、落雷等による過電流から基幹装置を保護するために適切な措置を施さなければならない。

④　配線

配線は、盗聴、損傷等を受けることがないように適切な措置を施さなければならない。また、ネットワーク接続口（ハブのポート等）は、不特定の者によって接続が行われないような措置を施さなければならない。

⑤　機器の多重化

機器の障害によるネットワークの停止が重大な影響を及ぼさないようサーバ又はネットワーク機器については、多重化による信頼性の向上を実施しなければならない。

(2) 管理区域

情報ネットワーク・システムを構成する重要な基幹装置は、情報セキュリティ担当部局が管理する区域（以下「コンピュータ機器室」という。）に設置しなければならない。

室内は温度、湿度にも配慮し、機器類は耐震対策を講じた場所に設置するとともに、防火措置等を施さなければならない。

コンピュータ機器室には、許可された者のみ入室できるような入退室管理を行い、外部からの侵入を防止するための対策を施さなければならない。

保守作業及び機器等の搬入には、必ず情報セキュリティ担当部局の職員等が立ち会わなければならない。

(3) 職員等のパソコン等の管理

情報セキュリティ管理者は、執務室等のパソコン等の端末が盗難に遭わないよう必要な措置を講じなければならない。

ネットワーク管理者及び情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

ネットワーク管理者及び情報システム管理者は、パソコン等の端末のディスクデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティ機能が搭載されている場合は、その機能を有効に活用しなければならない。

4　人的セキュリティ

(1) 職員等の遵守事項

① 職員等の遵守事項

(ｱ) 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵

守しなければならない。情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に報告し、指示を仰がなければならない。

(ｲ) 業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

(ｳ) パソコン等の端末の持ち出し及び外部における情報処理作業の制限

a　情報セキュリティ最高責任者は、重要な情報資産を外部で処理する場合における安全管理措置を定めなければならない。

b　職員等は、本学のパソコン等の端末、ソフトウェア等を外部に持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

c　職員等は、外部で情報処理作業を行う際、やむを得ず私物パソコン等を用いる場合は、安全管理措置を遵守しなければならない。

(ｴ) 情報ネットワーク・システムへの接続制限

職員等は、私物のパソコン等の端末や記録媒体を本学の情報ネットワーク・システムへ接続してはならない。

(ｵ) 端末等の持ち出しの記録

情報セキュリティ管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

(ｶ) パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

(ｷ) 机上の端末等の管理

職員等は、パソコン等の端末や記録媒体等について、第三者に使用されること及び情報セキュリティ管理者の許可なく情報を閲覧されることがないよう離席時の端末のロックや記録媒体の保管等、適切な措置を講じなければならない。

(ｸ) 退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合は、利用していた情報資産を引き継がなければならない。異動、退職等の後も業務上知り得た情報を漏らしてはならない。

②　有期雇用職員への対応

(ｱ) 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、有期雇用職員に対し、採用時に情報セキュリ

ティポリシー等のうち、有期雇用職員が守るべき内容を理解させ、実施及び遵守させなければならない。

(ｲ) 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、有期雇用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー等を閲覧できるようにしなければならない。

④　外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発、保守等を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(2) 教育・研修

①　教育の実施

情報セキュリティ委員会は、職員等向けのポリシーに関する研修の支援をしなければならない。また、職員等が行う学生向けのポリシーに関するオリエンテーション又は講義に協力しなければならない。

②　教育の受講

全ての職員等及び学生は、研修会若しくは説明会又は講義等に参加し、ポリシーを理解し、情報セキュリティ上の問題が生じないように努めなければならない。

(3) 事故・障害の発生時の対処

職員等は、情報セキュリティに関する事故、システム上の障害を発見した場合には、情報セキュリティ最高責任者に直ちに報告しなければならない。

情報セキュリティ管理責任者及び情報セキュリティ管理者は、報告のあった事故等について被害の状況を調査し、被害の規模を把握し、必要な措置を直ちに講じなければならない。

情報セキュリティ管理責任者は、発生した事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告するとともに、重大な事故に関しては、迅速な再発防止のための対策を講じなければならない。

(4) ＩＤ及びパスワード等の管理

①　ＩＤの取扱い

職員等は､自己の管理するＩＤに関し､次の事項を遵守しなければならない。

(ｱ) 自己が利用しているＩＤは、他人に利用させてはならない。

(ｲ) 共用ＩＤを利用する場合は、共用ＩＤの利用者以外の者に利用させてはならない。

② パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(ｱ) パスワードは、他者に知られないように管理しなければならない。

(ｲ) パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

(ｳ) パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

(ｴ) パスワードが流出したおそれがある場合は、情報セキュリティ管理者に速やかに報告し、当該パスワードを速やかに変更しなければならない。

(ｵ) パスワードは定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

(ｶ) 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

(ｷ) 仮のパスワードは、最初のログイン時点で変更しなければならない。

(ｸ) パソコン等の端末にパスワードを記憶させてはならない。

(ｹ) 共用パスワードを利用する場合は、共用パスワードの利用者以外の者に利用させてはならない。

5　技術的セキュリティ

本章に定める技術的対策は、サイバーセキュリティを確保するために必要な措置として講じるものとする。情報ネットワーク･システムを様々な脅威から保護するため、情報セキュリティ管理責任者は、技術的対策及び運用管理についての対策を講じなければならない。

(1) コンピュータ及びネットワークの技術的対策

① メール対策

メールサーバには、不正中継処理対策、スパムメール対策及びウィルス対策を講じなければならない。

② 暗号化

有線及び無線どちらにおいても、パスワード又は機密情報がネットワーク上に流れる際には必要に応じて暗号化されるような設定を施さなければならない。

③ アクセス制御

本学情報資源、ネットワークサービス等については、資源及びサービスごと

にアクセスできる者を定め、権限のないものがアクセスできないように制限しなければならない。

また、外部ネットワークとの接続は、業務上必要な場合は、情報セキュリティ管理者の許可を得て、接続することができる。なお、外部ネットワークとの接続においては、ファイアウォール装置などを用いたネットワークアクセス制御を行わなければならない。

④　コンピュータウィルス対策

サーバレベルでウィルスチェックを行い、学外からのウィルスチェックが行われるような対策を講じなければならない。

また、パソコン端末機器においてはリアルタイムでウィルスチェックが行われるような対策を講じなければならない。

⑤　不正アクセス対策

公開を目的としたサーバは、内部ネットワークとは別に配置するものとする。サーバは必要最小限のポートを開けるものとし、使用していないサービスは停止しなければならない。

また、不正侵入を検出可能な侵入検知システムを導入しなければならない。

(2) ネットワーク運用管理

①　セキュリティ情報の収集

セキュリティに関する情報を収集し、セキュリティ対策上必要な措置を講じるとともに、これらの情報を定期に取りまとめ、ポリシーの改定につながる情報については、情報セキュリティ委員会に報告しなければならない。

②　情報システムの監視

セキュリティに関する事案を検知するため、常に情報システムの監視を行わなければならない。

③　記録の管理

学内情報ネットワーク・システムにおけるシステム変更等の記録、情報システムの障害に対処した際の障害記録、サーバアクセス等の各種システムに関する記録を維持管理しなければならない。

④　媒体の管理

機密情報が記録された記録媒体（電子媒体及び紙媒体）を、第三者に使用されること、又は許可なく情報を閲覧されることがないように配慮しなければならない。

⑤　バックアップ管理

機密情報等を保持しているサーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にバックアップ用の複製をとらなければならな

い。

⑥　情報システムの開発、導入及び変更

ソフトウェアの開発及び変更並びに運用機器及び基本ソフトウェアの導入、保守及び撤去については、手順及び基準を明らかにしなければならない。また、それらの事項について情報セキュリティ上問題がないように対処しなければならない。

⑦　システムの受託業者への規定

新たなシステムの開発を外部の事業者に委託する場合は、委託先において必要なセキュリティ対策が確保されていることを確認するとともに、守秘義務及び必要なセキュリティ要件等を踏まえた契約を締結しなければならない。

⑧　機器の修理及び廃棄

機密情報等が含まれる機器について、外部業者に修理させ、又は廃棄する場合は、その内容が消去された状態で行わせなければならない。

⑨　情報システム仕様書等の管理

情報システム仕様書について、記録媒体にかかわらず業務上必要とする者のみが閲覧できる場所に保管しなければならない。

⑩　機器情報の把握

ネットワーク管理者及び情報システム管理者は、情報ネットワーク・システムの安全な環境を維持するため、情報ネットワーク・システムを構成する全ての機器について情報を把握しなければならない。

また、システムの安全な運用上、問題があると認められた場合は、その可否について情報セキュリティ最高責任者と協議及び検討を行うものとする。

6　運用

(1) 情報セキュリティポリシーの遵守状況の確認

①　遵守状況の確認及び対処

(ｱ) 情報セキュリティ管理責任者及び情報セキュリティ管理者は、本方針及び情報セキュリティポリシーの遵守状況について定期的に確認を行い、問題を認めた場合は、速やかに情報セキュリティ最高責任者に報告しなければならない。

(ｲ) 情報セキュリティ最高責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

(ｳ) ネットワーク管理者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合は、適切かつ速やかに対処し

なければならない。

② 端末及び記録媒体等の利用状況調査

情報セキュリティ管理者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

③ 職員等の報告義務

(ｱ) 職員等は、情報セキュリティポリシーに対する違反行為を発見した場合は、直ちに情報セキュリティ管理者に報告を行わなければならない。

(ｲ) 報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ最高責任者及び情報セキュリティ管理責任者に報告しなければならない。

(ｳ) 違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ最高責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(2) 侵害時の対応

緊急時対応計画は、地方自治法第 244 条の 6 第 1 項に基づく措置として策定・維持されるものとする。

① 緊急時対応計画の策定

情報セキュリティ最高責任者は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切に対処しなければならない。

② 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めなければならない。

(ｱ) 関係者の連絡先

(ｲ) 発生した事案に係る報告すべき事項

(ｳ) 発生した事案への対応措置

(ｴ) 再発防止措置の策定

③ 緊急時対応計画の見直し

情報セキュリティ最高責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

(3) 外部委託

① 外部委託先の選定基準

(ｱ) 情報セキュリティ管理責任者及び情報セキュリティ管理者は、外部委託先

の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

(ｲ)情報セキュリティ管理者及び情報システム管理者は､情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

② 契約項目

ネットワーク又は情報システムの保守、運用等を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

(ｱ) 情報セキュリティポリシーのうち、受託者に遵守させる事項
(ｲ) 委託先の責任者、委託内容、作業者及び作業場所の特定
(ｳ) 提供されるサービスレベルの保証
(ｴ) 従業員に対する教育の実施
(ｵ) 提供された情報資産の目的外利用及び受託者以外の者への提供の禁止
(ｶ) 業務上知り得た情報の守秘義務
(ｷ) 再委託に関する制限事項の遵守
(ｸ) 情報資産の複写及び複製の禁止
(ｹ) 委託業務の終了時の情報資産の返還、廃棄等
(ｺ) 委託業務の定期報告及び緊急時報告の義務
(ｻ) 本学による監査及び検査
(ｼ) 本学による事故時等の公表
(ｽ) 契約が遵守されなかった場合の規定(損害賠償等)

③ 確認・措置等

委託に関する責任を有する部署は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、前記②の契約に基づき措置し、その内容を情報セキュリティ管理者に報告するとともに、その重要度に応じて情報セキュリティ最高責任者及び情報セキュリティ管理責任者に報告しなければならない。

(4) 例外措置

① 例外措置の許可

職員等は、情報セキュリティ関係規定を遵守することが困難な状況で、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合は、情報セキュリティ最高責任者の許可を得て、例外措置を取ることができる。

② 緊急時の例外措置

情報セキュリティ管理責任者及び情報セキュリティ管理者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに情報セキュリティ最高責任者に報告しなければならない。

③　例外措置の申請書の管理

情報セキュリティ最高責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

(5) 法令等遵守

職員等は、職務の遂行において使用する情報資産を保護するため、次の法令等を遵守し、これに従わなければならない。

①　地方独立行政法人法（平成１５年法律第１１８号）
②　著作権法（昭和４５年法律第４８号）
③　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
④　個人情報の保護に関する法律（平成１５年法律第５７号）
⑤　前橋市個人情報保護条例（平成９年前橋市条例第４６号）
⑥　公立大学法人前橋工科大学法人情報等取扱規程（平成２５年規程第４４号）
⑦　その他情報システム及び情報資産に関する法令

7　評価及び更新

(1) 監査

情報セキュリティ監査は､方針の実施状況を評価するための手段として実施する。

①　実施方法

情報セキュリティ最高責任者は、情報セキュリティ監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

②　監査を行う者の要件

情報セキュリティ監査責任者は、監査を実施する場合には、監査及び情報セキュリティに関する専門知識を有する者に行わせなければならない。

③　監査実施への協力

(ｱ) 情報セキュリティ監査責任者は、監査を行うに当たって、監査実施計画を作成しなければならない。

(ｲ) 被監査部門は、監査の実施に協力しなければならない。

④　外部委託事業者に対する監査

外部委託事業者に委託している場合は、情報セキュリティ監査責任者は、外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティ対策について監査を必要に応じて行わなければならない

⑤　報告

情報セキュリティ監査責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

⑥　保管

情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

⑦　監査結果への対応

情報セキュリティ最高責任者は、監査結果を踏まえ、指摘事項を所管する情報システム管理者に対し、当該事項への対処を指示しなければならない。この場合において、指摘事項を所管していない情報システム管理者に対しても、同種の課題及び問題点がある可能性が高い場合は、当該課題及び問題点の有無を確認させなければならない。

⑧　情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーその他情報セキュリティ対策の見直し時に活用しなければならない。

(2) 自己点検

①　実施方法

(ｱ) 情報セキュリティ管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

(ｲ) 情報セキュリティ管理責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について､毎年度及び必要に応じて自己点検を行わなければならない。

②　報告

情報セキュリティ管理責任者及び情報セキュリティ管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、必要に応じ情報セキュリティ委員会に報告しなければならない。

③　自己点検結果の活用

(ｱ) 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

(ｲ) 情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーその他情報セキュリティ対策の見直し時に活用しなければならない。

(3) 情報セキュリティポリシーの見直し

情報セキュリティ委員会は、監査結果、自己点検結果及び法令・社会情勢・脅威動向の変化を踏まえ、情報セキュリティ確保のための方針及び情報セキュリティポ

リシーの見直し案を作成し、最高責任者に報告するものとする。

附　則

この運用方針は、平成２５年４月１日から施行する。

附　則

この運用方針は、平成２７年１月９日から施行する。

附　則

この運用方針は、平成２８年８月２４日から施行する。

附　則

この運用方針は、令和８年４月１日から施行する。