地方独立行政法人神奈川県立福祉機構

情報セキュリティポリシー

（令和８年４月１日制定）

神奈川県立福祉機構情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、地方独立行政法人神奈川県立福祉機構（以下「法人」という。）が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものをいう。情報セキュリティポリシーは、法人が所管する情報資産に関する業務に携わる全ての職員等に情報セキュリティへの取組みを浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分である情報セキュリティ基本方針と情報セキュリティを取り巻く状況の変化に依存する部分である情報セキュリティ対策基準とにより構成することとした。また、情報セキュリティポリシーに基づき、コンピュータ、ネットワーク及び情報システム（以下「情報システム等」という。）、又は情報セキュリティに係る具体的な実施手順を情報セキュリティ実施手順として策定することとする。

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の構成

分類	文 書 名	内 容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針に基づき定める情報システム等に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順	情報セキュリティ点検に関する基準 等	情報セキュリティポリシーに基づいて、情報システム等ごとに定める具体的な実施手順

第１章　情報セキュリティ基本方針

1　目的

法人の情報システム等が取り扱う情報には、施設利用者等の個人情報のみならず業務運営上重要な情報など、外部に漏えい等した場合に重大な結果を招く情報も含まれている。

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御することは、施設利用者等の財産、プライバシー等を守るためにも、また、業務の安定的な運営のためにも必要不可欠であり、さらに法人に対する利害関係者等からの信頼の維持向上に寄与するものである。

本基本方針は、法人が所管する情報資産の機密性、完全性及び可用性を維持するため、法人が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

情報セキュリティポリシーにおいて、次に掲げる用語の意義は、以下の各号に定めるところによる。

⑴　コンピュータ	サーバ、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。
⑵　ネットワーク	コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。
⑶　情報システム	コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。
⑷　データ	コンピュータ又は記録媒体に記録されている電磁的記録をいう。
⑸　情報資産	コンピュータ、ネットワーク、情報システム及びこれらが取り扱う情報（当該情報を印刷した文書を含む。）をいう。
⑹　記録媒体	データを記録するための媒体をいう。例えば、磁気テープ、ハードディスク、USB メモリ、CD-R、DVD-R、ボイスレコーダ、デジタルカメラ、SD メモリーカード、スマートフォンなど。
⑺　モバイル端末	コンピュータのうち、自席にとどまらず、施設内

		外に携帯し、利用できる端末をいう。
⑻	IoT 機器を含む特定用途機器	テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、ネットワークに接続されている又は電磁的記録媒体を内蔵しているものをいう。
⑼	外部サービス	事業者等の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において法人が所管する情報資産が取り扱われる場合に限る。
⑽	クラウドサービス	ネットワークに接続されたコンピュータを運営する事業者等が提供する様々なサービス・機能を利用する形態をいう。
⑾	ソーシャルメディア	インターネット上において不特定多数の者が情報を交換・共有する仕組みをいう。例えば、ブログ、ソーシャルネットワーキングサービス、動画共有サイトなど。
⑿	ソーシャルメディアサービス	インターネット上において不特定多数の者が情報を交換・共有する仕組みを提供するサービスをいう。
⒀	機密性	情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。
⒁	完全性	情報が破壊、改ざん又は消去されていない状態を確保することをいう。
⒂	可用性	情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。
⒃	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。
⒄	情報セキュリティ対策	情報セキュリティを確保するための対策をいう。
⒅	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、業務の遂行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。
⒆	職員等	法人が雇用する職員及び労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に

関する法律（昭和 60 年 7 月 5 日法律第 88 号）第２条第２項に規定する派遣労働者をいう。

⑳　施設　　法人がその事務を処理する目的で所有する建物及び敷地並びに賃借する建物内の区画（フロア内すべてを法人の機関のみで借用している場合はそのフロア全体）をいう。

3　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、法人が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の指針となるものである。

したがって、法人が所管する情報資産に関する業務に携わる全ての職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって情報セキュリティポリシーを遵守するものとする。

4　情報セキュリティ管理体制

法人は、法人が所管する情報資産について、情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

5　情報の分類

法人は、情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6　情報資産への脅威

情報セキュリティ対策基準を策定する上で、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると、特に情報セキュリティ対策を講ずべき脅威は次のとおりである。

⑴　部外者による故意の不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難等

⑵　職員等及び委託事業者の従業員による誤操作、故意の不正アクセス又は不正操作による情報若しくはプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難、正規の手続きによらない端末及び媒体の接続による情報漏えい等

⑶　地震、落雷、火災等の災害及び事故、故障等による業務の停止

⑷　大規模・広範囲にわたる疾病による職員等の要員不足に伴う情報システム運用の機能不全

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

7　情報セキュリティ対策

法人は、前項で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講じるものとする。

⑴　物理的対策

情報システム等を設置する執務室等への不正な立入り及び情報資産への損傷、妨害等から保護するための物理的な対策

⑵　人的対策

情報セキュリティに関する役割等を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を講じるための対策

⑶　技術的対策

情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策

⑷　運用における対策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、委託を行う際の情報セキュリティ確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

⑸　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

サービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

8　情報セキュリティ対策基準の策定

法人が所管する情報資産について、前項の情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を別に定めるものとする。

9　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、

個々の情報資産の情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、所管する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより情報セキュリティの確保に重大な支障を及ぼす恐れがあるため取扱いに注意するものとする。

10　情報セキュリティ監査の実施

法人は、情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施するものとする。

11　評価及び見直しの実施

法人は、情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施するものとする。

12　その他

この基本方針の実施に関して必要な事項は、別に定める。

第２章　情報セキュリティ対策基準

１　目的

この基準は、地方独立行政法人神奈川県立福祉機構情報セキュリティ基本方針（以下「基本方針」という。）に基づき、地方独立行政法人神奈川県立福祉機構（以下「法人」という。）が所管する情報資産に関する情報セキュリティ対策に関し、必要な事項を定める。

２　対象範囲

この基準が対象とする情報資産は、法人が業務遂行のために所有する情報資産とする。ただし、個人番号及び特定個人情報等他の規程により取り扱いが定められている場合は、当該規程によるものとする。

３　情報セキュリティ管理体制

基本方針第４項の法人における情報セキュリティ管理体制は、以下のとおりとする。

⑴　情報セキュリティ責任者

理事長を情報セキュリティ責任者とする。

情報セキュリティ責任者は、法人が所管する情報システム等の運営及び情報資産の情報セキュリティを統括する。

⑵　統括情報セキュリティ管理者

法人業務全般の総括を担任する副理事長を統括情報セキュリティ管理者とする。

ア　統括情報セキュリティ管理者は、情報セキュリティ管理者、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。

イ　統括情報セキュリティ管理者は、法人が所管する情報資産に対する侵害、又は侵害の恐れのある場合には、情報セキュリティ責任者の指示に従い、必要かつ十分な全ての措置を行う。ただし、特に緊急を要する場合及び情報セキュリティ責任者が不在の場合には、自らの判断に基づき、必要かつ十分な全ての措置を行う。

ウ　統括情報セキュリティ管理者は、情報セキュリティ実施手順の策定、維持及び管理を行う。

⑶　情報セキュリティ管理者

経営企画室長、研究センター長、人材育成センター長、統括園長、内部統制・コンプライアンスオフィスマネージャーを情報セキュリティ管理者とする。

ア　情報セキュリティ管理者は、統括情報セキュリティ管理者の下、所掌する所属における情報セキュリティを統括する。

イ　情報セキュリティ管理者は、所掌する所属において所管している情報資産に対

する侵害又は侵害の恐れのある場合の連絡体制の構築、並びに当該所属における情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

ウ　情報セキュリティ管理者は、所掌する所属における情報資産に対する侵害又は侵害の恐れのある場合には、情報システム管理者等へ速やかに報告を行い、指示を仰ぐとともに、統括情報セキュリティ管理者に対しても速やかに報告するものとする。

エ　情報セキュリティ管理者は、所掌する所属に係る情報セキュリティ実施手順の策定、維持及び管理を行う。

オ　情報セキュリティ管理者は、職員等に端末による作業を行わせる場合には、情報セキュリティポリシーについて、特に注意を喚起し、守るべき実施手順を理解させ、かつ実施及び遵守させるものとする。

⑷　情報システム管理者

経営企画室長を情報システム管理者とする。

ア　情報システム管理者は、法人が所管する情報システムの開発、ネットワークの構築、コンピュータの設定、設定の変更、運用、更新等を行う。

イ　情報システム管理者は、法人が所管する情報システム等の情報セキュリティを統括する。

ウ　情報システム管理者は、所管する情報システム等における情報資産に対する侵害、又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

エ　情報システム管理者は、法人が所管する情報システム等に係る情報セキュリティ実施手順の策定、維持及び管理を行う。

⑸　情報セキュリティ委員会

法人の情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティ委員会において情報セキュリティポリシーの策定等の情報セキュリティに関する重要な事項を審議する。

情報セキュリティ委員会の設置及び運営については、別途定める。

⑹　職員等

ア　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のうち職員等向けに定められている事項を遵守するものとする。

イ　職員等は、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については、速やかに情報セキュリティ管理者に相談し、指示等を仰ぐものとする。

4　情報の分類と管理

⑴　情報の分類

ア　情報セキュリティ管理者は、情報セキュリティ対策の対象となる情報システム等が取り扱う情報について、次のとおり、対策重要度の分類を行うものとする。

対策重要度

分類	基準
Ⅰ	個人情報
Ⅱ	個人情報以外の情報で、特に機密性が求められる情報
Ⅲ	対策重要度Ⅰ、Ⅱ及びⅣ以外の情報
Ⅳ	公開されている情報

⑵　情報の管理

ア　情報は、当該情報を所管する情報セキュリティ管理者が管理するものとする。

イ　情報は、原則として、ファイルサーバに保存するものとする。

ただし、各所属の業務の実態に合わせて、情報セキュリティ管理者が管理する外部記録媒体に情報を保存することができるものとする。

ウ　情報セキュリティ管理者は、外部記録媒体を適切に管理するものとする。

エ　情報セキュリティ管理者は、重要度に応じて、各々の情報にアクセスできる職員等及びアクセス権限を定めるものとする。

オ　情報システム管理者は、情報を取り扱うコンピュータについて、原則として暗号化機能を備えた記録装置を使用するものとする。

カ　情報セキュリティ管理者は、対策重要度Ⅰ又は対策重要度Ⅱに該当する情報（以下「重要情報」という。）について、パスワード等による暗号化を行った上で管理するものとする。

キ　情報セキュリティ管理者は、情報システム等が取り扱う情報について、ファイル名、記録媒体の表示等から第三者が重要性の識別を容易に認識できないように、適切な管理を行うものとする。

⑶　情報の取扱い

ア　情報の作成

(ｱ) 職員等は、業務上必要のない情報を作成してはならない。

(ｲ) 情報を作成する職員等は、情報の作成時に(1)の分類に基づき情報を分類し取り扱うものとする。

(ｳ) 情報を作成する職員等は、作成途中の情報についても、紛失、流出等を防止するために必要な措置を講じるものとする。また、情報の作成途中で不要になった場合は、当該情報を消去するものとする。

イ　情報の入手

(ｱ) 他所属の職員等が作成した情報を入手した職員等は、入手元の情報の分類に基づいた取扱いをするものとする。

(ｲ) 外部の者が作成した情報を入手した職員等は、(1)の分類に基づき情報を分類

し取り扱うものとする。

(ｳ) 情報を入手した職員等は、入手した情報の分類が不明な場合、情報セキュリティ管理者に判断を仰ぐものとする。

ウ　情報の利用

(ｱ) 情報を利用する職員等は、業務以外の目的に情報を利用してはならない。

(ｲ) 情報を利用する職員等は、情報の分類に従って、適切な取扱いをするものとする。

(ｳ) 情報を利用する職員等は、記録媒体に情報の分類が異なる情報が複数記録されている場合には、最高度の分類に従って、当該記録媒体を取り扱うものとする。

エ　情報の保管

情報セキュリティ管理者は、防災対策を必要とするファイル等について、全て別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管するものとする。

オ　情報の運搬

(ｱ) 職員等は、情報を、情報システム等の設置場所と外部の保管場所等との間で運搬する場合には、情報セキュリティ管理者に許可を得るものとする。

(ｲ) 情報セキュリティ管理者は、車両等により情報を運搬する場合には、パスワード等による暗号化を行い、鍵付きのケースに格納する等、必要に応じて、情報の不正利用を防止するための措置を講じるものとする。

カ　情報の提供

(ｱ) 職員等は、重要情報を外部に提供する場合には、パスワード等による暗号化を行うものとする。

(ｲ) 職員等は、重要情報を外部に提供する場合には、情報セキュリティ管理者に許可を得るものとする。

(ｳ) 情報セキュリティ管理者は、施設利用者等に提供する情報について、完全性を確保するために必要な措置を講じるものとする。

キ　情報の廃棄

職員等は、記録媒体を廃棄する場合には、次のとおり、記録されている情報の分類に応じ、当該記録媒体の情報を復元できないように破砕等の復元防止措置を講じた上で廃棄するものとする。廃棄に当たっては、情報セキュリティ管理者の許可を得ることとし、処理の日時、担当者及び復元防止措置の内容を記録するものとする。また、復元防止措置の作業完了までを職員が立ち合い確認するものとする。

(ｱ) 重要情報を含む場合

重要情報が保存された機器内部の記録装置については、物理的破壊または磁気的破壊により復元防止措置を行う。

(ｲ) 重要情報を含まない場合

重要情報を含まない機器内部の記録装置については、物理的破壊または磁気的破壊もしくはデータ消去専用ソフトウェアによる復元防止措置を行う。

ク　施設外で利用することが適当でない情報の取扱い

(ｱ) 情報セキュリティ管理者は、所管する情報のうち施設外へ持ち出したモバイル端末等からの利用を認めない情報を指定するものとする。

(ｲ) 職員等は、当該情報について、施設外へ持ち出したモバイル端末等から利用してはならない。

5　物理的対策

(1)　管理区域

ア　管理区域の構造等

(ｱ) 管理区域とは、ネットワークの基幹機器及び重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱う情報システムが設置され、当該機器及び情報システムの管理及び運用を行うための情報システム室並びに記録媒体の保管庫をいう。

(ｲ) 管理区域から外部に通ずるドアは必要最小限の箇所に設けるものとし、全てのドアは、制御機能、鍵、警報装置等によって、許可されていない者の立入りを防止できるようにするものとする。

(ｳ) 情報システム室には、ビデオカメラ等の監視機能を設置するものとする。

(ｴ) 情報システム室内の機器等は、耐震対策を講じた場所に設置するとともに、防火措置等を講じるものとする。なお、情報システム室内の機器等の配置は、緊急時に職員等及び委託事業者の従業員が円滑に避難できるように配慮するものとする。

(ｵ) 管理区域に配置する消火剤は機器及び記録媒体等に影響を与えないものを使用するものとする。

イ　管理区域の入退室管理

(ｱ) 情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行うものとする。

(ｲ) 職員等及び委託事業者の従業員は、管理区域に入室する場合には、身分証明書等を携帯し、求めにより提示するものとする。

(ｳ) 情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて管理区域内の立入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じるものとする。

(ｴ) 情報システム管理者は、管理区域に設置する情報システム等に関連しないコン

ピュータ、モバイル端末、通信回線装置、記録媒体等を持ち込ませないようにするものとする。

ウ　機器等の搬入

(ｱ) 情報システム管理者は、搬入する機器が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせるものとする。

(ｲ) 機器等及びそれらに用いる物品の搬入出には情報システム管理者が指定した職員等が同行する等の必要な措置を講じるものとする。

⑵　機器の設置

ア　機器の設置等

(ｱ) サーバ等の機器は、火災、水害、埃、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し、容易に取り外せないよう適切な固定等の必要な措置を講じるものとする。

(ｲ) 情報システム管理者は、サーバ等の機器について、情報システム管理者及び契約により操作を認められた委託事業者の従業員以外の者が容易に操作できないような措置を講じるものとする。

(ｳ) 重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱うサーバについては、原則として、二重化することにより常に同一データを保持し、現用機に障害が発生した場合は速やかに予備機に移行させ、情報システム等の運用が停止しないようにするものとする。なお、運用上支障がないと判断される場合には、RAID によるディスクの冗長化構成及び定期的なバックアップデータの取得などにより、機器障害によるシステム等の停止を最小限に抑える対策を講じるものとする。

(ｴ) 情報システム管理者は、サーバ等の機器について、定期保守を実施するものとする。

イ　電源

(ｱ) 情報システム管理者は、重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱うサーバ等の機器の電源について、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けるものとする。

(ｲ) 情報システム管理者は、落雷等による過電流に対してサーバ等の機器を保護するための措置を講じるものとする。

ウ　配線

(ｱ) 情報システム管理者は、配線について、傍受、損傷等を受けることがないように可能な限り必要な措置を講じるものとする。

(ｲ) 情報システム管理者は、ネットワーク幹線の配線を定期的に点検するものとする。

(ｳ) 情報システム管理者は、ネットワーク接続口（ハブのポート等）を、情報セキュリティ管理者が常時目視管理できる場所又はネットワーク管理者及び契約により操作を認められた委託事業者の従業員以外の者が容易に操作できない場所に設置するものとする。

(ｴ) 情報システム管理者は、情報システム管理者及び契約により操作を認められた委託事業者の従業員以外の者が、ネットワーク幹線の配線を変更又は追加できないように必要な措置を講じるものとする。

エ　外部に設置する機器

情報システム管理者は、執務室等以外に設置する機器の情報セキュリティ水準を定期的に確認するものとする。

⑶　端末の管理

ア　執務室等に職員等及び委託事業者の従業員がいない場合は、執務室等の施錠等による盗難防止措置を講じるものとする。

イ　執務室等で利用する端末のワイヤーによる固定、モバイル端末使用時以外の施錠保管等、盗難防止のための物理的措置を講じるものとする。

ウ　情報システム管理者は、情報システムにログインパスワードの入力が必要となるよう設定するものとする。

エ　情報システム管理者は、施設外に持ち出される端末について、施設外での使用方法を定め、管理簿を設ける等、適切に管理するものとする。

オ　情報システム管理者は、モバイル端末について、上記対策に加え、遠隔消去機能を利用する等の措置を講じるものとする。

⑷　外部記録媒体の管理

ア　情報セキュリティ管理者は、使用時以外の施錠保管等、盗難防止のための物理的措置を講じるものとする。また、情報が保存される必要がなくなった時点で速やかに記録した情報を消去するものとする。

イ　情報セキュリティ管理者は、施設外に持ち出される外部記録媒体について、施設外での使用方法を定め、管理簿を設け、持ち出しや使用の履歴を記録する等、適切に管理するものとする。

ウ　情報セキュリティ管理者は、外部記録媒体の利用を許可する場合、利用する外部記録媒体に対して利用の都度（必要最小限の期間）、許可を与えるものとする。

⑸　通信回線及び通信回線装置の管理

ア　情報システム管理者は、施設内の通信回線及び通信回線装置を適切に管理するものとする。

イ　情報システム管理者は、情報セキュリティ対策基準の適用範囲外のネットワーク（以下「外部ネットワーク」という。）との接続は必要最小限のものに限定し、可能な限り接続ポイントを減らすものとする。

ウ　情報システム管理者は、ネットワークに使用する回線について、伝送途上において情報の破壊、盗聴、改ざん、消去等が生じないように不正な通信の有無を監視する等の十分な情報セキュリティ対策を実施するものとする。

エ　情報システム管理者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施するものとする。重要情報を取り扱う情報システムに通信回線を接続する場合には、必要な情報セキュリティ水準を検討の上、適切な回線を選択するものとする。また、必要に応じ、情報システム管理者等は送受信される情報の暗号化を行うものとする。

オ　情報システム管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順（機能や動作の明確化、バージョンの把握、ソフトウェアの更新手順等）を定めるものとする。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じるものとする。

⑹　機器の廃棄・修理等

情報システム管理者は、機器の廃棄、修理、リース返却等を行う場合には、機器内部の記憶装置から全ての情報を消去の上、復元不可能な状態にするものとする。また、情報システム管理者は、委託事業者に機器を修理させる場合において、情報を消去することが難しいときは、秘密を守ることを契約に定めるものとする。

⑺　クラウドサービスを提供する情報システムの物理的セキュリティ対策

ア　クラウド利用者は、クラウド事業者側の管理区域及び保守運用拠点の管理において、「５　物理的対策　⑴　管理区域」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、当該クラウドサービスのサーバ等の管理条件を「５　物理的対策　⑵　機器の設置」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

６　人的対策

⑴　職員等の遵守事項

ア　業務目的以外の使用の禁止

(ｱ) 職員等は、業務目的以外での情報システムへのアクセス、電子メールの使用及びホームページの閲覧を行ってはならない。

(ｲ) 情報システム管理者は、職員等が業務目的以外でホームページを閲覧した場合には、当該職員等が所属する所属の情報セキュリティ管理者に通知し、適切な措置を求めるものとする。

(ｳ) (ｲ)の要請にもかかわらず、職員等の業務目的以外でのホームページ閲覧が改善されない場合には、情報システム管理者は、当該職員等のホームページ閲覧を

停止することができる。

(ｴ) 情報システム管理者は、職員等のホームページ閲覧を停止した場合には、統括情報セキュリティ管理者及び当該職員等が所属する所属の情報セキュリティ管理者にその旨を通知するものとする。

イ　端末等の持ち出し及び施設外における情報の取扱いの制限

(ｱ) 職員等は、端末や外部記録媒体を持ち出す場合には情報セキュリティ管理者の許可を得るものとする。

(ｲ) 職員等は、施設外でコンピュータ等を用いて情報を取り扱う場合には、情報セキュリティ管理者の許可を得るものとする。

なお、その際、次のことを遵守すること。

a　不特定多数の者が存在する空間（公共交通機関の船車内や待合室、飲食店等）では、原則、端末を利用しないこと。

緊急時等やむを得ない事情により利用する場合は、周囲から画面を覗き見ることができない対策を実施するなど、情報が漏えいすることのないよう十分に配慮すること。

b　訪問先等で端末を取り扱う場合は、その訪問先において必要なもの以外の情報を取り扱わないこと。また、端末は常に携行すること。

c　自宅で端末を取り扱う場合においては、家族に画面を覗き見されないよう配慮すること。また、端末から離れる際はロックをかけること。

d　万一の紛失や盗難の際に、他者による不正使用を防止するため、移動時、端末にはロックをかけること。

(ｳ) 情報セキュリティ管理者は、端末や外部記録媒体等の持ち出しについて、記録を作成し、保管するものとする。

ウ　支給以外の端末及び外部記録媒体等の業務利用

職員等は、原則として、支給以外の端末及び記録媒体を業務に利用してはならない。

エ　端末におけるセキュリティ設定変更の禁止

職員等は、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。

オ　机上の端末等の管理

職員等は、端末及び記録媒体が、他者に使用され、又は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に、離席時の端末のロック、記録媒体の保管等の適切な措置を講じるものとする。

カ　関係法令の遵守

職員等は、個人情報の保護に関する法律等の業務に係る関係法令を遵守し、これに従わなければならない。

キ　法人の機関以外の者が管理する情報資産の利用における遵守事項

職員等は、業務上の必要により法人の機関以外の者が管理する情報資産を利用する場合、その管理者が定める情報セキュリティポリシーその他の規定を遵守しなければならない。

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、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

⑵　非常勤職員、臨時職員等への対応

ア　インターネット接続、電子メール使用等の制限

常勤職員以外の有期雇用職員及び派遣労働者に端末による作業を行わせる場合において、インターネットへの接続、電子メールの使用等が必要でないときは、コンピュータ管理者又はネットワーク管理者に依頼してこれらを利用できないようにするものとする。

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、県の業務の一部を委嘱する場合において、端末等による作業を伴う等、必要な場合には、委嘱の際、情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

⑶　研修及び訓練

ア　統括情報セキュリティ管理者は、定期的に職員等に対する情報セキュリティに関する研修計画を定め、職員等が情報セキュリティに関する研修を受講できるようにするものとする。

イ　統括情報セキュリティ管理者は、新規採用の職員を対象とする情報セキュリティに関する研修を実施するものとする。

ウ　研修は、情報セキュリティ管理者、情報システム管理者等及びその他の職員等に対し、それぞれの役割に応じた内容とする。

エ　情報システム管理者等は緊急時対応を想定した訓練を職員等及び委託事業者の従業員に計画的に行わせるものとする。訓練の計画に当たっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定めるとともに、より効果的に実施できるよう計画を立てるものとする。

⑷　IC カード等の管理

ア　職員等は、自己の保有する IC カード等に関し、次の事項を遵守するものとする。

(ｱ) 職員等の個人認証に用いる IC カード等は、職員等の間で共有しないこと。

(ｲ) 業務上必要のない場合には、IC カード等をカードリーダ又は端末等のスロット等から抜いておくこと。

(ｳ) IC カード等を紛失した場合には、速やかに当該 IC カード等を発行した情報システム管理者に報告し、指示を仰ぐこと。

イ　情報システム管理者は、IC カード等の紛失の報告があった場合には、速やかに当該 IC カード等の効力を停止するものとする。

ウ　情報システム管理者は、IC カード等を切り替える場合には、切替え前の IC カード等を回収し、破砕する等復元不可能な処理を行った上で廃棄するものとする。

⑸　ID 及びパスワードの管理

職員等は、自己の保有する ID 及びパスワードに関し、次の事項を遵守するものとする。

ア　自己が利用している ID を他人に利用させないこと。

イ　共用 ID を利用する場合、共用 ID の利用者以外に利用させないこと。

ウ　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ないこと。

エ　パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。

オ　情報システムへの侵入の危険又はパスワード漏えいの恐れがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更すること。

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ないこと。

キ　仮のパスワードは、最初のログイン時点で変更すること。

ク　端末にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。

ケ　共用 ID 利用時を除き、職員等の間でパスワードを共有しないこと。

⑹　情報セキュリティインシデントの報告

ア　職員等は、情報セキュリティインシデント又は、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、速やかに情報セキュリティ管理者に報告しなければならない。

イ　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ管理者に報告しなければならない。

ウ　統括情報セキュリティ管理者は、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わなければならない。

エ　情報セキュリティインシデントであると評価した場合、報告を受けた統括情報セキュリティ管理者は、情報セキュリティ責任者に報告しなければならない。

オ　統括情報セキュリティ管理者は、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管理者に対し、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を行わなければならない。また、統括情報セキュリティ管理者は、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、必要に応じて情報システム管理者へ確認を指示しなければならない。

カ　情報セキュリティ管理者は、前項の指示に従い、応急措置の実施及び復旧を行わ

なければならない。

キ　情報セキュリティ管理者は、情報セキュリティインシデントについて「8　運用における対策　⑷　事案への対応　ア　連絡先」における連絡先の内、必要な対象者に報告しなければならない。

7　技術的対策

⑴　情報システム等の管理

ア　ログの取得等

重要情報を取り扱う情報システム等に対し、次の措置を講じるものとする。

(ｱ) 情報システム管理者は、情報セキュリティの確保に必要なアクセス記録、システム稼動記録、障害時のシステム出力記録等（以下「ログ」という。）を取得し、一定の期間保存するものとする。また、必要に応じ、記録媒体にバックアップするものとする。

(ｲ) 情報システム管理者は、ログとして取得する項目、保存期間、取り扱い方法及びログが取得できなくなった場合の対処等について定めるものとする。

(ｳ) 情報システム管理者は、定期的にログの取得状況を確認し、必要に応じて内容を精査するものとする。

イ　情報システム等における運用管理の記録及び作業の確認

(ｱ) 情報システム管理者は、所管する情報システム等において行った変更等の処理及び当該情報システム等の運用等において行った作業の記録を作成し、適切に管理するものとする。

(ｲ) 情報システム管理者及び契約により操作を認められた委託事業者の従業員が担当する情報システム等において変更等の重要な作業を行う場合には、２名以上で作業し、互いにその作業を確認するものとする。また、作業する者が委託事業者の従業員のみの場合は、職員等が立ち会うものとする。

ウ　障害記録

情報システム管理者は、職員等から報告のあった情報システム等の障害に対する処理、問題等を障害記録として体系的に記録し、常に活用できるよう保存するものとする。

エ　情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、業務上必要とする者のみが閲覧できる場所に保管するものとする。また、情報システム等の開発、保守又は運用を委託事業者に委託した場合、当該委託事業者に守秘義務を課すものとする。

オ　バックアップ

情報システム管理者は、情報システムのデータベースやファイルサーバ等に記

録された情報について、その重要度に応じて期間・取得間隔・バックアップ方法・遠隔地へのバックアップ保管の有無を設定し、定期的にバックアップ用の複製を作成するものとする。また、重要情報を取り扱う情報システムを構成するサーバ、通信回線装置等については、サイバー攻撃等への対策も含め、運用状態を復元するために必要な設定情報等のバックアップを取得し保管するものとする。

カ　電子メール等

(ｱ) 情報システム管理者は、外部から外部への電子メールの中継処理が行われないよう、電子メールサーバの設定を行うものとする。

(ｲ) 情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信をできないようにするものとする。

(ｳ) 情報システム管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知するとともに、電子メールの総量が定められた容量未満になるまで一時的に当該職員等の電子メールの利用を停止するものとする。

(ｴ) 情報システム管理者は、情報システムの開発、運用等のために施設内で業務を行う委託事業者の従業員による電子メールアドレス利用方法を定めるものとする。

(ｵ) 職員等は、業務上必要のない送信先に電子メールを送信してはならない。また、職員等は、外部に電子メールを送信する際には、複数人での確認を行う等、情報漏えい等が起こらないように措置を講じるものとする。

(ｶ) 職員等は、原則として、業務用に与えられた電子メールアドレスあての電子メールを外部の電子メールアドレスに自動転送しないものとする。業務上、外部の電子メールアドレスへ自動転送を必要とする場合は、情報システム管理者の許可を得るものとする。

　情報システム管理者は、外部への自動転送について、その許可条件を定めるものとする。

(ｷ) 職員等は、原則として、電子メールで重要情報（あて先の情報及び発信者に係る情報を除く。）を送ってはならない。業務上必要がある場合には、情報システム管理者が定める暗号化等の機密性確保のための措置を講じるものとする。

(ｸ) 職員等は、情報システム管理者が定める容量を超える電子メールの送信を行ってはならない。

(ｹ) 職員等は、受信済みの電子メールは、電子メールボックスから削除するものとする。

(ｺ) 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、受信者相互の電子メールアドレスが分からないようにするものとする。

(ｻ) 職員等は、重要情報を含む電子メールを誤送信した場合、情報セキュリティ管

理者に報告するものとする。

(ｼ) 職員等は、情報システム管理者が許可したもの以外のウェブメール及びネットワークストレージサービスを使用してはならない。

キ　ファイルサーバ

(ｱ) 情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知するものとする。

(ｲ) 情報システム管理者は、ファイルサーバを所属等の単位で構成し、他所属等のフォルダ及びファイルを閲覧又は使用できないように設定するものとする。

(ｳ) 情報セキュリティ管理者は、同一所属等であっても、施設利用者等の個人情報等特定の職員等しか取り扱うことができない情報については、別途フォルダを作成し、担当職員等以外の職員等が閲覧又は使用できないように設定するものとする。

ク　複合機

(ｱ) 統括情報セキュリティ管理者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定するものとする。

(ｲ) 統括情報セキュリティ管理者は、複合機が備える機能について適切な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講じるものとする。

(ｳ) 統括情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じるものとする。

ケ　IoT 機器を含む特定用途機器

情報セキュリティ管理者は、IoT 機器を含む特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施するものとする。

コ　電子署名及び暗号化

(ｱ) 情報システム管理者は、法人以外に送る情報について、機密性を担保することが必要な場合には暗号化の措置を、完全性を担保することが必要な場合には電子署名、パスワード等による暗号化等、セキュリティを考慮した措置を講じて送信させるものとする。

(ｲ) 職員等は、情報システム管理者が定める方法により暗号化及び暗号鍵の管理を行うものとする。

(ｳ) 統括情報セキュリティ管理者は、電子署名の正当性を検証するための情報または手段を、署名検証者へ安全に提供するものとする。

サ　無許可でのソフトウェア導入及びソフトウェアの不適切利用等の禁止

(ｱ) 情報セキュリティ管理者は、ソフトウェアの導入状況について、ソフトウェア管理台帳を設け、適切に管理するものとする。

(ｲ) 職員等は、業務上の必要から標準実装以外のソフトウェアを端末にインストールする場合には、情報システム管理者の許可を得るものとする。

(ｳ) 職員等は、使用許諾に違反してソフトウェアを利用してはならない。

(ｴ) 職員等は、十分な脆弱性対策が実施されないなど、情報セキュリティ上問題となる恐れのあるソフトウェアを利用してはならない。

(ｵ) 情報システム管理者は、端末におけるソフトウェアの変更状況等について、サーバにより監視するものとする。

シ　端末の改造の禁止

(ｱ) 職員等は、端末の改造をしてはならない。

(ｲ) 職員等は、業務を遂行するために端末に対して部品の増設、又は交換を行う必要がある場合は、情報システム管理者の許可を得るものとする。

ス　無許可でのネットワーク接続の禁止

(ｱ) 職員等は、情報システム管理者の許可なく端末等をネットワークに接続してはならない。

(ｲ) 情報システム管理者は、端末等が適切に管理されることを確認した上で接続を許可するものとする。

セ　ネットワーク

(ｱ) 情報システム管理者は、ネットワークを構築する場合は、統括情報セキュリティ管理者と協議するものとする。また、変更又は廃止する場合も同様とする。

(ｲ) 情報システム管理者は、適切な管理下で接続を行い、情報セキュリティに留意したネットワーク構成を採るものとする。

(ｳ) 情報システム管理者は、外部ネットワークの瑕疵による情報の漏えい、破壊若しくは改ざん又はシステムダウン等により業務への影響が生じた場合に対処するため、損害賠償責任等を契約により担保するよう努めるものとする。

(ｴ) 情報システム管理者は、ウェブサーバ等のインターネット上で運用する情報システムの場合、次のセキュリティ対策を実施する。

a.　内部ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続するものとする。

b.　脆弱性が存在する可能性が増大することを防止するため、ウェブサーバ等が備える機能のうち、必要な機能のみを利用するものとする。

c.　ウェブサーバ等からの不用意な情報漏えいを防止するための措置を講じるものとする。

d.　ウェブコンテンツの編集等の作業を行う主体を限定するものとする。

(ｵ) 情報システム管理者は、接続した外部ネットワークの情報セキュリティに問題

が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ管理者の判断に従い速やかに当該外部ネットワークとの接続を遮断するものとする。

ソ　ネットワークの盗聴対策

(ｱ) 情報システム管理者は、無線 LAN の利用を認める場合には、解読が困難な暗号化及び認証技術の使用を義務づけるものとする。

(ｲ) 情報システム管理者は、機密性の高い情報を扱うネットワークに対し、情報の盗聴等を防ぐため、通信の暗号化等の措置を講じるものとする。

タ　外部記録媒体

情報システム管理者は、外部記録媒体の適正利用のため、次の対策を行う。

(ｱ) 外部記録媒体の適正利用及び持ち込み記録媒体の不適正利用防止のために必要なセキュリティ要件を策定するものとする。

(ｲ) 利用制御の仕組みにより端末の適切な設定等を行うことにより、外部記録媒体の不適正利用防止のための対策を講じるものとする。

(ｳ) 外部記録媒体の不適正利用又はその恐れがある状況を確認した場合は、外部記録媒体の利用を禁止又は制限する対策を講じるものとする。

(ｴ) 外部記録媒体の利用状況を定期的に確認するものとする。

チ　モバイル端末等による施設外からの情報システムの利用

情報システム管理者は、情報システム内にモバイル端末等を利用して施設外から利用することが適当でない情報がある場合は、施設外からの利用を禁止又は制限する対策を講じるものとする。

ツ　ウェブ会議サービスの利用時の対策

(ｱ) 統括情報セキュリティ管理者は、ウェブ会議を適切に利用するための利用手順を定めなければならない。

(ｲ) 職員等は、定められた利用手順に従い、ウェブ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施するものとする。

(ｳ) 職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずるものとする。

(ｴ) 職員等は、外部からウェブ会議に招待される場合は、定められた利用手順に従うものとする。

テ　情報システムの基盤を管理又は制御するソフトウェア導入・運用時の対策

(ｱ) 情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じるものとする。

(ｲ) 情報システム管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備するものとする。

a. 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

b. 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(ｳ) 情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施するものとする。

a. 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

b. 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

(ｴ) 情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認（新しいソフトウェアの出現等）による見直しを行うものとする。

⑵ アクセス制御

情報システム管理者は、所管する情報システム等ごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限する。

ア ID の取扱い

(ｱ) 情報システム管理者は、利用者の登録、変更、抹消等の手続き及びそれらの情報管理、職員の異動、派遣及び退職に伴う ID の取扱い等の方法を定めるものとする。

(ｲ) 情報システム管理者は、人事異動等で利用されていない ID が放置されない、ID に不要なアクセス権限が付与されていないよう定期的に点検するものとする。

(ｳ) 情報システム管理者は、職員等に対し、個人を単位に ID を付与するのを原則とするが、業務上止むを得ない場合は共用 ID を利用できるものとする。また、共用 ID を利用する場合は、過去に遡って共用 ID の利用者を特定できるように利用の記録及び管理を行うものとする。

(ｴ) 情報システム管理者は、共用 ID について、利用者の人事異動等の際にはパスワードを変更する等の措置を行うものとする。

イ 管理者権限

(ｱ) 情報システム管理者は、所管する情報システム等の管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID 及びパスワードを厳重に管理するものとする。

(ｲ) 情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

(ｳ) 情報システム管理者は、特権を付与された ID 及びパスワードの変更を委託事業者に行わせてはならない。

(ｴ) 情報システム管理者は、特権を付与されたパスワードについて、変更期間や入

力回数制限の設定値を小さくすることなどにより、セキュリティ機能をより強固にするものとする。

(ｵ) 情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じるものとする。

ウ　ネットワークのアクセス制御等

(ｱ) 情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を講じるものとする。

(ｲ) 情報システム管理者は、フィルタリング及びルーティングの不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定するものとする。

(ｳ) 統括情報セキュリティ管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保するものとする。また、情報セキュリティ対策について、定期的な確認により見直すものとする。

エ　外部ネットワークからのアクセス

(ｱ) 情報システム管理者は、内部のネットワーク又は情報システムに対する外部ネットワークからのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定するものとする。

(ｲ) 情報システム管理者は、法人の情報システム等へのリモートメンテナンス等、外部ネットワークからのアクセスを、必要があると認められた場合にのみ、セキュリティ対策を確保した上で、許可するものとする。

(ｳ) 情報システム管理者は、外部ネットワークからのアクセスを認める場合には、システム上利用者の本人確認を行う機能を確保するものとする。

(ｴ) 情報システム管理者が外部ネットワークからのアクセスを認める場合には、情報システム管理者等は、通信途上の盗聴を防御するために暗号化等の措置を講じるものとする。

(ｵ) 情報システム管理者は、外部ネットワークからのアクセスに利用する端末等を職員等に貸与する場合には、情報セキュリティ確保のために必要な措置を講じるものとする。

(ｶ) 統括情報セキュリティ管理者は、情報システム管理者以外の者が管理するネットワークから内部のネットワーク、又は情報システムに接続することは原則として禁止するものとする。

オ　自動識別

情報システム管理者は、ネットワーク機器のうち必要なものについて、機器固有

情報によってアクセスの可否を自動的に判別するものとする。

カ　ログイン手順

情報システム管理者は、ログイン手順中におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン及びログアウト時刻の表示、ログイン失敗時の記録等、正当なアクセス権を持つ職員等がログインしたことを確認することができる手順を定めるものとする。

キ　認証情報の管理方法

(ｱ) 情報システム管理者は、職員等の認証情報を厳重に管理するものとする。職員等のパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後、速やかに正規のパスワードに変更させるものとする。

(ｲ) 情報システム管理者は、パスワードの変更を行わない職員等にパスワードを変更する旨を勧告し、当該職員等が勧告に従わない場合には、一定期間経過後に当該職員等のアクセス権を停止するものとする。

(ｳ) 情報システム管理者は、当該職員等からパスワード変更の申告があった場合は、直ちに当該職員等のアクセス権の停止を解除するものとする。

(ｴ) 情報システム管理者は、職員等のパスワードについて、定期的にその妥当性の調査を行うものとする。

(ｵ) 情報システム管理者は、パスワードが第三者に読まれることのないよう、暗号化等の方法を定めるものとする。

ク　接続時間の制限

情報システム管理者は、管理者権限による情報システム等への接続時間を必要最小限に制限するものとする。

⑶　情報システムの開発、導入、保守等

ア　情報システムの調達

(ｱ) 情報システム管理者は、情報システムの調達に当たっては、調達仕様書が情報セキュリティポリシーで定められた情報セキュリティを確保できる内容にするものとする。また、情報システムに誤ったプログラム処理が組み込まれる等、不具合を考慮した技術的なセキュリティ機能（プログラム処理を安全側に帰着させる仕組み等）を調達仕様書に記載するものとする。

(ｲ) 情報システム管理者は、機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないことを確認するものとする。

イ　情報システムの開発、更新、統合等

情報システム管理者は、情報システムの開発、更新若しくは統合時の事故又は不正行為の対策のため、次の事項を実施するものとする。

(ｱ) 管理者及び監督者の特定

(ｲ) システム開発のための規則の確立

(ｳ) 作業者及び作業範囲の特定
(ｴ) 情報漏えいが発生した場合の影響範囲等のリスクの検討
(ｵ) 情報システム及びデータ移行手続きが失敗した場合や移行直後に障害等が発生した場合における、旧情報システムへ戻す計画とその手順の作成
(ｶ) 情報システム及びデータ移行手続きにおける検証チェックポイントや移行の妥当性基準の明確化
(ｷ) 開発環境と運用環境の分離
(ｸ) ハードウエア及びソフトウェアの特定（特定したもの以外の利用禁止）
(ｹ) 情報セキュリティ上問題となる恐れのあるソフトウェアの使用禁止
(ｺ) ソースコードの点検
(ｻ) 管理者、作業者等が利用する ID の管理（開発、更新又は統合の終了後に不要となった時点での ID の速やかな抹消等）
(ｼ) 管理者、作業者等のアクセス制限の設定
(ｽ) 機器の搬出入の際の許可及び確認
(ｾ) 既知の種類のウェブアプリケーション等の脆弱性を排除するための措置

ウ　情報システムの導入

(ｱ) 情報システム管理者は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に十分なテストを行うものとする。
(ｲ) 情報システム管理者は、運用テストを行う場合には、あらかじめテスト環境による操作確認を行うものとする。
(ｳ) 情報システム管理者は、重要情報をテストデータに使用してはならない。
(ｴ) 情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入するものとする。
(ｵ) 情報システム管理者は、本稼動前に新たに導入する情報システムの脆弱性の有無について、原則として、第三者による技術的検証を実施し、脆弱性が存在しないことを確認するものとする。
(ｶ) 情報システム管理者は、情報システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行うものとする。
(ｷ) 情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認するものとする。
(ｸ) 情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発実施者から運用保守実施者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認するものとする。

エ　情報システムにおける入出力データの正確性の確保

(ｱ) 情報システム管理者は、情報システムに入力されるデータについて、適切なチェック等を行い、当該データが安全かつ正確であることを確実にするための対策を講じるものとする。

(ｲ) 情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施する。

a. 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等の見直しを行うものとする。

b. 運用中のアプリケーション・コンテンツにおいて、動作環境も含め定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じるものとする。

c. ウェブアプリケーションやウェブコンテンツにおいて、エラーによる情報の書換え又は故意による情報の改ざんの恐れがある場合には、これを検出する手段を講じるものとする。

また、必要な場合は情報の修復を行う手段を講じるものとする。

(ｳ) 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計するものとする。

オ　情報システムの保守

(ｱ) 情報システム管理者は、ソフトウェアの更新等を行う場合には、不具合及び他の情報システムへの悪影響が生じないことを確認し、計画的に実施するものとする。

(ｲ) 情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対して、速やかにプログラムの修正を行うものとする。

カ　システム開発・保守に関連する資料等の整備・保管

(ｱ) 情報システム管理者は、以下を含むシステム開発・保守に関連する資料及びシステム関連文書を、適切に整備・保管するものとする。

・情報システムを構成するサーバ装置及び端末関連情報
・情報システムを構成する通信回線及び通信回線装置関連情報
・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
・情報セキュリティインシデントを認知した際の対処手順
・情報システムが停止した際の復旧手順

(ｲ) 情報システム管理者は、使用したデータ及びテストの結果を一定期間適切に保管するものとする。

(ｳ) 情報システム管理者は、情報システムに係るソースコードを適切な方法で保管するものとする。

(ｴ) 情報システム管理者は、情報システムの変更等を行った場合は、その設定、構成等の履歴を記録し、保存するものとする。

キ　情報システム台帳の整備

統括情報セキュリティ管理者は、法人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、情報システム台帳を整備するものとする。また、情報システム台帳の整備にあたり、情報システム管理者は、協力するものとする。

⑷　不正プログラム対策

ア　情報システム管理者等は、次の事項を実施するものとする。

(ｱ) インターネットを通じて受信したファイルは、インターネットのゲートウェイにおいて、コンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムと疑われるファイルは削除するなど、不正プログラムの情報システム等への侵入を防止するものとする。

(ｲ) インターネットを通じて送信するファイルは、インターネットのゲートウェイにおいて、コンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムと疑われるファイルは削除するなど、不正プログラムの外部への拡散を防止するものとする。

(ｳ) コンピュータウイルス等の不正プログラムに関する情報を収集し、必要に応じ職員等に対する注意喚起を行うものとする。

(ｴ) サーバ及び端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させるものとする。

(ｵ) 不正プログラム対策ソフトウェアのパターンファイル等を常に最新のものに保つものとする。

(ｶ) 不正プログラム対策ソフトウェア等の設定変更権限については一括管理し、許可した職員を除く職員等に当該権限を付与してはならない。

(ｷ) 十分な脆弱性対策が実施されないなど、情報セキュリティ上問題となる恐れのあるソフトウェアを利用してはならない。特に、ソフトウェアの導入の際は、利用を予定している期間中に脆弱性対策に係る開発元のサポートが終了する予定がないことを確認するものとする。

イ　職員等は、次の事項を遵守するものとする。

(ｱ) 外部からデータ又はソフトウェアを取り入れる場合には、必ず無害化又は不正プログラム対策ソフトウェア等によるチェックを行うものとする。外部へ公開又は提供する場合においても同様とする。

(ｲ) 端末に搭載された不正プログラム対策ソフトウェアの設定内容を変更することにより、セキュリティレベルを低下させないものとする。

(ｳ) 不正プログラム対策ソフトウェアによるウイルスチェックの実行を途中で止めないものとする。

(ｴ) 添付ファイルのある電子メールを送受信する場合は、無害化又は不正プログラ

ム対策ソフトウェア等によるチェックを行い、不正プログラムと疑われる添付ファイルは開かず速やかに削除するものとする。

(ｵ) 情報システム管理者が提供するコンピュータウイルス等の不正プログラムに関する情報を確認し、その指示に従うものとする。

(ｶ) 職員等は、使用している端末等がコンピュータウイルス等の不正プログラムに感染又は感染が疑われる場合は、一切の操作を中止して情報セキュリティ管理者に報告しなければならない。その際、LAN ケーブルを取り外す又は無線 LAN 機能を停止する等の措置・対処については、情報セキュリティ管理者の指示に従わなければならない。

ウ　専門家の支援体制

情報システム管理者等は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにするものとする。

⑸　不正アクセス対策

情報システム管理者等は、次の事項を実施するものとする。

ア　使用されていないポートを閉鎖するものとする。

イ　不要なサービスについて、機能を削除又は停止するものとする。

ウ　不正アクセスによるホームページ書換え防止を確実にするために、データの書換えを検出し、情報システム管理者へ通報する設定を講じるものとする。

エ　対策重要度Ⅳに該当する情報を取り扱う情報システムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査するものとする。

オ　外部から攻撃を受けることが明確な場合には、関係機関との連絡を密にして情報の収集に努め、情報システムの停止を含む必要な措置を講じるものとする。

カ　不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号）に定める違反等犯罪の可能性がある攻撃を受けた場合には、記録の保存に努めるとともに、警察、関係機関との緊密な連携に努めるものとする。

キ　職員等又は委託事業者による不正アクセスがあった場合には、当該職員等が所属する所属の情報セキュリティ管理者に通知し、適切な措置を求めるものとする。

ク　外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じるものとする。

ケ　標的型攻撃による内部への侵入を防止するため、教育や自動再生無効化等の人的対策や入口対策を講じるものとする。また、内部に侵入した攻撃を早期検出して対処するために、通信をチェックする等の内部対策及び出口対策を講じるものとする。

8　運用における対策

⑴　情報システム等の監視

ア　情報システム管理者等は、情報システム運用時の監視に係る運用管理機能要件を策定した上で、情報システムを構成するサーバやネットワーク等の監視機能を実装し、情報システムに実装された監視を含むセキュリティ機能を適切に運用するものとする。また、情報資産への侵害等、情報セキュリティに関する異常事態、不正行為、事故、障害等（以下「事案」という。）を検知するため、常に情報システム等の監視を行うものとする。

イ　情報システム管理者等は、外部ネットワークと常時接続する情報システム等について、ネットワーク侵入監視装置を設置し、常時監視を行うものとする。

ウ　情報システム管理者等は、重要なアクセス記録等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じるものとする。

エ　情報システム管理者等は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入するものとする。

オ　情報システム管理者等は、情報システム等における監視の対象や手法を定期的に見直すものとする。

⑵　情報セキュリティに関する技術情報の収集、対応及び共有

ア　情報システム管理者等は、不正プログラム等のセキュリティ情報を収集し、ソフトウェアにパッチを当てる等、情報セキュリティ対策上必要な措置を講じるものとする。

　また、必要に応じ、対応方法を職員等に周知するものとする。

イ　情報セキュリティ管理者等は、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じるものとする。

　また、必要に応じ、情報セキュリティに関して収集した情報を関係者間で共有するものとする。

⑶　情報セキュリティポリシーの遵守状況の確認及び対処

ア　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、統括情報セキュリティ管理者に報告を行うものとする。

イ　統括情報セキュリティ管理者は、問題に適切に対処し、必要に応じて情報セキュリティ責任者に報告するものとする。

ウ　情報システム管理者等が指名した者は、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端末、アクセス記録、電子メールログ等を調査できるものとする。

エ　情報システム管理者等は、サーバ等のシステム設定が情報セキュリティポリシーに適合しているかどうかについて定期的に確認を行い、問題を認めた場合には、

速やかかつ適切に対処するものとする。

オ　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及び情報セキュリティ実施手順を参照できるよう配慮するものとする。

⑷　事案への対応

情報セキュリティインシデント、情報資産に対するセキュリティ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ける連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のアからウのとおり定める。

ア　連絡先

・情報セキュリティ責任者
・統括情報セキュリティ管理者
・情報システム管理者
・情報システム等に係る委託事業者
・コンピュータ緊急対応センター（JPCERT）
・管轄警察署
・神奈川県警察本部サイバー犯罪対策課
・神奈川県
・関係機関（独立行政法人情報処理推進機構（IPA）等）
・影響が考えられる個人及び法人

イ　事案の調査

情報セキュリティに関する事案を認めた職員等は、次の項目について、速やかに情報セキュリティ管理者及び情報システム管理者等に報告するものとする。

・事案の内容
・事案が発生した原因として、想定される行為
・確認した被害及び影響範囲

上記の報告を受けた情報システム管理者等は、事案の詳細な調査を行うとともに、統括情報セキュリティ管理者への報告を行うものとする。

ウ　事案への対処

情報システム管理者等は、事案に対処するために次の項目を実施するものとする。

⑺ 情報システム管理者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡する。

・サイバーテロその他の施設利用者等に重大な被害が生じる恐れがあるとき（情報セキュリティ責任者、統括情報セキュリティ管理者、警察、影響が考えられる個人及び法人）
・不正アクセスその他犯罪と思慮されるとき（統括情報セキュリティ管理者、警

察）
・踏み台となって他者に被害を与える恐れがあるとき（統括情報セキュリティ管理者、警察）
・情報システムに関する被害（情報システム管理者、必要と認められる事業者等）
・その他情報資産に係る被害（統括情報セキュリティ管理者）

(ｲ) 情報システム管理者は、次の事案が発生し情報資産の防護のためにやむを得ない場合は、ネットワークを切断する措置を講じる。
・異常なアクセスが継続しているとき、又は不正アクセスが判明したとき
・情報システムの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等の不正プログラムがネットワーク経由で拡がっているとき
・情報資産に係る重大な被害が想定されるとき

(ｳ) 情報システム管理者は、次の事案が発生し情報資産の防護のためにやむを得ない場合は、コンピュータ及び情報システムを停止する。
・コンピュータウイルス等の不正プログラムが情報資産に深刻な被害を及ぼしているとき
・災害等により電源を供給することが危険又は困難なとき
・その他の情報資産に係る重大な被害が想定されるとき

(ｴ) 情報システム管理者等は、事案に係る情報システム等のアクセス記録及び現状を保存する。

(ｵ) 情報システム管理者等は、事案に対処した経過を記録する。

(ｶ) 情報システム管理者等は、事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する。

(ｷ) 情報システム管理者等は、再発防止の暫定措置を講じた後、復旧する。

エ　再発防止の措置

(ｱ) 情報システム管理者等は、当該事案に係るリスク分析を実施し、情報セキュリティ対策の改善に係る再発防止計画を策定し、統括情報セキュリティ管理者へ報告するものとする。

　統括情報セキュリティ管理者は、情報セキュリティ対策の改善に係る再発防止計画が有効であると認められる場合は、これを了承し、情報セキュリティ責任者に報告するものとする。

(ｲ) 情報セキュリティ責任者は、統括情報セキュリティ管理者から、情報セキュリティ対策の改善に係る再発防止計画が有効であることを了承したことについて報告を受けた場合は、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ものとする。

オ　業務継続計画の策定

情報システム管理者等は、業務継続計画における情報セキュリティ関連事項について策定する場合は、地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン（平成 20 年 8 月総務省）を参考とするものとする。

⑸　業務委託

ア　情報セキュリティ管理者及び情報システム管理者等は、契約締結前に、委託事業者において必要な情報セキュリティ対策が確保されていることを確認するものとする。

イ　情報セキュリティ管理者及び情報システム管理者等は、開発、保守、運用等を委託する場合は、委託事業者に対し、守秘義務等の必要なセキュリティ要件を契約書に明記するものとする。

なお、重要情報を取り扱う委託業務の実施に当たっては、「業務委託等に係る情報管理要領」に従うものとする。

また、外部サービスを利用する場合も、同様の取扱いとする。

ウ　情報セキュリティ管理者及び情報システム管理者等は、委託事業者において必要な情報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、イの契約に基づき措置するものとする。

エ　情報セキュリティ管理者及び情報システム管理者等は、委託事業者との契約書において情報セキュリティポリシーが遵守されなかった場合における損害賠償、契約解除等の規定を定めるものとする。

⑹　外部サービスの利用

ア　統括情報セキュリティ管理者は、外部サービスの利用に関するセキュリティ要件等の規定を整備するものとする。

イ　情報セキュリティ管理者及び情報システム管理者等は、外部サービスを利用するに当たり、前項の規定「外部サービス利用に係る情報セキュリティ要領」に従うものとする。

⑺　ソーシャルメディアサービスの利用

ア　情報セキュリティ管理者は、法人が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めた運用手順を定めるものとする。

(ｱ) 法人のアカウントによる発信が、実際に法人による発信であることを明らかにするために、法人の公式ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自己記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

(ｲ) パスワードや認証のための情報を適切に管理するなど、不正アクセス対策を行うこと。

イ　職員等は、対策重要度Ⅳ以外の情報（あて先の情報及び発信者に係る情報を除

く。）をソーシャルメディアサービスで発信してはならない。

ウ　情報セキュリティ管理者は、管理するアカウントについて、責任者を定めるものとする。

エ　情報セキュリティ管理者は、アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じるものとする。

オ　情報セキュリティ管理者は、可用性が求められる情報の発信にソーシャルメディアサービスを用いる場合は、原則として法人の公式ウェブサイトに当該情報を掲載して参照できるようにするものとする。

9　評価及び見直し

⑴　監査

ア　統括情報セキュリティ管理者は、情報セキュリティ監査統括管理者を指名し、情報資産に対する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監査を行うものとする。

イ　情報セキュリティ監査統括管理者は、監査を実施する場合には、被監査部門から独立し、かつ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対して、監査の実施を依頼するものとする。

ウ　情報セキュリティ監査統括管理者は、監査を行うに当たって、監査実施計画を立案し、統括情報セキュリティ管理者の承認を得るものとする。

エ　被監査部門は、監査の実施に協力するものとする。

オ　情報システムの開発又は運用を委託事業者に委託している場合、情報セキュリティ監査統括管理者は委託事業者の情報セキュリティポリシーの遵守状況について、定期的に又は必要に応じて監査を行うものとする。

カ　情報セキュリティ監査統括管理者は、監査結果をとりまとめ、統括情報セキュリティ管理者に報告する。統括情報セキュリティ管理者は、情報セキュリティ監査統括管理者から報告を受けた監査結果を情報セキュリティ責任者に報告する。

キ　統括情報セキュリティ管理者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処（改善計画の策定等）を指示するものとし、改善状況を翌年度の監査時に確認する等、把握するものとする。統括情報セキュリティ管理者は、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させるものとする。また、法人で横断的に改善が必要な事項については、統括情報セキュリティ管理者は、当該事項への対処（改善計画の策定等）を指示するものとし、改善状況を翌年度の監査時に確認する等、把握するものとする。

ク　情報セキュリティ監査統括管理者は、監査の実施を通して収集した監査証拠、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する

ものとする。

ケ　統括情報セキュリティ管理者は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直しに際して活用するものとする。

⑵　点検

ア　情報システム管理者等は、所管する情報システム等について、定期的に又は必要に応じ自己点検を実施するものとする。

イ　情報セキュリティ管理者は、所管する所属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、定期的に又は必要に応じて自己点検を実施するものとする。

ウ　ア及びイの自己点検を行った者は、点検の結果に基づき、自己の権限の範囲内で改善を図るものとする。

エ　情報セキュリティ管理者等は、自己点検結果及びこれに基づく改善策をとりまとめ、統括情報セキュリティ管理者に報告するものとし、統括情報セキュリティ管理者は、当該報告の結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直しに際して活用するものとする。

⑶　情報システム等の見直し

情報セキュリティ管理者及び情報システム管理者等は、定期的に又は必要に応じて、次の観点によるところにより、情報セキュリティ対策について、見直すものとする。

ア　所管する情報システム等での新たな脅威の出現、運用、監視等の状況

イ　所管する情報システム等の機器の構成や設定情報等の変更

ウ　所管する業務又は情報資産の変更

エ　統括情報セキュリティ管理者による横断的に改善が必要となる情報セキュリティ対策に係る指示

オ　その他、情報セキュリティ対策に影響を与える事項の発生（国等からの通知、関係法令や関係規程の改正、情報セキュリティインシデントの発生等）

⑷　情報セキュリティポリシーの改正

情報セキュリティ監査及び点検の結果並びに情報セキュリティに関する状況の変化等により、横断的に改善が必要なものを含め新たに情報セキュリティ対策の必要が発生した場合又は、情報セキュリティポリシーの改正の必要性が生じた場合は、統括情報セキュリティ管理者は情報セキュリティポリシーの改正案を策定するものとし、その内容を情報セキュリティ責任者に報告するものとする。

10　例外措置

⑴　例外措置の協議

情報セキュリティ管理者及び情報システム管理者等は、情報セキュリティポリシーを遵守することが困難であるため、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には、統括情報セキュリティ管理者と協議の上、例外措置を取ることができる。

⑵　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者等は、緊急を要する等の場合であって、情報セキュリティポリシーを遵守することが困難であるときは、事後速やかに統括情報セキュリティ管理者に報告書を提出するものとする。

⑶　例外措置の協議書等の保管

統括情報セキュリティ管理者は、例外措置の協議書、協議結果及び報告書を適切な方法により保管するものとする。

附　則

この要綱は、令和８年４月１日から施行する。