一関市病院事業　情報セキュリティポリシー

令和８年４月

一関市病院事業

目次

第１章　情報セキュリティポリシーの構成 3
１．１　構成 3
第２章　情報セキュリティ基本方針 4
２．１　目的 4
２．２　定義 4
２．３　対象とする脅威 5
２．４　適用範囲 5
２．５　職員等の遵守義務 5
２．６　情報セキュリティ対策 5
２．７　情報セキュリティ監査及び自己点検の実施 6
２．８　情報セキュリティポリシーの見直し 7
２．９　情報セキュリティ対策基準の策定 7
２．１０　情報セキュリティ実施手順の策定 7
第３章　情報セキュリティ対策基準 8
３．１　組織体制 8
３．２　情報資産の分類と管理 10
３．３　情報システム全体の強靭性の向上 13
３．４　物理的セキュリティ 14
３．５　人的セキュリティ 16
３．６　技術的セキュリティ 20
３．７　運用 31
３．８　業務委託と外部サービス（クラウドサービス）の利用 34
３．９　評価・見直し 36

第１章　　情報セキュリティポリシーの構成

１．１　　構成

情報セキュリティポリシーとは、一関市病院事業が所掌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とりまとめたものを総称する。情報セキュリティポリシーは、当事業が所掌する情報資産に関する業務に携わる職員（再任用職員、会計年度任用職員を含む。以下「職員等」という。）及び委託事業者に浸透、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求される。

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へ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（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

第２章 情報セキュリティ基本方針

第３章 情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報セキュリティ対策を実施するための具体的な手順を定めた「情報セキュリティ実施手順」を策定することとする。

情報セキュリティポリシー構成表

文書名		内容
情報セキュリティポリシー	第２章 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
	第３章 情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システム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		情報セキュリティ対策基準に基づく情報セキュリティ対策を実施するための具体的な手順

第２章　　情報セキュリティ基本方針

２．１　　目的

本基本方針は、当事業が保有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、当事業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。

２．２　　定義

（1）ネットワーク

コンピュータ等を相互に接続するための通信網とその構成機器（ハードウェア及びソフトウェア）をネットワークといい、ネットワークのうち本市が構築している組織内のネットワークを事業内ネットワークという。

（2）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（3）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。

（4）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（6）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。

（7）可用性

情報にアクセスすることを認められた者が、必要な時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。

（8）業務系ネットワーク（情報システム接続系）

電子カルテや部門システム、介護保険情報システム等の患者情報を取扱う情報システム及びデータをいう。

（9）部門系ネットワーク（部門システム接続系）

部門独自に構築されたネットワークに接続された情報システム及びその情報システムで取扱うデータをいう。

（１０）　情報系ネットワーク（インターネット接続系）

インターネットに接続された情報システム及びその情報システムで取扱うデータをいう。

（１１）　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

２．３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの仕様等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）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

２．４　適用範囲

（１）適用組織の範囲

本基本方針の適用範囲は、病院事業を行うすべての施設とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

２．５　職員等の遵守義務

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ち、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義務を負う。

２．６　情報セキュリティ対策

２．３対象とする脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）組織体制

当事業の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

当事業の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき、情報セキュリティ対策を行う。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① 業務系ネットワーク（情報システム接続系）においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定等により、患者情報の流出を防ぐ。

② 部門系ネットワーク（部門システム接続系）においては、部門系ネットワーク（部門システム接続系）と接続する業務用システムと、業務系ネットワーク（統合情報システム接続系）の情報システムとの通信経路を分割する。なお、両ネットワーク間で通信する場合には、ファイアウォールや中間サーバを設置する等の情報セキュリティ対策を実施する。

③ 情報系ネットワーク（インターネット接続系）においては、必要に応じて不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（4）物理的セキュリティ

サーバ室への不正な立入り、情報資産への損傷及び利用の妨害等から保護するために物理的な対策を講じる。

（5）人的情報セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6）技術的セキュリティ

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理・暗号化処理等の技術的な対策を講じる。

（7）運用

情報システムの管理、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

① 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。

② 外部サービスを利用する場合は、あらかじめ情報セキュリティ管理者の承認を得たサービスのみを利用し、許可なく業務情報を保存または処理してはならない。利用にあたっては、二要素認証の設定やアクセス権限の最小化など、組織が指定する安全管理措置を講じるものとする

③ ソーシャルメディアサービスを利用する場合には、情報セキュリティ管理者が管理するアカウントを使用し、職員個人が私的に取得したアカウントは使用しない。

2.7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

２．８　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には、情報セキュリティポリシーを見直す。

２．９　情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

２．１０ 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に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。なお、情報セキュリティ実施手順は、公にすることにより当事業の運営に重大な支障を及ぼすおそれがあることから非公開とする。

第３章　　情報セキュリティ対策基準

本対策基準は、基本方針に基づいて全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準を定めるものである。

３．１　　組織体制

名称	対象者	主な役割
(1) 最高情報セキュリティ責任者(CISO)	病院事業管理者	情報資産の管理及び情報セキュリティ対策の最終決定権限及び責任
(2) 情報セキュリティ責任者	事務局長	CISO の補佐、欠員時の代理、(3)～(5) への指導・助言、セキュリティ侵害発生時の CISO への報告
(3) 情報セキュリティ管理者	院長、総看護師長、診療支援室長、所長、事務長、介護事業に置く管理者	所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任
(4) 情報システム管理者	各科・係の長	所管する科、係等の情報セキュリティ対策に関する権限及び責任と所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任
(5) 情報システム担当者	藤沢病院事務局において情報システムの管理に従事する職員	情報システム開発/変更/運用等の作業

(1)最高情報セキュリティ責任者（ Chief Information Security Officer、以下「ＣＩＳＯ」という。）ＣＩＳＯを置き、病院事業管理者をもって充てる。

(2)情報セキュリティ責任者

① 情報セキュリティ責任者を置き、事務局長をもって充てる。

② 情報セキュリティ責任者はＣＩＳＯを補佐するとともに、ＣＩＳＯに事故があるとき又は欠けたときはＣＩＳＯの職務を代理する。

③ 情報セキュリティ責任者は、当事業の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

④ 情報セキュリティ責任者は、当事業の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

⑤ 情報セキュリティ責任者は、情報セキュリティ管理者、情報システム管理者、及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑥ 情報セキュリティ責任者は、当事業の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セキュリティ侵害のおそれがある場合に、ＣＩＳＯの指示に従い、ＣＩＳＯ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を有する。

⑦　情報セキュリティ責任者は、当事業の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑧　情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑨　情報セキュリティ責任者は、緊急時にはＣＩＳＯに早急に報告を行うとともに、回復のための対策を講じなければならない。

（3）情報セキュリティ管理者

①　次に掲げる者を情報セキュリティ管理者とする。

1.　一関市国民健康保険藤沢病院

（ア）院長

（イ）総看護師長

（ウ）診療支援室長

2.　介護事業

（ア）所長

（イ）事務長

（ウ）介護事業に置く管理者

②　情報セキュリティ管理者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③　情報セキュリティ管理者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

（4）情報システム管理者

①　各科・係の長を情報システム管理者とする。

②　情報システム管理者は、その所管する科・係等の情報セキュリティ対策に関する権限及び責任と所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③　情報システム管理者は、特定個人情報を取り扱う職員を指定し、それ以外の職員には、特定個人情報の取扱をさせてはならない。

④　情報システム管理者は、その所管する科・係等において、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セキュリティ侵害のおそれがある場合には、情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

⑤　情報システム管理者は、その所管する科・係等において所有している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、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

（5）情報システム担当者

① 藤沢病院事務局総務係において情報システムの管理に従事する職員を情報システム担当者とする。

② 情報システム担当者は、情報セキュリティ管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

（6）兼務の禁止

① 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

② 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（7）情報セキュリティインシデントに対処するための体制（Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）の設置・役割

① ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化するものとする。

② ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置き、ＣＳＩＲＴ内の業務総括及び外部との連携等を行う職員を定めるものとする。

③ ＣＩＳＯは、情報セキュリティに関する統一的な窓口を設置し、情報セキュリティインシデントについて部局等や住民から報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④ ＣＩＳＯによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供するものとする。

⑤ 情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、岩手県、一関市等へ報告するものとする。

⑥ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

⑦ 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行うものとする。

３．２　情報資産の分類と管理

（1）情報資産の分類

当事業の情報資産の分類当院における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

① 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	・秘密文書に相当する情報資産 ・個人情報	・支給された端末以外での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄必要以上の複製及び配付禁止 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	・不開示情報のうち個人情報を除くもの ・秘密文書に相当する機密性は要しないが、一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

② 完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	情報資産のうち、改ざん、誤びゅう又は破損により、利用者等の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップの作成、保管 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

③ 可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、利用者等の権利が侵害される、又は病院事業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資産	・バックアップの作成、保管及び相当時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	上記以外の情報資産	

（２）情報資産の管理

① 管理責任

(ア)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。

(イ)情報セキュリティ管理者は、所管する情報資産について当該情報資産を適切に管理しなければならない。

(ウ)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（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

職員等は、情報資産の分類について、文書管理システムに入力するほか、ファイル（ファイル名、ファイルの属性（プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル等の情報資産に表示するものとし、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

③ 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)情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ)情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、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。

④ 情報資産の入手

(ア)当事業内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(イ)当事業外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ)情報資産を入手した者は、入手した情報資産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がなければならない。

⑤ 情報資産の利用

(ア)情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(イ)情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

(ウ)情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥ 情報資産の保管

(ア)情報セキュリティ管理者は、情報資産の分類に従って、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は、情報資産を記録した電磁的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は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦　情報の送信

電子メール等にファイルを添付することにより機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。また、電子メール等の本文には機密性２以上の情報を記載してはならない。

⑧　情報資産の運搬

(ア)車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(イ)機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨　情報資産の提供・公表

(ア)機密性２以上の情報資産を外部に提供する者は、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)機密性２以上の情報資産を外部に提供する者は、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は、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。

(エ)情報資産を提供する場合は、情報セキュリティ管理者が指定する電磁的記録媒体により必要に応じて暗号化やパスワードの設定を行い、提供しなければならない。

⑩　情報資産の廃棄

(ア)機密性２以上の電磁的記録を含む情報資産を廃棄する者は、情報を記録している機器又は媒体が不要になった場合、電磁的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)情報資産のうち、文書により記録されているものの廃棄は、一関市文書取扱規程（平成17 年一関市訓令第15 号）に定めるところによる。

(ウ)情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

(エ)情報資産の廃棄を行う者は、行った処理について、日時、実施者及び処理内容を記録しなければならない。

３．３　情報システム全体の強靭性の向上

(１)、業務系ネットワーク（医療・介護情報システム接続系）の情報システムにおいては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定等により、

利用者情報の流出を防ぐ。

（2）情報系ネットワーク（インターネット接続系）においては、必要に応じて不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

３．４　物理的セキュリティ

３．４．１サーバ等の管理

（1）機器の取付け

情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合、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に固定する等、必要な措置を講じなければならない。

（2）サーバの冗長化

① 情報セキュリティ管理者は、医療情報システムサーバを冗長化し、同一データを保持しなければならない。

（3）機器の電源

① 情報セキュリティ管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が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なければならない。

② 情報セキュリティ管理者は、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なければならない。

（4）通信ケーブル等の配線

① 情報セキュリティ管理者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② 情報セキュリティ管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、対応しなければならない。

③ 情報セキュリティ管理者は、自ら又は情報セキュリティ管理者、情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

（5）機器の定期保守及び修理

① 情報セキュリティ管理者は、サーバ等の機器の定期保守を実施しなければならない。

② 情報セキュリティ管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティ管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

（6）事業外への機器の設置

情報セキュリティ管理者は、事業外にサーバ等の機器を設置する場合、ＣＩＳＯの承認を得な

ければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

(7)機器の廃棄等

情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、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措置を講じなければならない。また、廃棄を委託した場合も同様とし、必要に応じて証明書等の提出を求めるものとする。

3.4.2 管理区域(情報システム室等)の管理

(1)管理区域の構造等

① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋(以下「サーバ室」という。)や電磁的記録媒体の保管庫をいう。

② 情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

(2)通信回線及び通信回線装置の管理

① 情報セキュリティ管理者は、事業内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

② 情報セキュリティ管理者は、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しなければならない。

③ 情報セキュリティ管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

④ 情報セキュリティ管理者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑤ 情報セキュリティ管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、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セキュリティ対策を実施しなければならない。

⑥ 情報セキュリティ管理者は、通信回線装置が動作するために必要なソフトウェアの状態等を把握し、認識した脆弱性等について対策を講じなければならない。

(3)機器等の搬入出

① 情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

② 情報システム管理者は、サーバ室の機器等の搬入出について、職員を立ち会わせなければならない。

（4）通信回線及び通信回線装置の管理

① 情報システム管理者は、事業内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

② 情報システム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③ 情報システム管理者は、情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

④ 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、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑤ 情報システム管理者は、情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

３．４．３職員等の利用する端末等の管理

① 職員等は、盗難時における情報漏えい防止のため、執務室等で利用する端末のハードディスク上には業務に必要な情報を保存してはならない。また、電磁的記録媒体については、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しなければならない。

② 情報セキュリティ責任者は、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。

３．５　人的セキュリティ

３．５．１職員等の遵守事項

（1）職員等の遵守事項

① 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。また、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。

② 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環境へのアクセスを行ってはならない。

③ 端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

④ 職員等は、病院事業の端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

⑤ 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なけれ

ばならない。

⑥　支給以外の端末及び電磁的記録媒体等の業務利用

⑦　職員等は、支給以外の端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、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利用することができる。

⑧　職員等は、支給以外の端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

⑨　前２項目により、支給以外の端末及び電磁的記録媒体等を利用する場合は、機密性３の情報資産を扱ってはならない。

⑩　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末及び電磁的記録媒体、書類等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑪　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

⑫　机上の端末等の管理

職員等は、端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること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や電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

（２）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には、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。

（３）職員等への対応

①　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、職員等に対し、採用時に情報セキュリティポリシーの守るべき内容を理解させ、また実施及び遵守させなければならない。

②　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、職員等の採用時に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　インターネット接続及び電子メール使用等の制限

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おいて、インターネット環境への接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（4）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及び情報セキュリティ実施手順を閲覧できるように掲示しなければならない。

（5）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・保守等を事業者に発注する場合、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。

３．５．２研修・訓練

（1）情報セキュリティに関する研修・訓練

情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（2）研修計画の策定及び実施

① 情報セキュリティ責任者は、職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を行わなければならない。なお、研修内容は、情報セキュリティ責任者、情報セキュリティ管理者、職員等に対し、それぞれの役割と情報セキュリティに対する理解度に応じたものにしなければならない。

② 情報セキュリティ責任者は、策定された研修計画に基づき、毎年度、職員等に情報セキュリティ研修を受講させなければならない。

③ 情報セキュリティ責任者は、新採用職員等を対象とする情報セキュリティ研修を実施しなければならない。

④ 情報セキュリティ責任者は、毎年度、情報セキュリティ委員会又はＣＩＳＯに対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（3）緊急時対応訓練

情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練は、ネットワーク及び各情報システムの規模等を考慮し、実施体制、範囲等を定め、効果的に実施できるようにしなければならない。

（4）研修・訓練への参加

職員等は、指定された研修・訓練に参加しなければならない。

３．５．３情報セキュリティインシデントの報告（セキュリティインシデント：マルウェアの感染や不正アクセス、あるいは機密情報の流出など、セキュリティ上の脅威となる事象）

（1）事業内からの情報セキュリティインシデントの報告

① 職員等は、情報セキュリティインシデントを認知した場合、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。

② 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責任者に報告しなければならない。

③ 情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、ＣＩＳＯに報告しなければならない。

（2）住民等外部からの情報セキュリティインシデントの報告

① 職員等は、当事業が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない

② 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責任者、情報セキュリティ責任者に報告しなければならない。

③ 情報セキュリティ責任者は、当該情報セキュリティインシデントについて、ＣＩＳＯ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、報告のあった情報セキュリティインシデントが、個人の権利利益を害するおそれが大きいと判断した場合は、当該個人に対し、当該情報セキュリティインシデントが生じた旨を通知しなければならない。

⑤ ＣＩＳＯは、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（3）情報セキュリティインシデント原因の究明・記録、再発防止等

① 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わなければならない。

② ＣＳＩＲＴ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、ＣＩＳＯに速やかに報告しなければならない。

③ ＣＳＩＲＴは、情報セキュリティインシデントに関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を行わなければならない。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セキュリティ管理者へ確認を指示しなければならない。

④ ＣＳＩＲＴは、これらの情報セキュリティインシデント原因を究明し、記録を保存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の原因究明の結果から、再発防止策を検討し、ＣＩＳＯに報告しなければならない。

⑤ ＣＩＳＯは、ＣＳＩＲＴから、情報セキュリティインシデント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しなければならない。

３．５．４ ＩＤ及びパスワード等の管理

（１）ＩＣカード等の取扱い

① 職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

(ア)認証に用いるＩＣカード等を、職員等間で共有してはならない。

(イ)IC カード等を紛失することがないよう適切に管理しなければならない。

(ウ)ＩＣカード等を紛失した場合には、速やかに情報セキュリティ管理者に通報し、指示に従わなければならない。

② IC カード発行部署は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

③ IC カード発行部署は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２）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。

① 自己が利用しているＩＤは、他人に利用させてはならない。

② 共用 ID を利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（３）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。

① 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。

② 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。

③ 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。

④ パスワードが流出したおそれがある場合には、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しなければならない。

⑤ 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。

⑥ 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よう努めなければならない。

⑦ 仮のパスワード（初期パスワード含む。）は、最初のログイン時点で変更しなければならない。

⑧ 端末にパスワードを記憶させてはならない。

⑨ 職員等間でパスワードを共有してはならない（共有ＩＤに対するパスワードは除く。）。

３．６　技術的セキュリティ

３．６．１ コンピュータ及びネットワークの管理

（１）ファイルサーバの設定等

① 情報セキュリティ管理者は、ファイルサーバを課室等の単位で構成する。

② 情報セキュリティ管理者は、個人情報、人事記録等、特定の職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（2）バックアップの実施

① 情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

② 情報セキュリティ管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

（3）情報システム仕様書等の管理

情報セキュリティ管理者又は情報システム担当者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（4）ログの取得等

① 情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（5）障害記録

情報セキュリティ管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（6）ネットワークの接続制御、経路制御等

① 情報セキュリティ管理者は、フィルタリング及びルーティングについて、設定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しなければならない。

② 情報セキュリティ管理者は、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施さなければならない。

③ 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しなければならない。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さなければならない。

（7）外部ネットワークとの接続制限等

① 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、情報セキュリティ責任者の許可を得なければならない。

② 情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器

構成、セキュリティ技術等を詳細に調査し、法人内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ 情報システム管理者は、接続した外部ネットワークの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、情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（8）複合機のセキュリティ管理

① 情報セキュリティ管理者は、調達する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しなければならない。

② 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なければならない。

③ 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なければならない。

（9）特定用途機器のセキュリティ管理

情報セキュリティ管理者は、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しなければならない。

（１０） 無線ＬＡＮ及びネットワークの盗聴対策

① 情報セキュリティ管理者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

② 情報セキュリティ管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（１１） 電子メールのセキュリティ管理

① 情報セキュリティ管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② 情報セキュリティ管理者は、スパム（無差別かつ大量に一括送信される）メール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③ 情報セキュリティ管理者は、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不可能にしなければならない。

④ 情報セキュリティ管理者は、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しなければならない。

（１２） 電子メールの利用制限

① 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。

② 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、他の送信先の電子メールアドレスが分からないようにしなければならない。

③　職員等は、重要な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しなければならない。

（１３）　電子署名・暗号化

①　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、情報セキュリティ管理者が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

②　職員等は、暗号化を行う場合に情報セキュリティ管理者が定める以外の方法を用いてはならない。また、情報セキュリティ管理者が定めた方法で暗号のための鍵を管理しなければならない。

③　ＣＩＳＯは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（１４）　無許可ソフトウェアの導入等の禁止

①　職員等は、端末に無断でソフトウェアを導入してはならない。

②　職員等は、業務上の必要がある場合は、情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

③　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１５）　機器構成の変更の制限

①　職員等は、端末に対し機器の改造及び増設・交換を行ってはならない。

②　職員等は、業務上、端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティ管理者の許可を得なければならない。

（１６）　無許可でのネットワーク接続の禁止

職員等は、情報セキュリティ管理者の許可なく端末をネットワークに接続してはならない。

①　職員等は、業務以外の目的でウェブを閲覧してはならない

②　情報セキュリティ管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ責任者に報告し、適切な措置を求めなければならない。

（１７）　Ｗｅｂ会議利用時の対策

①　情報セキュリティ管理者は、Ｗｅｂ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。

②　職員等は、定められた利用手順に従い、Ｗｅｂ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しなければならない。

③　職員等は、Ｗｅｂ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じなければならない。

④　職員等は、外部からＷｅｂ会議に招待される場合は、定められた利用手順に従い、必要に応

じて利用申請を行い、承認を得なければならない。

（１８） ソーシャルメディアサービスの利用

① 情報セキュリティ管理者は、当授業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情報セキュリティ対策を行わなければならない。

② 当事業のアカウントによる情報発信が、実際の当事業のものであることを明らかにするために、当事業の自己管理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由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実施すること。

③ パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、ＵＳＢメモリ、紙等）等を適切に管理するなどの方法で、不正アクセス対策を実施すること。

④ 機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

⑤ 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なければならない。

⑥ 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なければならない。

３．６．２アクセス制御

(１)アクセス制御

① アクセス制御等

情報セキュリティ管理者は、所管するネットワーク又は情報システム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、システム上制限しなければならない。

② 利用者ＩＤの取扱い

(ア)情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

(イ)職員等は、業務上必要がなくなった利用者ＩＤは、利用者登録を抹消するよう、情報セキュリティ管理者及び情報システム担当者に通知しなければならない。

(ウ)情報セキュリティ管理者及び情報システム担当者は、利用されていないＩＤが放置されないよう、事務局と連携し、点検しなければならない。

(エ)情報セキュリティ管理者及び情報システム担当者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

(オ)特権を付与されたＩＤの管理等

③ 情報セキュリティ管理者及び情報システム担当者は、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のパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

④ 情報セキュリティ管理者及び情報システム担当者は、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なければならない。

⑤ 情報セキュリティ管理者は、特権を付与されたＩＤ及びパスワードについて、使用期間の制限等のセキュリティ機能を強化しなければならない。

⑥ 情報セキュリティ責任者は、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

（２）職員等による外部からのアクセス等の制限

① 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報セキュリティ管理者の許可を得なければならない。

② 情報セキュリティ管理者は、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しなければならない。

③ 情報セキュリティ管理者は、外部からのアクセスを認める場合、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なければならない。

④ 情報セキュリティ管理者は、外部からのアクセスに利用する端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑤ 職員等は、持ち込んだ又は外部から持ち帰った端末を事業内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑥ 情報セキュリティ管理者は、公衆通信回線（公衆無線ＬＡＮ等）を事業内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）認証情報の管理

① 情報セキュリティ管理者及び情報システム担当者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

３．６．３ システム開発、導入、保守等

（１）情報システムの調達

① 情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

① システム開発における責任者及び作業者の特定

情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

② システム開発における責任者、作業者のＩＤの管理

② 情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

③ 情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③ システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。

（イ）情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（３）情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

② 情報セキュリティ管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

③ 情報セキュリティ管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

④ 情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

⑤ 情報セキュリティ管理者は、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しなければならない。

⑥ テスト

⑦ 情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

⑧ 情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

⑨ 情報セキュリティ管理者は、個人情報及び機密性の高い データを、テストデータに使用してはならない。

⑩ 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（4）情報システムの基盤を管理又は制御するソフトウェア運用時の対策

情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

（5）システム開発・保守に関連する資料等の整備・保管

① 情報システム管理者は、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正に整備・保管しなければならない。

② 情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について情報セキュリティ責任者に報告しなければならない。

③ 情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

④ 情報セキュリティ管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（6）情報システムにおける入出力データの正確性の確保

① 情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② 情報セキュリティ管理者は、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しなければならない。

③ 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を見直ししなければならない。

④ 運用中のアプリケーション・コンテンツにおいて、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なければならない。

⑤ ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

⑥ 情報セキュリティ管理者は、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しなければならない。

（7）情報システムの変更管理

情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（8）開発・保守用のソフトウェアの更新等

情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（9）システム更新又は統合時の検証等

情報セキュリティ管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確

化及び更新・統合後の業務運営体制の検証を行わなければならない。

（１０） 情報システムについての対策の見直し

情報セキュリティ管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本市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見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、情報セキュリティ管理者へ報告しなければならない。

３．６．４不正プログラム対策

(１)情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、不正プログラム対策として、次の事項を措置しなければならない。

① 外部ネットワークから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、不正プログラムのシステムへの侵入を防止しなければならない。

② 外部ネットワークに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不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④ 所掌するサーバ及び端末に、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なければならない。

⑤ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦ 業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

⑧ 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、情報セキュリティ管理者が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。

(２)情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

① その所掌するサーバ及び端末に、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システムに常駐させなければならない。

② 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

③ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

④ インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するため、管理外のものを職員等に利用させてはならない。ま

た、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

（３）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

① 端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

② 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、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③ 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④ 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをＬGWAN接続系に取り込む場合は無害化処理を行わなければならない。

⑥ 情報セキュリティ管理者が提供するウイルス情報を、常に確認しなければならない。

⑦ コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、直ちに利用を中止し、ネットワークに接続できないようにしなければならない。

（４）セキュリティアドバイザー等の支援体制

ＣＩＳＯは、実施している対策では対応できない事態が発生した場合に備え、専門的知識を有するセキュリティアドバイザー等の支援を受けられるようにしておかなければならない。

３．６．５不正アクセス対策

（１）情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

使用されていないポートを閉鎖しなければならない。

① 不要なサービスについて、機能を削除又は停止しなければならない。

② 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、情報セキュリティ管理者及び情報システム担当者へ通報するよう、設定しなければな

③ らない。

④ 情報セキュリティ管理者は、ＣＳＩＲＴと連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2）攻撃への対処

ＣＩＳＯは、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（3）記録の保存

ＣＩＳＯは、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃

情報セキュリティ管理者は、職員等及び委託事業者が使用している端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）職員等による不正アクセス

情報セキュリティ管理者及び情報システム担当者は、職員等による不正アクセスを発見した場合は、当該職員等の所属長に通知し、適切な処置を求めなければならない。

（6）サービス不能攻撃

情報セキュリティ管理者は、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なければならない。

（7）標的型攻撃

情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、職員等に対する教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

３．６．６セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

情報セキュリティ管理者及び情報システム担当者は、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（3）情報セキュリティに関する情報の収集及び共有

情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共

有しなければならない。また、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、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

３．７　運用

３．７．１情報システムの監視

（１）情報システムの運用・保守時の対策

① 情報セキュリティ管理者は、情報システムの運用・保守において、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しなければならない。

② 情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

③ 情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない

（２）情報システムの監視機能

① 情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

② 情報セキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

（３）情報システムの監視

① 情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 情報セキュリティ管理者は、重要なログ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なければならない。

３．７．２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

① 情報セキュリティ管理者は、所管する課室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確認を行い、問題を認めた場合には、速やかにＣＩＳＯに報告しなければならない。

② ＣＩＳＯ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。

③ 情報セキュリティ管理者及び情報システム担当者は、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には適切かつ速やかに対処しなければならない。

（２）端末及び電磁的記録媒体等の利用状況調査

ＣＩＳＯ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

る端末及び電磁的記録媒体等のログ、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

① 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、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。

② 違反行為が重大な影響を及ぼす可能性があるとＣＩＳＯが判断した場合、情報セキュリティ責任者の指示のもと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。

３．７．３侵害時の対応等

（１）緊急時対応計画の策定

ＣＩＳＯは、情報セキュリティインシデント、情報セキュリティポリシーの違反等により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、あらかじめ緊急時対応計画を定め、セキュリティ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、以下の内容を定めなければならない。

① 関係者の連絡先

② 生した事案に係る報告すべき事項

③ 発生した事案への対応措置

④ 再発防止措置の策定

（３）業務継続計画との整合性確保

ＣＩＳＯは、自然災害、大規模・広範囲にわたる疾病等に備えて情報システム部門の業務継続計画と情報セキュリティポリシーの整合性を確保するものとする。

（４）緊急時対応計画の見直し

ＣＩＳＯ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。

３．７．４例外措置

（１）例外措置の許可

情報セキュリティ管理者は、情報セキュリティに関する規定を遵守することが困難な状況で、行政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には、ＣＩＳＯ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者は、行政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ＣＩＳＯに報告しなければならない。

（３）例外措置の申請書の管理

ＣＩＳＯは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

３．７．５ 法令遵守

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に、次の法令のほか関係法令を遵守し、これに従わなければならない。

- 地方公務員法（昭和 25 年法律第 261 号）
- 著作権法（昭和 45 年法律第 48 号）
- 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）
- 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
- サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- 一関市個人情報の保護等に関する条例（令和５年条例第２号）
- 一関市個人情報の保護に関する法律等施行規則（令和５年規則第 23 号）
- 一関市個人情報等保護管理規程（令和５年訓令第１号）

３．７．６ 懲戒処分等

（１）懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

（２）違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

① 情報システム担当者が違反を確認した場合、情報セキュリティ責任者及び情報セキュリティ管理者に報告し、情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

② 情報セキュリティ管理者等が違反を確認した場合、違反を確認した者は速やかに情報セキュリティ責任者に報告し、適切な措置を求めなければならない。

③ 情報セキュリティ管理者の指導によっても改善されない場合、情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、その旨をＣＩＳＯに報告しなければならない。

３．８　業務委託と外部サービス（クラウドサービス）の利用

３．８．１業務委託

（１）業務委託に係る運用規程の整備

情報セキュリティ管理者は、業務委託に係る以下の内容を示さなければならない。

① 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

② 委託事業者の選定基準

（２）業務委託実施前の対策

① 情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

② 委託する業務内容の特定

③ 委託事業者の選定条件を含む仕様の策定

④ 仕様に基づく委託事業者の選定

⑤ 情報セキュリティ要件を明記した契約の締結（契約項目）

⑥ 情報システムの運用、保守等の重要な情報資産を取扱う業務を委託する場合には、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等に係る要件を明記した契約を締結しなければならない。

- 情報セキュリティポリシー等の遵守
- 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
- 提供されるサービスレベルの保証
- 委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
- 委託事業者の従業員に対する教育の実施
- 提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
- 業務上知り得た情報の守秘義務
- 再委託に関する制限事項の遵守
- 委託業務終了時の情報資産の返還、廃棄等
- 委託業務の定期報告及び緊急時報告義務
- 当事業による監査、検査
- 当事業による情報セキュリティインシデント発生時の公表
- 情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

⑦ 委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

（３）確認・措置等

情報セキュリティ管理者は、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、①の契約に基づき措置を実施しなければならない。

３．８．２情報システムに関する業務委託

（１）情報システムに関する業務委託における共通的対策

情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、情報システムに当事業の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

（２）情報システムの構築を業務委託する場合の対策

情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

① 情報システムのセキュリティ要件の適切な実装

② 情報システムの開発環境及び開発工程における情報セキュリティ対策

（３）情報システムの運用・保守を業務委託する場合の対策

① 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

② 情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

３．８．３外部サービス（クラウドサービス）の利用

外部サービス（クラウドサービス等）を利用する際は、以下の基準を満たし、情報セキュリティ責任者の承認を得たものに限定する。

（１）選定基準（セキュリティ要件）

情報セキュリティ責任者は、外部サービスの選定にあたり、以下の事項を評価し、一定のセキュリティ水準を満たしていることを確認するものとする。

① 情報セキュリティに係る国際規格（ISO/IEC 27001 及び ISO/IEC 27017）またはそれと同等以上のセキュリティ水準が講じられていること。

② サービス提供事業者における情報の管理体制、監査体制及び経営状態が適正であること。

③ データの保存場所、通信の暗号化、バックアップの実施状況が明確であること。

（２）遵守事項

外部サービスを利用する者は、次に掲げる事項を遵守しなければならない。

① サービスごとに管理責任者を定め、利用者のアカウント（ID・パスワード等）を厳重に管理すること。

② 退職等により利用権限を失った者のアカウントは、直ちに抹消すること。

③ 指定された重要情報（個人情報、人事評価等）については、必要最小限のアクセス権限に制限し、多要素認証等の安全な認証機能を利用すること。

（3）継続評価

情報セキュリティ責任者は、利用中の外部サービスについて、前述の要件が継続して維持されているか定期的に点検を行い、必要に応じて改善の指示又は利用の中止を行うものとする。

3.9　評価・見直し

3.9.1 監査

（1）実施方法

ＣＩＳＯは、情報セキュリティ監査統括責任者を指名し、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、毎年度及び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

① 監査を行う者は、客観性を確保するため、被監査部門（システム管理担当）から独立した立場の者または外部の専門家とする。

② 監査を行う者は、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でなければならない。

（3）外部委託先の確認

業務を委託している事業者（クラウドサービス事業者等）に対しては、セキュリティ対策の履行状況を定期的に確認する。なお、外部認証（ISO/IEC 27001 等）の取得確認や、事業者からの報告書の受領をもって確認に代えることができる。

（4）報告及び改善指示

① 監査を行った者は、その結果を速やかにＣＩＳＯに報告しなければならない。

② ＣＩＳＯは、監査結果に基づき改善が必要と認められた場合、関係する情報セキュリティ管理者に対して、是正及び改善を指示するものとする。

（5）ポリシーの見直しへの活用

ＣＩＳＯは、監査結果を情報セキュリティポリシー及び関係規定等の見直し、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。

3.9.2 自己点検

（1）実施方法

① 情報セキュリティ管理者は、情報セキュリティ管理者に対し、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するよう通知しなければならない。

② 情報セキュリティ管理者は、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、①の通知に基づき、自己点検を行わなければならない。

（2）報告

情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を情報セキュリティ管理者へ報告しなければならない。

（3）自己点検結果の活用

① 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。

② ＣＩＳＯは、こ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時に活用しなければならない。

３．９．３情報セキュリティポリシー及び関係規程等の見直し

ＣＩＳＯは、情報セキュリティ監査及び自己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を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、改善を行うものとする。