地方独立行政法人徳島県鳴門病院
情報セキュリティポリシー

令和６年２月　策　定

（目次）

第１章　情報セキュリティ基本方針

1. 目的

情報セキュリティ基本方針は、地方独立行政法人徳島県鳴門病院（以下、法人）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、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

（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、その構成機器（ハードウェア及びソフトウェア）をいう。

（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。

（8）HIS 接続系（総合医療情報システム系）
電子カルテや部門システム等に接続された情報システム及びその情報システムで取り扱うデータをいう。

（9）イントラ接続系
イントラ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) インターネット接続系
ＨＩＳ接続系及びイントラネット接続系を除く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り扱うデータをいう。

(11) 通信経路の分割
ＨＩＳ接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が

確保された通信だけを許可できるようにすることをいう。

(12) 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。

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使用等の規定違反、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

4. 適 用 範 囲

（1）適用組織：

徳島県鳴門病院および徳島県鳴門病院附属看護専門学校の各部署とする。

（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ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5. 職員等の遵守義務

職員及び嘱託職員等（以下「職員等」という。）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。

6. 情報セキュリティ対策

上記３の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

法人の情報資産について、情報セキュリティ対策を推進する法人全体の組織体制を確立す

る。

（2）情報資産の分類と管理

法人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実施する。

（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。

①ＨＩＳ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や端末への多要素認証の導入等により、患者情報の流出を防ぐ。

②イントラ接続系においては、イントラと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、情報セキュリティ対策を実施する。

③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、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（5）人的セキュリティ

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

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7）運 用

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、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正に対応するため、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。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディア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。

（9）評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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。

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になった場合には、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記６、７及び８に規定する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。（本書第２章）

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ものとする。

なお、情報セキュリティ実施手順は、公にすることにより法人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２章　情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針を実行に移すための、法人における情報資産に関する情報セキュリティ対策の基準を定めたものである。

1. 組織体制

	名称	対象者（充職）	主な役割
(1)	最高情報セキュリティ責任者（CISO）	理事長	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	院長	CISOの補佐/欠員時の代理/（3）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	各所属長	セキュリティ侵害発生時の（2）（8）及び（1）への報告
(4)	情報システム管理者	院長（あるいは病院長が指名した者）	情報システム開発/変更/運用等の権限及び責任
(5)	情報システム運用責任者/医療情報システム安全管理責任者	情報システム課長	情報システム開発/変更/運用等の管理
(6)	情報システム担当者	情報システム課担当者	情報システム開発/設定/変更/運用等の作業
(7)	職員等	全職員	ポリシー及び実施手順を遵守
(8)	（窓口担当）	情報システム課	セキュリティ侵害発生時の窓口

（１）最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

①法人に最高情報セキュリティ責任者（CISO）を置き、理事長をもって充てる。

②CISO は、法人における全て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。

③CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

（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、院長をもって充てる。

②情報セキュリティ責任者は CISO を補佐し、CISO に事故があるとき、又は CISO が欠けたときはその職務を代理する。

③情報セキュリティ責任者は、法人の全ての情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する。

④情報セキュリティ責任者は、情報セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤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、情報システム運用責任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。

⑥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。

⑦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 CISO にその内容を報告しなければならない。

（3）情報セキュリティ管理者

①各所属長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する部署の情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、その所掌する部署において、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担当窓口へ速やかに報告を行い、指示を仰がなければならない。

（4）情報システム管理者

①情報システム管理者を置き、病院長あるいは病院長が指名した者を充てる。

②情報システム管理者は、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、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権限及び責任を有する。

（5）情報システム運用責任者

①情報システムに関する運用を担当する責任者を置き、情報システム管理者が指名する。

②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恐れがある場合には、緊急時対応計画で定める CSIRT の窓口及び情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

（6）情報システム担当者

情報システム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、更新等の作業業を行う者を情報システム担当者とする。

（7）職員等

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向けに定

められている事項を遵守する。

（8）担当窓口

情報セキュリティに関する情報を一元化するため、情報システム課に窓口担当を置く。

（9）兼務の禁止

①情報セキュリティ対策の実施において、止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情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(10) CSIRT の設置・役割

CISO は、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下、「情報セキュリティインシデント」という。）に対処するための体制（CSIRT　シーサート：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、別に定める緊急時対応計画の中で役割を明確化しなければならない。

2. 情報資産の分類と管理

（1）情報資産の分類

法人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。

機密性による情報資産の分類

分類	分類基準	主な取扱制限
機密性３	・個人情報（行政手続き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第２条第８項で定める特定個人情報を含む。） ・法人の事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・法人支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・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
機密性２	・不開示情報のうち個人情報を除くもの ・法人の事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに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	－

完全性による情報資産の分類

分類	分類基準	主な取扱制限
完全性２	法人の事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、患者等の権利が侵害される又は法人内部の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	・情報資産のバックアップ ・外部で情報処理を行う際の安全管理措置の徹底 ・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の情報資産以外の情報資産	－

可用性による情報資産の分類

分類	分類基準	主な取扱制限
可用性２	法人の事務で取り扱う情報資産のうち、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、患者等の権利が侵害される又は法人の事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	・情報資産のバックアップ ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	－

（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。

（ウ）情報セキュリティ管理者は、その保有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。

（エ）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、各業務の実態に合わせて、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。

（オ）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。

（カ）情報セキュリティ管理者は、分類に応じて、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。

（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。

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）法人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）法人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）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、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）職員等は、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又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）情報セキュリティ管理者又は情報システム管理者は、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又は情報システム管理者は、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

電子メール等により情報を送信する者は、必要に応じ、パスワード等による暗号化またはパスワード設定を行わなければならない。

⑧情報資産の運搬

（ア）車両等により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、パスワード等による暗号化を行う等、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）情報資産を外部に提供する者は、必要に応じパスワード等による暗号化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）情報セキュリティ管理者は、情報資産を外部に利用させ、提供するときは、別に定める手続きによらなければならない。

⑩情報資産の廃棄等

（ア）情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、必要に応じて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）情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（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）情報セキュリティ管理者は、電磁的記録媒体の消去又は記録装置の破砕を外部の者に依頼する場合は、記録の消去に係る確認書の提出を受けなければならない。

3. 情報システム全体の強靭性の向上

（１）HIS 接続系(総合医療情報システム系)

① HIS 接続系と他の領域との分離

HIS 接続系と他の領域を通信できないようにしなければならない。HIS 利用系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、十分に安全性が確保された外部接続先の場合はその限りではない。

② 情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、設定可能な端末に対しては、二つ以上を併用する認証(多要素認証)を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

（イ）情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

（２）イントラ接続系

イントラ接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをイントラ接続系に

取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

① インターネット環境で受信したインターネットメールの本文のみをイントラ接続系に転送するメールテキスト化方式

② インターネット接続系の端末から、イントラ接続系の端末へ画面を転送する方式

③ 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3)インターネット接続系

① インターネット接続系においては、可能な限り、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びイントラ接続系への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

② 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産をイントラ接続系に配置する場合、又はインターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合は、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

4. 物理的セキュリティ対策

4.1. サーバ等の管理

(1)機器の取付け

情報システム運用責任者は、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正に固定する等、必要な措置を講じなければならない。また、パソコン等の機器を設置する場合、ディスプレイに表示される情報が他者から覗き見されないような措置を講じなければならない。

(2)機器の電源

① 情報システム運用責任者は、施設管理部門と連携し、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、当該機器が適正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 情報システム運用責任者は、施設管理部門と連携し、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。

(3)通信ケーブル等の配線

① 情報システム運用責任者は、施設管理部門と連携し、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 情報システム運用責任者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③ 情報システム運用責任者は、ネットワーク接続口(ハブのポート等)を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④ 情報システム運用責任者は、自ら又は情報システム担当者及び契約により操作を認められた外部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講じなければならない。

(4)機器の定期保守及び修理

① 情報システム運用責任者は、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 情報システム運用責任者は、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システム運用責任者は、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等を行わなければならない。

(5)法人の施設外への機器の設置

情報システム運用責任者は、法人の施設外に業務システムの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。

(6)機器の廃棄等

情報システム運用責任者は、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。

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 情報システム運用責任者は、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。

③ 情報システム運用責任者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

④ 情報システム運用責任者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

(2)管理区域の入退室管理等

① 情報システム運用責任者は、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や入退室管理簿の記載による入退室管理を行わなければな

らない。

② 職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③ 情報システム運用責任者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち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なければならない。

④ 情報システム運用責任者は、情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

(3)機器等の搬入出

① 情報システム運用責任者は、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 情報システム運用責任者は、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。

4.3. 通信回線及び通信回線装置の管理

(1)情報システム運用責任者は、法人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、適正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)情報システム運用責任者は、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)情報システム運用責任者は、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)情報システム運用責任者は、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)情報システム運用責任者は、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。

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

(1)情報システム運用責任者は、盗難防止のため、利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。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)情報システム運用責任者は、情報システムへのログインに際し、設定可能な機器に対して

パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

4.5. 取扱区域の管理

(1)情報システム運用責任者は、取扱区域における情報資産の盗難又は紛失等を防止しなければならない。

(2)情報システム運用責任者は、外部からの訪問者が取扱区域に入る場合には、必要に応じて職員が付き添うなど、担当者以外のものが容易に閲覧等できないようにしなければならない。

5. 人的セキュリティ対策

5.1. 職員等の遵守事項

(1) 職員等の遵守事項

①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相談し、指示を仰がなければならない。

②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。

③パソコン、モバイル端末及び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

(ア) 情報資産を外部で処理する場合は法人内における対策基準に加え、安全管理のための必要な措置を確認したうえで、実施手順を定めなければならない。

(イ) 職員等は、法人のパソコン、モバイル端末、電磁的記録媒体、情報資産及びソフトウエ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。

(ウ) 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。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア)職員等は、支給以外のパソコン、モバイル端末を原則業務に利用してはならない。

(イ)職員等は、支給以外のパソコン、モバイル端末を業務に利用する場合は、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に関する規定を遵守しなければならない。

(ウ)職員等は、支給以外の電磁的記録媒体を原則業務に利用してはならない。また、利用する USB メモリは、原則、パスワード認証等の暗号化機能付きのものとしなければな

らない。

⑤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。

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウエアに関するセキュリティ機能の設定をシステム管理部門又は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。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、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、離席時のパソコン、モバイル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、適正な措置を講じなければならない。

⑧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。

(２)嘱託職員及び非常勤職員への対応

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、嘱託職員及び非常勤職員に対し、採用時に情報セキュリティポリシー等のうち、嘱託職員及び非常勤職員が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、 嘱託職員及び非常勤職員にパソコンやモバイル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。

(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及び実施手順を閲覧できるように掲示しなければならない。

(４)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・保守並びにその他情報資産に関する業務等を事業者に発注する場合、再委託事業者も含めて、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。

5.2. 研修・訓練

(１)情報セキュリティに関する研修

CISO 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

①CISO は、管理者を含め全ての職員等に対する情報セキュリティに関する研修計画を策定しなければならない。

②研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

（３）緊急時対応訓練

CISO は、緊急時対応を想定して訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システム規模等を考慮し、訓練実施の体制、範囲等を定め、また、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

全ての職員等は、定められた研修・訓練に参加しなければならない。

5.3. 情報セキュリティインシデントの報告

（１）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及び情報セキュリティに関する窓口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 CISO に及び情報システム管理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、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 及び情報セキュリティ責任者に報告しなければならない。

（２)情報セキュリティインシデント原因の究明・記録、再発防止等

①CSIRT 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。

②CSIRT 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。

③CSIRT 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。

④CSIRT 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。

⑤CISO 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。

5.4. 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。

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。

(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。

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

⑥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。

⑦サーバ、 ネットワーク機器及び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。

⑧職員等間でパスワードを共有してはならない(ただし共有 ID に対するパスワードは除く)

6. 技術的セキュリティ対策

6.1. 情報システム全体の強靭性の向上

複雑・巧妙化しているサイバー攻撃の脅威により、法人の業務に重大な影響をあたるリスクが想定されるため、機密性、可用性、完全性の確保に十分配慮した攻撃に強い情報システムにしなければならない。

6.2. コンピュータ及びネットワークの管理

(１)文書サーバの設定等

①情報システム運用責任者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

②情報システム運用責任者は、文書サーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③情報システム運用責任者は、患者の個人情報、人事記録等、特定の職員等しか取り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、同一課等であっても、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

情報システム運用管理者は、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。

(3)システム管理記録及び作業の確認

①情報システム運用責任者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②情報システム運用責任者は、所管する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

③情報システム運用責任者は、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がシステム変更等の作業を行う場合は、2 名以上で作業し、互いにその作業を確認しなければならない

(4)情報システム仕様書等の管理

情報システム運用責任者は、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の閲覧や、紛失等がないよう、適正に管理しなければならない。

(5)ログの取得等

①情報システム運用責任者は、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情報システム運用管理者は、ログとして取得する項目、保存期間、取扱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、適正にログを管理しなければならない。

③情報システム運用責任者は、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。

(6)障害記録

情報システム運用責任者は、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、適正に保存しなければならない。

(7)ネットワークの接続制御、経路制御等

①情報システム運用責任者は、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情報システム運用責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

(8)外部の者が利用できるシステムの分離等

情報システム運用責任者は、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(9)外部ネットワークとの接続制限等

①情報システム運用責任者は、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情報システム運用責任者は、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情報システム運用責任者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④情報システム運用責任者は、ウェブサーバ等をインターネットに公開する場合、法人内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しなければならない。

⑤情報システム運用責任者は、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。

(10)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、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、適正なセキュリティ対策を講じなければならない。

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正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。

(11) IoT 機器を含む特定用途機器のセキュリティ管理

情報システム運用責任者は、特定用途機器(ネットワークカメラシステム等の通信又は電磁的記録媒体を内蔵する機器)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講じなければならない。

(12)無線 LAN の盗聴対策

①情報システム運用責任者は、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情報システム運用責任者は、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。

(13)電子メールのセキュリティ管理

①情報システム運用責任者は、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情報システム運用責任者は、大量のスパム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情報システム運用責任者は、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情報システム運用責任者は、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。

⑤情報システム運用責任者は、システム開発や運用、保守等のため法人施設内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

(14)電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②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。

③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。

④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。

(15)電子署名・暗号化

①職員等は、情報資産の分類に応じて、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、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て、送信しなければならない。

②情報システム運用責任者は、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。

(16)無許可ソフトウエアの導入等の禁止

①職員等は、パソコンやモバイル端末に無断でソフトウエ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、情報資産を管理している情報システム運用責任者者の許可を得て、ソフトウエアを導入することができる。なお、導入する際は、情報システム運用責任者は、ソフトウェアのライセンスを適切に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エアを利用してはならない。

(17) 機器構成の変更の制限

①職員等は、パソコンやモバイル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、パソコンやモバイル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、情報資産を管理している情報システム運用責任者の許可を得なければならない。

(18)業務外ネットワークへの接続の禁止

①職員等は、支給された端末(各所属で調達した端末を含む)を、有線・無線を問わず、その端末を接続して利用するよう情報システム運用責任者によって定められたネッ

トワークと異なるネットワークに接続してはならない。

②情報システム運用責任者は、支給した端末について、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(19)業務以外の目的での Web 閲覧の禁止

①職員等は、業務以外の目的で Web を閲覧してはならない。

②情報システム運用責任者は、職員等の Web 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、所属長に通知し適正な措置を求めなければならない。

(20) Web 会議サービスの利用時の対策

①情報システム運用責任者は、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、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。

(21)ソーシャルメディアサービスの利用

①所属長は、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、次の情報セキュリティ対策を行わなければならない。

（ア）法人のアカウントによる情報発信が、実際の法人のものであることを明らかにするために、法人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。

（イ)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)等を適正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。

②機密性 3 又は機密性 2 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。

③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。

④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。

6.3. アクセス制御

(1)アクセス制御等

①アクセス制御

情報セキュリティ責任者及び情報システム運用責任者は、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、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）情報セキュリティ責任者及び情報システム運用責任者は、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場合は、利用者登録を抹消するよう、情報システム運用責任者に通知しなければならない。

（ウ）情報セキュリティ責任者及び情報システム運用責任者は、利用されていない ID が放置されないよう、点検しなければならない。

③特権を付与された ID の管理等

(ア)情報セキュリティ責任者及び情報システム運用責任者は、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。

(イ)情報セキュリティ責任者及び情報システム運用責任者の特権を代行する者は、情報セキュリティ責任者又は情報システム運用責任者が認めた者でなければならない。

(ウ)情報セキュリティ責任者及び情報システム運用責任者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

(エ)情報セキュリティ責任者及び情報システム運用責任者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

(オ)情報セキュリティ責任者及び情報システム運用責任者は、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、情報システム運用責任者の許可を得なければならない。

②情報システム運用責任者は、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情報システム運用責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④情報システム運用責任者は、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。

⑤情報システム運用責任者は、外部からのアクセスに利用するモバイル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。

⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を法人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。

⑦情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。

（３）ログイン時の表示等

情報システム運用責任者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、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ようシステムを設定しなければならない。

（４）認証情報の管理

①情報セキュリティ責任者及び情報システム運用責任者は、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。

②情報セキュリティ責任者及び情報システム運用責任者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③情報セキュリティ責任者及び情報システム運用責任者は、認証情報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。

（５）特権による接続時間の制限

情報システム運用責任者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

6.4. システム開発、導入、保守等

(１)情報システムの調達

①情報セキュリティ責任者及び情報システム運用責任者は、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情報セキュリティ責任者及び情報システム運用責任者は、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

情報システム運用責任者は、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方針手順等を決定し、開発に適用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

(ア)情報システム運用責任者は、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。

(イ)情報システム運用責任者は、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）情報システム運用責任者は、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なければならない。

(イ) 情報システム運用責任者は、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

(ア)情報システム運用責任者は、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。

(イ)情報システム運用責任者は、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。

(ウ)情報システム運用責任者は、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。

(エ)情報システム運用責任者は、所管する情報システムの保守及び点検を定期的に実施しなければならない。

②テスト

(ア)情報システム運用責任者は、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。

(イ)情報システム運用責任者は、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。

(ウ)情報システム運用責任者は、個人情報及び機密性の高い生データを、テストデータに原則使用してはならない。

(エ)情報システム運用責任者は、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)システム開発・保守に関連する資料等の整備・保管

①情報システム運用責任者は、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情報システム運用責任者は、テスト結果を一定期間保管しなければならない。

③情報システム運用責任者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

(5)情報システムにおける入出力データの正確性の確保

①情報システム運用責任者は、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情報システム運用責任者は、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、これを防止することができるように情報システムを設計しなければならない。

③情報システム運用責任者は、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。

(6)情報システムの変更管理

情報システム運用責任者は、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。

(7)開発・保守用のソフトウェアの更新等

情報システム運用責任者は、開発・保守用のソフトウエ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。

(8)システム更新又は統合時の検証等

情報システム運用責任者は、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。

6.5. 不正プログラム対策

(1)システム管理部門の措置事項

情報システム運用責任者は、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パソコン等の端末に、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ァ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原則利用してはならない。

(2)情報システム運用責任者の措置事項

情報システム運用責任者は、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情報システム運用責任者は、その所掌するサーバ及びパソコン等の端末に、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に、法人が管理している媒体以外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。

⑤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、情報システム運用責任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。

(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パソコンやモバイル端末において、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送受信した場合は、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エ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イントラ接続系に取り込む場合は無害化しなければならない。

⑥情報システム運用責任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、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

(4)専門家の支援体制

情報システム運用責任者は、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しておかなければならない。

6.6. 不正アクセス対策

(1)情報セキュリティ責任者及び情報システム運用責任者の措置事項

情報セキュリティ責任者及び情報システム運用責任者は、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。

①使用されていないポートを閉鎖しなければならない。

②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。

③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、

情報セキュリティ責任者及び情報システム運用責任者へ通報するよう、設定しなければならない。

④情報セキュリティ責任者及び情報システム運用責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正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 及び情報セキュリティ責任者は、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、総務省、都道府県等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 及び情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法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

情報セキュリティ責任者及び情報システム運用責任者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの院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

情報セキュリティ責任者及び情報システム運用責任者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(6)サービス不能攻撃

情報セキュリティ責任者及び情報システム運用責任者は、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

情報セキュリティ責任者及び情報システム運用責任者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策(入口対策)や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策(内部対策及び出口対策)を講じなければならない。

6.7. 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

情報セキュリティ責任者及び情報システム運用責任者は、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

情報セキュリティ責任者及び情報システム運用責任者は、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

情報セキュリティ責任者及び情報システム運用責任者は、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。

7. 運用

7.1. 情報システムの監視

(1)情報セキュリティ責任者及び情報システム運用責任者は、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)情報セキュリティ責任者及び情報システム運用管理者は、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)情報セキュリティ責任者及び情報システム運用管理者は、外部と常時接続するシステムを常時監視しなければならない。

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情報セキュリティ責任者及び情報システム運用責任者は、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、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。

②CISO は、発生した問題について、適正かつ速やかに対処しなければならない。

③情報セキュリティ責任者及び情報システム運用責任者は、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正かつ速やかに対処しなければならない。

(2)パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及び 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パソコン、モバイル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、直ちに情報セキュリティ責任者に報告を行わなければならない。

②当該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管理者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処

しなければならない。

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、緊急時対応計画を定めておき、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発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

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、CISO は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

(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を見直さなければならない。

7.4. 例外措置

(1)例外措置の許可

情報セキュリティ責任者及び情報システム運用管理者は、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、法人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する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、例外措置を講じることができる。

(2)緊急時の例外措置

情報セキュリティ責任者及び情報システム運用管理者は、法人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。

7.5. 法令遵守

(1)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。

①著作権法(昭和４５年法律第４８号)

②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)

③個人情報の保護に関する法律(平成 15 年法律第５７号)

④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)

⑤サイバーセキュリティ基本法(平成２６年法律第１０４号)

⑥地方独立行政法人法(平成 15 年法律第 118 号)

(２)マイナンバーガイドライン

マイナンバーを扱う個人番号利用事務及び個人番号関係事務は、個人情報保護委員会が定める「特定個人情報の適正な取扱いに関するガイドライン」を遵守しなければならない。

7.6. 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情報セキュリティ責任者が違反を確認した場合は、情報セキュリティ責任者は当該職員等の所属長に通知し、適正な措置を求めなければならない。

②情報システム運用責任者等が違反を確認した場合は、違反を確認した者は速やかに当該職員等が所属する情報セキュリティ責任者に通知し、適正な措置を求めなければならない。

③情報セキュリティ責任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、情報セキュリティ責任者が、職員等の権利を停止あるいは剥奪した旨を CISO に通知しなければならない。

8. 業務委託と外部サービスの利用

8.1. 業務委託

(１)委託事業者の選定基準

情報セキュリティ管理者は、委託事業者の選定にあたり、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。

(２)契約項目

情報システムの運用、保守等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要件を明記した契約(契約書、覚書等)を締結しなければならない。

①情報セキュリティポリシー等の遵守

②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

③提供されるサービスレベルの保証
④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
⑤委託事業者の従業員に対する教育の実施
⑥提供された情報の目的外利用及び受託者以外の者への提供の禁止
⑦業務上知り得た情報の守秘義務
⑧再委託に関する制限事項の遵守
⑨委託事業者のデータの保管に関する事項
⑩データの複写及び複製の禁止に関する事項
⑪データの授受及び搬送に関する事項
⑫委託業務終了時の情報資産の返還、廃棄等
⑬委託業務の定期報告及び緊急時報告義務
⑬法人による監査、検査
⑭法人による情報セキュリティインシデント発生時の公表
⑮特定個人情報を取り扱う従事者の明確化に関する事項
⑯漏えい事案等が発生した場合の委託先の責任に関する事項
⑰その他データの保護に関し必要な事項
⑱ 前記各事項の定めに違反した場合における契約解除等の措置及び損害賠償に関する事項

(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、(2)の契約に基づき措置を実施しなければならない。また、その内容を情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

(1)外部サービスの利用に係る規定の整備

情報セキュリティ責任者及び情報システム運用責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する基準等を設けること。

①外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 8.2 節において「外部サービス利用判断基準」という。）
②外部サービス提供者の選定基準
③外部サービスの利用申請の許可権限者と利用手続
④外部サービス管理者の指名と外部サービスの利用状況の管理

(2)外部サービスの選定

①情報セキュリティ責任者及び情報システム運用責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。
②情報セキュリティ責任者及び情報システム運用責任者は、外部サービスで取り扱う情報の

格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

（ア）外部サービスの利用を通じて法人が取り扱う情報の外部サービス提供者における目的外利用の禁止

（イ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

（ウ）外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、法人の意図しない変更が加えられないための管理体制

（エ）外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

④情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの利用を通じて法人が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて法人の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

⑥情報セキュリティ責任者及び情報システム運用責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を法人に提供し、法人の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

⑧情報セキュリティ責任者及び情報システム運用責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

（3）外部サービスの利用に係る調達・契約

①情報セキュリティ責任者及び情報システム運用責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

②情報セキュリティ責任者及び情報システム運用責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

（4）外部サービスの利用承認

①情報セキュリティ責任者及び情報システム運用責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

（5）外部サービスを利用した情報システムの導入・構築時の対策

①情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を講ずること。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

②外部サービス管理者及び情報システム運用責任者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

（6）外部サービスを利用した情報システムの運用・保守時の対策

①情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を講ずること。

（ア）外部サービス利用方針の規定

（イ）外部サービス利用に必要な教育

（ウ）取り扱う資産の管理

（エ）不正アクセスを防止するためのアクセス制御

（オ）取り扱う情報の機密性保護のための暗号化

（カ）外部サービス内の通信の制御

（キ）設計・設定時の誤りの防止

（ク）外部サービスを利用した情報システムの事業継続

②情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

③外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

（7）外部サービスを利用した情報システムの更改・廃棄時の対策

①情報セキュリティ責任者及び情報システム運用責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を講じること。

（ア）外部サービスの利用終了時における対策

（イ）外部サービスで取り扱った情報の廃棄

（ウ）外部サービスの利用のために作成したアカウントの廃棄

②外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

8.3. 外部サービスの利用（機密性２以上の情報を取り扱わない場合）

（1）外部サービスの利用に係る規定の整備

情報セキュリティ責任者及び情報システム運用責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する基準等を設けること。

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの利用申請の許可権限者と利用手続

（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）外部サービスの利用の運用手順

（2）外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性２以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

②情報セキュリティ責任者及び情報システム運用責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

9 評価・見直し(監査、自己点検)

9.1. 監査

(1)実施方法

情報セキュリティ責任者は、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

①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、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

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)監査実施計画の立案及び実施への協力

①情報セキュリティ監査責任者は、監査を行うに当たって、監査実施計画を立案し、CISO の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

(4)委託事業者に対する監査

事業者に業務委託を行っている場合、情報セキュリティ監査責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

(5)監査の委託

情報セキュリティに関する監査は、外部の専門家を監査人として実施することができる。この場合において、客観的で公平な手続きに従って調達を行い、かつ、当該監査委託先は、監査対象と直接利害関係がないこととする。

(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、情報セキュリティ責任者及び CISO 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、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正に保管しなければならない。

(7)監査結果への対応

CISO 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、当該事項への対処を指示しなければならない。また、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なければならない。なお、法人内で横断的に改善が必要な事項については、情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

(8)情報セキュリティポリシー及び関係規程等の見直し等への活用

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。

9.2. 自己点検

(１)実施方法

①情報システム管理者及び情報システム運用責任者は、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。

②情報セキュリティ管理者及び情報システム運用責任者は、所管する部署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)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。

②CISO は、この点検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

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。