地方独立行政法人堺市立病院機構

情報セキュリティポリシー

【第１版】

施行日：令和８年２月２７日

はじめに

1.　概要

地方独立行政法人堺市立病院機構（以下「法人」という。）における情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定め、「基本方針」、「対策基準」の２階層で構成される。

なお、情報セキュリティポリシーに基づき作成される「実施手順」については、個別具体的なシステム、手順、手続等に応じて別途定めることとする。なお、「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恐れがあることから、原則、非公開とする。

2.　法人における情報セキュリティポリシーの維持

情報セキュリティポリシー及び実施手順の運用の維持にあたり、法人は、必要な人員、予算、教育等の支援を行うとともに、情報セキュリティ対策を実施するための組織・体制を整備し、以下に掲げる国のガイドライン等の最新情報と齟齬がないように適宜見直しを行うこととする。

（１）地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）

※法人は地方公共団体にはあたらないが、公的機関として本ガイドラインに準拠する形で情報セキュリティポリシーを作成する。

（２）医療情報システムの安全管理に関するガイドライン（厚生労働省）

（３）医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（経済産業省・総務省）

（４）医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（個人情報保護委員会／厚生労働省）

第１章　情報セキュリティ基本方針

1.　基本的な考え方

情報セキュリティ基本方針は、法人が保有する情報資産の機密性、完全性、可用性、真正性の確保を通じて医療安全の向上に資するとともに、法令等が定める個人情報保護及び情報セキュリティの遵守を目的とし、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

この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、当該各号に定めるところによる。

（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のことで、法人の所有であるかを問わず、法人の所掌する事務に使用するものすべてをいう。

（３）情報資産

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

（４）機密性（confidentiality）

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。

（５）完全性（integrity）

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。

（６）可用性（availability）

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。

（７）HIS（Hospital Information System）

電子カルテや部門システム等の患者情報を取扱うネットワーク、情報システムをいう。

（８）インターネット接続システム

インターネットによる外部との通信が可能なネットワーク、情報システムをいう。

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、ウィルス攻撃、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違反、設計・導入の不備、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、外部委託管理の不備、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・広範囲にわたる感染症等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. 情報資産利用者の責務

職員及び契約職員、ならびに委託等を受け法人の情報資産を取り扱う全ての者（以下「利用者」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。

5. 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組織体制を確立する。

（2）人的対策

情報セキュリティに関し、利用者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。

（3）物理的対策

サーバ、通信機器及びパソコン等のハードウェアの管理について、物理的な対策を講じる。

（4）技術的対策

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。

（5）脆弱性対策

サーバ、通信機器及びパソコン等の脆弱性について情報収集を行い管理するとともに、脆弱性が判明した時は改善対策を講じる。

（6）IT-BCP の確立

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、IT-BCP を策定する。

（7）事業者との契約

情報資産を取り扱う契約においては事業者を選定し、情報セキュリティ特記事項を明記した契約を締結し、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。

（8）外部サービスの利用

インターネット接続システムにおいて、クラウドシステム等外部サービスを利用する場合には、当該サービスを利用する利用者を所管する部署において、情報セキュリティポリシーを遵守するための手順を整備し対策を講じる。

6. 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。

7. 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。

8. 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本書とは別に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。具体的な運用は実施手順として別に定めるものとし、対策基準と実施手順が重複する項目については実施手順が優先されるものとする。

1. 組織体制

	名称	役職名（充職）	役割
A	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
B	統括情報セキュリティ責任者	法人本部長	ＣＩＳＯの補佐/欠員時の代理、Ｃへの指導/提言
C	情報セキュリティ責任者	院長・法人事務局長	D,Ｅへの指導/提言
D	情報システム管理者 （担当窓口）	情報システム課 課長	セキュリティ侵害発生時のA,B,Cへの報告 情報システム導入/変更/運用等の指示
	情報システム担当者 （担当窓口）	情報システム課 システム係	情報システム導入/設定/変更/運用等の作業
E	情報セキュリティ管理者	所属長	セキュリティ侵害発生時の C、Ｄへの報告、Ｆの教育、助言及び指示
F	利用者	全利用者	ポリシー及び実施手順を遵守

（1）最高情報セキュリティ責任者（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。

② CISO 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。

（2）統括情報セキュリティ責任者

① 法人に統括情報セキュリティ責任者を置き、本部長をもって充てる。

② 統括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 統括情報セキュリティ責任者は、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権限及び責任を有する。

④ 統括情報セキュリティ責任者は、情報セキュリティ責任者に対して、情報セキュリティに関する指導及び助言を行う。

（3）情報セキュリティ責任者

① 法人に情報セキュリティ責任者を置き、堺市立総合医療センターには院長、法人本部においては法人事務局長をもって充てる。

② 情報セキュリティ責任者は、その所管する情報資産に関する情報セキュリティを統括する権限及び責任を有する。

③ 情報セキュリティ責任者は、情報セキュリティ管理者及び情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う。

（4）情報システム管理者

① 情報システム課課長を法人の情報システム全般における情報システム管理者とする。

② 情報システム管理者は、法人の情報システムにおける導入、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対策に関する権限及び責任を有する。

④ 情報システム管理者は、法人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恐れがある場合には、統括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。合わせて、CISO 及び情報セキュリティ責任者への事象の報告を行わなければならない。

（5）情報システム担当者

① 情報システム担当者に情報システム課システム係係長を充て、情報システム管理者の指示等に従い、情報システムの導入、設定の変更、運用、更新等の作業を行う。

② 情報システム担当者は情報システム管理者が不在の場合、その職務を代理する。

（6）情報セキュリティ管理者

① 法人に情報セキュリティ管理者を置き、所属長（地方独立行政法人堺市立病院機構職務権限規程に定める課長、所属長が不在の場合は院長が指名する者）をもって充てる。

② 情報セキュリティ管理者は、その所管する情報資産に関す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。

③ 情報セキュリティ管理者は、利用者に対する教育、助言及び指示を行う。

④ 情報セキュリティ管理者は、その所管する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、情報システム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。

（7）利用者

利用者は、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利用者向けに定められている事項を遵守する。

（8）窓口担当

情報セキュリティに関する情報を一元化するため、法人において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、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。

（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：ComputerSecurity 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。なお、情報システムで複数の分類の情報資産を取り扱う場合、該当するすべての分類に応じ扱制限を行うものとする。

区分	種別	分類基準	主な取扱制限
機密性	第１種（極秘）	・個人情報（個人情報の保護に関する法律に定める事項） ・法人で取り扱う情報資産のうち、外部に漏えいすることで法人において著しく不利益を被るもの	・法人資産以外の端末での作業の原則禁止 ・保管場所の制限 ・保管場所への必要以上の外部記録媒体等の持ち込み禁止
	第２種（秘密）	・法人で取り扱う情報資産のうち、限られた特定の幹部等を対象とした内部の	・情報の送信、情報資産の運搬・提供時における暗号化・

		みで取扱うことを目的とした資料、人事情報、入札情報、公表前文書など	パスワード設定、鍵付きケースの利用 ・復元不可能な処理をしての廃棄
	第３種 （社外秘）	・外部への公開することにより業務に支障がでると情報セキュリティ管理者が判断したもの ・第１種及び第２種以外の情報資産	・情報セキュリティ管理者の組織単位で社外秘を定め管理
完全性	第１種	・法人で取り扱う情報資産のうち、改ざん、過失又は破損により、患者等の権利（生命、財産、プライバシー等）が侵害される又は法人の運営に支障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 ・外部やインターネット上のクラウドサービス等で情報処理を行う際の安全管理措置の徹底 ・施錠可能な場所への保管及びアクセス権の設定
	第２種	上記第１種以外の情報資産	・情報セキュリティ管理者で運用を定め管理
可用性	第１種	・法人で取り扱う情報資産のうち、滅失、紛失又は破損等により利用不可能な状態となり、患者等の権利が侵害される又は法人の安定的な運営に支障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 ・施錠可能な場所への保管及びアクセス権の設定
	第２種	上記第１種以外の情報資産	・情報セキュリティ管理者で運用を定め管理

（２）情報資産の管理

①　管理責任及び管理方法

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、（１）の分類に基づき情報資産を管理しなければならない（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含む)。

ウ　情報セキュリティ管理者は、保有する機密性第１種の情報資産について、情報セキュリティ管理者の判断により、必要に応じて台帳を作成し、当該情報資産を適切に管理するものとする。また、機密性第２種及び第３種の情報資産についても同様に、情報セキュリティ管理者の判断により、必要に応じて台帳を作成し、適切に管理するものとする。なお、台帳作成の対象は、紙媒体、Excel ファイル等の単体で管理される文書又はデータを原則とし、情報システム上にデータベースとして保存され、当該システムによりアクセス制御等の適切なセキュリティ管理が行われている情報資産については、台帳作成の対象外とすることができる。

エ　前項（ウ）に基づき台帳を作成する情報資産の管理において、同一の業務において複数のファイルを取り扱う場合は、当該ファイルを格納するディレクトリ（フォルダ）

単位で管理するものとし、その管理単位を台帳に明記する。

オ　業務で取り扱う文書やデータ等の情報資産は、原則として、組織が認可したファイルサーバ、業務システム、またはクラウドストレージ等の情報システム上に保存し、個人の端末や外部記憶媒体（USB メモリ、外付け HDD、私用 PC など）への保存は原則禁止とする。

カ　情報セキュリティ管理者は、外部記録媒体を利用し情報資産を保存せざるをえない場合は、情報システム管理者が定めたルールに従い適切に管理するものとする。

キ　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利用者及びアクセス権限を定めるものとする。

② 情報の作成

ア　利用者は、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、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③ 情報資産を取り扱うシステム等の導入

情報セキュリティ管理者は、情報セキュリティに支障が生じる可能性のある情報資産を取り扱うシステム・医療機器等を導入する場合は、あらかじめ情報システム担当者と対策を協議し、情報セキュリティ責任者に許可を得なければならない。

④ 情報資産の入手

ア　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。

イ　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　利用者は、業務以外の目的に情報資産を利用してはならない。

イ　利用者は、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　利用者は、情報資産を加工することによって分類に変更が生じる場合、加工後の分類に従い適正な取扱いをしなければならない。

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は、追記修正することによって不利益が生じる情報資産を保管する場合は、書込禁止等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、機密性の基準第 1 種又は第 2 種、完全性の基準第 1 種、可用性の基準第 1 種に該当する情報資産を保管する場合、紛失盗難等、及び災害等に

よる滅失を防ぐための対策を行わなければならない。

⑦　情報資産の送信

ア　電子メール等により情報資産を送信する者は、暗号化又はパスワード設定等の措置を講じなければならない。

イ　機密性の基準第１種又は第２種の情報資産を送信する者は、情報セキュリティ管理者に許可を得なければならない。

⑧　情報資産の運搬

ア　法人敷地外へ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　機密性の基準第１種又は第２種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・公開

ア　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　機密性の基準第１種又は第２種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、所管する部署における情報資産の提供又は公開に際し、適切な手順を策定し、利用者に遵守を徹底させなければならない。

⑩　情報資産の廃棄

ア　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。

イ　情報資産の廃棄する場合、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。

エ　電磁的記録媒体の消去又は記録装置の破砕等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.　情報システムのセキュリティ方針

（1）ＨＩＳ

①　外部との分離

HIS はインターネット等の外部通信から分離しなければならない。HIS と外部通信を行う必要性がある場合は、通信経路の限定（IP アドレス、MAC アドレス等）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。

② 利用の制限

HIS 系の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、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。ただし、感染症対策等において診療等業務上やむをえないと情報セキュリティ管理者が判断した場合はその限りではない。その場合、情報セキュリティ管理者は不正利用の対策を別途講じなければならない。

（2）ウィルス対策

情報システムにおいて OS（オペレーティングシステム）で動作するパソコン等全ての機器について原則、マルウェア等ウィルス対策を講じなければならない。

（3）脆弱性対策

情報システムにおいて OS、アプリケーション、ファームウェア等は原則、常に最新の脆弱性修正プログラムを適用しなければならない。

（4）技術的措置

外部から情報を受け取る際、次にあげる実現方法等により、無害化、及び監視等の対策を図らなければならない。

① インターネットメールのテキスト化

② 他のネットワークから HIS 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取り込む方式

④ 通信パケットの監視、ふるまい検知等の不正通信の監視

（5）クラウドサービスの利用

業務の効率性・利便性の向上を目的として、インターネット上のクラウドサービスを利用し、患者情報、入札情報、利用者の重要な情報資産を取り扱う場合は、必要な情報セキュリティ対策を講じた上で、必要に応じ外部監査及び脆弱性診断を実施し安全性を確保しなければならない。

4. 人的セキュリティ対策

（1）利用者の遵守事項

① 情報セキュリティポリシー等の遵守

利用者は、情報セキュリティポリシー及び実施手順を遵守し、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

利用者は、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 電子メールの利用制限

ア 利用者は、自動転送機能を用いて、電子メールを私的な電子メールアドレスへ転送

してはならない。

イ　利用者は、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。

ウ　利用者は、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。

エ　利用者は、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。

オ　利用者は、法人が提供するメール以外、他のサービス等を原則使用してはならない。

④　情報資産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　利用者は、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ェアを外部に持ち出す場合には、情報システム管理者の許可を得なければならない。

ウ　利用者は、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。

⑤　個人所有端末の業務利用

ア　利用者は、法人貸与以外のパソコン、モバイル端末等情報機器を原則業務に利用してはならない。

イ　利用者は、法人貸与以外のパソコン、モバイル端末等情報機器を業務に利用する場合であって且つ法人内のネットワークに接続する場合は、情報システム管理者が別に定める手続きによらなければならない。

ウ　利用者は、法人貸与以外の USB 等外部記録媒体を法人内の情報システムにおいて利用してはならない。

⑥　端末等の移動及び移設

ア　利用者は、業務で使用する端末等を所定の場所から一時的に移動させる必要がある場合、情報セキュリティ管理者の許可を得て、完了後は速やかに所定の場所へ戻さなければならない。

イ　利用者は、業務で使用する端末等を所定の場所から移設する場合は、情報セキュリティ管理者の許可を得なければならない。

ウ　情報セキュリティ管理者は、業務で使用する端末等を所定の場所から移設した場合、情報システム管理者に報告しなければならない。なお、医療機器等固定資産登録されたものにおいては固定資産管理者へ同時に報告しなければならない。

⑦　設定の変更の禁止

利用者は、情報システムの機器及びソフトウェアに関する設定、セキュリティ機能の設定を情報システム管理者の許可なく変更してはならない。

⑧　機器等の管理

利用者は、パソコン等情報システムを取り扱う機器及び印刷された文書等について、第三者に使用、閲覧されることがないように、離席時の端末等のロック、及び業務終了後に容易に使用、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。

⑨　退職時等の遵守事項

利用者は、退職等により業務を離れる場合、貸与された物品を速やかに返却し、業務上知り得た情報を漏らしてはならない。

（2）情報セキュリティポリシー等の掲示

情報システム管理者は、利用者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。

（3）委託事業者における情報セキュリティポリシーの遵守

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導入・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について、「情報セキュリティ特記事項」を締結しなければならない。

（4）研修

①　情報セキュリティに関する研修

情報システム管理者は、定期的に情報セキュリティに関する研修を実施しなければならない。

②　研修への参加

利用者は、定められた研修に参加しなければならない。

（5）情報セキュリティインシデントの報告

利用者は、情報セキュリティインシデント発生時において、報告、復旧、再発防止等について別に定める実施手順に従いすみやかに行わなければならない。

（6）ID、パスワードの取扱い

利用者が情報システムを利用する際、認証に使用する ID 及びパスワードの取扱いについては事項を遵守しなければならない。

①　個人 ID

利用者自身が利用している ID　は、他人に利用させてはならない。

②　共用 ID

ア　複数の利用者が共用の ID を利用して、情報システム等を利用することは原則禁止する。ただし、業務上やむを得ない場合においては、利用者を限定し、共用 ID 利用者以外に利用させてはならない。

イ　情報セキュリティ管理者は、所管する業務で共用 ID を使用する情報システムにおいて、利用者の情報資産の閲覧、変更、削除等がわかるように台帳等によって管理する措置を講じなければならない。

③　パスワードの取扱い

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワード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。

ウ　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。

エ　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。

オ　共用IDで認証する情報システムの端末等で、パスワードを記憶させてはならない。

5.　物理的セキュリティ対策

（1）サーバ等の管理

①　機器の取付け

情報システム管理者は、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正に固定する等、必要な措置を講じなければならない。

②　機器の電源

ア　情報システム管理者は、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。

イ　情報システム管理者は、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

ア　情報システム管理者は、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。

イ　情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、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。

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。

エ　情報システム管理者は、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

ア　情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。

イ　情報システム管理者は、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、情報システム管理者は、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

情報システム管理者は、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。

（２）管理区域（サーバ室等）の管理

①　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や電磁的記録媒体の保管庫をいう。

イ　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。

ウ　情報システム管理者は、情報システム室内の機器等に、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。

エ　情報システム管理者は、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

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。

イ　利用者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。

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利用者が付き添うものとし、外見上利用者と区別できる措置を講じなければならない。

エ　情報システム管理者は、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

ア　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。

イ　情報システム管理者は、情報システム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。

（３）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、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。

（４）利用者の利用する端末や電磁的記録媒体等の管理

① 情報セキュリティ管理者は、盗難防止のため、必要に応じ執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及びその他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。また、電磁的記録媒体については、業務上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 情報システム管理者は、情報システムへのログインに際し、パスワード、IC 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。

③ 情報システム管理者は、ＨＩＳ系では「知識」、「所持」、「存在（生体）」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。なお、医療機器に組み込まれたパソコン等においては診療、検査における運用等を考慮し可能な限り同様の措置を講じること。

（５）取扱区域の管理

① 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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。

6. 技術的セキュリティ対策

（１）情報システムの管理

① ファイルサーバ及び文書管理サーバ

ア ファイルサーバー及び文書管理サーバにおいて、利用者全体で閲覧及び使用可能な領域、及び課等の単位で構成し、利用者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領域に分けて構成しなければならない。

イ 患者の個人情報、人事記録等、特定の利用者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、担当職員以外の利用者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

ア 情報システム管理者は、情報システムに記録された情報について法人の運営に必要な情報については、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。

イ HIS 系のサーバについて電子カルテ及び医事システムにおいてはオフラインバックアップ等不正アクセスによる改ざん防止対策を必ず実施し、バックアップは複数世代取得しなければならない。また、法人において必要と判断した情報資産においても同様の措置を講じること。

③ システム管理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において、システム変更等の作業を行った場合は、作業の実務者に作業内容について報告書の提出を指示し、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。

イ 情報システム管理者は、情報システム担当者または、契約により作業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

情報システム管理者は、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

ア 情報システム管理者は、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。

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、取扱方法及びログが正常に取得できているか定期的に確認し、適正にログを管理しなければならない。

ウ 情報システム管理者は、取得したログを定期的に点検又は分析し、悪意ある第三者等からの不正侵入、不正操作等の兆候が発見された場合、速やかに対策を講じなければならない。

⑥ 障害記録

情報システム管理者は、利用者及び保守管理する委託業者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

ア　情報システム管理者は、不正アクセスを防止するため、ネットワークにファイアウォール等を設け適正なアクセス制御を施さなければならない。

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。

⑧　外部の者が利用できるシステムの分離等

情報システム管理者は、利用者以外の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または論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

ア　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。

イ　情報システム管理者は、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。

ウ　情報システム管理者は、インターネットに接続された全ての外部ネットワーク回線において、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。なお、ファイアウォール等の設置が困難な場合、必ず接続元制限を実施しアクセス状況の監視を行わなければならない。

エ　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、統括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　クライアント等情報機器のセキュリティ管理

ア　情報システム管理者は、クライアント等情報機器を調達する場合、当該機器が備える機能、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、情報セキュリティインシデントへの対策等適正な対策を講じなければならない。

イ　情報システム管理者は、情報機器の運用を終了する場合、情報機器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 機器等特定用途機器のセキュリティ管理

情報システム管理者は、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

ア　情報システム管理者は、無線 LAN を設置する場合、暗号化及び認証技術等を用いて盗聴等不正アクセスを防ぐ措置を講じなければならない。

イ　情報システム管理者は、機密性の高い情報を取り扱うネットワークについて、物理的または論理的に回線を分離しなければならない。

⑬　電子メールのセキュリティ管理

ア　情報システム管理者は、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、当該メールアカウントの運用を停止する等の措置を講じなければならない。

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不可能にしなければならない。

ウ　情報システム管理者は、利用者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利用者に周知しなければならない。

エ　情報セキュリティ管理者は、所管する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　電子署名・暗号化

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。

⑮　無許可ソフトウェアの導入等の禁止

ア　利用者は、法人貸与のパソコンやモバイル端末に無断でソフトウェアを導入してはならない。

イ　利用者は、業務上の必要がある場合は、情報システム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又は情報システム管理者は、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。

ウ　利用者は、不正にコピーしたソフトウェアを利用してはならない。

⑯　機器構成の変更の制限

ア　利用者は、法人貸与のパソコン等情報機器に対し機器の改造及び増設・交換を行ってはならない。

イ　利用者は、業務上、法人貸与のパソコン等情報機器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、情報システム管理者の許可を得なければならない。

⑰　業務外ネットワークへの接続の禁止

ア　利用者は、法人から貸与されたパソコン等情報機器を、有線・無線を問わず、情報システム管理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。

イ　情報システム管理者は、貸与する情報機器について、原則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措置を講じなければならない。

⑱　WEB 閲覧の制限

ア　利用者は、業務以外の目的で WEB を閲覧してはならない。

イ　情報システム管理者は、利用者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、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

ウ　情報システム管理者は、WEB 閲覧においてマルウェア等の感染の恐れがある危険性の高い、もしくは疑わしいサイトへのアクセス制限を講じなければならない。

エ　情報システム管理者は、業務上アクセス制限のかかったサイトの閲覧の必要性が生じた場合、そのサイトの安全性が確認できた場合のみ閲覧を許可することができる。

⑲ ウェブ会議サービスの利用時の対策

ア　情報システム管理者は、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　利用者は、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しなければならない。

⑳ 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、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。

イ　機密性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。

ウ　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。

エ　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）アクセス制御

① アクセス制御等

ア　アクセス制御

情報システム管理者は、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利用者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。

イ　利用者 ID の取扱い

（ア）情報システム管理者は、利用者の登録、変更、抹消等の情報管理、利用者の異動、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）利用者は、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、情報システム管理者に通知しなければならない。

（ウ）情報システム管理者は、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。

ウ　特権を付与された ID の管理等

（ア）情報システム管理者は、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）情報システム管理者の特権を代行する者は、情報システム管理者が認めた者でなければならない。

（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について、外部委託事業者に許可なく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 ID 及びパスワードについて、利用者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。

② 利用者による外部からのアクセス等の制限

ア　利用者が外部から法人施設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、情報システム管理者の許可を得なければならない。

イ　情報システム管理者は、法人施設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。

ウ　情報システム管理者は、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。

エ　情報システム管理者は、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。

オ　情報システム管理者は、外部からのアクセスに利用するモバイル端末を利用者に貸与する場合、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。

カ　利用者は、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施設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。

キ　利用者は、公衆通信回線（公衆無線 LAN 等）を用いて、法人施設内のネットワークに接続してはならない。

③ ログイン時の表示等

情報システム管理者は、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利用者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

ア　情報システム管理者は、利用者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。

イ　情報システム管理者は、利用者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。

ウ　情報システム管理者は、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。

（4）システム導入、保守等

① 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。

イ　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 情報システムの導入

ア　システム導入における責任者及び作業者の特定

情報システム管理者は、システム導入の責任者及び作業者を特定しなければならない。また、システム導入のための方針手順等を決定し、導入に適用しなければならない。

イ　システム導入における責任者、作業者の ID の管理

（ア）情報システム管理者は、システム導入の責任者及び作業者が使用する ID を管理し、導入完了後、導入用 ID を削除しなければならない。

（イ）情報システム管理者は、システム導入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い。

ウ　システム導入に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、システム導入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

ア　導入環境と運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は、システム導入・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、システム導入・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。

（ウ）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しなければならない。

（エ）情報システム管理者は、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。

イ　テスト

（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。

（ウ）情報システム管理者は、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）情報システム管理者は、テストが正常に完了したことを確認しなければならない。

④ システム導入・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、システム導入・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。

イ　情報システム管理者は、テスト結果を一定期間保管しなければならない。

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

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、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。

イ　情報システム管理者は、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。

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。

⑦　導入・保守用のソフトウェアの更新等

情報システム管理者は、導入・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。

⑧　システム更新又は統合時の検証等

情報システム管理者は、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。

（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。

ア　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。

イ　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。

ウ　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、必要に応じ利用者に対して注意喚起しなければならない。

エ　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常駐させなければならない。なお、常駐できない場合、他の安全性を確保するための対策を講じなければならない。

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は、常に最新の状態に保たなければならない。

カ　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。

キ　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導入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。継続利用する場合、継続利用期間を明確にし、セキュリティ対策、リスクを極力回避するための運用等対策を講

じなければならない。

ク　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利用者に利用させてはならない。また、不正プログラムの感染、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。

ケ　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、情報システム管理者が許可した職員を除く利用者に当該権限を付与してはならない。

コ　不正プログラム対策ソフトウェア等により以下の動作についてチェック、または無害化できる環境を整備しなければならない。

（ア）外部からデータ又はソフトウェアを取り入れる場合

（イ）添付ファイルが付いた電子メールを受信する場合

（ウ）インターネット接続システム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

③　利用者の遵守事項

利用者は、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。

ア　法人貸与の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。

イ　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。

ウ　情報システム管理者が提供するウィルス情報を、常に確認しなければならない。

エ　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、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

情報システム管理者は、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）不正アクセス対策

①　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。

ア　通信に使用するポートを明確化し許可したポートのみ通信できる措置を講じること。

イ　利用するサービス以外は、機能を削除又は停止しなければならない。

ウ　統括情報セキュリティ責任者は、情報セキュリティインシデントに対処するため、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 ホームページ、クラウドシステムの対処

ホームページ、クラウドシステムを管轄する情報セキュリティ管理者は、不正アクセス及びウェブページの改ざんのデータの書換えが認められた場合、すみやかにサービスを停止するなどの措置を講じ、統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③ 攻撃への対処

統括情報セキュリティ責任者及び情報システム管理者は、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。

④ 記録の保存

統括情報セキュリティ責任者及び情報システム管理者は、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。

⑤ 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、利用者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法人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。

⑥ 利用者による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、利用者による不正アクセスを発見した場合は、当該利用者の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。

⑦ サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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。

⑧ 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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。

（７）セキュリティ情報の収集

① 脆弱性に関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システム管理者は、脆弱性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、当該脆弱性の緊急度に応じて、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

統括情報セキュリティ責任者及び情報システム管理者は、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、情報セキュリティ管理者および利用者に周知しなければならない。

③ 新たな脅威に関する情報の収集及び対策

統括情報セキュリティ責任者及び情報システム管理者は、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

（1）情報システムの監視

① 統括情報セキュリティ責任者及び情報システム管理者は、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 統括情報セキュリティ責任者及び情報システム管理者は、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。

（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

ア 情報セキュリティ責任者及び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、問題を認めた場合には、速やかに関係各所に報告しなければならない。

イ CISO 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。

ウ 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合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、利用者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 利用者の報告義務

ア 利用者は、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、直ちに統括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を行わなければならない。

イ　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統括情報セキュリティ責任者が判断した場合において、利用者は、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。

（3）侵害時の対応等

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対処しなければならない。

（4）例外措置

①　例外措置の許可

法人は、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、法人運営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、例外措置を講じることができる。

②　緊急時の例外措置

法人は、法人運営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。

（5）法令遵守

①　法令遵守

利用者は、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、関係法令を遵守し、これに従わなければならない。

②　ガイドラインの準拠

利用者は、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、関係法令のガイドラインに準拠し、適切な管理体制を整備するとともに、必要な安全対策を講じなければならない。

（6）違反時の対応

利用者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　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該利用者の情報セキュリティ管理者に通知し、適正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の指導によっても改善されない場合、統括情報セキュリティ責任者は当該利用者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。

8　業務委託と外部サービスの利用

（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 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情報セキュリティ要件を明記した「情報セキュリティ特記事項」を締結しなければならない。

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、「情報セキュリティ特記事項」に基づき措置を実施しなければならない。

（2）外部サービスの利用

事業者等の法人の外部の組織が、情報システムの一部又は全部の機能を提供するサービス（以下「外部サービス」という。）の利用については、統括情報セキュリティ責任者が別に定める利用基準に基づいて行うこととする。

9 評価・見直し（監査・自己点検）

（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、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

ア 情報セキュリティ監査統括責任者は、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。

イ 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

ア 情報セキュリティ監査統括責任者は、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。

イ 被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を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。

⑥　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、統括情報セキュリティ責任者及び CISO に報告する。

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、統括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。

（2）自己点検

①　実施方法

ア　情報システム管理者は、所管する情報システム及び利用するパソコン等端末について、毎年度及び必要に応じて自己点検を実施しなければならない。

イ　情報セキュリティ管理者は、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

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

イ　情報システム管理者は、この点検結果を情報システム管理者に共有し、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）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。

【制定／改定履歴】

版数	日付	内容
第１版	令和８年２月２７日	制定