平成 31 年３月 12 日
神奈川県立病院機構理事会
資料７
総務企画部
第 25 号議案

地方独立行政法人神奈川県立病院機構コンピュータ、ネットワーク及び情報システム運営規程の制定及び情報セキュリティポリシーの一部改正について

１　制定及び改正の趣旨

業務方法書第 12 条第２号に基づき、情報システム等の運営に関し必要な事項を地方独立行政法人神奈川県立病院機構コンピュータ、ネットワーク及び情報システム運営規程（以下「規程」という。）として定めるものである。

これに併せ、情報セキュリティポリシー（以下「ポリシー」という。）の一部改正も行う。

２　主な規程の概要（規程）

(1)　理事長は、コンピュータ、ネットワーク及び情報システムを運営する体制の整備及び情報化の推進を図る。（第３条関係）

(2)　これまで情報セキュリティポリシーに規定していた最高情報統括責任者、コンピュータ管理者、ネットワーク管理者及び情報システム管理者（以下「情報システム管理者等」という。）に係る事項を、当該規程にも設けた。（第６条～第９条関係）

(3)　総長等及び本部事務局長は、必要に応じて、情報システム管理者等を別に指名することができる。（第 10 条）

(4)　情報システム管理者は、データ活用に係る整備に努める。（第 14 条関係）

３　主な改正の概要（ポリシー）

規程の内容と整合するよう、条項の順番等を見直した。

４　規程及びポリシー

別添資料１及び別添資料２のとおり

５　施行年月日

共に平成 31 年４月１日

（参考）

業務方法書　抜粋

（情報伝達及び情報システムに関する事項）

第 12 条 県立病院機構は、次の各号に掲げる事項を定めた情報伝達及び情報システムに関する規程等を整備するものとする。なお、業務変更に伴う情報システムの改変は適宜速やかに行うものとする。

⑴ 情報伝達に関する以下の事項

ア 理事長の指示、定款第１条の目的が確実に役職員に伝達される仕組み

イ 職員から役員に必要な情報（特に、危機管理、内部統制に関する情報）が伝達される仕組み

⑵ 情報システムに関する以下の事項

ア 情報システムを活用した効率的な業務運営（情報化の推進）

イ 情報を利用可能な形式に整えて活用できる以下の事項

(ｱ) 法人が保有するデータの所在情報の明示

(ｲ) データへのアクセス権の設定

(ｳ) データを汎用アプリケーションで利用可能とするツールの構築

(ｴ) 機種依存形式で作成されたデータ等に関するＡＰＩ（アプリケーション・プログラミング・インターフェイス）の策定

別添資料１（資料７関係）

地方独立行政法人神奈川県立病院機構コンピュータ、ネットワーク及び情報システム運営規程

（趣旨）

第１条　この規程は、地方独立行政法人神奈川県立病院機構業務方法書に基づき、地方独立行政法人神奈川県立病院機構（以下「法人」という。）における情報システム等の運営に関し必要な事項を定めるものとする。

（定義）

第２条　この規程において、次の各号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)　コンピュータ　汎用コンピュータ、サーバ、ワークステーション、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。

(2)　ネットワーク　コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。

(3)　情報システム　コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。

(4)　データ　コンピュータ又は記憶媒体に記録されている電磁的記録をいう。

(5)　情報資産　コンピュータ、ネットワーク、情報システム及びこれらが取り扱う情報（当該情報を印刷した文書を含む。）をいう。

(6)　総長等　地方独立行政法人神奈川県立病院機構組織規程（以下「組織規程」という。）第 15 条第２項に規定する総長等をいう。

(7)　本部事務局長　組織規程第７条第１項に規定する本部事務局長をいう。

（理事長の責務）

第３条　理事長は、地方独立行政法人法（平成 15 年法律第 118 号。）第 25 条第１項の規定により神奈川県知事から指示された中期目標等に基づき法令等を遵守しつつ業務を行い、地方独立行政法人神奈川県立病院機構定款第１条の目的を有効かつ効率的に果たすため、コンピュータ、ネットワーク及び情報システム（以下「情報システム等」という。）を運営する体制の整備及び情報化の推進を図るものとする。

２　理事長は、継続的に情報システム等を運営する体制の見直しを図るものとする。

（適用範囲）

第４条　この規程の適用範囲は、法人の業務運営に関与する全ての情報システム等とする。

（情報システム委員会）

第５条　法人における情報システム等を運営する体制の整備及び情報化の推進を図るため、法人に情報システム委員会を置く。

２　情報システム委員会の設置及び運営については、理事長が別に定める。

（最高情報統括責任者）

第６条　法人に最高情報統括責任者（ＣＩＯ）を置き、副理事長のうち理事長が指名する者をもって充てる。

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

（コンピュータ管理者）

第７条　病院及び本部にコンピュータ管理者を置き、病院においては総長等を、本部においては本部事務局長をもって充てる。

２　コンピュータ管理者は、所管するコンピュータの設定、運法、更新等を行う。

３　コンピュータ管理者は、所管するコンピュータの情報セキュリティを統括する。

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

５　コンピュータ管理者は、所管するコンピュータに係る情報セキュリティ実施手順の策定、維持及び管理を行う。

（ネットワーク管理者）

第８条　病院及び本部にネットワーク管理者を置き、病院においては総長等を、本部においては本部事務局長をもって充てる。

２　ネットワーク管理者は、所管するネットワークの構築、設定の変更、更新等を行う。

３　ネットワーク管理者は、所管するネットワークの情報セキュリティを統括する。

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

５　ネットワーク管理者は、所管するネットワークに係る情報セキュリティ実施手順の策定、維持及び管理を行う。

（情報システム管理者）

第９条　病院及び本部に情報システム管理者を置き、病院においては総長等を、本部においては本部事務局長をもって充てる。

２　情報システム管理者は、所管する情報システムの開発、設定の変更、運用、更新等を行う。
３　情報システム管理者は、所管する情報システムの情報セキュリティを統括する。
４　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資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。
５　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の策定、維持及び管理を行う。

（情報システム管理者等の指名）
第 10 条　総長等及び本部事務局長は、前３条の規定を達成するために、必要に応じて、コンピュータ管理者、ネットワーク管理者及び情報システム管理者（以下「情報システム管理者等」という。）を別に指名することができる。

（管理補助者の指名）
第 11 条　総長等及び本部事務局長は、情報システム等に係る実務を担当する管理補助者を別に指名する者とする。

（情報セキュリティ対策）
第 12 条　情報システム管理者等は、情報セキュリティ対策を講じると共に、最高情報統括責任者が定めるところにより定期的に点検を行うものとする。

（運営環境の整備）
第 13 条　情報システム管理者等は、情報システム等の運営を円滑に行うため、開発、運用体制の確保、研修の実施等運営環境の整備に努めるものとする。

（データ活用）
第 14 条　情報システム管理者は、情報システムを活用した効率的な業務運営を達成するため、次に掲げる事項の整備に努めるものとする。
(1)　保有するデータの所在情報の明示
(2)　データへのアクセス権の設定
(3)　データを汎用アプリケーションで利用可能とするツールの構築
(4)　機種依存的で作成されたデータ等に関するＡＰＩ（アプリケーション・プログラミング・インターフェース）の策定

（雑則）

第 15 条　この規程に定めるもののほか、情報システム等の運営に関し必要な事項は、理事長が別に定める。

附　則

この規程は、平成 31 年４月１日から施行する。

別添資料２（資料７関係）

情報セキュリティポリシー　新旧対照表（要綱）

新	旧
序　情報セキュリティポリシーの構成 情報セキュリティポリシーとは、地方独立行政法人神奈川県立病院機構（以下「法人」という。）が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものをいう。情報セキュリティポリシーは、法人が所管する情報資産に関する業務に携わる全ての職員等に情報セキュリティへの取組みを浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。 このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分である情報セキュリティ基本方針と情報セキュリティを取り巻く状況の変化に依存する部分である情報セキュリティ対策基準とにより構成することとした。 また、情報セキュリティポリシーに基づく詳細な実施手順についてはセキュリティ対策基準以上に頻繁な改正が見込まれることから、情報セキュリティポリシーに基づき定める実施手順とした（下表参照）。	序　情報セキュリティポリシーの構成 情報セキュリティポリシーとは、地方独立行政法人神奈川県立病院機構（以下「機構」という。）が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものをいう。情報セキュリティポリシーは、機構が所管する情報資産に関する業務に携わる全ての職員等に情報セキュリティへの取組みを浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。 このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分である情報セキュリティ基本方針と情報セキュリティを取り巻く状況の変化に依存する部分である情報セキュリティ対策基準とにより構成することとした。 また、情報セキュリティポリシーに基づく詳細な実施手順についてはセキュリティ対策基準以上に頻繁な改正が見込まれることから、情報セキュリティポリシーに基づき定める実施手順とした（下表参照）。

情報セキュリティポリシー及び情報セキュリティ実施手順の構成

分類	文書名	内容	
情報セキュリティポリシー	情報セキュリティポリシー（要綱）	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
		情報セキュリティ対策基準	情報セキュリティ基本方針に基づき定める情報システム等に共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順	－	情報セキュリティポリシーに基づいた情報システム等ごとに定める具体的な実施手順。	

第１章　情報セキュリティ基本方針

１　目的

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

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御することは、患者等の財産、プライバシー等を守るためにも、また、業務の安定的な運営のためにも必要不可欠であり、さらに法人に対する患者等からの信頼の維

情報セキュリティポリシー及び情報セキュリティ実施手順の構成

分類	文書名	内容	
情報セキュリティポリシー	情報セキュリティポリシー（要綱）	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
		情報セキュリティ対策基準	情報セキュリティ基本方針に基づき定める情報システム等に共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順	－	情報セキュリティポリシーに基づいた情報システム等ごとに定める具体的な実施手順。	

第１章　情報セキュリティ基本方針

１　目的

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

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御することは、患者等の財産、プライバシー等を守るためにも、また、業務の安定的な運営のためにも必要不可欠であり、さらに機構に対する患者等からの信頼の維

持向上に寄与するものである。 この基本方針は、法人が所管する情報資産の機密性、完全性及び可用性を維持するため、法人が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。	持向上に寄与するものである。 本基本方針は、機構が所管する情報資産の機密性、完全性及び可用性を維持するため、機構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 この要綱において、次に掲げる用語の意義は、以下の各号に定めるところによる。	2　定義 この要綱において、次に掲げる用語の意義は、以下の各号に定めるところによる。
(1) コンピュータ　汎用コンピュータ、サーバ、ワークステーション、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。	(1) コンピュータ　汎用コンピュータ、サーバ、ワークステーション、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。
(2) ネットワーク　コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。	(2) ネットワーク　コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。
(3) 情報システム　コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。	(3) 情報システム　コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。
(4) データ　コンピュータ又は記録媒体に記録されている電磁的記録をいう。	(4) データ　コンピュータ又は記録媒体に記録されている電磁的記録をいう。
(5) 情報資産　コンピュータ、ネットワーク、情報システム及びこれらが取り扱う情報（当該情報を印刷した文書を含む。）をいう。	(5) 情報資産　コンピュータ、ネットワーク、情報システム及びこれらが取り扱う情報（当該情報を印刷した文書を含む。）をいう。
(6) 記録媒体　データを記録するための媒体	

	をいう。例えば、磁気テープ、フロッピーディスク、ハードディスク、ＵＳＢメモリ、ＣＤ－Ｒ、ＤＶＤ－Ｒなど。
(7) 機密性	情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。
(8) 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。
(9) 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。
(10) 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。
(11) 情報セキュリティ対策	情報セキュリティを確保するための対策をいう。
(12) 情報システム等	コンピュータ、ネットワーク及び情報システムをいう。
(13) 情報システム管理者等	コンピュータ管理者、ネットワーク管理者及び情報システム管理者をいう。

(6) 記録媒体	データを記録するための媒体をいう。例えば、磁気テープ、フロッピーディスク、ハードディスク、ＵＳＢメモリ、ＣＤ－Ｒ、ＤＶＤ－Ｒなど。
(7) 機密性	情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。
(8) 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。
(9) 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。
(10) 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。
(11) 情報セキュリティ対策	情報セキュリティを確保するための対策をいう。
(12) 職員等	機構が雇用する職員及び労働者派遣事業の適正な運営の確

	保及び派遣労働者の就業条件の整備等に関する法律（昭和 60 年 7 月 5 日法律第 88 号）第 2 条第 2 項に規定する派遣労働者をいう。
(14)本部事務局長	地方独立行政法人神奈川県立病院機構組織規程（以下「組織規程」という。）第７条第１項に規定する本部の事務局長をいう。
(13)所属長	本部事務局事務局長、総長、所長及び足柄上病院病院長をいう。
(15)総長等	組織規程第 15 条第２項に規定する総長等をいう。
(16)職員等	法人が雇用する職員及び労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律(昭和 60 年 7 月 5 日法律第 88 号）（以下「労働者派遣法」という。）第 2 条第 2 項に規定する派遣労働者をいう。
(17)患者等	地方独立行政法人神奈川県立病院機構定款第 17 条に規定する病院の患者及びその家族をいう。
３　情報セキュリティポリシーの位置付けと職員等の義務 情報セキュリティポリシーは、法人が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の指針となるものである。	３　情報セキュリティポリシーの位置付けと職員等の義務 情報セキュリティポリシーは、機構が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の指針と

したがって、法人が所管する情報資産に関する業務に携わる全ての職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって情報セキュリティポリシーを遵守するものとする。	したがって、機構が所管する情報資産に関する業務に携わる全ての職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって情報セキュリティポリシーを遵守するものとする。
4　情報セキュリティ管理体制 法人は、法人が所管する情報資産について、情報セキュリティ対策を推進及び管理するための体制を確立するものとする。	4　情報セキュリティ管理体制 機構は、機構が所管する情報資産について、情報セキュリティ対策を推進及び管理するための体制を確立するものとする。
5　情報の分類 法人は、情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。	5　情報の分類 機構は、情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。
6　情報資産への脅威 情報セキュリティ対策基準を策定する上で、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると、特に情報セキュリティ対策を講ずべき脅威は以下のとおりである。 (1) 部外者による故意の不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難等 (2) 職員等及び委託事業者（再委託先等の事業者を含む。以下同じ。）の従業員による誤操作、故意の不正アクセス又は不正操作による情報若しくはプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難、正規の手続きによらない端末の接続による情報漏えい等 (3) 地震、落雷、火災等の災害及び事故、故障等による業務の停止 (4) 大規模・広範囲にわたる疾病による職員等の要員不足に伴う情報システム運用の機能不全	6　情報資産への脅威 情報セキュリティ対策基準を策定する上で、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると、特に情報セキュリティ対策を講ずべき脅威は以下のとおりである。 (1) 部外者による故意の不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難等 (2) 職員等及び委託事業者（再委託先等の事業者を含む。以下同じ。）の従業員による誤操作、故意の不正アクセス又は不正操作による情報若しくはプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難、正規の手続きによらない端末の接続による情報漏えい等 (3) 地震、落雷、火災等の災害及び事故、故障等による業務の停止 (4) 大規模・広範囲にわたる疾病による職員等の要員不足に伴

	う情報システム運用の機能不全
7　情報セキュリティ対策 法人は、前記で示した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ものとする。 (1) 物理的対策 情報システム等を設置する執務室等への不正な立入り及び情報資産への損傷、妨害等から保護するための物理的な対策 (2) 人的対策 情報セキュリティに関する役割等を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を講じるための対策 (3) 技術的対策 情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策 (4) 運用における対策 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、委託を行う際の情報セキュリティ確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策	7　情報セキュリティ対策 機構は、上記６で示した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ものとする。 (1) 物理的対策 情報システム等を設置する執務室等への不正な立入り及び情報資産への損傷、妨害等から保護するための物理的な対策 (2) 人的対策 情報セキュリティに関する役割等を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を講じるための対策 (3) 技術的対策 情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策 (4) 運用における対策 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、委託を行う際の情報セキュリティ確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策
8　情報セキュリティ対策基準の策定 法人が所管する情報資産について、前記の情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情	8　情報セキュリティ対策基準の策定 機構が所管する情報資産について、上記７の情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、情報セキ

報セキュリティ対策基準を第２章に定めるものとする。 9　情報セキュリティ実施手順の策定 情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、統括情報セキュリティ管理者は、情報セキュリティ実施手順を策定するものとする。 なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより情報セキュリティの確保に重大な支障を及ぼす恐れがあるため取扱いに注意するものとする。 10　情報セキュリティ監査の実施 法人は、情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施するものとする。 11　評価及び見直しの実施 法人は、情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施するものとする。	ュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を第２章に定めるものとする。 9　情報セキュリティ実施手順の策定 情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、統括情報セキュリティ管理者は、情報セキュリティ実施手順を策定するものとする。 なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより情報セキュリティの確保に重大な支障を及ぼす恐れがあるため取扱いに注意するものとする。 10　情報セキュリティ監査の実施 機構は、情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施するものとする。 11　評価及び見直しの実施 機構は、情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施するものとする。

第２章　情報セキュリティ対策基準	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とは、情報セキュリティ基本方針に基づき法人が所管する情報資産に関する情報セキュリティ対策の基準をいう。	情報セキュリティ対策基準とは、情報セキュリティ基本方針に基づく機構が所管する情報資産に関する情報セキュリティ対策の基準である。
１　対象範囲 (1) 情報セキュリティ対策基準が対象とする情報資産は、業務遂行のために法人が所管する情報資産とする。 また、計測、制御、実験、展示、教育訓練等のために用いる情報システム等であって、情報システム管理者等の協議により、統括情報セキュリティ管理者が情報セキュリティ対策基準を適用することが適当でないと認めた情報システム等は対象外とし、別途情報セキュリティ対策を実施するものとする。	１　対象範囲 (1) 情報セキュリティ対策基準が対象とする情報資産は、業務遂行のために機構が所管する情報資産とする。 また、計測、制御、実験、展示、教育訓練等のために用いる情報システム等であって、情報システム管理者、ネットワーク管理者及びコンピュータ管理者（以下「情報システム管理者等」という。）の協議により、統括情報セキュリティ管理者が情報セキュリティ対策基準を適用することが適当でないと認めた情報システム等は対象外とし、別途情報セキュリティ対策を実施するものとする。
２　情報セキュリティ管理体制 法人における情報セキュリティ管理体制は、以下のとおりとする。 (1) 最高情報統括責任者 ア　法人に最高情報統括責任者（CIO）を置き、副理事長のうち理事長が指名する者をもって充てる。 イ　最高情報統括責任者は、法人が所管する情報システム等の運営及び情報資産の情報セキュリティを統括する。	２　情報セキュリティ管理体制 機構における情報セキュリティ管理体制は、以下のとおりとする。 (1) 最高情報統括責任者（CIO） 本部事務局を所管する副理事長を、最高情報統括責任者（CIO）とする。 最高情報統括責任者（CIO）は、機構が所管する情報資産の情報セキュリティを統括する。
(2) 統括情報セキュリティ管理者 ア　法人に統括情報セキュリティ管理者を置き、本部事務局	(2) 統括情報セキュリティ管理者 本部事務局長を、統括情報セキュリティ管理者とする。

長をもって充てる。 イ　統括情報セキュリティ管理者は、神奈川県立病院機構ネットワークにおける情報セキュリティを統括する。 ウ　統括情報セキュリティ管理者は、情報セキュリティ管理者、ネットワーク管理者、情報システム管理者及びコンピュータ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。 エ　統括情報セキュリティ管理者は、法人が所管する情報資産に対する侵害又は侵害の恐れのある場合には、最高情報統括責任者の指示に従い、必要かつ十分な全ての措置を行う。ただし、特に緊急を要する場合及び最高情報統括責任者が不在の場合には、自らの判断に基づき必要かつ十分な全ての措置を行う。 オ　統轄情報セキュリティ管理者は、情報セキュリティ実施手順の策定、維持及び管理を行う。 (3) 情報セキュリティ管理者 ア　法人に情報セキュリティ管理者をおき、病院においては総長等を、本部においては本部事務局長をもって充てる。 イ　情報セキュリティ管理者は、統括情報セキュリティ管理者の下、所掌する所属における情報セキュリティを統括する。 ウ　情報セキュリティ管理者は、所掌する所属において所管している情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに当該所属における情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 エ　情報セキュリティ管理者は、所掌する所属における情報資産に対する侵害又は侵害の恐れのある場合には、情報シ	ア　統括情報セキュリティ管理者は、神奈川県立病院機構ネットワークにおける情報セキュリティを統括する。 イ　統括情報セキュリティ管理者は、情報セキュリティ管理者、ネットワーク管理者、情報システム管理者及びコンピュータ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。 ウ　統括情報セキュリティ管理者は、機構が所管する情報資産に対する侵害又は侵害の恐れのある場合には、最高情報統括責任者の指示に従い、必要かつ十分な全ての措置を行う。ただし、特に緊急を要する場合及び最高情報統括責任者が不在の場合には、自らの判断に基づき必要かつ十分な全ての措置を行う。 エ　統轄情報セキュリティ管理者は、情報セキュリティ実施手順の策定、維持及び管理を行う。 (3) 情報セキュリティ管理者 所属長を情報セキュリティ管理者とする。 ア　情報セキュリティ管理者は、統括情報セキュリティ管理者の下、所掌する所属における情報セキュリティを統括する。 イ　情報セキュリティ管理者は、所掌する所属において所管している情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに当該所属における情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 ウ　情報セキュリティ管理者は、所掌する所属における情報資産に対する侵害又は侵害の恐れのある場合には、情報シ

ステム管理者等へ速やかに報告を行い、指示を仰ぐとともに、統括情報セキュリティ管理者に対しても速やかに報告するものとする。 オ　情報セキュリティ管理者は、所掌する室課所に係る情報セキュリティ実施手順の策定、維持及び管理を行う。 カ　情報セキュリティ管理者は、職員等に端末による作業を行わせる場合には、情報セキュリティポリシーについて、特に注意を喚起し、守るべき実施手順を理解させ、かつ実施及び遵守させるものとする。 (4) コンピュータ管理者 ア　病院及び本部にコンピュータ管理者を置き、病院においては総長等を、本部においては本部事務局長をもって充てる。 イ　コンピュータ管理者は、所管するコンピュータの設定、運用、更新等を行う。 ウ　コンピュータ管理者は、所管するコンピュータの情報セキュリティを統括する。 エ　コンピュータ管理者は、所管するコンピュータにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 オ　コンピュータ管理者は、所管するコンピュータに係る情報セキュリティ実施手順の策定、維持及び管理を行う。	ステム管理者等へ速やかに報告を行い、指示を仰ぐとともに、統括情報セキュリティ管理者に対しても速やかに報告するものとする。 エ　情報セキュリティ管理者は、所掌する室課所に係る情報セキュリティ実施手順の策定、維持及び管理を行う。 オ　情報セキュリティ管理者は、職員等に端末による作業を行わせる場合には、情報セキュリティポリシーについて、特に注意を喚起し、守るべき実施手順を理解させ、かつ実施及び遵守させるものとする。 （第６号から移動）

(4) ネットワーク管理者 ア　病院及び本部にネットワーク管理者を置き、病院においては総長等を、本部においては本部事務局長をもって充てる。 イ　ネットワーク管理者は、所管するネットワークの構築、設定の変更、運用、更新等を行う。 ウ　ネットワーク管理者は、所管するネットワークの情報セキュリティを統括する。 エ　ネットワーク管理者は、所管するネットワークにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 オ　ネットワーク管理者は、所管するネットワークに係る情報セキュリティ実施手順の策定、維持及び管理を行う。 (5) 情報システム管理者 ア　病院及び本部に情報システム管理者を置き、病院においては総長等を、本部においては本部事務局長をもって充てる。 イ　情報システム管理者は、所管する情報システムの開発、設定の変更、運用、更新等を行う。 ウ　情報システム管理者は、所管する情報システムの情報セキュリティを統括する。 エ　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資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関	(4) ネットワーク管理者 ネットワークを運営している所属の長を、当該ネットワークに関するネットワーク管理者とする。 ア　ネットワーク管理者は、所管するネットワークの構築、設定の変更、運用、更新等を行う。 イ　ネットワーク管理者は、所管するネットワークの情報セキュリティを統括する。 ウ　ネットワーク管理者は、所管するネットワークにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 エ　ネットワーク管理者は、所管するネットワークに係る情報セキュリティ実施手順の策定、維持及び管理を行う。 (5) 情報システム管理者 情報システムを運営している所属の長を、当該情報システムに関する情報システム管理者とする。 ア　情報システム管理者は、所管する情報システムの開発、設定の変更、運用、更新等を行う。 イ　情報システム管理者は、所管する情報システムの情報セキュリティを統括する。 ウ　情報システム管理者は、所管する情報システムにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び

する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 オ　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の策定、維持及び管理を行う。 （第４号へ移動） (7) 情報セキュリティ委員会 情報セキュリティ委員会においては、法人の情報セキュリティの維持管理を統一的に行うため、情報セキュリティポリシーの策定等の情報セキュリティに関する重要な事項を審議する。 情報セキュリティ委員会の設置及び運営については、別途要綱で定める。 (8) 職員等 ア　職員等は、情報セキュリティポリシー及び情報セキュリ	指示を行う。 エ　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の策定、維持及び管理を行う。 (6) コンピュータ管理者 コンピュータを運営している所属の長を、当該コンピュータに関するコンピュータ管理者とする。 ア　コンピュータ管理者は、所管するコンピュータの設定、運用、更新等を行う。 イ　コンピュータ管理者は、所管するコンピュータの情報セキュリティを統括する。 ウ　コンピュータ管理者は、所管するコンピュータにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。 エ　コンピュータ管理者は、所管するコンピュータに係る情報セキュリティ実施手順の策定、維持及び管理を行う。 (7) 情報セキュリティ委員会 機構の情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティ委員会において、情報セキュリティポリシーの策定等の情報セキュリティに関する重要な事項を審議する。 情報セキュリティ委員会の設置及び運営については、別途要綱で定める。 (8) 職員等 ア　職員等は、情報セキュリティポリシー及び情報セキュリ

ティ実施手順のうち職員等向けに定められている事項を遵守するものとする。

イ　職員等は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示等を仰ぐものとする。

3　情報の分類と管理

(1) 情報の分類

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

イ　情報が複製又は伝送された場合には、当該複製等も原本の分類に準じて管理するものとする。

対策重要度

分類	基準
Ⅰ	個人情報
Ⅱ	分類Ⅰ及びⅢ以外の情報
Ⅲ	公開されている情報

(2) 情報の管理

ア　情報は、当該情報を所管する情報セキュリティ管理者が管理するものとする。

イ　情報は、原則として、ファイルサーバに保存するものとする。

ただし、各課所の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。

ウ　情報セキュリティ管理者は、外部記録媒体を適切に管理するものとする。

ティ実施手順のうち職員等向けに定められている事項を遵守するものとする。

イ　職員等は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示等を仰ぐものとする。

3　情報の分類と管理

(1) 情報の分類

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

イ　情報が複製又は伝送された場合には、当該複製等も原本の分類に準じて管理するものとする。

対策重要度

分類	基準
Ⅰ	個人情報
Ⅱ	分類Ⅰ及びⅢ以外の情報
Ⅲ	公開されている情報

(2) 情報の管理

ア　情報は、当該情報を所管する情報セキュリティ管理者が管理するものとする。

イ　情報は、原則として、ファイルサーバに保存するものとする。

ただし、各課所の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。

ウ　情報セキュリティ管理者は、外部記録媒体を適切に管理するものとする。

エ　情報セキュリティ管理者は、重要度に応じて、各々の情報にアクセスできる職員等及びアクセス権限を定めるものとする。 オ　情報セキュリティ管理者は、対策重要度Ⅰに該当する情報又は対策重要度Ⅱに該当し、かつ特に機密性を求められる情報（以下「重要情報」という。）について、暗号化又はパスワードの設定等を行った上で管理するものとする。 カ　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) 情報の取扱い ア　情報の作成 (ｱ) 情報を作成する職員等は、情報の作成時に(1)の分類に基づき情報を分類し取り扱うものとする。 (ｲ) 情報を作成する職員等は、作成途中の情報についても、紛失、流出等を防止するために必要な措置を講じるものとする。また、情報の作成途中で不要になった場合は、当該情報を消去するものとする。 イ　情報の入手 (ｱ) 他所属の職員等が作成した情報を入手した職員等は、入手元の情報の分類に基づいた取扱いをするものとする。 (ｲ) 外部の者が作成した情報を入手した職員等は、(1)の分類に基づき情報を分類し取り扱うものとする。 (ｳ) 情報を入手した職員等は、入手した情報の分類が不明な場合、情報セキュリティ管理者に判断を仰ぐものとする。	エ　情報セキュリティ管理者は、重要度に応じて、各々の情報にアクセスできる職員等及びアクセス権限を定めるものとする。 オ　情報セキュリティ管理者は、対策重要度Ⅰに該当する情報又は対策重要度Ⅱに該当し、かつ特に機密性を求められる情報（以下「重要情報」という。）について、暗号化又はパスワードの設定等を行った上で管理するものとする。 カ　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) 情報の取扱い ア　情報の作成 (ｱ) 情報を作成する職員等は、情報の作成時に(1)の分類に基づき情報を分類し取り扱うものとする。 (ｲ) 情報を作成する職員等は、作成途中の情報についても、紛失、流出等を防止するために必要な措置を講じるものとする。また、情報の作成途中で不要になった場合は、当該情報を消去するものとする。 イ　情報の入手 (ｱ) 他所属の職員等が作成した情報を入手した職員等は、入手元の情報の分類に基づいた取扱いをするものとする。 (ｲ) 外部の者が作成した情報を入手した職員等は、(1)の分類に基づき情報を分類し取り扱うものとする。 (ｳ) 情報を入手した職員等は、入手した情報の分類が不明な場合、情報セキュリティ管理者に判断を仰ぐものとする。

ウ　情報の利用 (ｱ) 情報を利用する職員等は、業務以外の目的に情報を利用してはならない。 (ｲ) 情報を利用する職員等は、情報の分類に従って、適切な取扱いをするものとする。 (ｳ) 情報を利用する職員等は、記録媒体に情報の分類が異なる情報が複数記録されている場合には、最高度の分類に従って、当該記録媒体を取り扱うものとする。 (ｴ) 情報セキュリティ管理者は、庁舎外に持ち出される記録媒体等について、庁舎外での使用方法を定め、管理簿を設ける等、適切に管理するものとする。 エ　情報の保管 (ｱ) 情報セキュリティ管理者は、情報の分類に従って、情報を記録した記録媒体を適切に保管するものとする。 (ｲ) 情報セキュリティ管理者は、最終的に確定した情報を記録した記録媒体について、書込み禁止措置を行った上で保管するものとする。 (ｳ) 情報セキュリティ管理者は、防災対策を必要とするファイル等について、全て別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管するものとする。 (ｴ) 情報セキュリティ管理者は、重要情報を記録した記録媒体について、耐火、耐熱、耐水及び耐湿の対策を講じた施錠可能な場所に保管するものとする。 オ　情報の運搬 (ｱ) 職員等は、重要情報を、情報システム等の設置場所と外部の保管場所等との間で運搬する場合には、情報セキュリティ管理者に許可を得るものとする。	ウ　情報の利用 (ｱ) 情報を利用する職員等は、業務以外の目的に情報を利用してはならない。 (ｲ) 情報を利用する職員等は、情報の分類に従って、適切な取扱いをするものとする。 (ｳ) 情報を利用する職員等は、記録媒体に情報の分類が異なる情報が複数記録されている場合には、最高度の分類に従って、当該記録媒体を取り扱うものとする。 (ｴ) 情報セキュリティ管理者は、庁舎外に持ち出される記録媒体等について、庁舎外での使用方法を定め、管理簿を設ける等、適切に管理するものとする。 エ　情報の保管 (ｱ) 情報セキュリティ管理者は、情報の分類に従って、情報を記録した記録媒体を適切に保管するものとする。 (ｲ) 情報セキュリティ管理者は、最終的に確定した情報を記録した記録媒体について、書込み禁止措置を行った上で保管するものとする。 (ｳ) 情報セキュリティ管理者は、防災対策を必要とするファイル等について、全て別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管するものとする。 (ｴ) 情報セキュリティ管理者は、重要情報を記録した記録媒体について、耐火、耐熱、耐水及び耐湿の対策を講じた施錠可能な場所に保管するものとする。 オ　情報の運搬 (ｱ) 職員等は、重要情報を、情報システム等の設置場所と外部の保管場所等との間で運搬する場合には、情報セキュリティ管理者に許可を得るものとする。

(ｲ) 情報セキュリティ管理者は、車両等により重要情報を運搬する場合には、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、情報の不正利用を防止するための措置を講じるものとする。 カ　情報の提供 情報セキュリティ管理者は、患者等に提供する情報について、完全性を確保するために必要な措置を講じるものとする。 キ　情報の廃棄 職員等は、重要情報を記録していた可能性のある記録媒体を廃棄する場合には、当該記録媒体の情報を復元できないように破断等の復元防止措置を講じた上で廃棄するものとする。廃棄に当たっては、情報セキュリティ管理者の許可を得ることとし、処理の日時、担当者及び復元防止措置の内容を記録するものとする。	(ｲ) 情報セキュリティ管理者は、車両等により重要情報を運搬する場合には、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、情報の不正利用を防止するための措置を講じるものとする。 カ　情報の提供 情報セキュリティ管理者は、患者等に提供する情報について、完全性を確保するために必要な措置を講じるものとする。 キ　情報の廃棄 職員等は、重要情報を記録していた可能性のある記録媒体を廃棄する場合には、当該記録媒体の情報を復元できないように破断等の復元防止措置を講じた上で廃棄するものとする。廃棄に当たっては、情報セキュリティ管理者の許可を得ることとし、処理の日時、担当者及び復元防止措置の内容を記録するものとする。
4　物理的対策 (1) 管理区域 ア　管理区域の構造等 (ｱ) ネットワークの基幹機器及び重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱う情報システムが設置され、当該機器及び情報システムの管理及び運用を行うための情報システム室並びに記録媒体の保管庫（以下「管理区域」という。）は、水害対策及び入退室管理を確実に行うために、可能な限り地階又は１階に設けてはならない。また、外部からの侵入が容易にできないように、可能な限り無窓の外壁等にするものとする。	4　物理的対策 (1) 管理区域 ア　管理区域の構造等 (ｱ) ネットワークの基幹機器及び重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱う情報システムが設置され、当該機器及び情報システムの管理及び運用を行うための情報システム室並びに記録媒体の保管庫（以下「管理区域」という。）は、水害対策及び入退室管理を確実に行うために、可能な限り地階又は１階に設けてはならない。また、外部からの侵入が容易にできないように、可能な限り無窓の外壁等にするものとする。

(ｲ) 管理区域から外部に通ずるドアは必要最小限の箇所に設けるものとし、全てのドアは、制御機能、鍵、警報装置等によって、許可されていない者の立入りを防止できるようにするものとする。 (ｳ) 情報システム室には、必要に応じてビデオカメラ等の監視機能を設置するものとする。 (ｴ) 情報システム室内の機器等は、耐震対策を講じた場所に設置するとともに、防火措置等を講じるものとする。なお、情報システム室内の機器等の配置は、緊急時に職員等及び委託事業者の従業員が円滑に避難できるように配慮するものとする。 (ｵ) 管理区域を囲む外壁等の床下開口部は全て塞ぐものとする。 (ｶ) 管理区域に配置する消火剤は機器等及び記録媒体に影響を与えないものを使用するものとする。 イ 管理区域の入退室管理 (ｱ) 情報システム管理者等は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行うものとする。 (ｲ) 職員等及び委託事業者の従業員は、管理区域に入室する場合には、身分証明書等を携帯し、求めにより提示するものとする。 (ｳ) 情報システム管理者等は、外部からの訪問者が管理区域に入る場合には、必要に応じて管理区域内の立入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じるものとする。	(ｲ) 管理区域から外部に通ずるドアは必要最小限の箇所に設けるものとし、全てのドアは、制御機能、鍵、警報装置等によって、許可されていない者の立入りを防止できるようにするものとする。 (ｳ) 情報システム室には、必要に応じてビデオカメラ等の監視機能を設置するものとする。 (ｴ) 情報システム室内の機器等は、耐震対策を講じた場所に設置するとともに、防火措置等を講じるものとする。なお、情報システム室内の機器等の配置は、緊急時に職員等及び委託事業者の従業員が円滑に避難できるように配慮するものとする。 (ｵ) 管理区域を囲む外壁等の床下開口部は全て塞ぐものとする。 (ｶ) 管理区域に配置する消火剤は機器等及び記録媒体に影響を与えないものを使用するものとする。 イ 管理区域の入退室管理 (ｱ) 情報システム管理者等は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行うものとする。 (ｲ) 職員等及び委託事業者の従業員は、管理区域に入室する場合には、身分証明書等を携帯し、求めにより提示するものとする。 (ｳ) 情報システム管理者等は、外部からの訪問者が管理区域に入る場合には、必要に応じて管理区域内の立入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じるものとする。

(ｴ) 情報システム管理者等は、管理区域に設置する情報システム等に関連しないコンピュータ、通信回線装置、記録媒体等を持ち込ませないようにするものとする。 ウ　機器等の搬入 (ｱ) 情報システム管理者等は、搬入する機器が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせるものとする。 (ｲ) 機器等及びそれらに用いる物品の搬入には情報システム管理者等が指定した職員等が同行する等の必要な措置を講じるものとする。 (2) 機器の設置 ア　機器の設置等 (ｱ) サーバ等の機器は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定等の必要な措置を講じるものとする。 (ｲ) 情報システム管理者等は、サーバ等の機器について、情報システム管理者等及び契約により操作を認められた委託事業者の従業員以外の者が容易に操作できないような措置を講じるものとする。 (ｳ) 重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱うサーバについては、原則として、二重化すること等により常に同一データを保持し、現用機に障害が発生した場合は速やかに予備機に移行させ、情報システム等の運用が停止しないようにするものとする。なお、運用上支障がないと判断される場合には、RAID によるディスクの冗長化構成及び定期的なバックアップデータの取得などにより、機器障害による	(ｴ) 情報システム管理者等は、管理区域に設置する情報システム等に関連しないコンピュータ、通信回線装置、記録媒体等を持ち込ませないようにするものとする。 ウ　機器等の搬入 (ｱ) 情報システム管理者等は、搬入する機器が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせるものとする。 (ｲ) 機器等及びそれらに用いる物品の搬入には情報システム管理者等が指定した職員等が同行する等の必要な措置を講じるものとする。 (2) 機器の設置 ア　機器の設置等 (ｱ) サーバ等の機器は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定等の必要な措置を講じるものとする。 (ｲ) 情報システム管理者等は、サーバ等の機器について、情報システム管理者等及び契約により操作を認められた委託事業者の従業員以外の者が容易に操作できないような措置を講じるものとする。 (ｳ) 重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱うサーバについては、原則として、二重化すること等により常に同一データを保持し、現用機に障害が発生した場合は速やかに予備機に移行させ、情報システム等の運用が停止しないようにするものとする。なお、運用上支障がないと判断される場合には、RAID によるディスクの冗長化構成及び定期的なバックアップデータの取得などにより、機器障害による

システム等の停止を最小限に抑える対策を講じるものとする。 (ｴ) 情報システム管理者等は、サーバ等の機器について、定期保守を実施するものとする。 イ　電源 (ｱ) 情報システム管理者等は、重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱うサーバ等の機器の電源について、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けるものとする。 (ｲ) 情報システム管理者等は、落雷等による過電流に対してサーバ等の機器を保護するための措置を講じるものとする。 ウ　配線 (ｱ) ネットワーク管理者及び情報システム管理者は、配線について、傍受、損傷等を受けることがないように可能な限り必要な措置を講じるものとする。 (ｲ) ネットワーク管理者は、ネットワーク幹線の配線を定期的に点検するものとする。 (ｳ) ネットワーク管理者は、ネットワーク接続口(ハブのポート等)を、情報セキュリティ管理者が常時目視管理できる場所又はネットワーク管理者及び契約により操作を認められた委託事業者の従業員以外の者が容易に操作できない場所に設置するものとする。 (ｴ) ネットワーク管理者は、ネットワーク管理者及び契約により操作を認められた委託事業者の従業員以外の者が、ネットワーク幹線の配線を変更又は追加できないように必要な措置を講じるものとする。	システム等の停止を最小限に抑える対策を講じるものとする。 (ｴ) 情報システム管理者等は、サーバ等の機器について、定期保守を実施するものとする。 イ　電源 (ｱ) 情報システム管理者等は、重要情報のうち対策重要度Ⅰに該当し、かつ特に可用性を求められる情報を取り扱うサーバ等の機器の電源について、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けるものとする。 (ｲ) 情報システム管理者等は、落雷等による過電流に対してサーバ等の機器を保護するための措置を講じるものとする。 ウ　配線 (ｱ) ネットワーク管理者及び情報システム管理者は、配線について、傍受、損傷等を受けることがないように可能な限り必要な措置を講じるものとする。 (ｲ) ネットワーク管理者は、ネットワーク幹線の配線を定期的に点検するものとする。 (ｳ) ネットワーク管理者は、ネットワーク接続口(ハブのポート等)を、情報セキュリティ管理者が常時目視管理できる場所又はネットワーク管理者及び契約により操作を認められた委託事業者の従業員以外の者が容易に操作できない場所に設置するものとする。 (ｴ) ネットワーク管理者は、ネットワーク管理者及び契約により操作を認められた委託事業者の従業員以外の者が、ネットワーク幹線の配線を変更又は追加できないように必要な措置を講じるものとする。

エ　外部に設置する機器 情報システム管理者等は、執務室等以外に設置する機器の情報セキュリティ水準を定期的に確認するものとする。 (3) 端末の管理 ア　執務室等に職員等及び委託事業者の従業員がいない場合は、執務室等の施錠等による盗難防止措置を講じるものとする。 イ　執務室等の端末は、ワイヤーによる固定等、盗難防止のための物理的措置を講じるものとする。 ウ　コンピュータ管理者は、BIOS パスワード、ハードディスクパスワード等を併用するものとする。 エ　情報システム管理者は、情報システムにログインパスワードの入力が必要となるよう設定するものとする。 オ　コンピュータ管理者は、庁舎外に持ち出される端末について、庁舎外での使用方法を定め、管理簿を設ける等、適切に管理するものとする。 カ　情報システム管理者等は、機器の廃棄、修理、リース返却等を行う場合には、機器内部の記憶装置からすべての情報を消去の上、復元不可能な状態にするものとする。また、情報システム管理者等は、委託事業者に機器を修理させる場合において、情報を消去することが難しいときは、秘密を守ることを契約に定めるものとする。 (4) 通信回線及び通信回線装置の管理 ア　ネットワーク管理者は、庁舎内の通信回線及び通信回線装置を適切に管理するものとする。 イ　ネットワーク管理者は、情報セキュリティ対策基準の適用範囲外のネットワーク（以下「外部ネットワーク」という。）との接続は必要最小限のものに限定し、可能な限り	エ　外部に設置する機器 情報システム管理者等は、執務室等以外に設置する機器の情報セキュリティ水準を定期的に確認するものとする。 (3) 端末の管理 ア　執務室等に職員等及び委託事業者の従業員がいない場合は、執務室等の施錠等による盗難防止措置を講じるものとする。 イ　執務室等の端末は、ワイヤーによる固定等、盗難防止のための物理的措置を講じるものとする。 ウ　コンピュータ管理者は、BIOS パスワード、ハードディスクパスワード等を併用するものとする。 エ　情報システム管理者は、情報システムにログインパスワードの入力が必要となるよう設定するものとする。 オ　コンピュータ管理者は、庁舎外に持ち出される端末について、庁舎外での使用方法を定め、管理簿を設ける等、適切に管理するものとする。 カ　情報システム管理者等は、機器の廃棄、修理、リース返却等を行う場合には、機器内部の記憶装置からすべての情報を消去の上、復元不可能な状態にするものとする。また、情報システム管理者等は、委託事業者に機器を修理させる場合において、情報を消去することが難しいときは、秘密を守ることを契約に定めるものとする。 (4) 通信回線及び通信回線装置の管理 ア　ネットワーク管理者は、庁舎内の通信回線及び通信回線装置を適切に管理するものとする。 イ　ネットワーク管理者は、情報セキュリティ対策基準の適用範囲外のネットワーク（以下「外部ネットワーク」という。）との接続は必要最小限のものに限定し、可能な限り

接続ポイントを減らすものとする。 ウ　ネットワーク管理者は、ネットワークに使用する回線について、伝送途上において情報の破壊、盗聴、改ざん、消去等が生じないように十分な情報セキュリティ対策を実施するものとする。 エ　ネットワーク管理者は、重要情報を取り扱う情報システムに通信回線を接続する場合には、必要な情報セキュリティ水準を検討の上、適切な回線を選択するものとする。また、必要に応じ、送受信される情報の暗号化を行うものとする。	接続ポイントを減らすものとする。 ウ　ネットワーク管理者は、ネットワークに使用する回線について、伝送途上において情報の破壊、盗聴、改ざん、消去等が生じないように十分な情報セキュリティ対策を実施するものとする。 エ　ネットワーク管理者は、重要情報を取り扱う情報システムに通信回線を接続する場合には、必要な情報セキュリティ水準を検討の上、適切な回線を選択するものとする。また、必要に応じ、送受信される情報の暗号化を行うものとする。
5　人的対策 (1) 職員等の遵守事項 ア　業務目的以外の使用の禁止 (ｱ) 職員等は、業務目的以外での情報システムへのアクセス、電子メールの使用及びホームページの閲覧を行ってはならない。 (ｲ) ネットワーク管理者は、職員等が業務目的以外でホームページを閲覧した場合には、当該職員等が所属する所属の情報セキュリティ管理者に通知し、適切な措置を求めるものとする。 (ｳ) (ｲ)の要請にもかかわらず、職員等の業務目的以外でのホームページ閲覧が改善されない場合には、ネットワーク管理者は、当該職員等のホームページ閲覧を停止することができる。 (ｴ) ネットワーク管理者は、職員等のホームページ閲覧を停止した場合には、統括情報セキュリティ管理者及び当該職員等が所属する所属の情報セキュリティ管理者に	5　人的対策 (1) 職員等の遵守事項 ア　業務目的以外の使用の禁止 (ｱ) 職員等は、業務目的以外での情報システムへのアクセス、電子メールの使用及びホームページの閲覧を行ってはならない。 (ｲ) ネットワーク管理者は、職員等が業務目的以外でホームページを閲覧した場合には、当該職員等が所属する所属の情報セキュリティ管理者に通知し、適切な措置を求めるものとする。 (ｳ) (ｲ)の要請にもかかわらず、職員等の業務目的以外でのホームページ閲覧が改善されない場合には、ネットワーク管理者は、当該職員等のホームページ閲覧を停止することができる。 (ｴ) ネットワーク管理者は、職員等のホームページ閲覧を停止した場合には、統括情報セキュリティ管理者及び当該職員等が所属する所属の情報セキュリティ管理者に

その旨を通知するものとする。 イ　端末等の持ち出し及び庁舎外における情報の取扱いの制限 (ｱ) 職員等は、端末を執務室以外に持ち出す場合にはコンピュータ管理者の許可を、外部記録媒体を持ち出す場合には情報セキュリティ管理者の許可を得るものとする。 (ｲ) 職員等は、庁舎外でコンピュータを用いて情報を取り扱う場合には、情報セキュリティ管理者の許可を得るものとする。 ウ　パソコン等の持込 職員等は、原則として、業務に使用する目的で私物のパソコン等及び記録媒体を庁舎内に持ち込んではならない。 エ　端末におけるセキュリティ設定変更の禁止 職員等は、端末のソフトウエアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。 オ　机上の端末等の管理 職員等は、端末及び記録媒体が、他者に使用され、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末のロック、記録媒体の保管等の適切な措置を講じるものとする。 (2) 契約職員、非常勤職員、短期非常勤職員、派遣労働者及び業務の一部を委嘱される者への対応 ア　インターネット接続、電子メール使用等の制限 情報セキュリティ管理者は、契約職員、非常勤職員、短期非常勤職員及び派遣労働者に端末による作業を行わせる場合において、インターネットへの接続、電子メールの使用等が必要でないときは、コンピュータ管理者又はネッ	その旨を通知するものとする。 イ　端末等の持ち出し及び庁舎外における情報の取扱いの制限 (ｱ) 職員等は、端末を執務室以外に持ち出す場合にはコンピュータ管理者の許可を、外部記録媒体を持ち出す場合には情報セキュリティ管理者の許可を得るものとする。 (ｲ) 職員等は、庁舎外でコンピュータを用いて情報を取り扱う場合には、情報セキュリティ管理者の許可を得るものとする。 ウ　パソコン等の持込 職員等は、原則として、業務に使用する目的で私物のパソコン等及び記録媒体を庁舎内に持ち込んではならない。 エ　端末におけるセキュリティ設定変更の禁止 職員等は、端末のソフトウエアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。 オ　机上の端末等の管理 職員等は、端末及び記録媒体が、他者に使用され、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末のロック、記録媒体の保管等の適切な措置を講じるものとする。 (2) 契約職員等への対応 ア　インターネット接続、電子メール使用等の制限 情報セキュリティ管理者は、契約職員、非常勤職員、短期非常勤職員及び派遣労働者に端末による作業を行わせる場合において、インターネットへの接続、電子メールの使用等が必要でないときは、コンピュータ管理者又はネッ

トワーク管理者に依頼してこれらを利用できないようにするものとする。 イ　情報セキュリティポリシー等の遵守に対する同意 情報セキュリティ管理者は、法人の業務の一部を委嘱する場合において、端末等による作業を伴う等必要に応じて、情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。 (3) 研修及び訓練 ア　統括情報セキュリティ管理者は、毎年度、職員等に対する情報セキュリティに関する研修計画を定め、職員等が情報セキュリティに関する研修を受講できるようにするものとする。 イ　統括情報セキュリティ管理者は、新規採用の職員を対象とする情報セキュリティに関する研修を所属と協力して実施するものとする。 ウ　研修は、情報セキュリティ管理者、情報システム管理者等及びその他の職員等に対し、それぞれの役割に応じた内容とする。 エ　情報システム管理者等は緊急時対応を想定した訓練を職員等及び委託事業者の従業員に計画的に行わせるものとする。訓練の計画に当たっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めるとともに、より効果的に実施できるよう計画を立てるものとする。 (4) IC カード等の管理 ア　職員等は、自己の保有する IC カード等に関し、次の事項を遵守するものとする。 (ｱ) 職員等の個人認証に用いる IC カード等は、職員等の	トワーク管理者に依頼してこれらを利用できないようにするものとする。 イ　情報セキュリティポリシー等の遵守に対する同意 情報セキュリティ管理者は、機構の業務の一部を委嘱する場合において、端末等による作業を伴う等、必要な場合には、委嘱の際、情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。 (3) 研修及び訓練 ア　統括情報セキュリティ管理者は、毎年度、職員等に対する情報セキュリティに関する研修計画を定め、職員等が情報セキュリティに関する研修を受講できるようにするものとする。 イ　統括情報セキュリティ管理者は、新規採用の職員を対象とする情報セキュリティに関する研修を所属と協力して実施するものとする。 ウ　研修は、情報セキュリティ管理者、情報システム管理者等及びその他の職員等に対し、それぞれの役割に応じた内容とする。 エ　情報システム管理者等は緊急時対応を想定した訓練を職員等及び委託事業者の従業員に計画的に行わせるものとする。訓練の計画に当たっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めるとともに、より効果的に実施できるよう計画を立てるものとする。 (4) IC カード等の管理 ア　職員等は、自己の保有する IC カード等に関し、次の事項を遵守するものとする。 (ｱ) 職員等の個人認証に用いる IC カード等は、職員等の

間で共有しないこと。 (ｲ) 業務上必要のない場合には、IC カード等をカードリーダ又は端末等のスロット等から抜いておくこと。 (ｳ) IC カード等を紛失した場合には、速やかに当該 IC カード等を発行した情報システム管理者に報告し、指示を仰ぐこと。 イ　情報システム管理者は、IC カード等の紛失の報告があった場合には、速やかに当該 IC カード等の効力を停止するものとする。 ウ　情報システム管理者は、IC カード等を切り替える場合には、切替え前の IC カード等を回収し、破砕する等復元不可能な処理を行った上で廃棄するものとする。 (5) ID 及びパスワードの管理 職員等は、自己の保有する ID 及びパスワードに関し、次の事項を遵守するものとする。 ア　自己が利用している ID を他人に利用させないこと。 イ　共用 ID を利用する場合、共用 ID の利用者以外に利用させないこと。 ウ　パスワードを秘密にし、パスワードの照会等には一切応じないこと。 エ　パスワードのメモを作らないこと。 オ　パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。 カ　情報システムへの侵入の危険又はパスワード漏えいの恐れがある場合には、パスワードを速やかに変更すること。 キ　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、古いパスワードの再利用はしないこと。	間で共有しないこと。 (ｲ) 業務上必要のない場合には、IC カード等をカードリーダ又は端末等のスロット等から抜いておくこと。 (ｳ) IC カード等を紛失した場合には、速やかに当該 IC カード等を発行した情報システム管理者に報告し、指示を仰ぐこと。 イ　情報システム管理者は、IC カード等の紛失の報告があった場合には、速やかに当該 IC カード等の効力を停止するものとする。 ウ　情報システム管理者は、IC カード等を切り替える場合には、切替え前の IC カード等を回収し、破砕する等復元不可能な処理を行った上で廃棄するものとする。 (5) ID 及びパスワードの管理 職員等は、自己の保有する ID 及びパスワードに関し、次の事項を遵守するものとする。 ア　自己が利用している ID を他人に利用させないこと。 イ　共用 ID を利用する場合、共用 ID の利用者以外に利用させないこと。 ウ　パスワードを秘密にし、パスワードの照会等には一切応じないこと。 エ　パスワードのメモを作らないこと。 オ　パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。 カ　情報システムへの侵入の危険又はパスワード漏えいの恐れがある場合には、パスワードを速やかに変更すること。 キ　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、古いパスワードの再利用はしないこと。

ク　仮のパスワードは、最初のログイン時点で変更すること。 ケ　端末にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。 コ　共有 ID 利用時を除き、職員等の間でパスワードを共有しないこと。	ク　仮のパスワードは、最初のログイン時点で変更すること。 ケ　端末にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。 コ　共有 ID 利用時を除き、職員等の間でパスワードを共有しないこと。
6　技術的対策 (1) 情報システム等の管理 ア　アクセス記録等の取得等 重要情報を取り扱う情報システム等に対し、次の措置を講じるものとする。 (ｱ) 情報システム管理者等は、情報セキュリティの確保に必要なアクセス記録、システム稼動記録、障害時のシステム出力記録等（以下「アクセス記録等」という。）を取得し、一定の期間保存するものとする。また、必要に応じ、外部記録媒体にバックアップするものとする。 (ｲ) 情報システム管理者等は、アクセス記録等が窃取、改ざん又は消去されないように必要な措置を講じるものとする。 (ｳ) 情報システム管理者等は、定期的にアクセス記録等を分析及び監視するものとする。 イ　情報システム等における運用管理の記録及び作業の確認 (ｱ) 情報システム管理者等は、所管する情報システム等において行った変更等の処理及び当該情報システム等の運用等において行った作業の記録を作成し、適切に管理	6　技術的対策 (1) 情報システム等の管理 ア　アクセス記録等の取得等 重要情報を取り扱う情報システム等に対し、次の措置を講じるものとする。 (ｱ) 情報システム管理者等は、情報セキュリティの確保に必要なアクセス記録、システム稼動記録、障害時のシステム出力記録等（以下「アクセス記録等」という。）を取得し、一定の期間保存するものとする。また、必要に応じ、外部記録媒体にバックアップするものとする。 (ｲ) 情報システム管理者等は、アクセス記録等が窃取、改ざん又は消去されないように必要な措置を講じるものとする。 (ｳ) 情報システム管理者等は、定期的にアクセス記録等を分析及び監視するものとする。 イ　情報システム等における運用管理の記録及び作業の確認 (ｱ) 情報システム管理者等は、所管する情報システム等において行った変更等の処理及び当該情報システム等の運用等において行った作業の記録を作成し、適切に管理

するものとする。 (ｲ) 情報システム管理者等及び契約により操作を認められた委託事業者の従業員が担当する情報システム等において変更等の重要な作業を行う場合には、２名以上で作業し、互いにその作業を確認するものとする。また、作業する者が委託事業者の従業員のみの場合は、職員等が立ち会うものとする。 ウ　障害記録 情報システム管理者等は、職員等から報告のあった情報システム等の障害に対する処理、問題等を障害記録として体系的に記録し、常に活用できるよう保存するものとする。 エ　情報システム仕様書等の管理 情報システム管理者等は、ネットワーク構成図、情報システム仕様書等について、業務上必要とする者のみが閲覧できる場所に保管するものとする。また、情報システム等の開発、保守又は運用を委託事業者に委託した場合、当該委託事業者に守秘義務を課すものとする。 オ　バックアップ 情報システム管理者等は、ファイルサーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にバックアップ用の複製を作成するものとする。 カ　電子メール (ｱ) ネットワーク管理者は、所管する電子メールサーバについて外部から外部への電子メールの中継処理が行われないよう、電子メールサーバの設定を行うものとする。 (ｲ) ネットワーク管理者は、電子メールの送受信容量の上	するものとする。 (ｲ) 情報システム管理者等及び契約により操作を認められた委託事業者の従業員が担当する情報システム等において変更等の重要な作業を行う場合には、２名以上で作業し、互いにその作業を確認するものとする。また、作業する者が委託事業者の従業員のみの場合は、職員等が立ち会うものとする。 ウ　障害記録 情報システム管理者等は、職員等から報告のあった情報システム等の障害に対する処理、問題等を障害記録として体系的に記録し、常に活用できるよう保存するものとする。 エ　情報システム仕様書等の管理 情報システム管理者等は、ネットワーク構成図、情報システム仕様書等について、業務上必要とする者のみが閲覧できる場所に保管するものとする。また、情報システム等の開発、保守又は運用を委託事業者に委託した場合、当該委託事業者に守秘義務を課すものとする。 オ　バックアップ 情報システム管理者等は、ファイルサーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にバックアップ用の複製を作成するものとする。 カ　電子メール (ｱ) ネットワーク管理者は、所管する電子メールサーバについて外部から外部への電子メールの中継処理が行われないよう、電子メールサーバの設定を行うものとする。 (ｲ) ネットワーク管理者は、電子メールの送受信容量の上

限を設定し、上限を超える電子メールの送受信をできないようにするものとする。 (ｳ) ネットワーク管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知するとともに、電子メールの総量が定められた容量未満になるまで一時的に当該職員等の電子メールの利用を停止するものとする。 (ｴ) ネットワーク管理者は、情報システムの開発、運用等のために庁舎内で業務を行う委託事業者の従業員による電子メールアドレス利用方法を定めるものとする。 (ｵ) 職員等は、業務上必要のない送信先に電子メールを送信してはならない。 (ｶ) 職員等は、原則として、業務用に与えられた電子メールアドレスあての電子メールを外部の電子メールアドレスに自動転送しないものとする。業務上、外部の電子メールアドレスへ自動転送を必要とする場合は、ネットワーク管理者の許可を得るものとする。 (ｷ) 職員等は、原則として、電子メールで重要情報（あて先の情報及び発信者に係る情報を除く。）を送ってはならない。業務上必要に応じて、ネットワーク管理者が定める暗号化等の機密性確保のための措置を講じるものとする。 (ｸ) 職員等は、ネットワーク管理者が定める容量を超える電子メールの送信を行ってはならない。 (ｹ) 職員等は、受信済みの電子メールを電子メールボックスから削除するものとする。 (ｺ) 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、受信者相互の電子メールアドレスが	限を設定し、上限を超える電子メールの送受信をできないようにするものとする。 (ｳ) ネットワーク管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知するとともに、電子メールの総量が定められた容量未満になるまで一時的に当該職員等の電子メールの利用を停止するものとする。 (ｴ) ネットワーク管理者は、情報システムの開発、運用等のために庁舎内で業務を行う委託事業者の従業員による電子メールアドレス利用方法を定めるものとする。 (ｵ) 職員等は、業務上必要のない送信先に電子メールを送信してはならない。 (ｶ) 職員等は、原則として、業務用に与えられた電子メールアドレスあての電子メールを外部の電子メールアドレスに自動転送しないものとする。業務上、外部の電子メールアドレスへ自動転送を必要とする場合は、ネットワーク管理者の許可を得るものとする。 (ｷ) 職員等は、原則として、電子メールで重要情報（あて先の情報及び発信者に係る情報を除く。）を送ってはならない。業務上必要がある場合には、ネットワーク管理者が定める暗号化等の機密性確保のための措置を講じるものとする。 (ｸ) 職員等は、ネットワーク管理者が定める容量を超える電子メールの送信を行ってはならない。 (ｹ) 職員等は、受信済みの電子メールを電子メールボックスから削除するものとする。 (ｺ) 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、受信者相互の電子メールアドレスが

分からないようにするものとする。 (ｻ) 職員等は、重要情報を含む電子メールを誤送信した場合、情報セキュリティ管理者に報告するものとする。 (ｼ) 職員等は、定められたもの以外の電子メールを使用してはならない。 キ　ファイルサーバ (ｱ) 情報セキュリティ管理者は、ソフトウェアの導入状況について、ソフトウェア管理台帳を設け、適切に管理するものとする。 (ｲ) 情報システム管理者等は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知するものとする。 (ｳ) 情報システム管理者等は、必要に応じてファイルサーバを所属等の単位で構成し、他所属等のフォルダ及びファイルを閲覧又は使用できないように設定するものとする。 (ｴ) 情報セキュリティ管理者は、同一所属等であっても、患者等の個人情報等特定の職員等しか取り扱うことができない情報については、別途フォルダを作成し、担当職員等以外の職員等が閲覧又は使用できないように設定するものとする。 ク　電子署名及び暗号化 (ｱ) 情報システム管理者等は、法人外に送る情報については、機密性を担保することが必要な場合には暗号化の措置を、完全性を担保することが必要な場合には電子署名の措置を講じて、送信するものとする。 (ｲ) 職員等は、情報システム管理者等が定める方法により暗号化及び暗号鍵の管理を行うものとする。	分からないようにするものとする。 (ｻ) 職員等は、重要情報を含む電子メールを誤送信した場合、情報セキュリティ管理者に報告するものとする。 (ｼ) 職員等は、定められたもの以外の電子メールを使用してはならない。 キ　ファイルサーバ (ｱ) 情報セキュリティ管理者は、ソフトウェアの導入状況について、ソフトウェア管理台帳を設け、適切に管理するものとする。 (ｲ) 情報システム管理者等は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知するものとする。 (ｳ) 情報システム管理者等は、必要に応じてファイルサーバを所属等の単位で構成し、他所属等のフォルダ及びファイルを閲覧又は使用できないように設定するものとする。 (ｴ) 情報セキュリティ管理者は、同一所属等であっても、患者等の個人情報等特定の職員等しか取り扱うことができない情報については、別途フォルダを作成し、担当職員等以外の職員等が閲覧又は使用できないように設定するものとする。 ク　電子署名及び暗号化 (ｱ) 情報システム管理者等は、機構以外に送る情報について、機密性を担保することが必要な場合には暗号化の措置を、完全性を担保することが必要な場合には電子署名の措置を講じて送信させるものとする。 (ｲ) 職員等は、情報システム管理者等が定める方法により暗号化及び暗号鍵の管理を行うものとする。

ケ　無許可でのソフトウエアの導入等の禁止 (ｱ) 職員等は、業務上の必要から標準実装以外のソフトウエアを端末にインストールする場合には、コンピュータ管理者の許可を得るものとする。 　コンピュータ管理者は、ネットワーク及び情報システムへの影響をネットワーク管理者及び情報システム管理者に照会した上で可否を決定するものとする。 (ｲ) 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。 (ｳ) コンピュータ管理者は、端末におけるソフトウエアの変更状況等について、サーバにより監視するものとする。 コ　端末の改造の禁止 (ｱ) 職員等は、端末の改造をしてはならない。 (ｲ) 職員等は、業務を遂行するために端末に対して部品の増設又は交換を行う等の必要がある場合は、コンピュータ管理者の許可を得るものとする。 　コンピュータ管理者は、ネットワーク管理者及び情報システム管理者にネットワーク及び情報システムへの影響を照会した上で可否を決定するものとする。 サ　無許可でのネットワーク接続の禁止 (ｱ) 職員等は、ネットワーク管理者の許可なく端末等をネットワークに接続してはならない。 (ｲ) ネットワーク管理者は、端末等が適切に管理されることを確認した上で接続を許可するものとする。 シ　患者等が利用する情報システム等の分離等 (ｱ) 情報システム管理者等は、患者等が直接利用する情報システム等と、情報セキュリティ対策基準の対象となる	ケ　無許可でのソフトウエアの導入等の禁止 (ｱ) 職員等は、業務上の必要から標準実装以外のソフトウエアを端末にインストールする場合には、コンピュータ管理者の許可を得るものとする。 　コンピュータ管理者は、ネットワーク及び情報システムへの影響をネットワーク管理者及び情報システム管理者に照会した上で可否を決定するものとする。 (ｲ) 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。 (ｳ) コンピュータ管理者は、端末におけるソフトウエアの変更状況等について、サーバにより監視するものとする。 コ　端末の改造の禁止 (ｱ) 職員等は、端末の改造をしてはならない。 (ｲ) 職員等は、業務を遂行するために端末に対して部品の増設又は交換を行う等の必要がある場合は、コンピュータ管理者の許可を得るものとする。 　コンピュータ管理者は、ネットワーク管理者及び情報システム管理者にネットワーク及び情報システムへの影響を照会した上で可否を決定するものとする。 サ　無許可でのネットワーク接続の禁止 (ｱ) 職員等は、ネットワーク管理者の許可なく端末等をネットワークに接続してはならない。 (ｲ) ネットワーク管理者は、端末等が適切に管理されることを確認した上で接続を許可するものとする。 シ　患者等が利用する情報システム等の分離等 (ｱ) 情報システム管理者等は、患者等が直接利用する情報システム等と、情報セキュリティ対策基準の対象となる

情報システム等を物理的に分ける等、特に強固な情報セキュリティ対策をとるものとする。 (ｲ) 患者等が直接利用する端末については、必要最小限の機能に限定した専用端末とする。 ス　ネットワーク (ｱ) ネットワーク管理者は、ネットワークを構築する場合は、統括情報セキュリティ管理者と協議するものとする。また、変更又は廃止する場合も同様とする。 (ｲ) ネットワーク管理者は、適切な管理下で接続を行い、情報セキュリティに留意したネットワーク構成を採るものとする。 (ｳ) ネットワーク管理者は、ウェブサーバ等をインターネットに公開する場合、内部ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続するものとする。 (ｴ) ネットワーク管理者は、接続した外部ネットワークの情報セキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ管理者の判断に従い速やかに当該外部ネットワークとの接続を遮断するものとする。 セ　ネットワークの盗聴対策 (ｱ) ネットワーク管理者は、無線 LAN の利用を認める場合には、暗号化及び認証技術の使用を義務づけるものとする。 (ｲ) ネットワーク管理者は、機密性の高い情報を扱うネットワークに対し、情報の盗聴等を防ぐため、暗号化等の措置を講じるものとする。	情報システム等を物理的に分ける等、特に強固な情報セキュリティ対策をとるものとする。 (ｲ) 患者等が直接利用する端末については、必要最小限の機能に限定した専用端末とする。 ス　ネットワーク (ｱ) ネットワーク管理者は、ネットワークを構築する場合は、統括情報セキュリティ管理者と協議するものとする。また、変更又は廃止する場合も同様とする。 (ｲ) ネットワーク管理者は、適切な管理下で接続を行い、情報セキュリティに留意したネットワーク構成を採るものとする。 (ｳ) ネットワーク管理者は、ウェブサーバ等をインターネットに公開する場合、内部ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続するものとする。 (ｴ) ネットワーク管理者は、接続した外部ネットワークの情報セキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ管理者の判断に従い速やかに当該外部ネットワークとの接続を遮断するものとする。 セ　ネットワークの盗聴対策 (ｱ) ネットワーク管理者は、無線 LAN の利用を認める場合には、暗号化及び認証技術の使用を義務づけるものとする。 (ｲ) ネットワーク管理者は、機密性の高い情報を扱うネットワークに対し、情報の盗聴等を防ぐため、暗号化等の措置を講じるものとする。

(2) アクセス制御 ア　ID の取扱い (ｱ) 情報システム管理者等は、利用者の登録、変更、抹消等の手続き及びそれらの情報管理、職員の異動、派遣及び退職に伴う ID の取扱い等の方法を定めるものとする。 (ｲ) 情報システム管理者等は、利用されていない ID が放置されないよう点検するものとする。 イ　管理者権限 (ｱ) 情報システム管理者等は、所管する情報システム等の管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID 及びパスワードを厳重に管理するものとする。 (ｲ) 情報システム管理者等は、特権を付与された ID 及びパスワードの変更を委託事業者に行わせてはならない。 (ｳ) 情報システム管理者等は、特権を付与されたパスワードについて、変更期間や入力回数制限の設定値を小さくすることなどにより、セキュリティ機能をより強固にするものとする。 ウ　ネットワークのアクセス制御等 (ｱ) ネットワーク管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を講じるものとする。 (ｲ) ネットワーク管理者は、フィルタリング及びルーティングの不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等を設定するものとする。 エ　外部ネットワークからのアクセス (ｱ) ネットワーク管理者は、内部のネットワーク又は情報	(2) アクセス制御 ア　ID の取扱い (ｱ) 情報システム管理者等は、利用者の登録、変更、抹消等の手続き及びそれらの情報管理、職員の異動、派遣及び退職に伴う ID の取扱い等の方法を定めるものとする。 (ｲ) 情報システム管理者等は、利用されていない ID が放置されないよう点検するものとする。 イ　管理者権限 (ｱ) 情報システム管理者等は、所管する情報システム等の管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID 及びパスワードを厳重に管理するものとする。 (ｲ) 情報システム管理者等は、特権を付与された ID 及びパスワードの変更を委託事業者に行わせてはならない。 (ｳ) 情報システム管理者等は、特権を付与されたパスワードについて、変更期間や入力回数制限の設定値を小さくすることなどにより、セキュリティ機能をより強固にするものとする。 ウ　ネットワークのアクセス制御等 (ｱ) ネットワーク管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を講じるものとする。 (ｲ) ネットワーク管理者は、フィルタリング及びルーティングの不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等を設定するものとする。 エ　外部ネットワークからのアクセス (ｱ) ネットワーク管理者は、内部のネットワーク又は情報

システムに対する外部ネットワークからのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定するものとする。 (ｲ) ネットワーク管理者は、法人の情報システム等へのリモートメンテナンス等、外部ネットワークからのアクセスを、必要があると認められた場合にのみ許可するものとする。 (ｳ) ネットワーク管理者は、外部ネットワークからのアクセスを認める場合には、システム上利用者の本人確認を行う機能を確保するものとする。 (ｴ) ネットワーク管理者は、外部ネットワークからのアクセスを認める場合には、通信途上の盗聴を防御するために暗号化等の措置を講じるものとする。 (ｵ) ネットワーク管理者は、外部ネットワークからのアクセスに利用する端末等を職員等に貸与する場合には、情報セキュリティ確保のために必要な措置を講じるものとする。 オ　自動識別 ネットワーク管理者は、ネットワーク機器のうち必要なものについて、機器固有情報によってアクセスの可否を自動的に判別するものとする。 カ　ログイン手順 情報システム管理者等は、ログイン手順中におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン及びログアウト時刻の表示、ログイン失敗時の記録等、正当なアクセス権を持つ職員等がログインしたことを確認することができる手順を定めるものとする。	システムに対する外部ネットワークからのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定するものとする。 (ｲ) ネットワーク管理者は、機構の情報システム等へのリモートメンテナンス等、外部ネットワークからのアクセスを、必要があると認められた場合にのみ許可するものとする。 (ｳ) ネットワーク管理者は、外部ネットワークからのアクセスを認める場合には、システム上利用者の本人確認を行う機能を確保するものとする。 (ｴ) ネットワーク管理者は、外部ネットワークからのアクセスを認める場合には、通信途上の盗聴を防御するために暗号化等の措置を講じるものとする。 (ｵ) ネットワーク管理者は、外部ネットワークからのアクセスに利用する端末等を職員等に貸与する場合には、情報セキュリティ確保のために必要な措置を講じるものとする。 オ　自動識別 ネットワーク管理者は、ネットワーク機器のうち必要なものについて、機器固有情報によってアクセスの可否を自動的に判別するものとする。 カ　ログイン手順 情報システム管理者等は、ログイン手順中におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン及びログアウト時刻の表示、ログイン失敗時の記録等、正当なアクセス権を持つ職員等がログインしたことを確認することができる手順を定めるものとする。

キ　パスワードの管理方法 (ｱ) 情報システム管理者等は、職員等のパスワードに関する情報を厳重に管理するものとする。職員等のパスワードを発行する場合は、仮のパスワードを発行し、ログイン後、速やかに正規のパスワードに変更させるものとする。 (ｲ) 情報システム管理者等は、パスワードの変更を行わない職員等にパスワードを変更する旨を勧告し、当該職員等が勧告に従わない場合には一定期間経過後に当該職員等のアクセス権を停止するものとする。 (ｳ) 情報システム管理者等は、当該職員等からパスワード変更の申告があった場合は、直ちに当該職員等のアクセス権の停止を解除するものとする。 (ｴ) 情報システム管理者等は、職員等のパスワードについて、定期的にその妥当性の調査を行うものとする。 (ｵ) 情報システム管理者等は、パスワードが第三者に読まれることのないよう、暗号化等の方法を定めるものとする。 ク　接続時間の制限 情報システム管理者等は、管理者権限による情報システム等への接続時間を必要最小限に制限するものとする。 (3) 情報システムの開発、導入、保守等 ア　情報システムの調達 (ｱ) 情報システム管理者は、情報システムの調達に当たっては、調達仕様書が情報セキュリティポリシーで定められた情報セキュリティを確保できる内容にするものとする。 (ｲ) 情報システム管理者は、機器及びソフトウエアを購入	キ　パスワードの管理方法 (ｱ) 情報システム管理者等は、職員等のパスワードに関する情報を厳重に管理するものとする。職員等のパスワードを発行する場合は、仮のパスワードを発行し、ログイン後、速やかに正規のパスワードに変更させるものとする。 (ｲ) 情報システム管理者等は、パスワードの変更を行わない職員等にパスワードを変更する旨を勧告し、当該職員等が勧告に従わない場合には一定期間経過後に当該職員等のアクセス権を停止するものとする。 (ｳ) 情報システム管理者等は、当該職員等からパスワード変更の申告があった場合は、直ちに当該職員等のアクセス権の停止を解除するものとする。 (ｴ) 情報システム管理者等は、職員等のパスワードについて、定期的にその妥当性の調査を行うものとする。 (ｵ) 情報システム管理者等は、パスワードが第三者に読まれることのないよう、暗号化等の方法を定めるものとする。 ク　接続時間の制限 情報システム管理者等は、管理者権限による情報システム等への接続時間を必要最小限に制限するものとする。 (3) 情報システムの開発、導入、保守等 ア　情報システムの調達 (ｱ) 情報システム管理者は、情報システムの調達に当たっては、調達仕様書が情報セキュリティポリシーで定められた情報セキュリティを確保できる内容にするものとする。 (ｲ) 情報システム管理者は、機器及びソフトウエアを購入

等する場合は、当該製品が情報セキュリティ上問題にならないことを確認するものとする。 イ　情報システムの開発、更新、統合等 情報システム管理者は、情報システムの開発、更新若しくは統合時の事故又は不正行為の対策のため、次の事項を実施するものとする。 (ｱ) 管理者及び監督者の特定 (ｲ) 作業者及び作業範囲の特定 (ｳ) 情報漏えいが発生した場合の影響範囲等のリスクの検討 (ｴ) 情報システム及びデータ移行手続きが失敗した場合や移行直後に障害等が 発生した場合における、旧情報システムへ戻す計画とその手順の作成 (ｵ) 情報システム及びデータ移行手続きにおける検証チェックポイントや移行 の妥当性基準の明確化 (ｶ) 開発環境と運用環境の分離 (ｷ)ハードウエア及びソフトウエアの特定 (ｸ)情報セキュリティ上問題となる恐れのあるソフトウエアの使用禁止 (ｹ)ソースコードの点検 (ｺ) 管理者、作業者等が利用する ID の管理（開発、更新又は統合の終了後に不要となった時点での ID の速やかな抹消等） (ｻ) 管理者、作業者等のアクセス制限の設定 (ｼ) 機器の搬出入の際の許可及び確認 (ｽ)作業時の記録の作成、点検及び保存	等する場合は、当該製品が情報セキュリティ上問題にならないことを確認するものとする。 イ　情報システムの開発、更新、統合等 情報システム管理者は、情報システムの開発、更新若しくは統合時の事故又は不正行為の対策のため、次の事項を実施するものとする。 (ｱ) 管理者及び監督者の特定 (ｲ) 作業者及び作業範囲の特定 (ｳ) 情報漏えいが発生した場合の影響範囲等のリスクの検討 (ｴ) 情報システム及びデータ移行手続きが失敗した場合や移行直後に障害等が 発生した場合における、旧情報システムへ戻す計画とその手順の作成 (ｵ) 情報システム及びデータ移行手続きにおける検証チェックポイントや移行 の妥当性基準の明確化 (ｶ) 開発環境と運用環境の分離 (ｷ)ハードウエア及びソフトウエアの特定 (ｸ)情報セキュリティ上問題となる恐れのあるソフトウエアの使用禁止 (ｹ)ソースコードの点検 (ｺ) 管理者、作業者等が利用する ID の管理（開発、更新又は統合の終了後に不要となった時点での ID の速やかな抹消等） (ｻ) 管理者、作業者等のアクセス制限の設定 (ｼ) 機器の搬出入の際の許可及び確認 (ｽ)作業時の記録の作成、点検及び保存

(ｾ)テスト結果、ソースコード等の資料の定められた場所への保管 (ｿ) ASP などクラウド型サービス利用時における統括情報セキュリティ管理者との協議 ウ　情報システムの導入 (ｱ) 情報システム管理者は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に十分なテストを行うものとする。 (ｲ) 情報システム管理者は、運用テストを行う場合には、あらかじめテスト環境による操作確認を行うものとする。 (ｳ) 情報システム管理者は、重要情報をテストデータに使用してはならない。 (ｴ) 情報システム管理者は、使用したデータ及びテストの結果を適切に保管するものとする。 (ｵ) 情報システム管理者は、本稼動前に、新たに導入する情報システムの脆弱性の有無について、原則として、第三者による技術的検証を実施し、脆弱性が存在しないことを確認するものとする。 エ　情報システムの入力データ (ｱ) 情報システム管理者は、情報システムに入力されるデータについて、適切なチェック等を行い、当該データが安全かつ正確であることを確実にするための対策を講じるものとする。 (ｲ) 情報システム管理者は、エラーによる情報の書換え又は故意による情報の改ざんの恐れがある場合には、これ	(ｾ)テスト結果、ソースコード等の資料の定められた場所への保管 (ｿ) ASP などクラウド型サービス利用時における統括情報セキュリティ管理者との協議 ウ　情報システムの導入 (ｱ) 情報システム管理者は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に十分なテストを行うものとする。 (ｲ) 情報システム管理者は、運用テストを行う場合には、あらかじめテスト環境による操作確認を行うものとする。 (ｳ) 情報システム管理者は、重要情報をテストデータに使用してはならない。 (ｴ) 情報システム管理者は、使用したデータ及びテストの結果を適切に保管するものとする。 (ｵ) 情報システム管理者は、本稼動前に、新たに導入する情報システムの脆弱性の有無について、原則として、第三者による技術的検証を実施し、脆弱性が存在しないことを確認するものとする。 エ　情報システムの入力データ (ｱ) 情報システム管理者は、情報システムに入力されるデータについて、適切なチェック等を行い、当該データが安全かつ正確であることを確実にするための対策を講じるものとする。 (ｲ) 情報システム管理者は、エラーによる情報の書換え又は故意による情報の改ざんの恐れがある場合には、これ

を検出する手段を講じるものとする。 また、必要に応じて情報の修復を行う手段を講じるものとする。 オ　情報システムの保守 (ｱ) 情報システム管理者は、ソフトウエアの更新等を行う場合には、不具合及び他の情報システムへの悪影響が生じないことを確認し、計画的に実施するものとする。 (ｲ) 情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対して、速やかにプログラムの修正を行うものとする。 (ｳ) 情報システム管理者は、情報システムの変更等を行った場合は、その設定、構成等の履歴を記録し、保存するものとする。 (4) 不正プログラム対策 ア　情報システム管理者等は、次の事項を実施するものとする。 (ｱ) インターネットを通じて受信したファイルは、インターネットのゲートウェイ等において、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、不正プログラムの情報システム等への侵入を防止するものとする。 (ｲ) インターネットを通じて送信するファイルは、インターネットのゲートウェイ等において、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、不正プログラムの外部への拡散を防止するものとする。 (ｳ) コンピュータウイルス等の不正プログラムに関する情報を収集し、必要に応じ職員等に対する注意喚起を行うものとする。 (ｴ) サーバ及び端末に、コンピュータウイルス等の不正プ	を検出する手段を講じるものとする。 また、必要な場合は情報の修復を行う手段を講じるものとする。 オ　情報システムの保守 (ｱ) 情報システム管理者は、ソフトウエアの更新等を行う場合には、不具合及び他の情報システムへの悪影響が生じないことを確認し、計画的に実施するものとする。 (ｲ) 情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対して、速やかにプログラムの修正を行うものとする。 (ｳ) 情報システム管理者は、情報システムの変更等を行った場合は、その設定、構成等の履歴を記録し、保存するものとする。 (4) 不正プログラム対策 ア　情報システム管理者等は、次の事項を実施するものとする。 (ｱ) インターネットを通じて受信したファイルは、インターネットのゲートウェイ等において、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、不正プログラムの情報システム等への侵入を防止するものとする。 (ｲ) インターネットを通じて送信するファイルは、インターネットのゲートウェイ等において、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、不正プログラムの外部への拡散を防止するものとする。 (ｳ) コンピュータウイルス等の不正プログラムに関する情報を収集し、必要に応じ職員等に対する注意喚起を行うものとする。 (ｴ) サーバ及び端末に、コンピュータウイルス等の不正プ

ログラム対策ソフトウエアを常駐させるものとする。 (ｵ) 不正プログラム対策ソフトウエアのパターンファイル等を常に最新のものに保つものとする。 イ　職員等は、次の事項を遵守するものとする。 (ｱ) 外部からデータ又はソフトウエ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エアによるチェックを行うものとする。 (ｲ) 端末に搭載された不正プログラム対策ソフトウエアの設定内容を変更することにより、セキュリティレベルを低下させないものとする。 (ｳ) 不正プログラム対策ソフトウエアによるウイルスチェックの実行を途中で止めないものとする。 (ｴ) 添付ファイルのある電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行い、不正プログラムと疑われる添付ファイルは開かず速やかに削除するものとする。 (ｵ) ネットワーク管理者が提供するコンピュータウイルス等の不正プログラムに関する情報を確認し、その指示に従うものとする。 ウ　専門家の支援体制 情報システム管理者等は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにするものとする。 (5) 不正アクセス対策 情報システム管理者等は、次の事項を実施するものとする。	ログラム対策ソフトウエアを常駐させるものとする。 (ｵ) 不正プログラム対策ソフトウエアのパターンファイル等を常に最新のものに保つものとする。 イ　職員等は、次の事項を遵守するものとする。 (ｱ) 外部からデータ又はソフトウエ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エアによるチェックを行うものとする。 (ｲ) 端末に搭載された不正プログラム対策ソフトウエアの設定内容を変更することにより、セキュリティレベルを低下させないものとする。 (ｳ) 不正プログラム対策ソフトウエアによるウイルスチェックの実行を途中で止めないものとする。 (ｴ) 添付ファイルのある電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行い、不正プログラムと疑われる添付ファイルは開かず速やかに削除するものとする。 (ｵ) ネットワーク管理者が提供するコンピュータウイルス等の不正プログラムに関する情報を確認し、その指示に従うものとする。 ウ　専門家の支援体制 情報システム管理者等は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにするものとする。 (5) 不正アクセス対策 情報システム管理者等は、次の事項を実施するものとする。

ア　使用されていないポートを閉鎖するものとする。 イ　不正アクセスによるホームページ書換え防止を確実にするために、データの書換えを検出し、ネットワーク管理者又は情報システム管理者へ通報する対策を講じるものとする。 ウ　対策重要度Ⅰに該当する情報を取り扱う情報システムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査するものとする。 エ　外部から攻撃を受けることが明確な場合には、関係機関との連絡を密にして情報の収集に努め、情報システムの停止を含む必要な措置を講じるものとする。 オ 不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号）に対する違反等犯罪の可能性がある攻撃を受けた場合には、記録の保存に努めるとともに、警察、関係機関との緊密な連携に努めるものとする。 カ　職員等又は委託事業者による不正アクセスがあった場合には、当該職員等が属する所属の情報セキュリティ管理者に通知し、適切な措置を求めるものとする。	ア　使用されていないポートを閉鎖するものとする。 イ　不正アクセスによるホームページ書換え防止を確実にするために、データの書換えを検出し、ネットワーク管理者又は情報システム管理者へ通報する対策を講じるものとする。 ウ　対策重要度Ⅰに該当する情報を取り扱う情報システムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査するものとする。 エ　外部から攻撃を受けることが明確な場合には、関係機関との連絡を密にして情報の収集に努め、情報システムの停止を含む必要な措置を講じるものとする。 オ 不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号）に対する違反等犯罪の可能性がある攻撃を受けた場合には、記録の保存に努めるとともに、警察、関係機関との緊密な連携に努めるものとする。 カ　職員等又は委託事業者による不正アクセスがあった場合には、当該職員等が属する所属の情報セキュリティ管理者に通知し、適切な措置を求めるものとする。
7　運用における対策 (1) 情報システム等の監視 ア　情報システム管理者等は、情報資産への侵害等、情報セキュリティに関する異常事態、不正行為、事故、障害等（以下「事案」という。）を検知するため、常に情報システム等の監視を行うものとする。 イ　情報システム管理者等は、外部ネットワークと常時接続する情報システム等について、ネットワーク侵入監視装置を設置し、常時監視を行うものとする。	7　運用における対策 (1) 情報システム等の監視 ア　情報システム管理者等は、情報資産への侵害等、情報セキュリティに関する異常事態、不正行為、事故、障害等（以下「事案」という。）を検知するため、常に情報システム等の監視を行うものとする。 イ　情報システム管理者等は、外部ネットワークと常時接続する情報システム等について、ネットワーク侵入監視装置を設置し、常時監視を行うものとする。

ウ　情報システム管理者等は、重要なアクセス記録等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じるものとする。 (2) 情報セキュリティに関する技術情報の収集、対応及び共有 ア　情報システム管理者等は、不正プログラム等のセキュリティ情報を収集し、ソフトウエアにパッチを当てる等、情報セキュリティ対策上必要な措置を講じるものとする。 また、必要に応じ、対応方法を職員等に周知するものとする。 イ　情報セキュリティ管理者等は、情報セキュリティに関する社会環境や技術環 境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然 に防止するための対策を速やかに講じるものとする。 また、必要に応じ、情報セキュリティに関して収集した情報を、関係者間で 共有するものとする。 (3) 情報セキュリティポリシーの遵守状況の確認及び対処 ア　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括情報セキュリティ管理者に報告するものとする。 イ　統括情報セキュリティ管理者は、問題に適切に対処し、必要に応じて最高情報統括責任者に報告するものとする。 ウ　情報システム管理者等が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用している端末、アクセス記録、電子メールログ等を調査できるものとする。	ウ　情報システム管理者等は、重要なアクセス記録等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じるものとする。 (2) 情報セキュリティに関する技術情報の収集、対応及び共有 ア　情報システム管理者等は、不正プログラム等のセキュリティ情報を収集し、ソフトウエアにパッチを当てる等、情報セキュリティ対策上必要な措置を講じるものとする。 また、必要に応じ、対応方法を職員等に周知するものとする。 イ　情報セキュリティ管理者等は、情報セキュリティに関する社会環境や技術環 境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然 に防止するための対策を速やかに講じるものとする。 また、必要に応じ、情報セキュリティに関して収集した情報を、関係者間で 共有するものとする。 (3) 情報セキュリティポリシーの遵守状況の確認及び対処 ア　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括情報セキュリティ管理者に報告するものとする。 イ　統括情報セキュリティ管理者は、問題に適切に対処し、必要に応じて最高情報統括責任者に報告するものとする。 ウ　情報システム管理者等が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用している端末、アクセス記録、電子メールログ等を調査できるものとする。

エ　情報システム管理者等は、サーバ等のシステム設定が情報セキュリティポリシーに適合しているかどうかについて定期的に確認を行い、問題を認めた場合には速やかかつ適切に対処するものとする。	エ　情報システム管理者等は、サーバ等のシステム設定が情報セキュリティポリシーに適合しているかどうかについて定期的に確認を行い、問題を認めた場合には速やかかつ適切に対処するものとする。
オ　情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び情報セキュリティ実施手順を参照できるよう配慮するものとする。	オ　情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び情報セキュリティ実施手順を参照できるよう配慮するものとする。
(4) 事案への対応 情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のアからウのとおり定める。	(4) 事案への対応 情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のアからウのとおり定める。
ア　連絡先 ・最高情報統括責任者 ・統括情報セキュリティ管理者 ・ネットワーク管理者 ・情報システム管理者 ・コンピュータ管理者 ・情報システム等に係る委託事業者 ・コンピュータ緊急対応センター（JPCERT） ・管轄警察署 ・神奈川県警察本部サイバー犯罪対策センター ・神奈川県 ・関係機関 ・影響が考えられる個人及び法人	ア　連絡先 ・最高情報統括責任者 ・統括情報セキュリティ管理者 ・ネットワーク管理者 ・情報システム管理者 ・コンピュータ管理者 ・情報システム等に係る委託事業者 ・コンピュータ緊急対応センター（JPCERT） ・管轄警察署 ・神奈川県警察本部サイバー犯罪対策センター ・神奈川県 ・関係機関 ・影響が考えられる個人及び法人
イ　事案の調査 情報セキュリティに関する事案を認めた職員等は、次の項目について、速やかに情報セキュリティ管理者及び情報	イ　事案の調査 情報セキュリティに関する事案を認めた職員等は、次の項目について、速やかに情報セキュリティ管理者及び情報

システム管理者等に報告するものとする。 ・事案の内容 ・事案が発生した原因として、想定される行為 ・確認した被害及び影響範囲 上記の報告を受けた情報システム管理者等は、事案の詳細な調査を行うとともに、統括情報セキュリティ管理者への報告を行うものとする。 ウ　事案への対処 情報システム管理者等は、事案に対処するために次の項目を実施するものとする。 (ｱ) ネットワーク管理者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡する。 ・サイバーテロその他の患者等に重大な被害が生じる恐れがあるとき(統括情報セキュリティ管理者、警察、影響が考えられる個人及び法人) ・不正アクセスその他犯罪と思慮されるとき(統括情報セキュリティ管理者、警察) ・踏み台となって他者に被害を与える恐れがあるとき(統括情報セキュリティ管理者、警察) ・情報システムに関する被害(情報システム管理者、必要と認められる事業者等) ・その他情報資産に係る被害(関係所属等) (ｲ) ネットワーク管理者は、次の事案が発生し情報資産の防護のためにやむを得ない場合は、ネットワークを切断する措置を講じる。 ・異常なアクセスが継続しているとき又は不正アクセスが判明したとき ・情報システムの運用に著しい支障をきたす攻撃が継	システム管理者等に報告するものとする。 ・事案の内容 ・事案が発生した原因として、想定される行為 ・確認した被害及び影響範囲 上記の報告を受けた情報システム管理者等は、事案の詳細な調査を行うとともに、統括情報セキュリティ管理者への報告を行うものとする。 ウ　事案への対処 情報システム管理者等は、事案に対処するために次の項目を実施するものとする。 (ｱ) ネットワーク管理者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡する。 ・サイバーテロその他の患者等に重大な被害が生じる恐れがあるとき(統括情報セキュリティ管理者、警察、影響が考えられる個人及び法人) ・不正アクセスその他犯罪と思慮されるとき(統括情報セキュリティ管理者、警察) ・踏み台となって他者に被害を与える恐れがあるとき(統括情報セキュリティ管理者、警察) ・情報システムに関する被害(情報システム管理者、必要と認められる事業者等) ・その他情報資産に係る被害(関係所属等) (ｲ) ネットワーク管理者は、次の事案が発生し情報資産の防護のためにやむを得ない場合は、ネットワークを切断する措置を講じる。 ・異常なアクセスが継続しているとき又は不正アクセスが判明したとき ・情報システムの運用に著しい支障をきたす攻撃が継

続しているとき ・コンピュータウイルス等の不正プログラムがネットワーク経由で拡がっているとき ・情報資産に係る重大な被害が想定されるとき (ｳ) コンピュータ管理者及び情報システム管理者は、次の事案が発生し情報資産の防護のためにやむを得ない場合は、コンピュータ及び情報システムを停止する。 ・コンピュータウイルス等の不正プログラムが情報資産に深刻な被害を及ぼしているとき ・災害等により電源を供給することが危険又は困難なとき ・その他の情報資産に係る重大な被害が想定されるとき (ｴ) コンピュータ管理者が個々の端末をネットワークから強制的に切断する場合は、事前にネットワーク管理者又は情報システム管理者の許可を得る。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合には、事後報告とすることができる。 (ｵ) 情報システム管理者等は、事案に係る情報システム等のアクセス記録及び現状を保存する。 (ｶ) 情報システム管理者等は、事案に対処した経過を記録する。 (ｷ) 情報システム管理者等は、事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する。 (ｸ) 情報システム管理者等は、再発防止の暫定措置を講じた後、復旧する。 エ　再発防止の措置 (ｱ) 情報システム管理者等は、当該事案に係るリスク分析	続しているとき ・コンピュータウイルス等の不正プログラムがネットワーク経由で拡がっているとき ・情報資産に係る重大な被害が想定されるとき (ｳ) コンピュータ管理者及び情報システム管理者は、次の事案が発生し情報資産の防護のためにやむを得ない場合は、コンピュータ及び情報システムを停止する。 ・コンピュータウイルス等の不正プログラムが情報資産に深刻な被害を及ぼしているとき ・災害等により電源を供給することが危険又は困難なとき ・その他の情報資産に係る重大な被害が想定されるとき (ｴ) コンピュータ管理者が個々の端末をネットワークから強制的に切断する場合は、事前にネットワーク管理者又は情報システム管理者の許可を得る。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合には、事後報告とすることができる。 (ｵ) 情報システム管理者等は、事案に係る情報システム等のアクセス記録及び現状を保存する。 (ｶ) 情報システム管理者等は、事案に対処した経過を記録する。 (ｷ) 情報システム管理者等は、事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する。 (ｸ) 情報システム管理者等は、再発防止の暫定措置を講じた後、復旧する。 エ　再発防止の措置 (ｱ) 情報システム管理者等は、当該事案に係るリスク分析

を実施し、情報セキュリティ対策の改善に係る再発防止計画を策定し、統括情報セキュリティ管理者へ報告するものとする。 統括情報セキュリティ管理者は、情報セキュリティ対策の改善に係る再発防止計画が有効であると認められる場合は、これを了承するものとする。 (ｲ) 統括情報セキュリティ管理者は、再発防止のために情報セキュリティポリシーの改正が必要な場合には、改正案を策定するものとする。 オ　業務継続計画の策定 情報システム管理者等は、業務継続計画を策定する場合は、神奈川県 ICT 部門業務継続計画（平成 22 年 3 月 31 日総務部長通知）を参考とするものとする。 (5) 外部委託 ア　情報セキュリティ管理者及び情報システム管理者等は、契約締結前に、委託事業者において必要な情報セキュリティ対策が確保されていることを確認するものとする。 イ　情報セキュリティ管理者及び情報システム管理者等は、開発、保守、運用等を委託する場合は、委託事業者に対し、守秘義務等の必要なセキュリティ要件を契約書に明記するものとする。 なお、重要情報を取り扱う委託業務の実施に当たっては、業務委託等に係る情報管理マニュアル（平成 21 年 3 月 30 日神奈川県情報化推進調整会議会長通知）に従うものとする。 また、ASP などクラウド型サービスを利用する場合も、同様の取扱いとする。 ウ　情報セキュリティ管理者及び情報システム管理者等は、	を実施し、情報セキュリティ対策の改善に係る再発防止計画を策定し、統括情報セキュリティ管理者へ報告するものとする。 統括情報セキュリティ管理者は、情報セキュリティ対策の改善に係る再発防止計画が有効であると認められる場合は、これを了承するものとする。 (ｲ) 統括情報セキュリティ管理者は、再発防止のために情報セキュリティポリシーの改正が必要な場合には、改正案を策定するものとする。 オ　業務継続計画の策定 情報システム管理者等は、業務継続計画を策定する場合は、神奈川県 ICT 部門業務継続計画（平成 22 年 3 月 31 日総務部長通知）を参考とするものとする。 (5) 外部委託 ア　情報セキュリティ管理者及び情報システム管理者等は、契約締結前に、委託事業者において必要な情報セキュリティ対策が確保されていることを確認するものとする。 イ　情報セキュリティ管理者及び情報システム管理者等は、開発、保守、運用等を委託する場合は、委託事業者に対し、守秘義務等の必要なセキュリティ要件を契約書に明記するものとする。 なお、重要情報を取り扱う委託業務の実施に当たっては、業務委託等に係る情報管理マニュアル（平成 21 年 3 月 30 日神奈川県情報化推進調整会議会長通知）に従うものとする。 また、ASP などクラウド型サービスを利用する場合も、同様の取扱いとする。 ウ　情報セキュリティ管理者及び情報システム管理者等は、

委託事業者において必要な情報セキュリティ対策が確保されていることを定期的に確認し、必要に応じ、イの契約に基づき措置するものとする。 エ　情報セキュリティ管理者及び情報システム管理者等は、委託事業者との契約書において情報セキュリティポリシーが遵守されなかった場合における損害賠償、契約解除等の規定を定めるものとする。	委託事業者において必要な情報セキュリティ対策が確保されていることを定期的に確認し、必要に応じ、イの契約に基づき措置するものとする。 エ　情報セキュリティ管理者及び情報システム管理者等は、委託事業者との契約書において情報セキュリティポリシーが遵守されなかった場合における損害賠償、契約解除等の規定を定めるものとする。
8　評価及び見直し (1) 監査 ア　最高情報統括責任者は、情報セキュリティ監査統括管理者を指名し、情報資産に対する情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行うものとする。 イ　情報セキュリティ監査統括管理者は、監査を実施する場合には、被監査部門から独立し、かつ監査及び情報セキュリティに関する専門知識を有する者に対して、監査の実施を依頼するものとする。 ウ　情報セキュリティ監査統括管理者は、監査を行うに当たって、監査実施計画を立案し、最高情報統括責任者の承認を得るものとする。 エ　被監査部門は、監査の実施に協力するものとする。 オ　情報システムの開発又は運用を委託事業者に委託している場合、情報セキュリティ監査統括管理者は委託事業者の情報セキュリティポリシーの遵守状況について、定期的に又は必要に応じて監査を行うものとする。 カ　情報セキュリティ監査統括管理者は、監査結果をとりまとめ、統括情報セキュリティ管理者に報告するものとし、	8　評価及び見直し (1) 監査 ア　最高情報統括責任者は、情報セキュリティ監査統括管理者を指名し、情報資産に対する情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行うものとする。 イ　情報セキュリティ監査統括管理者は、監査を実施する場合には、被監査部門から独立し、かつ監査及び情報セキュリティに関する専門知識を有する者に対して、監査の実施を依頼するものとする。 ウ　情報セキュリティ監査統括管理者は、監査を行うに当たって、監査実施計画を立案し、最高情報統括責任者の承認を得るものとする。 エ　被監査部門は、監査の実施に協力するものとする。 オ　情報システムの開発又は運用を委託事業者に委託している場合、情報セキュリティ監査統括管理者は委託事業者の情報セキュリティポリシーの遵守状況について、定期的に又は必要に応じて監査を行うものとする。 カ　情報セキュリティ監査統括管理者は、監査結果をとりまとめ、統括情報セキュリティ管理者に報告するものとし、

統括情報セキュリティ管理者は、当該報告の結果を情報セキュリティポリシーの見直しに際して活用するものとする。 キ　統括情報セキュリティ管理者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示するものとし、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させるものとする。 (2) 点検 ア　情報システム管理者等は、所管する情報システム等について、定期的に又は必要に応じ自己点検を実施するものとする。 イ　情報セキュリティ管理者は、所管する所属における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的に又は必要に応じて自己点検を実施するものとする。 ウ　ア及びイの自己点検を行った者は、点検の結果に基づき、自己の権限の範囲内で改善を図るものとする。 エ　情報セキュリティ管理者は、自己点検結果及びこれに基づく改善策をとりまとめ、統括情報セキュリティ管理者に報告するものとし、統括情報セキュリティ管理者は、当該報告の結果を情報セキュリティポリシーの見直しに際して活用するものとする。 (3) 情報セキュリティポリシーの改正 新たに情報セキュリティ対策の必要が発生した場合又は監査及び点検の結果、情報セキュリティポリシーの改正の必要性が生じた場合は、統括情報セキュリティ管理者が情報セ	統括情報セキュリティ管理者は、当該報告の結果を情報セキュリティポリシーの見直しに際して活用するものとする。 キ　統括情報セキュリティ管理者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示するものとし、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させるものとする。 (2) 点検 ア　情報システム管理者等は、所管する情報システム等について、定期的に又は必要に応じ自己点検を実施するものとする。 イ　情報セキュリティ管理者は、所管する所属における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的に又は必要に応じて自己点検を実施するものとする。 ウ　ア及びイの自己点検を行った者は、点検の結果に基づき、自己の権限の範囲内で改善を図るものとする。 エ　情報セキュリティ管理者は、自己点検結果及びこれに基づく改善策をとりまとめ、統括情報セキュリティ管理者に報告するものとし、統括情報セキュリティ管理者は、当該報告の結果を情報セキュリティポリシーの見直しに際して活用するものとする。 (3) 情報セキュリティポリシーの改正 新たに情報セキュリティ対策の必要が発生した場合又は監査及び点検の結果、情報セキュリティポリシーの改正の必要性が生じた場合は、統括情報セキュリティ管理者が情報セ

キュリティポリシーを改正するものとする。	キュリティポリシーを改正するものとする。
9　例外措置 (1) 例外措置の協議 情報セキュリティ管理者及び情報システム管理者等は、情報セキュリティポリシーを遵守することが困難であるため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、統括情報セキュリティ管理者と協議の上、例外措置を取ることができる。 (2) 緊急時の例外措置 情報セキュリティ管理者及び情報システム管理者等は、緊急を要する等の場合であって、情報セキュリティポリシーを遵守することが困難であるときは、事後速やかに統括情報セキュリティ管理者に報告書を提出するものとする。 (3) 例外措置の協議書等の保管 統括情報セキュリティ管理者は、例外措置の協議書、協議結果及び報告書を適切な方法により保管するものとする。	9　例外措置 (1) 例外措置の協議 情報セキュリティ管理者及び情報システム管理者等は、情報セキュリティポリシーを遵守することが困難であるため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、統括情報セキュリティ管理者と協議の上、例外措置を取ることができる。 (2) 緊急時の例外措置 情報セキュリティ管理者及び情報システム管理者等は、緊急を要する等の場合であって、情報セキュリティポリシーを遵守することが困難であるときは、事後速やかに統括情報セキュリティ管理者に報告書を提出するものとする。 (3) 例外措置の協議書等の保管 統括情報セキュリティ管理者は、例外措置の協議書、協議結果及び報告書を適切な方法により保管するものとする。
附　則 1　実施の時期 この要綱は、平成 22 年 4 月 1 日から施行する。	附　則 1　実施の時期 この要綱は、平成 22 年 4 月 1 日から施行する。
2　経過措置 統括情報セキュリティ管理者が別に定める項目については、第２章第９項(1)の規定による協議が行われた例外措置として取り扱うものとする。	2　経過措置 統括情報セキュリティ管理者が別に定める項目については、第２章第９項(1)の規定による協議が行われた例外措置として取り扱うものとする。

附　則 この要綱は、平成 24 年 7 月 1 日から施行する。 附　則 この要綱は、平成 31 年４月１日から施行する。	附　則 この要綱は、平成 24 年 7 月 1 日から施行する。