情報セキュリティポリシー（令和5年6月１日改定版）

第１章　情報セキュリティポリシーの位置付け、構成

情報セキュリティポリシーとは、江戸川区が所掌する情報資産について、その機密性、完全性、可用性*を維持するための対策について、総合的、体系的に取りまとめたものである。

江戸川区が所掌する情報資産に係る業務については、情報セキュリティポリシーに即して実施することとし、当該業務に携わる全職員並びに関係団体†の職員及び委託事業者が遵守するよう浸透、普及、定着を図るものとする。

情報セキュリティポリシーは一定の普遍性を備えた部分（江戸川区情報管理安全対策要綱）と情報資産を取り巻く状況の変化に対応する部分（江戸川区情報管理安全対策基準）から構成する。これらに基づき、情報システムごとに具体的な情報セキュリティ対策の実施手順を策定することとする。（下表参照）

情報セキュリティポリシーの構成

名　　称		内　　容
情報セキュリティポリシー	江戸川区情報管理安全対策要綱	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
	江戸川区情報管理安全対策基準	江戸川区情報管理安全対策要綱を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準
各情報システムの運用規程		情報システムごとに定める江戸川区情報管理安全対策基準に基づいた具体的な実施手順

* 機 密 性：情報資産にアクセスすることを認可されていない個人、実体又はプロセスに対して、情報資産を使用不可又は非公開にする特性又はその程度をいう。
　完 全 性：情報資産の正確さ及び完全さを保護する特性又はその程度をいう。
　可 用 性：情報資産にアクセスすることを許可されたものが要求したときに、アクセス及び使用が可能である特性又はその程度をいう。

† 関係団体：区が出資その他財政上の援助等を行う法人のうち、「公益財団法人えどがわ環境財団事務局」、「公益社団法人シルバー人材センター江戸川区高齢者事業団事務局」、「社会福祉法人江戸川区社会福祉協議会事務局」、「認定ＮＰＯ法人えどがわエコセンター事務局」及び「公益財団法人えどがわボランティアセンター」、「一般社団法人みんなの就労センター」をいう。

第２章　江戸川区情報管理安全対策要綱

（目的等）

第１条　この要綱は、情報セキュリティポリシーとして、江戸川区（以下「区」という。）が所管するあらゆる情報資産（情報システム等を含む。）について、その情報セキュリティを維持することを目的として、区が実施する情報セキュリティ対策に関する基本的な事項を定める。

２　情報資産の取扱い、情報システムの開発、運用及び管理並びに区の情報セキュリティに関する全ての施策又は規程は、この要綱を基本とする。

（定義）

第２条　この要綱において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　情報資産　区が所管する個人情報をはじめとする行政情報の電磁的記録及び記録媒体並びに情報システム並びに情報システムに関連する文書（仕様書、ネットワーク図等）、設備、施設等をいう。

(2)　ネットワーク　コンピュータ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）及び記録媒体により構成され、情報処理を行う仕組みをいう。

(3)　情報システム　コンピュータ（ハードウェア及びソフトウェア）、その周辺機器、ネットワーク及び記録媒体の全部又は一部により構成され、これを使用して業務を処理する仕組みをいう。

(4)　情報セキュリティ事象　情報セキュリティポリシーへの違反又は情報セキュリティへの侵害の発生（情報セキュリティ対策自体の不具合の可能性又は情報セキュリティに関連するかもしれない未知の状況の発生を含む。）をいう。

(5)　脅威　区が所管する情報資産に損害を与える可能性がある、情報セキュリティ事象の潜在的な原因をいう。

(6)　脆弱性　脅威がつけこむことができる、情報資産がもつ弱点をいう。

(7)　リスク　情報セキュリティ事象の発生確率と結果との組合せをいう。

(8)　アクセス　情報資産を利用することをいう。

(9)　機密性　情報資産にアクセスすることを認可されていない個人、実体又はプロセスに対して、情報資産を使用不可又は非公開にする特性又はその程度をいう。

(10)　完全性　情報資産の正確さ及び完全さを保護する特性又はその程度をいう。

(11)　可用性　情報資産にアクセスすることを許可されたものが要求したときに、アクセス及び使用が可能である特性又はその程度をいう。

(12)　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。

(13)　部　江戸川区の組織に関する規則（昭和 40 年３月江戸川区規則第８号)第７条に規定する部及びこれに相当する組織並びに教育委員会事務局、監査委員事務局、選挙管理委員会事務局、農業委員会事務局並びに区議会事務局をいう。

(14)　課　情報資産を所管する課（江戸川区の組織に関する規則（昭和 40 年３月江戸川区規則第８号）第７条に規定する課、副参事、江戸川区出張所設置条例（昭和 34 年４月条例第８号）第２条に規定する出張所、江戸川区保健所処務規程（昭和 50 年４月江戸川区訓令甲第３号）第２条に規定する課、江戸川区教育委員会事務局処務規則（昭和 46 年９月江戸川区教育委員会規則第２号）第２条に規定する課及び別表に定める組織並びに監査委員事務局、選挙管理委員会事務局、農業委員会事務局及び区議会事務局）をいう。

(15)　課長　前号に規定する課の長をいう。ただし、区議会事務局にあっては次長をいう。

(16)　学校　江戸川区立学校設置条例（昭和 32 年４月江戸川区条例第６号）別表に掲げる小学校、中学校及び幼稚園をいう。

(17)　学校長　前号に規定する学校の長をいう。

(18)　職員等　区が所管する情報資産に関する業務に携わる正規職員、再任用職員、会計年度任用職員等及び労働者派遣契約に基づき区の業務の処理に従事する派遣労働者をいう。

(19)　関係団体　区が出資その他財政上の援助等を行う法人又は団体のうち、公益財団法人えどがわ環境財団、公益社団法人シルバー人材センター江戸川区高齢者事業団、社会福祉法人江戸川区社会福祉協議会、認定ＮＰＯ法人えどがわエコセンター、公益財団法人えどがわボランティアセンター、一般社団法人みんなの就労センター及び江戸川区職員厚生会をいう。

(20)　指定管理者　地方自治法（昭和 22 年法律第 67 号）第 244 条の２第３項に定める指定管理者をいう。

(21)　LGWAN 接続系　業務用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。

(22)　インターネット接続系　インターネットメール、ホームページ管理システム等に関わる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。

(23)　通信経路の分割　LGWAN 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すること。

(24)　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ない等、

安全が確保された通信をいう。

（対象範囲）

第３条　この要綱が対象とする情報資産の範囲は、区長、教育委員会、監査委員、選挙管理委員会、農業委員会、区議会事務局が所管するものとする。

２　江戸川区学校教育情報管理安全対策要綱の適用を受ける情報資産（情報システム等を含む。）は対象外とし、対象外となる学校の情報システムはこの要綱の対象となる情報システムと物理的に分けなければならない。

（対象とする脅威及びリスク）

第４条　情報資産に対する脅威及びリスクとして、次に掲げる事態を想定し、情報セキュリティ対策を区が実施する。

(1)　サイバー攻撃をはじめとする部外者の侵入、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、風水害、事故等の災害によるサービス及び業務の停止。

(4)　電力供給の途絶、通信の途絶等の提供サービスの障害からの波及。

(5)　公共ネットワークにおける職員等による公序良俗に反する発言又はいわれのない外部からの誹謗中傷等による社会的信用の低下。

（情報セキュリティ対策）

第５条　区が所管する情報資産を前条に掲げた脅威及びリスクから保護するため、次の各号に掲げる区分に応じ、それぞれ当該各号に定める対策を区が講じる。

(1)　組織体制　区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する全庁的な組織体制を確立する。

(2)　情報資産の分類と管理　区が所管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講じる。

(3)　情報システム全体の強靭性の向上　情報システム全体に対し、次の対策を講じる。

ア　LGWAN 接続系においては、LGWAN 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の通信経路を分割した上で、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、住民情報の流出を防ぐ。

イ　インターネット接続系においては、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。高度な情報セキュリティ対策とし

て、都区市町村情報セキュリティクラウドに参加する。

(4)　物理的セキュリティ対策　情報システムを構成するコンピュータ、ネットワーク等を損傷、破壊又は盗難等から守り、関係者以外の利用から保護するため、適切な保安設備の設置や機器の運用等の保守対策を講じる。

(5)　人的セキュリティ対策　情報セキュリティ対策に関する権限や責任について定めるとともに、情報資産の保護のために職員等が遵守すべき事項を定めるものとする。

(6)　研修・訓練　職員等に対し、情報セキュリティ対策の適切な実施及び管理に関し、必要な訓練及び啓発を行う等の対策を講じる。

(7)　技術的セキュリティ対策　情報資産を外部からの不正なアクセス等から適切に保護するため、次の対策を講じる。

ア　利用記録の取得などの情報システムの適切な管理

イ　情報資産へのアクセスの制御

ウ　システムの開発、導入、保守等におけるセキュリティ確保

エ　不正プログラム、不正アクセス等のリスク対応

オ　情報システムの監視等

(8)　運用におけるセキュリティ対策　情報資産を適切に保護するため、情報セキュリティポリシー遵守状況の確認、委託を行う際のセキュリティ確保等、運用面の対策を講じるとともに、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対策を講じる。

(9)　業務委託実施時の対策　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。

(10)　外部サービス利用時の対策　外部サービスを利用する場合には、利用に係る規定等を整備し対策を講じる。

(11)　ソーシャルメディアサービス利用時の対策　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た上で利用することとし、ソーシャルメディアサービスごとの責任者を定める。

（違反に対する措置）

第６条　この要綱及びこれを受けて規定する情報セキュリティに関する規程に違反した者については、当該違反と過失の重大性に応じて、懲戒処分等の対象とする。

（情報セキュリティ対策の評価の実施）

第７条　情報セキュリティポリシーの遵守状況について、定期的かつ必要に応じて、情報セキュリティ点検及び情報セキュリティ監査により評価を区が実施するものとする。

（見直しの実施）
第８条　この要綱は、情報セキュリティ点検・監査の結果及び情報システムを取り巻く状況の変化を踏まえ、定期的かつ必要に応じて見直し、改正するものとする。
（関係団体等への対応）
第９条　関係団体が所管する情報資産について、区は、この要綱の趣旨にのっとり情報セキュリティを確保するため、関係団体に必要な措置を講じさせるよう努めるものとする。
２　関係団体へ区が所管する情報資産に関わる業務を委託する場合又は関係団体に区の保有する情報システムの利用を認める場合は、当該業務に関するセキュリティ管理者の指定等、情報セキュリティに関する協定を締結するものとする。
（委託事業者・派遣事業者への対応）
第 10 条　委託事業者が実施する業務において、区が所管する情報資産に関わる業務を実施する場合は、この要綱の趣旨にのっとり情報セキュリティを確保するため、当該委託業務に関する契約等において、必要な措置を定めるものとする。
２　派遣労働者が実施する業務において、区が所管する情報資産に関わる業務を実施する場合は、派遣事業者に対して、この要綱の趣旨にのっとり情報セキュリティを確保するため、当該派遣業務に関する契約等において、必要な措置を定めるものとする。
（指定管理者への対応）
第 11 条　指定管理者が実施する業務において、区が所管する情報資産に関わる業務を実施する場合は、この要綱の趣旨にのっとり情報セキュリティを確保するため、当該指定管理業務に関する協定等において、必要な措置を定めるものとする。
（江戸川区情報管理安全対策基準の策定）
第 12 条　この要綱で定める情報セキュリティ対策等を実施するために、具体的な遵守事項及び判断基準並びに実施に際して必要な対策を講じるため、江戸川区情報管理安全対策基準を区が定めるものとする。
（実施手順の策定）
第 13 条　江戸川区情報管理安全対策基準に定めた情報セキュリティ対策を実施するため、具体的な実施手順を区が策定するものとする。この場合において、情報システム固有の実施手順等が必要となるときは、情報システムごとに具体的な情報セキュリティ対策の実施手順を区が策定することとする。
２　前項に規定する実施手順は、公にすることにより区の行政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。
（その他）

第 14 条　この要綱に定めるもののほか、この要綱の施行に関し必要な事項は、別に区長が定める。

付　則

この要綱は、平成 14 年４月１日から施行する。

付　則

この要綱は、平成 15 年５月 19 日から施行する。

付　則

この要綱は、平成 17 年 12 月 26 日から施行する。

付　則

この要綱は、平成 18 年４月１日から施行する。

付　則

この要綱は、平成 19 年４月１日から施行する。

付　則

この要綱は、平成 29 年５月１日から施行する。

付　則

この要綱は、平成 31 年４月１日から施行する。

付　則

この要綱は、令和３年４月１日から施行する。

付　則

この要綱は、令和４年６月１日から施行する。

付　則

この要綱は、令和５年６月１日から施行する。

別表（第２条関係）

組　織
江戸川区教育研究所

第３章　江戸川区情報管理安全対策基準

１．目的

江戸川区情報管理安全対策要綱（以下「対策要綱」という。）第12条の規定に基づき、情報セキュリティ対策を講ずるに当たり遵守すべき行為、判断等の基準その他必要な事項を定める。

２．定義

この基準において用いる用語の意義は、対策要綱において定めるもののほか、次の各号に定めるところによる。

①　ID　情報システムの利用者を識別するための情報をいう。

②　パスワード　情報システムの利用者を認証するための情報をいう。

③　端末等　情報システムを構成する機器のうち利用者が情報システムにアクセスするため操作する情報機器をいう。

④　サーバ等　情報システムを構成する機器のうち、データの管理、端末等の制御など主要な役割を担うコンピュータをいう。

⑤　外部サービス　事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。外部サービスには、クラウドサービス、ソーシャルメディアサービス、Web会議サービスなどがある。

⑥　外部サービス提供者　外部サービスを提供する事業者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

⑦　外部サービス利用者　外部サービスを利用する自組織の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

⑧　クラウドサービス　事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

⑨　ソーシャルメディアサービス　インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアをいう。

⑩　Web会議サービス　専用のアプリケーションやWEBブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器同士で通信を行うもの(テレビ会議システム等)は含まれない。

⑪　支給された端末　支給された端末は、全庁 LAN へアクセス可能な全庁LAN端末、テレワーク用端末、その他には、オンライン会議用タブレット、オンライン相談用タブレット、地域BWAタブレット及び各課で独自調達した端末、タブレットであり、セキュリティ対策が施されたものをいう。

３．対象範囲

(1)　行政機関の範囲

本対策基準が適用される行政機関は、区長、教育委員会、監査委員、選挙管理委員会、農業委員会、区議会事務局の所掌するものとする。

(2)　情報資産の範囲

本対策基準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、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、ネットワーク図等のシステム関連文書。

④　江戸川区学校教育情報管理安全対策要綱の適用を受ける情報資産（情報システム等を含む。）は対象外とし、対象外となる学校の情報システム等は、このセキュリティポリシーの対象となる情報システムと物理的に分けなければならない。

４．組織体制

(1)　最高情報統括責任者（CISO）

①　副区長を最高情報統括責任者（以下「最高統括者」という。）とする。最高統括者は、本区における全てのネットワーク、情報システム等の情報資産の管理、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。また、情報通信技術の活用による住民の利便性の向上、行政運営改善等に関するものを統括する。

②　最高統括者は、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。

③　最高統括者は、最高統括者を助けて本区における情報セキュリティに関する事務を整理し、最高統括者の命を受けて本区の情報セキュリティに関する事務を統括する最高情報統括副責任者（副CISO）（以下「副最高統括者」という。）１人を必要に応じて置く。

④　最高統括者は、本対策基準に定められた自らの担務を、副最高統括者その他の本対策基準に定める責任者に担わせることができる。

(2)　情報セキュリティ統括者

①　経営企画部長を、最高統括者直属の情報セキュリティ統括者（以下「セキュリティ統括者」という。）とする。セキュリティ統括者は最高統括者及び副最高統括者を補佐しなければならない。

②　セキュリティ統括者は、本区の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③　セキュリティ統括者は、本区の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④　セキュリティ統括者は、情報セキュリティ総括管理者、情報セキュリティ管理者、情報システム運用担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤　セキュリティ統括者は、本区の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に最高統括者の指示に従い、最高統括者が不在の場合には自らの判断に基づき、必要か

つ十分な措置を行う権限及び責任を有する。

⑥　セキュリティ統括者は、緊急時等の円滑な情報共有を図るため、最高統括者、情報セキュリティ総括管理者、情報セキュリティ管理者、情報システム運用担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑦　セキュリティ統括者は、緊急時には最高統括者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。

⑧　セキュリティ統括者は、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、必要に応じて最高統括者にその内容を報告しなければならない。

(3)　情報セキュリティ責任者

①　各部の部長を情報セキュリティ責任者（以下「セキュリティ責任者」という。）とする。

②　セキュリティ責任者は、各部のネットワーク、情報システム等の情報資産を所管する情報システムの責任者として、この基準に規定する職務を実施する。区の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、セキュリティ統括者と連携し、その不在の場合には自らの判断に基づき、必要かつ十分な措置を行う。

③　セキュリティ責任者は、各部のネットワーク、情報システム等の情報資産に係る情報セキュリティ対策の実施手順の維持・管理を行う。

④　セキュリティ責任者は、各部のネットワーク及び情報システムについて、緊急時等における連絡体制の整備、職員等（職員、会計年度任用職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

⑤　経営企画部長は、経営企画部のセキュリティ責任者を兼ねる。

(4)　情報セキュリティ総括管理者

①　経営企画部ＤＸ推進課長を情報セキュリティ総括管理者（以下「セキュリティ総括管理者」という。）とする。

②　セキュリティ総括管理者は、全庁に共通的なネットワーク、情報システム等の情報資産を所管する情報セキュリティ管理者として、この基準に規定する職務を実施する。区の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、セキュリティ統括者の指示に従い、その不在の場合には自らの判断に基づき、必要かつ十分な措置を行う。

③　セキュリティ総括管理者は、全庁に共通的なネットワーク、情報システム等の情報資産に係る情報セキュリティ対策の実施手順の維持・管理を行う。

④　セキュリティ総括管理者は、全庁に共通的なネットワーク及び情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約、職員等に対する教育、訓練、助言及び指示を行う。

(5)　情報セキュリティ管理者

①　各課及び学校の課長及び学校長を、情報セキュリティ管理者（以下「セキュリティ管理者」という。）とする。

②　セキュリティ管理者はその所管する課等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　セキュリティ管理者は、その所掌する課等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがあ

る場合には、セキュリティ責任者、セキュリティ総括管理者、セキュリティ統括者及び最高統括者へ速やかに報告を行い、指示を仰がなければならない。

④　セキュリティ管理者のうち、このセキュリティポリシーの対象となる情報システムを所管する各課長は、情報システム管理者の役割を併せ持つ。セキュリティ管理者のうち、学校長については、システムを所管しておらず、情報システム管理者の役割を持たない。

⑤　セキュリティ管理者は、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。

⑥　セキュリティ管理者は、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。

⑦　セキュリティ管理者は、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維持・管理を行う。

⑧　セキュリティ管理者は、外部サービス利用における、外部サービス管理者を兼ねる。

(6)　情報システム運用担当者

セキュリティ管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム運用担当者（以下「運用担当者」という。）とする。セキュリティ管理者が指名した職員を充てる。また、クラウドサービスの管理等を行う者を、クラウドサービス管理者とし、セキュリティ管理者が指名した係長級の職員を充てる。

(7)　江戸川区ＤＸ推進本部

本区の情報セキュリティ対策を統一的に行うため、江戸川区ＤＸ推進本部（以下「ＤＸ推進本部」という。）において、必要に応じて情報セキュリティポリシー等、情報セキュリティに関する重要な事項を審議する。

(8)　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　情報セキュリティ監査の実施において、や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。

(9)　CSIRT の設置・役割

①　最高統括者は、CSIRT を整備し、その役割を明確化しなければならない。

②　最高統括者は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

③　最高統括者は、情報セキュリティインシデントの窓口の機能を有する組織を整備し、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には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④　最高統括者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

⑤　情報セキュリティインシデントを認知した場合には、最高統括者、総

務省、東京都等へ報告しなければならない。

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

⑦　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

(10)　クラウドサービス利用における組織体制

セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

５．情報資産の分類と管理方法

(1)　情報資産の分類

本区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	取扱制限
機密性３	区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	・　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） ・　ソーシャルメディアサービスにおける情報取扱い禁止（機密性２以上の情報） ・　必要以上の複製及び配付禁止 ・　保管場所の制限、保管場所への必要以上の外部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 ・　信頼のできるネットワーク回線の選択 ・　外部で情報処理を行う際の安全管理措置の規定 ・　電磁的記録媒体の施錠可能な場所への保管
機密性２	区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	取扱制限
完全性２	区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、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・ バックアップを行う ・ 電子署名を付与する ・ 外部で処理を行う際の安全管理措置の規定 ・ 電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	区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、住民の権利が侵害される又は区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	・ バックアップを行う ・ 指定する時間以内に復旧する ・ 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　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　セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も(1)の分類に基づき管理しなければならない。

ウ　セキュリティ管理者は、クラウドサービスの環境に保存される情報資産についても(1)の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

②　情報資産の分類の表示

職員等は、情報資産について、必要に応じて分類や取扱制限をするなど適切な管理を行わなければならない。

③　情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

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

ウ　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④　情報資産の入手

ア　職員等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　職員等以外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、セキュリティ管理者に判断を仰がなければならない。

⑤　情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

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

ウ　情報資産を利用する者は、複数の情報資産を一括して扱う場合に、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取り扱わなければならない。

⑥　情報資産の保管

ア　セキュリティ管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

イ　セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書き込み禁止の措置を講じなければならない。

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

⑦　情報の送信

電子メール等により機密性２以上の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を行わなければならない。また、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、電子署名を付与しなければならない。

⑧　情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、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、セキュリティ管理者に許可を得なければならない。

⑨　情報資産の提供・公表

ア　機密性２以上の情報資産を外部に提供する者は、必要に応じ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、セキュリティ管理者に許可を得なければならない。

ウ　セキュリティ管理者は、住民に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。

⑩　情報資産の廃棄等

ア　情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その記録されている情報の機密性に応じ、情報を復元できないように処置しなければならない。

イ　情報資産の廃棄やリース返却等を行う者は、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　情報資産の廃棄やリース返却等を行う者は、セキュリティ管理者の許可を得なければならない。

エ　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

６．情報システム全体の強靭性の向上

(1)　LGWAN 接続系

①　LGWAN 接続系とインターネット接続系の分離

LGWAN 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 LGWAN 接続系に転送する場合は、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。

ア　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 LGWAN 接続系に転送するメールテキスト化方式

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

②　マイナンバー利用事務における対策

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、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。

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。

ウ　マイナンバーを利用する環境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については、この限りではなく、インターネット等からマイナンバーを利用する環境との双方向でのデータの移送を可能とする。

③　マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本区の他の領域とはネットワークを分離しなければならない。

④　マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

⑤　LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

(2)　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、情報セキュリティインシデントの早期発見と対処及び LGWAN 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　都区市町村情報セキュリティクラウドに参加するとともに、関係省庁や都と連携しながら、情報セキュリティ対策を推進しなければならない。

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。

７．物理的セキュリティ

７．１．サーバ等の管理

(1)　機器の取付け

セキュリティ管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

(2)　機器の電源

①　セキュリティ管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②　セキュリティ管理者は、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(3)　通信ケーブル等の配線

①　セキュリティ管理者は、通信ケーブル、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の必要な措置を講じなければならない。

②　セキュリティ管理者は、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切に管理しなければならない。

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

(4)　機器の定期保守及び修理

①　セキュリティ管理者は、可用性２又は完全性２の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　セキュリティ管理者は、委託事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

(5)　庁外への機器の設置

セキュリティ総括管理者及びセキュリティ管理者は、庁外にサーバ等の機器を設置する場合、最高統括者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

①　セキュリティ管理者は、機器を廃棄や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　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

７．２．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、当該機器等の管理及び運用を行う区域や外部記録媒体の保管庫をいう。

②　セキュリティ総括管理者及びセキュリティ管理者は、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　セキュリティ総括管理者及びセキュリティ管理者は、管理区域内の機器等に、転倒、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　セキュリティ総括管理者及びセキュリティ管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び外部記録媒体等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　セキュリティ総括管理者及びセキュリティ管理者は、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、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わなければならない。

②　職員等及び委託事業者は、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)　機器等の搬入出

①　セキュリティ総括管理者及びセキュリティ管理者は、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

託業者に確認を行わせなければならない。

② セキュリティ総括管理者及びセキュリティ管理者は、管理区域へ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。

７．３．通信回線及び通信回線装置の管理

① セキュリティ総括管理者及びセキュリティ管理者は、庁内の通信回線及び通信回線装置を、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

② セキュリティ総括管理者及びセキュリティ管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③ セキュリティ総括管理者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

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

⑤ セキュリティ総括管理者は、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。

⑥ セキュリティ総括管理者は、可用性２の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。

７．４．職員等の端末等の管理

① セキュリティ管理者は、盗難防止のため、施錠による保管等の物理的措置を講じなければならない。

② セキュリティ管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ セキュリティ管理者は、マイナンバー利用事務では「知識」、「所持」、「存在」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。

④ セキュリティ管理者は、端末等の庁外での業務利用の際は、遠隔消去機能を利用する等の措置を講じなければならない。

８．人的セキュリティ

８．１．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　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　セキュリティ統括者は、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

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

④　支給以外の端末、電磁的記録媒体等の業務利用

ア　職員等は、支給以外の端末、電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末等の業務利用の可否判断をセキュリティ統括者又はセキュリティ責任者が行った後に、業務上必要な場合は、セキュリティ管理者の定める実施手順に従い、セキュリティ管理者の許可を得て利用することができる。

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

⑤　持ち出し及び持ち込みの記録

セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥　端末におけるセキュリティ設定変更の禁止

職員等は、端末のソフトウェアに関するセキュリティ機能の設定を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、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、電磁的記録媒体、文書等が容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

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。

⑨　クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

(2)　会計年度任用職員等への対応

①　情報セキュリティポリシー等の遵守

セキュリティ管理者は、会計年度任用職員等に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員等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　情報セキュリティポリシー等の遵守に対する同意

セキュリティ管理者は、会計年度任用職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③　インターネット接続、電子メール使用等の制限

セキュリティ管理者は、会計年度任用職員等に端末等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

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

セキュリティ管理者は、ネットワーク、情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、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。

８．２．研修・訓練

(1)　情報セキュリティに関する研修・訓練

①　セキュリティ総括管理者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

②　セキュリティ総括管理者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施しなければならない。

③　セキュリティ管理者は、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

(2)　研修計画の策定及び実施

①　セキュリティ総括管理者は、職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

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　新規採用の職員等を対象とする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。

④　研修は、職員等それぞれの役割、情報セキュリティに関する理解度や求められる力量等を考慮したものにしなければならない。

⑤　セキュリティ管理者は、所管する課等の教育の実施状況を記録し、セキュリティ総括管理者及びセキュリティ責任者に対して、報告しなければならない。

⑥　セキュリティ総括管理者は、セキュリティ統括者に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

(3)　緊急時対応訓練

セキュリティ総括管理者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク、各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、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

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

８．３．情報セキュリティインシデントの報告

(1)　庁内からの情報セキュリティインシデントの報告

①　職員等は、情報セキュリティインシデントを認知した場合、速やかに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（CSIRT）に報告しなければならない。

②　報告を受けたセキュリティ管理者は、速やかにセキュリティ総括管理者及びCSIRTに報告しなければならない。

③　セキュリティ責任者及び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、必要に応じて最高統括者、セキュリティ統括者及びセキュリティ総括管理者に報告しなければならない。

④　セキュリティ管理者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

(2)　住民等外部からの情報セキュリティインシデントの報告

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

②　報告を受けたセキュリティ管理者は、速やかにセキュリティ総括管理者に報告しなければならない。

③　セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて最高統括者、セキュリティ統括者、セキュリティ責任者及びセキュリティ総括管理者に報告しなければならない。

④　セキュリティ管理者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

(3)　情報セキュリティインシデント原因の究明・記録、再発防止等

①　CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

②　CSIRTは、情報セキュリティインシデントであると評価した場合、最高統括者に速やかに報告しなければならない。

③　CSIRTは、情報セキュリティインシデントに関係する情報セキュリティ管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

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

⑤　最高統括者は、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。

８．４．ID、パスワード等の管理

(1)　IC カード等の取扱い

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

ア　認証に用いる IC カード等を、職員等間で共有してはならない。

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

②　セキュリティ管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

③　セキュリティ管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

(2)　ID 及びパスワードの取扱い

職員等は、自己の管理する ID、ログイン用パスワード又は課、係等の単位で共有する ID（以下「共用 ID」という。）、ログイン用パスワードに関し、次の各号に掲げる事項を遵守しなければならない。

①　自己が利用している ID は、他人に利用させてはならない。

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

③　パスワードは、他者に知られないように管理しなければならない。

④　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。

⑤　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。

⑥　パスワードが流出したおそれがある場合には、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。

⑦　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑧　仮のパスワードは、最初のログイン時点で変更しなければならない。

⑨　端末等にパスワードを記憶させてはならない。

⑩　職員等間でパスワードを共有してはならない。

９．技術的セキュリティ

９．１．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　セキュリティ管理者は、職員等が使用できる共用のファイルサーバの容量を設定し、必要に応じて職員等に周知する。

②　セキュリティ管理者は、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　セキュリティ管理者は、住民の個人情報、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

①　セキュリティ管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

②　セキュリティ責任者及びセキュリティ管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その仕様がバックアップに関する本区が求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

(3)　他団体との情報システムに関する情報等の交換

セキュリティ管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、セキュリティ統括者の許可を得なければならない。

(4)　システム管理記録及び作業の確認

①　セキュリティ管理者は、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　セキュリティ管理者は、所管するシステムにおいて、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切に管理しなければならない。

③　運用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。

(5)　情報システム仕様書等の管理

セキュリティ管理者は、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が閲覧したり、紛失等がないよう、適切に管理しなければならない。

(6)　ログの取得等

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

②　セキュリティ管理者は、ログとして取得する項目、保存期間、取扱方法、ログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③　セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

④　セキュリティ責任者及びセキュリティ管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者か

ら提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

(7)　障害記録

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

(8)　ネットワークの接続制御、経路制御等

①　セキュリティ管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②　セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

(9)　外部の者が利用できるシステムの分離等

セキュリティ管理者は、電子申請の汎用受付システム等、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。

(10)　外部ネットワークとの接続制限等

①　セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、セキュリティ統括者の許可を得なければならない。

②　セキュリティ管理者は、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、庁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　セキュリティ管理者は、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。

④　セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、庁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　セキュリティ管理者は、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、セキュリティ統括者の判断に従い、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。

(11)　複合機のセキュリティ管理

①　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及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

②　セキュリティ管理者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③　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する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。

(12)　IoT 機器を含む特定用途機器のセキュリティ管理

セキュリティ管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

(13)　無線 LAN 及びネットワークの盗聴対策

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

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

(14)　電子メールのセキュリティ管理

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

②　セキュリティ管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止するなどの措置を取る。

③　セキュリティ管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④　セキュリティ管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤　セキュリティ管理者は、システム開発、運用、保守等のため庁舎内に常駐している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、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。

(15)　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、セキュリティ管理者に報告しなければならない。

(16)　電子署名・暗号化

①　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、セキュリティ統括者が定めた電子署名、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　職員等は、暗号化を行う場合にセキュリティ統括者が定める以外の方法を用いてはならない。

③　セキュリティ統括者は、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。

(17)　無許可ソフトウェアの導入等の禁止

①　職員等は、端末等に無断でソフトウェアを導入してはならない。

②　職員等は、業務上の必要がある場合は、セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、セキュリティ管理者は、ソフトウェアのライセンスを適正に管理する。

③　職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18)　機器構成の変更の制限

①　職員等は、端末等に対し機器の改造、増設及び交換を行ってはならない。

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

(19)　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。

②　セキュリティ管理者は、支給した端末について、端末に搭載されたOSのポリシー設定等により、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。

(20)　業務以外の目的でのウェブ閲覧の禁止

①　職員等は、業務以外の目的でウェブを閲覧してはならない。

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

(21)　Web会議サービス利用時の対策

①　セキュリティ統括者及びセキュリティ責任者は、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、本区の定める利用手順に従い、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すること。

③　職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

④　職員等は、外部からWeb会議に招待される場合は、本区の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(22)　ソーシャルメディアサービスの利用

①　セキュリティ責任者は、本区の管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

ア　本区のアカウントによる情報発信が、実際の本区のものであることを明らかにするために、区公式ホームページ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２以上の情報はソーシャルメディアサービスで発信してはならない。

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。

⑤　可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、区公式ホームページに当該情報を掲載して参照可能とすること。

９．２．アクセス制御

(1)　アクセス制御

①　アクセス制御等

セキュリティ統括者又はセキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、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　セキュリティ統括者又はセキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

イ　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、セキュリティ統括者又はセキュリティ管理者に通知しなければならない。

ウ　セキュリティ統括者又はセキュリティ管理者は、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。

③　特権を付与された ID の管理等

ア　セキュリティ統括者及びセキュリティ管理者は、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　セキュリティ統括者及びセキュリティ管理者の特権を代行する者は、セキュリティ統括者及びセキュリティ管理者が指名した者でなければならない。

ウ　代行者を認めた場合、速やかにセキュリティ統括者、セキュリティ総括管理者、セキュリティ管理者に通知しなければならない。

エ　セキュリティ統括者及びセキュリティ管理者は、特権を付与された ID 及びパスワードの変更について、許可なく委託事業者に行わせてはならない。

オ　セキュリティ統括者及びセキュリティ管理者は、特権を付与された ID 及びパスワードについて、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。

カ　セキュリティ統括者及びセキュリティ管理者は、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)　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、セキュリティ統括者及び当該情報システムを管理するセキュリティ管理者の許可を得なければならない。

②　セキュリティ統括者は、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　セキュリティ統括者は、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　セキュリティ統括者は、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　セキュリティ統括者及びセキュリティ管理者は、外部からのアクセスに利用する端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥　職員等は、持ち込んだ又は外部から持ち帰った端末を庁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、セキュリティ管理者の許可を得てから接続しなければならない。

⑦　セキュリティ統括者は、庁内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。ただし、やむを得ず接続を許可する場合は、ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

(3)　認証情報の管理

①　セキュリティ統括者又はセキュリティ管理者は、職員等の認証情報に関する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　セキュリティ統括者又はセキュリティ管理者は、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、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　セキュリティ統括者又はセキュリティ管理者は、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)　特権による接続時間の制限

セキュリティ管理者は、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。

９．３．システム開発、導入、保守等

(1)　情報システムの調達

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

②　セキュリティ統括者及びセキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セ

キュリティ上問題のないことを確認しなければならない。

(2)　情報システムの開発

①　システム開発における責任者及び作業者の特定

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

②　システム開発における責任者、作業者の ID の管理

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

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

③　システム開発に用いるハードウェア及びソフトウェアの管理

ア　セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

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

(3)　情報システムの導入

①　開発環境と運用環境の分離及び移行手順の明確化

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

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

ウ　セキュリティ管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

②　テスト

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

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

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

(4)　システム開発・保守に関連する資料等の整備・保管

①　セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

②　セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

③　セキュリティ管理者は、情報システムに係る必要なソースコード等を適切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　セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能、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　セキュリティ管理者は、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、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③　セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6)　情報システムの変更管理

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

(7)　開発・保守用のソフトウェアの更新等

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

(8)　システム更新又は統合時の検証等

セキュリティ管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

９．４．不正プログラム対策

(1)　セキュリティ統括者の措置事項

セキュリティ統括者は、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、端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

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

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

⑦　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中に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する予定がないことを確認しなければならない。

⑧　仮想マシンを設定する際に不正プログラムへの対策（必要なポート、

プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

(2)　セキュリティ管理者の措置事項

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

①　セキュリティ管理者は、その所掌するサーバ、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、区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、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　端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

②　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

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

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

⑤　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメールを LGWAN 接続系に転送する場合は無害化しなければならない。

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

⑦　端末にて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、LAN ケーブルの即時取り外しを行わなければならない。

(4)　専門家の支援体制

セキュリティ統括者は、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。

９．５．不正アクセス対策

(1)　セキュリティ統括者の措置事項

セキュリティ統括者は、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の対策を行い、また、セキュリティ統括者及びセキュリティ管理者へ通報しなければならない。

④　セキュリティ統括者は、情報セキュリティに関する窓口（CSIRT）と連携し、監視、通知、外部連絡窓口、適切な対応等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。

⑤　本セキュリティポリシーにおけるクラウドサービスの利用に係るアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑥　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑦　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本セキュリティポリシーのクラウドサービスの利用に関する項目を満たすことを確認しなければならない。

(2)　攻撃の予告

セキュリティ統括者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

(3)　記録の保存

セキュリティ統括者は、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

セキュリティ統括者は、職員等及び委託事業者が使用している端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視するように努めなければならない。

(5)　職員等による不正アクセス

セキュリティ統括者及びセキュリティ管理者は、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課等のセキュリティ管理者に通知し、適切な処置を求めなければならない。

(6)　サービス不能攻撃

セキュリティ統括者及びセキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者が

サービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じるように努めなければならない。

(7)　標的型攻撃

セキュリティ統括者及びセキュリティ管理者は、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。

９．６．セキュリティ情報の収集

(1)　セキュリティホールに関する情報の収集・共有、ソフトウェアの更新等

①　セキュリティ統括者及びセキュリティ管理者は、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　セキュリティ責任者及びセキュリティ管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本区の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認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

セキュリティ統括者は、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

セキュリティ統括者及びセキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境、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。

１０．運用

１０．１．情報システムの監視

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

②　セキュリティ総括管理者及びセキュリティ管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

③　セキュリティ総括管理者及びセキュリティ管理者は、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。

④　セキュリティ総括管理者及びセキュリティ管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

⑤　セキュリティ総括管理者及びセキュリティ管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑥　セキュリティ総括管理者及びセキュリティ管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）クラウドサービス利用の終了手順

（ウ）バックアップ及び復旧

１０．２．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　セキュリティ総括管理者及び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、速やかに最高統括者及びセキュリティ統括者に報告しなければならない。

②　最高統括者は、発生した問題について、適切かつ速やかに対処しなければならない。

③　セキュリティ総括管理者及びセキュリティ管理者は、ネットワーク、サーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

(2)　端末、外部記録媒体等の利用状況調査

最高統括者及び最高統括者が指名した者は、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、外部記録媒体等のログ、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、直ちにセキュリティ統括者及びセキュリティ総括管理者に報告を行わなければならない。

②　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セキュリティ統括者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

１０．３．侵害時の対応等

(1)　緊急時対応計画の策定

①　最高統括者又はＤＸ推進本部は、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　最高統括者又はＤＸ推進本部は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した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正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、ＤＸ推進本部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

最高統括者又はＤＸ推進本部は、情報セキュリティを取り巻く状況の変化、組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

１０．４．例外措置

(1)　例外措置の許可

セキュリティ総括管理者及びセキュリティ管理者は、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、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用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、セキュリティ統括者の許可を得て、例外措置を取ることができる。

(2)　緊急時の例外措置

セキュリティ総括管理者及びセキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにセキュリティ統括者に報告しなければならない。

(3)　例外措置の申請書の管理

セキュリティ統括者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

１０．５．法令遵守

(1)　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　地方公務員法(昭和二十五年法律第二百六十一号)
②　著作権法（昭和四十五年法律第四十八号)
③　不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号)
④　個人情報の保護に関する法律（平成十五年法律第五十七号）
⑤　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（平成二十五年法律第二十七号）
⑥　サイバーセキュリティ基本法（平成二十六年法律第十号）

(2)　セキュリティ統括者及びセキュリティ管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引

き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

１０．６．懲戒処分等

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 セキュリティ統括者が違反を確認した場合は、セキュリティ統括者は当該職員等が所属する課等のセキュリティ管理者に通知し、適切な措置を求めなければならない。

② セキュリティ管理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セキュリティ統括者に通知し、適切な措置を求めなければならない。

③ 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、セキュリティ統括者は、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、セキュリティ統括者は、職員等の権利を停止あるいは剥奪した旨を最高統括者、当該職員等が所属する課等のセキュリティ管理者に通知しなければならない。

１１．業務委託と外部サービスの利用

１１．１．業務委託

(1) 委託事業者の選定基準

① セキュリティ管理者は、委託事業者の選定に当たり、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 セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

(2) 契約項目

重要な情報資産を取り扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者及び作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類、範囲及びアクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・区による監査及び検査
・区による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

(3) 確認・措置等

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

措置しなければならない。また、その内容をセキュリティ統括者に報告するとともに、その重要度に応じて最高統括者に報告しなければならない。

１１．２．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

セキュリティ統括者は、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）の利用に関する規定を整備すること。

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「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

⑤ クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(2) 外部サービスの選定

① セキュリティ責任者は、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 セキュリティ責任者は、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。

③ セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、本セキュリティポリシーのクラウドサービスの利用に関する事項を満たしているか否かを評価すること。

ア 外部サービスの利用を通じて本区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、本区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、外部サービスの提供が行われる施設等の場所、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

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

④ セキュリティ責任者は、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。

⑤ セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

⑥　セキュリティ責任者は、外部サービスの利用を通じて本区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。

（注）クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（ＳＬＡ）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が本区によって受容可能か判断すること。

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

⑦　セキュリティ責任者は、外部サービスの利用を通じて本区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、必要に応じて本区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。

⑧　セキュリティ責任者は、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本区に提供し、本区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。

⑨　セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

⑩　セキュリティ責任者は、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。

⑪　セキュリティ統括者は、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　セキュリティ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、選定条件及び外部サービスの選定時に定めたセキュリティ条件を調達仕様に含めること。

②　セキュリティ責任者は、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　セキュリティ責任者は、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。（クラウドサービスを利用する場合も同様の措置を行う。）

(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 セキュリティ統括者は、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規定すること。
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
オ クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策
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、構築時に実施状況を確認・記録すること。
③ クラウドサービス管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録すること。

(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 セキュリティ統括者は、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規定すること。
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
ケ 設計・設定変更時の情報や変更履歴の管理
② セキュリティ責任者は、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。
④ クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

(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 セキュリティ統括者は、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規定すること。
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。

③　クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

１１．３．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

セキュリティ統括者は、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）の利用に関する規定を整備すること。

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　セキュリティ責任者は、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。

１２．評価・見直し

１２．１．監査

(1)　実施方法

セキュリティ統括者は、情報セキュリティ監査責任者(以下、セキュリティ監査責任者）を指名し、ネットワーク、情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

(2)　監査を行う者の要件

①　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　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、セキュリティ統括者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

①　事業者に業務委託を行っている場合、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。

② クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に又は必要に応じて監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

(5) 報告

セキュリティ監査責任者は、監査結果を取りまとめ、セキュリティ統括者に報告する。

(6) 保管

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切に保管しなければならない。

(7) 監査結果への対応

セキュリティ統括者は、監査結果を踏まえ、指摘事項を所管する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、庁内で横断的に改善が必要な事項については、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。

(8) 情報セキュリティポリシー、関係規程等の見直し等への活用

セキュリティ統括者は、監査結果を情報セキュリティポリシー、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。

１２．２．自己点検

(1) 実施方法

① セキュリティ総括管理者及びセキュリティ管理者は、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 セキュリティ総括管理者は、セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、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) 報告

セキュリティ総括管理者及びセキュリティ管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、セキュリティ統括者に報告しなければならない。

(3) 自己点検結果の活用

① 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

② セキュリティ統括者は、この点検結果を情報セキュリティポリシー、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。

１２．３．情報セキュリティポリシー、関係規程等の見直し

セキュリティ統括者は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー、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。

１３．その他

この基準に定めるもののほか、この基準の実施に必要な事項は最高統括者が別に定める。

付　則

（施行期日）

１　この基準は、平成 14 年４月１日から施行する。

（経過措置）

２　この基準の適用開始日において、稼動済みの情報システムについて、この基準に適合しない事項がある場合は、１年以内に対応を図るものとする。

付　則

この基準は、平成 17 年 12 月 22 日から施行する。

付　則

この基準は、平成 19 年４月１日から施行する。

付　則

この基準は、平成 29 年５月１日から施行する。

付　則

この基準は、平成 31 年４月１日から施行する。

付　則

この基準は、令和３年４月１日から施行する。

付　則

この基準は、令和４年６月１日から施行する。

付　則

この基準は、令和５年６月１日から施行する。