砂川市情報セキュリティポリシー

（平成 30 年改定版）

砂　川　市

目　　次

第１章　総則

１　砂川市情報セキュリティポリシー

砂川市情報セキュリティポリシーとは、砂川市の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

情報セキュリティポリシーは、砂川市が所掌する情報資産に関する業務に携わる全職員、非常勤および臨時職員および外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。また、情報の処理技術や通信技術等の進歩や新たな脅威等に対応するべく、情報セキュリティポリシーの評価・見直しを行い、情報セキュリティ対策の実効性を確保する必要がある。

２　砂川市における情報セキュリティの考え方

砂川市は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを提供している。また、本市の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、ＬＧＷＡＮ等のネットワークにより相互に接続しており、発生したＩＴ障害がネットワークを介して連鎖的に拡大する可能性は否定できない。

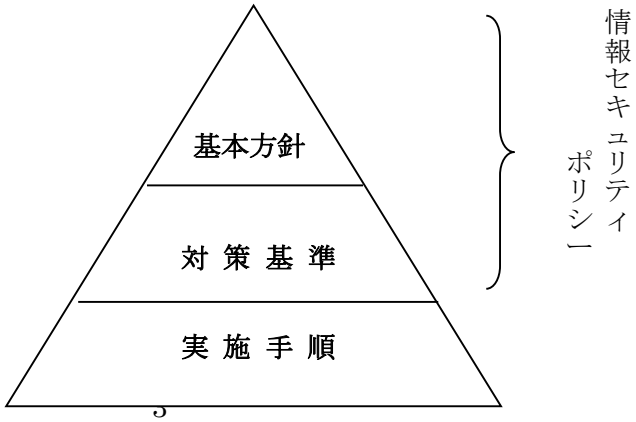
これらの事情から、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

３　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の体系は、下図に示す階層構造となっている。

砂川市の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。この基本方針に基づき、すべ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を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

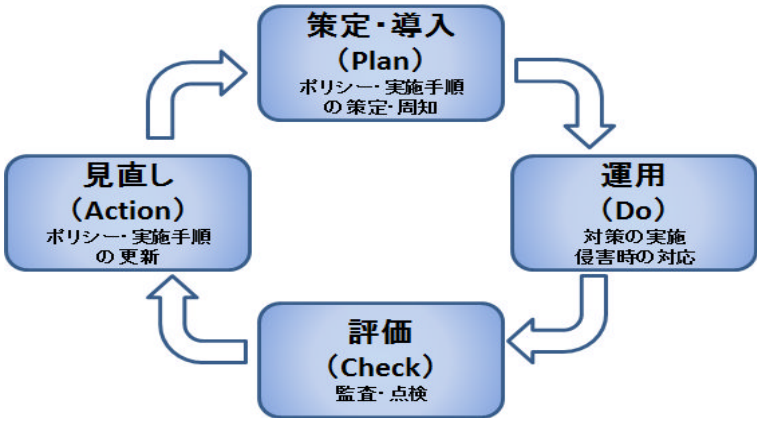
情報セキュリティポリシーに関する体系図



4　情報セキュリティ対策の実施サイクル

情報セキュリティ対策の実施プロセスは、下図に示すサイクルとなっている。策定･導入（Ｐｌａｎ）、運用（Ｄｏ）、評価（Ｃｈｅｃｋ）、見直し（Ａｃｔｉｏｎ）の４段階に分けることができ、この実施サイクルを繰り返すことによって情報セキュリティは確保される。この実施サイクルは、それぞれの項目の頭文字をとって、ＰＤＣＡサイクルとも呼ばれる。

情報セキュリティ対策のＰＤＣＡサイクル



第２章　情報セキュリティ基本方針

１　目的

本基本方針は、本市が保有する情報資産の機密性、完全性および可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

（１）　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウエアおよびソフトウエア）をいう。

（２）　情報システム

コンピュータ、ネットワークおよび記録媒体で構成され、情報処理を行う仕組みをいう。

（３）　情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

（４）　情報セキュリティポリシー

本基本方針および情報セキュリティ対策基準をいう。

（５）　機密性

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

（６）　完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

（７）　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）　ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等ＬＧＷＡＮ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。

(10)　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。

(11)　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した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12)　無害化通信

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

３　対象とする脅威

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

（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図

的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の搾取、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、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害によるサービスおよび業務の停止等

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

（５） 電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

４　適用範囲

（１） 行政機関の範囲

本基本方針が適用される行政機関は、砂川市事務分掌条例（昭和52年7月1日条例第18号）第１条に掲げる部、教育委員会、選挙管理委員会、公平委員会、監査委員および事務局、農業委員会、固定資産評価審査委員会、議会事務局、砂川市立病院、砂川地区広域消防組合および砂川地区保健衛生組合とする。

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システムおよびこれらに関する設備、電磁的記録媒体

② ネットワークおよ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およびネットワーク図等のシステム関連文書

５　職員等の遵守義務

職員、非常勤職員および臨時職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーおよび情報セキュリティ実施手順を遵守しなければならない。

６　情報セキュリティ対策

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

（１） 組織体制

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

（２） 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性および可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３） 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② 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との通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ 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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（4） 物理的セキュリティ

サーバ等、情報システム室等、通信回線等および職員等のパソコン等の管理について、物理的な対策を講じる。

（5） 人的セキュリティ

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

（6） 技術的セキュリティ

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

（7） 運用

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

（8） 外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

7 情報セキュリティ監査および自己点検の実施

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

8 情報セキュリティポリシーの見直し

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

9 情報セキュリティ対策基準の策定

上記６、７および８に規定する対策等を実施するために、具体的な遵守事項および判断基準等を定める情報セキュリティ対策基準を策定する。

10 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより本市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。

第３章　情報セキュリティ対策基準

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

１　組織体制

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

①　副市長を、ＣＩＳＯとする。ＣＩＳＯは、本市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および情報セキュリティ対策に関する最終決定権限および責任を有する。

②　ＣＩＳＯは、必要に応じ、情報セキュリティに関する専門的な知識および経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

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

（２）　情報セキュリティ管理責任者

①　総務部長をＣＩＳＯ直属の情報セキュリティ管理責任者とする。情報セキュリティ管理責任者はＣＩＳＯを補佐しなければならない。

②　情報セキュリティ管理責任者は、本市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および責任を有する。

③　情報セキュリティ管理責任者は、本市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および責任を有する。

④　情報セキュリティ管理責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報管理者および情報システム担当者に対して、情報セキュリティに関する指導および助言を行う権限を有する。

⑤　情報セキュリティ管理責任者は、本市の情報資産に対する侵害が発生した場合または侵害のおそれがある場合に、ＣＩＳＯの指示に従い、ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限および責任を有する。

⑥　情報セキュリティ管理責任者は、本市の全てのネットワーク、情報システムおよび情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限および責任を有する。

⑦　情報セキュリティ管理責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、情報セキュリティ管理責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報管理者、情報セキュリティ担当者を網羅する連絡体制を整備しなければならない。

⑧　情報セキュリティ管理責任者は、緊急時にはＣＩＳＯに早急に報告を行うとともに、回復のための対策を講じなければならない。

（３）　情報セキュリティ責任者

①　情報セキュリティ責任者は情報資産を取り扱う部長（これに準ずるものを含む）をもってこれに充てる。

②　情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限および責任を有する。

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

④　情報セキュリティ責任者は、その所管する部局等において所有している情報システムにつ

いて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、非常勤職員および臨時職員に対する教育、訓練、助言および指示を行う。

（4） 情報セキュリティ管理者

① 情報セキュリティ管理者は、総務課長をもってこれに充てる。

② 情報セキュリティ管理者は、本市の共通的なネットワーク、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および責任を有する。

③ 情報セキュリティ管理者は、本市の共通的なネットワーク、情報システムにおける情報セキュリティ対策に関する権限および責任を有する。

④ 情報セキュリティ管理者は、本市の共通的なネットワーク、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。

⑤ 情報セキュリティ管理者は、本市の共通的なネットワーク、情報システムにおいて、情報資産に対する侵害が発生した場合または侵害のおそれがある場合には、情報セキュリティ責任者、情報セキュリティ管理責任者およびＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（5） 情報管理者

① 情報管理者は情報資産を取り扱う課長（これに準ずるものを含む。）をもってこれに充てる。

② 情報管理者は、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および責任を有する。

③ 情報管理者は、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および責任を有する。

④ 情報管理者は、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。

⑤ 情報管理者は、所管する情報システムにおいて、情報資産に対する侵害が発生した場合または侵害のおそれがある場合には、情報セキュリティ責任者、情報セキュリティ管理責任者およびＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（6） 情報セキュリティ担当者

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

（7） 情報担当員

① 情報担当員は、情報資産を取り扱う課（これに準ずるものを含む。）の職員のうち、情報管理者が任命するものをもってこれに充てる。

② 情報担当員は、情報管理者を補佐し、情報管理者の指揮のもとに、所管する組織の情報セキュリティ対策を実施する。

（8） 情報セキュリティ会議

① 本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティ会議において、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決定する。

② 情報セキュリティ会議は、次に掲げる者をもって組織する。

（ア） ＣＩＳＯ

（イ） 情報セキュリティ管理責任者

（ウ） 情報セキュリティ管理者

（エ） 情報管理者

（オ） その他必要と認めるもの

③ 情報セキュリティ会議の議長

(ア) 会議に議長を置き、ＣＩＳＯをもって充てる。

(イ) ＣＩＳＯに事故があるときは、情報セキュリティ管理責任者が、その職務を代行する。

④ 情報セキュリティ会議の招集等

会議は議長が召集する。

(ア) 議長は、審議のため必要があると認めるときは関係する職員の出席を求め、その意見または説明を聴くことができる。

(イ) 会議の庶務は、総務課において処理する。

⑤ 情報セキュリティ会議は、次に掲げることを審議する。

（ア） データ漏えい、システムトラブルその他緊急時の対応策に関すること

（イ） 情報セキュリティポリシーの遵守状況の確認に関すること

（ウ） その他必要と認める事項

（9） 兼務の禁止

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

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

(10) ＣＳＩＲＴの設置・役割

① ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化すること。

② ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置くこと。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定めること。

③ ＣＩＳＯは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より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すること。

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

⑤ 情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、都道府県等へ報告すること。

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

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

２ 情報資産の分類と管理

（1） 情報資産の分類

本市における情報資産は、次の重要性分類に従って分類する。さらに重要性分類で分類された情報資産毎に機密性、完全性および可用性により、次のとおり細分化し、必要に応じ取扱制限を行うものとする。

重要性による情報資産の分類

① 重要性分類Ⅰ

（ア） 砂川市個人情報保護条例に規定する個人情報および特定個人情報

（イ） 法令または条例の定めにより守秘義務を課されている情報

（ウ） 法人その他の団体に関する情報で漏えいすることにより当該団体の利益を害するおそれのあるもの

（エ） 情報システムに係るパスワードおよびシステム設定情報

② 重要性分類Ⅱ

（ア） 公開することを予定していない情報

（イ） セキュリティ侵害が、行政事務の執行等に重大な影響を及ぼす情報

（ウ） 漏えいした場合、行政に対する信頼を著しく害するおそれのある情報
（エ） 滅失または棄損した場合、その復元が著しく困難となり、行政の円滑な執行を妨げるおそれのある情報

③ 重要性分類Ⅲ
外部に公開する情報のうち、セキュリティ侵害が行政事務の執行等に軽微な影響を及ぼす情報

④ 重要性分類Ⅳ
上記以外の情報

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	行政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	・私物パソコンでの作業禁止（機密性３の情報資産に対して） ・必要以上の複製および配付禁止 ・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 ・外部記録媒体の施錠可能な場所への保管
機密性２	行政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または機密性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	行政事務で取り扱う情報資産のうち、改ざん、誤謬または破損により、住民の権利が侵害される、また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、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・外部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	行政事務で取り扱う情報資産のうち、滅失、紛失また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、または行政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、指定する時間以内の復旧 ・外部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） 情報管理者は、その所管する情報資産について管理責任を有する。

（イ） 情報資産が複製または伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する外部記録媒体(ＣＤ－Ｒのラベル等)、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正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） 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

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

（ウ） 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤ 情報資産の利用

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

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

⑥ 情報資産の保管

（ア） 情報管理者または情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ） 情報管理者または情報セキュリティ管理者は、情報資産を記録した外部記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ） 情報管理者または情報セキュリティ管理者は、機密性２以上、完全性２または可用性２の情報を記録した外部記録媒体を保管する場合、耐火、耐熱、耐水およ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、必要に応じ暗号化またはパスワード設定を行わなければならない。

⑧ 情報資産の運搬

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

⑨ 情報資産の提供・公表
（ア） 機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化またはパスワードの設定を行わなければならない。
（イ） 機密性２以上の情報資産を外部に提供する者は、情報管理者に許可を得なければならない。
（ウ） 情報管理者は、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
（ア） 機密性２以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。
（イ） 情報資産の廃棄を行う者は、行った処理について、日時、担当者および処理内容を記録しなければならない。
（ウ） 情報資産の廃棄を行う者は、情報管理者の許可を得なければならない。

３ 情報システム全体の強靭性の向上

（１）マイナンバー利用事務系
① マイナンバー利用事務系と他の領域との分離
マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。
② 情報のアクセス及び持ち出しにおける対策
（ア）情報のアクセス対策
情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。
（イ）情報の持ち出し不可設定
原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。
（２）ＬＧＷＡＮ接続系
① ＬＧＷＡＮ接続系とインターネット接続系の分割
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接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。
（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
（３）インターネット接続系
① インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び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 市区町村のインターネット接続口を集約する自治体情報セキュリティクラウドに参加する

とともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

４　物理的セキュリティ

４．１　サーバ等の管理

（１）　機器の取付け

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

（２）　サーバの冗長化

①　情報セキュリティ管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバおよびその他の基幹系サーバを冗長化し、同一データを保持しなければならない。

②　情報セキュリティ管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

（３）　機器の電源

①　情報セキュリティ管理者は、情報セキュリティ管理責任者および施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②　情報セキュリティ管理者は、情報セキュリティ管理責任者および施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（４）　通信ケーブル等の配線

①　情報セキュリティ管理責任者および情報セキュリティ管理者は、施設管理部門と連携し、通信ケーブルおよび電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

②　情報セキュリティ管理責任者および情報セキュリティ管理者は、主要な箇所の通信ケーブルおよび電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③　情報セキュリティ管理責任者および情報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正に管理しなければならない。

④　情報セキュリティ管理責任者、情報セキュリティ管理者は、自らまたは情報セキュリティ担当者および契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（５）　機器の定期保守および修理

①　情報セキュリティ管理者は、可用性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　情報セキュリティ管理者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティ管理者は、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

（6） 敷地外への機器の設置

情報セキュリティ管理責任者および情報セキュリティ管理者は、庁舎の敷地外にサーバ等の機器を設置する場合、ＣＩＳＯの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（7） 機器の廃棄等

情報管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

４．２　管理区域(サーバ室等)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および重要な情報システムを設置し、当該機器等の管理ならびに運用を行うための部屋(以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

② 情報セキュリティ管理責任者および情報セキュリティ管理者は、管理区域を地階又は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しなければならない。

③ 情報セキュリティ管理責任者および情報セキュリティ管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④ 情報セキュリティ管理責任者および情報セキュリティ管理者は、サーバ室内の機器等に、転倒および落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤ 情報セキュリティ管理責任者および情報セキュリティ管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

⑥ 情報セキュリティ管理責任者および情報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、機器等および記録媒体に影響を与えないようにしなければならない。

（2） 管理区域の入退室管理等

① 情報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、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

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

③ 情報セキュリティ管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④ 情報セキュリティ管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、外部記録媒体等を持ち込ませないようにしなければならない。

（3） 機器等の搬入出

① 情報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、あらかじめ職員または委託した業者に確認を行わせなければならない。

② 情報セキュリティ管理者は、サーバ室の機器等の搬入出について、職員を立ち会わせなければならない。

４．３　通信回線および通信回線装置の管理

① 情報セキュリティ管理責任者は、庁内の通信回線および通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線および通信回線装置に関連する文書を適正に保管しなければならない。

② 情報セキュリティ管理責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。
③ 情報セキュリティ管理責任者は、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 情報セキュリティ管理責任者は、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、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
⑤ 情報セキュリティ管理責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。
⑥ 情報セキュリティ管理責任者は、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。

４．４　職員等のパソコン等の管理

① 情報セキュリティ管理者は、執務室等のパソコン等の端末について、盗難防止のための措置を講じなければならない。また、外部記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
② 情報セキュリティ管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報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 情報セキュリティ管理者は、ＢＩＯＳ パスワード、ハードディスクパスワード等を併用しなければならない。
④ 情報セキュリティ管理者は、マイナンバー利用事務系では「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（多要素認証等）を行うよう設定しなければならない。
⑤ 情報セキュリティ管理者は、パソコンやモバイル端末等のデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。
⑥ 情報セキュリティ管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、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。

５　人的セキュリティ

５．１　職員等の遵守事項

（１） 職員等の遵守事項

① 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシーおよび実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報管理者に相談し、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およびインターネットへのアクセスを行ってはならない。

③ パソコン等の端末の持ち出しおよび外部における情報処理作業の制限

（ア） ＣＩＳＯ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、本市のパソコン等の端末、記録媒体、情報資産およびソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者または情報管理者の許可を得なければならない。

（ウ） 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者または情報管理者の許可を得なければならない。

（エ） 職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理者または情報管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

④ パソコン等の端末等の持込

（ア） 職員等は、私物のパソコン、モバイル端末および記録媒体を庁舎内に持ち込んではならない。ただし、業務上必要な場合は、情報セキュリティ管理者または情報管理者の許可を得て、これらを持ち込むことができる。

（イ） 職員等は、私物のパソコン、モバイル端末および記録媒体を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤ 持ち出しおよび持ち込みの記録

情報セキュリティ管理者および情報管理者は、パソコンやモバイル端末および記録媒体等の持ち出しおよ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 パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者および情報管理者の許可なく変更してはならない。

⑦ 机上の端末等の管理

職員等は、パソコン、モバイル端末、記録媒体およ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、または情報管理者の許可なく情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（２） 非常勤および臨時職員への対応

① 情報セキュリティポリシー等の遵守

情報管理者は、非常勤および臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤および臨時職員が守るべき内容を理解させ、また実施および遵守させなければならない。

② 情報セキュリティポリシー等の遵守に対する同意

情報管理者は、非常勤および臨時職員の採用の際、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および電子メール使用等の制限

情報セキュリティ管理者および情報管理者は、非常勤および臨時職員にパソコンやモバイル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および電子メールの

使用等が不要の場合、これを利用できないようにしなければならない。

（3） 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシーおよ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） 外部委託事業者に対する説明

情報セキュリティ管理者および情報管理者は、ネットワークおよび情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守およびその機密事項を説明しなければならない。

５．２　研修・訓練

（1） 情報セキュリティに関する研修・訓練

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

（2） 研修計画の立案および実施

① ＣＩＳＯは、幹部を含めすべての職員等に対する情報セキュリティに関する研修計画を定期的に立案し、情報セキュリティ会議の承認を得なければならない。

② 研修計画において、職員等は適宜、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、情報セキュリティ管理責任者、情報セキュリティ責任者、情報管理者、情報セキュリティ管理者、情報セキュリティ担当者、情報担当員およびその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤ ＣＩＳＯは、毎年度１回、情報セキュリティ会議に対して、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

ＣＩＳＯ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、ネットワークおよ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

幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

５．３　情報セキュリティインシデントの報告

（1） 庁内での情報セキュリティインシデントの報告

① 職員等は、情報セキュリティに関する事故、システム上の欠陥および誤動作を発見した場合、速やかに情報管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

② 報告を受けた情報管理者は、当該事故等が情報システムに関連する場合、速やかに情報セキュリティ管理責任者および情報セキュリティ管理者に報告しなければならない。

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

（2） 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、本市が管理するネットワークおよび情報システム等の情報資産に関する事故、

欠陥について、住民等外部から報告を受けた場合、情報管理者に報告しなければならない。

② 報告を受けた情報管理者は、当該事故等が情報システムに関連する場合、速やかに情報セキュリティ管理責任者および情報セキュリティ管理者に報告しなければならない。また、当該事故等がネットワークに関連する場合は、情報セキュリティ管理責任者に報告しなければならない。

③ 情報管理者は、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ＣＩＳＯおよび情報セキュリティ責任者に報告しなければならない。

④ ＣＩＳＯは、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（3） 情報セキュリティインシデント原因の究明・記録、再発防止等

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

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

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

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

⑤ ＣＩＳＯは、ＣＳＩＲＴから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

５．４ ＩＤおよびパスワード等の管理

（1） ＩＣカード等の取扱い

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

（ア） 認証に用いるＩＣカード等を、職員等間で共有してはならない。

（イ） 業務上必要のないときは、ＩＣカード等をカードリーダもしくはパソコン等の端末のスロット等から抜いておかなければならない。

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

② 情報セキュリティ管理責任者および情報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 情報セキュリティ管理責任者および情報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の取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

① 自己が利用しているＩＤは、他人に利用させてはならない。

② 共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（3） パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

② パスワードを記載したメモを作成してはならない。

③ パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④　パスワードが流出したおそれがある場合には、情報管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
⑤　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑥　仮のパスワード(初期パスワード含む)は、最初のログイン時点で変更しなければならない。
⑦　サーバ、ネットワーク機器及びパソコン等の端末のパスワードの記憶機能を利用してはならない。
⑧　職員等間でパスワードを共有してはならない(ただし共有ＩＤ に対するパスワードは除く)。

６　技術的セキュリティ

６．１　コンピュータおよびネットワークの管理

（１）　文書サーバの設定等
①　情報セキュリティ管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。
②　情報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およびファイルを閲覧および使用できないように、設定しなければならない。
③　情報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および使用できないようにしなければならない。

（２）　バックアップの実施
情報セキュリティ管理責任者および情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

（３）　他団体との情報システムに関する情報等の交換
情報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およ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、情報セキュリティ管理責任者および情報セキュリティ責任者の許可を得なければならない。

（４）　システム管理記録および作業の確認
①　情報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　情報セキュリティ管理責任者および情報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、窃取、改ざん等をされないよう、適正に管理しなければならない。
③　情報セキュリティ管理責任者、情報セキュリティ管理者または情報セキュリティ担当者および契約により操作を認められた外部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
情報セキュリティ管理責任者および情報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、適正に管理しなければならない。

（６）　ログの取得等
①　情報セキュリティ管理責任者および情報セキュリティ管理者は、各種ログおよび情報セキ

ュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。
② 情報セキュリティ管理責任者および情報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、取得方法およびログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。
③ 情報セキュリティ管理責任者および情報セキュリティ管理者は、取得したログを定期的に点検また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または分析を実施しなければならない。

（7） 障害記録

情報セキュリティ管理責任者および情報セキュリティ管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果または問題等を、障害記録として記録し、適正に保存しなければならない。

（8） ネットワークの接続制御、経路制御等

① 情報セキュリティ管理責任者は、フィルタリングおよびルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
② 情報セキュリティ管理責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（9） 外部の者が利用できるシステムの分離等

情報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およ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 情報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、ＣＩＳＯおよび情報セキュリティ管理責任者の許可を得なければならない。
② 情報セキュリティ管理者は、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、庁内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
③ 情報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、改ざんまたはシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。
④ 情報セキュリティ管理責任者および情報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うえで接続しなければならない。
⑤ 情報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、情報セキュリティ管理責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11) 複合機のセキュリティ管理

① 情報セキュリティ管理責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類および管理方法に応じ、適正なセキュリティ要件を策定しなければならない。
② 情報セキュリティ管理責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する事故等への対策を講じなければならない。
③ 情報セキュリティ管理責任者は、複合機の運用を終了する場合、複合機が持つ記録媒体の全ての情報を抹消または再利用できないように対策を講じなければならない。

(12) 特定用途機器のセキュリティ管理

情報セキュリティ管理責任者は、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講じなければならない。

(13) 無線ＬＡＮ およびネットワークの盗聴対策

① 情報セキュリティ管理責任者は、無線LAN の利用を認める場合、解読が困難な暗号化および認証技術の使用を義務づけなければならない。

② 情報セキュリティ管理責任者は、機密性の高い情報を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 情報セキュリティ管理責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② 情報セキュリティ管理責任者は、大量のスパムメール等の受信または送信を検知した場合は、メールサーバの運用を停止しなければならない。

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

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

⑤ 情報セキュリティ管理責任者は、システム開発や運用等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。

⑥ 情報セキュリティ管理責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことがないように措置を講じなければならない。

(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送信する必要がある場合には、事前に情報管理者に許可を得なければならない。

⑤ 職員等は、重要な電子メールを誤送信した場合、情報管理者に報告しなければならない。

⑥ 職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用する必要がある場合には、事前に情報管理者に許可を得なければならない。

(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または完全性を確保することが必要な場合には、ＣＩＳＯが定めた電子署名、暗号化またはパスワード設定の方法を使用して、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ＣＩＳＯが定める以外の方法を用いてはならない。また、ＣＩＳＯが定めた方法で暗号のための鍵を管理しなければならない。

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

(17) 無許可ソフトウェアの導入等の禁止

① 職員等は、パソコン等の端末に無断でソフトウェアを導入してはならない。

② 職員等は、業務上の必要がある場合は、情報セキュリティ管理責任者および情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情

報セキュリティ管理責任者および情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

③　職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18)　機器構成の変更の制限

①　職員等は、パソコン等の端末に対し機器の改造および増設・交換を行ってはならない。

②　職員等は、業務上、パソコンやモバイル端末に対し機器の改造および増設・交換を行う必要がある場合には、情報セキュリティ管理責任者および情報セキュリティ管理者の許可を得なければならない。

(19)　無許可でのネットワーク接続の禁止

職員等は、情報セキュリティ管理責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

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

６．２　アクセス制御

（1）　アクセス制御

①　アクセス制御

情報セキュリティ管理責任者または情報セキュリティ管理者は、所管するネットワークまたは情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②　利用者ＩＤの取扱い

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

（イ）　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報セキュリティ管理責任者または情報セキュリティ管理者に通知しなければならない。

（ウ）　情報セキュリティ管理責任者および情報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、人事管理部門と連携し、点検しなければならない。

③　特権を付与されたＩＤの管理等

（ア）　情報セキュリティ管理責任者および情報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およびパスワードを厳重に管理しなければならない。

（イ）　情報セキュリティ管理責任者および情報セキュリティ管理者の特権を代行する者は、情報セキュリティ管理責任者および情報セキュリティ管理者が指名し、ＣＩＳＯが認めた者でなければならない。

（ウ）　ＣＩＳＯは、代行者を認めた場合、速やかに情報セキュリティ管理責任者、情報セキュリティ責任者、情報管理者および情報セキュリティ管理者に通知しなければならない。

（エ）　情報セキュリティ管理責任者および情報セキュリティ管理者は、特権を付与されたＩＤおよびパスワードの変更について、外部委託事業者に行わせてはならない。

（オ）　情報セキュリティ管理責任者および情報セキュリティ管理者は、特権を付与されたＩＤおよ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） 情報セキュリティ管理責任者および情報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または情報システムにアクセスする場合は、情報セキュリティ管理責任者および当該情報システムを管理する情報セキュリティ管理者の許可を得なければならない。

② 情報セキュリティ管理責任者は、内部のネットワークまたは情報システムに対する外部からのアクセスをアクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③ 情報セキュリティ管理責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④ 情報セキュリティ管理責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤ 情報セキュリティ管理責任者および情報セキュリティ管理者は、外部からのアクセスに利用するパソコン等の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、持ち込んだまたは外部から持ち帰ったパソコン等の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なければならない。

⑦ 情報セキュリティ管理責任者は、公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３） 自動識別の設定

情報セキュリティ管理責任者および情報セキュリティ管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（４） ログイン時の表示等

情報セキュリティ管理者は、ログイン時におけるメッセージおよ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・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（５） 認証情報の管理

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

② 情報セキュリティ管理責任者又は情報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。

（６） 特権による接続時間の制限

情報セキュリティ管理者は、特権によるネットワークおよび情報システムへの接続時間を必要最小限に制限しなければならない。

６．３　システム開発、導入、保守等

（１）　情報システムの調達

①　情情報セキュリティ管理責任者および情報セキュリティ管理者または情報セキュリティ責任者および情報管理者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②　情報セキュリティ管理責任者および情報セキュリティ管理者または情報セキュリティ責任者および情報管理者は、機器およびソフトウェアの調達にあたっては、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および作業者の特定

情報セキュリティ管理者または情報管理者は、システム開発の責任者および作業者を特定しなければならない。

②　システム開発における責任者、作業者のＩＤの管理

（ア）　情報セキュリティ管理者または情報管理者は、システム開発の責任者および作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）　情報セキュリティ管理者または情報管理者は、システム開発の責任者およ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およびソフトウェアの管理

（ア）　情報セキュリティ管理者または情報管理者は、システム開発の責任者および作業者が使用するハードウェアおよびソフトウェアを特定しなければならない。

（イ）　情報セキュリティ管理者または情報管理者は、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および移行手順の明確化

（ア）　情報セキュリティ管理者または情報管理者は、システム開発、保守およびテスト環境とシステム運用環境を分離しなければならない。

（イ）　情報セキュリティ管理者または情報管理者は、システム開発・保守およ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。

（ウ）　情報セキュリティ管理者または情報管理者は、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。

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

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

（ウ）　情報セキュリティ管理者または情報管理者は、個人情報および機密性の高い生データを、テストデータに使用してはならない。

（エ）　情報セキュリティ管理者または情報管理者は、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保管

① 情報セキュリティ管理者または情報管理者は、システム開発・保守に関連する資料および文書を適正な方法で保管しなければならない。

② 情報セキュリティ管理者または情報管理者は、テスト結果を一定期間保管しなければならない。

③ 情報セキュリティ管理者または情報管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（5） 情報システムにおける入出力データの正確性の確保

① 情報セキュリティ管理者または情報管理者は、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および不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② 情報セキュリティ管理者または情報管理者は、故意または過失により情報が改ざんされるまた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 情報セキュリティ管理者または情報管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（6） 情報システムの変更管理

情報セキュリティ管理者または情報管理者は、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

情報セキュリティ管理者または情報管理者は、開発・保守用のソフトウェア等を更新、また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） システム更新または統合時の検証等

情報セキュリティ管理者または情報管理者は、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。

6．4 不正プログラム対策

（1） 情報セキュリティ管理責任者の措置事項

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

① 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

② 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

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

④ 所掌するサーバおよびパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

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。

（2）　情報セキュリティ管理者の措置事項

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

①　情報セキュリティ管理者は、その所掌するサーバおよびパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

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

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

④　インターネットに接続していないシステムにおいて、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、市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およびパターンファイルの更新を実施しなければならない。

（3）　職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①　パソコン等の端末において、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　外部からデータまた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　差出人が不明または不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

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

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

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

⑦　コンピュータウイルス等の不正プログラムに感染した場合または感染が疑われる場合は、以下の対応が行わなければならない。

（ア）　パソコン等の端末の場合

ＬＡＮケーブルの即時取り外しを行わなければならない。

（イ）　モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

６．５　不正アクセス対策

（1）　情報セキュリティ管理責任者の措置事項

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

①　使用されていないポートを閉鎖しなければならない。

②　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、情報セキュリティ管理責任者および情報セキュリティ管理者へ通報するよう、設定しなければならない。

③　重要なシステムの設定を行った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しなければならない。

④　情報セキュリティ管理責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、

通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2） 攻撃への対処

ＣＩＳＯおよび情報セキュリティ管理責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

（3） 記録の保存

ＣＩＳＯおよび情報セキュリティ管理責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察および関係機関との緊密な連携に努めなければならない。

（4） 内部からの攻撃

情報セキュリティ管理責任者および情報セキュリティ管理者または情報セキュリティ責任者および情報管理者は、職員等および外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5） 職員等による不正アクセス

情報セキュリティ管理責任者、情報セキュリティ管理者および情報管理者は、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情報管理者に通知し、適正な処置を求めなければならない。

（6） サービス不能攻撃

情報セキュリティ管理責任者、情報セキュリティ管理者および情報管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（7） 標的型攻撃

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

６．６　セキュリティ情報の収集

（1） セキュリティホールに関する情報の収集・共有およびソフトウェアの更新等

情報セキュリティ管理責任者および情報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） 不正プログラム等のセキュリティ情報の収集・周知

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

（3） 情報セキュリティに関する情報の収集及び共有

情報セキュリティ管理責任者、情報セキュリティ管理者および情報管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリテ

ィ侵害を未然に防止するための対策を速やかに講じなければならない。

7　運用

7．1　情報システムの監視

① 情報セキュリティ管理責任者および情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
② 情報セキュリティ管理責任者および情報セキュリティ管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定およびサーバ間の時刻同期ができる措置を講じなければならない。
③ 情報セキュリティ管理責任者および情報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。

7．2　情報セキュリティポリシーの遵守状況の確認

（1） 遵守状況の確認および対処

① 情報セキュリティ責任者、情報セキュリティ管理者および情報管理者は、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ＣＩＳＯおよび情報セキュリティ管理責任者に報告しなければならない。
② ＣＩＳＯは、発生した問題について、適正かつ速やかに対処しなければならない。
③ 情報セキュリティ管理責任者および情報セキュリティ管理者またはセキュリティ責任者および情報管理者は、ネットワークおよびサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（2） パソコン、モバイル端末および外部記録媒体等の利用状況調査

ＣＩＳＯおよびＣＩＳＯが指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末および外部記録媒体等のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

（3） 職員等の報告義務

① 職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ管理者および情報管理者に報告を行わなければならない。
② 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ管理責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

7．3　侵害時の対応等

（1） 緊急時対応計画の策定

ＣＩＳＯまたは情報セキュリティ会議は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産へのセキュリティ侵害が発生した場合また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正に実施するために、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） 事業継続計画との整合性確保

自然災害等に備えて事業継続計画を策定する場合、情報セキュリティ会議は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（4） 緊急時対応計画の見直し

ＣＩＳＯまたは情報セキュリティ会議は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

７．４ 例外措置

（1） 例外措置の許可

情報管理者および情報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し、または遵守事項を実施しないことについて合理的な理由がある場合には、ＣＩＳＯの許可を得て、例外措置を講じることができる。

（2） 緊急時の例外措置

情報管理者および情報セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにＣＩＳＯに報告しなければならない。

（3） 例外措置の申請書の管理

ＣＩＳＯは、例外措置の申請書および審査結果を適正に保管しなければならない。

７．５ 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

① 地方公務員法(昭和二十五年十二月十三日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（平成十五年五月三十日法律第五十七号）
⑤ 行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成二五年法律第二十七号）
⑥ サイバーセキュリティ基本法（平成二十八年法律第三十一号）
⑦ 砂川市個人情報保護条例（平成十四年三月二十日条例第一号）

７．６ 懲戒処分等

（1） 懲戒処分

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

（2） 違反時の対応

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

① 情報セキュリティ管理責任者が違反を確認した場合は、当該職員等が所属する課等の情報管理者に通知し、適正な措置を求めなければならない。

② 情報セキュリティ管理者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情報セキュリティ管理責任者および当該職員等が所属する課等の情報管理者に通知し、適正な措置を求めなければならない。

③ 情報管理者の指導によっても改善されない場合、情報セキュリティ管理責任者は、当該職員等のネットワークまたは情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ管理責任者は、職員等の権利を停止あるいは剥奪した旨をＣＩＳＯおよび当該職員等が所属する課等の情報管理者に通知しなければならない。

８　外部サービスの利用

８．１　外部委託

（1） 外部委託先の選定基準

① 情報管理者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② 情報管理者は、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等を参考にして、事業者を選定しなければならない。

③ 情報管理者は、クラウドサービスを利用する場合は、個人の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（2） 契約項目

情報システムの運用等を外部委託する場合には、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および情報セキュリティ実施手順の遵守
- 委託先の責任者、委託内容、作業者の所属、作業場所の特定
- 提供されるサービスレベルの保証
- 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および受託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および緊急時報告義務
- 市による監査、検査
- 市による情報セキュリティインシデント発生等の公表
- 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

情報管理者および情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（2）の契約に基づき措置を実施しなければならない。また、その内容を情報セキュリティ管理責任者に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

８．２　約款による外部サービスの利用

（1） 約款による外部サービスの利用に係る規定の整備

情報管理者および情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報が取り扱われるよう規定しなければならない。

① 約款によるサービスを利用して良い範囲
② 業務により利用する約款による外部サービス
③ 利用手続および運用手順

（2） 約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

８．３ ソーシャルメディアサービスの利用

① 情報管理者および情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービスの運用手順を定めなければならない。

（ア） 本市のアカウントによる情報発信が実際に本市のものであることを明らかにするために、本市の自己管理ウェイブサイトに当該情報を記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およびこれを記録した媒体（ＩＣカード等）等を適正に管理する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。

９ 評価・見直し

９．１ 監査

（1） 実施方法

情報セキュリティ会議は、情報セキュリティ監査統括責任者を指名し、ネットワークおよび情報システム等の情報資産における情報セキュリティ対策状況について、定期的にまたは必要に応じて監査を行わせなければならない。

（2） 監査を行う者の要件

① 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。
② 監査を行う者は、監査およ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および実施への協力

① 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ会議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） 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的にまたは必要に応じて行わなければならない。

（5） 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ会議に報告する。

（6） 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

（7） 監査結果への対応

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報管理者に対しても、同種の課題および問題点がある可能性が高い場合には、当該課題および問題点の有無を確認させなければならない。

（8） 情報セキュリティポリシーの見直し等への活用

情報セキュリティ会議は、監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．２　自己点検

（1） 実施方法

① 情報セキュリティ管理責任者および情報セキュリティ管理者または情報セキュリティ責任者および情報管理者は、所管するネットワークおよび情報システムについて、定期的にまたは必要に応じ自己点検を実施しなければならない。

② 情報セキュリティ責任者は、情報管理者と連携して、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、毎年度または必要に応じ自己点検を行わなければならない。

（2） 報告

情報セキュリティ管理責任者、情報セキュリティ責任者、情報セキュリティ管理者および情報管理者は、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、情報セキュリティ会議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 情報セキュリティ会議は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．３　情報セキュリティポリシーおよび関係規定等の見直し

情報セキュリティ会議は、情報セキュリティ監査および自己点検の結果ならびに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシーおよび関係規定等について毎年度およ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。

用語解説

索引	用　語	解　　説
あ	ＩＣカード	薄い半導体集積回路(ＩＣチップ)を埋め込み、情報を記録できるようにしたカードのこと。大容量のデータを記録でき、データの暗号化も可能であるため安全性が高い。情報システムを利用する際の認証にも用いられる。
	アクセス記録	サーバの利用状況を記録すること。利用者のＩＰアドレスや利用された日付と時刻、利用されたファイル名などを記録する。
	アクセス権限	コンピュータの利用者に与えられた、ハードディスクなどに保存されたファイルやフォルダ、あるいは接続された周辺機器などを利用する権限のこと。
	アクセス制御	ハードディスクなどに保存されたファイルやフォルダ、あるいは接続された周辺機器などに対し、許可された者以外の利用や、許可された方式以外での利用を防止すること。
	暗号化	インターネットなどのネットワークを通じて文書や画像などのデジタルデータをやり取りする際に、通信途中で第三者に盗み見られたり、改ざんされたりされないよう、決まった規則に従ってデータを変換すること。
か	外部委託 (情報システムの外部委託)	情報システムに関する企画、開発、保守および運用等の情報処理業務の一部または全部を庁外の者に請け負わせること。
	外部からのアクセス	インターネット等を通じて庁外のネットワークから庁内のネットワークに接続すること。
	外部ネットワーク	インターネット等の庁外のネットワークのこと。
	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。
	監視 (情報システムの監視)	情報システムへの攻撃等を防ぐため、情報システムの稼働状況を常に監視すること。
	完全性	情報が破壊、改ざんまたは消去されていない状態を確保すること。
	管理区域	ネットワークの基幹機器および重要な情報システム機器を設置し、当該機器等の管理並びに運用を行うための場所（サーバー室等）や外部記録媒体の保管庫を指す。
	技術的セキュリティ	コンピュータの管理やアクセス制御等技術的なセキュリティのこと。
	機密性	情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保すること。
	外部記録媒体	情報を記憶するための媒体（メディア）のこと。例えば、ハードディスク、ＵＳＢメモリ、ＣＤ、ＤＶＤ、ＳＤカードなど。
	緊急時対応訓練	情報漏えいやサイバー攻撃等の事故が発生した場合に対応できる態勢を構築しておくために緊急時を想定した訓練のこと。
	緊急時対応計画	情報資産への侵害が発生した場合等に備えて、あらかじめ実施すべき具体的な措置を定めた計画のこと。
	経路制御(routing)	データを目的地まで送信するために、コンピュータネットワーク上のデータ配送経路を決定する制御のこと。
	コンピュータウイルス	インターネット等を介してコンピュータに入り込み、意図的に悪影響を及ぼすように作られたプログラム。悪意のあるものは、プログラムやデータ等のファイルの破壊、情報の漏えいなどを引き起こす。
さ	サービス不能攻撃	ネットワークを通じた攻撃の一つであり、相手のコンピュータやルータなどに不正なデータを送信して使用不能にし、トラフィックを増大させて相手のネットワークを麻痺させる攻撃のこと。ＤｏＳ攻撃(Denial of service attack)など
	事業継続計画(BCP)	災害等の問題発生シナリオに基づいて、具体的な作業手順を定め、事業等が停止する時間を可能な限り少なくする目的で作られる管理計画のこと。ＢＣＰ(Business Continuity Plan)

自己点検	情報システムを運用する職員等が情報セキュリティポリシーに基づく履行状況等を自ら点検、評価すること。
時刻同期	サーバ間で時刻設定を自動的に合わせること。
システム管理記録	情報システムの状況を正確に把握するため、情報システムに対して行った作業を記録しておくこと。
システム関連文書	システム設計書やプログラム仕様書等保有する情報システムに関わる文書のこと。
自動識別	ネットワークに不正な機器の接続を防止するため、機器固有情報によって端末とネットワークとの接続の可否を自動的に識別すること。
守秘義務契約	外部委託先等に対し、業務上知りえた情報を漏らさないことを義務づける契約のこと。
障害記録	システム障害の内容や発生期日等を記録したもの。システム障害への対応時に過去に起きた類似障害を参考とするため、適切に保存する。
情報管理者	担当課等の情報セキュリティに関する権限および責任を有する者のこと。
情報資産	ネットワーク、情報システム、これらに関する施設・設備、電磁的記録媒体、ネットワーク等で取り扱う情報およびシステム関連文書等のこと。
情報資産の分類	重要性、機密性、完全性および可用性の度合いに応じて情報資産の分類を行うこと。
情報システム	コンピュータ・ネットワークおよび記録媒体で構成され、情報処理を行うシステムのこと。
情報システム仕様書	情報システムの仕様（スペック）を記載した文書のこと。
情報セキュリティ	情報資産の機密性、完全性および可用性を維持すること。
情報セキュリティ会議	情報セキュリティポリシーの決定等、情報セキュリティに関する重要な事項を決定する機関のこと。
情報セキュリティ監査	ネットワーク、情報システム等における情報セキュリティ対策の実施状況について、客観的に専門的見地から評価し、関係者に改善事項等の助言、勧告を行うこと。
ＣＩＳＯ（最高情報セキュリティ責任者）	砂川市におけるすべてのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限および責任を有する者のこと。
情報セキュリティ管理責任者	ＣＩＳＯ（最高情報セキュリティ責任者）直属で、ＣＩＳＯを補佐し、当該団体の全てのネットワークにおける開発や情報セキュリティ等に関する権限および責任を有する者のこと。
情報セキュリティ責任者	担当部局等の情報セキュリティ対策に関する統括的な権限および責任を有する者のこと。
情報セキュリティ管理者	個々の情報システムの開発、設定の変更、運用、見直し等および当該情報システムに対する情報セキュリティ対策に関する権限および責任を有する者のこと。
情報管理者	所管する情報システムの開発、設定の変更、運用、見直し等の作業を行う権限および責任を有する者のこと。
情報セキュリティ担当者	情報システムの開発、設定の変更、運用、見直し等の作業を行う者のこと。
情報セキュリティ基本方針	情報セキュリティ対策の目的、体系等、各地方公共団体の情報セキュリティに対する基本的な考え方を定めた文書のこと。
情報セキュリティ実施手順	情報セキュリティ対策基準に基づき、職員等関係者が、各々の扱うネットワークおよび情報システムや携わる業務において、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかについて定めたマニュアルのこと。
情報セキュリティ対策	情報セキュリティを確保する対策のこと。
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、すべての情報システムに共通の情報セキュリティ対策を規定する文書のこと。

さ	情報セキュリティポリシー	組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書のことであり、「基本方針」と「対策基準」の総称のこと。
	職員等	本セキュリティポリシーにおいては、職員、非常勤職員および臨時職員を意味する。
	人的セキュリティ	情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育および啓発を行う等の人的な対策を講じること。
	スパムメール(Spam Mail)	受信者の都合を無視し、無差別に大量配信される迷惑メールのこと。
	セキュリティチップ	さまざまなセキュリティ機能を利用できる暗号化専用のチップのこと。
	セキュリティホール(Security Hole)	ソフトウェアの設計ミスなどによって生じた、システムのセキュリティ上の弱点のこと。
	総合行政ネットワーク	地方公共団体間を相互に接続する行政専用ネットワークのこと。 ＬＧＷＡＮ（Local Government Wide Area Network）
	ソースコード(SourceCode)	プログラミング言語を用いて記述したプログラムのこと。
	端末	ネットワーク経由でホストコンピュータと接続し、データの入出力などの操作を行うパソコン等の装置のこと。
	通信回線	情報を伝送する回線・ネットワークのこと。
	通信回線装置	通信回線に接続して、通信を行うための装置。ルータ等。
た	電子署名	デジタル文書の正当性を保証するために付けられる署名情報のこと。
	特権	情報システムにおいて一般の利用者が利用できない機能を利用することが認められた権限。管理者権限等。
な	ネットワーク	コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェアおよびソフトウェア）のこと。
	ネットワークストレージサービス	ネットワーク上でファイル保管用のディスクスペースにデータを保存することができるサービスのこと。
は	ハードディスクパスワード	盗まれても中身がコピー等されないようにするため、ハードディスクに設定するパスワードのこと。
	パスワード	暗証番号。コンピュータシステムに正当なユーザーであることを示すため、データベースや情報サービスなどを利用する際に必要となる。
	パターンファイル	ウイルス対策ソフトがウイルスを発見するための参考にするファイル。コンピュータウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録している。
	バックアップ	コンピュータに保存されたデータやプログラムを、破損やコンピュータウイルス感染などの事態に備え、別の記憶媒体に保存すること。
	パッチ	一旦完成したプログラムの一部を修正すること。また、修正を行なうために変更点(差分情報)のみを抜き出したファイルのこと。
	ファイアウォール	組織内のネットワークへ外部から侵入されるのを防ぐシステムのこと。 Firewall
	不正アクセス	政府機関、企業、団体等の内部のネットワークに外部から不正に侵入する行為のこと。
	不正プログラム	コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称。ウイルス、スパイウェアなど。
	物理的セキュリティ	サーバ、情報システム室、通信回線および職員等のパソコン等の管理について、物理的な対策を講じること。
	フリーメール	インターネットを通じて無料で提供される電子メールサービスのこと。申し込めば無料で自分のメールアドレスを開設し、電子メールの送受信が行えるようになる。

は	ポート	ＩＰアドレスの下に設けられた番号のこと。ポートにより一つのＩＰアドレスでホームページを閲覧しながらメールの送受信を行うこと等、複数のサービスを同時に使用することが可能となる。
ま	ミラーリング	データの複製を別の場所にリアルタイムに保存すること。
	無線ＬＡＮ	無線を使って構築されるＬＡＮのこと。
	無停電電源装置	何らかの要因で電力供給が途絶し、機器が緊急停止した場合には、情報システムの機能が損なわれるおそれがあるため、機器が適正に停止するまでの間電力を供給するために設けた予備の電源のこと。
ら	ログインパスワード	インターネット、あるいはその他のネットワークへ接続（ログイン）するために入力する数字や文字列による符号。正当な利用者かどうかを確認するためにユーザーＩＤと組み合わせて使用するパスワードのこと。
英	ＩＤ(Identification)	何らかの対象を集団の中で一意に識別するための識別符号のこと。
	ＢＩＯＳ（Basic Input Output System）	パソコンに接続された周辺機器を制御するためのソフトウェアのこと。ＯＳやアプリケーションに対し、周辺機器へのデータの入出力の手段を提供している。

情報資産の種類と例

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内臓電磁記録媒体、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

情報セキュリティ会議組織体制