複 製 禁 止

須賀川市情報セキュリティポリシー

情報セキュリティ対策基準

第９版

【サーバ設置、保守業者等開示用】

新規制定　平成１５年３月３１日
改　　定　令和　５年４月　１日

須賀川市

目　次

一部非公開

非公開

非公開

非公開

変更履歴

版数	変更年月日	変更内容
1	平成 15 年 3 月 31 日	初版制定
2	平成 23 年 4 月 1 日	改定
3	平成 24 年 6 月 1 日	改定
4	平成 27 年 6 月 1 日	改定
5	平成 29 年 6 月 1 日	改定
6	平成 30 年 6 月 1 日	改定
7	令和 2 年 4 月 1 日	改定
8	令和 4 年 4 月 1 日	改定
9	令和 5 年 4 月 1 日	改定

１．目的

本情報セキュリティ対策基準（以下「対策基準」という。）は、「情報セキュリティ基本方針」に基づき、須賀川市（以下「市」という。）が所管する情報資産の情報セキュリティ確保に必要な事項を定める。

２．定義

（１） 情報

広義には、「ある特定の目的について適切な判断を行い、行動の意思決定をするために役立つもの」をいう。

対策基準では、「市民への行政サービスの提供、行政運営並びに職員の管理及び監督を目的として、職員が適切な判断を行い、行動の意思決定をするために役立つもの」をいう。

なお、情報については、存在する形態がデジタル又はアナログであるかを問わない。

（２） 情報セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。市においては、基本方針及び対策基準を総称したものをいう。

（３） 情報資産

市として、市民への行政サービスの提供、行政運営並びに職員の管理及び監督を目的として取り扱われる全ての情報及び情報を取り扱うための各種資産の総称をいう。

情報を取り扱うための資産は、データ資産、ソフトウェア資産、ハードウェア資産、人的資産、電子媒体及びサービスで構成される。

（４） 個人情報

個人情報保護法上では、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」をいう。

対策基準では、「市として、市民への行政サービスの提供、行政運営並びに職員の管理及び監督を目的として取り扱われる情報のうち、容易か否かに関わらず、特定の個人を識別することが可能な市で所管する全ての個人情報（複数の情報を組合せることにより、個人が特定できる個々の個人情報（個人に帰属する情報）も含む。）」をいう。

（５） 情報システム

ハードウェア資産、ソフトウェア資産及び電子媒体で構成され、市民への行政サービスの提供、行政運営並びに職員の管理及び監督を目的として処理を行うための仕組みをいう。なお、主な情報システムは以下のとおりである。

ア　住民基本台帳ネットワーク

地方公共団体と行政機関で個々の日本国民を特定する情報を共有・利用することを目的として構築されたシステムをいう（マイナンバー利用事務系システムを含む)。

イ　総合行政ネットワーク「LGWAN」

地方公共団体を相互に接続するための行政専用のシステム及びネットワークをいう。

ウ　基幹系システム

税務、国保・年金、介護・福祉等のサービスを市民へ提供するためのシステムをいう。

エ　情報系システム

行政運営、情報共有、情報公開、職員管理等のためのシステムをいう。

オ　個別システム

業務遂行のために各課（廨）で所管する情報システム及び国、県等から貸与されたシステムをいう。

（6） 庁内ネットワーク

市の各施設内及び施設間を接続するためのネットワークの総称をいう。なお、主な庁内ネットワークは以下のとおりである。

ア　基幹系ネットワーク

市が所管し、基幹系システムを構成するサーバ、パソコン及び周辺機器を接続するネットワークをいう。マイナンバー利用事務系のこと。

イ　情報系ネットワーク

市が所管し、情報系システムを構成するサーバ、パソコン及び周辺機器を接続するネットワークで、インターネット接続不可のネットワークをいう。LGWAN 接続系のこと。

ウ　インターネット系ネットワーク

市が所管し、情報系システムを構成するサーバ、パソコン及び周辺機器を接続するネットワークで、インターネット接続可能なネットワークをいう。インターネット接続系のこと。

エ　個別ネットワーク

各課（廨）が所管し、個別システムを構成するサーバ、パソコン及び周辺機器を接続するネットワークをいう。

（7） 外部ネットワーク

庁内ネットワーク以外のネットワークで、協議会など市以外の外部団体が所管するネットワークをいう。

（8） 基幹系サーバ

基幹系ネットワークに接続されるサーバで、住民基本台帳情報サーバ（マイナンバーサーバを含む)、税務サーバ、国保・年金サーバ及び介護・福祉サーバをいう。

（９） 情報系サーバ

情報系ネットワークに接続されるサーバで、内部情報系サーバ、グループウェアサーバ、ファイルサーバ等をいう。

（１０） 情報公開サーバ

情報公開のため情報系ネットワークに接続されるサーバで、公開 WEB サーバ及び DNS サーバをいう。

（１１） インターネット接続サーバ

職員のインターネット利用のため情報系ネットワークに接続されるサーバで、電子メールサーバ及び Proxy サーバをいう。

（１２） 基幹系パソコン

基幹系ネットワークに接続され、基幹系サーバ及びマイナンバーサーバを利用するためのパソコンをいう。

（１３） 情報系パソコン

情報系ネットワークに接続され、情報系サーバ、インターネット、電子メール等を利用するためのパソコンをいう。

（１４） テレワーク用パソコン

個別ネットワークに接続され、主にテレワークに利用するためのパソコンをいう。

（１５） モバイル端末

業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。例えば、タブレット端末等が該当する。

（１６） 職員

雇用の形態及び職位に関わらず、又は市の業務に日常的若しくは非日常的に従事するかに関わらず、市が所管する情報資産を取り扱う正規職員、会計年度任用職員をいう。

なお、市との業務委託契約に基づいて市の施設に常駐し、業務に携わる委託事業者も含まれる。

市に常駐する委託事業者としては、例えば、警備会社社員、情報システムオペレーター等が該当する。

（１７）　リスク分析

リスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク分析を行った後、リスク対応を行う。リスク対応の手段には、リスク源の除去、起こりやすさの変更、結果の変更、他社とのリスク共有、リスクの保有などがある。

（１８）　標的型攻撃

明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

（１９）　多要素認証

システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認証の信頼性を高める意味でも有効である。

（２０）　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サービス。なお、特定用途機器同士で通信を行うもの(テレビ会議等)は含まれない。

（２１）　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在り方で、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のことをいう。利用者の発信した情報や利用者間のつながりによって、コンテンツを作り出す要素を持った Web サイトやネットサービスなどを総称する用語で、電子掲示板（BBS）やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄等を含む。

（２２）　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、当該機能において本市の情報が取り扱われる場合に限る。

（２３）　外部サービス管理者

外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行うものをいう。

（２４）　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本市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。

３．適用範囲

対策基準の適用範囲を、組織的側面、人的側面、施設面及び情報システムの各側面から次のとおり定める。

（１） 組織

ア　適用する範囲

適用される組織は、市長部局、各行政委員会、上下水道部、議会事務局とする。

イ　除外する組織

（ア）須賀川市立の各小、中学校

（イ）一部事務組合（公立岩瀬病院、須賀川地方保健環境組合等）

補足：除外理由

・小中学校については、学校向けのポリシーに基づき対策を定めていることから、対策基準の対象外とする。

・一部事務組合等については、派遣先の条例及び規則等を順守するものとし、対策基準の対象外とする。

（２） 人

ア　適用する人

（ア）正規職員、会計年度任用職員の雇用形態並びに特別職及び一般職の区別は問わず、市が所管する情報資産を取り扱う全ての職員、市の施設に常駐して市が所管する情報資産を取り扱う委託事業者の社員等

（イ）市の施設において業務を行う協議会等各種団体の職員

（ウ）市が所管する情報資産を取り扱う委託事業者（第三セクタを含む）の社員等

（エ）市から委託を受けた業務を行う民生委員等

（オ）市主催イベント等に参画し、市が所管する情報資産を取り扱うボランティア、市民団体職員、町内会会員等

イ　除外する人

（ア）須賀川市立の各小中学校に勤務する教職員及び事務職員

（イ）市が他の組織（一部事務組合等）に派遣した職員

（３） 施設

ア　適用する施設

（ア）庁舎（地方自治法第４条に定める事務所及びその出先施設）

（イ）公の施設、市が所管する施設等

イ　除外する施設

（ア）須賀川市立の各小中学校施設

（４） 情報システム

ア　適用する情報システム

（ア）住民基本台帳ネットワーク

（イ）総合行政ネットワーク「LGWAN」

（ウ）基幹系システム

（エ）情報系システム

（オ）各課（廨）等において所管する個別システム

イ　除外する情報システム

（ア）教育委員会が所管する小中学校の教育用システム

（イ）協議会等各種団体が所管するシステム

４．組織体制

情報セキュリティ対策を推進するための組織体制を別表に示す。

（１） 最高情報統括責任者（CIO：Chief Information Officer、以下「CIO」という。）

ア　市長をCIOとする。

イ　CIOは、市で取り扱われる情報資産を保護するための統括責任をもつとともに、その責任を果たすための全ての権限を有する。

ウ　CIOは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報統括アドバイザー（CIO補佐官）として置き、その業務内容を定めるものとする。

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

ア　副市長及び教育長をCISOとする。

イ　CISOは、情報セキュリティ対策に関する連絡及び調整を担当し、CIOが情報セキュリティインシデント等により、その任務を遂行できない場合に代理する。

（３） 統括情報セキュリティ責任者

ア　企画政策部長をCISO直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISOを補佐しなければならない。

イ　統括情報セキュリティ責任者は、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及び責任を有する。

ウ　統括情報セキュリティ責任者は、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及び責任を有する。

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

オ　統括情報セキュリティ責任者は、市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害の恐れがある場合に、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及び責任を有する。

カ　統括情報セキュリティ責任者は、市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

キ　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理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。

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

ケ　統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてCISO にその内容を報告しなければならない。

（４） 情報セキュリティ責任者

ア　部局内の情報セキュリティ全般に関する責任者を置く。

イ　各部局の部長等を情報セキュリティ責任者とする。

ウ　情報セキュリティ責任者は、所管する部局において取り扱われる情報資産を保護するための責任をもつとともに、その責任を果たすための全ての権限を有する。

エ　情報セキュリティ責任者は、所管する部局等において次の役割を担う。

（ア）情報セキュリティ委員会での審議と承認事項に係ることの情報セキュリティ管理者への通知

（イ）情報セキュリティアクシデント及び情報セキュリティインシデント発生時の情報収集並びに対応

（５） 情報セキュリティ管理者

ア　各課（廨）内の情報セキュリティに関する適正な運用及び管理を行う管理者を置く。

イ　課（廨）等の長を情報セキュリティ管理者とする。

ウ　情報セキュリティ管理者は、所管する課（廨）において取り扱う情報資産を保護するにあたり、管理責任を果たすための権限を有する。

エ　情報セキュリティ管理者は、所管する課（廨）において、次の役割を担う。

（ア）情報セキュリティポリシー及び実施手順書の遂行

（イ）情報セキュリティ委員会での審議・承認事項に係る職員への示達

（ウ）情報セキュリティポリシー及び実施手順書の遂行に係る職員への周知・徹底及び注意喚起

（エ）情報セキュリティポリシー、実施手順書に基づく、課（廨）内の情報セキュリティ対策の整備、運用、管理等

（オ）情報セキュリティアクシデント及び情報セキュリティインシデント発生時の情報収集並びに対応

（６） 情報セキュリティ管理者の代理者

ア　情報セキュリティ管理者が指名した者（各課（廨）の課長補佐等）を情報セキュリティ管理者の代理者とする。

イ　情報セキュリティ管理者の代理者は、当該課(廨)の規模又は業務を考慮して複数名指名することができる。

ウ　情報セキュリティ管理者が勤務する施設と異なる施設がある場合は、情報セキュリティ管理者の代理者を当該施設毎に配置することができる。

エ　情報セキュリティ管理者の代理者は、情報セキュリティ管理者が不在のときに、情報セキュリティ管理者が担う役割を代理して遂行する。

（７） 情報システム責任者

ア　市が所管する情報システムに係る責任者として、情報システム責任者を置く。

イ　情報政策課長を情報システム責任者とする。

ウ　情報システム責任者は、市が所管する情報システム及び各課（廨）が所管する個別システムの企画、開発、調達、運用・管理並びに保守に係る統括責任をもつとともに、その責任を果たすための全ての権限を有する。

エ　情報システム責任者は、次の役割を担う。

（ア）情報セキュリティ委員会での審議及び承認事項に関する情報システム管理者への通知

（イ）情報セキュリティアクシデント及び情報セキュリティインシデント発生時の情報収集並びに対応

（８） 情報システム管理者

ア　市が所管する情報システム及び各課（廨）が所管する個別システムの管理に関して、情報システム管理者を置く。

イ　個別システムを所管する課（廨）の長を当該個別システムに関する情報システム管理者とする。

ウ　情報システム管理者は、市で所管する情報システム又は課（廨）で所管する情報システムに係る管理責任を果たすための権限を有する。

エ　情報システム管理者は、情報システム責任者の指示に従い、市で所管する情報システム又は課（廨）で所管する情報システムに係る次の役割を担う。

（ア）情報セキュリティポリシー及び実施手順書の遂行

（イ）情報システムの企画、開発、調達、管理及び保守

（ウ）情報システムに係る職員への教育、訓練、助言及び指示

（エ）システム障害、情報セキュリティアクシデント及び情報セキュリティインシデント発生時の情報収集並びに対応

（９） 情報システム管理者の代理者

ア　情報システム管理者が指名した者（各課（廨）の課長補佐等）を情報システム管理者の代理者とする。

イ　情報システム管理者の代理者は、情報システム管理者が不在のときに、情報セキュリティシステム管理者が担う役割を代理して遂行する。

（１０） 職員

職員は、情報セキュリティポリシー及び実施手順書を順守する責務を負う。

（１１） 情報セキュリティ委員会

ア　市民及び職員の個人情報並びに行政運営上必要な情報を様々な脅威から保護することを目

的として、情報セキュリティの維持、確保及び向上を統一的な視点で推進するための重要な事項を審議するため、情報セキュリティ委員会（以下「委員会」という。）を設置する。

イ　委員会の構成員は、次のとおりとする。

（ア）CIO

（イ）CISO

（ウ）統括情報セキュリティ責任者

（エ）情報セキュリティ責任者

（オ）情報システム責任者

ウ　CISOは、委員会において議長としての任に就く。

エ　委員会に事務局（以下「事務局」という。）を置くこととし、情報政策課がこれを担当する。

オ　事務局は、以下の業務を担う。

（ア）委員会の庶務（議事録の作成、保管、CIOの命を受けての事務処理等）

（イ）情報セキュリティポリシー及び実施手順書の遂行

（ウ）情報システムの調達及び運用管理の遂行

カ　CIOは、会議の審議上必要があると認めるときは、組織外部を含む委員以外の者へ出席を求め、意見等を聴くことができる。

キ　委員会は、CIOが定期的又は必要に応じて招集し、以下の事項について審議する。

（ア）情報セキュリティ推進体制組織の確立及び役割に関すること。

（イ）情報セキュリティに係るリスク分析の実施に関すること。

（ウ）リスク分析及び監査結果に基づく、更新計画書の策定又は見直しに関すること。

（エ）リスク分析に基づく情報セキュリティポリシーの策定又は見直し及び実施手順書の策定又は見直しに関すること。

（オ）職員に対する情報セキュリティ研修及び訓練に関すること。

（カ）施設内の各区域、付帯設備、情報システム及びネットワークを対象とした情報セキュリティの確保に係る物理的・技術的保護策に関すること。

（キ）委託事業者の管理に関すること。

（ク）情報セキュリティインシデント及び情報セキュリティアクシデントの対応に関する事項

（ケ）情報セキュリティに係る監査の実施に関すること。

（コ）情報セキュリティ監査結果に基づく是正措置、情報セキュリティポリシー及び実施手順書の見直しに関すること。

（サ）情報セキュリティに関わる違反への対処に関すること。

（シ）その他情報セキュリティの推進に必要な事項に関すること。

ク　対策基準に照らして判断できない内容については、委員会で審議のうえ、対応を決定する。

（１２）CSIRT（シーサート）の設置・役割

ア　CIO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、その役割を明確化すること。

イ　CSIRT の組織体制は、別表のとおりとし、統括情報セキュリティ責任者を CSIRT 責任者として置くこと。

なお、CSIRT 責任者は、CSIRT 内の業務統括、外部との連携等を行う職員を定めること。

ウ　CSIRT は、情報セキュリティインシデントについて、部局等から事務局へ報告があった場合に、その状況を確認し、情報セキュリティインシデントであるか評価を行うこと。

エ　CSIRT は、CIO 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、その内容を関係部局等に提供すること。

オ　CSIRT は、情報セキュリティインシデントを認知した場合に、必要に応じて、CIO、CISO、総務省、都道府県等へ報告すること。

カ　CSIRT は、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・公表対応を行うこと。

キ　CSIRT は、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。

５．情報の分類と管理

５．１．情報の分類

ア　情報の分類対象は、データ資産を対象とする。

イ　市が所管するデータ資産は、重要性、完全性及び可用性により表 1、表 2 及び表 3 に分類する。

ウ　情報セキュリティ管理者は、所管するデータ資産の重要性を考慮し、重要性分類を行うことが望ましい。

エ　情報セキュリティ管理者は、重要性分類したデータ資産及び情報システムを取り扱う際のアクセス権限を定めることが望ましい。

オ　情報セキュリティ管理者は、前ウ及びエの内容について、情報資産管理台帳等を作成して管理することが望ましい。

表１　データ資産の重要性分類

分類	定義
Ⅰ	市民、職員の個人情報を含むデータ資産とする。 例）戸籍関係（氏名、生年月日、性別、配偶者、戸籍事項、本籍等)、税関係（氏名、生年月日、性別、住所、世帯番号、電話番号、口座番号、口座名義、総所得額、給与収入額、年金所得額、課税額、納税額等)、個人番号（特定個人情報含む)
Ⅱ	市民及び職員の個人情報を含まない情報公開前のデータ資産、開示請求によって開示するデータ資産並びに非公開・非開示のデータ資産とする。 例）公示前入札情報、情報システム関連文書等
Ⅲ	Ⅰ及びⅡ以外の情報で、既に情報公開されている、又は市民が容易に取得することが可能なデータ資産とする。 例）公布済み条例及び規則、Web で公開している情報、市広報、お知らせ、各種申請書様式、各種パンフレット等

表２　データ資産の完全性分類

分類	定義
Ⅰ	行政事務で取り扱うデータ資産のうち、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的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがあるデータ資産とする。
Ⅱ	完全性Ⅰ以外のデータ資産とする。

表３　データ資産の可用性分類

分類	定義
Ⅰ	行政事務で取り扱うデータ資産のうち、滅失、紛失又は当該データ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。）を及ぼすおそれのあるデータ資産とする。
Ⅱ	可用性Ⅰ以外のデータ資産とする。

５．２．情報の管理

（１）管理責任

ア　情報の所管は市とする。

イ　情報セキュリティ管理者は、課（廨）で取り扱う情報に対する管理責任を有する。

ウ　情報を利用する職員は、（２）～（１４）に従い保護する責任を有する。

（２）データ資産の分類表示

ア　委員会は、第三者が重要性の識別を容易に認識できないよう留意しつつ、データ資産の分類が分かるように表示方法を定めることが望ましい。

イ　情報セキュリティ管理者は、定められたデータ資産の表示を行い、管理することが望ましい。

（３）データ資産の収集

ア　職員は、業務上必要のない情報を収集し又は施設内に持ち込まないこと。

イ　情報セキュリティ管理者は、所管する業務の遂行上必要な情報を収集する場合（見聞による収集した情報も含む)、利用目的を定めること。

ウ　情報セキュリティ管理者は、市民の個人情報を含む情報を収集する場合は須賀川市個人情報の保護に関する法律施行条例第６条で定めた手続きに従って行うこと。

エ　情報セキュリティ管理者は、前イ及びウにおいて収集した情報は、データ資産の重要性に応じて分類することが望ましい。

オ　職員は、データ資産により収集した情報を持ち込む際には記録を残すことが望ましい。

カ　職員は、電子情報を収集して施設内に持ち込む場合、当該電子情報がマルウェアに感染していないことを、セキュリティ対策ソフトウェアを使用して確認すること。

（４）データ資産の作成

ア　職員は、業務上必要のないデータ資産を作成してはならない。

イ　職員は、作成途上のデータ資産についても、紛失や流出等を防止すること。また、情報の作成途上で不要になった場合は、当該情報を消去すること。

ウ　情報セキュリティ管理者は、職員が作成するデータ資産の利用目的を定めること。

（５） 情報資産の利用

ア　職員は、業務以外の目的に情報資産を利用してはならない。

イ　職員は、情報資産の分類に応じ、適正に取り扱うこと。

ウ　職員は、電子媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電子媒体を取り扱うこと。

（６） 情報資産の保管

※非公開

（７） データ資産の閲覧・更新

ア　職員は、原則担当業務以外のデータ資産を閲覧・更新しないこと。

イ　職員は、担当業務以外のデータ資産を閲覧・更新する必要がある場合は、所管する課（廨）の情報セキュリティ管理者に申請し、許可を受けたうえで行うことが望ましい。

（８） データ資産の複製

ア　職員は、原則担当業務以外のデータ資産を複製しないこと。

イ　職員は、担当業務以外のデータ資産を複製する必要がある場合は、所管する課（廨）の情報セキュリティ管理者に申請し、許可を受けた上で行うことが望ましい。

ウ　前イにおいて複製の許可をした情報システム管理者は、所管する課（廨）において複製させたデータ資産の内容、日時、利用目的等の記録を残すことが望ましい。

エ　職員は、複製したデータ資産の正・副を明確にすることが望ましい。

オ　職員は、複製されたデータ資産についても、正の情報と同様の取扱い及び保管を行うことが望ましい。

（９） 電子情報の送信

電子メールの利用の詳細については、「電子メール利用実施手順書」に従い行動すること。

ア　職員は、電子メールに電子情報を添付送信する場合、職員の間で送受信する場合の容量は、10MByte 以下とすること。なお、国、県、委託事業者等市以外の組織間の場合は、相手先の電子メールシステムに依存するため、あらかじめ相手先に添付ファイルの容量を確認して、上限値以下で送信すること。

イ　職員は、国、県、委託事業者等市以外の組織に、電子メール等で電子情報（重要性分類Ⅰ又はⅡ）を送信する場合には、所管する課（廨）の情報セキュリティ管理者の許可を得ることが望ましい。

ウ　職員は、前イにおいて、電子情報を送信する場合は、送信日時、送信者及び送信情報、送信先に関する記録を残すことが望ましい。

エ　職員は、国、県、委託事業者等市以外の組織に、電子メール等で電子情報（重要性分類Ⅰ

又はⅡ）を送信する場合は、パスワード、暗号化等の技術的保護策を行うこと。なお、電子メール等の添付ファイルに付与したパスワードはメール本文中に記載せず、相手と事前にパスワードを取り決めておく又は、別メールまたは電話にて相手に伝えることが望ましい。

オ　職員は、電子メールで電子情報を添付して送信する場合、当該添付ファイルがマルウェアに感染していないことを確認してから送信すること。

（１０）データ資産の持ち出し

データ資産の持ち出しに関する詳細については、「データ資産持ち出し実施手順書」に従い行動すること。

ア　職員は、セキュリティエリア外にデータ資産（重要性分類Ⅰ又はⅡ）を持ち出す場合、所管する課（廨）の情報セキュリティ管理者に申請し、許可を得てから持ち出すこと。

イ　職員は、前アにおいて、データ資産を持ち出す際には、持ち出し月日、持ち出し者、持ち出す情報、持ち出し先並びに持ち出しに使用するパソコン、周辺機器及び電子媒体に関する記録を残すこと。

ウ　職員は、セキュリティエリア内、間及び外に関わらず、執務室から電子情報をパソコン、周辺機器及び電子媒体により持ち出す場合、パスワード、暗号化等の技術的保護策を行うこと。

エ　職員は、セキュリティエリア内、間及び外に関わらず、執務室から電子情報を持ち出す場合、当該電子情報がマルウェアに感染していないことを確認してから持ち出すこと。

オ　職員は、セキュリティエリア内、間及び外に関わらず、執務室からデータ資産を持ち出す場合、専用かばんに入れる等の物理的保護策を行うこと。

（１１）データ資産の運搬

情報の運搬の詳細については、「データ資産運搬実施手順書」に従い行動すること。

ア　職員は、データ資産の運搬中は、肌身離さず携行し、紛失、盗難等の防止に努めること。

イ　職員は、データ資産を運搬する際に使用する専用かばん及び専用ケースを盗難されないように、自動車（公用車及び自家用車）、自転車及び公共機関（飛行機、電車、バス、タクシー等）の交通手段に応じた保護策を行うこと。

ウ　情報セキュリティ管理者は、データ資産の運搬を委託事業者等に委託する場合、「１１．１．業務委託」に従って委託事業者と契約を締結し、順守させること。

（１２）電子情報の消去

ア　職員は、コンピュータ、周辺機器及び電子媒体に保存された電子情報（重要性分類Ⅰ又はⅡ）を、その利用が終了した時点で速やかに再利用できないように消去すること。

イ　職員は、電子情報（重要性分類Ⅰ又はⅡ）を消去する場合、情報セキュリティ管理者の許可を得ることが望ましい。

ウ　職員は、前イの消去処理についての実施日時、作業実施者、処理内容等の記録を残すことが望ましい。

（１３） 紙情報及びパソコン、電子媒体の再利用

ア　職員は、紙情報（重要性分類Ⅰ又はⅡ）を、裏紙として再利用しないこと。

イ　情報セキュリティ管理者は、所管するパソコン、周辺機器及び電子媒体の再利用を行う場合、当該パソコン、周辺機器及び電子媒体に含まれる電子情報（重要性分類Ⅰ又はⅡ）について、再利用できないように消去したうえで再利用すること。

ウ　情報セキュリティ管理者は、前イの再利用処理についての実施日時、作業実施者、処理内容等を記録することが望ましい。

（１４） 情報資産の廃棄

情報資産の廃棄の詳細については、「データ資産廃棄実施手順書」に従い行動すること。

ア　職員は、紙情報（重要性分類Ⅰ又はⅡ）はシュレッダーを使用して廃棄すること。

イ　職員は、フィルム情報（重要性分類Ⅰ又はⅡ）は焼却により廃棄すること。

ウ　職員は、課（廨）で利用していたパソコン、周辺機器及び電子媒体が不要となった時点で情報セキュリティ管理者の許可を得た上で速やかに情報政策課に提出すること。

エ　職員は、前ウで提出したパソコン、周辺機器及び電子媒体に関する記録を残すこと。

オ　情報政策課は、各課（廨）の職員から受領したパソコン、周辺機器及び電子媒体の一時保管場所を定め、廃棄するまでの間保管すること。

カ　情報政策課は、各課（廨）の職員から受領したパソコン、周辺機器及び電子媒体に内蔵されているハードディスク及びメモリ内の電子情報が再利用できないように完全消去した上で定期的に廃棄（リース、レンタル等の場合は返却）すること。

キ　情報政策課は、各課（廨）の職員から受領した電子媒体は、メディアシュレッダー、はさみ等を使用して、再利用できないように物理的に破壊した上で定期的に廃棄すること。

ク　情報政策課は、前カ及びキの廃棄処理についての実施日、作業者及び処理内容を記録すること。

ケ　情報政策課は、前カ、キ及びクを委託事業者に委託する場合、「１１．１.業務委託」に従って委託事業者と契約を締結し順守させること。なお、廃棄の際は、作業に立ち会うものとし、電子情報が完全に消去され、確実に廃棄されたことを証明する「証明書」の発行を受けること。

６．庁内ネットワークの強靭性の向上

６．１．基幹系ネットワーク（マイナンバー利用事務系）

（１） 基幹系ネットワークと他の領域との分離

基幹系ネットワークと他の領域を通信できないようにすること。基幹系ネットワーク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うこと。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、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りでなく、から LGWAN-ASP を経由して、インターネット等と基幹系ネットワークとの双方向通信でのデータの移送を可能とする。

（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）を利用すること。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、電子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すること。

６．２．情報系ネットワーク（LGWAN 接続系）

情報系ネットワークとインターネット系ネットワークの分割

情報系ネットワークとインターネット系ネットワーク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すること。なお、メールやデータを情報系ネットワークに取り込む場合は、次の実現方法等により、無害化通信を図ること。

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情報系ネットワークに転送するメールテキスト化方式

イ　インターネット系ネットワークの端末から情報系ネットワークの端末へ画面を転送する方式

ウ　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、インターネット系ネットワークから取り込む方式

６．３．インターネット系ネットワーク（インターネット接続系）

ア　インターネット系ネットワークにおいては、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、情報系ネットワーク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ること。

イ　市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すること。

７．物理セキュリティ

７．１．施設の管理

（１） セキュリティゾーン

市の施設内のセキュリティエリア区域において、職員であって入室権限のある者のみが立ち入り可能な場所をいう。例えば、以下の場所がセキュリティゾーンに該当する。

サーバ室

（２） セキュリティエリア

市の施設内の区域をいい、職員以外の者（市民、家族、訪問者、市に常駐する者を除いた委託事業者等）の立ち入りを制限している場所をいう。

例えば、以下の場所がセキュリティエリアに該当する。

ア　執務室（会議室及び相談室を含む。）
イ　書庫
ウ　倉庫
エ　中央監視室
オ　更衣室等

（３） オープンエリア

市の施設内の区域で、職員以外の者（市民、家族、訪問者、委託事業者等）の立ち入りを制限していない場所をいう。例えば、以下の場所がオープンエリアに該当する。

ア　待合室（ホール）
イ　議場
ウ　廊下及び階段
エ　売店及び食堂
オ　トイレ等

（４） セキュリティエリア外

市の施設内以外の場所をいう。例えば、以下の区域がセキュリティエリア外に該当する。

ア　個人の住宅
イ　民間企業団体の施設
ウ　国、県等の施設
エ　協議会、外郭団体等の施設
オ　委託事業者の施設
カ　職員の自宅
キ　上記ア～カの各施設に移動する際に通る場所（道路、駐車場、駅等）

【セキュリティエリア設定の図解】

セキュリティゾーン	セキュリティエリア	オープンエリア	セキュリティエリア外
・サーバ室	・執務室 （会議室、相談室含む） ・書庫 ・倉庫　等	・待合室（ホール） ・議場 ・廊下及び階段 ・売店　等	・個人の住宅 ・民間企業団体の施設 ・国、県等の施設　等

７．２．サーバ等の管理

（１） 機器の取付け

ア　サーバは、サーバ室内に設置すること。

イ　サーバをサーバ室以外に設置する場合は、職員が監視可能な範囲に設置することが望ましい。

ウ　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、必要な措置を講じること。

（２） 機器の電源

ア　コンピュータ、通信機器及び設備の安定稼働に必要な電力量を把握し、規定容量を超えないように管理することが望ましい。

イ　サーバには、停電又は電源異常時等においても継続稼動又は安全に停止できるための無停電電源装置を設置し、定期的に点検及びバッテリ交換を行うこと。

ウ　電源ケーブルは、損傷から保護するために、床下配線、保護カバーの取付け、余長ケーブルを収納する等の対策をすることが望ましい。

エ　電源プラグがコンセントから抜けるのを防止するため、定期的に差し込み状況を点検することが望ましい。

オ　電源ケーブルには電源系統が分かるように、タグ等を貼付して管理することが望ましい。

（３） 通信ケーブル等の配線

ア　通信ケーブルは、損傷から保護するために、床下配線、保護カバーの取付け、余長ケーブルの収納等の対策をすることが望ましい。

イ　通信で使用するケーブル配線は、相互干渉による障害を防止するために、電源ケーブルから隔離することが望ましい。

ウ　通信ケーブルは、接続先機器等が分かるようにタグ等を貼付して管理することが望ましい。

エ　通信ケーブルは、誤接続の防止及び保守性を向上させるため、色分けすることが望ましい。

オ　予備ネットワーク配線等の常時使用しないケーブルは、人目につかないように敷設し、未使用の HUB ポートは容易に使用できないよう蓋をするなどの保護策を講じることが望ましい。

カ　ネットワーク配線の追加および変更は、情報システム責任者の許可を得なければならない。

（４） 機器の定期保守及び修理

ア　情報システム管理者は、ハードウェア資産、ソフトウェア資産等の保守契約を締結すること。保守契約は、「１１．１．業務委託」に従って締結し、委託事業者に順守させること。

イ　情報システム管理者は、電子媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせること。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行うこと。

ウ　情報システム管理者は、修理等の目的で委託事業者等が重要な情報（重要性分類Ⅰ又はⅡ）が保存されたコンピュータを施設外に持ち出す場合は、保存されている情報の漏えいを防止するために、電子情報の完全消去、電子媒体の取外し等の対策を行うこと。

エ　情報システム管理者は、障害対応を委託事業者に行わせる場合は、その作業に立ち会い、管理すること。

オ　情報システム管理者は、委託事業者による修理等の作業内容に関する報告を受け、その記録を残すこと。

（５） 庁外への機器の設置

ア　情報セキュリティ責任者及び情報システム責任者は、庁外にサーバ等の機器を設置する場合、CIO の承認を得ること。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すること。

イ　委託等により市が所管するコンピュータ及び通信機器をセキュリティエリア外の施設等に設置する場合は、当該委託事業者との委託契約に基づいて市と同等の対策及び運用・管理を行わせることが望ましい。

７．３．セキュリティゾーン（サーバ室等）の管理

（１） セキュリティゾーンの構造等

ア　サーバ室は、外部からの侵入が容易にできないように壁、間仕切り等で囲まれた構造とすること。

イ　サーバ室は、第三者に所在が分かる表示をしないこと。

ウ　サーバ室は、常時利用する出入口を１か所とし、許可された職員及び委託事業者のみがアクセスできるように、入退室管理システムによる管理を行うこと。

エ　サーバ室には、一定の温湿度を維持できるように空調設備を設け、定期的に点検すること。

オ　サーバ室内での作業を監視するための監視カメラを設置すること。

カ　サーバ室は、常に整理整頓を行い、非常時の避難経路を確保すること。

キ　情報セキュリティ管理者及び情報システム管理者は、サーバ室に配置する消火薬剤や消防用設備等が、機器及び電子媒体等に影響を与えないようにすること。

（２） セキュリティゾーンの入退室管理等

ア　情報システム管理者は、サーバ室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記録（ログ等）による入退室管理を行うこと。

イ　前アにおいて、入退室を許可された者は、入退室管理簿に入室日時および退室日時等の記録を取ること。

ウ　職員及び委託事業者は、サーバ室に入室する場合、身分証明書等を携帯し、求めにより提示すること。

エ　情報システム管理者は、外部からの訪問者がサーバ室に入る場合には、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が付き添うものとし、外見上職員と区別できる措置を講じること。

オ　情報システム管理者は、サーバ室に設置している当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電子媒体等を持ち込ませないようにすること。

（３） 機器等の搬入出

委託事業者等が、サーバ室にコンピュータ、通信機器の搬入・搬出作業等で立ち入る場合は、情報システム責任者、情報システム管理者又は情報システム管理者が指名する者が立ち会うこと。

（４） 通信回線及び通信回線装置の管理

ア　情報システム管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理すること。また、通信回線及び通信回線装置に関連する文書を適正に保管すること。

イ　情報システム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らすこと。

ウ　情報システム管理者は、行政系のネットワークを情報系ネットワークに集約するように努めること。

エ　情報システム管理者は、重要性分類Ⅰ又はⅡ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、適正な回線を選択すること。また、必要に応じ、送受信される情報の暗号化を行うこと。

オ　情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施すること。

カ　情報システム管理者は、可用性分類Ⅰ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すること。また、必要に応じ、回線を冗長構成にする等の措置を講じること。

７．４．セキュリティエリアの管理

※非公開

７．５．職員の利用するパソコンや電子媒体等の管理

※非公開

８．人的セキュリティ

８．１．職員の順守事項等

（１） 職員の順守事項

ア　情報セキュリティポリシー等の順守

職員は、情報セキュリティポリシー及び実施手順書を順守すること。また、情報セキュリティ対策について不明な点、順守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰ぐこと。

イ　業務以外の目的での使用の禁止

職員は、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。

ウ　支給以外のパソコン、モバイル端末及び電子媒体等の業務利用

（ア）職員は、支給以外のパソコン、モバイル端末及び電子媒体等を原則業務に利用してはならない。

（イ）個人が所有する携帯電話、スマートフォン、電子手帳等の機器及び紙媒体の手帳、ノート等については施設内への持ち込みを認めることとする。ただし、業務時間内において私的目的の利用は禁止する。

（ウ）職員は、前（イ）で持ち込んだ機器（以下、「個人持ち込み機器」という。）のうち、携帯電話、スマートフォン、電子手帳等の機器を業務目的で利用する場合は、あらかじめ情報セキュリティ管理者の許可を得ること。

（エ）情報セキュリティ管理者は、業務利用を許可した個人持ち込み機器に関して、使用者、使用期間、使用業務等に関する記録を残すこと。

エ　持ち出し及び持ち込みの記録

情報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、保管すること。

オ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員は、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の許可なく変更してはならない。

カ　机上の端末等の管理

（ア）職員は、パソコン、モバイル端末、電子媒体及び情報が印刷された文書等について、常に整理整頓に努めること。

（イ）職員は、プリンタ、コピー機、ファクシミリ装置等から出力された紙情報を長時間放置しないこと。

（ウ）職員は、長時間離席する場合、パソコン及びモバイル端末のロックや、電子媒体、文書等を容易に閲覧されない場所へ保管する等、適正な措置を講じること。

キ　退職時等の順守事項

職員は、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すること。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） 会計年度任用職員への対応

ア　情報セキュリティポリシー等の順守

情報セキュリティ管理者は、会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員が守るべき内容を理解させ、また実施及び順守させること。

イ　情報セキュリティポリシー等の順守に対する同意

情報セキュリティ管理者は、会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を順守する旨の同意書への署名を求めること。

ウ　インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにすること。

（３） 情報セキュリティポリシー等の掲示

ア　事務局は、職員が常に情報セキュリティポリシー及び実施手順書を閲覧できるようグループウェアに掲示すること。

イ　職員は、グループウェアに掲載された情報セキュリティポリシー及び実施手順書を閲覧すること。

ウ　事務局は、見直しにより情報セキュリティポリシー及び実施手順書を改版した場合、グループウェアに最新版を掲載し、全ての情報セキュリティ管理者に対して情報セキュリティポリシー及び実施手順書の改版を周知すること。

エ　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適用範囲以外の組織及び人へ対策基準を漏えいしてはならない。なお、漏えいが発生した場合は、委員会に報告すること。

（４） 委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守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順守及びその機密事項を説明すること。

８．２．研修・訓練

（１） 研修計画の策定及び実施

ア　事務局は、情報セキュリティに関わる研修計画を策定すること。

（ア）開催する研修の対象職員を明確にすること。

（イ）研修対象職員の情報セキュリティ上の役割毎に、達成すべき目標レベルを設定すること。

（ウ）対象職員が十分に参加できるように毎年定期的に開催するものとし、開催回数及び日程を考慮して計画すること。

（エ）研修で使用する資料等は、事前に委員会の承認を得ること。

（オ）研修結果を評価するための方法（確認テスト、アンケート等）を事前に定めて準備すること。

イ　委員会は、策定した情報セキュリティに関わる研修計画を承認すること。

ウ　事務局は、作成した研修計画に基づき教育を実施すること。

エ　事務局は、情報セキュリティポリシーに関する研修の実施結果について、必要に応じて確認テストにより評価を行い、委員会に報告すること。

オ　委員会は、前エの評価結果を確認のうえ承認し、設定した目標レベルに達していない職員に対して、事務局にフォローアップを指示することが望ましい。

カ　事務局は、評価の結果及び目標レベルに達していない職員に対して、個別に指導する等のフォローアップを行うこと。

（２）　緊急時対応訓練

ア　事務局は、情報セキュリティアクシデント及び情報セキュリティインシデントの発生を想定した訓練計画を策定することが望ましい。

（ア）訓練の目的と達成目標を定めること。

（イ）市として想定される情報セキュリティアクシデント及び情報セキュリティインシデントの被害シナリオを明確にすること。

（ウ）想定した被害シナリオに基づいて、関係する課（廨）及び関連する委託事業者と連携して訓練計画を策定し、訓練に必要な訓練手順の策定及び必要な情報資産の準備を行うこと。

（エ）訓練結果を評価するための方法（チェックシート等）を事前に定めて準備すること。

イ　委員会は、策定した訓練計画を承認すること。

ウ　事務局は、訓練計画に基づき、訓練を実施すること。

エ　職員及び関連委託事業者は、訓練に協力すること。

オ　事務局は、訓練結果について、チェックシート等により評価を行い、委員会に報告すること。

カ　委員会は、評価結果を確認のうえ承認し、目標に達していない場合は、事務局に原因の究明及び改善を指示すること。

（３）　研修・訓練への参加

ア　職員は、定められた情報セキュリティに関する研修に参加して、情報セキュリティポリシーを理解し、情報セキュリティ上の問題が生じないように努めること。

イ　職員は、定められた情報セキュリティに関する訓練に参加して、情報セキュリティインシデント及び情報セキュリティアクシデントが発生した場合の対応に問題が生じないように努めること。

８．３．情報セキュリティインシデントの報告等

（１） 情報セキュリティインシデントの報告

情報セキュリティインシデントの報告の詳細については、「情報セキュリティインシデント対応実施手順書」に従い行動すること。

ア　職員は、情報の取扱い、情報システムの利用等において、情報セキュリティポリシーに違反する行為を確認した場合は、当該職員に対して注意すること。

イ　職員は、前アで注意をしたにも関わらず、改善がみられない場合は、自身が所属する係長に報告すること。

ウ　報告を受けた係長は、情報セキュリティインシデントの内容を確認後、自身が所属する情報セキュリティ管理者に報告すること。

エ　情報セキュリティ管理者は、情報システム管理者と連携して状況を把握し、情報セキュリティインシデントのレベルを判定すること。

オ　情報セキュリティ管理者は、情報セキュリティインシデントレベルが「C」以外と判定した場合は、情報セキュリティインシデント報告書にて CSIRT に遅滞なく報告すること。

カ　CSIRT は、報告を受けた情報セキュリティインシデントを統括情報セキュリティ責任者と協議し、必要に応じて CIO 及び CISO に報告すること。

（２） 情報セキュリティインシデント原因の究明・記録、再発防止等

ア　情報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が、情報セキュリティインシデントレベルを「C」と判定した場合は、当該職員に対して注意を行うことにより対応すること。

イ　情報セキュリティ管理者は、前アにおいて対応した際の記録を残しておくこと。

ウ　CSIRT は、情報セキュリティ管理者から受けた情報セキュリティインシデント報告について、統括情報セキュリティ責任者と所管する部門の情報セキュリティ委員で協議し、必要な対応を行うこと。なお、必要に応じて CIO 及び CISO への対応をすること。

エ　事務局は、前ウにおいて対応した際の記録を残すこと。

８．４．ID 及びパスワード等の管理

（１） 職員証及び IC カード等の取扱い

ア　職員は、自己の管理する職員証及び IC カードに関し、次の事項を順守すること。

（ア）認証に用いる職員証及び IC カードを、職員間で共有しないこと。

（イ）職員は、施設内では常に職員証を着用すること。

（ウ）職員は、職員証を着用していない職員を施設内で見かけた場合は、注意を促すこと。注意をしても従わない場合は、「８．３．情報セキュリティインシデントの報告等」に従って、当該職員の所属する課（廨）の情報セキュリティ管理者に報告すること。

（エ）業務上必要のないときは、IC カード等をカードリーダ又はパソコン等の端末のスロット等から抜くこと。

（オ）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者に報告し、指示に従うこと。

イ　統括情報セキュリティ責任者及び情報システム管理者は、職員証及び IC カード等の紛失等の通報があり次第、当該職員証及び IC カード等を使用したアクセス等を速やかに停止すること。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、職員証及び 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すること。

（２） ID の取扱い

職員は、自己の管理する ID に関し、次の事項を順守すること。

ア　自己が利用している ID は、他人に利用させないこと。

イ　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ないこと。

（３） パスワードの取扱い

職員は、自己の管理するパスワードに関し、次の事項を順守すること。ただし、情報システムの実装上、当該パソコン、アプリケーションソフトウェアのパスワードを職員自ら変更できない場合は、この限りでない。

ア　パスワードは、他者に知られないように管理すること。

イ　パスワードは、メモの貼付などにより、他人に認知させ、若しくは認知されるおそれがある行為をしないこと。

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　パスワードは、情報システムで設定されている最低桁数以上の桁数で設定すること。

オ　パスワードの文字列は使用者の氏名、誕生日、ユーザ ID、職員コード、内線番号等の容易に推測可能なものは避け、想像しにくいものにすること。また、文字列は英大文字、英小文字、数字及び記号を組み合わせることが望ましい。

カ　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更すること。

キ　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いないこと。

ク　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すること。

ケ　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させないこと。

コ　職員間でパスワードを共有しないこと（ただし、共有 ID に対するパスワードは除く）。

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

※非公開

９．２．アクセス制限

※非公開

９．３．システム開発、導入、保守等

※非公開

９．４．不正プログラム対策

（１） 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置すること。

ア　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてマルウェア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すること。

イ　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてマルウェア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すること。

ウ　マルウェア等の不正プログラム情報を収集し、必要に応じ職員に対して注意喚起すること。

エ　所掌するサーバ及びパソコン等の端末に、マルウェア等の不正プログラム対策ソフトウェアを常駐させること。

オ　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。なお、βモデル又はβ´モデルを採用する場合は、不正プログラム対策ソフトウェアは、未知の不正プログラムに対する対応も可能となる対策を講じること。

カ　不正プログラム対策のソフトウェアは、常に最新の状態に保つこと。

キ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないこと。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すること。

（２） 情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置すること。

ア　情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、マルウェア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ること。ただし、インターネットに接続していないシステム等、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は、この限りでない。

イ　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つこと。な

お、βモデル又はβ´モデルを採用する場合は、不正プログラム対策ソフトウェアは、未知の不正プログラムに対する対応も可能となる対策を講じること。

ウ　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つこと。

エ　マルウェア等の感染を防止するため、インターネットに接続していないシステムで電子媒体を使う場合は、市が管理していない媒体を職員に利用させないこと。

オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員に当該権限を付与しないこと。

（3） 職員等の順守事項

職員は、不正プログラム対策に関し、次の事項を順守すること。

ア　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。

イ　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うこと。

ウ　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、速やかに削除すること。

エ　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することが望ましい。

オ　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情報系システムに取り込む場合は無害化すること。

カ　統括情報セキュリティ責任者が提供するマルウェア情報を、常に確認すること。

キ　マルウェア等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたマルウェア感染時の初動対応の手順に従って対応を行うこと。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施すること。

（4） 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにすること。

９．５．不正アクセス対策

（1） 統括情報セキュリティ責任者の措置事項

情報システムは、不正アクセス対策として、以下の事項を措置すること。

ア　使用されていないポートを閉鎖すること。

イ　不要なサービスについて、機能を削除又は停止すること。

ウ　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、

統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定すること。

エ　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すること。

（2） 攻撃への対処

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じること。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ること。

（3） 記録の保存

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めること。

（4） 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員及び外部委託事業者が使用しているパソコン等の端末からの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こと。

（5） 職員による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員による不正アクセスを発見した場合は、当該職員が所属する課（廨）の情報セキュリティ管理者に通知し、適正な処置を求めること。

（6） サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じること。

（7） 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じること。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）を講じること。

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・共有及びソフトウェアの更新等

情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有すること。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すること。

（2） 不正プログラム等のセキュリティ情報の収集・周知

情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員に周知すること。

（3） 情報セキュリティに関する情報の収集及び共有

ア　情報システム責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有すること。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ること。

イ　事務局は、平常時より国内外で発生している情報セキュリティアクシデント等の収集に努めることが望ましい。

ウ　情報セキュリティ管理者は、平常時より所管する課（廨）の情報セキュリティインシデントに関する情報収集に努めること。

１０．運用

１０．１．情報システムの監視

（１） サーバへのアクセス記録の取得・分析

ア　情報システム管理者は、サーバへのアクセス記録を取得すること。

イ　情報システム管理者は、上記アクセス記録を一定期間保存すること。

ウ　情報システム管理者は、情報システムのアクセス記録を定期的に確認し、不正なアクセスの有無を確認することが望ましい。

（２） パソコンの操作記録の取得・分析

ア　情報システム管理者は、パソコンの操作記録を取得すること。

イ　情報システム管理者は、パソコンの操作記録を一定期間保存すること。

ウ　情報システム管理者は、パソコンの操作記録を定期的に確認し、不正な操作の有無を確認することが望ましい。

（３） インターネット利用及び電子メール利用状況記録の取得・分析

ア　情報システム管理者は、インターネット利用及び電子メール利用状況記録を取得すること。

イ　情報システム管理者は、インターネット利用及び電子メール利用状況記録を一定期間保存すること。

ウ　情報システム管理者は、インターネット利用及び電子メール利用状況記録を定期的に確認し、不正な操作の有無を確認すること。

（４） 記録のアクセス制限及び改ざん防止

ア　情報システム管理者は、限られた者だけが個人所有のパソコン及び周辺機器の利用状況記録、アクセス記録、パソコンの操作記録並びにインターネット利用及び電子メール利用状況記録にアクセスできるように、制限を行うこと。

イ　情報システム管理者は、個人所有のパソコン及び周辺機器の利用状況記録、アクセス記録、パソコンの操作記録並びにインターネット利用及び電子メール利用状況記録の正確さを保障するため、記録の改ざん防止策を講じること。

（５） 時刻同期

情報システム管理者は、サーバへのアクセス記録及びパソコンの操作記録の正確さを保障するため、コンピュータ及び通信機器の時刻を正確に設定すること。

１０．２．ネットワークの監視

（１） 通信機器へのアクセス記録の取得・分析

ア　情報システム管理者は、通信機器へのアクセス記録を取得すること。

イ　情報システム管理者は、通信機器へのアクセス記録を一定期間保存すること。

ウ　情報システム管理者は、通信機器へのアクセス記録を定期的に確認し、不正なアクセスの有無を確認することが望ましい。

（２） 外部ネットワークからの不正アクセス記録の取得・分析

ア　情報システム管理者は、ファイアウォール、セキュリティ対策システム、不正侵入を防止する装置等の記録を取得すること。

イ　情報システム管理者は、ファイアウォール、セキュリティ対策システム、不正侵入を防止する装置等の記録を一定期間保存すること。

ウ　情報システム管理者は、ファイアウォール、セキュリティ対策システム、不正侵入を防止する装置等の記録を定期的に確認し、不正なアクセスの有無を確認することが望ましい。

１０．３．情報セキュリティポリシーの順守状況の確認

（１） 順守状況の確認及び対処

ア　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの順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CIOに報告すること。

イ　CIOは、発生した問題について、適正かつ速やかに対処すること。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク、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順守状況について、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すること。

（２） パソコン、モバイル端末及び電子媒体等の利用状況調査

CISO及び統括情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン、モバイル端末、電子媒体等のログ、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） 職員の報告義務

ア　職員は、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に報告を行うこと。

イ　当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性がある統括情報セキュリティ責任者が判断した場合において、職員は、緊急時対応計画に従って適正に対処すること。

１０．４．侵害時の対応等

（１）　緊急時対応計画の策定

CIO又は委員会は、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恐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すること。

（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、以下の内容を定めること。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　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、委員会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すること。

（４）　緊急時対応計画の見直し

CIO 又は委員会は、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すこと。

１０．５．例外措置

（１）　例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を順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、順守事項とは異なる方法を採用する又は順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、CIO の許可を得て、例外措置を講じることができる。

（２）　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、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 CIO に報告すること。

（３）　例外措置の申請書の管理

CIO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認すること。

１０．６．法令順守

（１）　法令等の順守の周知・徹底

ア　情報セキュリティ管理者は、職員に対して、情報セキュリティ上順守すべき法令についての周知・徹底すること。

イ　職員は、情報資産を取り扱う場合において、次に掲げる法令、市の例規等を順守すること。

（２）　情報セキュリティに関連する法律等

ア　地方公務員法

（ア）信用失墜行為の禁止（第 33 条）

（イ）秘密を守る義務（第 34 条）

（ウ）職務に専念する義務（第 35 条）等

イ　刑法

（ア）電磁的記録不正作出及び供用（第 161 条の 2）

（イ）電子計算機損壊等業務妨害（第 234 条の 2）

（ウ）電子計算機使用詐欺（第 246 条の 2）　等

ウ　個人情報の保護に関する法律（個人情報保護法）

エ　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（マイナンバー法）

オ　不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

カ　著作権法

キ　サイバーセキュリティ基本法

（３）　情報セキュリティに関連する例規

ア　須賀川市個人情報の保護に関する法律施行条例

イ　須賀川市個人情報の保護に関する法律施行条例施行規則

ウ　須賀川市議会の個人情報の保護に関する条例

エ　須賀川市議会の個人情報の保護に関する条例施行規程

オ　須賀川市選挙管理委員会の所管に係る須賀川市個人情報保護条例施行規程

カ　須賀川市監査委員の所管に係る須賀川市個人情報保護条例施行規程

キ　須賀川市固定資産評価審査委員会の所管に係る須賀川市個人情報保護条例施行規程

ク　須賀川市農業委員会の所管に係る須賀川市個人情報保護条例施行規則

ケ　須賀川市教育委員会の所管に係る須賀川市個人情報保護条例施行規則

コ　須賀川市情報公開条例

サ　須賀川市情報公開条例施行規則

シ　須賀川市議会の所管に係る須賀川市情報公開条例施行規則

ス　須賀川市選挙管理委員会の所管に係る須賀川市情報公開条例施行規程

セ　須賀川市監査委員の所管に係る須賀川市情報公開条例施行規程

ソ　須賀川市固定資産評価審査委員会の所管に係る須賀川市情報公開条例施行規程

タ　須賀川市農業委員会の所管に係る須賀川市情報公開条例施行規則

チ　須賀川市教育委員会の所管に係る須賀川市情報公開条例施行規則

ツ　須賀川市住民基本台帳カードの利用に関する条例

テ　須賀川市住民基本台帳カードの利用に関する条例施行規則

ト　須賀川市住民基本台帳ネットワークシステムセキュリティ規則
ナ　須賀川市職員の懲戒処分等に関する規程

（4）　その他
契約上の義務（委託事業者との契約等）

１０．７．懲戒処分等

（1）　情報セキュリティインシデントの原因に対する警告
ア　事務局は、情報セキュリティに関するインシデントの原因となる職員に対して、その職員が所属する課（廨）の情報セキュリティ管理者を通じて警告を行うことができるものとする。
イ　事務局は、前アの警告にも関わらず、改善が認められない場合は、当該職員に対して情報システム利用の一時停止等の措置を講じることができるものとする。
ウ　前ア及びイの対処については、人事考課及び懲戒処分には関係しない範囲で行われるものとする。

（2）　罰則の適用
ア　委員会は、職員が情報セキュリティポリシー、実施手順書及び関連する各種法令「１０．６.法令順守」に違反して、情報漏えい等の情報セキュリティアクシデント又は重大な情報セキュリティインシデントを発生させた場合、当該職員及び当該職員に対する監督責任を明らかにし、対処について審議するものとする。
イ　審議の結果、市は、須賀川市職員の懲戒処分等に関する規程に従って、懲戒処分を講ずることができるものとする。

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

ア　情報システム管理者又は情報セキュリティ管理者は、委託事業者の選定に際して、以下に示す事項について委託条件を満たすか事前に確認すること。

（ア）提供を受ける業務内容及びそのサービスレベル

（イ）当該委託事業者の情報セキュリティポリシー策定状況及び情報セキュリティ対策の実施状況

（ウ）委託事業者が市のセキュリティポリシーを順守可能か否かの確認

（エ）契約時に合意する「（２）契約項目」を順守可能か否かの確認

（オ）当該委託事業者の財務状況

イ　情報システム管理者又は情報セキュリティ管理者は、前アの委託条件を全て満たす委託事業者の中から、契約する委託事業者を選定すること。

ウ　情報セキュリティ責任者は、情報システム管理者が選定した委託事業者の承認をすること。

（２）　契約項目

情報セキュリティ管理者は、重要性分類Ⅰ又はⅡの情報を取り扱う場合、以下に示す委託事業者が順守すべき事項を必要に応じ委託契約書に明記し、様式　業務委託に関するセキュリティ要件チェックシートにより委託事業者との合意を得ること。

ア　須賀川市情報セキュリティポリシー及び実施手順書の順守に関する事項

イ　市が開示する情報の目的外使用、秘密保持及び第三者への提供の禁止に関する事項

ウ　市が開示する情報の複製の制限、保管、返却及び廃棄に関する事項

エ　著作権等の権利に関する事項

オ　再委託及び再々委託の禁止又は制限に関する事項

カ　身分証明の着用、持ち込み機器（パソコン）等作業条件に関する事項

キ　委託契約履行中における定期報告に関する事項

ク　情報セキュリティインシデント、及びそれらの報告に関する事項

ケ　市による情報セキュリティ監査の実施に関する事項

コ　委託事業者の責任者、委託内容、作業者の所属、作業場所の特定に関する事項

サ　提供されるサービスレベルの保証（SLA）に関する事項

シ　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理の実施に関する事項

ス　委託事業者の従業員に対する教育の実施に関する事項

セ　市による情報セキュリティインシデント発生時の公表に関する事項

ソ　須賀川市情報セキュリティポリシー及び実施手順書が順守されなかった場合の損害賠償等に関する事項

（３）　確認・措置等

ア　情報セキュリティ管理者は、委託事業者に対し、情報セキュリティの管理体制、実施内容等に関する実施計画書を提出させること。

イ　情報セキュリティ管理者は、委託事業者に開示又は提供する情報資産を必要最小限に止めること。

ウ　情報セキュリティ管理者は、委託業務に従事する全ての者に対し守秘義務を負わせ、情報セキュリティを順守することの誓約を取り交わすこと。

エ　情報セキュリティ管理者は、委託事業者に対して、契約上取り決めた外部委託事業者が順守すべき事項を上回る過剰な要求を行わないこと。

オ　情報セキュリティ管理者は、委託事業者に対し、委託業務の実施状況について定期的に報告させることが望ましい。

カ　情報セキュリティ管理者は、委託事業者に対し、情報セキュリティインシデント又は情報セキュリティアクシデントが発生した場合に、速やかに報告させること。

キ　情報セキュリティ管理者は、必要に応じて委託契約履行期間内に情報セキュリティ監査（事業所への実地監査を含む。）を年１回以上 実施することが望ましい。

１１．２．外部サービスの利用（重要性分類Ⅰ又はⅡの情報を取り扱う場合）

※非公開

１１．３．外部サービスの利用（重要性分類Ⅰ又はⅡの情報を取り扱わない場合）

※非公開

１２．評価・見直し

１２．１．監査

（１） 監査の計画

ア　CIOは､須賀川市情報セキュリティポリシーの順守状況に関する監査を定期的に行うこと。

イ　CIOは、監査の実施にあたり、監査員として監査責任者及び監査担当者を任命すること。

ウ　CIOは、監査を適切に行うため、監査員の育成に努めること。

エ　監査責任者は､監査対象､監査基準､監査項目等を定めた監査実施計画書を作成すること。

（２） 被監査部門の義務

ア　被監査部門は、監査員の協力要請に応じること。

イ　被監査部門は、監査作業の妨害、虚偽の報告及び事実の隠蔽をしないこと。

（３） 監査の実施

監査責任者は、監査実施計画書に基づき、監査を実施すること。

（４） 監査の報告

ア　監査責任者は、監査結果を取りまとめ、監査報告書を作成すること。

イ　監査責任者は、監査報告書を委員会に提出すること。

ウ　監査責任者は、必要に応じ、監査報告書の写しを被監査部門へ提出すること。ただし、機密事項等の記述に十分留意すること。

（５） 改善

ア　被監査部門は、指摘事項及び改善勧告に対する改善計画書を作成し、監査責任者及び委員会に提出すること。

イ　被監査部門は、改善計画書に基づき、指摘事項等の改善を実施すること。

ウ　監査責任者は一定期間経過後、被監査部門及び改善実施部門の改善実施状況を確認すること。

（６） 監査の委託

CIOは、必要に応じて事業者に対し監査の一部又は全部を委託することができる。

１２．２．点検

（１） 点検の計画

ア　情報セキュリティ管理者は、所管する課（廨）の情報セキュリティポリシーの順守状況に関し、定期的に点検を行うこと。

イ　情報セキュリティ管理者は､点検項目等を定めた､実施計画書を作成することが望ましい。

（２） 点検の実施

情報セキュリティ管理者は、実施計画に基づき、点検を実施することが望ましい。

（３） 点検結果の報告

ア　情報セキュリティ管理者は、点検結果を取りまとめ報告書を作成することが望ましい。

イ　情報セキュリティ管理者は、点検報告書を情報セキュリティ責任者に提出することが望ましい。

（４） 改善

情報セキュリティ管理者は、点検の結果、問題を発見した項目についての改善を実施することが望ましい。

１２．３．見直し

（１） 情報セキュリティポリシー、実施手順書の見直し

委員会は、情報セキュリティ監査及び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、基本方針、対策基準及び実施手順書の実効性を評価し、見直しが必要と判断した場合は、事務局に指示して更新を行うこと。

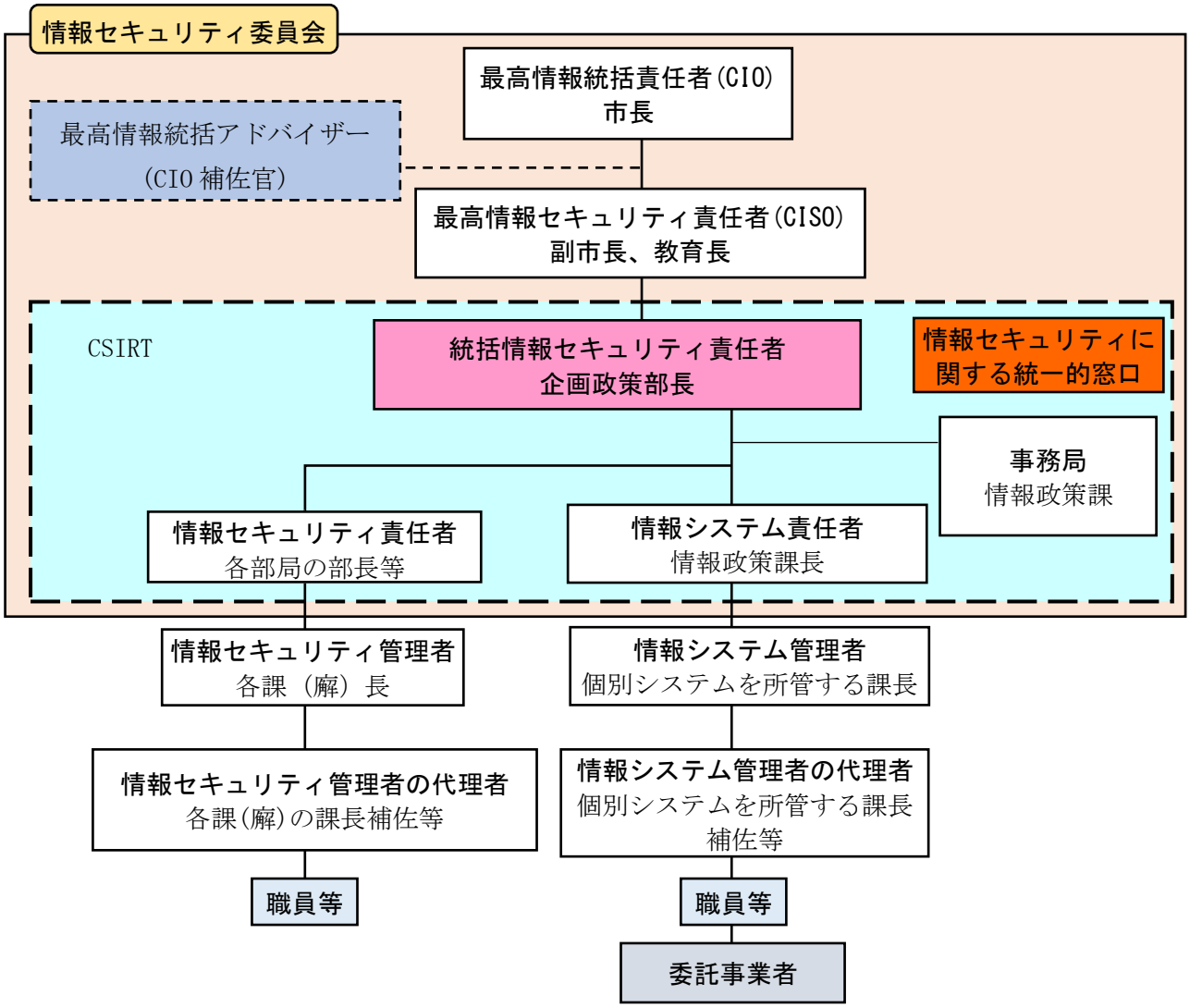
（２） セキュリティ対策の導入、見直し

ア　委員会は、情報セキュリティ監査及び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により情報システムに係る脆弱性を認めた場合は、該当する脆弱性への対策を検討し、物理的保護策及び技術的保護策の導入又は情報システムの見直しについて、所管する課（廨）の情報システム管理者に指示すること。

イ　情報システム管理者は、委員会からの指示に基づいて、物理的保護策及び技術的保護策の導入又は情報システムの見直しを実施すること。

ウ　委員会及び情報システム管理者は、実施した対策の確認を行うこと。

別表　情報セキュリティ推進組織体制表



様式　業務委託に関するセキュリティ要件チェックシート

項目	確認事項	チェック欄
1.基本事項	須賀川市情報セキュリティポリシー及び実施手順書の順守する。	□
2.秘密の保持	契約の履行に際して知り得た秘密を他に漏らさない。契約終了後、解除後及び退職後も同様とする。	□
3.目的外使用及び第三者への提供禁止	契約に係る情報を発注者が指示する目的以外に使用し、第三者に提供しない。	□
4.データの受領	発注者からデータ資産の提供を受けた場合は、データ資産持ち出し実施手順書（以下「持ち出し手順書」という。）に従い、受領証を発注者に提出する。	□
5.データの持ち出し	発注者の環境からデータ資産を持ち出す場合は、持ち出し手順書に従い持ち出す目的、データ資産の内容及び暗号化等の対策を記載し、発注者から承認を受ける。	□
	発注者の環境から業務システムで利用している本番データ（住民情報が含まれるデータ）を持ち出すことを禁止する。業務委託契約において本番データの持ち出しが認められている場合は、持ち出し手順書に従い発注者から承認を受ける。	□
6.権利侵害	著作権等の権利侵害及びソフトウェア等のライセンス違反をしないこと。	□
7.複写及び複製の禁止	本契約に係るデータ資産を発注者の承認なく、用紙、記録媒体等に複写し、又は複製しない。	□
8.パソコン及びデータの持ち込み	発注者の環境にパソコン及びデータ資産を持ち込み、作業を行う場合は、書面で発注者からパソコン及びデータ資産の持ち込みにかかる承認を受ける。	□
9.安全管理義務	契約に係るデータ資産の管理責任者を定め、業務の従事者を限定する。	□
	契約に係るデータ資産を取り扱う場所を特定する。	□
	データ資産の無断持ち出し禁止を周知徹底し、やむを得ず持ち出す場合は、持ち出し手順書に従い、発注者の承認を得たうえで、管理簿等の書面に記録する。	□
	紛失、損傷、焼失等の事故が生じないよう安全かつ適切な管理体制を整備する。	□
10.データの返却・消去	発注者から借用したデータ資産は、速やかに返却する。借用したデータ資産を複製・保存した場合は消去する。	□
11.記録媒体の廃棄	契約の履行上、発注者から廃棄指示がある場合の記録媒体等は、データ資産廃棄実施手順書に従い、すべての記録を復元不可能な状態に消去した後に廃棄し、廃棄したことがわかる書類を発注者に提出する。	□
12.監督及び監査	発注者が、契約の履行に関し必要があるときは、受注者及び再委託先に対して報告を求め、監査を行い、又は監査に立ち会うことができるよう体制等を整備する。	□
13.教育	従業員に対して、データ資産の保護及び秘密の保持等データ資産の取扱いに関し履行すべき責務について充分な教育を行う。	□
	受注者は、教育の実施状況を記録する。	□
14.事故発生の報告義務	安全管理措置等が履行できない場合及び情報漏えい等の事故が発生した場合等に備え、直ちに発注者へ通知、報告できる体制を整備する。	□
15.再委託の禁止	発注者の承諾なしに、業務を第三者に委託し又は請け負わせない。	□
	発注者の承諾を受けて再委託した場合は、再受注者に本契約の規定を順守させる。	□

付録　情報セキュリティポリシー関連用語集

用語	説明
電子情報	市が所管するコンピュータ、周辺機器及び電子媒体に電子的に記録された情報をいう（どこで誰が作成したかは問わない）。 例えば、以下のものが電子情報に該当する。 ア　パソコンを使用して作成した文書ファイル、図面ファイル等 イ　パソコンを使用して情報を入力したデータベース等 ウ　デジタルカメラ、ビデオカメラ、携帯電話等で撮影した画像ファイル、動画ファイル等 エ　IC レコーダー又は携帯電話等で録音した音声ファイル等 オ　市民が作成した文書ファイル等 カ　委託業者が作成した文書ファイル、図面ファイル等 キ　紙情報及びフィルム情報をスキャナで読み込み電子化したファイル等 ク　情報システムが生成した各種ログファイル及びシステム設定に係るファイル等
紙情報	手書きにより紙媒体に記入された情報及びプリンタ、プロッタ、コピー機等から紙媒体に印刷された情報をいう。 例えば、以下のものが紙情報に該当する。 ア　手書きにより情報が記入された各種申請書、請求書、メモ等 イ　市民からの請求によって提供される住民票、印鑑証明書等 ウ　収集又は作成した電子情報を、プリンタを使用して紙媒体に印刷した文書、入札仕様書図面、写真等 エ　情報システムが生成したログやシステム設定に係るファイルを、プリンタを使用して紙媒体に印刷したもの等
フィルム情報	文書、図面等を撮影したマイクロフィルム等、フィルム媒体に記録された情報をいう。
データ資産	電子情報、紙情報及びフィルム情報総称をいう。
情報セキュリティ	市が所管する情報資産に対する脅威、脆弱性に対して、組織的、人的、物理的及び技術的保護策を講じ、脅威が顕在化しないようにリスクを回避及び低減して、機密性、完全性及び可用性を維持することをいう。
機密性	市が所管する情報資産に対して、不正なアクセス（故意か過失かは問わない）を防止し、アクセスを許可された職員のみが、当該情報資産にアクセスできることをいう。

用語	説明
完全性	市が所管する情報資産に対して、改ざん及び破壊によるき損（故意か過失かは問わない）を防止し、誤りがなく正確であることをいう。
可用性	市が所管する情報資産に対して、許可された職員が必要とするときに確実に利用できることをいう。
脆弱性	市が所管する情報資産全般の取扱いにおける弱点であり、情報セキュリティ上の脅威が顕在化する可能性を高める要因をいう。
脅威	市が所管する情報資産が、漏えい、滅失、き損等の情報セキュリティアクシデントに遭遇するおそれのある潜在的な要因及び情報セキュリティアクシデントが顕在化した後に市が被るおそれのある事象をいう。 ア　潜在的な要因 (ア)職員（過失）：紛失、置き忘れ、操作ミス等 (イ)職員（故意）：不正アクセス、盗難、盗聴、改ざん、破壊等 (ウ)情報システム：マルウェア感染、システム停止等 (エ)災害等の脅威：地震、火災、水害等 イ　発生後に被る想定事象 (ア)改善命令 (イ)訴訟（刑事・民事） (ウ)信用の失墜等
リスク	市が所管する情報資産、環境及び組織における弱点によって、脅威が顕在化（情報セキュリティアクシデント）する可能性とその影響の大きさをいう。
ソフトウェア資産	ハードウェア資産を動作させる手順及び命令を当該ハードウェア資産が理解できる形式で記述したものの総称をいう。 例えば、以下のものがソフトウェア資産に該当する。 ア　オペレーティングシステム コンピュータ及び通信機器を動作させるための基本ソフトウェア イ　データベースソフトウェア 電子情報を蓄積する構造を定義し処理するためのソフトウェア ウ　アプリケーションソフトウェア 文書等を作成するソフトウェア及び特定の目的を達成するために情報を入力、加工及び出力処理するためのソフトウェア
記録媒体	情報を記録するために使用される、電子媒体、紙媒体及びフィルム媒体の総称をいう。

用語	説明
電子媒体	磁気式、光磁気式、光学式又はフラッシュメモリ方式により、電子情報を記録するために使用される媒体等をいう。 例えば、以下のものが電子媒体に該当する。 ア　磁気式 外付けハードディスク、デジタル音声テープ（DAT)、ビデオテープ等 イ　光学式 コンパクトディスク（CD,CD-R,CD-RW)、デジタル多目的ディスク（DVD-R,DVD-RW,DVD-RAM)、ブルーレイディスク（BD）等 ウ　フラッシュメモリ方式 USB メモリ、SD カード（SD,SDHC,SDXC)、マイクロ SD カード(microSD,microSDHC,microSDXC)、コンパクトフラッシュカード（CF）等
紙媒体	植物繊維その他の繊維を膠着させて製造したもので、筆記具等を使用した手書きによる情報の記録又はプリンタ及びプロッタを使用して、電子情報を印刷するために使用される媒体等をいう。 例えば、以下のものが紙媒体に該当する。 ア　帳票、様式 記入する情報の属性が予め印刷された申請書、請求書等の紙媒体 イ　カット紙 電子情報をプリンタ又はプロッタで印刷する際に使用したり、コピー機で複写する際に使用したりする紙媒体で、用途に応じて様々な材質及び寸法のものが存在する。 ウ　地紋紙 住民票等の印刷に使用する改ざん防止用の紙媒体
フィルム媒体	合成樹脂などの高分子成分などを薄い膜状に成型したもので、銀塩カメラ等で画像を記録するため使用される写真用フィルム、文書及び図面保管のためのマイクロフィルムをいう。
ハードウェア資産	コンピュータ、周辺機器、通信機器及び付帯設備の総称をいう。
周辺機器	情報システムを構成するハードウェア資産の１つであり、コンピュータと組合せて利用される各種機器の総称をいう。 機能別の分類として、入力系機器、出力系機器、ドライブ機器（電子媒体のリーダー／ライター装置)、特定の目的のために使用する機器及びこれらの機能が複合された機器（複合機）に大別される。 例えば、以下のものがある。

用語	説明
	ア　入力系機器 キーボード、マウス、スキャナ、OCR 等をいう。 イ　出力系機器 ディスプレイ、プリンタ、プロッタ、スピーカー等をいう。 ウ　ドライブ機器（電子媒体のリーダー／ライター） CD-R/RW ドライブ、DVD ドライブ、メモリカードリーダ等をいう。 エ　特定の目的のために使用する機器 オ　デジタルカメラ、ビデオカメラ、IC レコーダー、音楽プレイヤー等をいう。 カ　複合機 プリンタ、スキャナ、メモリカードリーダ等が１つの筐体に組み込まれた装置をいう。
サービスレベル	委託事業者等から提供を受けるサービスに係る安全面及び効率面での品質をいう。
人的資産	市の情報資産を取り扱う職員、委託業者、ボランティア等の総称をいう。
アクセス権限	市が所管する情報資産に対して、担当業務、職位等の組合せによって職員が取り扱える範囲をいう。
物理的保護策	電子情報を保存したパソコン、周辺機器及び電子媒体並びに紙情報及びフィルム情報が、物理的に破損、紛失、盗難、漏えいしないように物理的に保護するために行う対策をいう。 例えば、以下の対策が該当する。 ア　保管場所（ロッカー、机等）の施錠による保護 イ　セキュリティワイヤーによる保護（パソコン及び周辺機器） ウ　持ち出し時における専用かばん、専用ケース等による保護 エ　持ち出し時におけるエアーキャップ等による保護（電子媒体） オ　持ち出し時におけるネックストラップ等による保護（USB メモリ）等
技術的保護策	電子情報がアクセス権限のない者に取り扱われないように保護すること。及びマルウェア等から保護することで、漏えい、滅失、き損が起きないように行う対策をいう。 例えば、以下の対策が該当する。 ア　利用可能周辺機器及び電子媒体の制限 イ　本人認証による保護（アクセス制限） ウ　暗号化による保護

用語	説明
	エ　セキュリティ対策ソフトウェアによる保護等
情報セキュリティインシデント	職員が情報セキュリティポリシーを順守しない行為及び情報セキュリティ上のモラル等を順守しない行為又は情報システムの脆弱性により、情報セキュリティアクシデントが起こるおそれがある事象をいう。 市以外の第三者に認識されたかは不明だが、市民への被害等が想定されるものについて、外部への公表が必要な事象も含まれる。 例えば、以下のものが情報セキュリティインシデントに該当する。 ア　マルウェア感染 イ　パソコンの業務目的外利用 ウ　許可を受けない持ち出し（無断持ち出し） エ　情報資産の紛失又はそれらのおそれのある事象等
不正アクセス	コンピュータ及びアプリケーションソフトウェアへのアクセス権限を持たない者が、権限のある者のアカウントで不正にコンピュータ及びアプリケーションソフトウェアの利用を試みることをいう。
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、マルウェア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。
マルウェア	悪意のあるソフトウェアの総称。不正ソフトウェアとも呼ばれ、マルウェアがインストールされると、コンピュータに様々な影響を与える。主なマルウェアには、次のようなものがある。 ア　ルートキット セキュリティ攻撃を成功させた後に、その痕跡を消して見つかりにくくするためのツール イ　バックドア 正規の手続き（ログインなど）を行わずに利用できる通信経路。攻撃成功後の不正な通信などに利用される。 ウ　スパイウェア ユーザに関する情報を取得し、それを自動的に送信するソフトウェア。キーボードの入力を監視し、それを記録するキーロガーや、ユーザの承諾なしに新たなプログラムなどを無断でダウンロードし導入するダウンローダなどが該当する。 エ　ウイルス（コンピュータウイルス） 狭い意味では、自己感染機能、潜伏機能、発病機能がある悪意のあるソフトウェア。マルウェア一般の総称として用いられることもある。

用語	説明
	オ　トロイの木馬 悪意のないプログラムと見せかけて、不正な動きをするソフトウェア。自己感染機能は無い。 カ　ランサムウェア システムを暗号化するなどしてアクセスを制限し、その制限を解除するための代金（身代金）を要求するソフトウェア。 キ　アドウェア 広告を目的とした無料のソフトウェア。通常は無害だが、中にはユーザに気付かれないように情報を収集するような悪意のあるマルウェアが存在する。 ク　マクロウイルス 表計算ソフトやワープロソフトに組み込まれているマクロと呼ばれる簡易プログラムに感染するウイルス。 ケ　ボット インターネット上で自動化されたソフトウェア全般を指す。マルウェアとは限らない。不正目的のボットがボットネットとして協調して活動し、様々な攻撃を行う。例えば、離れたところから遠隔操作を行うことができる遠隔操作ウイルスは、ボットに該当する。近年では、攻撃者が用意したC&Cサーバ（Command &Control Server）を利用してボットに指令を出すことが増えている。 コ　ワーム 独立したプログラムで、自信を複製して他のシステムに拡散する性質をもったマルウェア。感染するときに宿主となるファイルを必要としない。
アプリケーション	応用ソフトとも呼ばれ、表計算やワープロ、インターネットの閲覧、音楽の再生など個別の機能に特化したソフトウェアを指す。
Web会議	離れた場所にいる相手とWebを介してリアルタイムで会議ができるツール。音声や映像だけでは区、データやアプリケーションの共有、文字のコミュニケーションが可能。