二本松市情報セキュリティポリシー

平成１８年３月　策定
平成２８年３月　改定
令和　３年３月　改定
令和　４年９月　改定

〈目　次〉

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、二本松市が所掌する情報資産の情報セキュリティを確保するための方針、体制、対策等を包括的に取りまとめたものを総称する。

情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であることから、明文化された文書として情報セキュリティポリシーを定めるものである。

情報セキュリティポリシーは、二本松市が所掌する情報資産に関する情報セキュリティ対策の頂点に位置するものであることから、市長をはじめ全ての職員等及び委託事業者は業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。

情報セキュリティポリシーの構成は、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「基本方針」と、基本方針に基づき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を定める「対策基準」の２階層に分けてそれぞれを策定する。

このほかに「対策基準」に基づき個別のネットワーク及び情報システム毎に具体化したものを「実施手順」として定めることとし、情報セキュリティポリシーの下部に位置づけ、体系は下表に示す階層構造とする。

情報セキュリティポリシーに関する体系

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第１章　情報セキュリティ基本方針

１．目的

二本松市の各情報システムが取り扱う情報は、法令等に基づき、市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、ほか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、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、市民生活や地域の社会経済活動を保護するため、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。

したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るために必要不可欠である。また、市政の安定的な運営や市民からの信頼の維持向上に寄与するものでもある。

今後、各種手続のオンライン利用の本格化や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、市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地方公共団体は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他の団体に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障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデント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。

そのため、二本松市が保有する情報資産の機密性、完全性及び可用性を維持するため二本松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

⑴　ネットワーク

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

⑵　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　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。

⑷　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

⑸　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。

⑹　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

⑺　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。

⑻　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。

⑼　ＬＧＷＡＮ接続系

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（マイナンバー利用事務系を除く。）。

⑽　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。

⑾　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。

⑿　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。

⑴　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、重要情報の詐取、内部不正等

⑵　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

⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　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

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

４．適用範囲

⑴　行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企

業とする。

⑵　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　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③　情報システムの仕様書及びネットワーク図等のシステム関連文書

５．職員等の遵守義務

職員、非常勤職員及び会計年度任用職員等（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及び情報セキュリティ実施手順を遵守しなければならない。

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。

⑴　組織体制

二本松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。

⑵　情報資産の分類と管理

二本松市の保有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実施する。

⑶　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、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、福島県及び市町村のインターネットとの通信を集約した自治体情報セキュリティクラウドに参加する。

⑷　物理的セキュリティ

サーバ、情報システム室、通信回線及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。

⑸　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、十分な教育及び啓

発を行う等の人的な対策を講じる。

⑹　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。

⑺　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、業務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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

⑻　業務委託と外部サービスの利用

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。

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。

⑼　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、適宜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及び自己点検の実施

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

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

９．情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及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二本松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２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、二本松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

⑴　最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「ＣＩＳＯ」という。）

①　副市長をＣＩＳＯとする。ＣＩＳＯは、二本松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及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

②　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及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。

④　ＣＩＳＯは、本対策基準に定められた自らの担務を、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。

⑵　統括情報セキュリティ責任者

①　情報政策担当部長を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。

②　統括情報セキュリティ責任者は、二本松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。

③　統括情報セキュリティ責任者は、二本松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。

④　統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及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及び助言を行う権限を有する。

⑤　統括情報セキュリティ責任者は、二本松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及び責任を有する。

⑥　統括情報セキュリティ責任者は、二本松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。

⑦　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、情報システム管理者、情報システム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。

⑧　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。

⑨　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。

⑶　情報セキュリティ責任者

①　内部部局の長、行政委員会事務局の長及び地方公営企業の部局の長を情報セキュリティ責任者とする。

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及び責任を有する。

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及び責任を有する。

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、非常勤職員及び会計年度任用職員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

⑷　情報セキュリティ管理者

①　内部部局の課長、内部部局の出先機関の長、行政委員会事務局の課長等及び地方公営企業の課長を情報セキュリティ管理者とする。

②　情報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　情報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、情報セキュリティ責任者、統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

⑸　情報システム管理者

①　各情報システムの担当課長等を当該情報システムに関する情報システム管理者とする。

②　情報システム管理者は、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。

③　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④　情報システム管理者は、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。

⑹　情報システム担当者

情報システム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担当者とする。

⑺　外部サービスの利用申請の許可権限者

① 統括情報セキュリティ責任者を外部サービスの利用申請の許可権限者とする。

② 外部サービスの利用申請の許可権限者は、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権限を有する。

③ 外部サービスの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。

⑻ 情報セキュリティ委員会

① 二本松市の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、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 二本松市電子情報化推進本部が、情報セキュリティ委員会を兼ねることとする。

⑼ 兼務の禁止

① 情報セキュリティ対策の実施において、止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、止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。

⑽ ＣＳＩＲＴの設置・役割

① ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化しなければならない。

② ＣＩＳＯ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 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しなければならない。

④ ＣＳＩＲＴは、ＣＩＳＯ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 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、ＣＩＳＯ、総務省、福島県等へ報告しなければならない。

⑥ 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・公表対応を行わなければならない。

⑦ 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、委託事業者等との情報共有を行わなければならない。

２．情報資産の分類と管理

⑴　情報資産の分類

二本松市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	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	・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） ・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電磁的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	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	行政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	・バックアップの実施、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 ・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の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	・バックアップの実施、指定する時間以内の復旧 ・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の情報資産以外の情報資産	－

⑵　情報資産の管理

①　管理責任

ア　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

イ　情報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⑴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）、格納する電磁的記録媒体のラベル、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⑴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、⑴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、電磁的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、当該電磁的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　情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

イ　情報セキュリティ管理者又は情報システム管理者は、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、書込禁止の措置を講じなければならない。

ウ　情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

エ　情報セキュリティ管理者又は情報システム管理者は、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。

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、情報セキュリティ管理者に許可を得なければならない。

⑨　情報資産の提供・公表

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、情報セキュリティ管理者に許可を得なければならない。

ウ　情報セキュリティ管理者は、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、情報セキュリティ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

⑴　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。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。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、この限りではなく、ＬＧＷＡＮを経由して、インターネット等とマイナンバー利用事務系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。

⑵　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

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、インターネット接続系から取り込む方式

⑶　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 都道府県及び市区町村のインターネットとの通信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

⑴ 機器の取付け

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

⑵ サーバの冗長化

① 情報システム管理者は、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及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

② 情報システム管理者は、重要情報を扱う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。

⑶ 機器の電源

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

⑷ 通信ケーブル等の配線

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

② 統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③ 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 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、自ら又は情報システム担当者及び契約により操作を認められた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。

⑸　機器の定期保守及び修理

①　情報システム管理者は、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　情報システム管理者は、電磁的記録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なければならない。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

⑹　庁外への機器の設置

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、庁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。

⑺　機器の廃棄等

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

４．２．管理区域（情報システム室等）の管理

⑴　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ための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

②　統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は１階に設けてはならない。

③　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、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　統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤　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、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　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、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的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。

⑵　管理区域の入退室管理等

①　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

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　情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された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　情報システム管理者は、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、電磁的記録媒体等を持ち込ませないようにしなければならない。

⑶　機器等の搬入出

①　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者に確認を行わせなければならない。

②　情報システム管理者は、情報システム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．通信回線及び通信回線装置の管理

①　統括情報セキュリティ責任者は、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、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

②　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、行政情報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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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．職員等の利用する端末や電磁的記録媒体等の管理

①　情報システム管理者は、盗難防止のため、執務室等で利用するパソコンの管理徹底、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的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 情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

③ 情報システム管理者は、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）を行うよう設定しなければならない。

④ 情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能や、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するよう努めなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用するよう努めなければならない。

⑤ 情報システム管理者は、モバイル端末の庁外での業務利用の際は、④の対策に加え、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

⑴ 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、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

② 業務以外の目的での使用の禁止

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 モバイル端末や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 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、二本松市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報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、情報セキュリティ管理者の許可を得なければならない。

④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア 職員等は、支給以外のパソコン、モバイル端末及び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、支給以外の端末の業務利用の可否判断をＣＩＳＯが行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報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、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合

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、保管しなければならない。

⑥　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、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情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、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。

⑵　非常勤及び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

情報セキュリティ管理者は、非常勤及び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、非常勤及び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

情報セキュリティ管理者は、非常勤及び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、非常勤及び会計年度任用職員等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しなければならない。

⑶　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。

⑷　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・保守等を委託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。

５．２．研修・訓練

⑴　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。

⑵　研修計画の策定及び実施

①　ＣＩＳＯは、幹部を含め全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の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会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、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、情報システム管理者、情報システム担当者及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　情報セキュリティ管理者は、所管する課等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報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　統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、ＣＩＳＯに情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

⑦　ＣＩＳＯは、適宜、情報セキュリティ委員会に対して、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。

⑶　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、ネットワーク及び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。

⑷　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。

５．３．情報セキュリティインシデントの報告

⑴　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、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ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　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③　情報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ＣＩＳＯ及び情報セキュリティ責任者に報告しなければならない。

⑵　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、二本松市が管理するネットワーク及び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、情報セキ

ュリティ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 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③ 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について、必要に応じてＣＩＳＯ及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。

⑶ 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及びパスワード等の管理

⑴ 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又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、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者は、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 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、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。

⑵　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。

⑶　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　パスワードは、他者に知られないように管理しなければならない。

②　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。

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。

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にパスワードを記憶させてはならない。

⑧　職員等間でパスワードを共有してはならない（ただし、共用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．コンピュータ及びネットワークの管理

⑴　文書サーバの設定等

①　情報システム管理者は、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　情報システム管理者は、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　情報システム管理者は、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。

⑵　バックアップの実施

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、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

⑶　他団体との情報システムに関する情報等の交換

情報システム管理者は、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、統括情報セキュリティ責任者及び

情報セキュリティ責任者の許可を得なければならない。

⑷　システム管理記録及び作業の確認

①　情報システム管理者は、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　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、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正に管理しなければならない。

③　統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた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。

⑸　情報システム仕様書等の管理

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。

⑹　ログの取得等

①　統括情報セキュリティ責任者及び情報システム管理者は、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　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、ログとして取得する項目、保存期間、取扱方法及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　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、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。

⑺　障害記録

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、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

⑻　ネットワークの接続制御、経路制御等

①　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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。

⑼　外部の者が利用できるシステムの分離等

情報システム管理者は、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。

⑽　外部ネットワークとの接続制限等

①　情報システム管理者は、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及び統括情報セキュリティ責任者の許可を得なければならない。

②　情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、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　情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④　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、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　情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑾　複合機のセキュリティ管理

①　統括情報セキュリティ責任者は、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、適正なセキュリティ要件を策定しなければならない。

②　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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。

⑿　ＩｏＴ機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、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。

⒀　無線ＬＡＮ及びネットワークの盗聴対策

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

②　統括情報セキュリティ責任者は、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。

⒁　電子メールのセキュリティ管理

①　統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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しなければならない。

③ 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、システム開発や運用、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。

⑥ 統括情報セキュリティ責任者は、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不可能となるように添付ファイルの監視等による措置を講じるものとする。

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、情報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、ＣＩＳＯが定めた電子署名、パスワード等による暗号化又等、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、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

② 職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを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、パソコンやモバイル端末に対し機器の改造及び増設・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及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム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 情報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 統括情報セキュリティ責任者は、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、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

㉑ Ｗｅｂ会議サービスの利用時の対策

① 統括情報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、二本松市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、二本松市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 情報セキュリティ管理者は、二本松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運用手順を定めなければならない。

ア 二本松市のアカウントによる情報発信が、実際の二本松市のものであることを明らかにするために、二本松市の自己管理Ｗｅｂサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

イ パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、ＵＳＢメモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

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には、二本松市の自己管理Ｗｅｂサイトに当該情報を掲載して参照可能とすること。

６．２．アクセス制御

⑴　アクセス制御等

①　アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない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　統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、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、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、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　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、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　統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、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に通知しなければならない。

エ　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、特権を付与されたＩＤ及びパスワードの変更について、委託事業者に行わせてはならない。

オ　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、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　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、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。

⑵　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、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　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、外部からのアクセスに利用するモバイル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モバイル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、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

⑦　統括情報セキュリティ責任者は、内部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、止むを得ず接続を許可する場合は、利用者の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。

⑶　自動識別の設定

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。

⑷　ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ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。

⑸　認証情報の管理

①　統括情報セキュリティ責任者又は情報システム管理者は、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 統括情報セキュリティ責任者又は情報システム管理者は、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、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③ 統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

⑹ 特権による接続時間の制限

情報システム管理者は、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。

６．３．システム開発、導入、保守等

⑴ 情報システムの調達

① 統括情報セキュリティ責任者及び情報システム管理者は、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 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、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。

⑵ 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

情報システム管理者は、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 情報システム管理者は、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、開発用ＩＤを削除しなければならない。

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

⑶ 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 情報システム管理者は、システム開発、保守及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 情報システム管理者は、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。

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

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

② テスト

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

イ　情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

ウ　情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

エ　情報システム管理者は、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。

⑷　システム開発・保守に関連する資料等の整備・保管

① 情報システム管理者は、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正に整備・保管しなければならない。

② 情報システム管理者は、テスト結果を一定期間保管しなければならない。

③ 情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

⑸　情報システムにおける入出力データの正確性の確保

① 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② 情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを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 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

⑹　情報システムの変更管理

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

⑺　開発・保守用のソフトウェアの更新等

情報システム管理者は、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。

⑻　システム更新又は統合時の検証等

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

６．４．不正プログラム対策

⑴　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　所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

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。

⑵　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、次の事項を措置しなければならない。

①　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、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、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、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

⑶　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　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

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接続系に取り込む場合は無害化しなければならない。

⑥　統括情報セキュリティ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又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。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しなければならない。

⑷　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しておかなければならない。

６．５．不正アクセス対策

⑴　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、設定しなければならない。

④　重要なシステムの設定を行ったファイル等について、適宜当該ファイルの改ざんの有

無を確認しなければならない。

⑤　統括情報セキュリティ責任者は、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。

⑵　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なければならない。また、総務省、福島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。

⑶　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なければならない。

⑷　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、職員等及び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。

⑸　職員等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セキュリティ管理者に通知し、適正な処置を求めなければならない。

⑹　サービス不能攻撃

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

⑺　標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

６．６．セキュリティ情報の収集

⑴　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

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティ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。

⑵　不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、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。

⑶　情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、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　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②　統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③　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　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、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入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

⑴　遵守状況の確認及び対処

①　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにＣＩＳＯ及び統括情報セキュリティ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　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

⑵　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

⑶　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、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

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

⑴ 緊急時対応計画の策定

ＣＩＳＯ又は情報セキュリティ委員会は、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。

⑵ 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

⑶ 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、情報セキュリティ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しなければならない。

⑷ 緊急時対応計画の見直し

ＣＩＳＯ又は情報セキュリティ委員会は、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さなければならない。

７．４．例外措置

⑴ 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、情報セキュリティに関係する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、ＣＩＳＯの許可を得て、例外措置を講じることができる。

⑵ 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ＣＩＳＯに報告しなければならない。

⑶ 例外措置の申請書の管理

ＣＩＳＯ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

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２５年法律第２６１号)
② 著作権法（昭和４５年法律第４８号）
③ 不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
④ 個人情報の保護に関する法律（平成１５年法律第５７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２５年法律第２７号）
⑥ サイバーセキュリティ基本法（平成２６年法律第１０４号）
⑦ 二本松市個人情報保護条例（平成１７年二本松市条例第１８号）
⑧ 二本松市電子計算機処理に係る管理運営規程（平成１７年二本松市訓令第１２号）
⑨ 二本松市特定個人情報等の安全管理措置に関する規程（平成３０年二本松市訓令第７号）

７．６．懲戒処分等

⑴ 懲戒処分

情報セキュリティポリシーに違反した職員等及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。

⑵ 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 統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
② 情報システム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統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
③ 情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該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、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨をＣＩＳＯ及び当該職員等が所属する課等の情報セキュリティ管理者に通知しなければならない。

８．業務委託と外部サービスの利用

８．１．業務委託

⑴　委託事業者の選定基準

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

②　情報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。

⑵　契約項目

情報システムの運用、保守等を業務委託する場合には、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。

①　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

②　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

③　提供されるサービスレベルの保証

④　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

⑤　委託事業者の従業員に対する教育の実施

⑥　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

⑦　業務上知り得た情報の守秘義務

⑧　再委託に関する制限事項の遵守

⑨　委託業務終了時の情報資産の返還、廃棄等

⑩　委託業務の定期報告及び緊急時報告義務

⑪　市による監査、検査

⑫　市による情報セキュリティインシデント発生時の公表

⑬　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）

⑶　確認・措置等

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、⑵の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ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．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）

⑴　外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、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８．２節において「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

⑵　外部サービスの選定

①　情報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　情報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。

ア　外部サービスの利用を通じて二本松市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、二本松市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並びに調達仕様書による施設の場所やリージョンの指定

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

③　情報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。

④　情報セキュリティ責任者は、外部サービスの利用を通じて二本松市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。

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

⑤　情報セキュリティ責任者は、外部サービスの利用を通じて二本松市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、必要に応じて二本松市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。

⑥　情報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二本松市に提供し、二本松市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。

⑦　情報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。

⑧　情報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。

⑨　統括情報セキュリティ責任者は、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。

⑶　外部サービスの利用に係る調達・契約

①　情報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及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

②　情報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。

⑷　外部サービスの利用承認

①　情報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。

⑸　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　統括情報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・設定時の誤り防止

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。

⑹　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　統括情報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、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

② 情報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、前各号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。

⑺ 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 統括情報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、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。

８．３．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）

⑴ 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、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。

① 外部サービスを利用可能な業務の範囲

② 外部サービスの利用申請の許可権限者と利用手続

③ 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

④ 外部サービスの利用の運用手順

⑵ 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 情報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。

９．評価・見直し

９．１．監査

⑴　実施方法

ＣＩＳＯは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、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。

⑵　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。

⑶　監査実施計画の立案及び実施への協力

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、情報セキュリティ委員会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。

⑷　委託事業者に対する監査

事業者に業務委託を行っている場合、情報セキュリティ監査統括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。

⑸　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、情報セキュリティ委員会に報告する。

⑹　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。

⑺　監査結果への対応

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

⑻　情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．２．自己点検

⑴　実施方法

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

⑵　報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、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、情報セキュリティ委員会に報告しなければならない。

⑶　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。

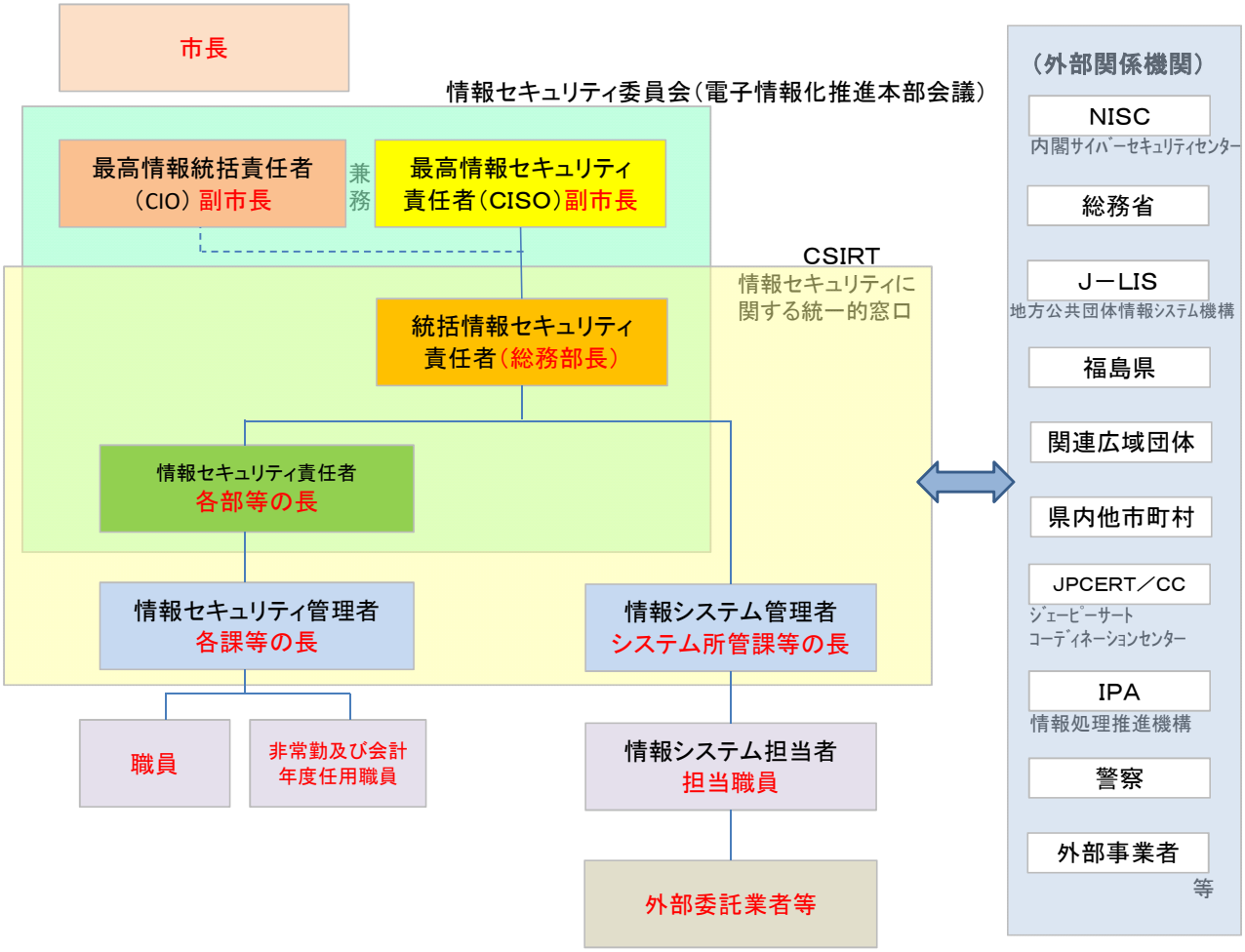
②　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．３．情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、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及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

付録1

情報セキュリティ推進の組織体制



付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）				項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ統括責任者（指名）	情報セキュリティ監査利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
1 組織体制	⑴	①		最高情報セキュリティ責任者の設置		○											
		②		最高情報セキュリティアドバイザーの設置		○											
		③		ＣＳＩＲＴの整備		○										△	
		④		対策基準に定められた担務の委譲		○	△	△	△	△		△					
	⑵	①		統括情報セキュリティ責任者の設置		△	○										
		②		ネットワークにおける開発等の権限及び責任			○										
		③		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			○										
		④		情報セキュリティ責任者等に対する指導及び助言			○	△	△	△	△						
		⑤		情報資産に対するセキュリティ侵害が発生した場合等の権限及び責任		△	○										
		⑥		情報セキュリティ実施手順の維持・管理の権限及び責任			○										
		⑦		最高情報セキュリティ責任者等との連絡体制の整備		△	○	△	△	△	△						
		⑧		緊急時の報告と回復のための対策		△	○										
		⑨		情報セキュリティ関係規程に係る課題及び問題点の報告		△	○										
	⑶	①		情報セキュリティ責任者の設置				○									
		②		部局等の情報セキュリティ対策に関する統括的な権限及び責任				○									
		③		部局等の情報システムの開発等の統括的な権限及び責任				○									
		④		部局等の情報システムにおける連絡体制の整備等				○							△		
	⑷	①		情報セキュリティ管理者の設置					○								
		②		課室等の情報セキュリティ対策に関する権限及び責任					○								
		③		情報資産に対するセキュリティ侵害が発生した場合等の報告等		△	△	△	○								
	⑸	①		情報システム管理者の設置						○							
		②		情報システムにおける開発等の権限及び責任						○							
		③		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						○							
		④		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						○							
	⑹			情報システム担当者の設置						△	○						
	⑺	①		外部サービスの利用申請の許可権限者の設置									○				
		②		外部サービスの利用申請に関する権限									○				
		③		承認済み外部サービスの記録と外部サービス管理者の指名									○		△		
	⑻	①		情報セキュリティ委員会の設置	○												
		②		二本松市電子情報化推進本部が情報セキュリティ委員会を兼ねる	○												
	⑼	①		情報セキュリティ対策の実施における承認等の申請者とその承認者等の兼務の禁止													
		②		監査を受ける者と監査を実施する者の兼務の禁止													
	⑽	①		ＣＳＩＲＴの整備		○										△	
		②		ＣＳＩＲＴに属する職員等の選任		○	△	△	△	△						△	
		③		情報セキュリティに関する統一的な窓口の設置		○											
		④		セキュリティ戦略の意思決定が行われた際に、内容を関係部局等に提供		△	△	△	△	△						○	
		⑤		情報セキュリティインシデントの関係機関への報告		△										○	
		⑥		情報セキュリティインシデントの報道機関への通知・公表等												○	
		⑦		情報セキュリティに関する他の関係機関や窓口等との情報共有												○	
2 情報資産の分類と管理	⑴			情報資産の分類													
	⑵	①	ア	情報資産の管理責任					○								
			イ	複製等された情報資産の管理責任					○								
		②		情報資産の分類の表示											○		
		③	ア	業務上必要のない情報の作成の禁止											○		
			イ	情報作成時の情報の分類と取扱制限の設定											○		
			ウ	作成途上の情報の取扱											○		
		④	ア	庁内の者が作成した情報資産の取扱い											○		
			イ	庁外の者が作成した情報資産の分類と取扱い											○		
			ウ	分類が不明な情報資産を入手した際の対応					△						○		
		⑤	ア	情報資産の業務外目的の利用の禁止											○		
			イ	情報資産の分類に応じた適正な取扱い											○		
			ウ	情報資産の分類が異なる電磁的記録媒体の取扱い											○		
		⑥	ア	情報資産の分類に応じた適正な保管					○	○							
			イ	長期保管する情報資産を記録した電磁的記録媒体の保管					○	○							
			ウ	利用頻度の低い電磁的記録媒体等の保管					○	○							

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。
※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）					項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ監査統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
［２］		⑵		エ	電磁的記録媒体の施錠可能な場所への保管					○	○							
			⑦		電子メール等での送信時の対策											○		
			⑧	ア	車両等での情報資産運搬時の対策											○		
				イ	情報資産運搬の許可					許						○		
			⑨	ア	情報資産の外部への提供時の対策											○		
				イ	情報資産の外部への提供の許可					許						○		
				ウ	住民に公開する情報資産の取扱い					○								
			⑩	ア	情報資産廃棄時やリース返却時等の対策											○		
				イ	情報資産廃棄時やリース返却時等の処理の記録											○		
				ウ	情報資産廃棄やリース返却時等の許可					許						○		
３ 情報システム全体の強靭性の向上		⑴	①		マイナンバー利用事務系と他の領域との分離		○	○										
			②	ア	情報のアクセス対策											○		
				イ	情報の持ち出し不可設定											○		
		⑵	①		ＬＧＷＡＮ接続系とインターネット接続系の分割		○	○										
		⑶	①		高度な情報セキュリティ対策		○	○										
			②		自治体情報セキュリティクラウドの導入		○	○										
４ 物理的セキュリティ	４．１ サーバ等の管理	⑴			サーバ等取付け時の必要な措置						○							
		⑵	①		サーバの冗長化						○							
			②		システム運用停止時間の最小化						○							
		⑶	①		予備電源の設置			△			○							
			②		過電流に対する機器の保護措置			△			○							
		⑷	①		通信ケーブル等の損傷防止措置			○			○							
			②		通信ケーブル等の損傷等時の対応			○			○							
			③		ネットワーク接続口の管理			○			○							
			④		配線の変更・追加の防止措置			○			○	△						△
		⑸	①		機器の定期保守の実施						○							
			②		修理時における事業者からの情報漏えい防止措置						○							△
		⑹			庁外への機器の設置		承	○			○							
		⑺			機器の廃棄等の措置						○							
	４．２ 管理区域（情報システム室等）の管理	⑴	①		管理区域の定義													
			②		管理区域の構造			○			○							
			③		管理区域への立入制限等			○			○							
			④		耐震対策等の対策			○			○							
			⑤		外壁等の床下開口部における措置			○			○							
			⑥		消火薬剤等の設置方法			○			○							
		⑵	①		入退室管理方法						○					○		○
			②		入室時の身分証明書等の携帯及び提示											○		○
			③		外部からの訪問者に対する入室管理						○					△		
			④		情報システムに関連しないコンピュータ等の持ち込み禁止						○							
		⑶	①		搬入する機器の既存情報システムへの影響確認						○					△		△
			②		機器等の搬入時の職員の立ち会い						○					△		
	４．３ 通信回線及び通信回線装置の管理		①		庁内の通信回線等の適正な管理等			○										
			②		外部へのネットワーク接続の限定措置			○										
			③		行政系ネットワークのLGWANへの集約			○										
			④		通信回線に利用する回線の選択等			○										
			⑤		回線の十分なセキュリティ対策の実施			○										
			⑥		可用性の高い情報を扱う通信回線の可用性の確保			○										
	４．４ 職員等の利用する端末や電磁的記録媒体等の管理		①		パソコン、モバイル端末等及び電磁的記憶媒体の盗難防止措置						○							
			②		情報システムへの認証情報の設定						○							
			③		多要素認証の設定						○							
			④		パソコン、モバイル端末等におけるデータの暗号化等の利用						○							
			⑤		モバイル端末に対する遠隔消去機能等の利用						○							
５ 人的セキュリティ	５．１ 職員等の遵守事項	⑴	①		情報セキュリティポリシー等の遵守					△						○		
			②		情報資産の業務目的以外での使用の禁止											○		
			③	ア	情報資産の外部での処理時の安全管理措置		○											
				イ	モバイル端末や電磁的記録媒体等の持ち出しの許可					許						○		

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）					項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
［５］	［５．１］	⑴		ウ	外部での情報処理業務の許可					許						○		
			④	ア	支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用禁止											○		
					支給以外の端末の業務利用可否判断		○											
					支給以外の端末の業務利用に係る実施手順			○		許								
				イ	支給以外のパソコン、モバイル端末及び電磁的記録媒体等の安全管理措置					許						○		
			⑤		端末等の持出及び持込の記録等					○								
			⑥		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					許						○		
			⑦		机上の端末等の管理					許						○		
			⑧		退職時等の遵守事項											○		
		⑵	①		非常勤職員等の採用時の対応					○						△		
			②		非常勤職員等の採用時の同意書への署名					○						△		
			③		インターネット接続等の利用制限					○						△		
		⑶			情報セキュリティポリシー等の掲示					○						△		
		⑷			委託事業者に対する説明					○								△
	５．２研修・訓練	⑴			情報セキュリティに関する研修・訓練の実施		○											
		⑵	①		研修計画の策定等	承	○											
			②		情報セキュリティ研修の受講											○		
			③		新規採用の職員等に対する研修の実施		○									△		
			④		理解度等に応じた研修の実施		○	△	△	△	△	△				△		
			⑤		所管する課室等の研修実施状況の記録及び報告			△	△	○								
			⑥		研修実施状況の分析、評価及び報告		△	○										
			⑦		研修の受講状況の報告	△	○											
		⑶			緊急時対応訓練の実施		○											
		⑷			研修・訓練の参加義務											○		
	５．３情報セキュリティインシデントの報告	⑴	①		情報セキュリティインシデントの報告					△						○	△	
			②		情報システムに関連する情報セキュリティインシデントの報告			△		○	△						△	
			③		情報セキュリティインシデントの必要に応じた報告		△		△	○								
		⑵	①		住民等外部からの報告時の対応					△						○	△	
			②		情報システム又はネットワークに関連する情報セキュリティインシデントの報告			△		○	△						△	
			③		情報セキュリティインシデントに関する報告		△		△	○								
			④		住民等外部に対する窓口の設置等		○											
		⑶	①		情報セキュリティインシデントの可能性に対する評価												○	
			②		情報セキュリティインシデントの報告		△										○	
			③		応急措置の実施及び復旧に係る指示			△	△	△	△	△				△	○	
			④		情報セキュリティインシデントの原因の究明、記録の保存、再発防止策の報告		△										○	
			⑤		再発防止策の実施に必要な措置の指示		○										△	
	５．４ＩＤ及びパスワード等の管理	⑴	①	ア	認証に用いるICカード等の職員等間共有の禁止											○		
				イ	ＩＣカード等のカードリーダ等への常時挿入禁止											○		
				ウ	ＩＣカード等紛失時の通報			△			△					○		
			②		ＩＣカード紛失時のアクセス停止措置			○			○							
			③		ＩＣカード切り替え時の旧カードの廃棄方法			○			○							
		⑵	①		自己のＩＤの他人による利用の禁止											○		
			②		共用ＩＤ利用者以外による共用ＩＤ利用禁止											○		
		⑶	①		パスワードの管理											○		
			②		パスワードの秘密保持											○		
			③		パスワードの文字及び文字数の選択											○		
			④		パスワードが流出したおそれのある時の措置					△						○		
			⑤		パスワードのシステム間の共有禁止											○		
			⑥		仮パスワードの変更											○		
			⑦		パスワードの記憶機能の利用禁止											○		
			⑧		職員等間でのパスワード共有禁止											○		

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。
※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）				項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
６ 技術的セキュリティ	６．１ コンピュータ及びネットワークの管理	⑴	①	文書サーバの容量の設定等						○							
			②	文書サーバの課等単位での構成						○							
			③	特定の情報のためのディレクトリ設定						○							
		⑵		定期的なバックアップの実施			○			○							
		⑶		他団体との情報システムに関する情報等の交換する場合の許可等			許	許		○							
		⑷	①	情報システムの運用に係る作業記録の作成						○							
			②	システム変更等時の作業内容の記録作成等			○			○							
			③	システム変更の作業方法			○			○	○						○
		⑸		ネットワーク構成図等の保管			○			○							
		⑹	①	ログの取得等			○			○							
			②	ログの管理			○			○							
			③	ログの点検・分析			○			○							
		⑺		システム障害等の記録、保存			○			○					△		
		⑻	①	通信ソフトウェア等の設定情報の管理			○										
			②	ネットワークのアクセス制御			○										
		⑼		外部の者が利用できるシステムの分離等						○							
		⑽	①	ネットワークを外部接続する際の許可		許	許			○							
			②	外部ネットワークの接続による影響の確認						○							
			③	外部ネットワーク管理責任者による損害賠償責任の契約上の担保						○							
			④	ファイアウォール等の設置			○			○							
			⑤	問題発生時の物理的な遮断			△			○							
		⑾	①	複合機を調達する場合のセキュリティ要件の策定			○										
			②	複合機に対するセキュリティ設定と情報セキュリティインシデント対策の実施			○										
			③	複合機の運用終了時の対策			○										
		⑿	①	ＩｏＴ機器を含む特定用途機器に対する対策の実施			○										
		⒀	①	無線ＬＡＮ利用時の暗号化等の使用義務設定			○										
			②	機密性の高いネットワークへの暗号化等の措置			○										
		⒁	①	電子メールサーバへの中継処理禁止の設定			○										
			②	内部からのスパムメール等の送信を検知した際のメールサーバの運用停止			○										
			③	電子メールの送受信容量の上限設定等			○										
			④	電子メールボックスの容量の上限設定等			○								△		
			⑤	委託事業者の電子メールアドレス利用取り決め			○										○
			⑥	電子メールの添付ファイルの監視等			○										
		⒂	①	電子メールの自動転送機能の禁止											○		
			②	業務上必要のない送信先への送信禁止											○		
			③	複数人に電子メールを送信する際の方法											○		
			④	重要メールの誤送信時の報告					△						○		
		⒃	①	電子署名、暗号化等による送信		○									○		
			②	暗号化の方法及び鍵の管理		○									○		
			③	電子署名の正当性を確認する手段の提供		○											
		⒄	①	ソフトウェアの無断導入の禁止											○		
			②	ソフトウェアの導入の許可の取得及びライセンスの管理			許			許					○		
			③	不正コピーしたソフトウェアの利用禁止											○		
		⒅	①	機器の改造及び増設・交換の禁止											○		
			②	機器の改造及び増設・交換等の許可			許			許					○		
		⒆	①	支給端末の許可されたネットワーク以外への接続禁止						許					○		
			②	支給端末への技術的な制限の実施					○								
		⒇	①	業務目的以外のウェブ閲覧の禁止											○		
			②	業務目的以外のウェブ閲覧発見時の対応			○		△								
		(21)	①	Ｗｅｂ会議サービスの利用手順の策定			○										
			②	Ｗｅｂ会議サービス利用時の情報セキュリティ対策											○		
			③	Ｗｅｂ会議主催時の対策											○		
			④	外部からＷｅｂ会議に招待される場合の必要に応じた利用申請											○		

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。
※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）					項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
［６］	［６．１］	(22)	①	ア	情報発信におけるなりすまし対策の実施					○								
				イ	認証情報及びこれを記録した媒体の適切な管理					○								
			②		機密性２以上の情報のソーシャルメディアサービスでの発信禁止					○								
			③		利用するソーシャルメディアサービスごとの責任者の決定					○								
			④		アカウント乗っ取り確認時の措置					○								
			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の措置					○								
	６．２アクセス制御	(1)	①		アクセス制御			○			○							
			②	ア	利用者の情報管理や利用者ＩＤの取扱い等の設定			○			○							
				イ	利用者登録抹消の申請			△			△					○		
				ウ	利用されていないＩＤの点検			○			○							
			③	ア	ＩＤ及びパスワードの管理			○			○							
				イ	統括情報セキュリティ責任者等の特権を代行する者の要件		○	○			○							
				ウ	特権代行者の通知		○	△	△	△	△							
				エ	特権付与されたＩＤ等の変更の委託事業者への委託禁止			○			○							○
				オ	特権付与されたＩＤ等のセキュリティ機能強化			○			○							
				カ	特権付与されたＩＤの初期設定以外のものへの変更			○			○							
		(2)	①		外部から内部ネットワーク等へのアクセスの許可			許			許					○		
			②		外部からのアクセス可能人数の制限			○										
			③		外部からのアクセス時の本人確認の機能の確保			○										
			④		外部からのアクセス時の通信の暗号化等の措置			○										
			⑤		外部アクセス用端末等付与時のセキュリティの確保			○			○							
			⑥		外部から持ち込んだ端末等のウイルスの確認等					許						○		
			⑦		インターネットを介した庁内ネットワークへの接続禁止			○										
		(3)			自動識別の設定			○			○							
		(4)			ログイン時のシステム設定						○							
		(5)	①		職員等の認証情報の管理等			○			○							
			②		パスワード発行等			○			○							
			③		認証情報の不正利用防止			○			○							
		(6)			特権によるネットワーク等への接続時間の制限						○							
	６．３システム開発、導入、保守等	(1)	①		調達仕様書への技術的なセキュリティ機能の明記			○			○							
			②		調達時のセキュリティ機能の調査等			○			○							
		(2)	①		システム開発の責任者及び作業者の特定と規則の確立						○							
			②	ア	システム開発の責任者等のＩＤの管理等						○							
				イ	システム開発の責任者等のアクセス権限の設定						○							
			③	ア	システム開発におけるソフトウェア等の特定						○							
				イ	認定外のソフトウェアの削除						○							
		(3)	①	ア	システム開発等環境とシステム運用環境の分離						○							
				イ	システム開発環境からシステム運用環境への移行の手順の明確化						○							
				ウ	移行に伴うシステム停止等の影響の最小化						○							
				エ	導入されるシステムやサービスの可用性の確保確認						○							
			②	ア	新たなシステム導入前の十分な試験の実施						○							
				イ	運用テスト時の擬似環境による操作確認の実施						○							
				ウ	テストデータとして個人情報等の使用禁止						○							
				エ	受け入れ時のテストの実施						○							
		(4)	①		システム開発等の資料等の整備・保管						○							
			②		テスト結果の保管						○							
			③		情報システムに係るソースコードの保管						○							
		(5)	①		入力データの正確性を確保できる情報システム設計						○							
			②		情報の改ざん等を検出する情報システム設計						○							
			③		出力データの正確性を確保できる情報システム設計						○							
		(6)			プログラム仕様書等の変更履歴の作成						○							
		(7)			ソフトウェア更新等時の他の情報システムとの整合性確認						○							
		(8)			システム更新又は統合時の検証等の実施						○							

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。
※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）				項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ監査統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
［６］	６．４不正プログラム対策	⑴	①	不正プログラムのシステムへの侵入防止措置			○										
			②	不正プログラムの外部への拡散防止措置			○										
			③	不正プログラム情報の収集、職員等への注意喚起			○										
			④	不正プログラム対策ソフトウェアの常駐			○										
			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の更新			○										
			⑥	不正プログラム対策ソフトウェアの更新			○										
			⑦	サポート終了ソフトウェアの使用禁止			○										
		⑵	①	不正プログラム対策ソフトウェアの常駐						○							
			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の更新						○							
			③	不正プログラム対策ソフトウェアの更新						○							
			④	インターネットに接続していないシステムにおける電磁的記録媒体の制限及び不正プログラム対策ソフトウェアの導入等						○							
			⑤	不正プログラム対策ソフトウェア等の設定変更権限の一括管理						○							
		⑶	①	不正プログラム対策ソフトウェアの設定変更の禁止											○		
			②	外部からのデータ又はソフトウェア取込時のウイルスチェックの実施											○		
			③	差出人が不明等の添付ファイルの削除											○		
			④	不正プログラム対策ソフトウェアによる定期的なフルチェックの実施											○		
			⑤	添付ファイル送受信時のウイルスチェック、無害化処理の実施											○		
			⑥	ウイルス情報の確認			△								○		
			⑦	パソコン等の端末のウイルス感染時の対処方法											○		
		⑷		外部の専門家の支援体制の整備			○										
	６．５不正アクセス対策	⑴	①	使用されていないポートの閉鎖			○										
			②	不要なサービス機能の削除、停止			○										
			③	ウェブページの改ざんを防止するための設定			○			△							
			④	定期的なファイルの改ざんの有無の検査			○										
			⑤	監視、通知、外部連絡窓口などの体制及び連絡窓口の構築			○									○	
		⑵		攻撃を受けた場合、または受けるリスクがある場合への対応		○	○										
		⑶		攻撃を受けた記録の保存		○	○										
		⑷		内部からの攻撃等の監視			○			○							
		⑸		職員等による不正アクセス発見時の対応			○		△	○							
		⑹		サービス不能攻撃対策の実施			○			○							
		⑺		標的型攻撃対策の実施			○			○							
	６．６セキュリティ情報の収集	⑴		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			○			○							
		⑵		不正プログラム等のセキュリティ情報の収集・周知			○										
		⑶		情報セキュリティに関する技術情報の収集及び共有			○			○							
７運用	７．１情報システムの監視		①	情報システムの監視			○			○							
			②	サーバの正確な時刻設定等の措置			○			○							
			③	外部と常時接続するシステムの監視			○			○							
			④	通信データの監視のための復号			○			○							
	７．２情報セキュリティポリシーの遵守状況の確認	⑴	①	情報セキュリティポリシーの遵守状況の確認等		△	△	○	○								△
			②	問題発生時の対処		○											
			③	システム設定等における情報セキュリティポリシー遵守状況の定期的な確認等			○			○							
		⑵		モバイル端末及び電磁的記録媒体等の利用状況調査		○											
		⑶	①	違反行為の発見時の報告			△		△						○		
			②	緊急時対応計画に従った対応			○								△		
	７．３侵害時の対応等	⑴		緊急時対応計画の策定	○	○											
		⑵		緊急時対応計画に盛り込むべき内容	○	○											
		⑶		業務継続計画と情報セキュリティポリシーの整合性の確保	○												
		⑷		緊急時対応計画の見直し	○	○											
	７．４例外措置	⑴		例外措置の許可		許			○	○							
		⑵		緊急時の例外措置		△			○	○							
		⑶		例外措置の申請書の管理		○											
	７．５法令順守			主要な法令遵守											○		

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）					項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ監査統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
［7］	７．６懲戒処分等	⑴			懲戒処分			○	○	○	○	○	○			○		
		⑵	①		違反時の対応（統括情報セキュリティ責任者確認時）			○		△								
			②		違反時の対応（情報システム管理者確認時）			△		△	○							
			③		違反を改善しない職員等のシステム使用の権利の停止等		△	○		△								
８業務委託と外部サービスの利用	８．１業務委託	⑴	①		委託事業者の選定時の確認事項					○								○
			②		国際規格の認証取得状況等を参考にした事業者の選定					○								○
		⑵			契約項目													○
		⑶			委託事業者のセキュリティ確保の確認・措置等		△	△		○								○
	８．２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）	⑴	①		外部サービスを利用可能な範囲の規定			○										
			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			○										
		⑵	①		外部サービスの利用の検討				○									
			②	ア	外部サービスで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る二本松市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に関する情報提供及び調達仕様書による施設の場所やリージョンの指定				○									
				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				○									
			③		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				○									
			④	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				○									
			⑤		外部サービスの利用を通じて取り扱う情報に対する国内法以外の法令及び規制が適用されるリスクの評価				○									
			⑥		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の対策				○									
			⑦		取り扱う情報の格付及び取扱制限に応じたセキュリティ要件と外部サービスの選定				○									
			⑧		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要件				○									
			⑨		情報セキュリティ監査報告書による外部サービス提供者の評価			○										
		⑶	①		外部サービスの調達時の調達仕様に含める事項				○									
			②		外部サービスを調達する場合の契約までの確認事項と契約内容				○									
		⑷	①		外部サービスを利用する場合の利用申請				○									
			②		職員等による外部サービスの利用申請の審査									○				
			③		外部サービスの利用承認時の記録と外部サービス管理者の指名									○				
		⑸	①	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			○										
			②		前項において定める規定内容の確認・記録			○							○			
		⑹	①	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			○										
			②		外部サービスで発生したインシデントの対処手順の整備				○									
			③		外部サービス運用・保守時の確認・記録										○			
		⑺	①	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		外部サービス利用終了時の確認・記録										○			

付録２

権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

※「８　業務委託と外部サービスの利用」に係る利用申請にあたっては、人事行政課電子情報係合議とすること。

区分（対策基準の規定箇所）				項目	情報セキュリティ委員会（本部会議）	最高情報セキュリティ責任者（副市長）	統括情報セキュリティ責任者（総務部長）	情報セキュリティ責任者（各部長等）	情報セキュリティ管理者（各課長等）	情報システム管理者（各システム担当課長等）	情報システム担当者（各システム担当者）	情報セキュリティ監査統括責任者（指名）	利用申請の許可権限者（総務部長）	外部サービス管理者	職員等の義務	（統一的窓口）ＣＳＩＲＴ	関係規定外部委託
［８］	８．３ 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）	⑴	①	外部サービスを利用可能な業務の範囲			○										
			②	外部サービスの利用申請の許可権限者と利用手続			○										
			③	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			○										
			④	外部サービスの利用の運用手順			○										
		⑵	①	機密性２以上の情報を取り扱わない場合の利用申請と措置										○	○		
			②	外部サービスの利用申請審査とその記録				許							○		
９ 評価・見直し	９．１ 監査	⑴		情報セキュリティ対策状況について監査の実施	○							△					
		⑵	①	被監査部門から独立した者への監査の実施依頼								○					
			②	監査を行う者の要件													
		⑶	①	監査実施計画の立案等	承							○					
			②	監査の実施に対する協力													
		⑷		委託事業者に対する監査								○					○
		⑸		監査結果の報告	△							○					
		⑹		監査証拠等の保管								○					
		⑺		監査結果への対応		○	△		△								
		⑻		監査結果の情報セキュリティポリシー及び関係規程等の見直し等への活用	○												
	９．２ 自己点検	⑴	①	ネットワーク等の自己点検の実施			○			○							
			②	情報セキュリティ対策状況の自己点検				○	○								
		⑵		点検結果と改善策の報告	△		○	○		○							
		⑶	①	自己の権限の範囲内での改善											○		
			②	点検結果の情報セキュリティポリシー及び関係規程等の見直し等への活用	○												
	９．３ 情報セキュリティポリシー及び関係規程等の見直し			情報セキュリティポリシー及び関係規程等の見直しに関する規定	○												

付録３

情報資産の種類と例

情報資産の種類	情報資産の例
①　ネットワーク	通信回線、ルータ等の通信機器等
②　情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
③　①・②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、通信ケーブル等
④　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蔵電磁的記録媒体、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等
⑤　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等（これらを印刷した文書を含む。）
⑥　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

付録４

情報の機密性に応じた機器の廃棄等の方法

分類	機器の廃棄等の方法	確実な履行を担保する方法
⑴　マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※　マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述⑶で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
⑵　機密性２以上に該当する情報を保存する記憶媒体（上記⑴に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③ＯＳ等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述⑶で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
⑶　機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、⑵に記述した方法①～⑤のほか、ＯＳ等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。ＯＳの初期化、および記憶装置の初期化（フォーマット等）による方法は、ＨＤＤの記憶演算子にはデータの記憶が残った状態となるため、適当ではない。	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。

付録５

用語の定義

【あ】

●「遠隔消去機能」

「遠隔消去機能」→「リモートワイプ機能」を参照。

●「暗号化消去」

「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の複合に用いる鍵を抹消することで情報の複合を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の Bitlocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrvpting Drive）等）などがある。

●「Ｗｅｂ（ウェブ）会議サービス」

「Ｗｅｂ（ウェブ）会議サービス」とは、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、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

【か】

●「外部サービス」

「外部サービス」とは、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。

●「外部サービス管理者」

「外部サービス管理者」とは、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者をいう。

●「外部サービス提供者」

「外部サービス提供者」とは、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。

●「外部サービス利用者」

「外部サービス利用者」とは、外部サービスを利用する自組織の職員等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。

●「業務継続計画」

「業務継続計画」。「事業継続計画」と同じ。→「ＢＣＰ」を参照。

●「クラウドサービス」

「クラウドサービス」とは、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。この構成要素として、ＳａａＳ（Software as a Service)、ＰａａＳ（Platform as a Service)、ＩａａＳ（Infrastructure as a Service）が存在する。

●「ゲートウェイ」

「ゲートウェイ」とは、ＬＡＮと外のネットワークなど、２つのネットワークを接続して、相互に通信するために必要となる機器、もしくはシステムをいう。

【さ】

●「情報セキュリティインシデント」

「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

●「ソーシャルメディアサービス」

「ソーシャルメディアサービス」とは、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などを含む。

【た】

●「多要素認証」

「多要素認証」とは、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。

●「端末」

「端末」とは、情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、二本松市が調達又は開発するものをいう。

●庁内ネットワーク

「庁内ネットワーク」とは、庁舎・出先機関を含めた二本松市が管理主体となるネットワーク及び同ネットワークを委託しているデータセンターに設置している情報システムをいう。

●「電子署名」

「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

●「特権ＩＤ」

「特権ＩＤ」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常のＩＤよりもシステムに対するより高いレベルでの操作が可能なＩＤをいう。

【は】

●「パソコン」

「パソコン」とは、端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

●「標的型攻撃」

「標的型攻撃」とは、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。

【ま】

●「モバイル端末」

「モバイル端末」とは、端末のうち、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。

【ら】

●「リスク分析」

「リスク分析」とは、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、他者とのリスクの共有、リスクの保有などがある。

●「リモートワイプ機能」

「リモートワイプ機能」とは、携帯電話などに記録してあるデータを、当該端末から操作するのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失したり盗難にあった場合の、情報漏えいを防ぐ目的で利用される。

【Ａ～Ｚ】

●「ＢＣＰ（Business Continuity Plan：事業継続計画）」

「ＢＣＰ」とは、組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適正に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。

●「ＣＳＩＲＴ（Computer Security Incident Response Team）」

「ＣＳＩＲＴ」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う組織の総称。

●「ＬＧＷＡＮ－ＡＳＰ（Local Government Wide Area Network - Application Service Provider）」

「ＬＧＷＡＮ－ＡＳＰ」とは、府省、地方公共団体、公益法人、民間企業等がＡＳＰ（ｱﾌﾟﾘｹｰｼｮﾝ・ｻｰﾋﾞｽ・ﾌﾟﾛﾊﾞｲﾀﾞ）として、インターネットから総合行政ネットワーク（ＬＧＷＡＮ）を通じて、サービス利用者である地方公共団体に各種行政事務サービスを提供するものである。

●「ＳＬＡ（Service Level Agreement）」

「ＳＬＡ」とは、サービス提供者と利用者との間でサービス内容に関し明示的になされた合意であり、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、サービス提供者に保証させることをいう。

●「ＶＰＮ（Virtual Private Network）」

「ＶＰＮ」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術である。