仙 台 市 行 政 情 報
セキュリティポリシー

仙　台　市

令和 3 年 3 月 24 日　実施

令和 3 年 3 月 24 日　改正

改　正　履　歴

改正年月日	改正内容	制定・実施年月日
平成 14 年 8 月 1 日	仙台市行政情報セキュリティポリシーの制定	制定：平成 14 年 8 月 1 日（市長決裁）
平成 18 年 10 月 4 日	仙台市行政情報セキュリティポリシーの一部改正 ①　情報セキュリティ管理体制の強化 ②　定期的な評価・見直しについて規定 ③　情報資産について分類・管理の変更 ④　その他文書整理	実施：平成 18 年 11 月 1 日（市長決裁）
平成 19 年 4 月 1 日	仙台市行政情報セキュリティポリシーの一部改正 ①　組織改正に伴う定義の変更	実施：平成 19 年 4 月 1 日（総務局長決裁）
平成 23 年 10 月 21 日	仙台市行政情報セキュリティポリシーの一部改正 ①　監査結果に伴う内容の見直し ②　組織改正に伴う変更 ③　その他文書整理	実施:平成 23 年 10 月 21 日（市長決裁）
平成 24 年 4 月 1 日	仙台市行政情報セキュリティポリシーの一部改正 ①　組織改正に伴う定義の変更	実施：平成 24 年 4 月 1 日（総務企画局長決裁）
平成 26 年 3 月 24 日	仙台市行政情報セキュリティポリシーの一部改正 ①　組織改正に伴う変更	実施：平成 26 年 4 月 1 日（総務企画局長決裁）
平成 27 年 10 月 1 日	仙台市行政情報セキュリティポリシーの一部改正 ①　遵守法令を追加	実施：平成 27 年 10 月 5 日（まちづくり政策局長決裁）
平成 28 年 12 月 22 日	仙台市行政情報セキュリティポリシーの一部改正 ①　総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う内容の見直し ②　その他文書整理	実施：平成 29 年 1 月 1 日（市長決裁）
令和 2 年 3 月 31 日	仙台市行政情報セキュリティポリシーの一部改正 ①　総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う内容の見直し ②　その他文書整理	実施：令和 2 年 4 月 1 日（まちづくり政策局長決裁）
令和 3 年 3 月 24 日	仙台市行政情報セキュリティポリシーの一部改正 ①　総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う内容の見直し ②　テレワークとの整合性見直し ③　クラウドサービスの活用に向けた見直し	実施：令和 3 年 3 月 24 日（まちづくり政策局長決裁）

目次

序　仙台市行政情報セキュリティポリシーの構成

仙台市行政情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは，仙台市が保有する情報資産に関するセキュリティ対策について，総合的，体系的に取りまとめたものである。

情報セキュリティポリシーは，本市の情報資産を取り扱う全職員に浸透，定着させるものであり，安定的な規範であることが要請される。しかし一方では，情報セキュリティ対策は，情報の処理技術や通信技術等の進展に伴う急速な状況の変化に，柔軟に対応することも必要である。

このようなことから，情報セキュリティポリシーは，一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と，情報資産を取巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の 2 階層のものとして構成する。また，情報セキュリティポリシーに基づく具体的な手順を示す「情報セキュリティ実施手順」として全庁的に共通する情報資産の取扱いを定める実施手順と，管理する情報システム毎の取扱いを定める実施手順を策定するものとする。

仙台市行政情報セキュリティポリシーの構成

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，全ての情報資産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		全庁的に共通する情報資産の取扱いを定める実施手順と，管理する情報システム毎の取扱いを定める実施手順。

第１章　情報セキュリティ基本方針

（１）目的

本市が取り扱う情報資産には，市民の個人情報を始めとし行政運営上重要な情報など，部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれており，これらの情報資産を人的脅威や災害，事故等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も，また，継続的かつ安全，安定的な行政サービスの実施を確保するためにも必要不可欠である。

さらに，市民サービスの向上，業務効率化や合理化の要請に対応するために，本市における情報システムによる業務量及び利用範囲は拡大の一途をたどっており，今や行政運営基盤として欠かせないものとなっている。そのため，本市の業務執行を今後も円滑に進めるためには，本市が管理している全ての情報システムが高度な安全性を有することが不可欠である。

このため，本市の情報資産の機密性，完全性及び可用性（注）を維持するための対策を整備するため，情報セキュリティポリシーを定めることとし，情報セキュリティの確保に最大限取組むこととする。

このうち情報セキュリティ基本方針においては，本市の情報セキュリティ対策の基本的な方針として，情報セキュリティポリシーの対象，位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセス出来ることを確実にすること。

完全性（integrity）　：情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

可用性（availability）　：許可された利用者が必要なときに情報にアクセス出来ることを確実にすること。

（２）定義

① 局等

仙台市事務分掌条例（昭和 34 年仙台市条例第 20 号）第 1 条に掲げる局及び室，並びに区役所，会計室，教育委員会事務局，人事委員会事務局，監査事務局，農業委員会事務局，議会事務局，選挙管理委員会事務局，消防局及び各公営企業をいう。

② 事務所管課

その保有するデータの一部又は全部の電子計算機処理を行うことにより所管する事務を遂行する課(これに準ずるものを含む。以下同じ。)をいう。

③ 電子計算機

ハードウェア及びソフトウェアで構成するコンピュータをいう。また，電子計算機のうち，職員等が情報処理を行うために直接操作する機器を端末といい，そのうち，必要に応じて移動させて使用することを目的として導入したものをモバイル端末という。また，モバイル端末のうち，庁舎内と同様の汎用的業務を庁舎外で行うために使用するものをテレワーク端末という。

④ 記録媒体

電子計算機に使用される磁気ディスク，磁気テープ，光ディスク，フラッシュメモリその他これらに類する媒体をいう。また，記録媒体のうち，取り外し可能で持ち出しが可能なものを外部記録

媒体という。

⑤ 電子計算機室等

本市の電子計算機を運用管理する目的で設置している部屋をいう。

⑥ ネットワーク

電子計算機等を相互に接続するための通信回線及びその構成機器（ハードウェア及びソフトウェア）で構成され，情報処理を行う仕組みをいう。

⑦ 情報システム

電子計算機，ネットワーク及び周辺機器で構成され，情報処理を行う仕組みをいう。

情報システムが接続するネットワークは以下のものをいう。

（ｉ）個人番号利用事務系ネットワーク

・個人番号（マイナンバー）利用事務を取扱う情報システムが接続する共用ネットワーク及び当該情報システム専用のネットワークをいう。

（ⅱ）LGWAN 接続系ネットワーク

・LGWAN に接続する共用ネットワーク及び LGWAN に接続する情報システム専用のネットワークをいう。

（ⅲ）インターネット接続系ネットワーク

・インターネットにアクセス又はインターネットからのアクセスを許可する情報システムが接続するネットワークをいう。

（ⅳ）独立系ネットワーク

・上記の（ｉ）から（ⅲ）の要件に該当しない情報システムが接続する共用ネットワーク及び情報システム専用のネットワークをいう。

⑧ 行政情報

本市の行政事務の執行に関わる情報で，情報システムで取り扱うものをいう。（入出力帳票及び情報システム仕様書等を含む。）

ただし，行政情報を外部へ提供した場合や IC カード等に行政情報を記録したものを市民に交付する等により，当該情報の管理責任が本市から離れたものを除く。

⑨ 情報資産

本市の情報システム，外部記録媒体及び行政情報をいう。

⑩ 特定用途機器

テレビ会議システム，IP 電話システム，ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって，通信回線に接続されている，又は内蔵の記録媒体を備えているものをいう。

⑪ ロボティック・プロセス・オートメーション

ロボティック・プロセス・オートメーション（以下「RPA」という。）はこれまで人間が行ってきた定型的な処理等をソフトウェアのロボットにより自動化するものをいう。

⑫ 外部サービス

外部サービスとは，外部の事業者が提供するサービスの総称であり，以下のものをいう。

（ｉ）委託による外部サービス

・本市の業務を外部の事業者に委託することにより調達する外部サービスのことをいう。

（ⅱ）約款等による外部サービス

・無料有料を問わず，以下の形態により調達する外部サービスのことをいう。

(a) 約款への同意のみにより利用可能となる外部サービス

・事業者が定める約款への同意によって利用可能となるサービスのことをいう。

(b) 約款に特約等を付して調達する外部サービス

・事業者が定める約款に取扱う行政情報の保護に関する特約等を付加し，利用するサービスのことをいう。

(c) 国や LGWAN-ASP により提供される外部サービス

・国が提供するサービスのほか，地方公共団体情報システム機構（以下，J-LIS という。）等が LGWAN を通じて地方公共団体向けに提供するサービスのことをいう。

⑬ **クラウドサービス**

データやソフトウェアをネットワーク経由でサービスとして利用者に提供するものをいい，主に仮想化技術により実現されているものをいう。

⑭ **仮想化技術**

サーバなどのハードウェア資源（ＣＰＵ，メモリ，ディスクなど）を抽象化し，物理的な制限にとらわれず，ソフトウェア的に統合・分割できるようにする技術のことをいう。

⑮ **テレワーク**

情報通信技術(ICT = Information and Communication Technology)を活用した，勤務場所にとらわれない柔軟な働き方のことをいう。

⑯ **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。

⑰ **セキュリティ障害**

セキュリティ障害とは，本市の情報資産に対する脅威が実際に生じることにより，情報資産の機密性，完全性又は可用性が損なわれることであり，以下のものをいう。

（ｉ）情報システムの故障，停止
（ii）情報システムへの不正アクセス攻撃
（iii）情報システムの不正な利用
（iv）情報システムにおける入出力内容の誤り
（ｖ）情報資産の盗難
（vi）情報資産の紛失，滅失
（vii）行政情報の漏えい
（viii）行政情報の改ざん
（ix）行政情報の誤送付，誤送信
（ｘ）その他の障害

（３）情報セキュリティポリシーの位置付け

情報セキュリティポリシーは，本市の情報資産に関する情報セキュリティ対策について，総合的，体系的に取りまとめたものであり，情報セキュリティ対策の最高位に位置するものである。

（４）情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は，本市の局等における情報資産及び情報資産を扱うす

べての職員（非常勤嘱託職員，会計年度任用職員，臨時的任用職員，アルバイト及び再任用職員を含む。以下同じ。）とする。

（５）職員の義務

職員は，情報セキュリティの重要性について共通の認識を持つとともに，情報資産の利用にあたっては情報セキュリティポリシーを遵守しなければならない。

（６）管理体制

本市の情報資産に関する情報セキュリティ対策を推進，管理するための体制を確立するものとする。

（７）情報資産の分類

情報資産をその重要度に応じて分類し，それに応じたセキュリティ対策を行うものとする。

（８）情報資産への脅威

情報セキュリティ対策を講ずるうえで，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に以下の脅威については十分な措置を講ずるものとする。

① 故意の不正アクセス又は不正操作によるデータやプログラムの持出，盗聴，改ざん，消去並びに機器及び外部記録媒体の盗難等

② 職員及び外部委託者による意図しない操作及び規定外の情報システムの機器操作によるデータ漏えい等

③ 地震，落雷並びに火災等の災害や事故，故障等

（９）情報セキュリティ対策

本市の情報資産を上記（８）の脅威から保護するため，以下の情報セキュリティ対策を講ずるものとする。

① 人的セキュリティ対策

情報資産に接する職員の情報セキュリティに関する権限や責任等を定めるとともに，すべての職員に情報セキュリティポリシーの内容を周知徹底するため，教育及び訓練を行う。

② 物理的セキュリティ対策

電子計算機，通信回線，外部記録媒体等の管理及び電子計算機室等の入退室管理について，物理的な対策を講じる。

③ 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため，情報資産へのアクセス制御，コンピュータウイルス対策等を実施する。

④ 運用

情報セキュリティポリシーの実効性を確保するため，また，不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため，ネットワークの監視等の運用面における必要な措置を講ずる。

また，セキュリティ障害が発生した際の迅速な対応と行政事務の円滑な執行を可能とするため，必要な措置を講ずるものとする。

（10）情報セキュリティ対策基準の策定

情報セキュリティ基本方針を実行に移すため，情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

（11）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。情報セキュリティ実施手順は，本市全体として遵守すべき事項を規定したものと，重要な情報システムの適切な運用に関する事項を規定したものを策定する。

なお，情報セキュリティ実施手順は，公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

（12）評価・見直し

① 監査及び自主点検の実施

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主点検を実施する。

② 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主点検の結果，情報セキュリティポリシーの見直しが必要に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。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは，情報セキュリティ基本方針を実行に移すための，本市の情報資産に関する情報セキュリティ対策の基準である。

（１）管理体制

情報セキュリティの管理体制は下記のとおりとする。

① 最高情報セキュリティ責任者

本市の情報資産に関する情報セキュリティを統括する最高責任者として最高情報セキュリティ責任者（CISO：Chief Information Security Officer，以下「CISO」という。）を置き，まちづくり政策局長をもってこれに充てる。

② 局（区）情報管理者

局等の情報セキュリティに関する適正な運用及び管理を監理するため，局等に総括的な権限及び責任を有する局（区）情報管理者を置き，局等の長をもってこれに充てる。

③ 情報管理者

情報セキュリティの適正な運用及び管理を行うため，情報資産を取り扱う課（これに準ずるものを含む。以下同じ。）に情報セキュリティに関する権限及び責任を有する情報管理者を置き，当該課の長をもってこれに充てる。

④ システム管理者

情報管理者のうち，重要な情報システムの情報セキュリティを維持し，情報システムの適正な管理並びに効率的な運用を図るため，システム管理者を置き，重要な情報システムに係る業務を所管する課の長をもってこれに充てる。

⑤ ネットワーク管理者

情報システム課で運用する情報システムのネットワークの情報セキュリティを維持し，効率的な運用を図るためネットワーク管理者を置き，情報システム課長をもってこれに充てる。

⑥ 副情報管理者

情報セキュリティの適正な運用及び管理に関して情報管理者の補佐を行うため，情報資産を取り扱う課に副情報管理者を置き，原則として，当該課の係長職の職員の中から情報管理者が指名する。

⑦ システム担当者

重要な情報システムにおける情報セキュリティの維持に関してシステム管理者の補佐を行うため，重要な情報システムに係る業務を所管する課にシステム担当者を置き，当該課の職員の中からシステム管理者が指名する。

⑧ CSIRT 責任者

本市のセキュリティ障害等に対応する組織（CSIRT：Computer Security Incident Response Team，以下「CSIRT」という。）の責任者として CSIRT 責任者を置き，まちづくり政策局情報管理課長をもってこれに充てる。

⑨ CSIRT 管理者

セキュリティ障害の発生連絡等のために，CSIRT 管理者を置き，局等の主管課長をもってこれに充てる。

⑩ CSIRT 担当者

CSIRT 担当者は，まちづくり政策局情報管理課セキュリティ対策係をもってこれに充てる。

（２）権限，役割及び責任

情報セキュリティの権限，役割及び責任は下記のとおりとする。

① CISO

・CISO は，情報セキュリティに関して局（区）情報管理者及び情報管理者に対して，必要な指示及び助言を行う。

・CISO は，CSIRT をまちづくり政策局情報管理課に設置し，その役割を明確にしなければならない。

・CISO は，全庁的に共通する情報資産の取扱いを定める情報セキュリティ実施手順（以下「共通実施手順」という。）を策定しなければならない。

・CISO は，まちづくり政策局の局（区）情報管理者の役割を兼ねる。

② 局（区）情報管理者

・局（区）情報管理者は，情報セキュリティに関し情報管理者に対して，必要な指示及び助言を行う。

・局（区）情報管理者は，所掌する局等に設置している情報システムで事務所管課を横断する情報システムの開発，設定の変更，運用及び更新等，当該システムに関する情報セキュリティ実施手順の策定，維持及び管理等の承認を行う。

・局（区）情報管理者は，所管する局等における情報セキュリティポリシーの遵守に関し，職員に対し教育，訓練，助言及び指示を行わなければならない。

③ 情報管理者

・情報管理者は，使用する情報システムの機器や記録媒体について，第三者に使用させること，又は許可なく情報を閲覧させることがないように，適切な措置を施さなければならない。

・情報管理者は，非常勤嘱託職員，会計年度任用職員，臨時的任用職員及びアルバイトを雇用する場合に，必ず情報セキュリティポリシーのうち，職員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。

・情報管理者は，所管する情報システムの開発，設定の変更，運用，更新等を行う権限及び責任を有する。

・情報管理者は，情報セキュリティに関する適正な運用及び管理を補佐する副情報管理者を１名以上指名し，情報管理者不在時における緊急時などの対応をあらかじめ定めておかなければならない。

・情報管理者は，所管する三種公所の長を副情報管理者に指名しなければならない。

④ システム管理者

・システム管理者は，重要な情報システムの開発，設定の変更，運用，更新等を行う権限及び責任を有する。

・システム管理者は，重要な情報システムに係る情報セキュリティ実施手順の策定，維持，管理等を行うとともに，当該情報システムが事務所管課を横断する場合は，当該実施手順について局（区）情報管理者の承認を得なければならない。また，定められている事項について職員に実施及び遵守させなければならない。

・システム管理者は，職員に対して必要な知識や技能を習得させる研修を受けさせなければならない。

⑤ **ネットワーク管理者**

・ネットワーク管理者は，情報システム課で運用する情報システムのネットワークについて，設定の変更，運用，更新等を行う権限及び責任を有する。

・ネットワーク管理者は，必要に応じシステム管理者の支援を行うものとする。

・ネットワーク管理者は，情報システム課における情報管理者及び所管する重要な情報システムに係るシステム管理者の役割を兼ねる。

⑥ **副情報管理者**

・副情報管理者は，情報管理者に情報セキュリティに必要な情報を提供するとともに，その指示により課内の情報セキュリティ対策を推進する。

・副情報管理者は，情報管理者不在の場合は，情報管理者に代わり，あらかじめ定めてある緊急時の対応等を行わなければならない。

⑦ **システム担当者**

・システム担当者は，システム管理者に重要な情報システムの運用，管理等に必要な情報を提供するとともに，その指示によりシステムの開発，設定の変更，運用，更新等を行う。

・システム担当者は，システム管理者不在の場合は，システム管理者に代わり，あらかじめ定めてある緊急時の対応等を行わなければならない。

⑧ **CSIRT 責任者**

・CSIRT 責任者は，セキュリティ障害の発生について局等より報告を受けた場合には，その状況を確認し，セキュリティ障害対応に必要な報告等が行われる体制の整備を行う。

・本市における情報セキュリティに関する施策等の内容を関係部局等に提供する。

・セキュリティ障害の発生を認めた場合には，必要に応じて，CISO，国，都道府県等へ報告する。

・情報セキュリティに関して，必要に応じて，国及び関係団体，民間事業者等との情報共有を行う。

⑨ **CSIRT 管理者**

・CSIRT 管理者は，セキュリティ障害の発生についてシステム管理者又は情報管理者より報告を受けた場合には，その状況を確認し，CSIRT 責任者に報告する。

⑩ **CSIRT 担当者**

・CSIRT 担当者は，CSIRT 責任者に情報セキュリティに必要な情報を提供するとともに，その指示により本市の情報セキュリティ対策を推進する。

（３）情報資産の分類と管理

① 行政情報の分類

情報管理者は，行政情報を脅威から保護するために，対象となるすべての行政情報を，重要度の高いものから重要性分類Ｓ，Ⅰ，Ⅱ及びⅢとし，以下の要件に従って分類する。

（ｉ）重要性分類Ⅰ

・仙台市情報公開条例（平成 12 年仙台市条例第 80 号）第 7 条第 1 号から第 4 号に定義されている非開示情報。

・情報システムの運用管理に関する情報で，情報セキュリティを維持するため，機密の取扱いを要する情報。

・上記に掲げる場合のほか，情報管理者が，情報の機密性，完全性及び可用性その他の事情を考慮して，重要性分類Ⅰとして管理することが適当と認める行政情報。

（ⅱ）**重要性分類Ｓ**

重要性分類Ⅰに分類される行政情報のうち，滅失又はき損した場合，復元が著しく困難となり，行政の円滑な執行に重大な支障をきたすおそれのある行政情報。

（ⅲ）**重要性分類Ⅱ**

・仙台市情報公開条例第 7 条第 5 号及び第 6 号に定義されている非開示情報。

・上記に掲げる場合のほか，情報管理者が，情報の機密性，完全性及び可用性その他の事情を考慮して，重要性分類Ⅱとして管理することが適当と認める行政情報。

（ⅳ）**重要性分類Ⅲ**

重要性分類Ｓ，Ⅰ及びⅡ以外の行政情報。

② **情報システムの分類**

情報管理者は，情報システムを脅威から保護するために，所管する情報システムのうち，以下のいずれかに該当する情報システムを重要な情報システムに分類する。

・複数の課公所で業務に利用されている情報システム。

・重要性分類Ｓの行政情報を取扱っている情報システム。

・セキュリティ障害により一日以上情報システムの通常運用が不可能になった場合に，行政の円滑な執行や組織の運営に重大な支障をきたすおそれのある情報システム。

・上記に掲げるもののほか，情報管理者が，情報システムの情報の機密性，完全性及び可用性その他の事情を考慮して，重要な情報システムとして管理することが適当と認める情報システム。

③ **情報システムが接続するネットワークの分類**

情報管理者及びシステム管理者は，情報システムを脅威から保護するために，所管する情報システムが接続するネットワークを，以下の要件に従って分類する。

（ｉ）**個人番号利用事務系ネットワーク**

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）を取扱う情報システムが接続する共用ネットワーク及び当該情報システム専用のネットワークは，個人番号利用事務系ネットワークに分類する。

（ⅱ）**LGWAN 接続系ネットワーク**

LGWAN にアクセスする情報システムが接続する共用ネットワーク及び当該情報システム専用のネットワークは，LGWAN 接続系ネットワークに分類する。

（ⅲ）**インターネット接続系ネットワーク**

インターネットにアクセス又はインターネットからのアクセスを許可する情報システムが接続するネットワークは，インターネット接続系ネットワークに分類する。ただし，インターネットを利用した仮想専用線は，インターネット接続系には含めないものとする。

（ⅳ）**独立系ネットワーク**

上記の（ｉ）から（ⅲ）の要件に該当しない情報システムが接続する共用ネットワーク及び当該情報システム専用のネットワークは，独立系ネットワークに分類する。

④ **行政情報の管理方法**

（ｉ）**行政情報の管理及び取扱い**

・情報管理者は，パスワード等によるアクセス制限を適切に行わなければならない。

・情報管理者は，重要性分類Ｓ，Ⅰ及びⅡの行政情報について，原則として，台帳を作成して管理しなければならない。
・職員は，業務目的以外に行政情報を利用してはならない。
・職員は，行政情報の不用意な複製，送付及び送信を行ってはならない。
・職員は，業務上必要な場合は，情報管理者の許可を得た上で行政情報の送付及び送信を行わなければならない。
・職員は，インターネットに接続するモバイル端末に，原則として重要性分類Ｓ，Ⅰ及びⅡの行政情報の記録を行ってはならない。また，インターネットに接続しないモバイル端末であっても，重要性分類Ｓ，Ⅰ及びⅡの行政情報の記録は必要最小限としなければならない。
・職員は，行政情報を執務室外へ持ち出す場合は，情報管理者の許可を得なくてはならない。
・職員は，行政情報を持ち出す場合は，適切な保護対策を講じなければならない。
・職員は，行政情報を情報管理者の許可なく部外者へ提供してはならない。
・職員は，離席する場合及び退庁する場合は，行政情報を記録した電子計算機，情報システム及び行政情報を印刷した書類を容易に使用又は閲覧できる状態で放置してはならない。
・職員は，記録した情報の消去が可能な記録媒体に記録した行政情報について，保存しておく必要がなくなった場合は速やかに，当該行政情報を消去しなければならない。

（ｉ）－２　テレワーク端末における行政情報の管理及び取扱いに関する特則

・職員は，テレワーク端末において行政情報を取扱う場合は，（ｉ）の定めのほか，CISO 及びネットワーク管理者が定める実施手順を遵守しなければならない。

（ⅱ）外部記録媒体及びモバイル端末の管理

・外部記録媒体及びモバイル端末は，未使用のものも含め，行政情報の無断持ち出しや漏えいを防止するため，施錠可能な安全な場所に保管する等適切に管理するとともに，その状況等を記録しなければならない。
・行政情報を記録した外部記録媒体及びモバイル端末を送る場合は，物理的な保護措置を講じなければならない。また，重要性分類Ｓ，Ⅰ及びⅡの行政情報を記録した外部記録媒体の送付を外部業者に委託する場合は守秘義務を明記した契約を締結しなければならない。
・職員は，離席する場合及び退庁する場合は，外部記録媒体及びモバイル端末を容易に使用又は閲覧できる状態で放置してはならない。
・外部記録媒体及びモバイル端末を保管する場合は，行政情報を消去した状態であっても，記録する行政情報の重要性分類に応じた管理をしなければならない。

（ⅱ）－２　テレワーク端末の管理に関する特則

・テレワーク端末の管理については，（ⅱ）の定めのほか，CISO 及びネットワーク管理者が定める実施手順を遵守しなければならない。

（ⅲ）行政情報のバックアップ

・情報管理者は，重要性分類Ｓの行政情報について，外部記録媒体等へのバックアップを取り，施錠等の出来る安全な場所へ保管しなければならない。また，保管状況等を記録しなければならない。
・情報管理者は，重要性分類Ⅰ及びⅡの行政情報について，必要に応じバックアップを取り，行政情報の管理に努めなければならない。

（ⅳ）行政情報を記録した記録媒体の廃棄

・重要性分類Ｓ，Ⅰ及びⅡの行政情報を記録した記録媒体を廃棄する場合は，当該媒体に記録されている行政情報をいかなる方法によっても復元できないように消去を行うか，消去できないものにあっては物理的破壊を行った上で廃棄しなければならない。

・行政情報を記録した記録媒体の廃棄にあたり，当該行政情報の消去を外部業者に行わせる場合は，守秘義務を明記した契約を締結しなければならない。

・重要性分類Ｓ，Ⅰ及びⅡの行政情報を記録した記録媒体を廃棄する場合は，情報管理者の許可を得ることとし，廃棄を行った日時，担当者及び処理内容を記録しなければならない。

・廃棄する記録媒体は，廃棄されるまでの間，記録されている行政情報の重要度に応じた管理をしなければならない。

（ｖ）ウェブページ等における行政情報の取扱い

・情報管理者は，ウェブページ等により外部へ行政情報を発信する場合，その内容について正確かつ適切なものとするとともに，不正アクセス等により行政情報が改ざんされないよう対策を講じなければならない。

（vi）約款への同意のみにより利用可能となる外部サービスの利用における行政情報の取扱い

・職員は，第１章（２）⑫（ⅱ）(a)に規定するサービスを利用する場合には，重要性分類Ｓ，Ⅰ及びⅡの行政情報の保存，送信等を原則行ってはならない。

・職員は，重要性分類Ⅲの行政情報の保存，送信等に当該サービスを利用する場合には，利用するサービスの約款，その他提供条件から，利用に当たってのリスクが許容出来ることを確認し，情報管理者の許可を得た上で約款による外部サービスの利用を申請しなければならない。

・職員は，適切な措置を講じた上で，当該サービスを利用しなければならない。

（vii）約款に特約等を付して調達する外部サービスの利用における行政情報の取扱い

・情報管理者は，第１章（２）⑫（ⅱ）(b)に規定する外部サービスを利用する場合には，取り扱う情報資産の重要性分類及びその分類に応じた取扱制限を踏まえ，当該サービスの利用可否を判断しなければならない。

（viii）国や LGWAN－ASP により提供される外部サービスにおける行政情報の取扱い

・職員は，第１章（２）⑫（ⅱ）(c)に規定する外部サービスを利用する場合には，当該システム等の利用目的に即した重要性分類の行政情報の保存，送信等を行うことが出来る。

（ix）クラウドサービスの利用に関する特則

・情報管理者は，第１章（２）⑬に規定するクラウドサービスを利用する場合には，あらかじめ CISO が定める基準を満たしていることを確認しなければならない。

⑤ 情報システムの管理方法

情報管理者及びシステム管理者は，本章（６）物理的セキュリティ及び（７）技術的セキュリティに基づき情報システムを管理しなければならない。

⑥ 情報システムが接続するネットワークの管理方法

ネットワーク管理者及び情報システムが接続するネットワークを所管する情報管理者及びシステム管理者は，ネットワーク毎の要件に基づいた対策を行い，適切に管理しなければならない。

（ｉ）個人番号利用事務系ネットワーク

個人番号利用事務系ネットワークは，以下の対策を行わなければならない。

ア　個人番号利用事務系ネットワークと他のネットワークとの分離

・個人番号利用事務系ネットワークは，原則として，外部ネットワークとの接続又は通信を

行ってはならない。ただし，セキュリティ確保等のため，やむを得ず個人番号利用事務系ネットワークと他のネットワークとの接続又は通信を行う必要がある場合は，安全が確認された通信対象に限定した上で，セキュリティ障害が生じないよう，フィルタリング及びルーティング等の必要な対策を講じなければならない。

イ　情報へのアクセス及び持ち出しにおける対策

・個人番号利用事務系ネットワークに接続する情報システムは，複数要素による利用者認証の導入や端末からの行政情報の持ち出し制限等により，情報漏えい対策を実施しなければならない。

ウ　コンピュータウイルス対策

・複数の情報システムが接続する個人番号利用事務系ネットワークは，ネットワーク全体として均質なウイルス対策を講じなければならない。

（ⅱ）LGWAN 接続系ネットワーク

LGWAN 接続系ネットワークは，以下の対策を行わなければならない。

ア　LGWAN 接続系とインターネット接続系ネットワークとの分離

・LGWAN 接続系ネットワークは，原則として，インターネット接続系ネットワークとの接続又は通信を行えないようにしなければならない。ただし，セキュリティ確保等のため，やむを得ず LGWAN 接続系ネットワークとインターネット接続系ネットワークとの接続又は通信を行う必要がある場合は，安全が確認された通信対象に限定した上で，セキュリティ障害が生じないよう，フィルタリング及びルーティング等の必要な対策を講じなければならない。

イ　コンピュータウイルス対策

・複数の情報システムが接続する LGWAN 接続系ネットワークは，ネットワーク全体として均質なウイルス対策を講じなければならない。

（ⅲ）インターネット接続系ネットワーク

インターネット接続系ネットワークは，以下の対策を行わなければならない。

ア　情報セキュリティクラウドへの参加

・インターネット接続系ネットワークは，市区町村のインターネット接続口を集約する宮城県自治体情報セキュリティクラウドに参加し，国及び関係団体，民間事業者等と連携しながら，情報セキュリティ対策を推進しなければならない。

イ　独自にインターネット接続を行うネットワークにおける対策

・宮城県自治体情報セキュリティクラウドに参加しないインターネット接続系ネットワークは，セキュリティ障害の検知と対応及び不正アクセスの監視等の対策を講じなければならない。

（ⅳ）独立系ネットワーク

独立系ネットワークは，接続する情報システムの機密性，完全性，可用性を確保するために必要な対策を講じなければならない。また，複数の情報システムが接続する独立系ネットワークは，ネットワーク全体として均質なウイルス対策を講じなければならない。

（４）人的セキュリティ

① 職員の遵守事項

・職員は，情報セキュリティポリシー及び情報セキュリティ実施手順（共通実施手順及び情報システム毎の実施手順。以下同じ。）に定めている事項を遵守しなければならない。

・職員は，情報セキュリティポリシー及び情報セキュリティ実施手順について不明な点，遵守することが困難な点がある場合には，直ちに情報管理者に相談し，指示を仰がなければならない。

・職員は，情報管理者の指示等に従い，情報システムの開発，設定の変更，運用及び更新等の作業を行わなければならない。

・職員は，パソコン等の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システム管理者（システム管理者を置かない情報システムにおいては情報管理者）の許可なく変更してはならない。

・職員は，情報管理者の許可なく情報システムの機器を執務室外に持ち出してはならない。

・情報管理者は，情報システムの機器の執務室外への持ち出しを許可した場合は，記録を作成し，保管しなければならない。

・職員は，テレワーク端末を庁舎外で使用する場合，CISO 及びネットワーク管理者が定める実施手順を遵守しなければならない。

・職員は，個人で所有する電子計算機及び記録媒体に行政情報を記録してはならない。

・職員は，個人で所有する電子計算機，外部記録媒体及び電子機器等と，本市の電子計算機，ネットワーク及び外部記録媒体等を接続してはならない。

・職員は，本市の保有する行政情報を漏らしてはならない。その職を退いた後も同様とする。

・職員は，ネットワークを通じて会議等に参加をする場合は，状況に応じて必要な情報漏洩対策を行わなければならない。

② 外部サービスに関する管理

（ｉ）委託による外部サービス

システム管理者及び情報管理者は，第１章（２）⑫（ｉ）に規定するサービスを利用する場合には，守秘義務等，情報セキュリティポリシーのうち外部委託業者が守るべき内容の遵守を明記した契約を締結し，その遵守状況を管理しなければならない。

（ⅱ）約款への同意のみにより利用可能な外部サービス

システム管理者及び情報管理者は，第１章（２）⑫（ⅱ）(a)に規定するサービスを利用する場合には，外部サービスを提供する事業者より提示される使用条件等に基づき利用契約の締結を行うとともに，必要に応じてその遵守状況について報告を求めなければならない。

（ⅲ）約款等による外部サービス

システム管理者及び情報管理者は，第１章（２）⑫（ⅱ）(b)に規定するサービスを利用する場合には，守秘義務等，情報セキュリティポリシーのうち当該サービスを提供する事業者が守るべき内容の遵守を明記した利用契約の締結，又は同意書や覚書等の取り交わしを行い，その遵守状況を管理しなければならない。

（ⅳ）国や LGWAN-ASP により提供されるサービス

システム管理者及び情報管理者は，第１章（２）⑫（ⅱ）(c)に規定するサービスを利用する場合には，国や J-LIS 又は LGWAN を通じて当該サービスを提供する事業者より提示される使用条件等に基づき利用契約の締結，又は同意書や覚書等の取り交わしを行うとともに，必要に応じてその遵守状況について報告を求めなければならない。

③ **パスワードの管理**

職員は，自己の保有するパスワードについて，不用意にもらしたり他者に知られることのないよう適切に管理しなければならない。

・パスワードは，原則として職員等の間で共有してはならない。ただし，共有 ID 等で使用するパスワードを除く。

・共有 ID 等で使用するパスワードは，人事異動等によりパスワードの機密性が低下した場合は，変更等を行わなければならない。

④ **ID カードの管理**

・職員は，情報システムの認証等に用いるため個別に貸与されている ID カードを，職員間で共有してはならない。

・職員は，業務上必要のないときは，ID カードをカードリーダもしくは端末のスロット等から抜いておかなければならない。

・職員は，ID カードを紛失した場合には，速やかにシステム管理者及び情報管理者に通報し，指示に従わなければならない。

・システム管理者及び情報管理者は，ID カードの紛失の通報があり次第，当該 ID カード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。

・システム管理者及び情報管理者は，利用しなくなった ID 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うえで廃棄しなければならない。

⑤ **アクセスの制限**

・職員は，重要な情報システムへの接続については，必要最小限の接続時間で行うように努めるものとする。

・職員は，業務目的外の行政情報にアクセスしてはならない。

（５）セキュリティ教育，訓練

① **研修の受講**

・CISO は，情報セキュリティポリシーについて啓発に努めるとともに，職責に応じた情報セキュリティに関する研修を定期的に実施しなければならない。

・局（区）情報管理者は，局（区）情報管理者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受講しなければならない。

・情報管理者は，情報管理者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受講しなければならない。

・副情報管理者は，情報管理者を補佐する者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受講しなければならない。

・職員は，情報セキュリティポリシーに関する研修を受講し，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理解し，情報セキュリティ上の問題が生じないようにしなければならない。

・情報システムの開発，保守及び運用管理等に携わる職員は，担当者として必要な知識や技能を習得及び維持するための研修を受講しなければならない。

② **セキュリティ障害時等の緊急時の訓練**

システム管理者は，重要な情報システムの運用に支障を来さない範囲において，緊急時の対応を

想定した訓練等を実施しなければならない。

（６）物理的セキュリティ

① 入退室の管理

情報管理者は，重要性分類Ｓ及びＩの行政情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所への入退室の管理について必要な措置を講じなければならない。

② 電子計算機室等の管理

システム管理者及び情報管理者は，電子計算機室等においては，電子計算機や記録媒体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。

③ 機器の管理

・職員は執務室に職員が不在となる場合には，施錠するなど部外者の侵入を防ぐ措置を講じなければならない。

・情報管理者は，情報システムの機器等に盗難防止用ワイヤーの設置等の盗難防止対策を必要に応じて施すものとする。

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

④ 機器等の搬入及び搬出

情報管理者は，機器等の搬入及び搬出の場合に，職員が立ち会う等の必要な措置を講じなければならない。

⑤ 電源

情報管理者は，停電及び電圧異常等によりデータ等が破壊され，業務処理に支障を来すおそれのある情報システム等の機器の電源を，当該機器を適切に停止するまでの間に必要な電力を供給する容量の予備電源を備え付ける等の措置を講じなければならない。

⑥ 配線

・情報管理者は，配線については，傍受又は損傷等を受けることがないよう可能な限り必要な措置を施さなければならない。

・情報管理者は，主要な箇所の配線については，損傷等についての定期的な点検を行わなければならない。

（７）技術的セキュリティ

① 情報システムの管理

（ｉ）台帳の作成と管理

システム管理者及び情報管理者は，所管する情報システムについて，原則として，台帳を作成して管理しなければならない。

（ii）情報システムの管理記録の作成と管理

システム管理者は，担当する重要な情報システムにおけるシステムの変更作業を記録し，適切に管理しなければならない。

（iii）情報システム仕様書の管理

・システム管理者は，重要な情報システムの仕様書を最新の状態にしなければならない。また，

システムの仕様変更等をした場合は，その記録を作成しなければならない。

・システム管理者は，重要な情報システムの仕様書を業務上必要とする者のみが閲覧出来る場所に保管しなければならない。

（ⅳ）アクセス記録の取得

・システム管理者は，アクセス記録及びセキュリティ障害に関する記録（以下「障害記録」という。）を取得し，一定の期間保存しなければならない。

・システム管理者は，アクセス記録として取得する項目，保存期間，取扱方法及びアクセス記録が取得できなくなった場合の対処等について定め，適切に管理しなければならない。

・システム管理者は，アクセス記録が，窃取，改ざん又は消去されないように必要な措置を講じなければならない。

・システム管理者は，アクセス記録を定期的に点検又は分析する機能を設け，必要に応じて不正アクセス，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。

（ⅴ）障害記録の作成

システム管理者は，障害記録を作成し，一定の期間保存しなければならない。

（ⅵ）ソフトウェアの導入に関する注意

・職員は，新たにソフトウェアを導入する場合は，システム管理者の許可を得るとともに，著作権及び著作隣接権に配慮しなければならない。

・職員は，正規のライセンスのないソフトウェアを導入してはならない。

・職員は，業務上不必要なソフトウェア及び出所不明なソフトウェア等安全性が確認されないソフトウェアをインストールしてはならない。

・職員は，導入されているソフトウェアを適切に運用管理しなければならない。

（ⅶ）電子メールの送受信等

・職員は，電子メールで送受信を行う場合は，原則として city.sendai.jp 又は city.sendai.lg.jp のドメインを冠したメールアドレスを使用しなければならない。ただし，業務上必要な場合であって，CISO の許可を得た場合はこの限りでない。

・職員は，ウェブページ等が有するデータ送受信機能を用いて電子メールの送受信を行う場合は，重要性分類Ⅱ以上の行政情報の送信を原則行ってはならない。ただし，業務上必要な場合であって，CISO の許可を得た場合はこの限りでない。

・職員は，業務上不必要な者へ電子メールを送信してはならない。

・職員は，チェーンメールや不審な電子メールを他者に転送してはならない。

・職員は，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。ただし，業務上必要な場合であって，システム管理者又は情報管理者の許可を得た場合はこの限りではない。

・職員は，重要性分類Ｓ，Ⅰ又はⅡの行政情報に該当する添付ファイルのある電子メールを送信する必要がある場合には，事前に情報管理者の承認を受けなければならない。

・原則として，仙台市個人情報保護条例（平成 16 年仙台市条例第 49 号）第 2 条第 1 項に該当する個人情報は送信してはならない。

・職員は，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わからないようにしなければならない。ただし，庁内ネットワーク内のみで送受信するグループウェアの電子メールについてはこの限りではない。

・職員は，差出人が不明な，又は不自然なファイルが添付された電子メールを受信した場合は，

直ちに廃棄しなければならない。

（viii）電子メールのセキュリティ管理

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

・ネットワーク管理者は，大量のスパムメール等の受信又は送信を検知した場合は，メールサーバの運用を停止しなければならない。

・ネットワーク管理者は，電子メールの送受信容量の上限を設定し，上限を超える電子メールの送受信を不可能にしなければならない。

・ネットワーク管理者は，職員等が使用出来る電子メールボックス等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。

（ix）暗号化

情報管理者は，必要に応じて行政情報を暗号化して管理するものとし，暗号化に用いた暗号鍵及び暗号化された行政情報は，別々に適切な管理をしなければならない。

（x）職員以外の者が利用出来る情報システム

システム管理者は，職員以外の者が利用出来る情報システムについては，情報セキュリティに関して危険性に応じた対策をとらなければならない。

（xi）情報システムの入出力データ

・情報管理者は，情報システムに入力されるデータの適切なチェック等を行い，それが正確であることを確実にするための対策を施さなければならない。

・情報管理者は，情報システムから出力されるデータが正しく処理されていることを確認しなければならない。

（xii）業務目的以外での使用禁止

職員は，業務目的以外での情報システムへのアクセス，電子メールの使用及びウェブの閲覧を行ってはならない。

② 情報システムアクセス制御

（ⅰ）利用者登録

・システム管理者は，重要な情報システムの利用者の登録，変更及び抹消等については，情報システム毎に定められた方法に従って行わなければならない。

・利用者の登録及び変更等は，システム管理者に対する申請により行わなければならない。

（ⅱ）複数要素認証

・システム管理者及び情報管理者は，重要性分類Ｓ又はⅠの行政情報を取り扱う情報システムの認証においては，行政情報の重要度に応じて，「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（複数要素認証）の導入を検討しなければならない。

・システム管理者及び情報管理者は，以下の場合であって，重要性分類Ⅱ以上の行政情報を取り扱う場合は，複数要素認証を導入しなければならない。

●クラウドサービスの利用を前提としたシステムを構築又は調達し，運用を行う場合

●テレワークに供するシステムを構築又は調達し，運用を行う場合

（iii）アクセス制御

・システム管理者は，不必要なネットワークサービスにアクセスできないよう必要な措置を講じ

なければならない。

・システム管理者は，情報システムへのアクセス許可は必要最小限にしなければならない。

（ⅳ）外部からのアクセス

・システム管理者は，外部からのアクセスの許可は，必要最小限にしなければならない。

・システム管理者及び情報管理者は，公衆通信回線（公衆無線 LAN 等）を情報システムに接続することを原則禁止しなければならない。ただし，やむを得ず接続を認める場合は，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。

（ⅴ）内部からのアクセス

情報管理者は，行政情報ネットワークシステムや内部ネットワークを持つシステム上の共有フォルダへのアクセスの許可は，必要最小限にしなければならない。

（ⅵ）外部ネットワークとの接続

・個人情報を取扱う情報システムは，外部ネットワークとの接続を行ってはならない。ただし，法令等に定めがある場合，仙台市個人情報保護審議会が公益上必要があると認める場合，又は第１章（２）⑫（ⅱ）(b)及び(c)に規定するサービスで CISO が必要と認める場合は，この限りではない。

・システム管理者は外部ネットワークとの接続に際しては，当該外部ネットワークのネットワーク構成，機器構成及び情報セキュリティレベル等を詳細に検討し，本市の情報資産に影響が生じないことを明確に確認し，ネットワーク管理者との協議の上， CISO の許可に基づき接続しなければならない。

・システム管理者及びネットワーク管理者は，外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることの無いようにセキュリティ対策に努めなければならない。

・ネットワーク管理者は，フィルタリング及びルーティングについて，不都合が発生しないよう，必要な対策を講じるものとする。

・ネットワーク管理者は，不正アクセスを防止するため，アクセス制御等必要な対策を講じるものとする。

・システム管理者及びネットワーク管理者は，接続した外部ネットワークの情報セキュリティに問題が認められ，本市の情報資産に脅威が生じることが想定される場合には，直ち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。

・システム管理者及びネットワーク管理者は，内部ネットワークの情報セキュリティに問題が認められた場合には，直ちに当該内部ネットワークを，外部ネットワークから遮断しなければならない。

（ⅶ）無許可でのネットワーク接続禁止

職員は，システム管理者又は情報管理者の許可なくパソコン等をネットワークに接続してはならない。

（ⅷ）特権を付与された ID 等の管理

・システム管理者及び情報管理者は，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 及びパスワードを厳重に管理しなければならない。

・システム管理者及び情報管理者は，特権を付与された ID 及びパスワードの変更について，外部委託事業者に行わせる必要性がある場合は，十分な管理のもと，行うものとする。

・システム管理者及び情報管理者は，特権を付与された ID 及びパスワードについて，職員が事

務用に使用する電子計算機等のパスワードよりも，定期的な変更や入力回数の制限等セキュリティ機能の強化に努めるものとする。

（ix）情報システム利用者の ID の管理

・システム管理者及び情報管理者は，利用者の登録，変更及び抹消等の情報管理，職員の異動，出向及び退職等に伴う利用者 ID の取扱い等の方法を定めなければならない。

・職員は，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，システム管理者又は情報管理者に通知しなければならない。

・システム管理者及び情報管理者は，利用されていない ID が放置されないよう，定期的に点検しなければならない。

③ 情報システムの開発，導入及び保守

システム管理者及び情報管理者は，情報システムの開発，導入及び保守をする場合は，必要に応じネットワーク管理者と協議するものとする。

（ｉ）情報システムの開発及び導入

・システム管理者及び情報管理者は，情報システムのソフトウェアを開発及び導入する場合は，情報セキュリティ上問題にならないように対策を講じなければならない。

・システム管理者は，重要な情報システムのソフトウェアを開発する場合は，ソフトウェアの仕様書及びネットワーク構成図等を整備しなければならない。

・システム管理者は，開発したソフトウェアを重要な情報システムに取り入れる場合は，既に稼動しているシステムに情報セキュリティ上の影響が及ばないように，接続する前に十分な試験を行わなければならない。

（ii）情報システムの変更管理

システム管理者は，重要な情報システムを追加，変更又は廃棄等した場合は，その際の設定，構成等の履歴を記録及び保存し，必要な場合には復旧出来るようにしなければならない。

（iii）ソフトウェアの保守及び更新

・システム管理者及び情報管理者は，情報セキュリティに重大な影響を及ぼすソフトウェアについては，適切な保守が行われるようにし，その不具合については，直ちに修正等の対応を行わなければならない。

・システム管理者及び情報管理者は，パッチやバージョンアップ等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。

・システム管理者は，重要な情報システムのソフトウェアの更新等については，計画的に実施しなければならない。

（iv）機器の修理，廃棄又は返却

・情報管理者は，記録媒体の含まれる機器を，外部業者に修理させる場合又は賃貸借期限終了等により返却若しくは廃棄する場合は，可能な範囲でバックアップを取り，記録媒体内のすべての行政情報を消去しなければならない。

・情報管理者は，当該機器を外部業者に修理させる際，行政情報を消去することが難しい場合は，修理を行わせる業者と守秘義務を明記した契約を締結しなければならない。

（ｖ）機器構成の変更

・職員は，情報システムの機器について業務を遂行するため機器の増設又は交換を行う必要がある場合には，システム管理者又は情報管理者の許可を得なければならない。

・職員は，通信機器等を増設して，他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には，情報管理者を通じ，システム管理者の許可を得なければならない。

・システム管理者は，機器構成の変更等の許可に当たって，重要な情報システムや他のシステムに情報セキュリティ上の問題を生じさせてはならない。

（vi）クラウドサービスの利用を前提とした情報システムの調達と導入

・システム管理者及び情報管理者は，情報システムにクラウドサービスを導入する場合は，クラウドサービスの仕様が取り扱う行政情報の重要性分類に相応しい可用性及び機密性を備えていることを確認しなければならない。

④ コンピュータウイルス対策

（ｉ）情報管理者の実施事項

・情報システムのサーバ及び必要な機器にウイルス対策ソフトを導入すること。

・ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

・定期的に新種のウイルスに関する情報収集や情報システム内部の感染状況等について情報収集をすること。

・コンピュータウイルスについて，職員に対して必要な啓発活動を行うこと。

・事務所管課で調達した端末の場合，ウイルス対策ソフトの設定変更権限については，情報管理者又は副情報管理者が一括管理し，その他の職員に当該権限を付与しないこと。

（ii）職員の遵守事項

・データ又はソフトウェアを外部から取り入れ，又は外部に持ち出す場合は，必ずウイルスチェックを行うこと。

・ウイルスチェックの実行を途中で止めないこと。

・添付ファイルのあるメールを送受信する場合は，ウイルスチェックを行うこと。

⑤ 不正アクセス対策

・システム管理者及び情報管理者は，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。

・システム管理者及び情報管理者は，セキュリティホール等の情報収集に努め，メーカー等から修正プログラムの提供があり次第，速やかに対応するとともに，その修正履歴を記録及び保存しなければならない。

・システム管理者及び情報管理者は，情報システムに修正プログラムの導入ができない場合は，他の手段によって，情報セキュリティを確保する措置を講じなければならない。

・システム管理者及び情報管理者は，情報システムに不正な侵入や利用があった場合に探知等出来るよう，適切な対策に努めなければならない。

・システム管理者及び情報管理者は，情報システムに攻撃を受けていることが明らかな場合には，システムの停止を含め必要な措置を講じなければならない。

・局（区）情報管理者又は情報管理者は，職員により本市ネットワーク及び外部ネットワークに対して不正なアクセスがあった場合は，当該職員が属する情報管理者に通知し，適切な処置を求めなければならない。

・職員は，外部ネットワークより不正アクセスがあった場合は，システム管理者及び情報管理者に報告し，適切な措置を講じなければならない。

⑥ セキュリティ情報の収集

・システム管理者は，重要な情報システムの設定に係るファイル等について，定期的に当該ファイルの改ざんの有無を検査しなければならない。

・局（区）情報管理者は，セキュリティに関する情報について，国及び関係団体，民間事業者等から適宜情報を収集しなければならない。

⑦ ネットワークに接続する機器の管理

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

⑧ RPA の管理

・システム管理者及び情報管理者は，RPA によって自動化された処理を文書等で可視化しなければならない。また，処理内容の変更が行われた場合は，必ず当該文書等にも反映しなくてはならない。

・システム管理者及び情報管理者は，RPA による処理に誤りがないことを検知できる仕組みの構築又は処理結果の定期的な点検を行わなければならない。

・システム管理者及び情報管理者は，RPA による処理を不正に使用されないために，認証等による使用制限を設けなければならない。

（８）運用

① 情報システムの監視

・システム管理者は，重要な情報システムの運用にあたっては，常に情報システムを監視するとともにセキュリティ障害に対して注意を払わなければならない。

・システム管理者は，セキュリティ障害時の調査を確実なものとするために，重要な情報システムのサーバ等の時刻について，正確な時刻を保つようにしなければならない。

② 情報セキュリティポリシーの遵守状況の確認と対処

・局（区）情報管理者及び情報管理者は，情報セキュリティポリシーの遵守状況について，また，運用上支障が生じていないかについて確認を行い，問題が発生していた場合には適切かつ速やかに対処しなければならない。

・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切かつ速やかに対処しなければならない。

③ セキュリティ障害時の対応

局（区）情報管理者，CSIRT 管理者，システム管理者及び情報管理者は，セキュリティ障害が発生した場合には，直ちに対応するとともに，再発防止の措置を講じなければならない。

（ⅰ）障害の発生

・職員は，セキュリティ障害の発生について，他の職員からの検知・連絡だけでなく，市民等外部からの連絡によって検知した場合も，直ちに情報管理者へ報告しなければならない。

・情報管理者は，セキュリティ障害が発生した情報システムが重要な情報システムに関するものにあっては，直ちにシステム管理者へその旨を報告しなければならない。

（ⅱ）障害発生の報告

・システム管理者及び情報管理者は，セキュリティ障害が発生した場合，直ちに次の項目について調査を行い，その内容について局（区）情報管理者及び CSIRT 管理者へ報告を行わなければならない。

・セキュリティ障害の内容

・セキュリティ障害が発生した原因

・確認した被害及び影響範囲

・CSIRT 管理者は，セキュリティ障害の発生の報告を受けた場合，以下の対応を実施しなければならない。

ア　発生したセキュリティ障害の影響が他システムや他課に及ぶ可能性があるなど，技術的支援等が必要な場合は CSIRT 責任者へ報告を行う。

イ　発生したセキュリティ障害への対応等のため，技術的な助言又は必要な情報の提供を CSIRT 責任者に求める。

ウ　セキュリティ障害の程度が軽微なものについては報告を要しないものとする。

・局（区）情報管理者は，セキュリティ障害の程度が外部に重大な影響を及ぼすおそれがある場合には，直ちに CISO に報告のうえ必要な指示を仰がなければならない。

（ⅲ）障害拡大の防止措置

・システム管理者及び情報管理者は，業務を継続することにより，セキュリティ障害による影響が拡大する可能性が高い場合には，重要な情報システムの停止を含む必要な措置を講じるとともに，CSIRT 責任者へ報告しなければならない。

・システム管理者及び情報管理者は，セキュリティ障害が発生し，その障害の原因となる行為が不正アクセスの可能性がある場合には，当該セキュリティ障害に関する記録（アクセスログ等）の保存に努めるとともに，CSIRT 責任者の求めに応じ，提供しなければならない。

（ⅳ）障害復旧及び再発防止の報告

・システム管理者及び情報管理者は，局（区）情報管理者の指示の下，直ちにセキュリティ障害を復旧し，その措置について局（区）情報管理者及び CSIRT 管理者に報告しなければならない。

・局（区）情報管理者は，必要な再発防止の措置を講じるとともに，外部に重大な影響を及ぼしたセキュリティ障害について，その対応結果を CISO 及び CSIRT 責任者に報告しなければならない。

④ 大規模災害時等における例外措置

（ⅰ）例外措置の許可

局（区）情報管理者は，情報セキュリティ関係規定を遵守することが困難な状況で，行政事務の適正な遂行を継続するため，遵守事項とは異なる方法を採用し，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，例外措置を実施することが出来る。

（ⅱ）緊急時の例外措置

局（区）情報管理者は，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，（ⅰ）の許可を得ることなく例外措置を実施することができる。ただし，例外措置の実施後速やかに CISO に報告しなければならない。

（９）法令等遵守

職員は，次の法令等を遵守しなければならない。

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）

③著作権法（昭和 45 年法律第 48 号）

④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)

⑤サイバーセキュリティ基本法（平成 28 年法律第 31 号）

⑥仙台市個人情報保護条例

⑦事務処理指針（H20 年総総行第 532 号，別添）

また，マナーと倫理をもって情報システムを利用しなければならない。

(10) 評価，見直し等

① 自主点検

・局（区）情報管理者及び情報管理者は，当該部署の情報セキュリティが確保されていることを確認するため，定期的及び必要に応じて自主点検を行い，その結果を組織の課題の有無を確認する観点から分析・評価し，必要に応じ改善措置を講じるものとする。

・職員は，自主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。

・CISO は，この点検結果を情報セキュリティポリシーの見直し及びその他の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。

② 監査

・CISO は，重要な情報システムの管理体制やシステムのぜい弱性調査等について定期的及び必要に応じ監査を実施するものとする。

・CISO の命により監査を行う者は，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。

・CISO は，監査の結果を通して収集した監査証拠及び監査報告書作成のための書類を適切に保管しなければならない。

・CISO は，監査結果を踏まえ，指摘事項に係る情報システムを所管している情報管理者又はシステム管理者に対し，当該事項への対処を指示しなければならない。また，指摘事項に係る情報システムを所管していない情報管理者又はシステム管理者に対しても，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。

・CISO は，監査結果を取りまとめ，必要に応じて「仙台市デジタル行政推進本部」に報告するものとする。

・CISO は，監査結果を情報セキュリティポリシーの見直し及び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。

③ 見直し

CISO は，情報セキュリティポリシーの見直しが必要となる事象が発生した場合には，「仙台市デジタル行政推進本部」に諮り必要な見直しを行い，情報セキュリティの維持及び情報セキュリティポリシーの適切な運用に努めなければならない。