令和４年３月29日
庁　議　資　料

# 狛江市情報セキュリティポリシー

- はじめに
- 狛江市情報セキュリティ基本方針
- 狛江市情報セキュリティ対策基準

令和４年３月

狛　江　市

# 目　次

# はじめに

## ⅰ 情報セキュリティポリシーの必要性

地方公共団体は，法令等に基づき，住民の個人情報や企業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，住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。

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，住民生活や地域の社会経済活動に重大な支障が生じる可能性も高まる。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の未然防止のみならず，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。

そこで，狛江市は，情報セキュリティの確保のためには，情報システム利用者の情報セキュリティに対する意識向上はもちろん，これらの情報に関して利用者個人の裁量で，その扱いが判断されることのないよう，組織として意思統一し，明文化された情報セキュリティポリシーを策定し，総合的にセキュリティ対策に取り組んでいくこととする。

## ⅱ 情報セキュリティポリシーの構成

狛江市情報セキュリティポリシーとは，狛江市が所掌する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，体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは，狛江市が所掌する情報資産に関する業務に携わる全ての職員に浸透，普及，定着させるものであり，安定的な規範であることが要請される。しかしながら一方では，技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ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を一定の普遍性を備えた部分としての①「情報セキュリティ基本方針」と情報資産を取り巻く環境の変化に対応し，情報セキュリティの水準を向上していく部分としての②「情報セキュリティ対策基準」に分け，それぞれを策定することとする。また，情報セキュリティ対策基準に基づき，情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする。

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すべ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 | | 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 |

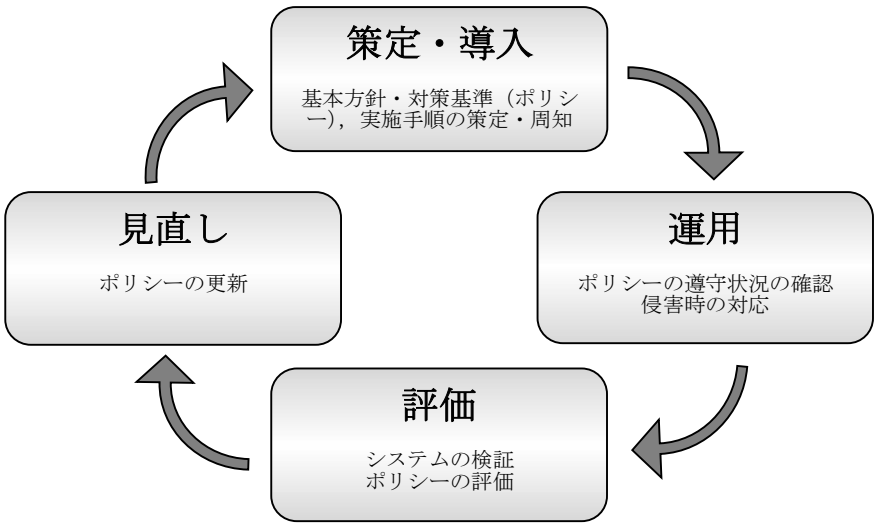
## iii 情報セキュリティの実施サイクル

ＩＣＴの発展速度は極めて速いため，ある時に講じた最高の情報セキュリティ対策が将来にわたって最高のものとして持続することはなく，また，継続性も保証されてはいない。セキュリティ対策は，ポリシーを策定することによって完結する一過性の取組ではなく，策定及びそれに続く運用・評価・見直しを継続的に繰り返すことによって確保される性質のものであることを十分に認識する必要がある。

ポリシーの中には，継続的な情報収集及びセキュリティ確保の体制の構築，また，「破られたときにどうするか」の危機管理対策も規定し，規定に基づいた対策を十分に構築しておくことが重要である。

また，ポリシー及び実施手順等の規定類を定期的に見直すことによって，新たな脅威の発生や環境の変化はないか確認し，継続的に対策を講じていくことが必要である。情報セキュリティの分野では，技術の進歩やハッカーの手口の巧妙化により早いサイクルでの見直しを行っていくことが重要であることから，以下のような実施サイクルで進めていくこととする。

**情報セキュリティサイクルの実施サイクル図**



狛江市情報セキュリティ基本方針

令和４年３月 24 日
規則第９号

１　目的

狛江市の各情報システムが取り扱う情報資産には，市民の個人情報のみならず行政運営上重要な情報など，外部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いる。

したがって，これらの情報資産及び情報資産を取り扱う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も，事務の安定的な運営のためにも必要不可欠である。ひいては，このことが狛江市に対する市民からの信頼の維持向上に寄与するものである。

また，近年のＩＣＴ分野を取り巻く環境の変化は急激であり，国や都のデジタル化等の動きが加速する中で，狛江市がこれらに積極的に対応するためには，全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

本基本方針は，狛江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，実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

（１）　ネットワーク

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

（２）　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。

（３）　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。

（４）　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。

（５）　機密性

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

（６）　完全性

情報が破壊，改ざん又は消去されていない状態を確保することをいう。

（７）　可用性

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

（８）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障，地方税若しくは防災に関する事務），又は戸籍事務等に関わる情報システム及びその情報システムで取り扱うデータをいう。

（９）　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。）。

(10)　インターネット接続系

インターネットメール，ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11)　通信経路の分割

ＬＧＷＡＮ接続系及びインターネット接続系の両環境間の通信環境を分離した上で，安全が確保された通信だけを許可できるようにすることをいう。

(12)　無害化通信

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

(13)　職員等

職員及び会計年度任用職員をいう。

３　対象とする脅威

情報資産に対する脅威として，次に掲げる脅威を想定し，情報セキュリティ対策を実施する。

（１）　不正アクセス，ウイルス攻撃，サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去，重要情報の詐取，内部不正等

（２）　情報資産の無断持ち出し，無許可ソフトウェアの使用等の規定違反，設計・開発の不備，プログラム上の欠陥，操作・設定ミス，メンテナンス不備，内部・外部監査機能の不備，外部委託管理の不備，マネジメントの欠陥，機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）　地震，落雷，火災等の災害によるサービス及び業務の停止等

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

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

４　適用範囲

（１）　行政機関の範囲

本基本方針が適用される行政機関は，市長部局，行政委員会，議会事務局とする。

（２）　情報資産の範囲

本基本方針が対象とする情報資産は，次のとおりとする。

ア　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

イ　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。）

ウ　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　情報セキュリティポリシーの意義と職員等の義務

情報セキュリティポリシーは，狛江市が所掌する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，体系的かつ具体的に取りまとめたものである。

したがって，狛江市長をはじめとして狛江市が所掌する情報資産に関する業務に携わる全ての職員等及びこれらの業務を受託する者（以下「受託者」という。）は，情報管理の重要性について共通の認識を持つとともに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ものとする。

６　情報セキュリティ対策

前記３で示した脅威から情報資産を保護するために，次の情報セキュリティ対策を行うものとする。

（１）　組織体制

狛江市の情報資産について，情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

（２）　情報資産の分類と整理

狛江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。

（３）　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。

ア　マイナンバー利用事務系においては，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，端末への多要素認証の導入等により，住民情報の流出を防ぐ。

イ　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。ただし，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。

ウ　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。この場合において，情報セキュリティ対策として，東京都が構築する自治体情報セキュリティクラウドを利用する。

（４）　物理的セキュリティ

情報システムを設置する施設への不正な立入り，通信回線及び職員等のパソコン等の管理について等，情報資産の損傷及び情報資産への妨害等から保護するために物理的な対策を講じる。

（５）　人的セキュリティ

情報セキュリティに関する権限や責任を定め，全ての職員等及び受託者に情報セキュリティポリシーの内容を周知徹底する等，十分な教育及び啓発が行われるように必要な対策を講じる。

（６）　技術的セキュリティ

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

（７）　運用

情報システムの監視，情報セキュリティポリシーの遵守状況の確認，外部委託を行う際のセキュリティ確保等，情報セキュリティポリシーの運用面の対策を講じるものとする。この場合において，情報資産に対するセキュリティ侵害発生時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。

（８）　外部サービスの利用対策

ア　外部委託する場合には，外部委託事業者を選定し，情報セキュリティに係る要件を明記した契約を締結するとともに，外部委託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ずる。

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

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

（９）　評価・見直し

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

9　情報セキュリティ対策基準の策定

前記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ものとする。

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狛江市の行政運営に重大な支障を及ぼすおそれがある情報資産であることから，狛江市情報公開条例（平成 12 年条例第６号）第９条第５号オに基づき非公開とする。

付　則

この規則は，公布の日から施行する。

狛江市情報セキュリティ対策基準

令和４年３月24日
市長決裁

本対策基準は，狛江市情報セキュリティ基本方針（令和４年規則第９号）を実行に移すための，狛江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。

第１　組織体制

１　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は本市における全てのネットワーク情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終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，ＣＩＳＯを助けて本市における情報セキュリティに関する事務を整理し，ＣＩＳＯの命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副ＣＩＳＯ」という。）１人を必要に応じて置く。

（５）　ＣＩＳＯは，本対策基準に定められた自らの担務を，副ＣＩＳＯその他の本対策基準に定める責任者に担わせることができる。

２　統括情報セキュリティ責任者

（１）　企画財政部長を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及び副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，本市の全てのネットワークにおける開発，設定の変更，運用，見直し等を行う権限及び責任を有する。

（３）　統括情報セキュリティ責任者は，本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

（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，本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，本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及び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定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。

(10)　統括情報セキュリティ責任者は，本対策基準に定められた自らの担務を，情報政策課長に担わせることができる。

３　情報セキュリティ責任者

（１）　部長相当職（選挙管理委員会事務局，監査委員事務局及び農業委員会事務局においては局長とする。）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，所掌する部，委員会並びに事務局（以下「部等」という。）の情報セキュリティ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，部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，その所掌に属する部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等に対する教育，訓練，助言及び指示を行う。

４　情報セキュリティ管理者

（１）　情報資産のセキュリティ対策を実施するため，情報セキュリティ管理者を置き，課長相当職をもってこれに充てる。

（２）　情報セキュリティ管理者は，その所掌する課，室，館，委員会及び事務局（以下「課等」という。）において，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，情報資産に関する侵害が発生した場合又は侵害のおそれがある場合には，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。

５　情報システム管理者

（１）　各情報システムの担当所属長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，更新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。

６　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し，情報システム管理者が職員等の中から指定する。

７　狛江市行政情報化推進委員会

（１）　本市の情報セキュリティ対策を統一的に実施するため，狛江市行政情報化推進委員会において，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）　狛江市行政情報化推進委員会は，毎年度，本市における情報セキュリティ対策の実施状況を確認し，必要に応じて情報セキュリティ責任者に改善計画を策定させることができる。

８　兼務の禁止

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

（２）　情報セキュリティ監査の実施において，やむを得ない場合を除き，監査を受ける者とその監査を実施する者は，同じ者が兼務してはならない。

９　ＣＳＩＲＴの設置・役割

（１）　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外部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）　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，東京都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，外部の事業者等との情報共有を行わなければならない。

## 第２　情報資産の分類と管理

### １　情報資産の分類

本市における情報資産は，機密性，完全性及び可用性により，次の表のとおり分類し，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 | 取扱制限の例 |
|---|---|---|
| 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までの情報資産に対して）<br>・必要以上の複製及び配付禁止<br>・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込み禁止<br>・情報の送信，情報資産の運搬，提供時における暗号化，パスワード設定及び鍵付きケースへの格納<br>・復元不可能な処理を施しての廃棄<br>・信頼のできるネットワーク回線の選択<br>・外部での情報処理を行う際の安全管理措置の規定遵守<br>・電磁的記録媒体等の施錠可能な場所での保管 |
| 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 | 取扱制限の例 |
|---|---|---|
| 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，電子署名付与<br>・外部で情報処理を行う際の安全管理措置の規定遵守<br>・電磁的記録媒体等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 | 取扱制限の例 |
|---|---|---|
| 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・指定する時間以内の復旧<br>・電磁的記録媒体等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 | ― |

２　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　情報資産が複製し，又は伝送された場合には，複製等された情報資産も１の分類に基づき管理しなければならない。

（２）　情報資産の分類の表示

職員等は，機密性２以上，完全性２又は可用性２の情報資産について，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，文書の隅等に重要情報であることを表示し，必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

（３）　情報の作成

ア　職員等は，業務上必要のない情報を作成してはならない。

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

ウ　情報を作成する者は，作成途上の情報についても，紛失や流失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となった場合は，当該情報を消去しなければならない。

（４）　情報資産の入手

ア　庁内の者が作成した情報資産を入手した者は，入手元の情報資産の分類に基づいた取扱いをしなければならない。

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

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

（５）　情報資産の利用

ア　情報資産を利用する者は，業務以外の目的に情報資産を利用してはならない。

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

ウ　情報資産を利用する者は，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には，自然災害を被る可能性が低い場所に保管しなければならない。

エ　情報セキュリティ管理者は，機密性２以上，完全性２又は可用性２の情報を記録した電磁的記録媒体を補完する場合，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，暗号化又はパスワード設定を行わなければならない。

（８）　情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は，必要に応じ，鍵付きのケース等に格納し，暗号化又はパスワードの設定を行う等，情報資産の不正利用を防止するための措置を講じなければならない。

イ　機密性２以上の情報資産を運搬する者は，情報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・公開

ア　機密性２以上の情報資産を外部に提供する者は，必要に応じ暗号化又はパスワードの設定を行わなければならない。

イ　機密性２以上の情報資産を外部に提供する者は，情報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

ア　情報資産の廃棄を行う者は，情報を記録している電磁的記録媒体が不要となった場合，記録されている情報の機密性に応じ，電磁的記録媒体の情報を復元できないように処置をした上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は，行った処理について，日時，担当者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。

エ　機密性２以上の情報資産を外部に提供した者は，提供先での破棄について，ア及びイを実施させ，報告を受けなければならない。

## 第３　情報システム全体の強靭性の向上

### １　マイナンバー利用事務系

（１）　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。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アドレス等）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，外部接続先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，インターネット等からマイナンバー利用事務系との双方向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，業務ごと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の持ち出しができないように設定しなければならない。

### ２　ＬＧＷＡＮ接続系

（１）　ＬＧＷＡＮ接続系とインターネット接続系の分割

ＬＧＷＡＮ接続系とインターネット接続系は両環境間の通信環境を分離した上で，必要な通信だけを許可できるようにしなければならない。なお，電子メールやデータを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

３　インターネット接続系

（１）　インターネット接続系においては，通信パケットの監視，ふるまい検知等の不正通信の監視機能の強化により，情報セキュリティインシデントの早期発見と対処及びＬＧＷＡＮへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

（２）　東京都と狛江市のインターネット接続口を集約する東京都の自治体情報セキュリティクラウドに参加するとともに，関係省庁や東京都等と連携しながら，情報セキュリティ対策を推進しなければならない。

## 第４　物理的セキュリティ

１　サーバ等の管理

（１）　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，温度及び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に適正に固定する等の必要な措置を講じなければならない。

（２）　サーバの冗長化

ア　情報システム管理者は，必要に応じて，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。

イ　上記の措置を行った場合において，情報システム管理者は，メインサーバに障害が発生した際は，速やかにセカンダリサーバを起動する等，システムの運用停止時間を最小限にしなければならない。

（３）　機器の電源

ア　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。

イ　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。

（４）　通信ケーブルの配線

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，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，配線収納管等を使用し，ＯＡフロア化を行う等の必要な措置を講じなければならない。

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。

ウ　統括情報セキュリティ責任者及び情報システム管理者は，ネットーワーク接続口（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。

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，自身や操作を指示した情報システム担当者，又は契約により操作を認められた外部委託事業者以外の者が配線を変更，追加できないように必要な措置を講じなければならない。

（５）　機器の定期保守及び修理

ア　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。

イ　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外部の業者に修理させる場合，内容を消去した状態で行わなければならない。内容を消去できない場合，情報システム管理者は，外部の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。

（６）　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，外部委託事業者のデーターセンター等，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。

（７）　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，全ての情報を消去した上，復元不可能な状態にする措置を講じなければならない。

２　管理区域（情報システム室）の管理

（１）　管理区域の構造等

ア　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。

イ　統括情報セキュリティ責任者及び情報システム管理者は，管理区域を地階又は１階に設けてはならない。また，外部からの侵入が容易にできないように無窓の外壁に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施設管理部門と連携して，管理区域から外部に通じ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。

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施設管理部門と連携して，管理区域を含む外壁等の床下開口部を全て塞がなければならない。

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，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。

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，管理区域に配備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。

（２）　管理区域の入退室管理等

ア　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カードや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。

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

ウ　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，外見上職員等特別できる措置を講じなければならない。

エ　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，又は個人所有であるコンピュータ，モバイル端末，通信回線装置，電磁的記憶媒体等を持ち込ませないようにしなければならない。

（３）　機器等の搬入出

ア　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した業者に確認を行わせなければならない。

イ　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。

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。この場合において，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の情報資産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　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ワイヤーによる固定，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，又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，必要に応じて，端末の電源起動時のパスワード（ＢＩＯＳパスワード，ハードディスクパスワード等）を併用しなければならない。

（４）　情報システム管理者は，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。

（５）　情報システム管理者は，必要に応じて，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を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合，その機能を有効に活用しなければならない。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しなければならない。

（６）　情報システム管理者は，必要に応じて，モバイル端末の庁外での業務利用の際は，上記対策に加え，遠隔消去機能を利用する等の措置を講じなければならない。

## 第５　人的セキュリティ

### １　職員等の遵守事項

#### （１）　職員等の遵守事項

ア　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又に相談し，指示を受けなければならない。

イ　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。

ウ　パソコン，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又は完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）　職員等は，本市のパソコン，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，統括情報セキュリティ責任者の定める手続に従い，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，統括情報セキュリティ責任者の定める手続に従い，情報セキュリティ管理者の許可を得なければならない。

エ　支給以外のパソコン，モバイル端末及び電磁的記録媒体の業務利用

（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順守しなければならない。

オ　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。

カ　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統括情報セキュリティ管理者及び情報システム管理者の許可なく変更してはならない。

キ　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を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。

ク　退職時等の遵守事項

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

（２）　会計年度任用職員への対応

ア　情報セキュリティポリシー等の遵守

情報セキュリティ管理者は，会計年度任用職員に対し，採用時に情報セキュリティポリシー等のうち，当該職員が守るべき事項を確実に理解させ，また，実施及び遵守させなければならない。

イ　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，会計年度任用職員に必要に応じ，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。

ウ　インターネット接続及び電子メール使用等の制限

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

（３）　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は，職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

（４）　外部委託事業者に対する説明

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

２　研修・訓練

（１）　情報セキュリティに関する研修・訓練

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

（２）　研修・訓練

ア　ＣＩＳＯは，職員等に対し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，職員等を対象とした情報セキュリティポリシーに関する研修の機会を定期的に設けなければならない。

イ　統括情報セキュリティ責任者は，統括情報セキュリティ責任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

けなければならない。

ウ　情報政策課長は，最新の技術力を維持するための研修を常に受けなければならない。また，情報政策課長は統括情報セキュリティ責任者の指示に基づき，緊急時対応を想定した訓練を職員等に行わせなければならない。

エ　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，情報セキュリティ対策を実施する上で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けなければならない。

オ　情報システム管理者は，情報システムの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けなければならない。

カ　情報システム管理者は，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対応を想定した訓練等を職員等に行わせなければならない。

キ　職員等は，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。

ク　情報システムの開発，保守及び運用管理に携わる職員等は，担当者として必要な技術力の習得及び維持するための研修を受けなければならない。

（３）　緊急時対応訓練

ＣＩＳＯは，緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は，ネットワーク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。

（４）　研修・訓練への参加

幹部を含めた全ての職員等は，定められた研修・訓練に参加しなければならない。

３　情報セキュリティインシデントの報告

（１）　庁内での情報セキュリティインシデントの報告

ア　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。

イ　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関連する情報システム管理者に報告しなければならない。

ウ　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，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。

（２）　住民等外部からの情報セキュリティインシデントの報告

ア　職員等は，本市が管理するネットワーク，情報システム等の情報資産に関する情報セキュリティインシデントについて，住民等外部から報告を受けた場合，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。

イ　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

責任者及び関連する情報システム管理者に報告しなければならない。

ウ　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。

エ　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なければならない。

（３）　情報セキュリティインシデント原因の究明・記録，再発防止等

ア　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。

イ　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。

ウ　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。

エ　ＣＳＩＲＴは，これらの情報セキュリティインシデントの原因を究明し，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。

オ　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。

４　ＩＤ及びパスワード等の管理

（１）　ＩＣカード等の取扱い

ア　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，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。

イ　統括情報セキュリティ責任者及び情報システム管理者は，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。

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，ＩＣカード等を切り替える場合，切り替え前のカードを回収し，破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２）　ＩＤの取扱い

職員等は，自己の管理するＩＤに関し，次の事項を遵守しなければならない。

（ア）　自己が利用しているＩＤは，他人に利用させてはならない。
（イ）　共用ＩＤを利用する場合は，共用ＩＤの利用者以外に利用させてはならない。

（３）　パスワードの取り扱い

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。

（ア）　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
（イ）　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。
（ウ）　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。
（エ）　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。
（オ）　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。
（カ）　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。
（キ）　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。
（ク）　職員間でパスワードを共有してはならない（ただし，共有ＩＤに対するパスワードは除く。）。

## 第６　技術的セキュリティ

### １　コンピュータ及びネットワークの管理

（１）　文書サーバの設定等

ア　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。

イ　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作成，変更及び削除できないように，設定しなければならない。

ウ　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，パスワードの設定や必要に応じて別途ディレクトリを作成する等の措置を講じ，同一課等であっても，担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（２）　バックアップの実施

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

（３）　他団体との情報システムに関する情報等の交換

情報システム管理者は，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。

（４）　システム管理記録及び作業の確認

ア　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。

イ　統括情報セキュリティ責任者及び情報システム管理者は，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適正に管理しなければならない。

ウ　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外部委託事業者がシステム変更等の作業を行う場合は，２名以上で作業を行い，互いにその作業を確認しなければならない。

（５）　情報システム仕様書等の管理

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，記録媒体にかかわらず，業務上必要とする者以外の者が閲覧したり，紛失等がないよう，適正に管理しなければならない。

（６）　ログの取得等

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，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。

イ　統括情報セキュリティ責任者及ぶ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。

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，取得したログを定期的に点検又は分析する機能を設け，必要に応じて悪意の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。

（７）　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，障害記録として作成し，適正に保存しなければならない。

（８）　ネットワークの接続制御，経路制御等

ア　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。

イ　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。

（９）　外部の者が利用できるシステムの分離等

統括情報セキュリティ責任者は，電子申請の汎用受付システム等，外部の者が利用できるシステムについて，必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(10)　外部ネットワークとの接続制限等

ア　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。

イ　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。

ウ　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。

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，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，適正な設定を行った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。

オ　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。

(11)　複合機のセキュリティ管理

ア　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，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。

イ　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。

ウ　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し，又は再利用できないよう対策を講じなければならない。

(12)　IoT機器を含む特定用途機器のセキュリティ管理

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。

(13)　無線ＬＡＮ及びネットワークの盗聴対策

ア　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づけなければならない。

イ　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，情報の盗聴を防ぐため，暗号化等の措置を行わなければならない。

(14)　電子メールのセキュリティ管理

ア　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。

イ　統括情報セキュリティ責任者は，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。

ウ　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。

エ　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。

オ　統括情報セキュリティ責任者は，システム開発や運用，保守等のために庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について，外部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。

カ　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りシステム上措置を講じなければならない。

(15)　電子メールの利用制限

ア　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。

イ　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。

ウ　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。

エ　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をしなければならない。

オ　職員等は，統括情報セキュリティ責任者が認めるものを除いて，ウェブで利用できる電子メール，ネットワークストレージサービス等を使用してはならない。

(16)　電子署名・暗号化

ア　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，暗号化又はパスワード設定等，セキュリティを考慮して，送信しなければならない。

イ　職員等は，暗号化を行う場合には，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。

ウ　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

ア　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。

イ　職員等は，業務上の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。

ウ　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

ア　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。

イ　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)　無許可でのネットワーク接続の禁止

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

(20)　業務以外の目的でのウェブ閲覧の禁止

ア　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。

イ　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，情報システム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

ア　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。

イ　職員等は，本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。

ウ　職員等は，Web会議を主催する場合，会議に無関係のものが参加できないよう対策を講ずること。

エ　職員等は，外部からWeb会議に招待される場合は，本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

ア　情報セキュリティ管理者は，本市が管理するアカウントでソーシャルメディアサービスを利用する場合，なりすまし対策や不正アクセス対策等の情報セキュリティ対策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。

イ　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。

ウ　情報セキュリティ管理者は，ソーシャルメディアサービスの利用に当たり，責任者を定めなければならない。

エ　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。

オ　ソーシャルメディアサービスによる情報発信が，実際に本市によるものであることを明らかにするために，本市が管理している公式なWebサイトに当該ソーシャルメディアサービスのアカウント情報を掲載して参照可能とすること。

2　アクセス制御

（1）　アクセス制御等

ア　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，システム上制限しなければならない。

イ　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，職員の異動，出向，退職に伴う利用者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及び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。

ウ　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とし，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任命し，ＣＩＳＯが認める者でなくてはならない。

（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，外部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。

（２）　職員等による外部からのアクセス等の制限

ア　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管理者の許可を得なければならない。

イ　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。

ウ　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。

エ　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。

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，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。

カ　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定義されたポリシーに従って接続しなければならない。

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

（３）　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ている機器について，機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（４）　ログイン時の表示等

情報システム管理者は，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。

（５）　認証情報の管理

ア　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，これを有効活用しなければならない。

イ　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。

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，認証情報の不正利用を防止するための措置を講じなければならない。

（６）　特権による接続時間の制限

情報システム管理者は，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。

３　情報システムの開発・導入・保守

（１）　情報システムの調達

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，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。

イ　統括情報セキュリティ責任者及び情報システム管理者は，機器及びソフトウェアの調達に当たっては，当該製品のセキュリティ機能を調査し，情報セキュリティ上問題のないことを確認しなければならない。

（２）　情報システムの開発

ア　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。

イ　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い。

ウ　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ソフトウェア及びハード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は，当該ソフトウェアをシステムから削除しなければならない。

（３）　情報システムの導入

ア　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・保守環境及びテスト環境と，システムの運用環境を可能な限り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に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。

イ　テスト

（ア）　情報システム管理者は，新たにシステムを導入する場合，既に稼動している情報システムに接続する前に十分なテスト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，あらかじめ疑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，受入テストを行う場合，開発した組織と導入する組織が，それぞれ独立したテストを行わなければならない。

（４）　システム開発・保守に関連する資料等の保管

ア　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。

イ　情報システム管理者は，テストの結果を一定期間保管しなければならない。

ウ　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等を適正な方法で保管しなければならない。

（５）　情報システムにおける入出力データの正確性の確保

ア　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。

イ　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。

ウ　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。

（６）　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。

（７）　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。

（８）　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。

4　不正プログラム対策

（1）　統括情報セキュリティ責任者の措置事項

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

ア　外部ネットワークから受信したファイルは，インターネットのゲートウエイにおいて，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。

イ　外部ネットワークに送信するファイルは，インターネットのゲートウエイにおいて，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，不正プログラムの外部への拡散を防止しなければならない。

ウ　コンピュータウイルス等の不正プログラムについて情報を収集し，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。

エ　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。

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

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

キ　業務で利用するソフトウェアは，パッチやバージョンアップなどの開発元のサポートが終了したものを利用してはならない。

（2）　情報システム管理者の措置事項

情報システム管理者は，不正プログラム対策に関し，次の事項を措置しなければならない。

ア　情報システム管理者は，その所掌するサーバ及びパソコン等の端末に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。

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

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

エ　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，本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。

エ　コンピュータウイルス等の不正プログラムに関する情報の収集に努めること。

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

（３）　職員等の遵守事項

職員等は，不正プログラム対策に関し，次の事項を遵守しなければならない

ア　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。

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

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

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

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

カ　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。

キ　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。

（４）　専門家の支援体制

統括情報セキュリティ責任者は，実施している不正プログラム対策では不十分な事態が発生した場合に備え，外部の専門家の支援を受けられるようにしておかなければならない。

５　不正アクセス対策

（１）　統括情報セキュリティ責任者の措置事項

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，次の事項を措置しなければならない。

ア　使用されていないポートを閉鎖しなければならない。

イ　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。

ウ　不正アクセスによるウェブページの改ざんを防止するために，データの書換えを検出し，統括情報セキュリティ責任者及び情報システム管理者へ

通報するよう，設定しなければならない。

エ　重要なシステムの設定を行ったファイル等について，定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ　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及び連絡網を構築しなければならない。

（２）　攻撃への対処

ＣＩＳＯ及び統括情報セキュリティ責任者は，サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は，システムの停止を含む必要な措置を講じなければならない。また，総務省，東京都と連絡を密にして情報の収集に努めなければならない。

（３）　記録の保存

ＣＩＳＯ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。

（４）　内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は，職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）　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には，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。

（６）　サービス不能攻撃

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

（７）　標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は，標的型攻撃による内部への侵入を防止するために，教育等の人的対策を講じなければならない。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する対策，侵入範囲の拡大を防止する対策，内部から外部へ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　セキュリティ情報の収集

（１）　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

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，ソフトウェアの更新等の対策を実施しなければならない。

（２）　不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者及は，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等について，職員等に通知しなければならない。

（３）　情報セキュリティに関する情報の収集及び共有

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。

## 第７　運用

### 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）　暗号化された通信データ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。

### ２　情報セキュリティポリシーの遵守状況の確認

（１）　遵守状況の確認及び対処

ア　情報セキュリティ責任者及び情報セキュリティ管理者は，情報セキュリティポリシーの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。

イ　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。

ウ　統括情報セキュリティ責任者及び情報システム管理者は，ネットワーク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。

（２）　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。

（３）　職員等の報告義務

ア　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。

イ　当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性がある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。

３　侵害時の対応等

（１）　緊急時対応計画の策定

ＣＩＳＯ又は行政情報化推進委員会は，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。

（２）　緊急時対応計画に盛り込むべき内容

緊急時対応計画には，次の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案の対応措置

エ　再発防止措置の策定

（３）　業務継続計画との整合性確保

自然災害，大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し，行政情報化推進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。

（４）　緊急時対応計画の見直し

ＣＩＳＯ又は行政情報化推進委員会は，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。

４　例外措置

（１）　例外措置の許可

情報セキュリティ管理者及び情報システム管理者は，情報セキュリティ関係規定を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。

（２）　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は，行政事務の遂行に緊急を要する等の場合であって，例外措置を実施することが不可避のときは，ＣＩＳＯの許可を得ず例外措置を講じることができる。この場合において，事後速やかにＣＩＳＯに報告しなければならない。

（３）　例外措置の申請書の管理

ＣＩＳＯは，例外措置の申請書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。

５　法令等遵守

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）　狛江市個人情報保護条例（平成 13 年条例第１号）

（８）　狛江市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条例（平成 27 年条例第 19 号）

６　懲戒処分等

（１）　懲戒処分

情報セキュリティポリシーに違反した職員等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。

（２）　違反時の対応

職員等が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。

ア　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属する課室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。

イ　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。

ウ　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は剥奪した旨をＣＩＳＯ及び当該職員等が所属する課室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。

## 第８　外部委託

### １　外部委託

#### （１）　外部委託の選定基準

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

イ　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事業者を選定しなければならない。

#### （２）　契約項目

情報システムの運用・保守等を外部委託する場合には，外部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。

ア　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

イ　外部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

ウ　提供されるサービスレベルの保証

エ　外部委託事業者にアクセスを許可する情報の種類と範囲，アクセス法

オ　外部委託事業者の従業員に対する教育の実施

カ　提供された情報の目的外利用及び受託者以外への提供の禁止

キ　業務上知り得た情報の守秘義務

ク　再委託に関する制限事項の厳守

ケ　委託業務終了時の情報資産の返還，廃棄等

コ　委託業務の定期報告及び緊急報告義務

サ　狛江市による監査及び検査の実施

シ　狛江市による情報セキュリティインシデント発生時等の公表

ス　情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

#### （３）　確認・措置等

情報セキュリティ管理者は，外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し，必要に応じ，前号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。

### ２　外部サービスの利用（機密性２以上の情報を取り扱う場合）

#### （１）　外部サービス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

ア　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を取り扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）

イ　外部サービス提供者の選定基準

ウ　外部サービス利用申請の許可権限者と利用手続
エ　外部サービス管理者の指名と外部サービス利用状況の管理

（２）外部サービスの選定

ア　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。

イ　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，次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基準に含めること。

（ア）　外部サービスの利用を通じて本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ものによって，本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異本関係・役員等の情報，外部サービスの提供が行われる施設等の場所，外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（オ）　情報セキュリティインシデントへの対処方法

（カ）　情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）　情報セキュリティ対策の履行が不十分な場合の対処方法

ウ　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遂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。

エ　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本市が取り扱う情報の格付等を勘案し，必要に応じて次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

オ　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本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，必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判所轄を選定条件に含めること。

カ　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本市に提供し，本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承認の可否を判断すること。

キ　情報セキュリティ責任者は，取り扱う情報の格付け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。

ク　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。

ケ　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等から，外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

（３）　外部サービスの利用に係る調達・契約

ア　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。

イ　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。

（４）　外部サービスの利用承認

ア　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，行政情報化推進委員会へ外部サービスの利用申請を行うこと。

イ　行政情報化推進委員会は，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。

ウ　行政情報化推進委員会は，外部サービスの利用申請を承認した場合，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。

（５）　外部サービスを利用した情報システムの導入・構築時の対策

ア　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，次に掲げる対策を含む外部サービスを利用して情報システムを構築際のセキュリティ対策を規定すること。

（ア）　不正なアクセスを防止するためのアクセス制御

（イ）　取り扱う情報の機密性保護のための暗号化

（ウ）　開発時におけるセキュリティ対策

（エ）　設計・設定時の誤りの防止

イ　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。

（６）　外部サービスを利用した情報システムの運用・保守時の対策

ア　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，次に掲げる対策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

イ　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，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。

ウ　外部サービス管理者は，前各項において定める規定に対し，運用・保守時に実施状況を定期的に確認・記録すること。

（７）　外部サービスを利用した情報システムの更改・廃棄時の対策

ア　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，次に掲げる対策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

イ　外部サービス管理者は，前項において定める規定に対し，外部サービスの利用終了時に実施状況を確認・記録すること。

３　外部サービスの利用（機密性２以上の情報を取り扱わない場合）

（１）　外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は，次に掲げる対策を含む外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

ア　外部サービスを利用可能な業務の範囲

イ　外部サービスの利用申請の許可権限者と利用手続

ウ　外部サービス管理者の指名と外部サービスの利用状況の管理

エ　外部サービスの利用の運用手順

（２）　外部サービスの利用における対策の実施

ア　職員等は，利用するサービスの約款，その他の提供条件から，利用に当たってのリスクが許容できることを確認した上で機密性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。

イ　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。

## 第９　評価・見直し

### １　監査

（１）　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。

（２）　監査を行う者の要件

ア　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。

イ　監査を行う者は，監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（３）　監査実施計画の立案及び実施への協力

ア　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，行政情報化推進委員会の承認を得なければならない。

イ　被監査部門は，監査の実施に協力しなければならない。

（４）　外部委託事業者に対する監査

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

（５）　報告

情報セキュリティ監査統括責任者は，監査結果を取りまとめ，行政情報化推進委員会に報告する。

（６）　保管

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

（７）　監査結果への対応

ＣＩＳＯは，監査結果を踏まえ，指摘事項を所管する情報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。

（８）　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

行政情報化推進委員会は，監査結果を情報セキュリティポリシー及び関係

例規等の見直し，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。

2　自己点検

（1）　実施方法

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，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。

イ　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。

（2）　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，行政情報化推進委員会に報告しなければならない。

（3）　自己点検結果の活用

ア　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。

イ　行政情報化推進委員会は，この点検結果を情報セキュリティポリシー及び関係例規等の見直し，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。

3　情報セキュリティポリシー及び関係例規等の見直し

行政情報化推進委員会は，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　則

この基準は，市長決裁の日から施行する。

# 情報セキュリティインシデントにおける緊急時対応計画

令和４年３月

狛江市行政情報化推進委員会

目　　次

## 第１　総則

### １．目的

情報セキュリティインシデントは，情報資産に対する脅威が脆弱性により具現化することで，業務に影響を与え，市の情報セキュリティを脅かす事件・事故となる。

本計画は，狛江市情報セキュリティ対策基準第７第３項第１号に規定する緊急時対応計画として，情報セキュリティインシデント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，情報システム及びネットワークの情報セキュリティ対策を実施するために具体的な対処手順を定めることを目的とする。

### ２．情報セキュリティインシデント発生時における基本的事項

情報セキュリティ管理者は，情報セキュリティインシデントを認知した場合，次に掲げる対応を実施する。

（１）所管する情報システムにどの様な影響が発生しているか調査し，情報セキュリティインシデントの総合窓口であるＰＯＣ（情報政策課）に報告する。

（２）別紙「情報セキュリティインシデント判定基準」を参照し，情報セキュリティインシデント判定レベルがレベル２の場合には，「レベル２又はレベル１の情報セキュリティインシデント発生時の対応」に基づいて対処する。情報セキュリティインシデントの判定基準がレベル３の場合には，「緊急時対応計画」に基づいて対処する。

（３）対処完了後は，再発防止のため，様式「再発防止計画書」の記載事項に基づき，具体的予防策を検討し，統括情報セキュリティ責任者に対して報告する。

## 第２　レベル１又はレベル２の情報セキュリティインシデント発生時の対応

### １．初期対応

情報セキュリティ管理者は，情報セキュリティインシデント判定基準がレベル１又はレベル２の場合は，次のとおり対応する。

（１）物理的・環境的事故

職員等は，管理区域の出入口電子キーの故障，来訪者の不審行為又は不審物の発見等，執務室の情報セキュリティが担保されない環境を発見した場合は，直ちに情報セキュリティ管理者に連絡し対応を求める。

（２）技術的事故

ア　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停止を伴わない障害，防御された不正アクセス及び不正プログラムの感染又は侵入，対応可能な機器の故障及びソフトウェアの誤動作等が発生した場合は，直ちにＰＯＣ（情報政策

課）及び保守委託先の外部委託事業者に速やかに連絡し，対応を求める。

イ　ＰＯＣ（情報政策課）は，技術的な助言等を行うとともに情報セキュリティインシデント判定基準に基づき，必要に応じて統括情報セキュリティ責任者に報告する。

ウ　情報セキュリティ管理者は，情報セキュリティインシデントによる被害の拡大を防ぐため，ネットワーク及び情報システムの緊急停止が必要な場合には，ネットワーク及び情報システムの停止を実施する。この場合，統括情報セキュリティ責任者に報告する。

エ　情報セキュリティ管理者は，情報セキュリティインシデントによりネットワーク及び情報システムが使用不可能となった場合，手作業等による代替手段により事務作業を行うよう職員等に指導する。

（３）人的事故

ア　職員等は，端末やＩＤカード（職員証を兼ねるものを含む。）を紛失した場合は，直ちに情報セキュリティ管理者及びＰＯＣ（情報政策課）に連絡し，対応を求める。

イ　ＰＯＣ（情報政策課）は，技術的な助言等を行うとともに情報セキュリティインシデント判定基準に基づき，必要に応じて統括情報セキュリティ責任者に報告する。

２．復旧対応

（１）物理的・環境的事故

ア　来訪者の不審行為等の場合，情報セキュリティ管理者は直ちに現地に赴き，不審行為における対応を行う。不審行為を抑止できない場合には，警察に通報し，対応を委ねる。

イ　不審物の場合，情報セキュリティ管理者は直ちに現地に赴き，不審物の状況を確認する。危険性がある場合には，直ちに消防及び警察に通報し，対処を委ねる。

ウ　入退場を管理する電子的機器等の故障が発生した場合，管理区画を所管する情報システム管理者が現地に赴き確認を行う。必要に応じて専門業者に連絡し，修理等の対応を行う。

（２）技術的事故

ア　情報セキュリティインシデント判定基準に基づき，情報セキュリティ管理者及び統括情報セキュリティ責任者は，保守委託先である外部委託事業者と協力し，情報セキュリティインシデント発生の原因を特定する。

イ　情報セキュリティインシデント判定基準に基づき，情報セキュリティ管理者及び統括情報セキュリティ責任者は，原因が特定され，安全性が確認でき次第，システムを再起動させる。

（３）人的事故

ア　情報セキュリティ管理者は，職員等から端末やＩＤカード等を紛失した旨の報告を受けた場合，現行のアカウント及び資格情報を抹消し，新たなアカウント及び資格情報を付与する。情報セキュリティ管理者に付与権限がない場合については，統括情報セキュリティ責任者に報告し，指示を受ける。

イ　統括情報セキュリティ責任者は，必要に応じて付与権限のある情報システム管理者に現行のアカウント及び資格情報の抹消及び新規の付与を指示する。

ウ　情報セキュリティ管理者は，紛失した職員等に対して，新たな端末やＩＤカードを付与する場合，あらかじめ，必要に応じたセキュリティ教育を実施する。

３．事後対応

（１）情報セキュリティ管理者は，発生した緊急事態について，総務省様式１「インシデント報告書（IT 障害)」に基づき，記録を作成して保管する。

（２）情報セキュリティ管理者は，緊急事態が復旧した場合は，速やかに全職員に対して連絡する。

（３）情報セキュリティ管理者は，緊急事態の復旧後に，記録した総務省様式１「インシデント報告書（IT 障害)」に基づいて，再発防止策を検討し，統括情報セキュリティ責任者に報告する。

（４）統括情報セキュリティ責任者は，報告を受けた再発防止策に基づき，必要な措置を実施する。

## 第３　緊急時対応計画（準備）

１．想定する情報セキュリティインシデント

狛江市ＣＳＲＩＴが，本計画において対応する情報セキュリティインシデントは，別紙「インシデント判定基準」のレベル３に該当する場合（以下「緊急事態」という。）であるが，具体的な種別を表１に示す。ただし，自然災害，疫病，テロ，大規模な障害等により，全庁的に影響が発生し，業務の実施が困難な場合は，別途定めるＢＣＰ（業務継続計画）に従う。

表１　想定する情報セキュリティインシデント一覧

| 種　別 | 内　　容 |
|---|---|
| 障　害 | 機器故障等によるネットワーク又は情報システムの停止 |
| 事　故 | 情報漏えい等，パソコンや電子媒体の盗難，法令違反等 |

２．体制

本計画においては，迅速かつ機動的な対応を行うための体制を，狛江市情報セキュリティインシデントに関する緊急即応体制（ＣＳＩＲＴ）管理運営要綱第３条から第８条までに規定する所掌事項等に基づき，表２の緊急即応体制とする。

表２　緊急即応体制

| 狛江市ＣＳＩＲＴ | |
|---|---|
| 所掌事項<br>（１）インシデント情報の収集及び分析に関すること。<br>（２）インシデント対応の実施に関すること。<br>（３）平常時におけるインシデント発生の予防に関すること。<br>（４）その他インシデント関する重要事項に関すること。 | |
| ＣＳＩＲＴ責任者 | 本計画の責任者で企画財政部長をもって充てる。<br>計画の発動や終了の決定，要員招集等の全体的な指揮を担う。<br>また，所管課等に対して，情報資産や情報システム及びネットワークの運用状況の確認・連絡を行う。 |
| ＣＳＩＲＴ管理者 | 本計画においてインシデント対応のため，実務的な指揮者として企画財政部情報政策課長をもって充てる。<br>インシデントハンドラーを課内職員の中より指名し，インシデント対応の指示及び進行管理を担い，ＣＳＩＲＴ責任者に進行報告を行う。 |
| インシデントハンドラー | ＣＳＩＲＴ管理者が情報政策課職員の中から指名する。<br>ＣＳＩＲＴ管理者を補佐し，インシデント発生における速やかな対応にあたる。また，対応の進行状況等について，ＣＳＩＲＴ管理者に適宜報告し，その指示を受ける。<br>設備面：サーバやネットワーク機器，設備の被害状況を把握し，必要であれば予備機等への切り替えやバックアップデータの復旧等の手配を行う。<br>広報面：情報セキュリティ管理者等から情報を収集し，情報資産，情報システム及びネットワークの利用者に被害状況と普及作業の見通しをアナウンスする。 |
| ＣＳＩＲＴ事務局 | 情報政策課職員をもって充てる。 |
| 情報セキュリティ管理者<br>情報システム管理者 | 所管する情報資産，情報システム及びネット―ワークの状況について，ＣＳＩＲＴ責任者及びＣＳＩＲＴ管理者へ報告を行う。 |

３．予防対策

統括情報セキュリティ責任者は，表１の想定する情報セキュリティインシデントに対し，緊急時に即応できるように，図１に記載する連絡体制図に従って確実に行動ができるように次の予防対策を行う。

（１）連絡網の最新化

（２）重要な情報資産のバックアップ

（３）主要電子機器の代替機確保，又はそれに準ずる対策

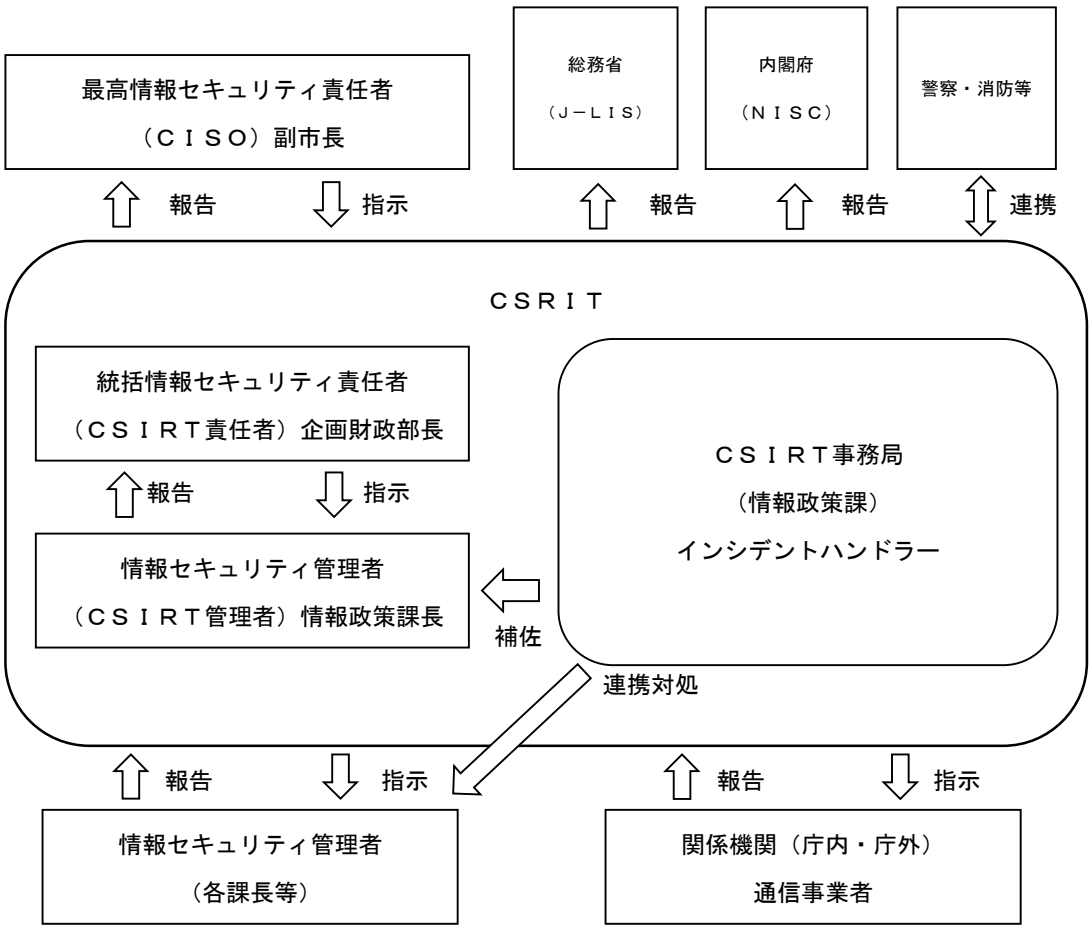



図１　連絡体制図

４．見直し

ＣＩＳＯ又は統括情報セキュリティ責任者は，次の場合，緊急時対応計画の見直しを検討し，必要に応じて改訂する。

（１）「業務継続計画（ＢＣＰ）」の変更

（２）想定する情報セキュリティインシデントの変更

（３）人事異動や組織の大幅な変更
（４）対象とする情報システムの構成変更
（５）準拠すべき法令等の施行，改正
（６）その他，ＣＩＳＯ又は統括情報セキュリティ責任者が必要と認める場合

第４　緊急時対応計画（行動計画）

緊急事態発生時の行動の大まかな流れは，図２のとおりとする。

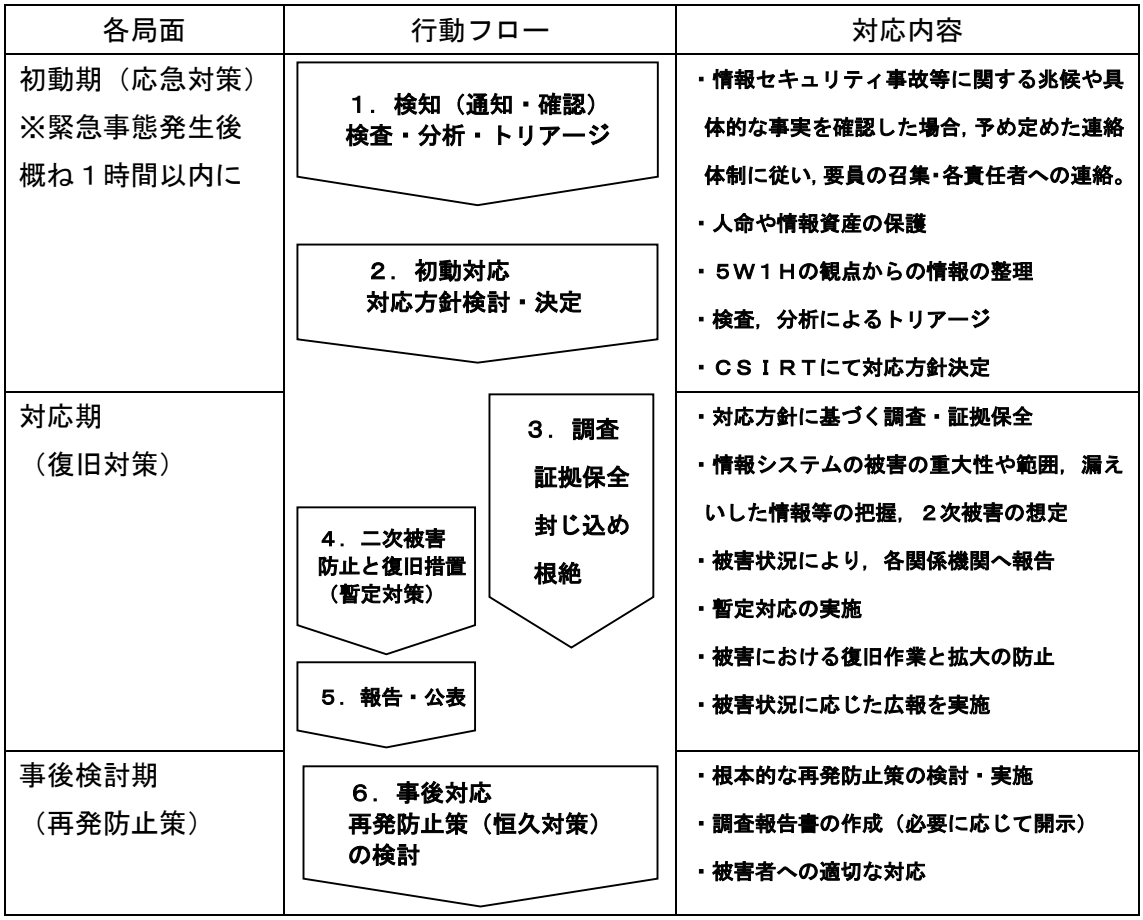



図２　緊急事態発生時の行動の流れ

第５　緊急時対応計画（初動）

初動期において，ＰＯＣ（情報政策課）は，緊急事態を検知した際，速やかにＣＳＩＲＴ責任者である統括情報セキュリティ責任者へ連絡し，要員の招集を行う。なお，ＣＳＩＲＴ責任者は，職員等及び関係者の安全確保を最優先し，その後復旧対策の実施に移るものとする。

１．ＣＳＩＲＴ責任者（統括情報セキュリティ責任者）への連絡

（１）職員等は，情報漏えい等の発生並びに情報システム及びネットワークの異常が発生した場合，情報セキュリティ管理者及びＰＯＣ（情報政策課）に内容を報告する。

（２）報告を受けたＰＯＣ（情報政策課）は緊急事態と認識した際にはＣＳＩＲＴ責任者へ連絡を行う。

（３）ＣＳＩＲＴ責任者と連絡が取れない場合，ＣＳＩＲＴ管理者である情報政策課長へ連絡する。連絡を受けたＣＳＩＲＴ管理者はＣＳＩＲＴ責任者と連絡が取れるまで，ＣＳＩＲＴ責任者の代理を行う。

（４）ＣＳＩＲＴ管理者と連絡が取れない場合，ＣＳＩＲＴ事務局である情報政策課職員に連絡する。連絡を受けた情報政策課職員はＣＳＩＲＴ責任者及びＣＳＩＲＴ管理者と連絡が取れるまで，ＣＳＩＲＴ責任者の代理を行う。

２．要員招集

（１）ＣＳＩＲＴ責任者は，緊急時対応計画を発動する上で，情報漏えい等の状況，情報システム及びネットワークの状況並びに緊急時対応計画の発動について，ＣＩＳＯに報告する。

（２）ＣＳＩＲＴ責任者は，様式「要員連絡先一覧」に基づき，緊急時対応計画の実施に関わる要員を招集する。なお，招集できない要員がいる場合には，要員に対する作業の割当内容を見直すとともに，必要に応じて他の職員等に対して応援を指示する。

３．初動期におけるインシデントハンドリングの流れ

（１）ＣＳＩＲＴ管理者は，招集後速やかに情報政策課職員の中よりインシデントハンドラーを指名し，初期対応の指示をする。

（２）インシデントハンドラーは，指名後速やかに担当部署へのヒアリング，ログ等の検査を実施し，当該緊急事態における情報を収集・整理するとともに，各インシデント事項の分析を行う。なお，ヒアリングについては正確な情報を得るため５Ｗ１Ｈを意識した質問事項を用意し実施する。

（３）インシデントハンドラーは，各インシデント事項の分析結果を基に被害状況と重要度に基づいてトリアージを行い，ＣＳＩＲＴ管理者へ報告する。なお，分析に当たっては，必要に応じて保守委託先の外部事業者と連携する。

（４）ＣＳＩＲＴ管理者はインシデントハンドラーの報告を基に，対応方針案を決定し，ＣＳＩＲＴ責任者へ報告する。

（５）ＣＳＩＲＴ責任者はＣＳＩＲＴ管理者の報告を基に対応方針を決定し，初動対応を実施するようＣＳＩＲＴ管理者に指示するとともに，ＣＩＳＯに報告する。

（６）インシデントハンドラーは，決定した対応方針に基づき，インシデントが発生した

機器等を特定し，詳細調査に必要となる次の証拠を同一ネットワーク上に保存することなく別途専用デバイスを用いて収集・確保する。該当機器の電源のオフやアンチウイルス・マルウェア対策ソフトによるスキャンにより，必要な情報が失われることがあることに留意して証拠保全を行う。なお，調査に当たっては，必要に応じて保守委託先の外部事業者と連携する。

ア　ディスクイメージ所得
イ　メモリイメージ取得
ウ　ウイルス・マルウェア等の検体の取得
エ　ファイアウォールログ
オ　プロキシサーバログ
カ　メールサーバログ
キ　ＤＮＳサーバログ
ク　その他必要なログなど

（７）インシデントハンドラーは，必要な証拠保全を行った後，インシデントが発生した機器等のネットワーク等からの隔離，アンチウイルス・マルウェア対策ソフトによるスキャンの実施，不正アクセスを受けたサイトや情報システムのネットワークからの切り離し及び停止，外部からのアクセス制限を行うなどの方法により，被害の拡大を防ぎ，緊急事態における影響範囲を最小化する。なお，必要に応じて保守委託先の外部事業者と連携する。

（８）インシデントハンドラーは，影響範囲の最小化後に，ウイルスやマルウェアの駆除，セキュリティパッチの適用，ユーザアカウントの削除・無効化，アクセス制御設定見直し等の実施により，緊急事態におけるインシデントの要素を排除する。なお，必要に応じて保守委託先の外部事業者と連携する。

（９）インシデントハンドラーは，（６）～（８）の実施に際して，必要に応じて対応状況をＣＳＩＲＴ管理者に報告する。また，初動対応を終了した時点で対応状況と復旧の見通し，情報漏えい等が確認された場合又はそのおそれがある場合はその影響範囲について，ＣＳＩＲＴ管理者に報告する。

(10) インシデントハンドラーから報告を受けたＣＳＩＲＴ管理者は，ＣＳＩＲＴ責任者に報告する。

(11) 初動対応が終了した時点で，ＣＳＩＲＴ責任者はＣＩＳＯに報告する。

４．人命や情報資産の保護

（１）ＣＳＩＲＴ責任者は，緊急時対応計画を発動する上で，人命が危機にさらされている場合は，人命の尊重を第一に考え，警察・消防への連絡等，必要な措置を講ずる。

（２）ＣＳＩＲＴ管理者は，情報漏えい等の発生又はその恐れがある報告を受けた際には速やかに被害状況を把握し，ＣＳＩＲＴ責任者に報告する。併せて，被害状況の庁外

への報告に備えるため，被害状況の整理をインシデントハンドラー以外の情報政策課職員に指示する。

（３）ＣＳＩＲＴ責任者は，緊急時対応計画を発動する上で，情報資産，情報システム及びネットワークに存在する機密性２以上の情報資産が漏えい，滅失及び毀損等の脅威にさらされている場合は，情報システム及びネットワークの緊急停止又は切断等の必要な措置を講ずる。なお，緊急停止等の措置を行う場合，保守委託先の外部委託事業者等のアドバイスを受けることができる。

（４）ＣＳＩＲＴ責任者は，情報システム及びネットワークを緊急停止又は切断する場合もしくは実施した場合，ＣＩＳＯに報告する。

## 第６　緊急時対応計画（復旧対策）

対応期においてＣＳＩＲＴ責任者は，情報漏えい等発生時の状況，機器・設備の被害状況等を把握し，外部専門家や外部委託事業者などと連携しつつ，必要な人的支援及び機器・設備を手配する。復旧に必要な，人員，対策，必要な機器・設備が準備でき次第，復旧作業を開始する。

### １．機器・設備損害調査

（１）インシデントハンドラーは，被害状況の把握を指示し，情報を収集するとともに，被害状況と復旧の暫定見通しをＣＳＩＲＴ管理者に報告する。また，必要に応じて障害の対象機器・設備について，代替機や交換部品の調達の手配やバックアップデータを早急に取り寄せる。

（２）インシデントハンドラーは，庁内ネットワークに障害の原因が存在する場合は，ＣＳＩＲＴ管理者へ報告し，その指示により，保守委託先の外部事業者等に連絡し，現在の状況や復旧の見通しを確認する。

（３）ＣＳＩＲＴ管理者は，復旧の見通しをＣＳＩＲＴ責任者に報告するとともに，ＣＳＩＲＴ責任者からの指示に基づき，情報漏えい等やシステムの被害状況，影響範囲，復旧の見通し等を関連機関（庁内・庁外）へ連絡するとともに，内外からの問い合わせに対応する。

### ２．暫定対応実施（情報システム及び機器等の場合）

（１）ＣＳＩＲＴ責任者は，正式な復旧手続が行われるまでに長時間を要することが予想される場合は，代替手段による運用の開始を，ＣＳＩＲＴ管理者へ指示する。

（２）ＣＳＩＲＴ管理者は，ＣＳＩＲＴ責任者の指示に基づき，代替手段として，予備機との切替えや予備回線との切替えを保守委託先の外部事業者等と協力して実施する。

（３）ＣＳＩＲＴ管理者は，代替手段による運用開始について，情報システム及び該当ネットワークの利用者に連絡するとともに，問い合わせに対応する。

３．復旧対応実施（情報システム及び機器等の場合）

（１）ＣＳＩＲＴ責任者は，原因を特定し，回復の目途がついた段階で，ＣＳＩＲＴ管理者に復旧開始を指示する。

（２）ＣＳＩＲＴ管理者は，各種情報システムや機器等のマニュアルに従い，保守委託先の外部事業者等と協力して，サーバやネットワーク機器等を復旧させるようインシデントハンドラーに指示する。

（３）インシデントハンドラーは，当該インシデントにより影響を受けた情報システムや機器等を次の内容で運用可能な状態に戻す。バックアップのリストアを行う際には，侵害される前のデータを用い，使用するバックアップ時点から侵害時までのデータについては消失するため，その期間を特定する。なお，必要に応じて保守委託先の外部事業者と連携する。

ア　バックアップからのリストア
イ　システムの再構築
ウ　侵害ファイルの復旧
エ　セキュリティパッチの適用
オ　アカウント情報の変更
カ　パスワード変更
キ　アクセス制限の強化
ク　障害が発生した機器の変更

（４）インシデントハンドラーは，リストア後にセキュリティパッチを適用し，アンチウイルス及びアンチマルウェア対策ソフトでフルスキャンを実施する。

（５）インシデントハンドラーは，バックアップを用いて復旧した際，消失したデータがある場合について期間を特定し，ＣＳＩＲＴ管理者に報告を行う。

（６）データの消失について報告を受けたＣＳＩＲＴ管理者は，ＣＳＩＲＴ責任者に報告を行うとともに，該当データの影響を受ける情報セキュリティ管理者に連絡する。

（７）データの消失について連絡を受けた情報セキュリティ管理者は特定した期間において発生した作業を洗い出し，再作成を行う。

４．回復連絡（情報システム及び機器等の場合）

（１）インシデントハンドラーは，サーバやネットワーク機器等を復旧した場合，稼働状況の確認を行い，ＣＳＩＲＴ管理者に報告する。なお，必要に応じて保守委託先の外部事業者と連携する。

（２）ＣＳＩＲＴ管理者は，情報システム及びネットワークの復旧について，ＣＳＩＲＴ

責任者に報告するとともに，関係機関（庁内・庁外）並びに情報システム及びネットワークの利用者に通知する。

（３）インシデントハンドラーは，情報システム及びネットワークが復旧した後も，サーバやネットワーク機器等の稼働状況が安定するまで監視する。なお，必要に応じて保守委託先の外部事業者と連携する。

５．二次被害の防止

（１）個人情報が漏えいした場合で，漏えいした情報に個人の機密情報（ＩＤ・パスワード等）が含まれている場合は，本人に連絡し，ＩＤの停止等の処置を実施してもらう。

（２）サイトへの誤公開，ブログ，掲示板への書込みなどサイト上に情報が公開された場合については，Ｗｅｂ検索サイト等にキャッシュの削除依頼を行い，検索結果に表示されないよう対処する。

（３）第三者に個人情報（電子ファイル等）が誤送信された場合は，当該人に対して，個人情報の破棄及び回収を行う。

６．個人情報漏えいによる報告・公表

個人情報漏えい等，市民に影響があるインシデントが発生し，ＣＩＳＯにより公表が必要であると判断された場合，狛江市公式ホームページ又は記者会見での公表を行う。

（１）透明性・開示の原則から，個人情報漏えいが発生した場合は速やかに公表を行う。

（２）公表する場合，事前に被害者や関係者に連絡し，公表の意向を確認する。

（３）問い合わせの窓口は一本化し，対外的な情報の整合性を確保する。

（４）狛江市公式ホームページで公表をする場合，公表用資料（次の内容を含む。）を掲載し，トップページからのリンク等で必要な情報について容易に閲覧ができるようにする。

ア　事故発生に関する状況報告

イ　事実経緯

ウ　調査方法及び状況

エ　漏えいした情報の内容

オ　事故の被害内容（二次被害の影響を含む。）

カ　事故原因

キ　当面の対応策

ク　再発防止策

ケ　問い合わせ窓口（事故に対する連絡先）

## 第７　事後検討期（再発防止策）

### １．原因調査・検証

発生した緊急事態に関して，回復後にその内容を詳細に検証し，設計や運用の見直しも含めて再発防止策の検討材料とする。

（１）ＣＳＩＲＴ責任者は，復旧作業後に関係者と協力し，情報漏えい等並びに情報システム及びネットワークに関する緊急事態の原因について，ＣＳＩＲＴ管理者に対して調査分析により明らかにするよう指示する。

（２）ＣＳＩＲＴ管理者は，緊急事態に対応したインシデントハンドラーとともに，原因調査に際して，次の内容について整理する。

ア　発生原因・兆候

イ　対処の経緯

ウ　緊急事態の特性・被害内容

（３）ＣＳＩＲＴ管理者は，原因調査を行う場合，影響が及ぶシステムの担当部署以外に，必要に応じて外部の専門組織（保守委託先の外部事業者，政府系機関（情報セキュリティを所管），警察，セキュリティコンサルタント等）と連携する。

（４）ＣＳＩＲＴ管理者は，原因調査・検証に基づき，再発防止策案をまとめ，総務省様式１「インシデント報告書（ＩＴ障害)」，又は総務省様式２「インシデント報告書（情報漏えい)」に基づきＣＳＩＲＴ責任者へ報告する。

### ２．再発防止及び公表

同様の緊急事態の再発を防止し，又は被害の発生を最小限に食い止めるため，検証結果に基づき，緊急事態の再発防止策を検討するとともに，当該事案について公表する。

（１）ＣＳＩＲＴ責任者は，明らかにした緊急事態の発生原因から，情報資産，情報システム及びネットワークを保護するため，再発防止策を検討する。なお，再発防止策については，費用対効果を考慮し，有効な対策を選択する。

（２）ＣＳＩＲＴ責任者は，緊急事態の再発防止策を検討する場合，次の内容について検討する。

ア　発生原因の排除

イ　発生の兆候への早期対応

ウ　被害軽減対策の実施

エ　対応体制の整備

オ　関係者・機関に対する研修の実施

カ　記録の作成

キ　有効な未然防止策の検討

（３）ＣＳＩＲＴ責任者は，再発防止策について，様式「再発防止計画書」により行政情

報化推進委員会に報告し，承認を得なければならない。

（４）ＣＳＩＲＴ責任者は，承認を得た再発防止策について，速やかに実施する。

（５）ＣＳＩＲＴ責任者は，承認を得た様式「再発防止計画書」を総務省様式１「インシデント報告書（ＩＴ障害)」，又は総務省様式２「インシデント報告書（情報漏えい)」とともに保管する。

（６）ＣＩＳＯは，当該事案の事実関係，発生原因，影響範囲及び再発防止策について，その影響範囲を見極めながら，速やかに公表する。

別紙

情報セキュリティインシデント判定基準

| | | レベル１ | レベル２ | レベル３ |
|---|---|---|---|---|
| 判定 | | セキュリティ事故とはしない | セキュリティ事故とする | |
| 基準 | | ・一時的にリスクとして想定した事象が発生した状態で，実害がほとんどないもの，又は計画されたもの<br>・定められた対策を遵守していない状態で事故とは呼べないもの<br>・情報システム又はサービスにセキュリティ的な脆弱性又はその疑いがあるもの | ・事故による影響が軽微なもの<br>・復旧に特別な対応を必要としないもの<br>・ネットワークに対する外部からの攻撃でシステム的に防御されたもの | ・情報漏えい等が実際に発生した場合<br>・長期間のシステム停止等，可用性に重大な影響が発生した場合<br>・外部からの攻撃により被害が発生した場合 |
| 事件事故の種類・例 | 物理・環境的事故 | ・来訪者受付ミス<br>（職員が了解しているもの）<br>・建物内各種設備の点検等による停止，一部故障又はメンテナンス<br>・職員在室時の入口開放状態<br>・収納庫等の破損<br>・上記以外で軽微な問題がある時 | ・入口電子キー故障<br>・来訪者の事務室内の不審行為<br>・不審物の発見 | ・不審者の侵入<br>・運営に支障をきたすレベルの物理的・環境的障害 |
| | 電子的事故 | ・メンテナンス等による計画的なネットワーク，サービス停止<br>・クライアント端末への定められた管理策の未実施（パスワード設定等）<br>・限られた範囲でのデータの紛失・誤った変更（復旧可能）<br>・上記以外に情報システム又はサービスのセキュリティに弱点又はその疑いがある時 | ・ネットワーク又はハード障害で概ね２時間以内に回復（ただし障害の原因が明らかに外部からの攻撃の場合はレベル３とする）<br>・システムにより防御された不正アクセスや，ウイルスメール等の不正プログラム対策ソフトウェアでの防御<br>・機器（クライアント又はネットワーク機器等）の故障で，代替機等により対応可能なもの<br>・組織内システムの軽微なバグ<br>・ソフトウェアの誤動作 | ・回復の見込みの立たないネットワーク障害<br>・外部からの攻撃によるサーバ等停止<br>・サーバ又はクライアントのコンピュータウイルス，マルウェア感染<br>・情報資産の大量喪失又は改ざん（故意・過失，復旧の可否を問わず） |
| | 人的事故 | ・離席による情報放置<br>・職員証不携帯<br>・共有スペースでの業務に関する会話<br>・上記以外に軽微な問題がある時 | ・業務用携帯電話等の紛失<br>・職員証の盗難又は紛失 | ・情報漏えい等（故意又は過失を問わず）<br>・法令違反<br>・端末や電子媒体等の盗難又は紛失 |
| 対応 | | ・必要に応じて注意喚起等<br>・情報システム又はサービスに脆弱性又はその疑いがある場合は個別のシステムは所管する情報システム管理者へ報告，全庁的なものについてはＰＯＣ（情報政策課）へ報告 | ・インシデント報告書の作成<br>・ＰＯＣ（情報政策課）へ報告 | ・インシデント報告書の作成<br>・ＰＯＣ（情報政策課）へ報告<br>・緊急時対応計画又は業務継続計画により対処 |

＜様式＞

# 再　発　防　止　計　画　書

行政情報化推進委員会
　委員長　　様

年　　月　　日
統括情報セキュリティ責任者

以下の通り再発防止策を検討しましたので承認をお願いいたします。

| | |
|---|---|
| 今回の緊急事態の概要 | |
| 発生組織<br>**（システム名もしくは課名を記載）** | |
| 原因 | |

■再発防止策について

| | | | |
|---|---|---|---|
| 対応方針 | **※原因排除，早期対応，被害軽減策の視点から記載のこと** | | |
| 対応策 | 内容 | | 計画 |
| | １ | | |
| | ２ | | |
| | ３ | | |
| | ４ | | |
| その他 | | | |

＜様式＞

要員連絡先一覧

| 担当名 | 所属部署・役職 | 内線番号 | 緊急連絡先 |
|---|---|---|---|
| ＣＩＳＯ | 副市長 | | |
| 統括情報セキュリティ責任者 | 企画財政部長 | | |
| 事務局（情報政策課） | 情報政策課長 | | |
| | 情報政策課情報政策係長 | | |
| | 情報政策課情報政策係員 | | |
| | 情報政策課情報政策係員 | | |
| | 情報政策課情報政策係員 | | |
| | 情報政策課情報政策係員 | | |
| 行政情報化推進委員会 | 総務部長 | | |
| | 政策室長 | | |
| | 財政課長 | | |
| | 職員課長 | | |
| 庁舎管理 | 総務課長 | | |
| | | | |

＜様式＞

構築・保守等外部事業者連絡先一覧

| システム・機器・設備 | 数量 | 事業者名 | 担当者名 | 緊急連絡先 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

（地方公共団体→総務省）

# インシデント報告書（IT障害）

（第　　報*）

※1：(*が付与された項目は必須事項)

**情報連絡日時*** 　　年　　月　　日

| | | | | |
|---|---|---|---|---|
| **情報連絡元*** | 団体名 ： | | 担当者名 ： | |
| | 部局名 ： | | | |
| | 電話番号 ： | | FAX番号 ： | |
| | 電子メールアドレス ： | | | |

## ①発生した事象の分類 （別紙参照）

| 事象の類型 | | 事象の例 | チェック（1つのみ選択(※2)） |
|---|---|---|---|
| 未発生の事象 | | 予兆・ヒヤリハット | ☐ |
| 発生した事象 | 機密性を脅かす事象 | 情報の漏えい<br>（組織の機密情報等の流出など） | ☐ |
| | 完全性を脅かす事象 | 情報の破壊<br>（Webサイト等の改ざんや組織の機密情報等の破壊など） | ☐ |
| | 可用性を脅かす事象 | システム等の利用困難<br>（制御システムの継続稼働が不能やWebサイトの閲覧が不可能など） | ☐ |
| | 上記につながる事象(※3) | マルウェア等の感染<br>（マルウェア等によるシステム等への感染） | ☐ |
| | | 不正コード等の実行<br>（システム脆弱性等をついた不正コード等の実行） | ☐ |
| | | システム等への侵入<br>（外部からのサイバー攻撃等によるシステム等への侵入） | ☐ |
| | | その他 | ☐ |

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

## ②上記事象における原因の分類 （別紙参照）

| 原因の類型 | 原因 | チェック（複数選択可） |
|---|---|---|
| 意図的な原因 | 不審メール等の受信 | ☐ |
| | ユーザID等の誤り | ☐ |
| | DoS攻撃等の大量アクセス | ☐ |
| | 情報の不正取得 | ☐ |
| | 内部不正 | ☐ |
| | 適切なシステム運用等の未実施 | ☐ |
| 偶発的な原因 | ユーザの操作ミス | ☐ |
| | ユーザの管理ミス | ☐ |
| | 不審なファイルの実行 | ☐ |
| | 不審なサイトの閲覧 | ☐ |
| | 外部委託先の管理ミス | ☐ |
| | 機器等の故障 | ☐ |
| | システムの脆弱性 | ☐ |
| | 他分野の障害からの波及 | ☐ |
| 環境的な原因 | 災害や疾病等 | ☐ |
| その他の原因 | その他 | ☐ |
| | 不明 | ☐ |

◆情報連絡の内容(※4)　（別紙有無*：☐有　☐無 ）

<table>
<tr><th>項　目</th><th>情報の内容</th></tr>
<tr><td>③分野名*(※5)</td><td>政府・行政サービス分野</td></tr>
<tr><td>④事象が発生した重要インフラ事業者等名</td><td></td></tr>
<tr><td>⑤概　要</td><td>判明日時：　　年　月　日　時　分<br>（発生日時：　　年　月　日　時　分 ）<br>事象が発生したシステム・委託先：<br><br>発生事象の概要：<br><br><br><br>システムの稼働状況：☐影響なし　☐停止中　☐一部稼働中　☐復旧済</td></tr>
<tr><td>⑥重要インフラサービス等への影響</td><td>重要インフラサービスのサービス維持レベル(※5)逸脱の有無：☐有　☐無<br>他の事業者等への波及の可能性：☐有　☐無</td></tr>
<tr><td>⑦当該事象に係る推移等</td><td>
<table>
<tr><th>日時</th><th>事象・対応状況等</th></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
（補足情報）<br><br><br><br>対外的な対応状況<br>報道発表、報道等への掲載：☐済　☐予定有　☐無　（済・予定有では日時・件名を記入）<br><br>NISC以外に連絡を行った先：</td></tr>
<tr><td>⑧今後の予定</td><td>☐事象継続中 （続報あり）<br>☐事後調査実施中 （続報あり）<br>☐今後の対応策を継続検討 （続報なし）<br>☐対応完了 （続報なし）</td></tr>
<tr><td>⑨その他<br>・得られた教訓等</td><td></td></tr>
</table>

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「重要インフラの情報セキュリティ対策に係る第3次行動計画」に定める「分野名」、「サービス維持レベル」を指す。

様式２

# インシデント報告書（情報漏えい）

【情報連絡日時】：　令和　　年　　月　　日（第　　報）　【団　体　名】：＿＿＿＿＿＿

【部　局　名】：＿＿＿＿＿＿　【担 当 者 名】：＿＿＿＿＿＿

【電 話 番 号】：＿＿＿＿＿＿　【ＦＡＸ 番 号】：＿＿＿＿＿＿

【電子メールアドレス】：＿＿＿＿＿＿

【流出の区分】：

・USB メモリ等記録媒体や書類等の紛失　・USB メモリ等記録媒体や書類等の盗難

・Winny 等のファイル共有ソフトの利用による流出　・メールの誤送信による流出

・その他（　　）

【事案が発生した団体名】

【流出元】

・当該団体　・委託先　・再委託先　・その他（　　）

【流出させた者】

・職員（従業員）　・第３者　・不明（調査中）　・その他（　　）

【流出に係る経過】

・令和　　年　　月　　日発生　・令和　　年　　月　　日発覚　・令和　　年　　月　　日公表

【事案の概要】（流出した契機）

【流出した個人情報の概要と件数】

（情報概要）

（流出件数）

【被害状況】

【事案発生の原因】

【流出した個人情報の本人への対応】

【組織の対応】（再発防止策等）

【警察への連絡状況】（連絡先部署名及び電話番号を記載）

【インシデント報告送信先】（報告は可能な限り LGWAN メールにてお願いします）

メール：lg-security@soumu.go.jp　ＦＡＸ：03-5253-5529　ＴＥＬ：03-5253-5525

# 記載要領

※【情報連絡日時】・・・漏えいが発生したら（市区町村から報告を受けたら）まず「第１報」として、その時点で知り得た情報のみを報告し、その後詳しいことが判明し次第「第２報」「第３報」として報告すること（第２報以降は追記箇所がわかるように朱書きにする）

※【流出の区分】・・・該当するものを〇で囲むこと。該当がなければ「その他」に記載すること

※【流出が発生した団体名】・・・市区町村、地方独立行政法人等で流出が発生した場合は、発生団体名を必ず記載すること。関係団体が複数に及ぶ場合はすべて記載すること。県、市区町村ともに同一被害（システムの共同利用など）の場合は併記すること

※【流出元】・・・該当する区分を〇で囲むこと。該当がなければ「その他」に記載すること

※【流出させた者】・・・該当する区分を〇で囲むこと。該当がなければ「その他」に記載すること

※【警察への連絡状況】・・・被害届の提出若しくは電話連絡の有無、提出（連絡）日時、連絡先部署名と電話番号を記載すること

# 外部サービス利用基準

令和４年３月24日
情報政策課

（趣旨）

第１条　この基準は，狛江市情報セキュリティポリシー対策基準「第８　外部委託」中の２及び３にある外部サービスの利用に関して必要な事項を定めるものとする。

（外部サービスの種類）

第２条　外部サービスとは，次に掲げるものをいう。

（１）　クラウドサービス

（２）　Ｗｅｂ会議サービス

（３）　ＳＮＳ（ソーシャルネットワークサービス）

（４）　検索サービス，翻訳サービス，地図情報サービス

（５）　ホスティングサービス

（６）　前各号に掲げるもののほか，狛江市情報セキュリティポリシー対策基準第１「組織体制」の１に規定する最高情報セキュリティ責任者（ＣＩＳＯ）である副市長が認めるもの

（利用可能な業務及び範囲）

第３条　外部サービスの利用については，法令等で個人情報及び情報資産の取扱いについて，外部サービスの利用が禁じられている以外の業務及び範囲とする。民間事業者等が不特定多数の利用者に対して提供するＳＮＳ等の画一的な約款，規約等への同意のみで利用可能となる外部サービスについては，機密性２以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから，原則として利用することはできない。

（選定基準）

第４条　機密性２以上の情報を取り扱う外部サービス提供者の選定基準は，次に掲げるとおりとする。

（１）　外部サービスを利用する所管部署の求める仕様・要件定義を全て満たしていること。

（２）　システム開発フェーズから，運用，廃棄に至るまでのシステムライフサイクルを通じた費用が低廉であること。

（３）　個人情報・情報資産等の取扱い，情報セキュリティインシデント対応等について，ＩＳＭＳ認証の国際規格，ＩＳＭＡＰの管理基準等を満たしていること。

（４）　市が意図しない変更が加えられないことを保証する管理が，一貫した品質保証体制の下でなされていること。

（５）　外部サービスにおけるデータセンターの物理的所在地が日本国内であること。

（６） 外部サービスにおけるデータセンターについて，利用するサービス形態から適正なデータファシリティスタンダードが適用されていること。

（７） 一切の紛争は日本の裁判所が管轄するとともに，契約の解釈が日本の国内法に基づくものであること。

２ 機密性２以上の情報を取り扱わないときは，前項各号に掲げる基準に準じて外部サービス提供者を選定するものとする。

（利用申請）

第５条 外部サービスを利用しようとする所管課は，狛江市電子計算組織管理運営規則（昭和63年規則第13号。以下「規則」という。）第15条の２第１項に規定する電子計算組織処理計画書を規則第３条第１項に規定する電子計算組織総括管理者（以下「総括管理者」という。）に提出しなければならない。

（利用許可）

第６条 前条の規定により提出を受けた総括管理者は，その内容を狛江市行政情報化推進委員会設置要綱（平成11年要綱第60号）に基づき設置する狛江市行政情報化推進委員会（以下「情報化推進委員会」という。）に諮るものとする。

２ 情報化推進委員会は，外部サービスの利用に関して審議し，利用の可否を判断するとともに，利用を可とした外部サービス提供者については承認済外部サービスとして記録する。

（利用状況の報告）

第７条 情報化推進委員会は，外部サービスを利用する所管課に対して外部サービスの利用状況の報告を求めることができる。

# 狛江市パソコン等の外部持ち出しに関する要綱

令和４年３月22日
要綱第20号

（目的）

第１条　この要綱は，職員がパソコン等を外部に持ち出すときの手続，遵守事項その他必要な事項を定めることを目的とする。

（定義）

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

（１）　職員　一般職の職員，再任用職員及び会計年度任用職員

（２）　外部　庁舎その他市の施設以外の場所

（３）　パソコン等　日常的に職員がＬＧＷＡＮ接続系ネットワークで使用する情報端末及び在宅勤務，研修のために職員に貸し出す情報端末

（４）　情報セキュリティ管理者　対策基準第１「組織体制」の４に規定する情報セキュリティ管理者である各課の課長相当職

（持ち出し許可）

第３条　職員は，次に掲げる用途に該当し，次項に規定する持ち出しの許可を得たときに限り，外部でパソコン等を使用することができる。

（１）　在宅勤務

（２）　職員研修

（３）　管理職が外部においてパソコン等を用いて連絡し，又は指示する必要がある場合

（４）　前３号に掲げるもののほか，職員が外部で業務を行うに当たり，パソコン等の使用に相当の理由があると情報政策課長が認める場合

２　業務遂行においてパソコン等を外部へ持ち出す職員は，事前に情報セキュリティ管理者に許可を得た上で，情報政策課長に庁内グループウエアにより申請し，持ち出しの許可を得なければならない。

３　情報政策課長は，使用状況等を鑑み，必要に応じて前項に規定する持ち出しの許可を解除することができる。

４　職員は，パソコン等を外部へ持ち出して業務を遂行する必要がなくなったときは，速やかに本来の設置場所に戻さなければならない。

（遵守事項）

第４条　パソコン等を使用して外部で業務を行う職員は，次に掲げる事項を遵守し，善良なる管理者の注意をもって当該端末を管理し，及び運用しなければならない。

（１）　パソコン等を業務の範囲外の用途に使用しないこと。

（２）　常にパソコン等を自身の管理下に置くとともに，使用時においても，画面等を他者に閲覧されることにより情報資産の流出等がないようにすること。

（３） 情報セキュリティに関連する規程について，最新の内容を十分に理解すること。

（４） パソコン等が紛失し，又は盗難に遭ったときは，直ちに情報政策課長及び情報セキュリティ管理者に報告し，情報セキュリティ管理者は情報政策課長の指示に従うこと。

（緊急措置）

第５条　情報政策課長は，市の情報資産の保護のために必要なときは，職員が所持するパソコン等とＬＧＷＡＮ接続系ネットワークとの接続を強制的に解除することができる。

（委任）

第６条　この要綱に定めるもののほか必要な事項は，市長が別に定める。

付　則

（施行期日）

１　この要綱は，公布の日から施行する。

（狛江市職員の在宅勤務に用いるパソコン端末の貸出しに関する要綱の廃止）

２　狛江市職員の在宅勤務に用いるパソコン端末の貸出しに関する要綱（令和３年要綱第２号）は，廃止する。

（狛江市職員の在宅勤務の実施に関する要綱の一部改正）

３　狛江市職員の在宅勤務の実施に関する要綱（令和３年要綱第１号）の一部を次のように改正する。

| 改　正　後 | 改　正　前 |
| --- | --- |
| （使用端末）<br>**第９条**　在宅勤務中に使用する端末は，狛江市パソコン等の外部持ち出しに関する要綱（令和４年要綱第20号）第３条第２項の規定により持ち出しの許可を受けた端末又は狛江市在宅勤務に係る私的パソコン等の取扱いに関する要綱（令和４年要綱第19号）第４条第１項の規定により使用の許可を受けた私的パソコン等（以下「自宅パソコン」という。）とする。 | （使用端末）<br>**第９条**　在宅勤務中に使用する端末は，狛江市職員の在宅勤務に用いるパソコン端末の貸出しに関する要綱（令和３年要綱第２号）に基づき貸出しを受けた端末又は，職員が所有するウイルス対策ソフトウェアが有効なパソコン（以下「自宅パソコン」という。）を使用することとする。<br><br>２　自宅パソコンで作成したファイルは，所属のメールアドレスへの送信その他可能な方法により，市で管理するサーバ等に保存することとし，作業中の一時的な保存を除き，自宅パソコン等には保存してはならない。 |

| 改　正　後 | 改　正　前 |
| --- | --- |
| | 3　自宅パソコンから所属のメールアドレスに送信したファイルを，職場で受信する際には，メール無害化サービスの使用や，ウイルスの手動検索など，必要なセキュリティ対策を行うものとする。 |

# 狛江市在宅勤務に係る私的パソコン等の取扱いに関する要綱

令和４年３月22日
要綱第19号

（趣旨）

第１条　この要綱は，狛江市職員の在宅勤務の実施に関する要綱（令和３年要綱第１号）に基づく在宅勤務（以下「在宅勤務」という。）で使用する私的パソコン等の取扱いに関して必要な事項を定めるものとする。

（定義）

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

（１）　職員　狛江市職員の在宅勤務の実施に関する要綱第２条第１項各号に掲げる職員

（２）　私的パソコン等　職員が私的に所有する情報端末で，ウイルス対策ソフトが有効なもの

（３）　自治体テレワークシステム　地方公共団体情報システム機構が提供する自治体テレワークシステム

（４）　統括情報セキュリティ責任者　狛江市情報セキュリティポリシー対策基準（以下「対策基準」という。）第１「組織体制」の２に規定する統括情報セキュリティ責任者である企画財政部長

（５）　情報セキュリティ管理者　対策基準第１「組織体制」の４に規定する情報セキュリティ管理者である各課の課長相当職

（対象）

第３条　この要綱は，在宅勤務を行う職員に適用する。

２　市の業務委託を受けて，市の情報システムに接続する外部委託事業者等は，私的パソコン等から市の情報システムへ接続することは，統括情報セキュリティ責任者の許可がある場合を除き禁止とする。

（使用許可）

第４条　私的パソコン等を使用して在宅勤務を行う職員は，事前に情報セキュリティ管理者に許可を得た上で，情報政策課長に庁内グループウエアにより申請し，使用の許可を得なければならない。

２　情報政策課長は，使用状況等を鑑み，必要に応じて前項に規定する使用の許可を解除することができる。

３　職員は，業務遂行のために私的パソコン等を追加で使用する必要が生じたときは，第１項に規定する許可を受けなければならない。

４　職員は，業務遂行において私的パソコン等を使用する必要がなくなったとき，又は使用の許可を受けている私的パソコン等を廃棄するときは，庁内グループウエアにより情報政策課長に届け出なければならない。

５　前項に規定する届出を行った職員は，自治体テレワークシステムの使用のた

めに私的パソコン等に登録されている情報を全て消去しなければならない。
６　職員は，機種変更等の事由により業務遂行において私的パソコン等を変更するときは，庁内グループウエアにより変更の手続を行わなければならない。
７　統括情報セキュリティ責任者は，私的パソコン等で使用するアプリケーション等について，必要に応じて業務での使用を許可することができる。
（遵守事項）
第５条　私的パソコン等で在宅勤務を行う職員は，次に掲げる事項を遵守しなければならない。
（１）　私的パソコン等のセキュリティソフトは，最新のバージョンを適用させること。
（２）　許可を受けたアプリケーション等の使用及び自治体テレワークシステムの接続に必要なＩＤ及びパスワードは，職員以外の者が自治体テレワークシステムに接続しないように厳格に管理すること。
（３）　許可を受けたアプリケーション等の使用及び自治体テレワークシステムに接続しているときは，常に私的パソコン等を自身の管理下に置くとともに，使用時においても，画面等を他者に閲覧されることにより情報資産の流出等がないようにすること。
（４）　情報セキュリティに関連する規程について，最新の内容を十分に理解すること。
（５）　業務で使用する情報とプライベートで使用する情報を明確に分けること。
（６）　業務で取得し，又は作成した情報を私的パソコン等には保存しないこと。
（７）　私的パソコン等が紛失し，又は盗難に遭ったときは，直ちに情報政策課長及び情報セキュリティ管理者に報告し，情報セキュリティ管理者は情報政策課長の指示に従うこと。
（監査）
第６条　私的パソコン等で市の情報システムに接続する職員は，統括情報セキュリティ責任者の求めがあったときは，情報セキュリティ等の規程等に係る適用状況について，監査を受けなければならない。
２　私的パソコン等で市の情報システムに接続する職員は，監査において，デバイスの安全性及び設定状態，業務情報の保存状態の開示並びにこれらを確認するための操作に協力的に対応しなければならない。
（緊急措置）
第７条　情報政策課長は，市の情報資産の保護のために必要なときは，使用の許可を受けたアプリケーション等の停止及び私的パソコン等の市と自治体テレワークシステムの接続を解除することができる。
２　私的パソコン等の取扱いについて情報政策課長が処理に関する指示を行ったときは，職員は当該指示に従って私的パソコン等に処理を行わなければならない。
（委任）
第８条　この要綱に定めるもののほか必要な事項は，市長が別に定める。

付　則

この要綱は，公布の日から施行する。

# Ｗｅｂ会議サービス運用マニュアル

令和４年３月24日
情報政策課

（目的）

第１条　本運用マニュアルは，狛江市情報セキュリティポリシー対策基準「第６技術的セキュリティ」の「１　コンピュータ及びネットワークの管理」中の「(21)　Ｗｅｂ会議サービスの利用時の対策」に基づき，Ｗｅｂ会議サービスを利用する際の取扱いと情報管理を規定し，Ｗｅｂ会議サービス利用時の情報セキュリティの維持・向上並びに業務効率の向上を図ることを目的とする。

（対象）

第２条　本運用マニュアルの対象者は，Ｗｅｂ会議サービスを使用する市職員及び会計年度任用職員（以下「職員等」という。）とする。

（サービス利用に係る留意事項）

第３条　職員等は，Ｗｅｂ会議サービスを利用するに当たっては，会議用庁内端末において，用意されている次に掲げるサービスを利用しなければならない。

（１）　ＣｉｓｃｏＷｅｂｅｘＭｅｅｔｉｎｇ

（２）　ＺＯＯＭ

（３）　ＭｉｃｏｒｏｓｏｆｔＴｅａｍｓ

２　前項の規定にかかわらず，やむを得ず，同項各号に掲げるＷｅｂ会議サービス以外のものを利用するときは，次に掲げる事項について留意しなければならない。

（１）　会議データの所在

ア　Ｗｅｂ会議サービスは，音声，映像，共有，資料，チャット，録画・録音データ等，多種のデータを扱うことから，これらのデータがどこに格納されるかは，情報漏えいリスクに大きく影響することとなる。主催者として使用するときは，そのＷｅｂ会議サービスがクラウドサービス，オンプレミス等，どの様な形態となってるかを確認すること。

イ　クラウドサービスのときは，負荷分散のため海外のデータセンターが利用されることがあることから，データセンターが置かれた国によっては，政府が法に基づきデータを強制的に取得するリスクが発生することを理解すること。

ウ　クラウド上に録画・録音データを保存するときは，復元不可能な形で完全削除ができるか（セキュアデリート機能の有無）を確認すること。

（２）　暗号化

ア　通信経路が安全でないと認められるときは，重要な会議データの盗聴又は改ざんの脅威が発生することを理解すること。

イ　Ｗｅｂ会議サービス提供者（以下「サービス提供者」という。）が暗号鍵を持つのか否かを確認し，Ｗｅｂ会議サービスがサービス提供者が暗号

鍵を持たないエンドツーエンド暗号化か，サービス提供者が暗号鍵を持ち会議データがサーバで復号可能な方式かを確認すること。

ウ　エンドツーエンド暗号化のときは，会議参加者の音声・映像データが参加者端末で暗号化され，他の参加者端末で復号することとなること。暗号鍵は，参加者のみが保有するため，サービス提供者は復号できなくなることを理解すること。

エ　サービス提供者が暗号鍵を持つときは，サービス提供者が信頼できるとしても，海外には政府によるサーバのデータの強制取得の可能性があることを理解すること。

オ　Ｗｅｂ会議サービスがエンドツーエンド暗号化とそれ以外の両方の動作モードを持つときは，エンドツーエンド暗号化を選択するとサーバでの復号を必要とする機能は使えなくなる可能性があることから，制限事項を事前に確認すること。

カ　サービス提供者のホームページ等で，安全性が確認されている暗号アルゴリズム又は通信方式が採用されているかを確認すること。

（３）　会議参加者の確認・認証方式

ア　意図しない者が会議に参加することにより，会議進行の妨害又は機密情報の漏えいが発生することから，意図しない者の会議への参加を防ぐため，会議案内メールの安全な経路での配布するとともに，会議参加者の確認・認証方式の選定を行うこと。

イ　会議参加者の確認会議参加者の確認・認証方式に関しては，会議パスワード設定機能，待機室（ロビー）での参加者確認機能，参加者の事前登録機能，参加者名の設定機能，二要素認証等，各種メニューが用意されていることから，主催する会議の機密性，参加人数等に応じた最適な方式の選択をすること。

ウ　主催者が，誰が参加しているかを容易に確認でき，万が一の場合には参加者を強制退室できる機能があること。

（４）　プライバシーポリシー

Ｗｅｂ会議サービスでは音声・映像，参加者のメールアドレス等の属性等，様々な個人情報を扱うことから，これら個人情報が会議目的以外で第三提供を含め使用されないこと，個人情報の保護に関する規程の規制に準拠していることを確認すること。

（５）　脆弱性及び企業姿勢

ア　サービス提供者のウェブサイト，ニュース等の脆弱性情報を確認し，Ｗｅｂ会議サービスの脆弱性の発生状況，対策状況を把握すること。

イ　サービス提供者のセキュリティに対する取組及び情報公開に関する対応が重要であることから，各サービス提供者のウェブサイト等で，一般の利用者にも分かりやすいセキュリティ上の注意事項等，最新のセキュリティ対策状況が公開されているかを確認すること。

（会議開催に係る留意事項）

第４条　Ｗｅｂ会議サービスを利用して会議を開催するために留意すべき点は，次に掲げるとおりとする。

（１）　会議の準備

ア　会議の機密性の確認

（ア）　会議の機密性を確認すること。

（イ）　セミナー・講演会への参加と，個人情報又は機密情報を扱う会議では，会議の機密性が異なることから，それぞれに応じ最適な会議の開催方法を選択すること。

イ　会議の機密性に応じた開催方法の決定

（ア）　エンドツーエンド暗号化の会議を利用できないときは，サーバで復号化される場合のリスクが許容可能か確認すること。

（イ）　主催した会議の参加者に外部組織の者がいるときは，各組織のセキュリティポリシーに準拠しているかについての参加者の同意を得ること。

（ウ）　主催した会議に参加できる者の制限を明確にし，参加の設定を適切に行うこと。

（エ）　内容から非公開とすべきときは，会議を非公開に設定にすること。

（オ）　意図しない参加者を避けるため，会議パスワードを設定し，待機室機能を有効にすること。

（カ）　参加者の入室時に許可する機能（主催者以外全員ミュート状態等）を確認すること。

（キ）　会議の機密性，会議参加者の人数に応じ，会議案内メールと別経路での会議パスワードの送付，参加者の二要素認証，参加者の事前登録機能等を適切に使用すること。

（ク）　万が一意図しない参加者が登場した場合に備え，参加者の強制退室機能が使えることを確認すること。

ウ　Ｗｅｂ会議サービスの開催案内

（ア）　会議ＵＲＬ，パスワード等を記載した会議開催案内の送付は，安全な経路で行うこと。

（イ）　非公開会議のときは，ホームページ又はソーシャルメディア経由の案内等は行わず，メール等で直接送付を行うこと。

（ウ）　機密性の高い会議のときは，万が一の案内メールの漏えいに備え，メールの題名は，機密性を悟られない文面とすること。

（２）　会議の実施

ア　参加者の確認

（ア）　組織外の参加者がいる会議では，特に意図しない第三者が会議に参加しないように参加者の確認を明確にすること。

（イ）　機密性の高い会議のときは，必要に応じて，画面・声により参加者本人であることを確認すること。

イ　会議終了後のデータ削除

会議録音・録画データ，共有資料，チャット等の会議データがクラウド上に存在するときは，クライアント端末への移動・暗号化，クラウド上からの削除を実施すること。

（３）　その他の一般的留意事項

ア　会議で使用する庁内端末のセキュリティ

（ア）　Ｗｅｂ会議サービスを利用した会議の開催・参加に当たっては，セキュリティ対策がされている庁内端末を使用すること。

（イ）　市で管理していない端末を使用するときは，ＢＹＯＤ（ＢｒｉｎｇＹｏｕｒＯｗｎＤｅｖｉｃｅ）として統括情報セキュリティ責任者の許可を受け，一定のセキュリティ対策が施されている端末を使用すること。

（ウ）　脆弱性の悪用を防ぐため，Ｗｅｂ会議サービスのクライアントソフトが常に最新の状態となっていることを確認すること。

（エ）　Ｗｅｂ会議サービスのクライアントソフトをダウンロードするときは，「偽サイト」に注意し，サービス提供者の公式サイト，公式マーケット等からダウンロードすること。

イ　会議の参加環境

（ア）　Ｗｅｂ会議サービスを利用した会議を開催し，又は参加するときは，会議における庁内端末の設置場所に配慮し，可能であれば映像の背景画面を設定する等，重要な情報資産等が，意図せず会議画面へ映り込むことのないようにすること。

（イ）　周囲の音声等が庁内端末の音声入力デバイスに取り込まれることにより，重要な情報資産が漏えいし，又は市の信頼の失墜につながらないよう配慮すること。

（情報資産の種別における留意事項）

第５条　Ｗｅｂ会議サービスを利用した会議において市の情報資産を扱うときの会議データの所在，暗号化及び会議参加者の確認・認証方式の留意点は，次に掲げるとおりとする。

（１）　機密・個人情報等を含む情報資産を扱う会議

ア　音声データ等を含む会議データのクラウド上での復号は，会議の機密性の観点により許されないことから，Ｗｅｂ会議サービスの資料共有，録画機能は使用せず，音声・映像交換及びチャット機能のみを使用すること。その際，資料の共有は暗号化する等の安全な形でメールの添付ファイル等として事前に会議の参加者に配布し，それを参照する形とすること。

イ　Ｗｅｂ会議サービスは，エンドツーエンド暗号化ができる製品を使用することが望ましい。使用するデータセンターは，国の安全保障上の輸出管理において，優遇されるグループＡの国のものであること。

ウ　会議パスワードを設定するとともに待機室機能等を有効とし，会議パスワードは会議案内メールとは別経路で組織外参加者に安全に届けること。組織外参加者については，会議実施時に声，顔等での本人確認を実施する

こと。

（２） 機密・個人情報等を含まない情報資産を扱う会議

ア　会議資料のクラウド上への保存は，情報漏えいリスクを考え望ましくないことから，Ｗｅｂ会議サービスの資料共有，録画機能は使用せず，資料の共有は安全な形でメール添付ファイルとして事前配布し，それを参照する形とすること。使用するデータセンターは，国の安全保障上の輸出管理において優遇されるグループＡの国のものであること。

イ　暗号化に関しては，サーバで一時的に復号される方式であることを確認し，参加者端末サーバ間の通信が安全であることを確認すること。

ウ　会議パスワードを設定，待機室機能を有効とし，会議案内メールは安全な形で参加者に届け，会議実施時の参加者確認は参加者リストと突合をすること。

（３） 情報資産を扱わない会議及び事前申込みを必要とする講習会等

ア　会議資料，会議の内容とも機密性が低いことから，Ｗｅｂ会議サービスは全機能（音声・映像交換，資料共有，チャット等）を使用することができるものとする。

イ　参加者端末，サーバ間の通信が安全であることを確認すること。

ウ　参加人数が多いときは，参加者事前登録の機能を使用し，参加者の事前確認をするとともに，会議のＵＲＬは参加者のみに届け，会議実施時の参加者確認は参加者リストと突合すること。