長崎市
情報セキュリティポリシー

制定日：平成 18 年 3 月 23 日

改定日：令和 8 年 4 月 1 日

第１章
長崎市情報セキュリティポリシーの目的等

第１章　長崎市情報セキュリティポリシーの目的等

１　目的

本市の各情報システムが取り扱う情報には、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極めて重大な結果を招く情報が多数含まれている。

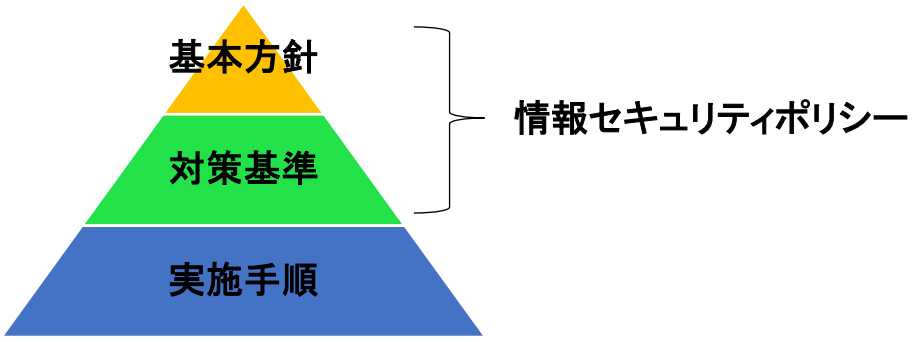
これらの情報及び情報を取り扱う情報システム（以下「情報資産」という。）を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。

本情報セキュリティポリシーは、本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、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　構成

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、情報資産を取り巻く状況の変化に対応する部分としての「情報セキュリティ対策基準」から構成する。また、これらに基づき、情報システムごと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」を作成し、実務レベルでの情報セキュリティ対策を実施することとする（下表参照）。

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システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順	ガイドライン	情報セキュリティ対策基準に基づいた実施手順を作成するためのガイドライン
	業務マニュアル	情報セキュリティ対策基準に基づいた実施手順

３　策定

長崎市情報セキュリティポリシーは、市長、上下水道事業管理者、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会が共同で策定するものとする。

第２章
情報セキュリティ
基本方針

第2章　情報セキュリティ基本方針

１　目的

この情報セキュリティ基本方針は、本市の情報セキュリティ対策の基本的な方針を定めるものとする。

２　定義

情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　情報

情報システムで取り扱う情報及びシステム関連文書のことをいう（書面を含む）。

(2)　情報資産

ネットワーク、情報システム、ネットワーク及び情報システムに関する施設・設備、電磁的記録媒体、ネットワーク及び情報システムで取り扱う情報並びにシステム関連文書のことをいう。

(3)　電磁的記録媒体

サーバー装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体や USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体のことをいう。

(4)　コンピュータ

電子回路を利用して、計算を自動的に行なう装置の総称。数値計算のほか、自動制御やデータ処理、事務管理等にも利用されるものをいう。

(5)　ネットワーク

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

(6)　ハードウェア

コンピュータを動作させるために必要となる物理的な機器のことをいう。

(7)　ソフトウェア

コンピュータを動作させる命令の集まりであるプログラムを組み合わせ、何らかの機能や目的を果たすようまとめたものをいう。

(8)　情報システム

ネットワーク、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、長崎市が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。

(9)　データ

コンピュータ処理に係る出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

(10)　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。

(11)　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。

(12)　情報セキュリティ実施手順

対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ

定める必要のある具体的な手順をいう。

(13) 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。

(14) 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。

(15) 可用性

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

(16) 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)又は住民基本台帳と密接に関わる戸籍事務等に供する情報システム及びデータをいう。

(17) LGWAN 接続系

人事給与、財務会計及び文書管理等 LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

(18) 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。

(19) 通信経路の分割

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

(20) 無害化通信

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

3 対象とする脅威

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

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

本基本方針が適用される機関は、長崎市個人情報の保護に関する法律施行条例(令和4年長崎市条例第40号)第2条第2項に規定する市長、上下水道事業管理者、消防長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び長崎市議会の個人情

報の保護に関する条例（令和4年長崎市条例第49号）第1条に規定する議会とする。ただし、対象機関の範囲以外の者であっても、本基本方針に規定する情報資産を利用する場合にあっては、本基本方針が適用されるものとみなす。

(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

ただし、当該情報資産のうち、国の監督官庁において策定されたセキュリティポリシーに関する対策基準のガイドライン等に基づき策定した独自の基本方針が別途適用されている場合は、本基本方針の対象外とする。

5 職員等の遵守義務

長崎市職員定数条例（昭和 24 年長崎市条例第 59 号）第1条に規定する職員、非常勤職員、会計年度任用職員及び本市への任期付派遣職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6 情報セキュリティ対策

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

(1) 組織体制

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

(2) 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性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、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

ただし、国が認めた特定通信（eLTAX、ぴったりサービス等）に限り、インターネット等から LGWAN-ASP を経由して、マイナンバー利用事務系にデータを取り込むことを可能とする。

イ LGWAN 接続系においては、LGWAN と接続する情報システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

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。高度な情報セキュリティ対策として、長崎県と長崎県内市町のインターネット接続口を集約した長崎県情報セキュリティクラウドに接続することとする。

(4) 物理的セキュリティ対策

情報資産を保有する施設、情報機器や通信回線等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ対策

情報セキュリティに関する職員の責務を定め、職員等に情報セキュリティ対策を周知徹底する等、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術セキュリティ対策

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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

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

(8) 業務委託と外部サービスの利用

業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

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

7 情報セキュリティ監査及び自己点検の実施

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

8 情報セキュリティポリシーの見直し

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

9 情報セキュリティ対策基準の策定

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

10 情報セキュリティ実施手順の策定

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

なお、この情報セキュリティ実施手順の中で、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のある情報については、非公開とする。