名護市情報セキュリティ基本方針

平成 16 年 4 月 1 日　　策定

平成 27 年 12 月 7 日　全部改定

令和 5 年 3 月 1 日　一部改定

目　次

序　情報セキュリティポリシーとは

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

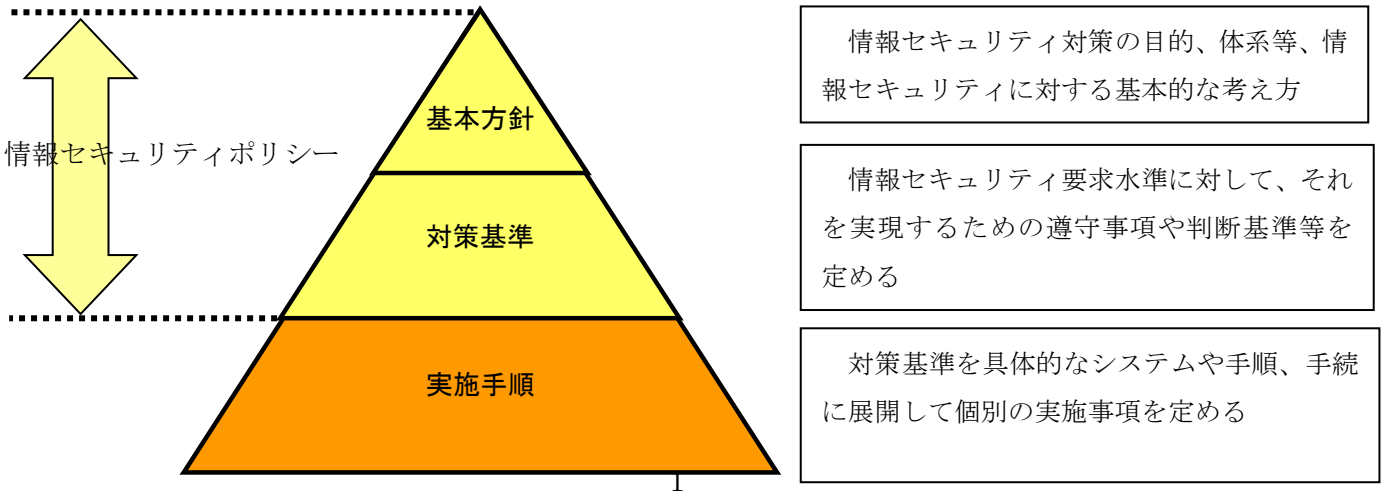
市においても、市民の個人情報や行政運営上必要な情報などの重要な情報を多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定性、継続的な運営のためにも必要不可欠である。また、市には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

これらの状況を鑑み、市における情報資産に対する安全対策を推進し、市民からの信頼を確保し、さらに地域に貢献するため、情報セキュリティポリシーの定期的な評価・見直しを行い、情報セキュリティの実効性を確保するとともに、対策レベルを高めていくことが重要である。また、社会保障・税番号制度におけるセキュリティ対策の状況を踏まえ、名護市情報セキュリティポリシーについても改定を実施する。

「名護市情報セキュリティポリシー」は、一定の普遍性を備えた情報セキュリティ対策の基本的な考え方を定めた「情報セキュリティ基本方針」とその基本方針を実行に移すための全てのネットワーク及び情報システムに共通の対策基準としての「情報セキュリティ対策基準」で構成される。

また、「情報セキュリティポリシー」に基づき、具体的な実施手順として「情報セキュリティ実施手順」を策定していくものとする。

情報セキュリティポリシーの構成



名護市情報セキュリティ基本方針

（目的）

第１条　この基本方針は、市が保有する情報資産を事故、災害、不正侵入、漏えい、改ざん、サービス利用妨害等の様々な脅威から保護するために必要な対策について、組織的かつ継続的に取り組むための基本的な考え方を定め、市における情報セキュリティ水準を維持し、向上させることを目的とする。

（用語の定義）

第２条　この基本方針において、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）　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。

（２）　情報システム　ハードウェア、ソフトウェア、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できることをいう。

（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。

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

（１２）　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。

（１３）　市の組織　市長事務部局、議会事務局、水道事業部局、選挙管理委員会事務局、監査委員事務局、農業委員会事務局、教育委員会事務部局及び消防機関をいう。

（１４）　職員等　市の組織に属する職員、非常勤職員及び会計年度任用職員をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次の各号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、ウィルス攻撃、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

（適用範囲）

第４条　情報セキュリティポリシーは、当該各号に定める範囲に適用する。

（１）　適用対象者の範囲　本基本方針が適用される対象者の範囲は、第２条第１４号で定めるところの職員等とする。

（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　個人情報、特定個人情報など行政事務で取り扱う全ての情報

イ　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

ウ　ネットワーク及び情報システムで取り扱う情報（有体物含む。）

エ　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

（職員等の遵守義務）

第５条　職員等は、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。

（情報セキュリティ対策）

第６条　前条の脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講じる。

（１）　組織体制　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　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行う。

（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制限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。

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。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、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）　物理的セキュリティ　サーバ等、情報システム室等、通信回路等及び職員等のパソコン等の管理について物理的な対策を講じる。

（５）　人的セキュリティ　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（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。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切に対応するため、緊急時対応計画を策定する。

（８）　業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対

策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（情報セキュリティ監査及び自己点検の実施）

第７条　情報セキュリティポリシーの遵守状況を検証するため、自己点検及び情報セキュリティ監査を定期的に、また必要に応じて実施する。

（情報セキュリティポリシーの見直し）

第８条　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。

（情報セキュリティ対策基準の策定等）

第９条　第６条から前条までに規定する対策等を実施するため、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定める。

２　対策基準は、公開することにより市のセキュリティを侵害するおそれがあるため、非公開とする。

（情報セキュリティ実施手順の策定等）

第１０条　情報セキュリティ対策基準に基づき、情報資産の管理手順及び業務遂行に係る手順等を明記した情報セキュリティ実施手順（以下「実施手順」という。）を定める。

２　実施手順は、公開することにより市のセキュリティを侵害するおそれがあるため、非公開とする。

（教育及び訓練）

第１１条　本方針の適用範囲である情報資産に係る全ての職員等に対し、その職務に応じて必要な情報セキュリティに関する教育及び訓練を必要に応じて実施する。

（基本方針の公開）

第１２条　この基本方針は、広く一般に公開する。