長崎県情報セキュリティ基本方針

令和４年４月１日

長崎県総務部スマート県庁推進課

目次

第１章 目的

長崎県の各情報システムが取り扱う情報には、県民の個人情報のみならず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いる。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、県民の財産、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。ひいては、このことが長崎県に対する県民からの信頼の維持向上に寄与するものである。

また、近年のいわゆる Society5.0 実現に向けた自治体 DX の推進や行政手続きのオンライン化に対し積極的に対応するためには、利便性の確保と併せて、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。そのため、長崎県の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために長崎県情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については長崎県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。

※１　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。
※２　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。
※３　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。

第２章 定義

（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）及び電磁的記録媒体で構成され、処理を行う仕組みをいう。
（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	情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態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）	LGWAN	総合行政ネットワークとも呼び、地方公共団体の組織内ネットワークを相互に接続し、地方公共団体相互のコミュニケーションの円滑化や情報の共有による情報の高度利用を図ることを目的とした、高度なセキュリティを維持した行政専用の閉域ネットワーク（インターネット環境に接続されていないネットワーク）をいう。
（６）	県庁LAN	スマート県庁推進課が管理し、知事部局、交通局、教育庁、県警、監査事務局、人事委員会事務局、労働委員会事務局、選挙管理委員会書記室、議会事務局において主に一般行政事務用に使用される閉鎖されたネットワークをいう。(スマート県庁推進課以外が独自に管理するネットワークは含まない。) 県庁LANにおけるネットワークは、マイナンバー利用事務系、LGWAN接続系、インターネット接続系の３種類に分類される。（三層分離）

（７）	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。 LGWAN接続系とは最低限の通信しか許可されておらず、特定の職員等が専用システムを利用することでアクセスすることができる。
（８）	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。）。 職員用のパソコンは、LGWAN接続系に接続されており、インターネット環境からの通信は無害化されている。
（９）	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。 マイナンバー利用事務系やLGWAN接続系からは分離されており、職員用パソコンからは、仮想ブラウザ等により分離環境を経由してアクセスすることができる。

第３章　適用範囲

本基本方針が適用される範囲は、以下のとおりとする。

（１）行政機関の範囲

本対策基準が適用される行政機関は、第2章　定義　（５）県庁ＬＡＮと同じ。但し、教育庁の県立学校においては県庁LANに接続された箇所、県警においては、県庁LANに接続された箇所のみとする。

（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）職務上取り扱う情報、文書（ネットワーク及び情報システムで取り扱う情報並びにこれらを印刷したものを含む各種文書）
（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

（３）上記（１）における情報資産及び関連する職員等

（４）上記（１）における外部委託事業者

（５）上記（１）～（４）に含まれない所属において県庁LANに接続している端末

（６）住民基本台帳ネットワークについてはシステムの性格上別途定める情報セキュリティ対策基準に準じるものとし、本対策基準の適用範囲外とする。

第４章　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、長崎県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り、情報セキュリティ対策の頂点に位置するものである。

したがって、知事をはじめとして県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部外受託者は、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。

第５章　情報セキュリティ管理体制

県の情報資産について、幹部が率先して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。

第６章　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を実施する。

第７章　情報資産への脅威

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、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、火災等の災害並びに事故、故障等によるサービス及び業務の停止。

（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。

第８章　情報セキュリティ対策

（１）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、他の系統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。

（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。インターネット接続口において、高度な情報セキュリティ対策を講じるために自治体情報セキュリティクラウド

の導入等を実施する。

（２）物理的セキュリティ対策

サーバ、情報システム等を設置する管理区域、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（３）人的セキュリティ対策

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講じられるように必要な対策を講ずる。

（４）技術及び運用におけるセキュリティ対策

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及び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。

第９章　情報セキュリティ対策基準の策定

上記のセキュリティ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。

なお、情報セキュリティ対策基準は、公にすることにより長崎県の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

第 10 章　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長崎県の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

第 11 章　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。

第 12 章　評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜情報セキュリティポリシーを見直す。

第 13 章　基本方針の公開

基本方針は、原則公開とする。