長野県情報セキュリティポリシー
（基 本 方 針）Ver 4.0

長野県情報通信技術活用推進本部

（平成14年８月５日決定）

（平成18年６月12日改定）

（平成28年４月１日改定）

（平成31年４月１日改定）

まえがき

コンピュータを利用した業務は、ホストコンピュータとこれに接続された端末機を利用して一部の職員が限られた情報処理業務を行う形態から、すべての職員がネットワークに接続された端末を利用して様々な事務処理を行うものへと進化している。

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、あらゆる面で拡大している一方、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の発生という側面も併せ持っている。

県が保有するネットワークを上記のような脅威から防御し、個人情報等の重要性の高い情報資産や行政運営上必要なプログラムなどの重要な情報を守ることは、県政の円滑で安定的な運営を図る上で、欠くことのできない必要条件である。

このことから、情報システムに関するセキュリティ対策の基本を示すものとして、ここに長野県情報セキュリティポリシーを定める。

長野県情報セキュリティポリシー（基本方針）

（目的）

第１　県が保有する情報資産を様々な脅威から防御し、情報資産の機密性、完全性及び可用性を維持するため、県が行う情報セキュリティに関する対策の統一的かつ基本的事項を定めることを目的とする。

（適用範囲）

第２　対象範囲

この長野県情報セキュリティポリシー(基本方針)（以下「セキュリティポリシー」という。）が対象とする県機関の範囲は、知事部局、会計局、企業局、教育委員会事務局（教育機関を含む）、監査委員事務局、人事委員会事務局、労働委員会事務局及び議会事務局とする。

（定義）

第３　用語の定義

（１）　ネットワーク

コンピュータ等を相互に接続する通信網、その構成機器（ハードウエア及びソフトウエア）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）　情報資産

ア　ネットワーク、情報システム

イ　コンピュータ、ネットワーク及び情報システムで取り扱うデータ（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

（４）　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。

（５）　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。

（６）　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。

（７）　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。

（８）　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。

（９）　LGWAN（総合行政ネットワーク）

地方公共団体情報システム機構が整備・運営する、地方公共団体間のコミュニケーションの円滑化と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、行政機関専用のコンピュータネットワークをいう。

(10) 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。

(11) LGWAN接続系（個人番号関係事務系）
　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。
(12) 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。
(13) 通信経路の分割
　既存のネットワークを、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。
(14) 無害化通信
　インターネットメール本文のテキスト化、マクロ除去等のサニタイズ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。

（管理体制）
第４　情報セキュリティ対策を確実に管理するための体制を整備するものとする。

（情報資産の分類と管理）
第５　県が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。
（情報資産への脅威）
第６　情報資産に対する脅威として、特に認識すべき脅威は以下のとおりである。
（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、機器及び媒体の盗難、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

（情報セキュリティ対策）
第７　情報資産への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講じるものとする。
（１）情報システム全体の強靭性の向上
　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。
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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（２）　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及び遵守すべき事項を明確に定め、職員に対する周知及び徹底を図るとともに、十分な教育、啓発が行われるよう必要な対策を講ずる。

（３）　物理的セキュリティ対策

コンピュータ及びネットワーク機器等を設置する施設への不正な立入り、情報資産への損傷、盗難等からの保護及び職員のパソコン等の管理について物理的な対策を講ずる。

（４）　技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、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、ネットワーク管理等の技術的対策を講じる。

（５）　運用セキュリティ対策

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、セキュリティポリシー運用面の対策を講ずる。

また、緊急事態が発生した場合に、迅速かつ適切な対応が可能となるような危機管理体制の整備等による対策を講ずる。

（６）外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

約款によ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。

クラウドサービスを利用する場合には、情報セキュリティ確保に必要な事項を十分に考慮し、適切な措置を講じる。

（情報セキュリティ対策基準の策定）

第８　このセキュリティポリシーに基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項や、判断の統一的な基準として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。）を定めるものとする。

（情報セキュリティ実施手順の策定）

第９　このセキュリティポリシーに基づき、情報セキュリティ対策を具体的に実施するために、情報セキュリティ対策実施手順（以下「実施手順」という。）を定めるものとする。

（対策基準及び実施手順の扱い）

第10　対策基準及び実施手順は、公にすることにより県の行政運営に重大な支障を及ぼす恐れのある情報を含むことから、非公開とする。

（職員等の義務）
第11　職員、行政嘱託職員、非常勤職員及び臨時職員(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。

（情報セキュリティに関する違反への対応）
第12　セキュリティポリシーに違反した者については、その重大性、発生した事案の状況等に応じて懲戒処分を含む必要な措置を講ずる。

（監査）
第13　セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。

（評価及び見直し）
第14　情報セキュリティ監査の結果等に基づき、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、必要に応じてこのセキュリティポリシーの見直しを実施する。