宇城広域連合

情報セキュリティポリシー

基本方針

2026 年 4 月 1 日

宇城広域連合　総務課　企画財政係

【改定履歴】

施行年月日	版番号	改定理由・内容
令和８年４月１日	第1.0版	令和６年６月２６日に公布された地方自治法の一部を改正する法律（令和６年法律第６５号）に基づき改正された「地方公共団体等におけるサイバーセキュリティを確保するための方針等に係る規定（地方自治法（昭和２２年法律第６７号）第２４４条の６及び地方独立行政法人法（平成１５年法律第１１８号）第２４条の２）」の施行（令和８年４月１日）による初版発行

目　次

はじめに

宇城広域連合情報セキュリティポリシーとは、宇城広域連合が保有する情報資産を漏えい、改ざん等の脅威から防御するための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の総称である。

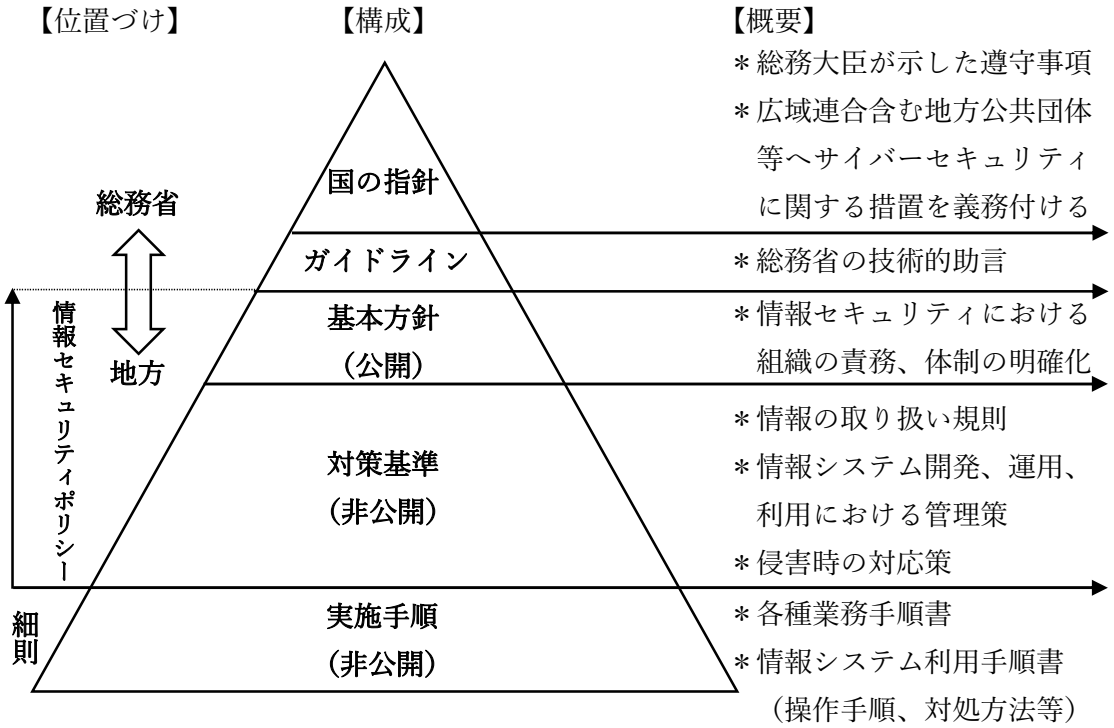
宇城広域連合情報セキュリティポリシーは、宇城広域連合の情報資産を取り扱う全職員が十分に理解し、遵守すべきものであるため、安定的な規範であることが要請される。しかし一方では、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、宇城広域連合情報セキュリティポリシーは、一定の普遍性を備えた「情報セキュリティ基本方針」（以下「本方針」という）と、情報資産を取り巻く状況の変化に適切に対応する「情報セキュリティ対策基準」とに分けて策定することとする。

また、「情報セキュリティ対策基準」に基づく細則として、具体的な情報セキュリティ対策の実施手順および既存の各種業務手順書を含めた「情報セキュリティ実施手順」を策定することとする。

なお、宇城広域連合情報セキュリティポリシーは、総務大臣が定める「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針」に基づき、総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」に沿って構成するものとする。

以上の構成について、その関係性及び位置付けを明確にするため、国の指針から本方針、対策基準及び実施手順に至るまでの構成を図示した構成図を、以下に示す。



１　目的

本方針は、宇城広域連合(以下「本連合」という。)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、本連合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。

※ 機密性　情報にアクセスすることが認可された者だけがアクセスできることを確保することをいう。
※ 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。
※ 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。

２　定義

本方針における用語の定義は、次に掲げるとおりとする。

（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、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）情報資産
　住民情報、財務情報、機密情報、技術情報等の業務遂行の過程で生み出される価値あるものをいう。
（５）職員
　本連合の情報資産を取り扱い、又は情報システムを利用する立場にあるすべての者をいう。これには、本連合に在職する職員（派遣職員、人事交流職員、再任用職員、会計年度任用職員、臨時的職員を含む）、地方公務員法（昭和 25 年法律第 261 号）第 3 条第 3 項に規定する特別職非常勤職員、広域連合議会、選挙管理委員会及び監査委員に属する特別職職員並びに連合長及び副連合長を含む。
　また、将来、本連合において新たな任用形態又は身分区分が設けられた場合においても、本連合の業務に従事し、又は情報資産を取り扱う者は、すべて本方針における「職員」に含まれるものとする。
（６）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)に関わる情報システム及びデータをいう。

（７）基幹系（LGWAN 接続系）

本連合の庁内ネットワーク、及び 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。)。

（８）情報系（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。

（９）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。

(10) 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、安全性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、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及び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）行政機関の範囲

本方針が適用される行政機関は、宇城広域連合事務局設置条例(平成 19 年条例第 6 号)第 1 条に規定する事務局、宇城広域連合会計管理者の補助組織設置規則(平成 19 年規則第 2 号)第 1 条に規定する会計課、宇城広域連合消防本部及び消防署設置条例(平成 19 年条例第 46 号)第 2 条に規定する消防本部・消防署、宇城広域連合選挙管理委員会規程(平成 19 年訓令第 1 号)に規定する選挙管理委員会、宇城広域連合監査委員に関する条例(平成 19 年条例第 5 号)に規定する監査、及び宇城広域連合議会会議規則(平成 19 年規則第 1 号)に規定する議会をいう。

（2）情報資産の範囲　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　職員の遵守義務

職員は、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

本連合の情報資産を上記3の脅威から保護するために、次に掲げる情報セキュリティ対策を講じる。

（1）組織体制

本連合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

本連合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3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。

エ　その他、ア～ウに該当しない情報システムにおいては、クラウドサービスや外部事業者が提供するシステムを含め、情報資産の機密性・完全性・可用性を考慮し、必要な技術的・組織的・人的対策を講じるものとする。なお、契約内容や運用状況の確認等を通じて、適切な情報セキュリティ水準が確保されていることを継続的に確認するものとする。

（4）物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員のパソコン等の管理について、物理的な対策を講じる。

（5）人的セキュリティ

情報セキュリティに関し、職員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、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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対策計画を策定する。

（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、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（クラウドサービス）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。

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、及び調整

（１）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。

（２）情報セキュリティ対策基準に基づき、情報資産に係る既設の各種業務手順書、情報システム利用手順書等について見直しを行い、必要に応じて調整する。

11　情報セキュリティ対策基準及び情報セキュリティ実施手順の非公開

情報セキュリティ実施手順は、公にすることにより本連合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

附　則

本方針は、令和８年４月１日から施行する。