八代広域行政事務組合情報セキュリティポリシー
基本方針抜粋版

◆改定履歴

No.	年月日	内容
1	平成２０年　４月　１日	新規作成
2	平成２５年　４月　１日	改訂
3	令和　６年　４月　１日	ガイドライン改訂に合わせて全面改定。地方自治法改正（令和８年４月１日施行）に伴い、「基本方針」の公表が必要となった。このことを踏まえ、「八代広域行政事務組合情報セキュリティポリシー（令和６年４月１日改定）」のうち、基本方針のみ記載した「八代広域行政事務組合情報セキュリティポリシー基本方針抜粋版」を作成し、改正地方自治法の施行と併せて公表するもの。 ※なお、八代広域行政事務組合情報セキュリティポリシー基本方針については、改正地方自治法第２４４条の６第１項の方針に位置づけるものとする。
4	令和　８年１１月１日	地方自治法第 244 条の 6 に基づくサイバーセキュリティ確保方針の策定義務への対応として、組合議会に係る情報セキュリティ管理体制を明確化するための改訂するもの。なお、本ポリシーは改正地方自治法第２４４条の６第１項の方針に基づき、組合議会と共同で策定するものとする。公表についは、「八代広域行政事務組合情報セキュリティポリシー基本方針抜粋版」として行うものとする。

目次

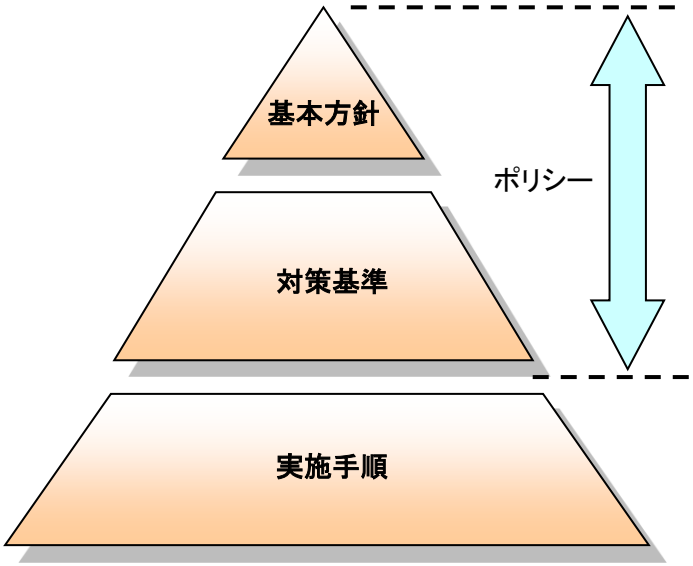
第１章　情報セキュリティポリシーの構成 0
第２章　情報セキュリティ基本方針 1
１　目的 1
２　定義 1
３　対象とする脅威 1
４　適用範囲 2
５　職員等の遵守義務 2
６　情報セキュリティ対策 2
７　情報セキュリティポリシーの見直し 3
８　情報セキュリティ対策基準の策定 3
９　情報セキュリティ実施手順の策定 3

第１章　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、八代広域行政事務組合（以下「本組合」という）の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を総称する。これは、本組合の情報資産に接する全ての職員及び議員（以下「職員等」という。）並びに委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、情報処理技術や通信技術の進歩等に伴う情報資産を取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを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適切に対応する部分としての「情報セキュリティ対策基準」の２階層に分けて策定する。

また、情報セキュリティポリシーに基づき、ネットワーク及び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」を別途策定することとする。



【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

【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ネットワーク及び情報システムに共通の情報セキュリティ対策の基準

【実施手順】
ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第２章　情報セキュリティ基本方針

１　目的

本基本方針は、本組合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、本組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。

２　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）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）情報セキュリティポリシー等

情報セキュリティポリシー及び実施手順をいう。

（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 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。

(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情報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

本組合の情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は、次のとおりである。

脅威の区分	内容
部外者	・不正アクセス（※）、コンピュータウイルス（※）等のサイバー攻撃（※）

	・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、盗難等
職員等又は外部委託事業者	・情報資産の無断持ち出しや目的外利用、無許可の機器の接続やソフトウェア使用等の規定違反 ・情報システムの設計の不備、プログラムの欠陥 ・操作・設定ミス、メンテナンス不備 ・外部委託管理の不備
その他	・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 ・地震、落雷、火災等の災害によるサービス及び業務の停止 ・電力供給の途絶、通信の途絶等のインフラの障害

（※）不正アクセス：不正アクセス禁止法第２条第４項に規定する不正アクセス行為、その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセス

（※）コンピュータウイルス：データに対して意図的に何らかの被害を及ぼすように作られたプログラム

（※）サイバー攻撃：コンピュータシステムやインターネット等を利用して、標的のコンピュータやネットワークに不正に侵入してデータの詐取や破壊、改ざん等を行ったり、標的のシステムを機能不全に陥らせること

4　適用範囲

（１）適用する機関の範囲

本基本方針が適用される範囲は、組合の執行機関（会計管理者の補助組織を含む。）並びに組合議会とする。

（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。

①　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

②　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。）

③　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　職員等の遵守義務

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等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に、以下の情報セキュリティ対策を講じる。

（１）組織体制

本組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

本組合の保有する情報資産をその重要性（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、次の二段階の対策を講じる。

①　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。

② 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。

（4）物理的セキュリティ

サーバ、情報システム室、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。

（5）人的セキュリティ

情報セキュリティに関し、職員等及び外部委託事業者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。

（※）アクセス制御：情報資産、情報システムに対して、利用できる者を制限する機能

7　情報セキュリティポリシーの見直し

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又は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は、情報セキュリティポリシーを見直す。

8　情報セキュリティ対策基準の策定

上記６、７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。

9　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本組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。