広　島　県　議　会　議　長

# 広島県議会情報セキュリティ方針の公表について

広島県議会情報セキュリティ方針（令和８年４月１日策定）について、地方自治法第 244 条の６第１項に規定する方針に位置づけるものとし、同条第２項に基づき、別紙のとおり公表する。

別紙

# 広島県議会情報セキュリティ方針

## 第１　目的

本方針は、県議会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、情報資産の取扱い等の情報セキュリティ対策の基本的な考え方及び方策を定め、本県議会における情報資産の管理を徹底することを目的とする。

## 第２　対象機関

対象となる機関は、議会（議会事務局を含む）とする。

## 第３　用語の定義

１　情報

情報システムで取り扱う電磁的データをいう。

２　情報資産

本方針が対象とする情報資産は、情報及び情報を管理する仕組み（情報システム並びに情報システムの開発、運用及び保守のための資料等を含む。）をいう。

３　情報システム

コンピュータのハードウェア・ソフトウェア、ネットワーク及び記録媒体等で構成されるものであって、これら全体で業務処理を行うための情報処理の体系をいう。

４　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。

５　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。

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、情報にアクセスできる状態を確保することをいう。

９　内部ネットワーク

単一の情報システム及びそれを構成するネットワークをいう。

１０　外部ネットワーク

単一の情報システムを中心とした際の内部ネットワーク以外の全ての領域をいう。

**第４　議員及び職員の遵守義務**

県議会の保有する情報資産にアクセスすることができるすべての議員及び職員（再任用職員、会計年度任用職員、任期付職員その他の任用期間又は任用に当たっての短時間勤務等の定めがある職員及び市町等からの派遣職員等を含む。以下同じ。）は、情報セキュリティの重要性についての共通の認識を持つとともに、本方針を遵守する義務を負う。

**第５　情報セキュリティ管理体制**

県議会の保有する情報資産について、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ものとする。

**第６　情報資産の分類**

情報資産については、機密性、完全性及び可用性に応じて分類し、その分類に応じた情報セキュリティ対策を行うものとする。

**第７　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ものとする。

１　部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、不当な目的による利用等

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、火災等の災害並びに事故、故障等によるサービス及び業務の停止

**第８　情報セキュリティ対策**

第７で示した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　物理的セキュリティ対策

情報システムを設置する施設への不正な立入りの防止や、パソコン等の機器及び記録媒体等の適切な管理など、情報資産を損傷・妨害等から保護するために物理的な対策を講じる。

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を定め、議員及び職員に本方針及び情報セキュリティに関する法令等の内容を周知徹底するなど、十分な研修及び啓発が行われるよう必要な対策を講じる。

３　技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、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等の技術的な対策を講じる。

４　運用

各種対策の実施状況を確認するため、情報システムの監視、本方針の遵守状況の確認、外部委託を行う際のセキュリティ確保等の運用面の対策を講じる。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、緊急時対応計画を策定する。

５　業務委託と外部サービス（クラウドサービス・ソーシャルメディアサービス）の利用

業務委託を行う場合には、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する等の必要な措置を講じる。また、外部サービス（クラウドサービス・ソーシャルメディアサービス）を利用する際の留意事項を定め、議員及び職員に周知する。

## 第９　情報セキュリティ監査及び自己点検の実施

本方針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１０　評価及び見直し

情報セキュリティ監査及び自己点検の実施による検証結果等を踏まえるとともに、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新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等のリスクを検討したうえで、本方針の見直しを適宜行うこととする。

## 附　則

１　本方針は、令和８年４月１日から施行する。

２　第５及び第８で定める情報セキュリティ対策を講じるに当たっての管理体制や基本的な要件等については、令和８年度中に、別に定めることとする。