

広島県情報セキュリティ基本方針(一部抜粋)

第1 目的

基本方針は、県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、情報資産の取扱い及び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

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。

11 庁内ネットワーク

行政 LAN・WAN ネットワーク及びそれと接続された情報システムを構成するネットワークのうち、オンプレミスで構築されたもの（クラウドサービスに構築されたものは除く。）をいう。

12 庁外ネットワーク

庁内ネットワーク以外の全ての領域をいう。

13 閉域接続系

行政 LAN・WAN ネットワーク及びそれと閉域接続された情報システム（クラウドサービスに構築されたものを含む。）を構成するネットワークをいう。

第5 情報セキュリティ管理体制

県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、プログラム上の欠陥、操作ミス、故障等の非意図的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、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、職員に基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、十分な教育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

情報資産を外部からの不正なアクセス等から適切に保護するため、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、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。

第9 対策基準の策定

第8の情報セキュリティ対策を講じるに当たって、遵守すべき行為、判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した対策基準を策定するものとする。

なお、対策基準は公にすることにより本県の行政運営に重大な支障を及ぼすことがあることから非公開とする。

第10 実施手順の策定

セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の情報システムについて具体的な手順を明記した実施手順を策定するものとする。

なお、実施手順は公にすることにより本県の行政運営に重大な支障を及ぼすことがあることから非公開とする。

第11 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 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、セキュリティポリシー及び実施手順の見直しを適宜行うこととする