別記１

岡山県情報セキュリティ基本方針

平成16年 3月29日策定
平成27年12月28日改訂
平成31年 3月20日改訂
令和 3年 4月 1日改訂

目次

第１章　概要

第１節　本書の目的

本書は、岡山県情報セキュリティポリシー（以下「ポリシー」という。）の構成文書の１つで、本県の職員及び外部委託事業者等、情報資産を取り扱う者全員が、情報資産を使用するときに従うべき、情報セキュリティを守るための基本的な考え方や方向性を定めたものである。

第２節　適用範囲

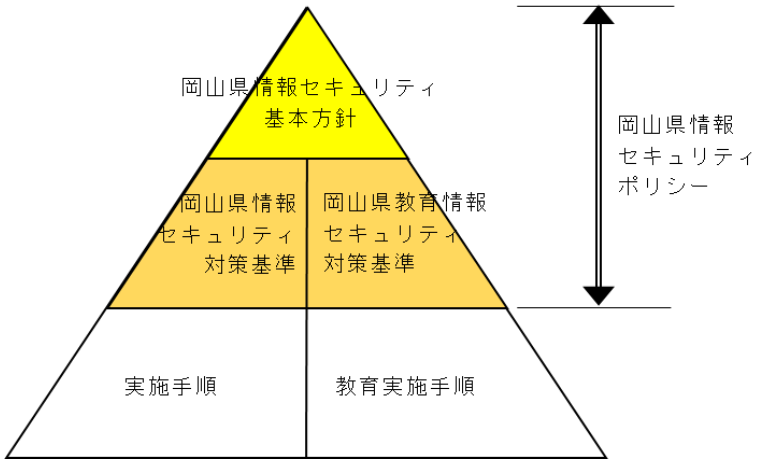
本書の適用範囲は、本庁及び出先機関において取り扱う情報資産全てとする。

ただし、岡山県警察が、管理運用する情報システム等で取り扱う情報資産は対象外とする。

第３節　ポリシーの構成

ポリシーとは、本県が取り扱う情報資産を脅威から守るために、職員が遵守すべきことを、総合的、体系的に.取りまとめ、文書化したものであり、以下の文書で構成される。

・岡山県情報セキュリティ基本方針（本書）
・岡山県情報セキュリティ対策基準
・岡山県教育情報セキュリティ対策基準



情報セキュリティポリシー及び実施手順の構成

第４節　用語定義

(1) 情報資産
　本県が取り扱う電磁的データ並びに情報システム及びネットワークの開発・運用に係る文書及び電磁的データ

(2) 情報システム
　電子計算機（以下「コンピュータ」という。）を用いて、本県の行政事務を処理するための仕組み

(3) ネットワーク
　本県がコンピュータを相互に接続するために構築及び運営する通信網及び通信機器
(4) 情報セキュリティ
　情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態の維持
(5) 保護管理要件
　情報資産を脅威からどのように保護するのかを示したもの
(6) マイナンバー利用事務系ネットワーク
　税務システム及び社会保障システム等でマイナンバー利用事務（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第10項による「個人番号利用事務」をいう。）を行う端末を接続するネットワーク
(7) 行政事務系ネットワーク
　職員が通常業務に使用する端末を接続するネットワーク
(8) インターネット業務系ネットワーク
　インターネットに接続できるネットワーク
(9) 通信経路の分割
　行政事務系ネットワークとインターネット業務系ネットワーク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。
(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ない等、安全が確保された通信

第２章　基本的な考え方

第１節　対象とする脅威

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。

(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、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

第２節　セキュリティレベル

脅威から情報資産を保護するための観点として、不当に他者に漏洩されない（機密性）、改ざんされない（完全性）、継続して提供される（可用性）の３つを定義する。

セキュリティレベルは、上記３つの観点から、情報資産の重要度に応じて必要十分なものに設定する。あわせて、保護管理要件を検討し、個別に想定されるリスク及びその対策を明確にする。

第３節　情報セキュリティ対策

(1) 管理的対策

情報セキュリティに関する権限及び責任を定め、職員にポリシー及び関連法令等を周知徹底するなど、十分な教育及び啓発を行うための対策を講ずる。

(2) 物理的対策

情報資産、情報システム、ネットワークを盗難、損傷、妨害等から保護するための物理的な対策を講ずる。

(3) 技術的対策

情報資産を不正アクセス等から適切に保護するため、アクセス制御、ネットワーク管理等の技術的な対策を講ずる。

(4) 開発・運用上の対策

情報システム開発時及び運用時におけるポリシーの遵守及び事故発生時等の迅速な復旧などを確保するための対策を講ずる。

(5) 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ずる。

ア　マイナンバー利用事務系ネットワークにおいては、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　行政事務系ネットワークにおいては、LGWAN と接続する業務用システムと、インターネット業務系ネットワーク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　インターネット業務系ネットワークにおいては、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、県と市町村のインターネット接続口を集約した自治体情報セキュリティクラウドを導入する。

(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。

ソーシャルメディアサービスを利用する場合には、情報セキュリティ対策に関する事項を含めたソーシャルメディアサービス運用ガイドラインを定める。

第３章　ポリシー等の取扱い

第１節　基本方針

基本方針は、個人情報等、行政運営上重要な情報資産の管理及び情報セキュリティ対策についての基本的な考え方や方向性を定めたものである。
一般に公開する。

第２節　対策基準

対策基準は、基本方針実現のために、遵守すべき行為及び判断等の基準を定めたものである。
対策基準及び次節で規定する実施手順は、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恐れのある情報であることから非公開とする。

第３節　実施手順

実施手順は、業務ごとに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の具体的な手順を明記したものである。

第４節　ポリシー等の改訂

情報セキュリティを取り巻く環境の変化に迅速に対応するため、ポリシー及び実施手順（以下「ポリシー等」という。）は定期的に見直し、必要に応じて改訂する。

第４章　情報資産の取扱い

情報資産は、セキュリティレベル毎に分類するとともに、必要な保護管理要件を設定し、職員が適切に取り扱わなければならない。
なお、業務のより効率的な実施等のため、情報資産を外部委託事業者に取り扱わせる場合は、情報資産の保護に関する必要事項を明記した契約を締結しなければならない。

第５章　組織及び役割と責任

第１節　職掌上の役割と責任

第１項　所属長の役割と責任

所属長は、所属における情報セキュリティ確保の責任を負う。

第２項　職員の役割と責任

職員は、関係法令及びポリシー等を遵守するとともに所属長の指示に基づき情報資産を適切に取り扱わなければならない。

第２節　情報セキュリティ管理体制

最高情報セキュリティ責任者（CISO）及び情報セキュリティ委員会を設置する等、全庁的な管理体制を構築・運用する。

第６章　監査等

第１節　自己点検

ポリシー等の遵守状況を確認するため、定期的に自己点検を行う。

第２節　情報セキュリティ監査

ポリシー等の遵守状況を検証及び評価・見直しのため、定期的に監査を行う。

第３節　罰則

職員が、ポリシー等に違反した場合の処分は、その重大性、発生した事案の状況に応じて地方公務員法等の定めによるものとする。

外部委託事業者が、ポリシー等に違反した場合の対応については、予め契約に定めておくものとする。