

徳島県情報セキュリティ基本方針

目次

徳島県情報セキュリティ基本方針.....	1
1. 目的.....	1
2. 適用範囲.....	1
3. 用語の定義.....	1
4. 対象とする脅威.....	1
5. 職員等の遵守義務.....	2
6. 情報セキュリティ対策.....	2
7. 情報セキュリティ監査及び自己点検の実施.....	3
8. 情報セキュリティポリシーの見直し.....	3
9. 情報セキュリティ対策基準の策定.....	3
10. 情報セキュリティ実施手順の策定.....	3

更新年月日	備考
平成15年3月27日	施行
平成19年5月1日	全面改正
平成19年7月23日	一部改正
平成20年4月1日	一部改正
平成21年3月17日	一部改正（平成21年4月1日施行）
平成21年4月1日	一部改正
平成22年3月23日	一部改正
平成23年3月10日	一部改正
平成24年4月1日	一部改正
平成27年8月26日	一部改正
平成28年4月1日	一部改正
平成29年4月1日	一部改正
平成31年3月12日	一部改正
令和元年5月1日	一部改正
令和3年4月1日	一部改正
令和5年1月1日	一部改正
令和5年4月1日	一部改正
令和5年6月1日	一部改正
令和6年4月1日	一部改正
令和6年11月14日	全面改正
令和7年4月1日	一部改正
令和8年3月13日	一部改正（一部令和8年4月1日施行）

徳島県情報セキュリティ基本方針

1. 目的

この基本方針は、県の保有する情報資産について、情報セキュリティ対策の基本的な事項を定め、もって情報資産の機密性の保持並びに完全性及び可用性の維持を確保することを目的とする。なお、この基本方針は、知事、議会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会、公営企業管理者及び病院事業管理者における地方自治法（昭和22年法律第67号）第244条の6に定めるサイバーセキュリティを確保するための方針とする。

2. 適用範囲

- 1 この基本方針は、知事、議会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会、公営企業管理者及び病院事業管理者の事務局等における情報資産の取扱いについて適用する。
- 2 この基本方針が対象とする情報資産は、次のとおりとする。
 - ・情報システム及びこれらに関する施設及び設備
 - ・情報システムで取り扱う情報及びソフトウェア（これらを印刷した文書を含む。）
 - ・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
- 3 前項第2号の印刷した文書については、情報セキュリティポリシーによるもののほか、徳島県公文書管理規則、徳島県文書規程その他の県の公文書の管理等に関する規則等の定めるところによる。

3. 用語の定義

- 1 情報セキュリティ 情報資産の機密性を保持し、情報の完全性及び可用性を維持することをいう。
- 2 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状態を確保することをいう。
- 3 完全性 情報が破壊、改ざん又は消去されていない正しい状態を確保することをいう。
- 4 可用性 許可された利用者が、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。
- 5 情報システム コンピュータ（サーバ、パソコン等）、ネットワーク、電磁的記録媒体及びそれを制御するソフトウェア並びにその運用体制などで構成され、情報処理を行う仕組みをいう。
- 6 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。
- 7 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、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。
- 8 LGWAN接続系 人事給与、財務会計及び文書管理等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。
- 9 インターネット接続系 ホームページ管理システム、公共施設予約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。
- 10 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。
- 11 無害化通信 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、LGWAN接続系とインターネット接続系を繋ぐ通信をいう。
- 12 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。

4. 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、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な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サービス及び業務の停止等
- 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

5. 職員等の遵守義務

職員、会計年度任用職員（以下「職員等」という。）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

上記4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
本県の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。
- 2 情報資産の分類と管理
本県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実施する。
- 3 情報システム全体の強靱性の向上
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、次の三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、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。
- 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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
- 8 業務委託とクラウドサービスの利用
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。
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。

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に新たに対策が必要となった場合には、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を分析し、リスクを検討したうえで、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。なお、情報セキュリティ対策基準は、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おそれがあることから非公開とする。

10. 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県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

この基本方針は、令和8年3月13日から施行する。ただし、第1条の規定中、地方自治法（昭和22年法律第67号）第244条の6に定めるサイバーセキュリティを確保するための方針に関する部分は、令和8年4月1日から施行する。