徳島県情報セキュリティポリシーにおける基本方針

（目的）

第１条 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考え方及び方策を定め，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。

（適用範囲）

第２条 この基本方針は，知事，議会，教育委員会，選挙管理委員会，人事委員会，監査委員，公安委員会，警察本部長，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。ただし，知事の事務局以外については，知事が現に直轄管理運営する情報システム及びその利用に限る。

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。

（１） 情報システム及びこれらに関する施設及び設備

（２） 情報システムで取り扱う情報及びソフトウエア（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

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。

（用語の定義）

第３条 この基本方針において，次の各号に掲げる用語の意義は，当該各号に定めるところによる。

（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） 情報セキュリティポリシー 県が保有する情報資産のセキュリティ対策について取りまとめたもので，この基本方針並びにこれに基づく情報セキュリティ対策基準及び情報セキュリティ実施手順をいう。

（３） 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。

（４） 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。

（５） 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。

（６） 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エ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。

（７） 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（ハードウエア及びソフトウエア）をいう。

（８） 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。

（９） 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。

（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。

（情報セキュリティ管理体制）

第４条 県は，情報セキュリティポリシーを守るための体制を確立するものとする。

（情報資産の分類に基づく対策）

第５条 県は，取り扱う情報の内容に応じて情報資産を分類し，その重要度に応じた情報セキュリティ対策を講ずるものとする。

（対象とする脅威）

第６条 情報資産に対する脅威として，次の脅威を想定し，県は，情報セキュリティ対策を講ずるものとする。

（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，消去等

（２） 情報資産の無断持出し，無許可ソフトウエ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

（情報セキュリティ対策）

第７条 情報資産を保護するために，県は，次の情報セキュリティ対策を講ずるものとする。

（１） 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じる。

① 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、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。

② 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。

③　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。高度な情報セキュリティ対策として、徳島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への接続を実施する。

（２）　人的セキュリティ対策 情報セキュリティに関し，すべての職員（非常勤職員及び臨時職員を含む。以下「職員等」という。）が守るべき事項を定めるとともに，十分な教育及び啓発を行うことや罰則規定を定める等の人的な対策を講ずる。

（３）　物理的セキュリティ対策 サーバ等，管理区域及び通信回線等の管理について，物理的な対策を講ずる。

（４）　技術的セキュリティ対策 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及び不正アクセス対策並びに情報の一元化及び集中化等，機密性，完全性及び可用性の確保を可能な限り自動化しルーチン化する技術的な対策を講ずる。

（５）　運用におけるセキュリティ対策 情報システムの監視及び管理，情報セキュリティに関する遵守状況の把握その他の対策並びに緊急時における迅速な対応を可能とするための危機管理対策を講ずる。

（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。

約款による外部サービスを利用する場合には、利用にかか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。

（７）　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、情報セキュリティポリシーの見直しを行う。

（情報セキュリティ対策基準の策定）

第８条 前条の対策を講ずるに当たって，守るべき事項及び判断等の基準を統一的に定めるため，県は，必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。なお，この対策基準は，公にすることにより，県の情報セキュリティの維持に支障を及ぼすおそれがあることから，非公開とする。

（情報セキュリティ実施手順の策定）

第９条 県は，この基本方針及び前条の対策基準等を守り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，具体的な実施手順を明記し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，この実施手順は，公にすることにより，県の情報セキュリティの維持に支障を及ぼすおそれがあることから，非公開とする。

（職員等の義務）

第１０条 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を守らなければならない。また，外部委託事業者に業務を行わせようとする場合は，契約や別途取決めを行うことにより，情報セキュリティポリシーを守らせるために必要な措置を講じなければならない。

（評価及び見直しの実施）

第１１条 県は，情報セキュリティポリシーが守られていることを検証するため，定期的に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行う。

２ 前項の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並びに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となった場合には，情報セキュリティポリシーの見直しを行うことにより，高いセキュリティ水準を実現するものとする。

附則

この基本方針は，平成１５年３月２７日から施行する。

附則

この基本方針は，平成１９年５月１日から施行する。

附則

この基本方針は，平成２７年８月２６日から施行する。

附則

この基本方針は，平成３１年３月１２日から施行する。