埼玉県情報セキュリティポリシー
Ⅰ　情報セキュリティ基本方針

附　則

この情報セキュリティポリシーは、平成２２年４月１日から施行する。

附　則

この情報セキュリティポリシーは、平成２３年２月１４日から施行する。

附　則

この情報セキュリティポリシーは、平成２５年４月１日から施行する。

附　則

この情報セキュリティポリシーは、平成２６年４月１日から施行する。

附　則

この情報セキュリティポリシーは、平成２７年６月２６日から施行する。

附　則

この情報セキュリティポリシーは、平成２８年４月１日から施行する。

附　則

この情報セキュリティポリシーは、平成２９年４月１日から施行する。

附　則

この情報セキュリティポリシーは、平成３１年４月１日から施行する。

附　則

この情報セキュリティポリシーは、令和２年４月１日から施行する。

附　則

この情報セキュリティポリシーは、令和３年４月１日から施行する。

情報セキュリティポリシーとは

この情報セキュリティポリシーは、県が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものの総称です。

情報システムの技術的安全の確保及び職員の意識啓発を図り、もって県民の県に対する信頼性を確保することを目的とします。

構成

この情報セキュリティポリシーは、県の業務に携わる職員に浸透、普及、定着させるものであり、安定的な規範であることが要請されます。

このため、この情報セキュリティポリシーを、一定の普遍性を備えた情報セキュリティ基本方針と、これを実行に移すための情報セキュリティ対策基準の２階層の構成とします。

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための、全ての情報システムに共通な情報セキュリティ対策に関する基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づき、情報システムごとに定める具体的な実施手順

目　次

Ⅰ　情報セキュリティ基本方針

第１　目的

この基本方針は、県が保有する情報資産を様々な脅威から保護するために必要な様々な対策について、組織的かつ継続的に取り組むための基本的な考え方を定めるものであり、県における情報セキュリティ水準を維持し、及び向上させることを目的とする。

第２　用語の定義

この情報セキュリティポリシーにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) 情報　電磁的に記録されている全ての文字、図表などの総称をいう。

(2) 情報資産　情報、情報を管理するための仕組み及びそれを記載している資料等の総称をいう。

(3) 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。

(4) 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。

(5) 可用性　情報にアクセスすることを認められた者が、必要なときに中断されることなく、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。

(7) 情報セキュリティインシデント　情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

(8) 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。

(9) 電磁的記録媒体　ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の情報を電磁的に記録しておくメディアをいう。

(10) 機器　ハードウェア及びソフトウェアから構成され、情報を作成、処理、保存する装置をいう。

(11) ネットワーク　機器等を相互に接続するための通信網、その構成機器をいう。

(12) 情報システム　機器、ネットワーク及び電磁的録媒体で構成されるシステムをいう。ただし、専ら設備の監視及び制御を目的とするシステムは対象外とする。

(13) インターネット接続系　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。
(14) ＬＧＷＡＮ接続系　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。
(15) 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）に関わる情報システム及びデータをいう。
(16) 通信経路の分割　インターネット接続系及びＬＧＷＡＮ接続系、マイナンバー接続系間の通信環境を分離したうえで、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。

第３　対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウィルス攻撃、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、及び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、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、空調の途絶、水道供給の途絶等のインフラの障害からの波及等

第４　適用範囲

１　この情報セキュリティポリシーの対象となる県の機関は、知事部局、企業局、下水道局、教育局、県立学校その他の教育機関、議会事務局、監査事務局、人事委員会事務局、労働委員会事務局、収用委員会事務局とする。
２　この情報セキュリティポリシーの対象となる情報資産は、県の機関が保有する情報資産のうち、次に掲げるものとする。
(1) 情報システム、ネットワーク及びネットワーク図、マニュアル等のシステム関連資料等（以下「資料等」という。）
(2) 情報（クラウドサービス上のものを含む）

(3) 機器
(4) 電磁的記録媒体
(5) 環境設備（電源設備、空調設備等をいう。）

3　この情報セキュリティポリシーは、１の県の機関の職員（非常勤職員及び会計年度任用職員を含む。）に適用する。

第５　職員の責務

職員は、情報資産を安全に管理することの重要性について、共通の認識を持つとともに、職務の遂行に当たって、情報セキュリティポリシー及び実施手順（以下「情報セキュリティポリシー等」という。）を遵守し、関係する法令等に従う。

第６　情報セキュリティ対策

県は、第３の「対象とする脅威」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

情報セキュリティ対策を組織的に推進するため、 情報セキュリティ委員会及び庁内 CSIRT を設置し、組織体制を確立する。また、情報セキュリティ対策に関し、各管理者等の役割、権限及び責任を明確にする。

(2) 情報資産の分類と管理

情報をその重要度に応じて分類するとともに、機密性、完全性及び可用性を確保した上で、情報資産を保護する。

(3) 物理的セキュリティ

サーバー等、情報システム室等、通信回線等及び職員のパソコン等の情報処理機器類の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、職員が遵守すべき事項を明確かつ具体的に定めるとともに、十分な教育及び啓発及び標的型攻撃を想定した訓練等を行うなどの人的な対策を講じる。

(5) 技術的セキュリティ

コンピューター等の管理、アクセス制御、不正プログラム対策、標的型攻撃やサービス不能攻撃などのサイバー攻撃を含む不正アクセスへの対策等の技術的対策を講じる。

(6) 情報セキュリティポリシーの運用

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、外部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等の運用上の対策を講じる。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、緊急時対応体制を整備する。

(7) 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 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及び未知の不正プログラムへの対策等を実施する。

② ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務システムと、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。

③ 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うえで、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等を導入する。

(8) 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。

第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等の有効性及び遵守状況について定期的に監査及び自己点検を実施する。

第８　情報セキュリティポリシー等の見直し

情報セキュリティ監査及び自己点検の結果等を踏まえ、情報セキュリティポリシー等で定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化等を考慮し、情報セキュリティポリシー等の見直しを行う。

第９　情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づき、具体的な遵守事項及び判断基準等を明記した情報セキュリティ対策基準を定める。

第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県の機関共通の実施手順である共通実施手順及び情報システムに係る実施手順である個別実施手順を定める。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。