静岡県情報セキュリティ基本方針

第１　目的

この基本方針は、静岡県高度情報化推進規程（平成７年訓令乙第４号）第７条５項の情報セキュリティに関する事項について定めること及び情報セキュリティに関する対策について基本的な事項を定め、静岡県の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ことを目的とする。

第２　定義

この基本方針において、次に掲げる用語の意義は、それぞれ定めるところによる。

(1) 情報資産　　資産として価値を有する情報をいう。

(2) 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。

(3) 情報システム　　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(4) 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。

(5) 情報セキュリティポリシー　　この基本方針及び第９に規定する情報セキュリティ対策基準をいう。

(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、必要なときに中断されることなく情報にアクセスできることをいう。

(9) 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。

(10) 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（マイナンバー利用事務系を除く。）。

(11) 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。

(12) 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。

(13) 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。

第３ 対象とする脅威

この基本方針が対象とする情報資産に対する脅威（以下「脅威」という。）は、次に掲げるとおりとする。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃その他のサイバー攻撃、部外者の侵入その他の意図的な要因による情報資産の漏えい、破壊、改ざん及び消去並びに重要情報の詐取並びに内部不正等

(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、情報システムの設計又は開発の不備、プログラム上の欠陥、情報システムの操作又は設定ミス、情報システムのメンテナンスの不備、内部監査又は外部監査の機能の不備、委託管理の不備、マネジメントの欠陥並びに機器故障等の非意図的要因による情報資産の漏えい、破壊及び消去等

(3) 地震、落雷、火災その他の災害によるサービス及び業務の停止等

(4) 大規模かつ広範囲にわたる疾病による要員不足に伴う情報システムの運用の機能不全等

(5) 電力供給の途絶、通信の途絶及び水道供給の途絶その他のインフラの障害等

第４ 適用範囲

(1) 行政機関の範囲

この基本方針が対象とする行政機関の範囲は、知事部局、企業局、がんセンター局、議会事務局、教育委員会、各行政委員会及び警察本部とする。なお、がんセンター局、教育委員会及び警察本部については、知事部局が管理運用する情報システムを利用する所属のみを対象とする。

(2) 情報資産の範囲

この基本方針が対象とする情報資産の範囲は、次に掲げるとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図その他の情報システムに関する文書

(3) 情報システム又はネットワークの範囲

この基本方針が対象とする情報システム又はネットワークの範囲は、(1)に定める行政機関が所管するものとする。ただし、行政系ネットワーク（マイナンバー利用事務系及びLGWAN 接続系）と分割され、各行政機関又は各行政機関の所属において情報セキュリティに関する事項を定めて管理運用するものは対象外とする。

第５ 職員等の遵守義務

職員及び会計年度任用職員（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第10に規定する情報セキュリティ実施手順を遵守しなければならない。

第６ 情報セキュリティ対策

脅威から情報資産を保護するために、次に掲げる情報セキュリティに関する対策を講じるものとする。

(1) 組織体制

本県の情報資産について、情報セキュリティに関する対策を推進する全庁的な体制（以下「推進管理体制」という。）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その内容に応じて分類し当該情報資産の重要性に応じた情報セキュリティに関する対策を行う。

(3) 情報システム全体の強靭性の向上

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は、原則として、他の領域と分離するほか住民情報の流出を防ぐ対策を講じる。

イ　LGWAN 接続系は、インターネット接続系と通信経路の分割を行う。

ウ　インターネット接続系においては、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等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及び不正アクセス対策その他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、委託を行う際のセキュリティの確保等及び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切に対応するため、必要に応じて緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

業務委託する場合、外部サービスを利用する場合又はソーシャルメディアサービスを利用する場合には、それぞれの場合に応じた情報セキュリティ確保のための取り組みを行う。

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の遵守の状況を検証するため、定期的に、又は必要に応じて情報セキュリティに関する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の見直し

情報セキュリティに関する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新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

第９ 情報セキュリティ対策基準の策定

第６から第８までに規定する対策等を実施するために、具体的な遵守すべき事項及び判断の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、公開することにより本県の行政運営に支障を及ぼすおそれがあることから、原則として非公開とする。

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、個別の情報システム等について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、公開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

（施行期日）

この基本方針は、平成16 年７月７日から施行する。

附則

（施行期日）

この基本方針は、平成17 年４月１日から施行する。

附則

（施行期日）

この基本方針は、平成19 年４月１日から施行する。

附則

（施行期日）

この基本方針は、平成30 年３月23 日から施行する。

附則

（施行期日）

この基本方針は、平成30 年４月１日から施行する。

附則

（施行期日）

この基本方針は、令和３年４月１日から施行する。

附則

（施行期日）

この基本方針は、令和４年２月 28 日から施行する。

附則

（施行期日）

この基本方針は、令和５年 10 月２日から施行する。