神奈川県市町村電子自治体共同運営協議会情報セキュリティポリシー

情報セキュリティ基本方針

令和３年１月29日

神奈川県市町村電子自治体共同運営協議会

目　次

序　神奈川県市町村電子自治体共同運営協議会情報セキュリティポリシーの構成

神奈川県市町村電子自治体共同運営協議会情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は、神奈川県市町村電子自治体共同運営協議会（以下「協議会」という。）が、神奈川県市町村電子自治体共同運営事業の遂行にあたり、神奈川電子自治体共同運営サービス（以下「共同運営サービス」という。）の運営において取り扱う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をいう。情報セキュリティポリシーは、情報セキュリティへの取組みを共同運営サービスの運営に携わる協議会事務局職員（以下「職員」という。）及び協議会規約及び規程等に基づき設置される、総会、運営委員会、情報保護委員会、事業部会及び研究会等の構成員（以下「構成員」という。）に浸透、普及及び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る。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

①情報セキュリティ基本方針
②情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、共同運営サービス運営業務に関わる実施手順として、神奈川県市町村電子自治体共同運営協議会情報セキュリティ実施手順を策定することとする(下表参照)。

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の構成

文　書　名		内　容
神奈川県市町村電子自治体共同運営協議会情報セキュリティポリシー	神奈川県市町村電子自治体共同運営協議会情報セキュリティ基本方針	共同運営サービスにおける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
	神奈川県市町村電子自治体共同運営協議会情報セキュリティ対策基準	共同運営サービスにおける情報セキュリティ基本方針を実行に移すための共同運営協議会全般の情報資産に関する情報セキュリティ対策の基準
神奈川県市町村電子自治体共同運営協議会情報セキュリティ実施手順		共同運営サービス運営業務に関わる情報セキュリティ対策基準に基づいた具体的な実施手順

情報セキュリティ基本方針

１　目的

共同運営サービスにおいて取り扱う情報には、個人情報のみならず行政運営上重要な情報など、外部に漏洩した場合には重大な結果を招く情報も含まれている。

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御するため、全ての情報システム等が高度な安全性を有することが、共同運営サービスの運営にあたっての不可欠な前提条件である。

このため、情報セキュリティ基本方針は、共同運営サービスにおいて取り扱う情報資産の機密性、完全性及び可用性を維持する上で必要な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を定めるものである。

２　定義

この基本方針において、次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）コンピュータ

汎用コンピュータ、サーバ、ワークステーション、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。

（２）ネットワーク

コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。

（３）情報システム

コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。

（４）情報

意味を持つデータの集まりをいい、紙媒体及び電磁的記録媒体（以下「記録媒体」という。）に記録されたものの全てを含む。

（５）情報資産

コンピュータ、ネットワーク、情報システム、これらに関連する設備及び情報の全てをいう。

（６）モバイル端末

コンピュータのうち、自席にとどまらず、庁舎内外に携帯し、利用できる端末をいう。

（７）特定用途機器

テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、ネットワークに接続されている又は電磁的記録媒体を内蔵しているものをいう。

（８）クラウドサービス

ネットワークに接続されたコンピュータを運営する事業者等が提供する様々なサービス・機能を利用する形態をいう。

（9）ソーシャルメディア
　インターネット上において不特定多数の者が情報を交換・共有する仕組みをいう。例えば、ブログ、ソーシャルネットワーキングサービス、動画共有サイトなど。

(10) ソーシャルメディアサービス
　インターネット上において不特定多数の者が情報を交換・共有する仕組みを提供するサービスをいう。

(11) 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。

(12) 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。

(13) 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。

(14) 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。

(15) 情報セキュリティインシデント
　望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(16) 庁舎
　協議会運営事業に係る事務を処理する目的で利用する建物及び敷地（ただし、庁舎を管理する団体のネットワークに有線ＬＡＮ又は無線ＬＡＮで接続できない区画を除く。）をいう。

3　適用範囲

（1）組織の範囲
　本基本方針は、協議会を適用範囲とする。

（2）物理的エリアの範囲
　本基本方針は、共同運営サービス運営業務を実施する場所等を適用範囲とする。

（3）情報資産の範囲
　本基本方針は、共同運営サービス運営業務遂行のために協議会が保有する情報資産を対象とする。
　なお、電子申請システム、施設予約システム及び電子入札システムの運営に係る情報セキュリティ対策については、契約主体が神奈川県であることから、神奈川県情報セキュリティポリシーに従い実施することとする。

4　職員及び構成員の義務

職員及び構成員は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあ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。

5　情報資産への脅威

情報セキュリティポリシーを策定する上で、情報資産への脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（1）意図的な要因による部外者の侵入、不正アクセス、ウィルス攻撃、サービス不能攻撃等の情報資産の漏えい、破壊、改ざん、消去、重要情報の詐取、内部不正等

（2）非意図的な要因による情報資産の無断持ち出し、設計・開発の不備、プログラム上の欠陥、誤操作、設定ミス、メンテナンス不備、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、不正アクセス、不正操作、正規の手続きによらない端末の接続等による情報資産の漏えい、破壊、改ざん、消去等

（3）地震、落雷、火災等の災害及び事故、故障等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

6　情報セキュリティ対策

協議会は、前記５で示した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ものとする。

ア　個人番号利用事務を取り扱うネットワークにおいては、原則として、外部ネットワーク及び他の内部ネットワーク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パスワード以外の生体認証等を加えた二要素認証の導入等により、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。また、インターネット接続口は、原則として神奈川情報セキュリティクラウドに集約する。

（2）情報セキュリティ管理体制

協議会が所管する情報資産について、情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

（3）情報の分類と管理

情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

（4）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り及び情報資産への損傷、妨害等から保護するために物理的な対策を講ずる。

（5）人的セキュリティ対策

情報セキュリティに関する権限及び責任を定め、十分な教育及び啓発を行う等の人的な対策を講ずる。

（6）技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御及びネットワーク管理等の技術的な対策を講ずる。

（7）運用におけるセキュリティ対策

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及び外部委託を行う際の情報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ずる。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

7　情報セキュリティ対策基準の策定

共同運営サービスの運営において取り扱う様々な情報資産について、前記6の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で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、情報セキュリティ対策基準は、公にすることにより共同運営サービスの運営に重大な支障を及ぼす恐れがあるため非公開とする。

8　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を遵守して情報セキュリティ対策を実施するために、共同運営サービスの運営における個々の情報システムの情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、情報セキュリティ対策基準の基本的な要件に基づき、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共同運営サービスの運営に重大な支障を及ぼす恐れがあるため非公開とする。

9　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が遵守されていることを検証するために、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ものとする。

10　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並びに情報セキュリティに関する状況の変化により、情報セキュリティポリシーを見直すものとする。

附則

この規程は、平成 22 年3月 1 日から施行する。

附則

この規程は、平成 23 年4月 1 日から施行する。

附則

この規程は、平成 28 年5月 9 日から施行する。

附則

この規程は、令和3年1月 29 日から施行する。