

入間東部地区事務組合情報セキュリティポリシー

第1版

令和元年10月11日策定

入間東部地区事務組合

目 次

入間東部地区事務組合情報セキュリティ基本方針

1 目的	- 1 -
2 定義	- 1 -
3 対象とする脅威	- 1 -
4 適用範囲	- 2 -
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 -

入間東部地区事務組合情報セキュリティ基本方針

1 目的

この基本方針は、入間東部地区事務組合（以下「組合」という。）が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ため、組合が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2 定義

(1) 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。

(2) 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。

(3) 情報資産

ネットワーク及び情報システムで取り扱う情報で、開発及び運用に係るものを含む全ての情報をいう。

(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、その情報にアクセスできる状態を確保することをいう。

(7) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(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、その情報にアクセスできる状態を確保することをいう。

3 対象とする脅威

組合は、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、コンピュータウイルス攻撃、サービス不能攻撃等のサイバー攻撃及び部外者の侵入等の意図的な要因に伴う情報資産の漏えい、破壊、改ざん、消去等

(2) 職員等又は外部委託業者による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程違反、プログラムの欠陥、操作・設定ミス、メンテナンス不備、内部・外部監

査機能若しくは外部委託管理の不備、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) 大規模及び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、水道供給、通信の途絶等のインフラの障害からの波及等

4 適用範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関は、管理者、議会事務局及び各行政委員会とする。

(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並びに電磁的記録媒体
- 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等のシステム関連文書

5 職員等の遵守義務

職員、非常勤職員及び臨時的任用職員（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

組合は、上記3の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対策を講じる。

(1) 組織体制

組合の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

組合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、当該分類により情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ、機械室、通信回線、職員等の使用するパソコン等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などの人的な対策を講じるものとする。

(5) 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ものとする。

(6) 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について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、緊急時対応計画を策定するものとする。

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ものとする。

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において、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又は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ものとする。

9 情報セキュリティ対策基準の策定

組合は、上記6から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ものとする。

10 情報セキュリティ実施手順の策定

組合は、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組合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。