吾妻広域町村圏振興整備組合
情報セキュリティポリシー

吾妻広域町村圏振興整備組合

令和８年３月

序章 吾妻広域町村圏振興整備組合情報セキュリティポリシーの構成について

吾妻広域町村圏振興整備組合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）とは、吾妻広域町村圏振興整備組合が所掌する情報資産に関する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総称する。情報セキュリティポリシーは、吾妻広域町村圏振興整備組合が所掌する情報資産に関する業務に携わる全職員（再任用職員・会計年度任用職員を含む。）（以下、「職員等」という。）及び外部委託事業者に普及、定着をさせるものであり、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、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求められている。

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。

なお、情報セキュリティポリシーに基づき、具体的な実施手順として「情報セキュリティ実施手順」を別に策定することとする。（下表参照）

※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は、公にすることにより吾妻広域町村圏振興整備組合の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

情報セキュリティポリシーの構成

文書名		内容
吾妻広域町村圏振興整備組合情報セキュリティポリシー	①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
	②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ネットワーク及び情報システムに関する情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システムごとに定め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

第１章 情報セキュリティ基本方針

１．目的

本基本方針は、本組合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、本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、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。

（4） 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。

（5） 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。

（6） 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。

（7） 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。

３．情報資産への脅威

情報資産に対する脅威として、以下の脅威を想定し、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、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、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、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．情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、本組合すべての情報資産及び情報資産に接するすべての職員、非常勤職員及び臨時職員（以下「職員等」という）並びに委託事業者とする。

５．職員等の遵守義務

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

上記３の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

本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

本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、当該分類に基づき情報セキュリティ対策を実施する。

（3） 物理的セキュリティ

サーバ、情報システム室、通信回線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。

（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等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。

（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、業務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正に対応するため、緊急時対応計画を策定する。

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、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。

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、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。

9．情報セキュリティ対策基準の策定

上記6、7及び8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。

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、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより本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。