

山武郡市広域行政組合
情報セキュリティ
基本方針

目 次

序 山武郡市広域行政組合情報セキュリティポリシーの構成	1
山武郡市広域行政組合情報セキュリティ基本方針	
1 適用範囲	2
2 定義	2
(1) ネットワーク	2
(2) 情報システム	2
(3) 情報資産	2
(4) 情報セキュリティ	2
(5) 内部情報システムネットワーク	2
(6) 自治体情報システムネットワーク	3
3 情報セキュリティ管理体制	3
4 対象とする脅威	3
5 情報資産の分類	3
6 情報セキュリティ対策	3
(1) 情報システム全体の強靱性の向上	4
(2) 物理的セキュリティ	4
(3) 人的セキュリティ	4
(4) 技術的セキュリティ	4
(5) 運用	4
(6) 業務委託と外部サービス（クラウドサービス）の利用	4
7 情報セキュリティ監査の実施	4
8 職員等及び受託業者の義務	5
9 評価及び見直しの実施	5
10 情報セキュリティ対策基準の策定	5

序 山武郡市広域行政組合情報セキュリティポリシーの構成

1 趣旨

当組合の情報システムが取り扱う情報には、個人情報や行政運営上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。

これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、住民の財産や、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが当組合に対する住民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子商取引の発展や電子自治体の実現が期待される場所である。組合がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、組合が所掌する情報資産に関する情報セキュリティ対策を総合的、体系的かつ具体的に整備するために山武郡市広域行政組合情報セキュリティポリシーを定める。

2 情報セキュリティポリシーの構成と位置付け

山武郡市広域行政組合情報セキュリティポリシーは、基本方針及び対策基準により構成され、組合の情報セキュリティ対策の頂点に位置する。また、情報セキュリティを取り巻く状況の変化に対応するために見直しを実施し、継続的に改善を行うものとする。

(1) 山武郡市広域行政組合情報セキュリティ基本方針

情報セキュリティポリシーの最上位に位置する文書であり、組合のセキュリティマネジメントにおける方針を記述したものである。

(2) 山武郡市広域行政組合情報セキュリティ対策基準

情報セキュリティ基本方針の下層に位置する文書であり、項目ごとに遵守すべき事項について基準を記述したものである。

3 情報セキュリティ実施手順書

情報セキュリティポリシーには含まれないものの、情報セキュリティ対策基準で記述された文書を配付すべき対象者ごとに具体的な内容で記述したものである。

山武郡市広域行政組合情報セキュリティ基本方針

1 適用範囲

山武郡市広域行政組合情報セキュリティ基本方針は、当組合が所管する情報資産及びこれらの情報に携わる管理者以下全ての職員（以下「職員等」という。）を対象とする。また、組合との契約により情報資産を扱う委託事業者（以下「委託事業者」という。）にも適用する。

2 定義

(1) ネットワーク

ハードウェア、ソフトウェア、データなどを共有する目的でコンピュータを相互に接続した通信網をいう。またその構成機器及び電磁的記録媒体で構成された処理を行う仕組みをいう。

(2) 情報システム

パソコン、業務端末機、通信関係装置、プログラム等の全部又は一部により構成される数々のデータを処理するためのシステムをいう。

(3) 情報資産

電子情報及び電子情報を管理する仕組み（情報システム、システム開発、運用及び保守のための資料等）の総称をいう。

(4) 情報セキュリティ

情報の機密性、安全性及び利用の可用性を維持することをいう。

- ・ 機密性 情報にアクセスすることが認可されたものだけがアクセスできることを確実にすることをいう。
- ・ 安全性 情報及び処理方法の正確さ及び安全である状態を完全防護することをいう。
- ・ 可用性 認可されたものが必要時に情報及び関連財産にアクセスできることをいう。

(5) 内部情報システムネットワーク

電子メール、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。

(6) 自治体情報システムネットワーク

住民情報、税務、福祉など、厳格な管理が求められる個人情報を取り扱う業務のために構築された専用の閉域ネットワーク及びその情報システムで取り扱うデータをいう。

当該ネットワークは外部インターネットと物理的・論理的に分離されており、適切なアクセス管理と監査体制のもとで、安全かつ確実に情報を処理できる環境として運用している。

3 情報セキュリティ管理体制

当組合の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立する。

4 対象とする脅威

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) 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、水道供給の途絶等のインフラの障害からの波及等

5 情報資産の分類

情報資産をその内容ごとに応じて分類し、その重要度に応じた情報セキュリティ対策を行う。

6 情報セキュリティ対策

情報資産への脅威から情報資産を保護するために、物理的セキュリティ対策、人的セキュリティ対策、技術及び運用におけるセキュリティ対策を講ずる。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。

(1) 情報システム全体の強靱性の向上

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、次の対策を講じる。

内部情報システムネットワークにおいては、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。高度な情報セキュリティ対策として、外部インターネットとの通信を集約した上で、クラウド型UTM導入等を実施する。

(2) 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。

(3) 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。

(4) 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。

(5) 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

(6) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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、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。外部サービス（クラウドサービス）を利用する場合には、利用に係るガイドライン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。

7 情報セキュリティ監査の実施

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、定期的に監査を実施する。

8 職員等及び委託業者の義務

組合が所管する情報資産に関する業務に携わる全ての職員等及び委託業者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当たって情報セキュリティポリシーを遵守する義務を負うものとする。

9 評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに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に対応するために、情報セキュリティポリシーの見直しを実施する。

10 情報セキュリティ対策基準の策定

上記6、7及び9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。

なお、情報セキュリティ対策基準は、公にすることにより当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。

