

南部箕蚊屋広域連合
情報セキュリティポリシー



令和8年3月31日 改定

第1章 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	4
9. 情報セキュリティ対策基準及び実施手順の策定	4

第1章 情報セキュリティ基本方針

1. 目的

本基本方針は、南部箕蚊屋広域連合（以下「広域連合」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、広域連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。なお、本基本方針は、地方自治法第244条の6第1項の規定に基づき規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

また、本基本方針は、広域連合長、議会、選挙管理委員会及び監査委員が共同して策定するものである。

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ものだけが、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. 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、メンテナンスの不備、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

4. 適用範囲

(1) 対象範囲

本基本方針が適用される実施機関は、広域連合長、議会、選挙管理委員会及び監査委員とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報（印刷した文書を含む。）
- ③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

(3) 対象職員の範囲

本基本方針は、広域連合の保有する情報資産を取り扱うすべての職員（会計年度任用職員を含む。）に加え、議員、選挙管理委員及び監査委員とする。

なお、職員以外であって、広域連合の保有する情報資産を取り扱う者については、本基本方針に準じた対応を求めるものとする。

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、業務の遂行にあたって情報セキュリティポリシー等を遵守しなければならない。また、議員、選挙管理委員及び監査委員も執行機関としての責務に基づき、本基本方針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

広域連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組織的体制を確立する。

(2) 情報資産の分類と管理

広域連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行う。

(3) 物理的セキュリティ

サーバー等、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。

(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、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な対策を講じる。

(6) 運用

情報システム監視、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、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。

(7) 業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、委託業者を選定し、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。また、再委託（二以上の段階にわたる委託を含む。）が行われる場合においても、委託事業者を通じて適切な監督及び指導を行うものとする。

外部サービス（クラウドサービスを含む。）を利用する場合には、利用にかかる規定を整備し適切な設定及び管理を行うなど、対策を講じる。

(8) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて、情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。また、監査及び自己点検の結果を踏まえ、必要に応じて情報セキュリティポリシー及び関連規定の不断の見直しを行うものとする。

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、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となった場合には、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及び実施手順の策定

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。

また、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。

なお、情報セキュリティ確保の観点から、情報セキュリティ対策基準及び実施手順については非公開とする。