

人吉球磨広域行政組合
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8年3月 改定

人吉球磨広域行政組合

目次

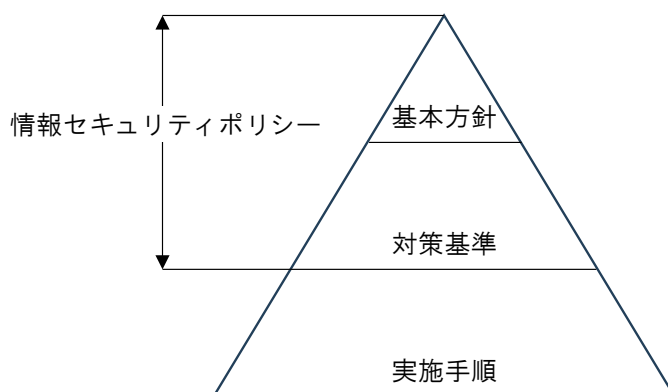
序 人吉球磨広域行政組合情報セキュリティポリシーの構成	1
1. 目的	2
2. 定義	2
3. 対象とする脅威	3
4. 適用範囲	3
5. 職員等の遵守義務	4
6. 情報セキュリティ対策	4
7. 情報セキュリティ監査及び自己点検の実施	5
8. 情報セキュリティポリシーの見直し	5
9. 情報セキュリティ対策基準の策定	5
10. 情報セキュリティ実施手順の策定	5

序 人吉球磨広域行政組合情報セキュリティポリシーの構成

情報セキュリティポリシーとは、地方公共団体が所有する電子計算機やネットワークで取り扱うデータ等の情報を、不正アクセスやウイルスなどの脅威から守るために基本的な考え方を示し、情報の安全性を確保するための体制を確立し、その組織や運用を規定したものである。

人吉球磨広域行政組合情報セキュリティポリシーは、本組合の情報資産を取り扱う全職員に浸透、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。しかし一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、人吉球磨広域行政組合情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の2階層から成るものとして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、情報システム毎に、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。



【基本方針】

情報セキュリティ対策に関する統一かつ基本的な方針

【対策基準】

情報セキュリティ基本方針を実効的に移すための、全ての情報資産に共通の情報セキュリティ対策の基準

【実施手順】

情報システム毎に定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順

1. 目的

本組合が取り扱う情報資産には、住民の個人情報を始めとし行政運営上重要な情報など、部外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おり、これらの情報資産を人的脅威や災害、事故等から防御することは、住民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

また、近年のいわゆるデジタル化の進展により、電子政府や電子自治体の実現が期待されているところである。本組合がこれらに積極的な対応をするためには、本組合が管理しているすべての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となる。

このため、本基本方針では、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) 情報資産

情報システムの開発と運用に係る全てのデータ及び情報システムで取り扱う全てのデータをいう。

(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

本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、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、情報にアクセスできる状態を確保することをいう。

(9) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

- (10) L G W A N 接続系
L G W A N 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（マイナンバー利用事務系を除く。）。
- (11) インターネット接続系
インターネットメール、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。
- (12) 通信経路の分割
L G W A N 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
- (13) 無害化通信
インターネットメール本文のテキスト化や端末への画面転送等により、コンピューターウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3. 対象となる脅威

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な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) 行政機関の範囲
本基本方針が適用される行政機関は、事務局、監査委員及び議会事務局とする。
- (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ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
 - ②ネットワーク及び情報システムで取り扱う情報（これらを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

5. 職員等の遵守義務

職員、非常勤職員及び会計年度任用職員等（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

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) 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、次の三段階の対策を講じる。

- ①マイナンバー利用事務系においては、原則として、他の領域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端末への多要素認証の導入等により、住民情報の流出を防ぐ。
- ②L G W A N 接続系においては、L G W A N 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。
- ③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。高度な情報セキュリティ対策として、熊本県及び本組合のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 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。

(5) 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。

(6) 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。

(7) 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切に対応するため、緊急時対応計画を策定する。

(8) 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、利用にかかる規定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。

(9) 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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、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。

なお、情報セキュリティ対策基準は、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。

10. 情報セキュリティ実施手順

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。