安達地方広域行政組合情報セキュリティポリシー

令和８年４月１日
安達地方広域行政組合

第１章　安達地方広域行政組合情報セキュリティ基本方針

（平成２１年６月１９日決裁）
（令和６年４月１日改正）
（令和８年４月１日改正）

（目的）

第１　安達地方広域行政組合情報セキュリティ基本方針（以下「基本方針」という。）は、本組合が保有する情報資産の機密性、完全性及び可用性の維持するため、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。

（用語の定義）

第２　本基本方針において、次の各号に掲げる用語の定義は、当該各号に定めるとおりとする。

⑴　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。

⑵　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。

⑶　情報資産

情報システム及び情報システムの開発と運用に係る全てのデータ並びに情報システムで取り扱う全てのデータ

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　可用性

情報にアクセスすることを認められた者が、必要な時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。

⑼　LGWAN接続系

LGWAN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。

⑽　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及び財務会計・人事給与シ

ステム（クラウドサービス）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。

⑾　通信経路の分割

LGWAN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。

⑿　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。

⒀　職員等

非常勤職員を除く組合の職員(再任用職員及び会計年度任用職員を含む。以下「職員」という。)

（対象とする脅威）

第３　情報資産に対する脅威、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴　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

⑵　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、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

⑶　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

⑷　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

⑸　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

（管理体制）

第４　組合の保有する情報資産について、情報セキュリティ対策を推進・管理するための全庁的な組織体制を確立する。

（適用範囲）

第５　本基本方針の適用範囲は、総務課（議会事務局、監査事務局を含む。）、あだたら聖苑、もとみやクリーンセンター、東和クリーンヒル、あだたら環境共生センター、消防本部総務課、消防本部警防課、北消防署（出張所を含む。）及び南消防署とする。

（情報資産の範囲）

第６　本基本方針が対象とする情報資産は、次のとおりとする。

⑴　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記録媒体
⑵　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。）
⑶　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

（職員等の遵守義務）

第７　職員及び契約により認められた作業従事者は、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。

（情報セキュリティ対策）

第８　前記第３で示した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。

⑴　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。

⑵　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。

⑶　情報システム全体の強靭性の向上

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。

①　LGAWN接続系においては、LGWAN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。

②　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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。

⑼　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、適宜見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第９　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。

（情報セキュリティポリシーの見直し）

第１０　情報セキュリティの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、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。

（情報セキュリティ対策基準の策定）

第１１　前記第８、９及び１０に規定する対策を実施するために、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。

（情報セキュリティ実施手順の策定）

第１２　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。

（情報セキュリティポリシーに関する違反への対応）

第１３　情報セキュリティポリシーに違反した職員等については、地方公務員法等に基づき懲戒処分等の対象とする。

附　則

この情報セキュリティ基本方針は、平成２１年６月２２日から施行する。

附　則

この情報セキュリティ基本方針は、令和６年４月１日から施行する。

附　則

この情報セキュリティ基本方針は、令和８年４月１日から施行する。