多野藤岡広域市町村圏振興整備組合
情報セキュリティ基本方針

令和　8年　5月制定

多野藤岡広域市町村圏振興整備組合情報セキュリティ基本方針

1　目的

本基本方針は、多野藤岡広域市町村圏振興整備組合（以下「本組合」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、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及び通信機器（ハードウェア及びソフトウェア）。

(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。

(3)　情報資産

ネットワーク、情報システム、情報システムに関する施設・設備、情報システムで取り扱う情報及びシステム関連データ等。

(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。

(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。

(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。

(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、情報にアクセスすることができる状態を確保すること。

(8)　情報セキュリティポリシー

本基本方針と情報セキュリティ対策基準の総称。

(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等。

(10)　LGWAN接続系

LGWAN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（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、ウェブサイト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。

(12)　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。

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)　情報資産の無断持出し、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作・設定ミス、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

本基本方針の適用される範囲は、ネットワーク及び情報システムで取り扱う情報資産、並びに、本組合の全ての情報資産に接する職員、再任用職員及び会計年度任用職員（以下「職員等」という。）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、以下のセキュリティ対策を講じる。

(1)　組合体制

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、次の三段階の対策を講じる。

ア　マイナンバー利用事務系

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、情報の流出を防ぐ。

イ　LGWAN接続系

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。

ウ　インターネット接続系

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。

(4)　物理的セキュリティ

サーバ、電子計算機室、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、アクセス制限、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

情報セキュリティの監視、情報セキュリティポリシーの遵守状況の確認、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、緊急時の対応策を講じる。

(8)　業務委託と外部サービスの利用

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よう努めるものとする。

外部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よう努めるものとする。

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よう努めるものとする。

(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、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恐れがあることから非公開とする。