御浜町農業委員会情報セキュリティ基本方針

制定 令和8年4月1日
御浜町農業委員会

（目的）

第1条 この基本方針は、御浜町農業委員会（以下「本委員会」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、本委員会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。

（定義）

第2条 この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（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） 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。

（5） 完全性
情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

（6） 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。

（7） 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。

（8） 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。

（9） 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、コンピュータウィ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。

（10） 農業委員等
農業委員会長、農業委員会長職務代理者、農業委員、農地利用最適化推進委員、農業委

員会事務局職員のことをいう。

（対象とする脅威）

第3条　本委員会は、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、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、通信の途絶等のインフラの障害からの波及等

（適用範囲）

第4条　この基本方針が適用される行政機関は、農業委員会等に関する法律（昭和 26 年法律第 88 号）に定める農業委員会とする。

2　この基本方針が適用される情報資産は、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(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

（農業委員等の遵守義務）

第5条　農業委員等は、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基本方針を遵守しなければならない。

（情報セキュリティ対策）

第6条　本委員会は、第3条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）　本委員会が保有する情報資産の重要性を機密性、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。

（2）　情報システムに対し、次の対策を講じる。

ア　LGWAN 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。

イ 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、都道府県及び市区町村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。

（3） 農業委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） 情報セキュリティに関し、農業委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。

（5） 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。

（6） 情報システムの監視、情報セキュリティ基本方針の遵守状況の確認、外部委託を行う際のセキュリティ確保等、運用面の対策を講じるものとする。

（7） 情報セキュリティ基本方針の遵守状況を検証するため、定期的又は必要に応じて自己点検を実施し、運用改善を行い情報セキュリティの向上を図るとともに、必要に応じて情報セキュリティ基本方針の見直しを実施する。

付 則

この方針は、令和8年4月1日から適用する。