笠岡市農業委員会情報セキュリティポリシー

笠岡市農業委員会

令和８年３月　策定
令和８年５月　改定

（目的）

第１条　本ポリシーは，笠岡市農業委員会（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。

本委員会の情報資産には，農地の権利移動に関する情報，農業者の個人情報，農業委員会の行政運営上重要な情報など，外部に漏えい等した場合には極めて重大な結果を招く情報が含まれている。これらの情報及び当該情報を取り扱う情報システムを様々な脅威から防御することは，農業者及び市民の財産，プライバシー等を守るためにも，また，事務の安定的な運営のためにも必要不可欠である。

（定義）

第２条　本ポリシーにおいて，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) コンピュータ

パーソナルコンピュータ，サーバ，ストレージ等の機器をいう。

(2) 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。

(3) 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。

(4) 情報資産

本委員会が保有するネットワーク，情報システム及びこれらに関する設備及びデータ（紙媒体を含む。）をいう。

(5) 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。

(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維持し，データの正当性，正確性，一貫性等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。

（対象とする脅威）

第３条　本委員会の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) 人による脅威（故意）

不正アクセスやウイルス攻撃等のサイバー攻撃，機器の盗難，情報資産の不正な操作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等

(2) 人による脅威（過失）

情報資産の管理不備，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，メンテナンス不備，外部委託管理の不備等の過失による情報資産の漏えい・破壊・消去等

(3) 災害による脅威

地震，落雷，火災，水害等の災害によるサービス及び業務の停止，情報資産の消失等

(4) 必要資源の不足，故障等による脅威

災害の影響又はその他の原因による電力，通信，水道の途絶，交通機能の麻痺や大規模・広範囲にわたる疾病の蔓延による要員の不足，機器の故障等によるサービスや業務の停止，システム運用の機能不全等

（適用範囲）

第４条　本ポリシーが適用される組織は，本委員会とする。ただし，本委員会事務局が笠岡市情報セキュリティポリシーで適用される情報資産を取り扱う場合は，笠岡市情報セキュリティポリシーを遵守するものとする。

２　情報資産の範囲

本ポリシー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

（職員等及び委員の遵守義務）

第５条　本委員会事務局職員，会計年度任用職員等（以下「職員等」という。）並びに農業

委員及び農地利用最適化推進委員（以下「委員」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は本ポリシー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　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) 組織体制

本委員会の情報資産について，適切に情報セキュリティ対策を推進・管理するための体制を確立する。

(2) 情報資産の分類と管理

本委員会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) 物理的セキュリティ対策

通信回線及び端末等への物理的な対策を講ずる。

(4) 人的セキュリティ対策

情報セキュリティに関し，職員等及び委員が遵守すべき事項を定めるとともに，研修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対策

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) 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は，笠岡市が定める緊急時対応計画を準用し，迅速かつ適正に対応する。

(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。また，外部サービス（クラウドサービス等）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。

（情報セキュリティ管理体制）

第７条　本委員会の情報セキュリティ対策を推進するため，以下の管理体制を整備する。

(1) 会長　　最高情報セキュリティ責任者

(2) 事務局長　　統括情報セキュリティ責任者，情報セキュリティ責任者，情報資産管理責任者

(3) 事務局職員　　情報システム担当者

（情報セキュリティに関する監査及び自己点検の実施）

第８条　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に関する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９条　情報セキュリティに関する監査及び自己点検の結果又は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，情報セキュリティポリシーを見直しを行い，必要に応じて改定する。

（その他）

第１０条　本ポリシーに定めのない事項については，原則として笠岡市情報セキュリティ基本方針及び笠岡市情報セキュリティ対策基準の規定を準用するとともに，会長が決定する。