情報セキュリティ基本方針

株式会社三重県農協情報センター

改廃履歴

Ｒｅｖ	改 廃 内 容	実　施　日
1.0	初版	2005.04.01
1.1	新社長就任	2005.08.01
1.2	ＩＳＯ２７００１移行対応	2006.11.01
1.3	社長交代	2008.10.30
1.4	規程表題等、全面見直し	2009.10.01
1.5	センター長設置に伴う変更および書式変更	2010.07.01
1.6	役員執行体制の変更に伴う改正	2010.08.31
1.7	役員執行体制の変更に伴う改正	2011.07.08
1.8	第２条　表現修正	2012.01.01
1.9	監査部から監査室に改称	2012.04.01
2.0	フロッピーディスクの文言削除	2016.09.01
2.1	役員執行体制の変更に伴う改正	2021.06.30
3.0	ＩＳＭＳ規格改訂対応	2024.10.01
3.1	旧規格名称（JIS Q 13335-1:2006）を削除	2024.12.01

目　　次

情報セキュリティ基本方針

制 定 日　２００５年　4月　1日
改 正 日　２０２４年12月　1日

（目　　的）

第　１条　当社が所有する情報資産は経営資源としての資産価値が高まってきている。その一方で、情報資産に悪影響を与える脅威も増加してきており、このような脅威の具現化によって社会的信用の失墜、事業の中断および経営資産を喪失するセキュリティ事件・事故は、当社にとっても早急に対応しなければならない経営課題である。従って当社は、様々な脅威から当社の情報資産を保護するとともに、緊急時においても従業員が迅速にかつ適切に対応し、情報セキュリティに関する責任を果たせるようにするために、情報セキュリティマネジメントシステムを構築する。

本書は情報セキュリティマネジメントを実践するにあたり、基本的な考え方および方針を定め、当社における情報資産の管理を徹底することを目的とする。

（用語の定義）

第　２条　用語の定義は以下のとおりとする。なお、本定義は、情報セキュリティ管理・運用で使用する全ての文書に適用する。

(1)　情報資産 情報（紙文書、電子データ、電子データの印刷物およびコンピュータ・ディスプレイ等へ表示されたものを含む)、情報を取り扱うための機器（情報を処理するコンピュータおよびそれを利用するために必要なデータ通信装置、電子データを格納する保存媒体、空調設備等を含む)、サービス（電力、通信サービス等を含む)、ソフトウェア、施設およびそれらを取り扱う人材をいう。
(2)　情報セキュリティ 情報資産の機密性、完全性および可用性を確保し維持することをいう。機密性、完全性、可用性の定義は以下のとおりとする。 ①　機密性（ Confidentiality ） 許可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性。 ②　完全性（ Integrity ） 資産の正確さおよび完全さを保護する特性。 ③　可用性（ Availability ） 認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性。
(3)　ＩＳＭＳ(Information Security Management System) マネジメントシステム全体の中で、事業リスクに対する取り組み方に基づいて、情報セキュリティの確立、導入、運用、監視、レビュー、維持および改善を担う部分。 注記：マネジメントシステムには、組織の構造、方針、計画作成活動、責任、実践、手順、プロセスおよび経営資源が含まれる。
(4)　従業員等 当社の取締役、監査役（以下「役員」という）ならびに、当社と雇用契約を締結する全ての従業員（社員、試雇社員、嘱託社員、受入出向社員、雇員、パートタイム社員等を含む）および当社の業務に従事する派遣社員、外部委託契約をした企業の要員をいう。

(5)	情報利用者 従業員等のうち当社の情報資産を取り扱う者をいう。

（適用範囲）

第　３条　情報セキュリティ基本方針の適用範囲は、当社の保有する次の全ての情報資産に適用する。

(1)	情報システム
(2)	情報システム内に存在する情報
(3)	その他、情報資産に関連する人的、物理的、環境的リソース

（適用対象者とその責務）

第　４条　　情報セキュリティ基本方針の適用対象者は、当社従業員等のうち情報資産を利用する全ての者であり、情報セキュリティ基本方針の定める事項を認識し、理解し、遵守する責務を負う。

(1)	役員、センター長、部長および副部長の責務 ①意思決定が、情報セキュリティ基本方針に背反しないこと。 ②率先してＩＳＭＳを推進すること。 ③セキュリティ事件・事故に対する復旧策や再発防止策を講じること。 ④情報資産が適切に管理・保護されていることを確認すること。 ⑤派遣業者、外部委託業者に作業・業務を委託する場合は、契約上で機密保持にかかる事項を明確にし、適切に管理すること。
(2)	従業員の責務 ①情報セキュリティ基本方針に準拠した手順を実施すること。 ②セキュリティ事件・事故を発見した場合には、手順に従って速やかに報告すること。

（情報セキュリティ対策の体系）

第　５条　当社のＩＳＭＳで使用する文書・記録の体系は、以下の通りとする。

(1)	情報セキュリティ基本方針 情報セキュリティ基本方針は、文書体系の上位に位置し、本書は、経営者の意思を表明したものであり、情報セキュリティ管理・運用を実現するための基本方針を示す。
(2)	情報セキュリティ対策規程等関連規程 情報セキュリティ対策規程等関連規程は、情報セキュリティ基本方針に基づき、情報セキュリティ対策を実施するにあたって、従業員等が遵守すべき管理策を示す。
(3)	情報セキュリティ実施手順 情報セキュリティ実施手順は、情報セキュリティ対策規程等関連規程で定める管理策に基づき、情報セキュリティ管理・運用に関する具体的な実施手順を示す。
(4)	情報セキュリティ実施記録 ＩＳＭＳ要求事項の適合性と効果的な運用がされている事を示す記録を適切な期間保存する。

（情報セキュリティ対策の体制）

第　６条　当社の情報セキュリティ管理・運用の維持改善を推進することを目的として、最高情報セキュリティ責任者、最高情報セキュリティ責任者代理、情報セキュリティ責任者、情報

セキュリティ管理者を定め、情報セキュリティ管理・運用の運営体制を整備し、個々の役割と責任を明確にする。また、これらのメンバーによる情報セキュリティ委員会および情報セキュリティ委員会事務局を設置する。

（情報の分類および管理）

第　７条　情報利用者は、情報資産については、情報の機密性、完全性、可用性を踏まえ、その重要度に応じて分類し、それに応じたセキュリティ対策を施し、適切に管理する。

（リスクマネジメント）

第　８条　情報セキュリティ委員会は、情報資産に対する脅威を洗いだし、その脆弱性について十分認識しておかなければならない。また、脅威から情報資産を保護するために、必要なセキュリティ対策を講じなければならない。

（関連法規の遵守）

第　９条　情報利用者は、関連法令および関連規格（ｶﾞｲﾄﾞﾗｲﾝ）を遵守し、必要に応じて当社独自の管理基準を設定し、継続的な情報セキュリティの確保を維持する。

（教育・研修）

第１０条　情報セキュリティ委員会は、情報セキュリティ基本方針および情報セキュリティ対策規程等関連規程の従業員等への浸透と情報セキュリティ意識の向上のため、情報セキュリティに関する教育・研修を定期的に実施する。情報利用者は、会社が提供する情報セキュリティの教育を受けなければならない。また、情報セキュリティに関する最新情報の取得に努めなければならない。

（情報セキュリティに関する違反への対応）

第１１条　情報セキュリティ基本方針および情報セキュリティ対策規程等関連規程に違反した場合は、その重大性、発生した事案の状況に応じて就業規則等に基づき、懲戒処分等の対象とする。

（情報セキュリティ事件・事故時の対応）

第１２条　情報利用者は、当社の情報セキュリティが侵害されたと思われる事象が判明した場合は、速やかに定められた手順に従って対応しなければならない。

（監査）

第１３条　監査室は、情報セキュリティ基本方針および情報セキュリティ対策規程等関連規程が遵守されていることを確認するため、定期的に情報セキュリティ実施状況を監査する。

（評価および見直し）

第１４条　情報セキュリティ委員会は、情報セキュリティ実施状況の監査結果から、情報システムの変更、新たな脅威等、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティ基本方針および情報セキュリティ対策規程等関連規程、情報セキュリティ実施手順の見直しを定期的に実施する。

（例外事項）

第１５条　本方針は、原則として例外は認めない。ただし、情報セキュリティ委員会が判断し、かつ最高情報セキュリティ責任者が承認した場合にはこれを認める。

（改廃）
第１６条　本方針の改廃は、情報セキュリティ委員会事務局が起案し、社長が決裁する。