情報セキュリティ運営要領

制定 H2402　改定 H2710　改定　R803

第一章　基本事項

（目　的）

第１条　本要領は、「情報セキュリティ基本方針」「情報セキュリティ基本規程」に従い、当組合における情報セキュリティマネジメントシステムの運営のために必要な事項を定めるものである。農業協同組合連合会、農業協同組合中央会、その他農業協同組合系統組織等からの情報セキュリティに関する指示がある場合、それに従うものとする。また、本要領に定めるものの他、別途、官公庁、行政、その他関連団体等からの情報セキュリティに関する指示がある場合、それに従うものとする。

（用語の定義）

第２条　本要領で使用する用語は、「情報セキュリティ基本方針」「情報セキュリティ基本規程」に従う。

②　その他の用語については、必要に応じて定める。

第二章　情報の分類と管理

（情報の管理責任の明確化）

第３条　情報セキュリティ統括管理者は、すべての情報資産に関する情報セキュリティを統括する権限及び責任を有し、情報セキュリティ部門管理者及び情報システム管理者を指導、監督する。

②　情報は、当該情報の作成等を行った各室部等が管理責任を有し、情報セキュリティ部門管理者を責任者とする。ただし、各室部等において、特別の定めがある場合はこの限りではない。

③　情報セキュリティ部門管理者は、該当情報について分類を行い、その重要性に応じた管理を行うよう努める。

（利用者の責任）

第４条　情報を使用する者は、情報の分類に従い使用する責任を有する。利用者は、情報の分類に関する定義及び管理方法を理解し、定められた規則に従った利用を行う。（個人番号関係事務実施者の責任）

第５条　当組合は、特定個人情報等の漏えい、滅失又は毀損の防止等、特定個人情報等の管理のために、必要かつ適切な安全管理措置を講じなければならない。

②　当組合は、職員が特定個人情報等を取扱うに際し安全管理措置が適切に講じられるよう、当該職員に対する必要かつ適切な監督を行われなければならない。

（情報の分類及び表示）

第６条　役職員等の扱う重要な情報は、以下の３種類に分類する。

１「極秘情報」とは、組合経営（事業）に大きな影響が予想される情報。個人情報、特定個人情報、機密情報等。

２「秘密情報」とは、情報の開示を制限する等厳格な取扱いを行う情報。実績、規程等。

３　その他情報とは、上記以外の情報であり、開示を制限しない情報。

②　情報の分類の表示については、第三者が当該情報の重要性を容易に認識できないように注意する。

（情報の取扱い）

第７条　役職員等の扱う重要な情報は、定められた分類に従って取り扱う。

１　情報は、各分類に従いアクセス権限を定める。

２　情報の保管場所は以下に定める条件を満たす場所とする。

極秘情報　…紙、外部記憶媒体等、物理的媒体は金庫室又は耐火金庫とし、原則として使用時以外は施錠を行うものとする。電子データに関してはアクセス制限されたサーバ上の領域又はアクセス制限されたパソコン上に保存する。外部記憶媒体上に保存する際には暗号化又はデータへのパスワードの付加を行う。

ＦＡＸによる送信を行う際は、発信前に受信者に対し発信の旨を連絡の上、送信する。

郵便等の手段により送付する際には、事故時に送付経路をさかのぼり可能とするため、書留、配達記録、宅配便等の手段を必須とするものとする。また損傷を防止するため、保護材の使用等、物理的な防護策を講じた上で送付する。

秘密情報　…紙、外部記憶媒体等、物理的媒体は、施錠可能な書庫・書棚（キャビネット）とし、業務時間外は施錠を行うものとする。電子データに関してはアクセス制限されたサーバ上の領域又はアクセス制限されたパソコン上に保存する。

その他情報…原則として保管場所の指示は行わない。

３　法令、規制、契約及び事業上の要求により、安全に保管する必要がある文書

は、消失、破壊及び改ざんから保護するため、適切な保管期間、記録媒体、保管及び取扱いの手順を定めるよう努める。

4　機密情報は、保有、廃棄、アクセス権限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いの方法等を定める。

5　極秘情報及び秘密情報は暗号化やマスキング等の取扱い方法等を定める。

（特定個人情報の管理）

第８条　特定個人情報を取扱う事業者は以下の事項を遵守する。

1　特定個人情報の提供の要求は、個人番号関係事務を処理するための場合に限ってのみ行う。当組合で認められている業務範囲内及び国の機関が法令で定める事務を除き個人番号の提供を求めてはならない。

2　特定個人情報の提供を求める期限は、個人番号関係事務が発生した時点で個人番号を求めることが原則だが、役職員や顧客との法律関係に基づき、個人番号関係事務の発生が予想される場合には、契約を締結した時点で個人番号の提供を求められるが、契約内容等から、個人番号関係事務が明らかに発生しないと認められる場合には、個人番号の提供を求めてはならない。

3　特定個人情報の提供制限として、番号法で限定的に明記された場合を除き、特定個人情報を提供してはならない。

4　特定個人情報の第三者提供として、特定個人情報の提供を求められた場合には、その提供を求める根拠が、番号法第19条各号に該当するものかどうかをよく確認し、同条各号に該当しない場合には、特定個人情報を提供してはならない。

5　個人番号の収集は、当組合で定めた場合を除き、他人の個人番号を含む特定個人情報を収集又は保管してはならない。

6　個人番号が記載された書類等で所管法令により一定期間保存が義務付けられているものは、その期間を超えて保管してはならず、保存期間を経過した場合には、個人番号をできるだけ速やかにマスキング、廃棄又は削除しなければならない。

　また、特定個人情報等を削除又は廃棄した場合は、その記録を保存し責任ある立場の者が確認を行う。

7　本人確認として、当組合が定めた方法で本人確認を行わなければならない。

8　特定個人情報が違法に第三者に提供されていることを知った本人から、その提供の停止が求められた場合であって、その求めに理由があるときは、遅滞なく、当該特定個人情報の第三者への提供を停止しなければならない。

　ただし、第三者への提供を停止することが困難であり、本人の権利利益を保護するために代わりの措置をとるときは、第三者への提供を停止しないことを認める。

②　特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善を行

うため、以下の事項について確認する。

１　取扱規程等に基づいて、特定個人情報等の取扱いが行われているか確認する。

２　特定個人情報等の取扱い状況について、「個人データ取扱台帳」を整備し、当該台帳上に、当組合が管理する特定個人情報ファイルおよび付随する特定個人情報等の種類について記録する。

３　取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。

（利用者の情報管理）

第９条　当組合が利用者の重要情報を網羅的に洗い出し、把握、管理する。洗い出しの範囲は、業務、システム、外部委託先とし、以下の情報を対象とする。

１　通常の業務では使用しないシステム領域に格納されたデータ

２　害解析のためにシステムから出力された障害解析用データ

３　ATM(店舗外含む)等に保存されている取引ログ等

②　洗い出した利用者の重要情報について、重要度判定やリスク評価を行い、重要度やリスクに応じて、情報管理ルールを策定する。

１　情報の暗号化、マスキングのルール

２　情報を利用する際の利用ルール

３　記録媒体等の取扱いルール

４　機密情報の暗号化、マスキングのルール

第三章　リスク分析・評価の実施

（リスク分析・評価の実施）

第１０条　情報セキュリティ部門管理者は、自室部が保有する情報資産について、定期的にリスク分析・評価を実施し、自室部が保有する対象情報資産を把握する。

第四章　人的セキュリティ

（教育及び研修）

第１１条　情報セキュリティ事務管理者及び情報セキュリティ部門管理者は、全ての役職員等及び関係する者に対し、説明会や研修を定期的に行う。説明会や研修には、以下の事項を含めるよう努める。

１　情報セキュリティ基礎

ア．電子メール、Web の利用方法

イ．パスワード管理

ウ．マルウェア対策等
エ．情報セキュリティ侵害事例等

２　当組合における情報セキュリティに関する取り組み内容
ア．情報セキュリティ基本方針の説明
イ．情報セキュリティ基本規程等の説明(体制、責任者、懲罰等)
ウ．役職員等の遵守義務
エ．情報資産の正しい取扱い方法
オ．情報セキュリティ侵害などの発生時の対応
カ．関連法令等

（非常勤職員等の雇用）

第１２条　情報セキュリティ部門管理者は、非常勤職員等の雇用時に非常勤職員等が守るべき情報セキュリティ基本方針、情報セキュリティ基本規程及び関連する規程類等の内容について説明を行い、遵守を義務付ける。

１　非常勤職員等を雇用する場合、非常勤職員等が守るべき事項を契約書等に記載する。

（外部委託者の管理）

第１３条　情報セキュリティ部門管理者は、外部委託者等が守るべき情報セキュリティ基本方針、情報セキュリティ基本規程及び関連する規程類等の内容について説明を行い、遵守を義務付ける。

②　情報セキュリティ部門管理者は、外部委託者のアクセス制御を以下のように行う。

１　外部委託者が端末による作業を行う場合、外部発信アドレスを付与しないことにより、インターネットや電子メールの使用を制限する。業務上必要な場合は、情報システム管理者の許可を得る。

２　情報システムにおけるアクセス権限等を明確にし、外部委託者が不正アクセスできないようにする。

３　外部委託者が持ち込んだ端末の情報ネットワーク接続は行わせない。

③　外部委託先に対して自らが果たすべき安全管理措置と同等の措置が講じられるように監督する。

④　当組合は、外部委託先の再委託先を以下のように管理する。

１　外部委託先が再委託を行う場合は、当組合の許諾を得た場合に限り再委託をすることができる。

２　再委託を受けた者は、再委託を受けた個人番号関係事務を行うことができるほか、当組合の許諾を得た場合に限り、その事務を更に再委託することができる。

３　当組合は、委託先が再委託先に対し必要かつ適切な監督を行っているかどうかを監督する。

（役職員等の異動及び退職）

第１４条　情報セキュリティ部門管理者は、役職員等の異動及び退職時には、それに伴って不要となる鍵やパソコンなど情報セキュリティに関する配付物を回収する。

回収したパソコンについては、引継ぎ等で事後も必要となる情報を除き、他の役職員へ再配付する前に内容を消去する。

②　情報セキュリティ部門管理者及び情報システム管理者は、役職員等の異動及び退職時には、それに伴って不要となるアクセス権限を変更又は消去する。

（利用者の対応）

第１５条　利用者が当組合の情報システムを使用する上で、以下の対応を行う。

１　インターネット上での暗証番号等の個人情報の詐取の危険性、類推されやすい暗証番号の使用の危険性、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクの説明や、利用者に求められるセキュリティ対策事例の周知を含めた注意喚起等を利用者に対して行う。

２　利用者からの届出を速やかに受け付ける態勢を整備する。

３　不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングする。

４　不正取引に係る損失の補償については、利用者保護を徹底する観点から、個人利用者及び法人利用者への対応方針等を定める。

５　不正取引に関する記録を適切に保存するとともに、利用者や捜査当局から当該資料の提供等の協力を求められたときは、これに誠実に協力する。

第五章　不測事態対応

（情報セキュリティ侵害時対応）

第１６条　情報セキュリティ委員会は、侵害に備え情報セキュリティ侵害への対応手順を策定する。

②　情報セキュリティ侵害に際しては、情報セキュリティ侵害への上記対応手順に従い対応する。

（災害対応）

第１７条　情報セキュリティ委員会は、災害発生に備え、災害への対応手順を策定する。

② 災害発生に際しては、上記対応手順に従い対応する。

第六章 法令遵守

（関係法令等の特定、認識及び見直し）

第１８条 遵守すべき法規制等を特定し、情報セキュリティ基本規程及び本要領等と法令等との矛盾を発見した場合、直ちに関係各文書を改訂しなければならない。

② 遵守すべき法令等に関して、適宜、新たに対応が必要となる法令等の有無や、既に特定された法令等の改正の状況等を把握するものとする。

第七章 情報セキュリティに関する違反への対応

（処分）

第１９条 役職員等は、情報セキュリティ基本規程及び本要領に違反した時は、就業規則に定める手順に基づく処分の対象となる。

② 番号法に違反した時は、法的な罰則の対象となりうる。

第八章 予防処置

（未然防止に関連する情報の把握、調査）

第２０条 情報セキュリティ統括管理者は、常に以下のような内部・外部環境の変化に関する各種情報を把握し、組合の情報セキュリティに対する影響を検討するよう努める。これらには、実際に事象が確認されたものだけでなく、将来的なもの、潜在的なものも考慮する。

１ 組合内の組織変更
２ 新規事業の開始、事業プロセスの大幅な変更
３ 法令等の改定、社会環境の変化
４ 情報セキュリティ技術革新等に伴う情報セキュリティ上のリスクの変化
５ サイバー攻撃の高度化・巧妙化

② 緊急事態が発生した場合の対応として、あらかじめコンティンジェンシープランを策定し、緊急時体制を構築する。コンティンジェンシープランの策定は、以下の内容を考慮する。

１ 客観的な水準が判断できる根拠
２ 災害による緊急事態
３ 当組合の内部又は外部に起因するシステム障害等
４ 他の JA 及び金融機関におけるシステム障害等の事例

５　中央防災会議等の検討結果

（システムリスクに対する認識、対策）

第２１条　代表理事は、システム障害等の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備する。

②　代表理事及び理事は、システム障害等発生の危機時において、果たすべき責任やとるべき対応について具体的に定める。また、自らが指揮を執る訓練を行い、その実効性を確保する。

③　理事会は、コンピュータシステムのネットワーク化の進展等により、リスクが顕在化した場合、その影響が連鎖し、広域化・深刻化する傾向にある等、経営に重大な影響を与える可能性があるということを十分踏まえ、リスク管理態勢を整備する。

④　情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、自らの利用者や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備をする。

（緊急事態に備える訓練の実施）

第２２条　コンティンジェンシープランに基づく訓練を全体的なレベルで行い、外部委託先等と合同で、定期的に実施し、業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害等が発生した場合に、速やかに業務を継続できる態勢を整備する。

第九章　評価及び見直し

（監査）

第２３条　内部監査部門のシステム関係に精通した要員が定期的にセキュリティ監査を行う。また、外部の業者に委託する場合には、情報システム管理者の承認を得て委託事業者を選定する。監査を行う際の留意点について、以下の事項を考慮する。

１　監査活動が業務に与える影響を最小限に抑えるための計画策定

２　監査を受ける部門から独立した監査人による監査

３　情報セキュリティ基本規程及び関係要領等に準拠した監査

４　システムリスクに関する業務全体をカバーした情報セキュリティ監査

５　管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢の継続的な見直し

６　監査結果の理事会への報告

７　監査結果に基づいて、不十分と指摘された事項の適切な措置

（点検）

第２４条　情報セキュリティ基本規程及び本要領に沿った情報セキュリティ対策が実施されているかどうかについて、定期的に、情報セキュリティにかかる自主点検等を行うよう努める。

第十章　その他

（要領の改廃）

第２５条　この要領の改廃は組合長が行う。この要領に定めなき事項は、組合長がその都度定めるものとする。

附　則

この要領は、平成 24 年 2 月 27 日から施行する。

この要領の改正は、平成　年　月　日から施行する。

この要領の改正は、令和　年　月　日から施行する。