情報システム運用要領

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システムの運用に必要な事項を定めるものである。

（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」、「情報セキュリティ運営要領」に従う。

②　その他定めのない用語については、必要に応じて定める。

（管理の対象）

第３条　本要領における管理の対象は、当組合内の情報資産とする。

　情報資産には組合外の情報システム等により作成又は保持されている情報を組合内に取り込んだものも含む。

　取り込み手段にはデータの複製、紙媒体、外部記憶媒体のいずれも該当するものとする。

第二章　技術的セキュリティ

（アクセスログの取得と管理）

第７条　情報システム管理者又はその指名する者は、次のログを取得するよう努める。ログは、アクセス権限を設定して許可されていないアクセスから保護し、一定期間保管するよう努める。

１　役職員等及び情報システム管理者等のログイン及びログオフ状況（時刻、利用者アカウント、成功又は失敗、接続元端末等）。

２　組合内情報ネットワーク、インターネットへのアクセスログ（時刻、接続元、接続先、許可/拒否等）。

３　ファイアウォール及び不正侵入監視装置（設置されている場合）のログ。

４　アプリケーション及びオペレーティングシステムのエラーログ。

② 情報システム管理者又はその指名する者は、ログが窃取、改ざん、消去されないように、ログのアクセス権限をシステム管理者権限に限定しておく。
③ 情報システム管理者又はその指名する者は、対象ログを記録する機器の時刻設定を適正に保ち、定期的にログを分析、監視する。
④ 役職員等にログを取得している旨を通知することにより、不正アクセスの牽制を行う。

（システム管理および作業の確認）
第８条 情報システム管理者又はその指名する者は、以下のシステム変更等の処理について指示を行う。
１ 機器、ソフトウェアの運用手順、および設定の変更
２ 登録済みのプログラムの変更
３ 新規プログラムのインストール作業

（障害の記録）
第９条 情報システム管理者は、情報セキュリティ部門管理者又は役職員等から報告のあった情報システム障害又は通信システムの問題等について、次の事項を記録する。
１ 発生日時、発生場所、発見者。
２ 対象（オペレーティングシステム、アプリケーション、機器、回線の別等）と発生内容。
３ 障害解決の方法。
４ 対応者、復旧後の平常運用の確認方法

（情報システムに関する文書等の管理）
第１０条 情報システム管理者は、情報システムに関する文書（仕様書、設定文書、操作手順書、ソフトウェア等）について、記録の媒体に関わらず、業務上必要とする者のみが閲覧できるように保管する。
② 組合外の組織と情報システムに関する情報及びソフトウェア等をやりとりする場合は、情報システム管理者の許可を得て行う。

（電子メール）
第１１条 電子メールが適切に使用されるように次の対策を行う。
１ 電子メールの不正中継の禁止
２ 私用メールアドレスへの転送禁止
３ 重要電子メールのアクセス制御

４　電子メールで送信する重要ファイルの暗号化（パスワードファイル、個人情報ファイル、機密情報ファイル等）

（外部の者が利用できる情報システムへの対策）

第１２条　外部公開 Web サーバ等の外部の者が利用できる情報システムについては、公開する情報の正確性の確認や意図しない秘密情報の公開を防止するため、情報を外部に公開する前に、情報セキュリティ部門管理者による承認を得る。

②　情報システム管理者は、外部に公開するサーバについては、次の内容を考慮し、必要な対策を講じる。

１　適切なセキュリティパッチ等の適用
２　不要なサービスの削除
３　侵入検知システムによる監視
４　改ざんチェックシステムによる監視
５　業務に応じた適切な不正防止策
６　利用者が取引相手を誤認しないための構成
７　フィッシング詐欺対策
８　サイバー攻撃に対する監視

③　外部の者から公開サーバを介して個人情報等の重要情報を受信する場合には、情報の収集時、保管時に暗号化等（ＳＳＬの利用等）による保護を行う。

（電子署名の利用）

第１３条　情報システム管理者は、役職員等が必要に応じて電子署名の利用が行えるよう、必要な整備を行うよう努める。

（業務目的外利用の牽制）

第１４条　役職員等は、業務目的以外での組織外部の Web サイトの閲覧、電子メール・システムの使用等をしてはならない。

②　情報システム管理者又はその指名する者は、役職員等に対して、Web サイトの閲覧やメールの送受信が監視されていることを周知する。

③　情報システム管理者又はその指名する者は、役職員等の不正利用が明らかとなった場合には、上司へその旨通報し、本人へもその旨通知する。

（無許可ソフトウェア導入の牽制）

第１５条　情報システム管理者は、許可していないソフトウェアを役職員等が勝手に端末にインストールができないように制限する。

②　情報システム管理者が許可していないソフトウェアのインストールが業務上必要

な場合には、役職員等からの申請を受けた上で、情報セキュリティ部門管理者及び情報システム管理者が許可する。

③　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許可するにあたって、事前に情報システム等への影響を考慮し、問題が起きないことを確認する。

（情報システム機器の管理）

第１６条　情報システム機器の構成及びユーザの管理は、情報セキュリティ部門管理者を通じて、情報セキュリティ事務管理者の承認を得る。

②　情報システム管理者は、役職員等による、端末に対する改造及び機器の増設･交換を禁じる。

③　端末に対する改造及び機器の増設･交換が業務上必要な場合には、役職員等からの申請を受けた上で、情報セキュリティ部門管理者及び情報システム管理者が許可する。変更時の設定及び構成情報等は記録し、履歴として保存する。

（外部接続機器の導入時の遵守事項）

第１７条　情報システム管理者は、役職員等による、モデム等の機器の増設による他の情報ネットワーク接続や、外部からのアクセスを可能とする情報システムの構築を禁じる。

②　それらが業務上必要な場合には、役職員等からの申請を受けた上で、情報セキュリティ部門管理者及び情報システム管理者が許可する。

（電子取引・オンライン取引における遵守事項）

第１８条　役職員等は、電子的な取引が必要な場合は、利用規約等に示されるセキュリティ事項を確認した上で、取引を行う。

②　買い手が当組合のシステムを利用する際の留意事項等についての説明を行う。

③　インターネット等の通信手段を利用した非対面の取引を行う場合には、次のような対策の複数の組合せによる効果的なセキュリティ対策を行う。

１　可変式パスワードや電子証明書等の認証方式

２　複数経路による取引認証

３　ハードウェアトークン等でトランザクション署名を行うトランザクション認証

４　取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供

５　利用者のパソコンのウィルス感染状況を組合側で検知し、警告を発するソフトの導入

６　電子証明書をICカード等、取引に利用しているパソコンとは別の媒体・機器への格納する方式の採用

７　不正なログイン、異常な取引等を検知し、速やかに利用者に連絡する体制の整備

（情報へのアクセス）

第１９条　組合は、情報資産がその目的に沿って適切に使用されるよう、正当な必要性に基づくアクセスのみを許可する。組合はこのために必要な時間、資源を投入し、情報システム機器を含む情報資産へのアクセスを管理、監視するよう努める。

注）ＪＡでサーバ等を設置し管理する場合は、次の条項を追加し以下の条項を繰り下げる。

（自動識別）

第２０条　組合内で使用する重要なサーバ等において、機器の固有情報（MAC アドレスや IP アドレス等）により、アクセスのフィルタリングを行う。

②　アクセス制御に関するルールを作成し、定期的な見直し、更新を行う。

（利用者アカウント及びアクセス権限の管理）

第２１条　情報セキュリティ部門管理者は、利用者アカウントの登録、変更、抹消及び利用者アカウントに付随するアクセス権限を管理する。

②　利用者アカウント及びアクセス権限の管理に必要な管理者権限は情報セキュリティ事務管理者の指示のもと、情報システム管理者が使用するものとする。

③　パスワード等、管理者権限を行使するために必要かつ機密性を要する事項は、情報システム管理者が既存のシステム運用や業務の遂行に支障がないことを確認した後、情報セキュリティ事務管理者の指示により変更する。

④　情報セキュリティ部門管理者は、役職員の役職員の採用、異動、退職及び組合外への出向等による利用者アカウントの登録、変更、抹消を次のように行う。

１　情報セキュリティ部門管理者の申請のもと、情報セキュリティ事務管理者の承認を得た上で、情報システム管理者又はその指名する者は、人事異動情報に基づき、必要な役職員等の利用者アカウントの登録･変更・抹消処理を行う。

２　非常勤役職員等のアカウント登録は、業務上必要な場合に限り行う。

３　退職等により不要となった役職員の利用者アカウントは、直ちに取り消す。異動や組合外への出向の場合は、付与されているアクセス権限について時宜を得た変更を行う。

４　利用者アカウント登録にあたっては、該当利用者の情報システム又はサービスへの使用許可を事前に情報システム管理者又はその指名する者から得る。

５　役職員等と利用者アカウントが関連づけられ、役職員等の責任を明確にするために、固有の利用者アカウントを使用する。（特定の情報システムにおいて、別に

規定があるものを除く）

６　アクセス権限の付与時には、役職員等に対し、利用者アカウント、パスワード等の管理方法、情報システムへのアクセス方法、アクセスできる範囲（アクセス権限）と禁止事項等を通知する。

７　アクセス権限の登録・抹消作業においては、不正行為を防止するため、作業担当者は作業結果を情報セキュリティ事務管理者に報告しなければならない。

⑤　情報システムを使用して個人番号関係事務を行う場合、事務取扱担当者及び当該事務で取扱う特定個人情報ファイルの範囲を限定するため、適切なアクセス制御を行う。

⑥　不正アクセス、不正情報取得、情報漏えい等を牽制、防止するために、職員の権限に応じて必要な範囲に限定されたアクセス権限を付与し、アクセス記録の保存、検証を行う。

（情報ネットワークの使用目的、範囲）

第２２条　組合は業務の質、効率の向上及び、報告・連絡の伝達向上を目的として組合内情報ネットワークを運営する。

②　組合内情報ネットワークの適用範囲は、組合内に配置された通信回線、サーバ、情報ネットワーク機器とこれらに接続して使用するパソコン端末機器、周辺装置から構成される情報ネットワークであり、インターネットへ接続するルータまでをいう。

（情報ネットワークのセキュリティ）

第２３条　情報ネットワークのセキュリティ管理はセキュリティ事務管理者を通じて、情報システム管理者があたる。

②　情報システム管理者は、情報ネットワークに接続するパソコン端末機の全てにウイルス対策を設定し、その機能が最新の状態を維持するよう実施する。

③　情報システム管理者は、役職員が送受信する電子メールの送受信記録及び閲覧するインターネットの閲覧を記録し、必要な措置を取ることが出来る。

④　ユーザは、使用する機器の故障や通信回線の異常などを発見した場合、速やかに情報セキュリティ部門管理者を通じて情報システム管理者へ報告する。

⑤　特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を行う。

⑥　外部ネットワークと接続する場合は、次のセキュリティ対策を行う。

１　ファイアウォールの導入

２　アクセス履歴（ログ）の採取・安全な保管

３　ホストセキュリティの強化

４　侵入検知システムの導入

（情報システム管理者権限の管理）

第２４条　情報システム管理者は、情報システムの管理者権限について、次の事項を遵守し、厳重に管理する。

１　オペレーティングシステムやデータベース等のシステムに関連する管理者権限と役職員等の職務は区別する。

２　役職員等に対し、情報システムの管理者権限を割り当てる必要がある場合は、情報セキュリティ統括管理者の事前承認を得る。

３　システムの管理者権限は、職務上必要とされる時に限って、その役割における最小限の要求事項に従って割り当てる。

４　システムの管理者権限の利用許可手続及びオペレーションについては、記録・保存するよう努める。

５　システムの管理者権限は、通常の業務に使用する利用者アカウントとは異なる利用者アカウントに対して、割り当てる。

（アクセス権限の見直し）

第２５条　情報システム管理者は、アクセス権限が適正に維持されていることを確認する。確認の内容は、退職等により取り消されるべき利用者アカウントが残っていないかについての確認とし、年１回確認する。

（情報ネットワークのアクセス制御）

第２６条　情報ネットワークは、情報セキュリティ部門管理者及び情報システム管理者の許可を得た者にのみ、アクセスを可能とする。

②　情報システム管理者又はその指名する者は、情報ネットワーク機器上のフィルタリング機能等を利用し、不適切な情報ネットワークサービスが提供されないよう制御を行うことができる。

③　情報システム管理者又はその指名する者は、サーバ上にある不要な情報ネットワークサービスを停止することができる。

（経路制御（情報ネットワークルーティング制御））

第２７条　情報システム管理者又はその指名する者は、不正アクセスを防止するため、情報ネットワーク機器で必要最低限の経路のみに利用を制限する。

②　インターネットへのアクセスは、アクセス制限サーバで経路を限定することができる。

（利用者による外部からのアクセスへの対策）

第２８条　外部からのアクセスは、原則禁止とする。業務上必要がある場合は、情報セキュリティ部門管理者及び情報システム管理者の許可の下、必要最低限のアクセスを可能とする。

（外部組織等が保有する設備への接続に関する対策）

第２９条　外部組織等が保有する設備への相互接続が業務上必要となる場合は、あらかじめ次のような接続要件を定め、情報システム管理者又はその指名する者の承認を得る。

１　ファイアウォールの設置。

２　情報セキュリティ上の安全を考慮した情報ネットワーク構成。

３　情報セキュリティ上の安全を考慮した管理体制の確立。

４　情報セキュリティ侵害への対応。

５　保守体制の確立。

（ログイン手順）

第３０条　不正なログインを防ぐため、ログインの連続失敗回数を制限するよう努める。一定回数以上の連続したログインの失敗が行われた場合は、該当利用者のアカウントをロックアウトするよう努める。

（パスワードの管理方法）

第３１条　情報システム管理者は、次の事項を考慮し、役職員等のパスワードを厳重に管理する。

１　役職員等には、原則として個別のパスワードを使用させる。

２　パスワードは定期的に更新する。

３　パスワード更新時に、以前に使用していたパスワードを再使用できないようにする。

４　パスワードは、入力時に画面上に表示しないようにする。

②　仮のパスワードを付与する場合は、安全な方法で役職員等に通知する。

③　パスワードが第三者に読まれることのないよう、パスワードファイル等へのアクセス権を必要最小限のものにする。

（接続時間の制限）

第３２条　重要な情報を含む情報システムへの接続については、必要最小限の接続時間に制限するよう努める。

（情報システムの調達、導入における遵守事項）

第３３条　機器及び基本ソフトウェアの導入（変更等を含む）及び撤去に際しては、導入や撤去による既存の情報システムへの影響、障害発生を未然に防ぐため、事前に検証を行い、情報システム管理者又はその指名する者の承認を得た後、導入及び撤去する。

②　機器の廃棄時等、情報漏えい防止のために事前にデータ消去が必要な場合には、データ消去ソフトウェア等でデータを消去し、実施した作業内容を記録する。

③　機器及びソフトウェアを購入等する場合、情報システム管理者又はその指名する者は、当該製品に情報セキュリティ上の問題がないかどうか、次の事項を重点的に確認する。

１　既知の情報セキュリティ上の弱点への対策実施の有無。

２　機器及びソフトウェア供給元の保守・サポート体制。

④　ソフトウェア（独自開発ソフトウェア、及び汎用ソフトウェア）の更新又は修正プログラムの導入に際しては、その更新又は導入による既存の情報システムへの悪影響、障害発生を未然に防ぐため、事前に情報システム管理者又はその指名する者とともに次の事項について確認する。

１　オペレーティングシステム、ミドルウェア等との親和性。

２　バージョン相違等による不整合等。

（情報システムの委託業者の選定、契約及び管理）

第３４条　外部委託する場合は、委託に関する責任を有する部署を明確にし、委託業者の経営の健全性、安定度、営業規模、信用度（実績）、保有資格、要員のモラル、機密保護や内部不正防止への取り組みについて調査し、信頼性を確認した上で複数の業者から比較検討して委託業者を選定する。当該部署は、委託業者に対し、委託する業務の種類や範囲に応じて、必要な情報セキュリティ要件を記載した契約書等による契約を締結しなければならない。

②　外部委託している業務に関しての委託先からの定期的な報告を受け、委託業務の実施内容を確認する。

③　委託業者からの報告に疑義がある場合、及び情報システム管理者が必要と判断した場合は、委託業者に対し作業の進捗やスケジュールの管理状況、品質管理状況等について検査を行う。検査結果及び指摘事項への是正対策の内容によっては、委託先の変更を検討する。

④　委託業者には、委託業務の内容や管理内容を事前の承認を得ずに変更させてはならない。

⑤　インターネット等、外部情報ネットワーク業者の選定においては以下の要件を備えた者とする。

１　不正アクセス防止の対策がなされていること。
２　運用の信頼性、安全性について対策されていること。

⑥　共同開発等における、委託業者との共有可能な情報については情報セキュリティ事務管理者の承認を得て、セキュリティ管理部門がこれを監視する。

（情報システム機器等の管理及び廃棄）

第３５条　情報システム機器、情報ネットワーク機器及び外部記憶媒体等の情報資産は、部門毎に保管場所を指定し、不要になった場合には、内部に保持されている情報が流出しないよう初期化又はデータ消去ソフト等による情報消去を行う。

②　外部記憶媒体は各部門で独自のものを使用しない。

（機器の修理及び廃棄時の遵守事項）

第３６条　外部業者を利用して記憶媒体の含まれる機器を修理及び破棄する場合、その内容を消去した状態で、委託業者に受け渡す。

②　情報を消去した状態で委託業者に引き渡すことが難しい場合は、事前に情報システム管理者の許可を得て、委託業者との秘密保持契約を締結の上で、引き渡す。なお、業務基幹サーバや業務支援サーバ等の重要な機器については、記憶媒体の消磁、破壊等により復元不可能な状態で廃棄するよう指示する。

③　廃棄を外部業者に委託する場合は、委託先が完全に削除又は廃棄したことについて証明書等により確認する。

（マルウェア対策及び技術的な弱点の対策）

第３７条　情報システム管理者又はその指名する者は、適宜、次の信頼できる情報収集先から最新のマルウェアに関する情報及び、その他のセキュリティ情報を入手するよう努める。

１　使用しているセキュリティソフトベンダー。
２　セキュリティ情報を提供する団体等。

②　収集した情報は、情報システム管理者又はその指名する者が取りまとめ、必要に応じて情報セキュリティ部門管理者に電子メール、イントラネットシステム等にて周知するよう努める。その中でも特に重要なものに関しては、電子メールにて全役職員等に周知を行う。

③　情報システム管理者又はその指名する者は、次の情報システムのバージョン情報を管理する。

１　オペレーティングシステムの種類、バージョン、及びパッチのレベル。
２　使用しているアプリケーションの種類、バージョン及びパッチのレベル。

④　情報システム管理者又はその指名する者は、情報セキュリティに重大な影響を及

ぼす弱点に対するパッチ等について、次を遵守し速やかな対応を行う。

１　オペレーティングシステムのパッチは信頼できるところから入手する。

２　パッチ等が既存のアプリケーション等の動作に悪影響を及ぼさないか評価する。

３　可能な限り開発環境にて事前に動作確認を行う。

４　その他のソフトウェアの更新等については、計画的に実施する。

⑤　情報システム管理者又はその指名する者は、サーバ及び端末においてウィルス対策を行う。

１　ワクチンソフトを導入する。

２　ウィルスチェックは自動的に行うように設定する。

３　持込み媒体は使用する前にウィルスチェックを行う。

⑥　情報システム管理者又はその指名する者は、ウィルスチェック用のウィルス定義ファイルを自動更新機能にて常に最新のものに保つ。

⑦　情報システム管理者又はその指名する者は、重要な情報システム設定に係るファイル等については、定期的に、当該ファイルの改ざんの有無を検査する。

（サイバーセキュリティ対策）

第３８条　サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を行う。

②　サイバーセキュリティの脆弱性についての必要な対策、点検、評価を行う。

（個人のプライバシーに係わる情報の閲覧）

第３９条　電子メール等個人の役職員等のプライバシーに係わる情報を閲覧する場合、情報セキュリティ統括管理者又はその指名する者の許可を得なければならない。

②　個人情報の保護に関係する情報の閲覧に関しては、当該法規制等に定められた手続、その他別途定める当該領域の関連規程に従うものとする。

（要領の改廃）

第４０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。