○石川県農業共済組合情報セキュリティポリシー

第１　目的

この情報セキュリティポリシー（以下「ポリシー」という。）は、石川県農業共済組合（以下「組合」という。）が保有する情報資産をあらゆる脅威から保護するための情報セキュリティ対策の包括的な事項を定めることを目的とする。

第２　定義

このポリシーに関する用語の定義は次のとおりである。

（１）　情報セキュリティ

情報資産を外部及び内部からのさまざまな脅威から保護することであり、情報資産の機密性、完全性及び可用性を維持すること。

機密性：	情報にアクセスすることを認可された者だけがアクセスできることを確実にすること。
完全性：	情報及び処理方法の正確さ及び完全、ある状態を安全防護すること。
可用性：	許可された利用者が、必要なときに、情報にアクセスできることを確実にすること。

（２）　情報資産

情報資産とは、情報及び情報システムのことをいい、それぞれ次のように定義する。

ア　情報とは、組合が保有する一切のデータ等をいい、コンピュータシステム及び記憶媒体に保存されているデータ・文書のほか、紙に印字・記入されたもの等を含む。

イ　情報システムとは、情報を扱うハードウェア、ソフトウェア、ネットワーク、記録媒体のみならず、それらを適切に運用・管理するために必要なすべての人やものを含むものとする。

（３）　情報の種類

情報の種類には次のものがある。

ア　組合の運営・業務に関する情報（次に含まれるものを除く。）

イ　個人情報（別に定める「個人情報の保護に関する規則」において規定する個人情報をいう。）

ウ　取引相手先情報

エ　知的財産（著作権や工業所有権（特許権、実用新案権、商標権、意匠権）、その他組合がオリジナルで作成したシステムや手順、ノウハウ）

オ　組合の役職員等の個人情報

（４）　情報システムの種類

情報システムには、次のものがある。

ア　農業共済ネットワーク化情報システム（農業共済事業の事務処理システム）

イ　経理システム

ウ　給与システム

エ　農業共済新聞購読者管理システム

オ　その他業務上のシステム

（５）　情報セキュリティポリシー

情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的に取りまとめたもの。どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための組織体制、運用（外部委託を含む。）情報セキュリティ基本方針（以下「基本方針」という。）及び情報セキュリティ対策基準（以下「対策基準」という。）から構成されるもの。

（６）　コンピュータの不正アクセス

他人の利用者識別コード（以下「ユーザＩＤ」という。）やパスワードを使って、コンピュータに不正にログインする行為、又は、ハードウェアやＯＳ・アプリケーションなどに存在するセキュリティ上の弱点（セキュリティホール）を攻撃する行為。

（７）　リスク分析

保護すべき情報資産を明らかにし、それらの情報について被害が発生した際の被害の大きさ等を踏まえて、分類・評価を行うこと。

第３　情報セキュリティ基本方針

（１）　基本方針

組合が担う農業共済事業が継続的かつ安定的に実施できる環境を確保するとともに、国の農業政策の基盤としてふさわしいセキュリティ水準を達成するため、組合における情報セキュリティ対策の包括的規定として、次の事項を内容とするポリシーを策定する。

ア　組織体制

情報セキュリティを確保していくためには、管理職員が情報セキュリティの重要性を十分理解し率先して推進することが重要である。

また、セキュリティ水準を向上させていくためには、役職員一体として情報セキュリティ対策に取り組んでいくことが重要であることから、組合に設置する「石川県農業共済組合情報化推進委員会（以下「委員会」という。）」に、その責任及び権限を与えるとともに、情報セキュリティに関する権限や責任を有する者を選任し、積極的に推進する。

イ　情報の分類と管理

組合で構築した情報システムで取り扱う情報については、必要に応じて重要度に応じた情報分類を行い、その重要度に応じた情報の管理を行う。

ウ　物理的セキュリティ

情報システムの設置場所について、不正な立入り、損傷及び妨害から情報資産を保護するために、管理区域の設置や施錠の徹底など外部委託先も含めて物理的な対策を講じる。

エ　人的セキュリティ

すべての役職員が情報資産の管理の面で遵守しなければならない事項を定めるとともに、その周知徹底を図るなど、十分な教育及び啓発措置を講じる。

オ　技術的セキュリティ

組合の情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、不正プログラム対策、ネットワーク管理等について対策を講じる。

カ　運用

ポリシーの実効性を確保するとともに、不正アクセス及び不正アクセスによって他の情報システムへの攻撃に悪用されることを防ぐため、ポリシーの遵守状況の確認、ネットワークの監視などの運用面の対策を講じる。また、緊急事態が発生した際の迅速な対応を可能とするため、緊急連絡網等の整備を図る。

キ　法令遵守・違反者への措置等

役職員は、職務の遂行において使用する情報資産について法令を遵守しなければならない。また、ポリシーに違反した職員に対して、その発生した事案の状況等に応じて懲戒処分を含む厳正な処分等を行う。

ク　評価・見直し

ポリシー及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等を踏まえ、必要に応じてセキュリティポリシーの見直しを行う。

ケ　予算措置

組合における情報セキュリティ対策を積極的に推進するため、対策に必要な経費の確保に努める。

（２）　ポリシーの対象範囲

（追録第七号）

ポリシーの対象範囲は、次表に掲げた情報システム等、情報システムに記録される情報及びこれらの情報に接するすべての者とする。

区　分	対　象　範　囲
情報システム等	ハードウェア：（情報機器）　各種サーバ、UPS、ルータ、HUB、TA、モデム、端末、パソコン、記録媒体（MO、FD、CDR、DVD、USBメモリ）等 ソフトウェア：　すべての基本ソフトウェアすべての応用ソフトウェア そ の 他：　ファイア：ウォール、システム設定情報、システム構成図等
情報システムに記録される情報	アクセス記録（ログ）、文書及び図面等の電磁的記録
これらの情報に接するすべての者	役員、職員、嘱託職員、臨時職員、委託先事業者

（３）　実施手順の作成

組合において構築された情報システムについて、それぞれの情報システムの管理・運営の状況を勘案の上、本ポリシーを踏まえて具体的な実施手順を定めることとする。

第４　情報セキュリティ対策基準

（１）　組合における情報セキュリティ対策の組織体制

ア　組織体制

（ア）　情報セキュリティに関する事項の総括及びポリシーに関する重要事項の決定、評価及び見直しは、組合に設置する委員会（委員長：参事、委員長代理：総務部長、委員：参事及び総務部長を除く管理職）において行う。

（イ）　委員会の委員長を最高情報セキュリティ責任者（以下「最高責任者」という。）とする。

（ウ）　委員長代理を情報セキュリティ管理責任者（以下「管理責任者」という。）とし、最高責任者を補佐し、組合内の情報システムの管理とセキュリティ対策を推進する。

（エ）　課、室及び所内（以下「課内」という。）の情報セキュリティ対策を推進するため、委員会の委員を情報セキュリティ管理者（以下「管理者」という。）とする。

（オ）　管理者は、緊急時における連絡体制を強化するため、連絡員を指名する。（(６)のエの緊急時対応計画参照）

（カ）　システム管理者

委員会の下に、組合が管理運営する情報システムのシステム管理者を置く。

イ　任務

（ア）　最高責任者は、組合が所有するすべての情報資産及び組合における情報セキュリティに関する権限と責任を負うとともに、情報セキュリティ対策の総括を行う。

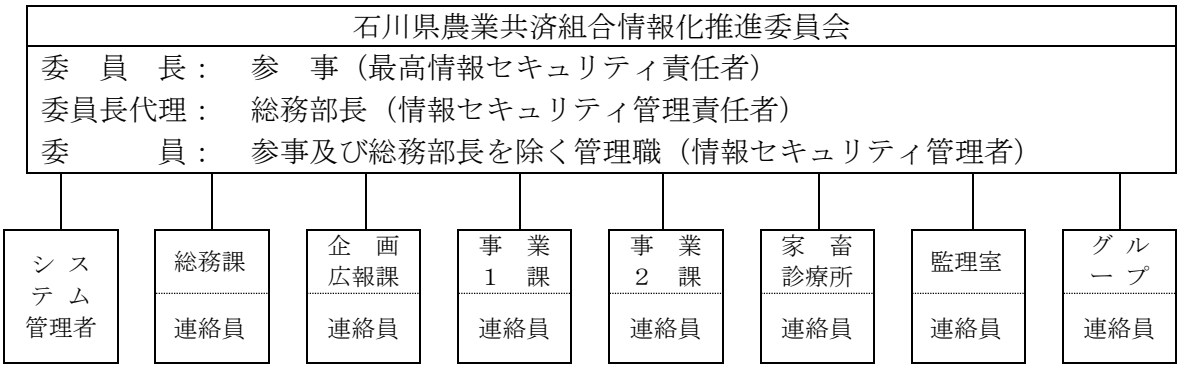
（イ）　管理責任者は、最高責任者の補佐を行うとともに、組合におけるすべての情報資産及び情報セキュリティの管理を行い、必要に応じて管理者及びシステム管理者に指示する。

（ウ）　管理者は当該課内における情報セキュリティに関する権限と責任を有し、当該課内に設置された情報システム等の管理並びに連絡体制の構築、ポリシーの遵守に関する事項及び教育等に関する事項を行う。

（エ）　連絡員は、所属する課内の意見の取りまとめ、管理者からの連絡事項の周知及び緊急時の対応等を行う。

（オ）　システム管理者は、自らが管理運営している情報システムに係る情報セキュリティについての責任及び取り扱う情報資産の管理業務を行う。

本組合における情報セキュリティ対策の組織体制



（２）　情報の分類と管理

ア　情報の管理責任

（ア）　管理責任

情報の管理責任は、当該情報を作成・入手した部署が負う。

（イ）　利用者の責任

情報を利用する者は、情報の分類に従い利用する責任を負う。

（追録第十号）

（ウ）　情報の重要性の効力

複製された情報及び伝送した情報等についても、複製・伝送前の情報の分類に基づき管理する。

イ　情報の分類

本ポリシーの対象となるすべての情報について、各々の情報の機密性、完全性及び可用性を踏まえ、重要度の区分を次のように職員が判断し、管理者が決定する。ただし、個人情報及び取引相手先情報のうち未公開情報は最重要の情報とし、「石川県農業共済組合個人情報の取扱いに関する方針」及び「個人情報の保護に関する規則」において別に定めるものとする。

（ア）「最重要」

情報漏洩等により組合の運営に重大な影響が予想される情報で、情報の利用者を限定し、厳格な取扱いを要するものであり、原則として内部関係者や関係部門以外に開示することを許さないもの。

（イ）「重要」

「最重要」に分類されるもの以外で、原則として組合外に開示することを許されないもの。

（ウ）「一般」

上記「最重要」、「重要」に該当しない情報

ウ　情報の管理

（ア）　情報の管理方法

a　情報の分類の表示

システム管理者は、第三者が重要性の識別を容易に認識できないよう留意しつつ、情報システムで扱う情報については、ファイル名、記録媒体等に情報の分類が分かるように表示をするなどの適切な管理を行う。

b　情報の管理及び取扱い

システム管理者は、情報の重要性分類に従い、利用者の範囲（アクセス権限）を定め管理する。

c　記録媒体の管理

① システム管理者は、取り外しが可能な記録媒体について盗難等を避けるための管理措置を講ずる。

② 特に、重要な情報を記録した記録媒体は施錠可能な場所に保管する。

d　記録媒体の処分

① 情報が記録された記録媒体が不要となった場合は、その内容が絶対に復元できないように消去を行った上で廃棄する。

② 管理責任者は、重要な情報を記録した記録媒体の廃棄を行う場合は、廃棄した日時、担当者及び処理内容を記録しておく。

エ　情報資産の入手

組合外の者が作成した情報資産を入手した者は、イの分類に基づき、当該情報の分

類を定めなければならない。

オ　情報の送信

電子メール等により情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

カ　情報資産の利用

（ア）　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

キ　情報資産の提供・公表

（ア）　情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ）　情報資産を外部に提供する者は、最高責任者に許可を得なければならない。

ク　外部委託先の管理

外部委託を行う場合は、当該委託先との間に情報資産保護について必要な要件を記載した契約書による契約を締結し、委託先に秘密保持義務を課すものとする。

ケ　重要な情報資産の開示に関する特例

「最重要」に区分されている情報資産を組合外に開示する必要が生じた場合は、組合長の許可を得た上で行わなければならない。

また、「重要」に区分されている情報資産を組合外に開示する必要が生じた場合は、最高責任者の許可を得た上で行わなければならない。この組合の情報資産を組合外に開示する場合は、秘密保持契約を締結し、開示先に秘密保持義務を課すものとする。

（３）　物理的セキュリティ

ア　情報システム等の設置

（ア）　管理区域の設置

a　重要なサーバ等を設置する場合は、外部から容易に侵入できないような管理区域（以下「電子計算機室等」という。）に設置する。

b　電子計算機室等からすべての外部に通ずるドアや窓は、制御機能、鍵、警報装置等によって許可されていない者の立入りを防止するなどの措置を講じる。

c　電子計算機室等に設置する情報機器等は、耐震対策を講じた場所に設置するとともに、防火措置等を講じる。

（イ）　電子計算機室等の入退室管理

電子計算機室等の入退室については、許可者に限定するなどの措置を講じる。

（ウ）　情報機器等の搬入

a　電子計算機室等に情報機器等を搬入する場合は、あらかじめ当該情報機器等の既存情報システムに対する安全性を確認してから行う。

b　業者が情報機器等を搬入する場合は、必ず職員が立ち会う等の措置を講じる。

（エ）　情報機器の取付け

a　情報機器の取付けを行う場合は、火災、水、埃、振動等の影響を可能な限り排

除した場所に設置し、必要に応じて容易に取り外せないよう適切な固定等の措置を講じる。

b　システム管理者以外の者が重要なサーバ等を容易に操作できないように、必要に応じてユーザＩＤ、パスワードの設定等の措置を講じる。

c　情報機器の取付けに当たっては、ディスプレイ、配線等から放射される電磁波により重要な情報が破壊されたり、外部に漏えいしたりすることがないよう必要に応じて措置を講じる。

（オ）　電源

a　サーバ等の情報機器の電源については、停電等に備えるため、当該情報機器を適切に停止するまでの間に十分な電力が供給できる容量の予備電源（ＵＰＳ）を備え付ける。

b　落雷等による過電流から、サーバ等の情報機器を保護するための措置を講じる。

（カ）　配線

a　配線は、傍受又は損傷等を受けることがないように、可能な限り必要な措置を講じる。

b　主要な箇所の配線については、安定かつ円滑な運用を図るため、必要に応じて点検を行う。

c　基幹的なネットワーク接続機器は、必要に応じて、配線の変更及び追加等が容易にできないような措置を講じる。

（キ）　外部に設置する装置

外部に装置（委託先事業者の施設に置かれるサーバ等）を設置する場合は、最高責任者の承認を得る。また、定期的に当該装置の情報セキュリティ対策の状況を把握する。

イ　職員に貸与しているパソコン等の管理

事務所等に職員がいない場合は、ドアや窓に施錠をするなど情報機器及び情報の盗難防止等の措置を講じる。

（４）　人的セキュリティ

ア　職員の責務

情報に接するすべての職員は、情報資産の管理の面から、次の事項を遵守する。

a　ポリシー及び実施手順に定められている事項を遵守すること。

b　業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

c　付与されたユーザＩＤ及びパスワードを他の者に知られないよう厳重な管理を行うこと。特に、パスワードについては、次の事項に留意すること。

・パスワードは秘密にし、第三者に漏らさないこと。

・パスワードをメモに記録しないこと。また、机や情報機器等に貼付しないこ

と。

・パスワードの長さは十分な長さ（５桁以上）とし、文字列は他人が予想しにくいものとすること。

・パスワードの内容が漏えいされたと思われる場合は、直ちにパスワードを変更すること。

・パスワードは、定期的に若しくはアクセス回数に基づいて変更し、古いパスワードの再利用は行わないこと。

・パソコン等にパスワードを記憶させないこと。

・システム管理者の許可のない限り、職員間でパスワードを共有しないこと。

d　貸与されているパソコン等が常に良好な状態で稼働できるよう適正に管理するとともに、システム管理者の許可なく情報機器の増設・交換及び搭載されているソフトウェアを改変しないこと。

なお、業務を円滑に遂行するために必要なソフトウェアを新たにパソコン等に組み込む場合は、システム管理者の許可を得ること。

e　貸与されているパソコン等の情報機器及び利用者本人が所有している情報資産がコンピュータウィルスに感染しないよう十分な注意を払い、異常を認めたとき及びコンピュータウィルスの感染が認められたときは、直ちに、（４）のウの(ア)に基づきシステム管理者若しくは連絡員に報告し、指示を受けること。

f　使用しているパソコンや記録媒体等を、第三者に使用されること又は許可なく情報を閲覧されることがないよう適切な管理を行うこと。

g　パソコンや記録媒体等を組合外に持ち出す場合は、事前にシステム管理者の許可を得ることとし、情報の盗難、漏えい等に十分注意を払うこと。

h　情報セキュリティ対策について不明な点等については、速やかに連絡員に相談し、指示等を得ること。

イ　教育・訓練

（ア）　最高責任者は、ポリシーの周知及び情報セキュリティの重要性等について、管理職員を含めすべての職員に対して、説明会や講習会等を実施する。

なお、管理者は、課内の職員が積極的に受講できるよう特段の配慮を行う。

（イ）　新規採用者を対象とするポリシーに関する講習会を実施する。

（ウ）　ポリシーに関する教育・訓練プログラムは、委員会において決定する。

（エ）　システム管理者は、システム管理者向けの講習会を受講する。

（オ）　職員は、定められた説明会や講習会を積極的に受講し、ポリシーを理解し、情報セキュリティ上の問題が生じないよう努める。

ウ　事故・欠陥に対する報告

（ア）　職員は、情報セキュリティに関する事故、欠陥及び誤動作を発見した場合は、直ちに次の者に報告し、指示を受ける。

a　組合で管理運営している情報システムの場合は、システム管理者。

b　a 以外の情報システムの場合は、連絡員。

（イ）　システム管理者及び連絡員は、報告のあった事故等について、管理者に報告するとともに、その重要性に応じこれらの事故等を管理責任者に報告する。

（ウ）　管理責任者は、報告のあったこれらの事故等を（６）のエの(イ)より調査・分析し、（６）のエの(エ)の再発防止措置手順に基づく措置を講ずる。

エ　非常勤及び臨時職員の雇用及び契約

管理者は、非常勤及び臨時職員に対して、雇用契約時に必ずポリシーのうち、非常勤及び臨時職員が守るべき内容を説明し遵守させる。

また、臨時職員にパソコン等による作業を行わせる場合は、職員が責任を持って管理する。

（５）　技術的セキュリティ

システム管理者は、情報システムの管理運用に当たって、次の事項を遵守する。

ア　情報システム機器及びネットワークの管理

（ア）　アクセス記録の取得

ａ　アクセス記録及びセキュリティ関連事案に関する記録を取得し、一定の期間保存するとともに、必要に応じてアクセス記録を分析、監視する。

ｂ　アクセス記録が窃取、改ざん、消去されないように必要な措置を講じる。

（イ）　システム管理記録及び作業の確認

システム変更等の処理を行った場合は、その変更内容を記録するとともに、適切な管理を行う。

（ウ）　障害記録

職員から報告のあった情報、システムの障害に対する処理又は通信システムの問題等については、障害記録として体系的に記録し、常に活用できるよう保存する。

（エ）　情報システム仕様書等の管理

情報システムに係るネットワーク構成図、情報システム仕様書等は、記録媒体、紙媒体に関わらず、閲覧できる者を限定するとともに、厳重に保管する。

（オ）　情報システムの交換

情報システムを交換する場合は、管理責任者の許可を得る。ただし、緊急の場合には事後速やかに報告を行う。

（カ）　バックアップ処理

サーバ等の機器に記録された情報については、その重要度に応じて期間を設定し、定期的にバックアップ処理を行う。

（キ）　メール

メールの中継処理（外部からのメールを当組合のネットワークや情報システム等を経由（踏み台にすること）し、外部へメールを転送するなど）ができないようにするなど、他の情報システムに悪影響を与えないような設定を講じる。

（ク）　外部の者が利用できるシステム

外部の者が利用できるシステムは、強固な情報セキュリティ対策を講じる。

（ケ）　情報システムの入出力データ

a　エラー又は故意に情報が改ざんされることがあるため、必要に応じて改ざんを検出するチェックシステムを導入する。

b　情報システムから出力されるデータが、保存された情報から正しく反映された結果となっているかを必要に応じて確認する。

（コ）　電子署名・暗号化

a　外部に送るデータが完全であることを保証する必要がある場合は、定められた電子署名方法等を使用して送信する。

b　暗号化については、定められた方法以外の方法は利用しない。また、暗号のための鍵の管理方法について、別に定められた方法により管理する。

（サ）　組合外のネットワークへの接続等

モデム等の機器を増設して、他機関のネットワークへの接続、外部からのアクセスを可能とする仕組を構築する場合は、管理責任者の承認を得る。

（シ）　電子取引

電子的な取引を行う場合は、管理者と協議の上、最高責任者及び管理責任者の許可を得る。

イ　アクセス制御

（ア）　利用者登録

利用者の登録、変更、抹消、登録情報の管理、異動や組合外への出向等の職員及び退職者におけるユーザＩＤ及びパスワード等の取扱いについて、定められた方法に従って行う。

（イ）　管理者権限

情報システムの管理者権限は、必要最小限の者に与え、厳重に管理・利用する。

（ウ）　ネットワークのアクセス制御

アクセス可能なネットワーク及びネットワークサービス等を利用する場合は、ネットワークごとにアクセスできる者を定める。

（エ）　適切な経路制御

不正アクセスを防止するため、適切なネットワーク経路制御を講じる。

（オ）　外部からのアクセス

a　外部からのアクセス許可は、利用形態に応じて必要最小限にする。

b　モバイル端末等から組合のシステムにアクセスする場合は、外部アクセスサーバに限定して許可することとし、直接内部のネットワークに接続しない。

c　モバイル端末等からのアクセス方法及び使用方法等は、利用者が本人であることを確実に認証できるものとする。

（カ）　遠隔地にあるシステムへのアクセス

a　遠隔地（地理的に離れた地点）にあるシステムどうしを接続する場合には、安全なアクセスが可能となるよう適切な制御（ネットワーク接続点にアクセス制限、サービスの制限、プロトコルの制限等）を行い、適切に管理を行う。

b　業務上、民間企業等が保有する設備への相互接続が必要な場合は、あらかじめ

各設備への接続要件を定め、管理責任者の承認を得る。

（キ）　外部ネットワークとの接続

外部のネットワークに組合のネットワークを接続して利用する場合は、管理責任者の承認を得ることとし、適切な管理の下で行う。

ただし、ネットワーク化情報システムの転送システム及び組合へのリモートメンテナンスは除く。

（ク）　自動識別

組合内で使用するネットワーク機器については、必要に応じて機器固有情報によって自動的にアクセスチェックができるシステムを導入する。

（ケ）　ログイン手順

情報システムのログイン手順を定め、利用者が適切にログインできるようにする。

（コ）　パスワードの管理方法

ａ　情報システムを利用する職員のパスワードについては、厳重に管理する。

ｂ　パスワードが第三者に解読されないよう、必要に応じて暗号化を行うなどパスワードの取り扱い方法を定める。

（サ）　接続時間の制限

管理者権限による情報システムへの接続は、可能な限り短時間に限定して行う。

ウ　システム開発、導入、保守等

（ア）　情報システムの調達

ａ　応用ソフトウェアの開発、変更及び運用についての手順等を定める。

ｂ　警報機器及び基本ソフトウェアの導入、保守及び撤去についての手順等を定める。

ｃ　情報システムの調達に当たって、調達仕様書に情報セキュリティ確保の規定を必ず盛り込む。

ｄ　情報機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかを確認する。

（イ）　システムの変更管理

重要なシステムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、厳重に管理する。

（ウ）　システムの開発

システム開発及び保守時の事故・不正行為対策のため、次の事項を必ず定める。

ａ　責任者、監督者を定めること。

ｂ　作業者及び作業範囲を明確にすること。

ｃ　システム開発及び保守等の事故・不正行為に係るリスク分析を行うこと。

ｄ　開発・保守するシステムは、可能な限り運用システムと切り離すこと。

ｅ　開発・保守に際しては、可能な限りソースコードの提出を求めること。

ｆ　開発・保守に際しては、セキュリティ上問題となりうるおそれのあるソフトウェアを使用しないこと。

g　開発・保守の際のアクセス制限を明確にすること。

h　機器の搬出入は、システム管理者が立ち会い、その内容を確認すること。

i　開発・保守記録の提出を義務づけること。

j　マニュアル等は、定められた場所に保管すること。

k　開発・保守を行った者のユーザＩＤ、パスワードを当該開発・保守終了後速やかに抹消すること。

（エ）　情報システムの導入

a　情報システムを導入する場合は、原則として既に稼働しているシステムに接続する前に、十分な試験を行う。ただし、導入前に十分な試験を行うことが困難な場合は、リスク分析を行い、その結果を踏まえ対処方針を決定する。

b　試験に使用したデータ及びその結果は厳重に保管する。

（オ）　ソフトウェアの保守及び更新

a　ソフトウェア（独自開発ソフトウェア、汎用ソフトウェア）を更新又は一部修正プログラムを組み込む場合は、不具合、他のシステムとの相性等の確認を行う。

b　情報セキュリティに重大な影響を及ぼす不具合に対処した修正プログラムについては速やかに組み込む。

また、更新することで、従来に増して強固なセキュリティ対策ができる場合は、早期に計画的に導入する。

（カ）　情報システムの開発等に係る委託先事業者への規定

a　新たな情報システムの開発を外部の事業者に委託する場合は、システムの導入前の検査要求事項、守秘義務、資格証明等の規定を調達仕様書等に記載する。

b　情報システムの開発・保守を外部の事業者に委託する場合は、委託先事業者（下請けを行う事業者を含む）に対してポリシーのうち委託先事業者が遵守すべき事項を調達仕様書等に明記するとともに、誓約書等の提出を求めるなどの措置を講じた上で、契約を行う。

c　契約書に、ポリシーの遵守に関する事項を規定する。

（キ）　情報機器の修理及び廃棄等

a　情報が記録された情報機器を外部の事業者に修理させる場合は、前項に準じた調達仕様書を作成し、契約を行う。

b　情報が記録された情報機器を廃棄する場合は、その内容が絶対に復元できないようにする。

ただし、委託先事業者（リース返却先事業者、交換契約による下取り処分先事業者を含む。）に廃棄させる場合は、その内容が絶対に復元できない方法を用いることを調達仕様書等に明記するとともに、その方法等を審査し、契約を行う。

エ　コンピュータウィルス対策

（ア）　管理者は、次の事項を実施する。

a　システム管理者から通知されたウィルス情報について、職員に対して十分な注意喚起を行うこと。

b　システム管理者に対して、重要な情報システムの情報等について、定期的に当該情報に基づく検査を指示すること。

c　サーバ及びパソコン等を定期的にウイルスチェックするよう職員に周知すること。また、ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

（イ）　職員は、次の事項を遵守する。

a　外部からデータ又はソフトウェアを入手した場合は、必ずウイルスチェックを行うこと。データに個人情報が含まれている場合は、対応について管理者に連絡する。

b　差出人が不明、又は不自然に添付されたファイルは開かないこと。

c　システム管理者が提供するウィルス情報を常に確認すること。

d　ウィルス感染のおそれのあるＷＥＢ閲覧は行わない。

オ　セキュリティ情報の収集

（ア）　管理者は、セキュリティに関する情報を次のとおり収集し、必要に応じて職員に通知する。

a　情報収集先（委託先事業者、ＩＲＴサイト、ベンダーのサイト等）を定めること。

b　情報システムのバージョン情報を管理し、得られた情報との確認ができるようにすること。

（イ）　システム管理者は、管理者の行う上記（ア）について支援・協力を行う。

（６）　運用

ア　情報システムの監視

システム管理者は、情報システムが円滑に運用できるよう、次の事項について監視する。

a　情報セキュリティに関する事案を検知するため、システム管理者は、常に情報システムの監視を行うこと。

b　外部と常時接続する情報システムについては、必要に応じて侵入検知装置を設置し監視すること。

c　内部の情報システムについて、必要に応じて侵入検知装置を設置し、監視を行うこと。

d　監視により得られた結果については、厳重に管理すること。また、これらの記録の正確性を確保するため、正確な時刻を設定するなどの措置を講じること。

［情報システムの監視項目例］

・サーバのアクセス記録及びセキュリティ関連イベント
・ネットワーク侵入監視装置
・入退室記録
・配線、中継機器への不正な接続
・ネットワーク負荷
・システムダウン

・プロセス
・ファイルの改ざん
・情報システムへの操作
・ログイン・ログアウトの時刻
・アクセス権限
・インターネット接続記録
・パスワードの変更記録
・コピー履歴
・印刷履歴

イ　ポリシーの遵守状況の確認

（ア）　管理者は、ポリシーが遵守されているかどうか、問題が生じていないかなどについて常に確認を行い、必要に応じて管理責任者に報告する。

（イ）　管理責任者は、報告結果を取りまとめ、必要に応じて委員会に報告する。

（ウ）　委員会は、管理責任者から報告を受けた内容を検討し、職員に周知すべき事項及び改善すべき事項などがあれば、速やかに実施するよう連絡員に指示する。

（エ）　職員は、ポリシーに違反する行為を発見した場合は、（４）のウの(ア)の事故・欠陥に対する報告手順に従い連絡する。

ウ　運用管理における留意点

（ア）　職員は、他の職員のプライバシーに係る情報を、原則として、本人の許可なく閲覧してはならない。ただし、情報セキュリティ対策上問題がある場合は、最高責任者の許可を受けた場合に限り、管理責任者、管理者及びシステム管理者が閲覧できるものとする。また、他の法令等で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令等に定められた手続に従う。

（イ）　管理責任者は、電子掲示板等を活用して、職員が常にポリシー等が閲覧できるようにする。

エ　侵害時の対応

管理責任者は、情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に行うとともに実施し、再発防止の措置を講じるために、緊急時対応計画を次のとおり定める。

（ア）　連絡先

・システム管理者
・情報システムに係る委託先事業者
・課内情報セキュリティ対策連絡体制
・関係機関

（イ）　事案の調査

ａ　（４）のウ若しくは(６)のイの(エ)で情報セキュリティに関する事案を認めた者は、次の項目について報告する。

・事案の内容

・事案が発生した原因として、想定される行為
・確認した被害・影響範囲

b　管理者は、報告のあった事案について事案が発生したシステム管理者等と連携して詳細調査を実施し、必要に応じてその調査結果を最高責任者及び委員会へ報告する。

（ウ）　事案への対処

a　管理責任者は次の事案が発生した場合は、それぞれ定められた連絡先へ連絡する。

・サイバーテロその他重大な被害が生じるおそれがあるとき（警察、農林水産省）
・不正アクセスその他犯罪と思慮されるとき（警察、農林水産省）
・踏み台となって他者に被害を与えるおそれがあるとき（警察、農林水産省）
・情報システムに関する被害（必要と認められる事業者等）
・その他情報資産に係る被害（関係機関等）

b　ネットワークを管理するシステム管理者は、次の事案が発生した場合は情報資産の防護のため、ネットワークを切断する措置を講じる。

・不正アクセスが継続しているとき。
・ＤｏＳ攻撃等の情報システムの運用に著しい支障をきたす攻撃が継続して発生しているとき。
・ウィルス等不正プログラムがネットワーク経由で拡がっているとき。
・その他の情報資産に係る重大な被害が発生したとき。

c　システム管理者は、次の事案が発生した場合は情報資産の防護のため、情報システムを停止する措置を講じる。

・ウィルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき。
・災害等により電源を供給することが危険又は困難なとき。
・その他の情報資産に係る重大な被害が発生したとき。

d　システム管理者は、事案に係る情報システムのアクセス記録及び事案内容並びに経過について整理し、保存しておく。また、事案に係る再発防止の措置を検討し、速やかに対策を講じる。

（エ）　再発防止の措置

a　管理責任者は、事案が発生したシステム管理者と連携して、当該事案に係るリスク分析を実施し、ポリシー、実施手順、各種セキュリティ対策の改善等再発防止計画を策定し、委員会へ報告する。

b　委員会は、再発防止計画が有効であると認められる場合はこれを承認し、管理者が中心になって直ちに取り組む。

オ　委託先事業者への運用委託

システム管理者は、情報システムに係る運用の一部又は全部を外部の事業者に委託する場合は、委託先事業者に対するセキュリティ要件を契約書等に明記する。

（追録第七号）

（７）　法令遵守

職員は、職務の遂行において使用する情報資産について、次の法令を遵守する。

・不正アクセス行為の禁止等に関する法律

・著作権法

・個人情報の保護に関する法律等

（８）　情報セキュリティに関する違反者への措置

最高責任者は、ポリシーに違反した職員に対して、その重大性、発生した事案の状況等に応じて懲戒処分を含む厳正な処分等を行う。なお、処分の決定に際し、自らの責任において発生した情報セキュリティ上の問題について自己申告した場合は、状況等に応じて考慮されるものとする。

（９）　評価及び見直し

ア　監査

ａ　委員会は、必要に応じて組合の中心的なネットワークシステムであるネットワーク化情報システム（以下「組合ＬＡＮシステム」という。）及び各課が管理運営している情報システムの監査を実施する。

ｂ　当該監査を外部の事業者に委託する場合は、組合ＬＡＮシステムにあっては管理責任者が、各課が管理運営している情報システムにあっては、管理者が管理責任者と連携し、監査方針及び監査事項等を作成し、委員会の承認を得て実施する。

イ　点検

管理責任者は、ポリシーに沿った情報セキュリティ対策の実施状況を把握するため、アンケートを含め必要に応じて点検を行う。また、その点検結果を委員会に報告する。

ウ　ポリシーの更新

監査・点検の結果等を踏まえ、新たに講ずべき対策の必要性が生じた場合は、委員会においてポリシーの実効性を評価し、必要に応じてポリシーを改定する。

（10）　予算措置

組合における情報セキュリティ対策を的確かつ着実に推進するため、全体に関わる対策経費については、各課との連携を図りつつ、企画広報課において確保に努めることとし、各課が管理運営している情報システムに関わる対策経費は、当該各課において確保に努める。

第５　附　則

（１）　改正手続

このポリシーの改正は、理事の過半数によって定める。

（２）　実施

このポリシーは、平成27年４月１日から施行する。

（３）　実施

このポリシーは、平成29年11月27日に改正し、平成30年１月１日から施行する。

（４）　実施

このポリシーは、令和３年５月13日に改正し、令和３年７月１日から施行する。

（追録第七号）

（５）　実施

このポリシーは、令和６年５月８日に改正し、令和６年６月１日から施行する。

（追録第十号）