情報セキュリティポリシー

第１章　情報セキュリティ基本方針

（目　　的）

第１条　この情報セキュリティポリシー（以下「ポリシー」という。）は、情報セキュリティ対策の包括的な事項を定め、この組合が保有する情報資産を様々な脅威から守ることを目的とする。

（適用範囲）

第２条　この基本方針は、情報システム、事業システム等、それらに記録される情報及びこれらの情報に接する職員等に適用する。

（定　　義）

第３条　この基本方針で用い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様々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をいう。

①　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。

②　完全性：情報及び処理方法の正確かつ完全である状態を安全防護すること。

③　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（電磁的に記録されたものに限る。）及び情報を管理する仕組み（情報システム及びシステム開発、運用並びに保守のための資料等を含む。）の総称をいう。

(3)　個人情報

「個人情報の保護に関する法律」（以下「法」という。）第２条第１項に規定する個人情報をいう。

(4)　個人データ

法第２条第４項に規定する個人情報データベース等を構成する個人情報であって、本組合の情報システム及び事業システム等で管理される個人情報に関わるデータをいう。

(5)　情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うものをいう。

(6) 事業システム等

ＮＩＣシステムをはじめとする各事業システム、経理処理システム、給与計算システム、新聞購読者管理システム及び職員が作成したＥＵＣシステムをいう。

(7) 不正アクセス

他人の利用者識別コード（ユーザーＩＤ）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またはハードウェアや基本ソフトウェア（ＯＳ）等に存在するセキュリティ上の弱点（セキュリティホール）を攻撃する行為をいう。

(8) 職員等

組合役員及び職員（期間契約職員等を含む。）並びに情報システムを利用するすべての者をいう。

（情報資産への脅威）

第４条　情報資産に対して想定される脅威は、次のとおりである。

(1) 故意または過失による情報資産の持ち出し、盗聴、改ざん、消去、盗難、漏えい及び破損

(2) 地震、落雷、火災等の災害、事故及び故障による事業システム等の停止

（情報セキュリティ対策）

第５条　情報資産を、前項の脅威から保護するため、次の情報セキュリティ対策を講じるものとする。

(1) 物理的情報セキュリティ対策

情報システムの設置場所について、不正な立ち入り、損傷など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物理的な対策を講じる。

(2) 人的情報セキュリティ対策

職員等が情報資産を利用するうえで遵守しなければならない事項を定め、周知徹底を図るとともに、十分な教育及び啓発が行われるよう必要な人的な対策を講じる。

(3) 技術的情報セキュリティ対策

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、ウィルス対策等の技術的な対策を講じる。

(4) 運用による情報セキュリティ対策

情報資産の管理、セキュリティ対策の遵守状況の確認、緊急事態発生時の危機管理対策等の運用面の対策を講じる。

（情報セキュリティ対策基準の策定）

第６条　前項の情報セキュリティ対策を具体的に実施するにあたり遵守すべき事項や判断等の基本的な基準は、「情報セキュリティ対策基準」に定めるものとする。

（情報セキュリティ管理体制）

第７条　情報セキュリティ対策に対する管理体制は次のとおりとする。

(1) 組合長をセキュリティ対策統括管理者（以下「統括管理者」という。）とし、セキュリティ対策に関する業務を統括するものとする。

(2) 参事をセキュリティ対策事務管理者（以下「事務管理者」という。）とし、統括管理者を補佐し、情報セキュリティに関する立案とその実施についての指揮・監督を行うものとする。

(3) 事務管理者は、総務部長を情報セキュリティ部門管理者として、情報セキュリティに関する施策の実施に当たらせる。

(4) 統括管理者は、毎年度１回、ポリシーの遵守状況を監査し、ポリシーの見直しの必要性など情報セキュリティ対策の検証を行うこととする。

(5) 事務管理者は、ポリシーの監査結果等を職員等が閲覧できるようにしなければならない。

（情報の管理）

第８条　情報は次により適切に管理されなければならない。

(1) 情報の管理責任

情報の管理責任は、当該情報を作成・入手した部署の長が負うものとする。

(2) 情報の管理方法

① 個人情報の入手及び利用等にあたっては、「個人情報保護に関する規則」に従った方法で行わなければならない。

② 情報システムにある情報は、原則として外部に開示したり、外部に持ち出してはならない。

③ 業務上やむを得ず情報を外部へ持ち出す場合は、事前に事務管理者の許可を受けなければならない。

④ 業務上知り得た情報を私的な目的のために利用してはならない。

⑤一時的にパソコンに機密情報をコピーして取り扱う場合、取り扱い後不要になった時点で情報（データ）を削除しなければならない。

第２章　情報セキュリティ対策基準

第９条　物理的情報セキュリティ対策

（ネットワーク機器等の設置)

(1) ネットワーク機器等の設置にあたっては、損傷等を防止するための対策を講じなければならない。

① サーバー機など重要なハードウェアの電源については、停電に備えるため、必ず無停電電源装置（ＵＰＳ）を備えつける。

② 地震等災害からネットワーク機器等を保護するため耐震設備を設置する。

③ サーバー機及びパソコンには、別に定めるソフトウェアをインストールしなければならない。また、職員等にパソコンを配置する際には、必要な設定、各種ソフトウェアのセキュリティに関する修正プログラム（以下「セキュリティパッチ」という。）を必要に応じて適用しなければならない。

（ネットワーク機器等の管理)

(2) ネットワーク機器等は、次の事項に従って管理しなければならない。

① ネットワーク機器等の発注並びに保守契約、ソフトウェアのライセンス、インストールメディア等は、一括して管理しなければならない。

② 購入したネットワーク機器等は、管理台帳で管理しなければならない。

③ 購入したソフトウェアのライセンスは、適切に管理し、不正な使用がないようにしなければならない。

④ 組合事務所等に職員等がいない場合は、事務所等に施錠し、情報資産及びネットワーク機器等の盗難防止の措置を講じなければならない。

（サーバー機の設置場所)

(3) サーバー機の設置は、外部から容易に侵入できないように施錠できる場所でなければならない。

（ネットワーク機器等の廃棄)

(4) ネットワーク機器等の廃棄を行う場合は、ハードディスクからデータが取り出せないように対策しなければならない。

第10条　人的情報セキュリティ対策

（パソコンの利用)

(1) 職員等は、パソコンを利用するにあたり、次の事項を遵守しなければならない。

① 職員等は、組合が貸与したパソコンのみを使用するものとし、個人が所有するパソコンを内部ネットワークに接続してはならない。

業務上やむを得ず、個人が所有するパソコンを接続する場合は、事務管理者に申請し、セキュリティ上問題がないか検査を受けなければならない。

② 職員等は、指定された以外のソフトウェアを導入してはならない。

業務上やむを得ず、指定された以外のソフトウェアを導入する場合は、事務管理者へ申請し、許可を得なければならない。

③ 職員等は、離席する場合、パソコンにロックをかけ、第三者が無断でパソコンを利用すること、データを閲覧することがないよう適切に管理しなければならない。

④ 職員等は、許可なくパソコンを移設してはならない。

パソコンの移設が必要な場合には、事務管理者に申請し、許可を得なければならない。

⑤ 職員等は、業務上やむを得ず、パソコンや記録媒体等を外部に持ち出す場合は、事前に事務管理者の許可を受け、パソコンの盗難、データの漏えい等がないよう十分な注意を払わなければならない。

⑥ 職員等は、使用しているパソコン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、事務管理者の許可なくネットワーク機器等の増設・交換及び搭載されているソフトウェアを改変してはならない。

⑦ 外部の者にパソコンによる作業を行わせる場合は、職員等が責任を持って管理しなければならない。

(ユーザーＩＤ及びパスワード等の管理)

(2) 内部ネットワーク環境で使用するユーザーＩＤ及びパスワードを使用するにあたって、次の事項を遵守しなければならない。

① １つのユーザーＩＤを複数人で共有してはならない。

② パスワードは秘密とし、第三者に漏らしてはならない。

③ パスワードはメモに記録してはならない。ただし、係るメモに機密性が保持される場合はこの限りではない。

④ パスワードが漏えいしたと思われる場合、直ちにパスワードを変更しなければならない。

⑤ 新たなユーザーＩＤが必要な場合は、事務管理者に申請しなければならない。

(コンピュータウィルス対策)

(3) 職員等は、コンピュータウィルスから内部ネットワーク環境を保護するために、次の事項を遵守しなければならない。

① 常駐設定されたコンピュータウィルス対策ソフトを許可なく停止してはならな

い。

② 定期的にパソコンのハードディスク内の全ファイルに対してウィルスチェック

を行わなければならない。

③ 電子メールや記録媒体等で外部からデータを取り入れる場合、ウィルスチェックを行わなければならない。

④ 外部ネットワークに接続したパソコンを内部ネットワーク環境に接続する場合は、接続前にハードディスク内の全ファイルに対してウィルスチェックを行わなければならない。

(インターネットの利用)

(4) 職員等は、インターネットを利用するにあたり、不正アクセスやコンピュータウィルスの感染を防止するために次の事項を遵守しなければならない。

① 公序良俗に反するようなサイトを閲覧してはならない。

② 法律に抵触するようなサイトを閲覧してはならない。

③ 出所が不明なファイルや内容に確証が持てないデータをダウンロードまたは実行してはならない。

ただし、業務上必要とされるデータをダウンロードした場合は、必ずウィルスチェックを行わなければならない。

(電子メールの利用)

(5) 職員等は、電子メールを利用するにあたり、次の事項を遵守しなければならない。

① 差出人が不明なメールや不自然なファイルが添付されたメールを受信した場合、これを開いてはならない。

② ファイルを添付したメールを送受信する場合は、ウィルスチェックを行わなければならない。

(データのバックアップ処理)

(6) 事業システム等を運用する職員は、不測の事態に備えて、定期的にバックアップ処理を実施し、使用する記録媒体は所定の場所に保管しなければならない。

(報　　告)

(7) 職員等は、次の事項を認めたときは、直ちに事務管理者に報告し、指示を受けなければならない。

① パソコンに異常を認めたとき

② コンピュータウィルスに感染したと思われるとき

③ 対策基準に違反する行為を発見したとき

第11条　技術的情報セキュリティ対策

（情報システムの管理）

(1) 情報システムを管理するにあたっては、次の技術的措置を講じなければならない。

① 事務管理者は、職員等がやむを得ない理由により個人が所有するパソコンを接続させる場合は、申請に基づき、セキュリティ上問題がないか検査しなければならない。

② 事務管理者は、緊急を要する場合など、必要に応じて職員等のネットワーク接続を制限することができる。

なお、コンピュータウィルス感染などの緊急時においては、事務管理者は職員等に対して指示を与える前にネットワーク接続を制限することができる。

③ 情報システムに係るネットワーク構成図並びに情報システム仕様書等は、常に最新の状態にし、電磁的記録媒体、紙媒体に関わらず、閲覧できる者を限定するとともに、厳重に保管しなければならない。

④ 情報資産は定期的にバックアップ処理を実施しなければならない。

⑤ サーバー機の管理者権限を有するユーザーＩＤのパスワードには、推測困難なものを設定しなければならない。

（アクセス制御）

(2) 情報システムには、適切なアクセス制御を設定し、許可された者のみがアクセスできるようにしなければならない。

① 管理者権限は必要最小限の者に与え、パスワード等については厳重に管理し、利用しなければならない。

② 情報資産に対しては、重要性に合わせて厳密なアクセス権を設定しなければならない。

③ 職員等がパソコンの設定を安易に変更できないように、職員等には管理者権限を与えてはならない。

④ 外部システムとの接続は、業務上必要がある場合のみ認めるものとする。

⑤ 外部システムからアクセスできる情報資産は必要最小限なものにしなければならない。

⑥ 外部システムから不正にアクセスが行われていることが認められた場合、直ちに外部システムとの接続を遮断し、原因等を調査しなければならない。

（システム開発、導入及び保守）

(3) システム開発、導入を行う場合は、現在稼働しているシステムに影響が及ばないよう措置を講じなければならない。また、業務を外部に委託する場合、個人データの安全管理が図られるよう、適切な監督を行わなければならない。

① 導入前の既存システムとの分離

新しいシステムを開発、導入する際には、稼働しているシステムと分離した上で開発、導入準備を行わなければならない。

② 導入前の十分な検証

新しいシステムを稼働しているシステムと接続する前には十分な検証を行い、稼働しているシステムに影響を与えることなく導入しなければならない。

③ 修正プログラムの適期な対応

情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、速やかに対応を行い、その他の更新等については、計画的に実施しなければならない。

④ 委託先事業者と誓約書等の締結

システムの開発、導入及び保守業務を外部に委託する場合、個人情報の取り扱いに関して、個人データの安全管理が図られるよう、委託先事業者に対する必要かつ適切な監督を行わなければならない。

（コンピュータウィルス対策）

(4) 情報システムからコンピュータウィルスの感染を防止するために、次の対策を講じなければならない。

① サーバー機への対策

ア サーバー機で使用する基本ソフトウェアには、最新のセキュリティパッチを適用し、不要なサービスは削除しておかなければならない。

イ 常に最新のコンピュータウィルス定義ファイルを適用し、定期的にウィルスチェックを行わなければならない。

ウ コンピュータウィルス対策ソフトのサポートが終了した場合、最新のソフトに変更し、継続的にコンピュータウィルス定義ファイルが適用できるようにしなければならない。

② パソコンへの対策

ア コンピュータウィルス定義ファイルの適用状況を定期的に確認しなければならない。

イ パソコンで使用する基本ソフトウェアには、必要に応じて最新のセキュリティパッチを適用しなければならない。

ウ コンピュータウィルス定義ファイル、セキュリティパッチについては、自動的に適用できるようにシステム化するものとする。

（不正アクセス対策）

(5) 情報システムに外部から不正なアクセスがされないよう物理的及び技術的な措置を講じるとともに、定期的にアクセス履歴を確認しなければならない。

（セキュリティ情報の収集）

(6) 情報セキュリティに関する技術的情報を収集し、必要な措置を講じなければならない。

また、必要に応じて、職員等に情報提供を行い、情報セキュリティの確保につとめなければならない。

第12条　運用による情報セキュリティ対策

（情報システムの監視）

(1) 事務管理者は、重要な情報資産を扱う情報システムについては、必要に応じ、アクセス記録等、情報セキュリティの確保に必要な記録を取得し、一定期間保存したうえで、当該記録を定期的に分析しなければならない。

（ポリシーの遵守状況の確認）

(2) 事務管理者は、ポリシーが遵守されているか常に確認を行うとともに、職員に対して指導しなければならない。

（侵害時の対応）

(3) 事務管理者は、情報資産への侵害が発生した場合、証拠保全、被害拡大の防止、復旧等に必要な措置と再発防止の措置を講じなければならない。

① 侵害時の報告及び調査

情報セキュリティに対する侵害の発生を認めた職員は、次の項目について速やかに事務管理者に報告し、事務管理者は詳細な調査を行わなければならない。

ア 侵害の内容

イ 侵害の発生原因

ウ 確認した被害及び影響範囲

エ 予測される被害及び影響範囲

② 侵害への対処

事務管理者は、情報システムに対する侵害に対処するため、次の項目のうち、必要となる事項を実施しなければならない。

ア 定められた連絡先への連絡

イ 情報システムの停止

ウ ネットワーク機器等の情報システムからの切断

エ 情報システムのアクセス記録及び現状の保存

オ 対処の経過の保存

カ　証拠保全及び再発防止の暫定措置の検討

キ　再発防止の暫定措置を講じた後の復旧措置

ク　その他状況に応じて必要と思われる事項

（情報セキュリティ実施手順の策定）

(4) 情報セキュリティ対策基準を運用するにあたり、必要に応じて、より詳細な手順等を定めた「情報セキュリティ実施手順」を策定するものとする。

情報セキュリティ実施手順は、情報システムの環境変化、情報処理技術の進展等に伴って、事務管理者が定めるものとする。

（職員への開示）

(5) 事務管理者は、電子掲示板等を活用し、職員等が常にポリシーを閲覧できるようにしなければならない。

第３章　法令の遵守

（法令遵守）

第13条　職員等は、職務の遂行において使用する情報資産について、次の関係法令を遵守しなければならない。

(1) 不正アクセス行為の禁止等に関する法律

(2) 著作権法

(3) 個人情報の保護に関する法律

第４章　罰　　則

（罰　　則）

第14条　このポリシーに違反した職員、あるいは違反者を看過した職員に対して、その重大性及び発生した事案の状況等に応じて職員就業規則第65条及び第66条の規定に基づき懲戒処分を含む厳正な処分等を行う。

（改正手続）

第15条　このポリシーの改正は、理事の過半数によって定める。