情報セキュリティ基本規程

（目的）

第１条　本規程は、当組合の「情報セキュリティ基本方針」に基づき、当組合における情報セキュリティ維持および推進を行うために必要な基本的事項を定めたものであり、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（組織的に情報セキュリティの維持および向上のための施策を立案、運用、見直しおよび改善すること）を確立することを目的とする。

（定義）

第２条　本規程における用語の定義は、次の各号に定めるとおりとする。

(1) 「情報」とは、有形、無形を問わず、当組合が保有する一切の情報（当組合固有の情報の他、契約その他の正当な手段に基づき入手した、組合員および利用者その他の第三者から取得した情報を含む。）をいう。

(2) 「情報資産」とは、有形、無形を問わず、情報を含む媒体と伝達手段をいう。全ての紙面、記憶媒体、情報システム等と、口頭や電気通信等で伝達される情報を含む。

(3) 「情報システム」とは、情報を取扱う機器装置等のハードウェア、ソフトウェア、プログラム、伝送経路等および、これらにより構成される電子システムおよびその収納施設等をいい、情報に関連する一切の資産および処理方法を含む。

(4) 「リスク」とは、想定される脅威（情報資産に対して損害を与える要因をいう。以下同じ。）が、情報資産に対して損害を与える可能性をいう。

(5) 「リスク評価」とは、情報資産について、脅威に対する脆弱性を分析し、かつリスクが顕在化した場合の事業に対する影響度を評価することをいう。

(6) 「情報セキュリティ」とは、情報資産に対し、①機密性（正当に許可した者だけが当該情報資産にアクセスできること）、②完全性（正確および完全であるよう、情報資産を不正な改ざんおよび破壊から保護すること）および③可用性（正当にアクセスを許可された者が、使用許諾の範囲内で、必要なときに円滑に当該情報資産にアクセスできること）を確保し維持することをいう。

(7)「サイバーセキュリティ事案」とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS 攻撃等の、サイバーセキュリティが脅かされる事案をいう。

(8) 「対象情報」とは、リスク評価の結果、情報セキュリティの確保および維持が必要と判断した情報をいう。

(9) 「対象情報システム」とは、リスク評価の結果、情報セキュリティの確保および維持が必要と判断した情報システムをいう。

(10) 「対象情報資産」とは、対象情報および対象情報システムの総称をいう。

(11)「不測事態」とは、情報セキュリティの確保および維持に重大な影響を与える災害、障害、セキュリティ侵害等の事態をいう。
(12)「役職員等」とは、当組合の役職員ならびにこれに準ずる者（嘱託、臨時職員、パートタイマー、アルバイト等、および当組合との間に委任契約又は雇用契約が成立した者）をいう。
(13)「部室」とは、部室およびこれに準じる組織をいう。

（適用範囲）
第３条　本規程は、役職員等に適用する。

（情報セキュリティ管理体制）
第４条　当組合は、情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にする。
２．経営管理委員会又は理事会は、システムリスクの重要性を十分に認識した上で、システムを統括管理する役員を定める。なお、当該役員はシステムに関する十分な知識・経験を有し業務を適切に遂行できる者であることが望ましい。
３.「情報セキュリティ委員会」は、情報セキュリティ統括管理者、情報セキュリティ事務管理者、情報システム管理者、情報セキュリティ部門管理者により構成されるものとする。
４．情報セキュリティ委員会は、当組合における情報セキュリティ維持および向上に必要な基準、規程類を制定し、これらの周知徹底、運用および見直し、改善を図るとともに、施策等の審議、評価、見直し、および改善を行う。
５．情報セキュリティ委員会は、情報セキュリティに関する不測事態が生じた場合の連絡体制を整備、運営および見直し、改善を行う。
６.「情報セキュリティ統括管理者」とは、理事会の決議に基づき役員の中から選任された者であって、当組合における情報セキュリティに係る業務について情報セキュリティ実施手順書に記載した統括的責任と権限を有するものとする。
７．情報セキュリティ統括管理者は、情報セキュリティ委員会の委員長を務めるものとする。
８.「情報セキュリティ事務管理者」は、当組合の情報セキュリティを主管する部門の長であって、情報セキュリティ委員会および本規程に従い、当組合における情報セキュリティに係る業務を実施する情報セキュリティ実施手順書に記載した責任と権限を有するものとする。
９.「情報システム管理者」は、当組合の情報システムを主管する部門の長であって、情報セキュリティ事務管理者を補佐し、当組合の情報システムのセキュリティに係る業務について情報セキュリティ実施手順書に記載した責任と権限を有するものとする。
10.「情報セキュリティ部門管理者」は、部室の長であって、情報セキュリティ事務管

理者の指示に従い、当該部室における情報セキュリティに係る業務について一義的な情報セキュリティ実施手順書に記載した責任と権限を有する者をいう。
11.「情報セキュリティ担当者」は、情報セキュリティ部門管理者の管理責任において、選任された１名又は複数名の者であって、当該部室における「情報セキュリティ部門管理者」より指示された業務を行うものとする。
12. 情報セキュリティ部門管理者は、情報セキュリティ担当者を選任後、速やかにその役職、氏名等を情報セキュリティ事務管理者に届け出るものとし、情報セキュリティ担当者を変更する場合も同様とする。

（教育）
第５条　情報セキュリティ統括管理者は、人事部長その他の関係部門長と協議のうえ、役職員等に対し、情報セキュリティ意識の向上を図り、情報セキュリティ管理体制、規程類および関係法令等を理解させるために必要な研修実施計画を策定する。
２．情報セキュリティ事務管理者および情報セキュリティ部門管理者は、前項に基づき研修等を実施する。
３．研修等に関する事項は「個人情報保護・情報セキュリティ研修内規」に定める。

（システムリスク管理態勢）
第６条　システムリスクについて代表理事をはじめ､役職員がその重要性を十分認識し、定期的なレビューを行う。
２.経営管理委員会会長又は代表理事は､システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）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。
３．経営管理委員会又は理事会は、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ことを十分踏まえ、リスク管理態勢を整備し、適宜見直しを行う。
４．情報セキュリティ部門管理者は、自部室が保有する対象情報資産について情報資産台帳の作成により把握し、定期的にリスク評価を実施しなければならない。
５．情報セキュリティ事務管理者は、法務、その他の関係部門長と協議のうえ、部室がリスク評価を実施するために必要な事項等を定めた基準を作成し、情報セキュリティ委員会の審議に付す。
６．情報セキュリティ事務管理者は、情報セキュリティ委員会の審議の結果に従い、前項の基準を制定し、この周知徹底、運用および見直し、改善を図る。
７．情報セキュリティ部門管理者は、前項に基づき制定された基準に従い、自部室においてリスク評価の周知徹底、実施、運用を行い、自部室の役職員等への指示を行う。

８．情報セキュリティ監査部門は、リスクが多様化していることを踏まえ、定期的に又は適時にリスクの認識・評価を行う。
９．情報システム管理者は、洗い出したリスクに対し、十分な対応策を講じ、情報セキュリティ委員会に付議する。

（対象情報資産に関する情報セキュリティ）
第７条　役職員等は、自己が扱う対象情報資産を適切に管理しなければならない。
２．役職員等は、対象情報資産の管理にあたり、「個人情報保護規程」その他の情報セキュリティに関連する規程類を遵守しなければならない。
３．情報セキュリティ事務管理者は、関係部室長と協議のうえ、役職員等が対象情報資産を適切に管理するために必要な事項等を定めた基準および規程等を制定し、周知徹底、運用を行い、定期的または、システム基盤等の変更の都度、見直し、改善を図る。
４.情報セキュリティ部門管理者は、前項に基づき制定された基準および規程類に従い、自部室の役職員等が、自部室の対象情報資産を適切に管理するよう、周知徹底、運用を行い、自部室の役職員等への指示を行う。
５．役職員等は、対象情報資産の使用および管理に際し、情報セキュリティに関連する規程、要領等を遵守しなければならない。

（対象情報システムに関する情報セキュリティ）
第８条　情報システム管理者は、当組合の保有する対象情報システムについて、その設計、開発から導入、運用、保守を通じ、対象情報システムの重要度や特性に適合した情報セキュリティの確保、維持のための施策（コンピュータウィルスからの保護、記録情報のバックアップ、情報システムの運用の記録、ネットワークの管理、情報システムの付属媒体の管理、電子メールのセキュリティ、アクセス制御、不正アクセス対策を含むが、これらに限らない。）を講じるものとする。
２．情報システム管理者は、対象情報システム、ネットワーク等のサイバーセキュリティに対し、サイバー攻撃の施策（ファイヤウォールの設置、抗ウィルスソフトの導入、脆弱性診断、これらに限らない。）を講じるものとする。
３．情報システム管理者は、システム、データ、ネットワーク管理上のセキュリティに関して統括を行う。
４．情報システム管理者は、コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を行う。
５．情報システム管理者は、関係部室長と協議のうえ、対象情報システムを適切に管理するために必要な事項等を定めた基準および規程類を作成し、情報セキュリティ委員会で制定したうえで、この周知徹底、運用を行い、定期的またはシステム基盤等の変更の都度、見直し、改善を図る。
６.情報セキュリティ部門管理者は、前項に基づき制定された基準および規程類に従い、

自部室の対象情報システムを適切に管理するために、周知徹底、運用を行い、自部室の役職員等への指示を行う。
７．役職員等は、対象情報システムの利用および管理に際し、情報セキュリティに関連する規程、要領等を遵守しなければならない。
８．当組合は、インターネット取引をする場合の利用者に対して、留意事項を説明するための適切な措置を講じるものとする。

（人的セキュリティ）
第９条　情報システム管理者は、関係部室長と協議のうえ、役職員等の情報セキュリティ管理体制における役割および責任を記載した職務規程等を作成し、理事会において制定する。
２．役職員等の採用を行う責任者は、その採用のときに、情報セキュリティの確保、維持に関する必要な事項を定めた誓約書等を当該役職員等から取得するものとする。
３．派遣社員の受入責任者は、受け入れのときに、情報セキュリティの確保、維持に関する必要な事項を定めた誓約書等を当該派遣社員から取得するものとする。
４．情報セキュリティ事務管理者は、関係部室長と協議のうえ、役職員等および派遣社員の受入に関する規程類において、前２項に定める誓約書等の取得のために必要な事項等を確保するとともに、これにかかる周知徹底、運用および見直し、改善を図る。

（取引先等に関する情報セキュリティ）
第１０条　情報セキュリティ部門管理者は、対象情報資産を取引先等の第三者に開示する場合、対象情報資産を第三者に預ける場合、その他第三者が対象情報資産を知り得る場合は、当該第三者との間で情報セキュリティの確保、維持のために必要な契約を締結する等の適切な措置を講じなければならない。
２．情報セキュリティ部門管理者は、前項の場合、当該第三者による当該対象情報資産の適切な情報セキュリティの確保、維持のために必要な監督に努めるものとする。
３．情報セキュリティ事務管理者は、関係室部長と協議のうえ、取引先等の第三者との契約に関する基準および規程類において、第１項に定める適切な措置を講じるために必要な事項等を確保するとともに、これにかかる周知徹底、運用および見直し、改善を図る。

（保管環境に関する情報セキュリティ）
第１１条　情報セキュリティ事務管理者は、対象情報資産を保管する建物、区画、書棚等について、当該対象情報資産につき不当なアクセス、紛失、盗難等を防止するため、管理区域の入退出管理その他の適切な措置を講じるものとする。
２．情報セキュリティ事務管理者は、関係部室長と協議のうえ、前項に基づき基準および規程類を定め、これにかかる周知徹底、運用および見直し、改善を図る。

（不測事態対応計画）
第１２条　情報セキュリティ事務管理者は、不測事態が生じた場合においても、事業活動に支障を来さない、又は支障を最小限化するための計画（以下「不測事態対応計画」という。）を立案、策定、周知および見直し・改善を行うものとする。
２．情報セキュリティ事務管理者は、不測事態対応計画の実効性について定期的に見直し、必要に応じ改善を図るものとする。
３．情報セキュリティ事務管理者は、関係部門長と協議のうえ、不測事態対応計画の策定等を行うために必要な事項等を定めた組織基準を制定し、情報セキュリティ委員会に付議、この周知徹底、運用および見直し、改善を図る。
４．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。

（不測事態の報告等）
第１３条　役職員等は、不測事態の発生又は発生の兆候を知った場合、直ちにこれを所属する情報セキュリティ部門管理者に報告するものとする。
２．情報セキュリティ部門管理者は、前項の報告を受けた場合、速やかに不測事態対応計画を実行するとともに、当該不測事態の原因究明を行う。また、不測事態の発生等につき、情報セキュリティ事務管理者に報告し、情報セキュリティ事務管理者は直ちにこれを情報セキュリティ統括管理者に報告するものとする。
３．情報セキュリティ事務管理者は、情報セキュリティ統括管理者の指示に基づき、関係部室長と協議のうえ、当該不測事態の対応を行い、事態の収束を図るものとする。
４．情報セキュリティ事務管理者は、不測事態の再発防止の観点から、不測事態への対応結果につき、必要に応じ情報セキュリティ委員会に報告する。

（自主点検）
第１４条　情報セキュリティ部門管理者は、検査実施指示担当部署長の指示に基づき、自部室における情報セキュリティの確保、維持について定期的に自主点検し、改善を図らなければならない。
２．情報セキュリティ部門管理者は、前項の自主点検の結果を速やかに情報セキュリティ事務管理者および検査実施指示担当部署長に報告する。
３.情報セキュリティ事務管理者は､前項により提出を受けた自主点検の結果を評価し、その結果に応じ、改善を図るために必要な指導を部門管理者に対して行うものとする。
４．情報セキュリティ事務管理者は、検査実施指示担当部署長その他の関係部門長と協議のうえ、部門管理者が第１項の自主点検を実施するために必要な事項等を定めた基準

を制定し、この周知徹底、運用および見直し、改善を図る。

（監査）
第１５条　監査室長は、本規程ならびに本規程に基づき情報セキュリティ事務管理者が制定する基準および規程類の遵守状況を監査し、その結果を組合長に報告する。
２．監査室長は、前項の監査の結果を情報セキュリティ部門管理者に通知し、必要に応じて改善を図るための助言・提案を行うものとする。

（規程等の遵守）
第１６条　役職員等は、情報セキュリティの重要性を認識のうえ、本規程および本規程に基づき制定される基準および規程類、関係法令その他の規範および第三者との契約に定められた事項を遵守しなければならない。

（違反時の措置）
第１７条　本規程および本規程に基づき情報セキュリティ委員会等が制定する基準および規程類に違反した場合、就業規則等に基づき懲戒処分その他の処分に付することがある。

（規程等の見直し・改善）
第１８条　情報セキュリティ事務管理者は、本規程および本規程に基づき制定された基準の実効性を確保するために、第１３条に基づき報告を受けた不測事態の発生原因等を考慮のうえ、定期的にこれらを見直し、必要に応じ改善を図るものとする。
２．情報セキュリティ事務管理者は、情報セキュリティ部門管理者に対し、前項の見直し・改善が確実に行われるように指導する。
３．当組合以外における不正、不祥事件も参考に、情報セキュリティ管理態勢のＰＤＣＡサイクルによる継続的な改善を図る。
（附　則）
1.この規程は、平成 18 年 10 月 31 日から施行する。
2.この規程は、平成 27 年 11 月 27 日から施行する。

以　　上