情報安全管理基本規程

（目　的）

第１条　この規程は、当組合の「情報安全管理基本方針」に基づき、当組合における情報の安全管理体制の確立及び維持並びに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及び向上のための施策を立案、運用、見直し及び改善すること。）を確立することを目的とする。

２　この規程及びこれに附属する基準等に定めのない事項については、組合の諸規程に定めるほか、これらの定めに基づいて締結された第三者との契約、コンピューター犯罪に関する法律、不正アクセス行為の禁止等に関する法律、高度情報通信ネットワーク社会形成基本法（IT 基本法）、その他の情報セキュリティに関係する諸法令の定めるところによる。

（定　義）

第２条　この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ほか、契約その他の正当な手段に基づき入手した、組合員及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、当組合が業務に用いるすべての情報、及び口頭・記憶・書面・電磁的方法等有形無形又は形態の別を問わずこれら情報を記録した媒体、並びに情報システムをいう。

(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・伝達経路等、及びこれらにより構成される電子システム並びにその収納装置等をいい、情報に関連する一切の資

産及び処理方法を含む。

(4)「リスク」とは、想定される脅威（情報資産の価値を失わせる要因をいう。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、あらかじめ情報資産にとっての脅威を想定した上で、その脅威に対する情報資産の脆弱性を分析し、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、必要な時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)「対象情報」とは、リスク評価の結果、当組合が情報セキュリティの確保及び維持が必要と判断した情報をいう。

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

(9)「対象情報資産」とは、リスク評価の結果、当組合が情報セキュリティの確保及び維持が必要と判断した情報資産をいう。

(10)「不測事態」とは、情報セキュリティの確保及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。

(11)「役職員等」とは、組合の役職員並びにこれに準じる者（雇員、パートタイマー、派遣職員等、組合との間に委託契約又は雇用契約が成立した者）をいう。

(12)「部門」とは、部、課、工場及びこれに準じる機構をいう。

(適用範囲)

第３条　この規程は、役職員等に適用する。

（情報セキュリティ管理体制）

第４条　当組合における情報セキュリティ維持及び向上に必要な実施基準等を設定し、これらの周知徹底、運用及び見直し若しくは改善を図るとともに、これらに係る施策等の審議、評価、見直し若しくは改善を行うため、「情報セキュリティ委員会」を設置する。

２　情報セキュリティ委員会は、常勤理事及び部門長によって構成し、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及び情報セキュリティ部門管理者を置く。

３　情報セキュリティ委員会は、情報セキュリティに関して不測事態が生じた場合の連絡体制を整備・運営するとともに、必要に応じ見直し若しくは改善を行う。

４　「情報セキュリティ統括管理者」には常勤理事が就任し、当組合における情報セキュリティに係る業務全般について、統括的責任と権限を有するものとする。

５　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。

６　「情報セキュリティ事務管理者」には参事が就任し、情報セキュリティ委員会の決定及びこの規程の定めるところに従い、組合における情報セキュリティに係る業務を実施する責任と権限を有するものとする。

７　「情報システム管理者」には参事補が就任して、情報セキュリティ事務管理者を補佐し、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責任と権限を有するものとする。

8　「情報セキュリティ部門管理者」には各部門長が就任し、情報セキュリティ事務管理者の指示に従い、部門内の情報セキュリティに係る業務について、一義的な責任と権限を有するものとする。

9　情報セキュリティ部門管理者は、部門内において１名ないし複数名の職員を「情報セキュリティ担当者」として選任し、必要に応じ前項に定める役割を代行させるものとする。

10　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　情報セキュリティ部門管理者は、統括管理者の指示に基づき、役職員等に対して情報セキュリティ管理体制、この規程を始めとする関係諸規定、並びに関係法令等を理解させるために必要な教育を実施する。

（リスク評価）

第６条　情報セキュリティ委員会は、各部門がリスク評価を行うために必要な事項等を定めた基準を設定する。

2　情報セキュリティ部門管理者は、前項で設定された基準に従い、部門内で保有する情報資産について定期的にリスク評価を実施し、常にそれらの内容及び管理状況を把握しなければならない。

3　情報セキュリティ部門管理者は、リスク評価の過程と結果を踏まえ、職員等の意識と習熟度の向上を図る。

（対象情報に関する情報セキュリティ）

第７条　情報セキュリティ委員会は、役職員等が対象情報を適切に管理するために必要な事項等を定めた方針又は基準等を設定する。

２　情報セキュリティ部門管理者は、前項の方針又は基準に従って、それぞれの部門の役職員等に必要な指示を行い、部門内の対象情報を適切に管理するよう努めなければならない。

３　役職員等は、対象情報の使用及び管理に際し、第１項に定める方針又は基準等のほか、情報セキュリティに関連する諸規定を遵守しなければならない。

（対象システムに関する情報セキュリティ）

第８条　情報セキュリティ委員会は、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を確保、維持するために必要な施策等（コンピューター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、アクセス制御を含むが、これらに限らない。）を定めた基準及び手続等を設定する。

２　情報セキュリティ部門管理者は、前項の基準及び手続等に従い、それぞれの部門の役職員等に必要な指示を行い、部門内の対象情報システムを適切に管理するよう努めなければならない。

３　役職員等は、対象情報システムの利用及び管理に際し、第１項に定める基準及び手続等のほか、情報セキュリティに関連する諸規定を遵守しなければならない。

（人に関する情報セキュリティ）

第９条　役職員等の情報セキュリティ管理体制における役割及び責任については、別途定める。

２　職員等の採用及び受け入れに当たって徴収する、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については、別途定める。

(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、又はその第三者が業務上対象情報資産の内容を知り得る立場にあると認められる場合には、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、適切な措置を講じなければならない。

2　情報セキュリティ委員会は、取引先等の第三者との契約に関して第 1 項に定める適切な措置を盛り込んだ基準等を設定する。

3　情報セキュリティ部門管理者は、前項の基準等に基づき、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、必要な監督業務を行わなければならない。

（保管環境に関する情報セキュリティ）

第 11 条　情報セキュリティ委員会は、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、適切な措置を盛り込んだ基準等を設定する。

2　情報セキュリティ事務管理者は、前項の基準に基づき、適切な情報資産の管理を行うものとする。

（不測事態対応計画）

第 12 条　情報セキュリティ委員会は、不測事態が生じた場合においても、事業活動に支障を来たさないか、又は支障を最小限に止めるための計画（以下「不測事態対応計画」という。）を立案、策定するために必要な事項等を定めた組合内基準を設定するとともに、この基準に沿って具体的な不測事態対応計画を策定する。

2　情報セキュリティ部門管理者は、部門内の対象情報資産について不測事態が生じた場合又はその

兆候を知った場合、前項に基づき直ち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。

3　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を定期的に評価し、必要に応じ見直し若しくは改善を図る。

（不測事態の報告等）

第 13 条　役職員等は、不測の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、前条第 2 項に基づき速やかに不測事態対応計画を実行するとともに、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する。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、関係部門長と協議の上、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、部門内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及び監事に報告する。

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、監事及びその他の関係部門長と協議の上、部門管理者が第 1 項の自主点検を行うために必要な事項等を定めた基準を設定し、その周知徹底に努めるとともに、必要に応じてこれらの見直し若しくは改善を図る。

（監　査）

第 15 条　監事は、この規程並びにこの規程に基づき情報セキュリティ事務管理者が設定する基準及び手続等の遵守状況を監査する。

2　情報セキュリティ事務管理者は、前項の監査の結果に応じ、情報セキュリティ部門管理者に対して改善を図るための指導を行うものとする。

（規程等の見直し・改善）

第 16 条　情報セキュリティ事務管理者は、この規程及びこの規程に基づき設定された基準等の実効性を確保するために、第 1 3 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上、定期的にこれらを見直すとともに、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。

（違反等の措置）

第 17 条　この規程及びこの規程に基づき情報セキュリティ委員会等が設定する基準等に違反した場合、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。

（規程の改廃）

第 18 条　この規程の改廃は、理事会の決議をもって行う。

附則　　この規程は、平成１７年４月１日から実施する。

この規程は、平成１７年６月１６日一部改正実施する。