長野県済生会情報セキュリティ規程

平成２１年１２月

社会福祉法人 恩賜財団 済生会支部長野県済生会

目次

長野県済生会　情報セキュリティ対策基本方針

平成２１年１２月　１日制　　定

（基本理念）

第１条　ネットワークを通じて福祉を求める人と提供する者が、また、施設と行政が、更に、地域の福祉施設が相互に繋がり、コミュニケーションの活性化を高めることで、今後一層のサービスの向上と効率化を図る。

開かれた福祉、開かれた施設の推進には、個人情報などの保護すべき情報資産が、高い安全管理のもとに運用されているシステムへの信頼が欠かせない。システムへの信頼が、福祉を求める人と提供者の信頼を高め、地域の福祉施設間の協働による地域福祉づくりの推進に寄与する。

２　当会管下施設は、今後の情報保護技術の発展に留意しながら、制度・技術・運用の全般にわたる安全管理措置を講じるとともに、不断の見直しによって情報資産の保護をより確実にする。

特に、蓄積した個人情報の保護は、情報セキュリティ対策の上で最も配慮する。

（目　　的）

第２条　長野県済生会情報セキュリティ対策基本方針（以下、「基本方針」という。）は、当会管下施設の保有する情報の機密性、完全性、可用性を維持するため、情報資産の取扱いと情報管理安全対策の基本的な考え方および方策を定め、当会管下施設の情報資産の管理を徹底することを目的とする。

（用語の定義）

第３条　この基本方針の用語の定義は次の各号とする。

①　情報とは、組織が判断を下したり行動を起したりするために必要な知識をいい、紙文書だけではなく、電子的な情報、会話での情報を含む。

②　情報セキュリティとは、情報の機密性、完全性、可用性を維持することをいう。

ア、機密性とは、記録された情報の参照等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をいう。

イ、完全性とは、情報の参照および記録・保管等が、正確かつ完全であることを保護することをいう。

ウ、可用性とは、認可された利用者が、必要なときに必要な時間内で、記録された情報に確実にアクセスできることをいう。

③　情報システムに関連した資産（以下、「情報資産」という。）は次のものをいう。

ア、情報

データベースおよびデータファイル、契約書および同意書、入所者・利用者に関する記録等、各種システムに関する文書、各種調査情報、各種マニュアル、訓練資料、運用手順またはサポート手順、事業計画、事業報告、代替手段の取決め、監査証跡、保存情報等。

イ、ソフトウェア資産

業務用ソフトウェア、システムソフトウェア、開発用ツールおよびユーティリティソフトウェア等。

ウ、物理的資産

コンピュータ装置、通信装置、取外し可能な媒体、その他装置等。

エ、サービス

計算処理サービス、通信サービス、一般ユーティリティ（例えば、照明、電源、空調）等。

（対象情報）

第４条　対象情報は、記録媒体を問わず、保管する全ての電子化情報、非電子化情報とし、業務に関する記録情報を含む。

（保護対象）

第５条　保護対象は、情報のみに限らず、記録媒体、保管手段および各種システム等の全てとする。

（適用範囲）

第６条　本基本方針は、全職員に適用する。また、退職した職員も同様とする。

（目的外利用の禁止）

第７条　情報は、定められた目的以外に利用してはならない。

２　情報資産および情報システムは、私的な目的に利用してはならない。

３　情報は、非合法な手段による利用、社内規則に違反した利用及び社会通念に反する利用をしてはならない。

４　情報は、提供を強要してはならない。

（情報の開示）

第８条　施設外へ情報を開示する場合は、施設長の許可を受けなければならない。

（情報セキュリティ遵守措置）

第９条　当会管下施設は、当会管下施設の情報資産を利用するすべての者（以下、「職員等」という。）に対し、基本方針の趣旨を理解・認識・遵守させるために必要な措置を講じる。

２　職員に対し、採用時に情報セキュリィティ等について、必要な内容を理解させ、実施及び遵守させるための必要な措置を講じる。

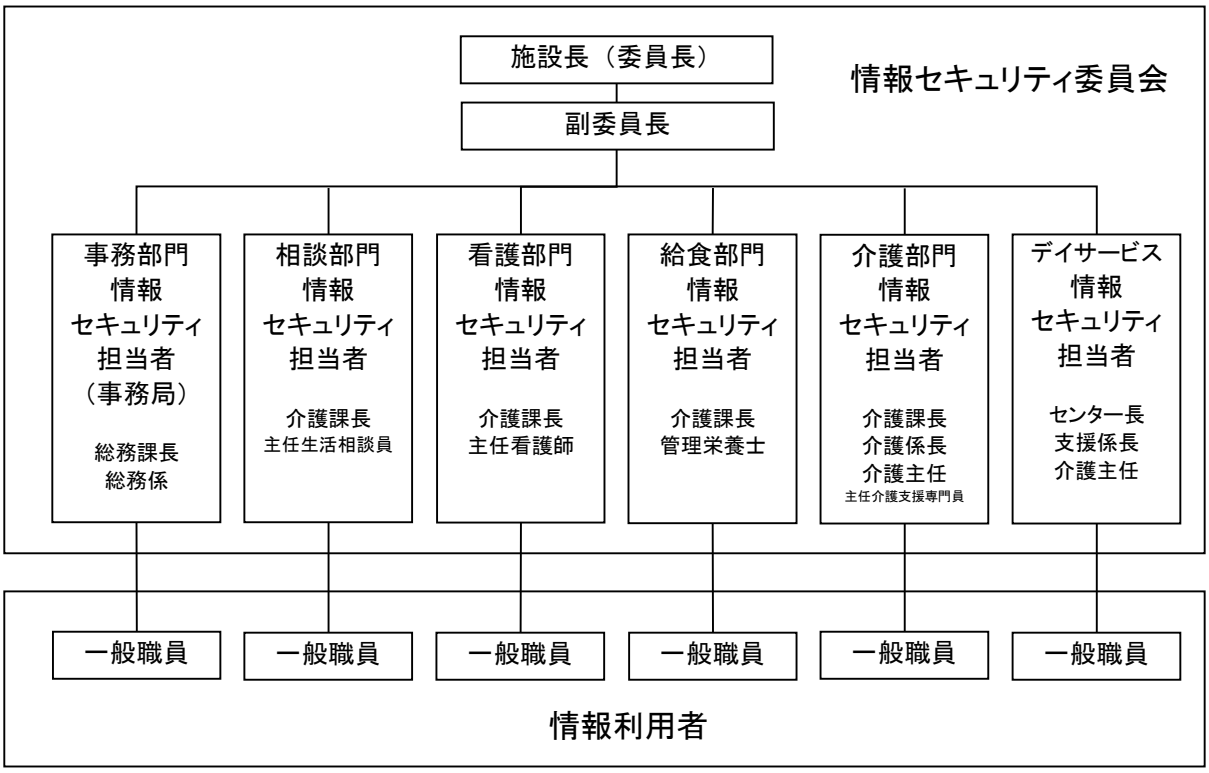
３　また外部委託業者および関係施設・団体に対しては、契約等により、また別途取決めを行うことにより、基本方針を遵守させるための必要な措置を講ずる。

４　職員は、退職等により業務を離れる場合には、業務上知り得た情報を漏らしてはならない。

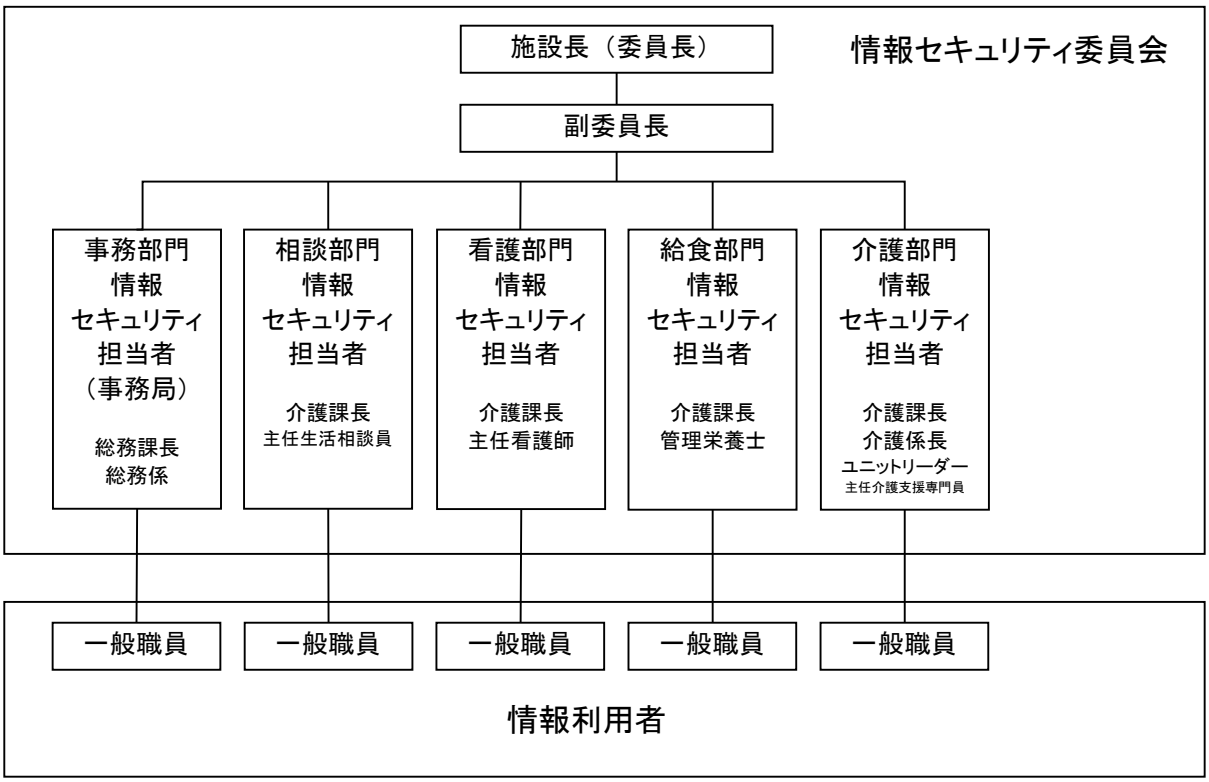
（情報セキュリティ対策体制）

第１０条　当会管下施設の保有する情報資産のセキュリティ対策を推進管理するため、施設長直属の情報セキュリティ管理委員会（以下、「委員会」という。）を設置する。

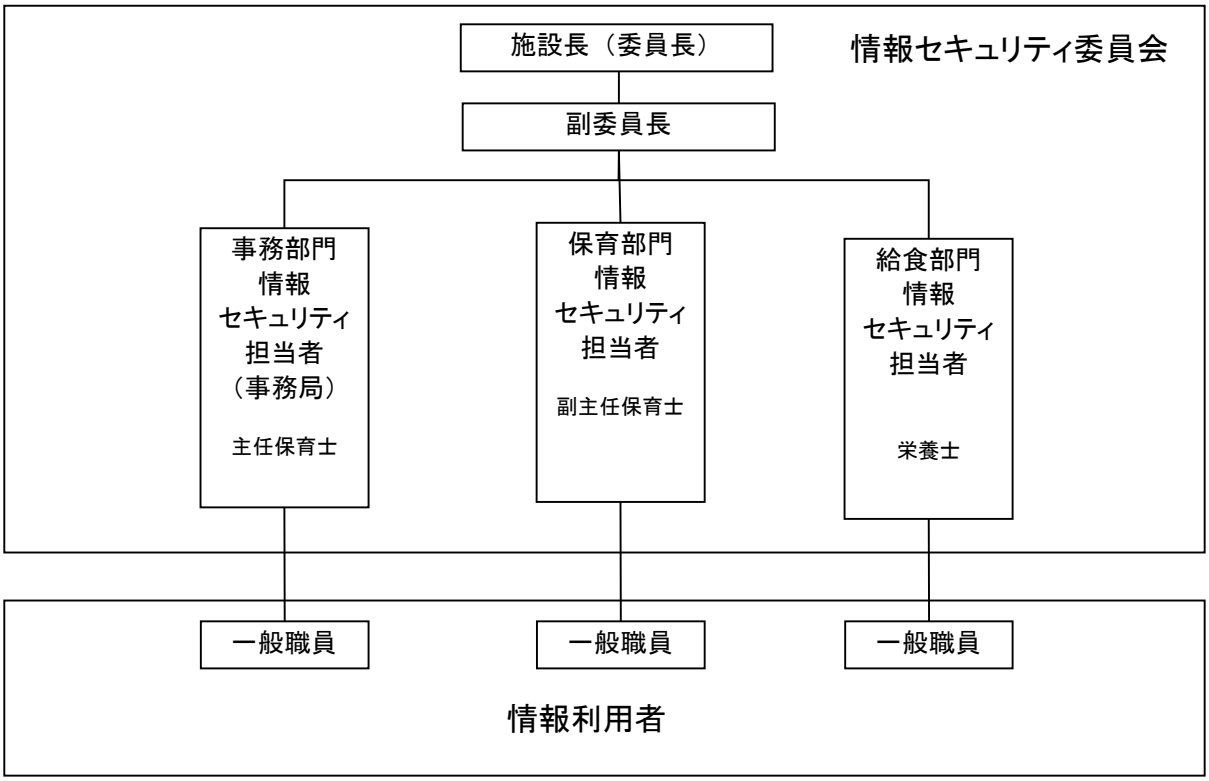
1　シルバーランドみつい



2　シルバーランドきしの



３　長野保育園



（情報資産の分類）

第１１条　情報資産は、情報の重要性の度合いに応じて評価基準に従い分類し、取扱いについて管理方法を定め、必要に応じ取扱いの制限を行う。

（情報資産への脅威）

第１２条　情報資産に対する脅威の発生度合や発生した場合の影響を考慮し、特に認識すべき脅威は次のとおりとする。

①　部外者による故意の不正アクセスまたは不正操作によるデータやプログラム、記録等の持出・盗聴・改ざん・消去、機器・媒体の盗難、故意の障害発生行為による福祉サービスをはじめとする業務の停止。

②　職員等および外部委託業者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラム、記録等の持出・盗聴・改ざん・消去、機器・媒体の盗難および規定外の端末接続によるデータ漏えい。

③　地震・落雷・火災等の災害および事故・故障等による福祉サービスをはじめとする業務の停止。

（情報セキュリティ対策）

第１３条　前条の脅威から情報を保護するため、次のセキュリティ対策を行う。

①　物理的セキュリティ対策

情報システム機器を設置する場所等への不正な立ち入り、情報資産への損傷・妨害などから保護するため、パスワード等で物理的に対処する。

②　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、職員等に情報セキュリティに関する法令および規程等の内容を周知徹底するため、十分に教育および啓蒙する。

③　技術的セキュリティ対策
　情報資産を外部からの不正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、ネットワーク管理等で技術的に対処する。

④　運用におけるセキュリティ対策
　アクセス権限の管理、情報セキュリティに関する法令および基本方針の遵守状況を確認する等の運用体制を確立する。また、緊急事態が発生した場合に、迅速な対応を可能とする危機管理体制を定める。

（情報セキュリティ対策標準の策定）
第１４条　前条の対策を講ずる際、遵守すべき行為および判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した「情報セキュリティ対策標準（以下、「対策標準」という。）」を策定する。

（情報セキュリティ実施手順の策定）
第１５条　前２条の情報セキュリティ対策を実施するため、個々の情報システムの具体的な実施手順を明記した「情報セキュリティ実施手順（以下、「実施手順」という。）」を別に策定する。

（職員教育）
第１６条　基本方針および対策標準の職員等への周知と、情報セキュリティの意識向上のため、情報セキュリティに関する教育を実施する。

（違反への対応）
第１７条　職員等が、基本方針および対策標準等の関係規程に違反した場合は、次の対応とする。

①　当会管下施設が雇用した職員については、シルバーランドみつい及びシルバーランドきしの職員就業規則第４７条４号、長野保育園就業規則第５４条４号に基づく懲戒処分等の対象とする。

②　当会管下施設が契約を締結したサービス提供業者、下請負業者、人材派遣業者等、およびこれら業者の従業者であって、当会管下施設と締結した契約の履行のために派遣された者などについては、法令および別途取決めにより、補償を請求する。

（情報セキュリティ実施状況の検証）
第１８条　基本方針および対策標準の遵守状況を確認するため、情報セキュリティ実施状況を検証する。

（評価および見直しの実施）
第１９条　前条の検証結果を踏まえた上、情報セキュリティを取り巻く状況の変化に対応するため、基本方針、対策標準および実施手順の見直しを適宜行う。

付　　則
この情報セキュリティ対策基本方針は、平成２１年１２月　１日から施行する。

長野県済生会　情報セキュリティ対策標準

平成２１年１２月　１日制　　定

１．総則

（１）目　的

この情報セキュリティ対策標準（以下、「対策標準」という。）は、情報セキュリティ対策基本方針（以下、「基本方針」という。）第１４条に基づくセキュリティ対策の基本的な要件を定め、もって情報システムの適正な運用と確実な情報管理に資することを目的とする。

（２）適用範囲

この対策標準の適用範囲は、次のとおりとする。

１）情報の範囲

情報システムで取扱うデータおよび情報システムの開発、運用に伴うすべてのデータをはじめ、ＣＤ、ＤＶＤ等の媒体に記録されたデータ、紙に印字・記録されたデータおよび会話を含む、施設の運営に関するすべての情報とする。

２）システムおよびシステム機器の範囲

①　所有権の有無に関わらず（リース等を含む)、業務の用に供しているすべてのコンピュータ機器、コンピュータ周辺機器およびその機器上で使用するソフトウェアとする。

②　委員会の許可を得て業務上使用する個人所有の情報機器も、適用範囲とする。

３）対象者の範囲

①　対象者の範囲は、基本方針第９条の定めに基づき、シルバーランドみつい及びシルバーランドきしの職員就業規則第４条に規定する常勤職員、済生会長野保育園職員就業規則第３条に規定する常勤職員、パート職員、実習生、研修生、ボランティア、派遣社員等とする。

②　前項のほか、施設内で作業する外部業者、サービス記録等の外部保存委託先でデータ管理業務に携わる者および一般来訪者等であっても、当会管下施設の情報資産を利用する場合には、対象者とする。

（３）位置付け

この対策標準は、施設の業務全般に関わる重要な財産である情報資産の取扱いを定めるので、施設の他の規程と同様の手続きにより、制定、運用し、改廃する。

（４）施設長の責務

１）施設長は、基本方針、対策標準を早急に作成し、また、施設内外の状況等に変化があった場合は、基本方針、対策標準の改訂を遅滞なく行う。

２）施設長は、職員等に対し、基本方針、対策標準の趣旨・内容を理解・遵守させ、また、そのために必要な教育・研修等を行う。

（５）職員等の責務

１）職員等は、円滑な業務遂行、サービスの向上のために情報資産の利用が認められていることを認識し、情報資産の私的利用や悪用を行わない。

２）職員等は、基本方針、対策標準の趣旨を理解して遵守する。また、これに違反した者は、その結果に責任を負う。

（６）外部委託業者の取扱い

この対策標準の範囲内で行われる作業や管理等を外部業者等に依頼する場合は、基本方針、対策標準を遵守し、情報セキュリティ事故発生時の責任の所在等に関し、契約あるいは別途

取決めにより明確にする。

２．基本用語の定義

（１）情報
情報の定義は、基本方針第３条第１号の定めによる。

（２）情報システムに関連した資産
情報システムに関連した資産（以下、「情報資産」という。）の定義は、基本方針第３条第３号の定めによる。

（３）情報セキュリティ
情報セキュリティの定義は、基本方針第３条第２号の定めによる。

（４）ネットワーク
１）ネットワークとは、コンピュータを接続して通信を行い、ハードウェア、ソフトウェア、データ等を共有する仕組みをいう。
２）この対策標準では、基幹システム（利用者情報システム等)、各部門システムおよび関連機器などの各種オンラインシステムのデータ伝送を目的とした情報通信基盤をいう。

（５）情報システム
情報システムとは、情報を適切に保存・管理・流通する仕組みであり、この対策標準では、福祉等の業務を行うコンピュータとネットワーク、それを制御するソフトウェアおよびその運用体制までをいう。

（６）リスク
リスクとは、情報および情報処理施設・設備に対する危険（脅威）あるいは損害を受ける可能性をいう。
○　リスク分析とは、リスク因子（内容）を特定するためおよびリスクの危険度（発生頻度等）を算定するため、情報の系統的分類・調査をいう。
○　リスク対応とは、リスクを変更させるための方策を選択および実施するプロセスをいう。

（７）リスクアセスメント（リスク評価）
リスクアセスメントとは、リスクの大きさを評価し、そのリスクが許容できるか否かを決定する全体的なプロセスをいう。
情報および情報処理施設・設備に対する危機（脅威）の発生に際し、発生源、伝播の経路、被害者の反応、発生頻度等のデータに基づき、どれだけの影響があるかを評価する。

（８）リスクマネジメント
リスクマネジメントとは、リスクに関して組織を指揮し管理する調整された活動であり、許容されるコストで、情報システムに影響を及ぼす可能性があるセキュリティリスクを明確にし、制御し、最小限に抑制するか、または除去するプロセスをいう。

（９）脅威
脅威とは、システムまたは組織に損害を与える可能性があるインシデント（事象）の潜在的な原因、自然災害、機器障害、悪意のある行為等の損失発生要因をいう。
１）災害（地震、落雷、火災、水害など）
２）障害（ハードウェア障害、ソフトウェア障害、ネットワーク障害、設備の故障など）
３）人為的な脅威（不正侵入、コンピュータウイルス、盗聴、窃盗、不正使用、改ざん、

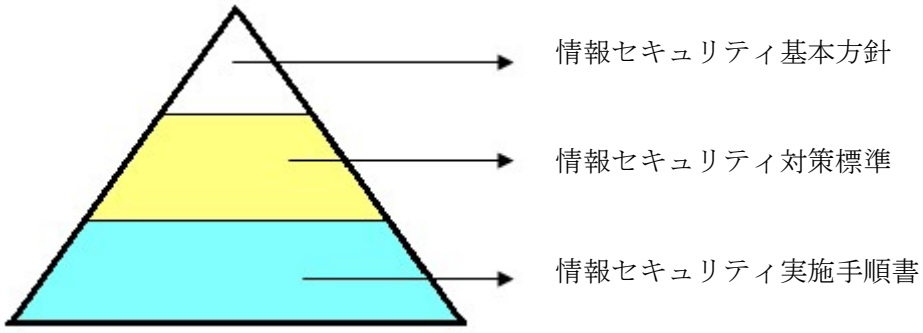
なりすまし、過失など）

（10）脆弱性
1）脆弱性とは、脅威がつけ込むことができる情報資産がもつ弱点のことをいう。
2）脆弱性には、建物の構造上の欠陥、定期点検の不備、情報セキュリティ規程・要員教育の不備等がある。
○　特に、情報システムでは、第三者が保安上の脅威となる行為（システムの乗っ取りや機密情報の漏えいなど）に利用できる可能性のあるシステム上の欠陥や仕様上の問題点がある。

３．情報セキュリティ実施手順書

基本方針第５条により設置する情報セキュリティ管理委員会（以下、「委員会」という。）は、基本方針と対策標準に基づいて、情報セキュリティの具体的な実施手順を定めた「情報セキュリティ実施手順書」および各種申請様式等を制定し、その実施、徹底に努め、必要に応じて改正する。

○　各セキュリティ対策文書の位置づけ
【参考図】



４．情報セキュリティ規程類の配付、周知標準

（１）目的
この項は、新たに制定され、または、改正された情報セキュリティ規程類の配付と周知に関する事項を定め、もって情報の取扱いに万全を期すことを目的とする。

（２）職員等への周知
委員会は、情報セキュリティ規程類の制定、および改正をした場合は、迅速にすべての職員等へ周知する。

（３）配付の手段
1）情報セキュリティ規程類の周知は、印刷配付等で行う。
2）情報セキュリティ規程は、すべての職員等が閲覧できるようにする。

（４）職員等の確認
職員等は、委員会からの周知を受けたときは、速やかに情報セキュリティ規程類の内容を確認し、理解に努める。

５．情報セキュリティ規程更新手順に関する標準

（１）目的

この項は、当会管下施設の情報セキュリティ規程を更新する場合の手順およびそれに関わる遵守事項を定め、もって規程類の陳腐化を防ぐことを目的とする。

（２）更新案件の提案

委員会のメンバーは、情報セキュリティ規程に更新の必要性を認識したときは、その更新について提案できる。

（３）委員会での審議および決定

委員会は、提案された更新案件に関し、提案日の属する月またはその翌月中に、更新の可否について審議する。

（４）更新結果の反映と記録

委員会は、実施を決定した更新案件について、情報セキュリティ規程の改正を行い、改正内容の記録を議事録等により保管する。

（５）施設長および担当役員に対する報告

委員会は、決定した更新案件について、改正後の規程とともに、施設長および支部事務局に報告する。

（６）対策標準の改正

１）この対策標準に、改正が必要な事項があると判断した者は、改正理由を付して委員会に申請できる。

２）委員会は、申請日の属する月またはその翌月中に申請内容を審議し、改正が必要と認めた場合は速やかに改正に必要な手続きを行い、（５）に準じた報告をした後、改正内容をすべての職員等に周知する。

３）委員会が改正の必要を認めなかったときは、その理由を明示して申請者に回答するほか、掲示等により職員等にも周知する。

６．情報セキュリティ管理体制

（１）目的

この項は、基本方針第１０条により設置する委員会（第３項の情報セキュリティ実施手順書を参照)、および情報システム担当部署に関する事項を定め、もって保有情報資産の情報セキュリティ管理体制を実効あるものにすることを目的とする。

（２）委員会の構成

委員会は、次の各委員により構成する。

１）委員長

①　委員長は、施設長とする。

②　委員長は、随時、委員会を招集し、その議長となる。

２）副委員長

副委員長は、各部署の長の中から委員長が任命する。

３）委員

次の者を委員とし、施設長が委嘱する。

① 各部署の長
各部署内で情報セキュリティ対策の推進責任者とする。
② 各部署の情報セキュリティ担当者
各部署の長が部署ごとに推薦し、委員長が認定する者とし、情報セキュリティ対策の実施にあたり各部署の長を補佐する。
③ 委員長は、審議の必要に応じ、情報システム担当部署職員等を臨時委員として参加させ、意見を求めることができる。また、必要に応じ、外部業者等に作業を委託できる。

3）委員会の事務局
委員会の事務局は、情報システム担当部署（またはそれに該当する部署）が行う。

（3）委員会の役割と責務
委員会の主な役割は次のとおりとする。

1）規程等の周知徹底
委員会は、全職員等に対し、対策標準の周知徹底に努め、教育・研修を実施する。

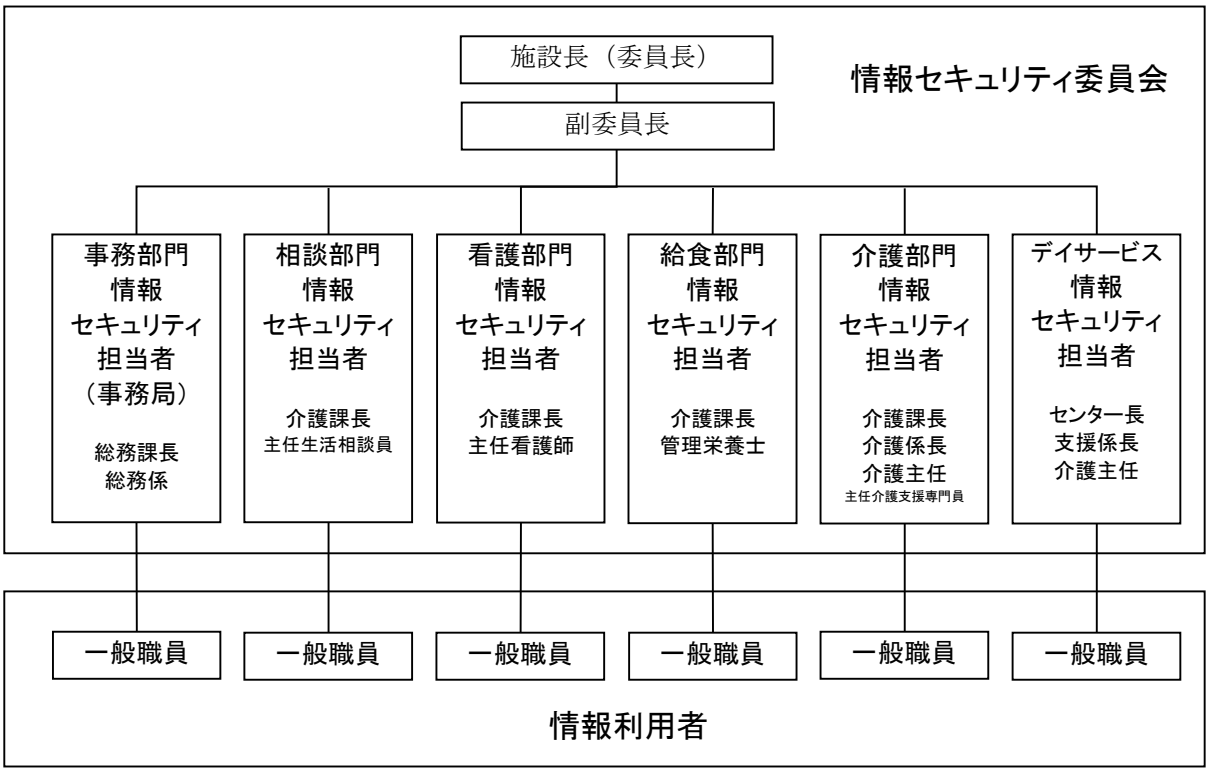
2）監査、評価
① 委員会は、情報セキュリティに関する監査および評価を行い、対策標準に反映させる。
② 委員会は、前項を行うため、各部署に立ち入り、または、関係者を招集し調査することができる。

3）規程の改訂
委員会は、必要に応じて対策標準その他セキュリティ関連諸規程を改訂し、施設長の認可を得た上、執行する。

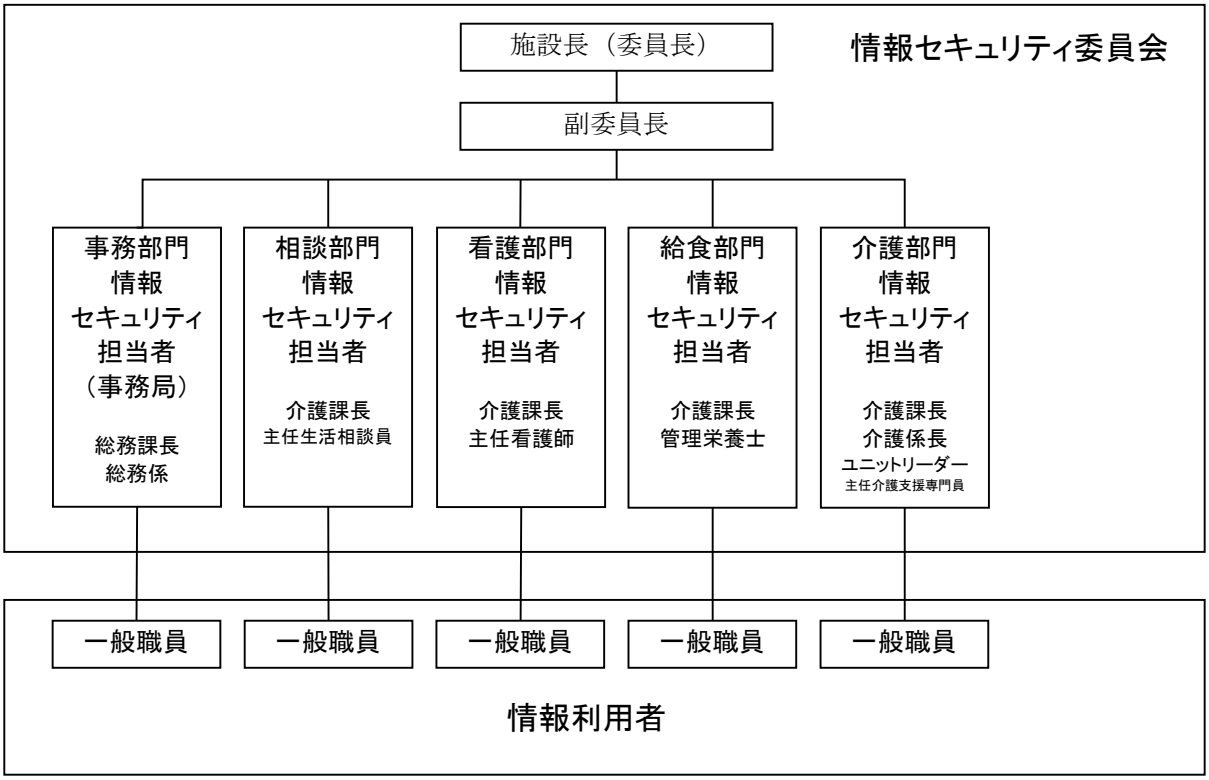
4）職員教育
① 委員会は、情報資産を扱うすべての職員等に対し、情報セキュリティを教育する。
② 委員会は、情報セキュリティ関連教育を企画立案し、運営を担当する。

5）違反者の処罰（処分）
委員会は、職員がセキュリティ関連諸規程に違反したと判定したときは、施設長に、シルバーランドみつい及びシルバーランドきしの職員就業規則第４７条４号、長野保育園職員就業規則第５４条４号に基づく懲戒処分を申請できる。

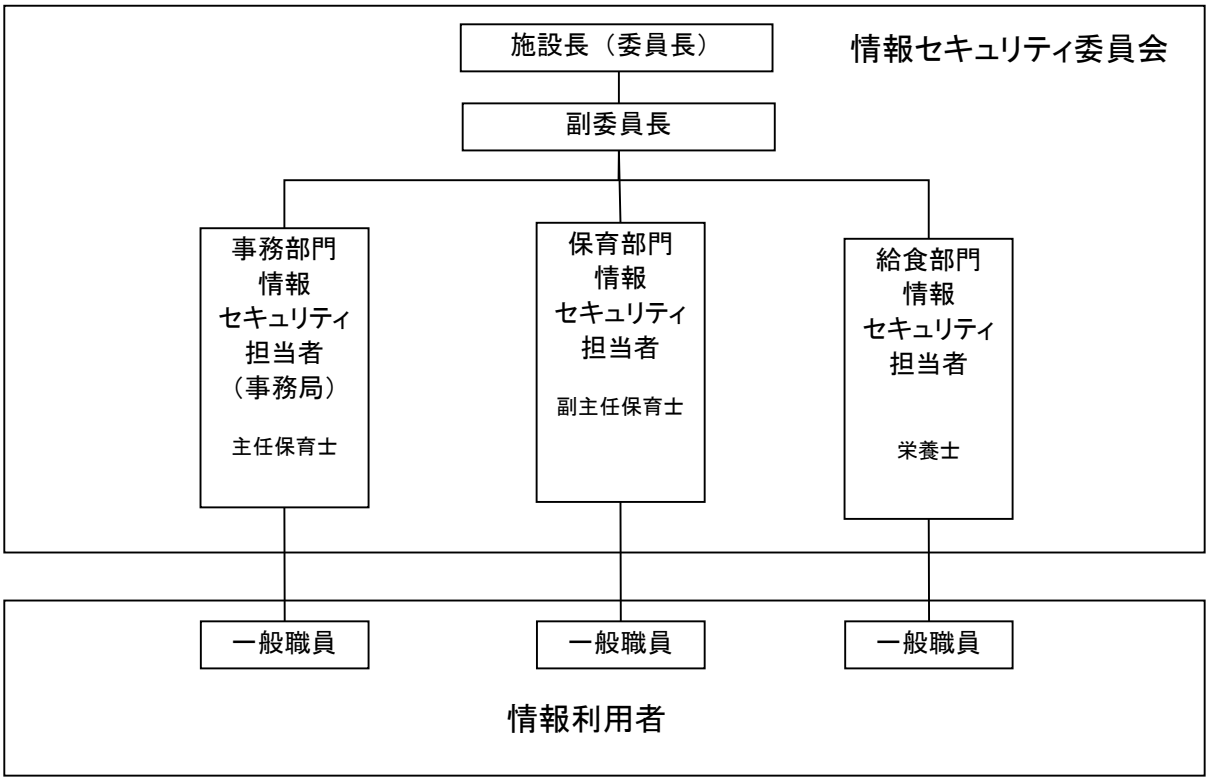
1　シルバーランドみつい



2　シルバーランドきしの



3　長野保育園



（4）情報システム担当部署

1）情報システム担当部署は、事務部門とし、委員会で決定した対策事項を実施および推進する。

2）情報システム担当部署は、施設の情報機器の管理責任を有し、施設に関係するセキュリティ情報収集を行い、施設内のセキュリティ対策に反映させる。

（5）システム担当者

1）システム担当者は、情報システム担当部署よりシステム担当者を任命する。

2）システム担当者は、委員会で決定した管理作業を行う。

7．委託時の契約に関する標準

（1）目的

この項は、当会管下施設の業務を外部業者に委託する場合に、契約および委託作業時に関して必要な事項を定め、もって問題発生を未然に防ぐことを目的とする。

（2）対象システム

委託業務で使用するすべてのもの

（3）委託先の選定に関する遵守事項

委託しようとする業者は、信頼できる業者の中から入札等により選定する。

（4）委託契約に関する遵守事項

委託先を決め、契約を締結するときは、委託業務の仕様以外に、機密保持に関する以下の事項を盛り込む。

・委託業者は、当会管下施設の業務で知り得た情報を、第三者に漏えいしないこと。

・情報漏えいがあった場合の、罰則や補償に関すること。

８．情報資産の保護

（１）情報資産の保護

委員会およびシステム担当者は、部署ごとに情報資産を洗い出し、本項の定めに従い、情報資産の特定、分類およびリスク分析ならびに保護を行う。

（２）情報資産の特定

委員会およびシステム担当者は、「情報資産管理台帳」を作成し、情報資産を管理する。

（３）情報資産の評価

１）委員会およびシステム担当者は、分類された情報資産の価値を体系的に評価し、「情報資産管理台帳」の「情報資産の価値」に記載する。

２）前項の評価は、①機密性、②完全性、③可用性に関し、以下の評価基準による。

① 機密性

基 準	評価値	説 明
極秘	D	所定の関係者のみに開示・提供可能
(秘)	C	特定な関係者または部署のみに開示・提供可能
施設外秘	B	組織内では開示・提供可能
公開	A	第三者に開示・提供可能

② 完全性

基 準	評価値	説 明
重要	C	完全性が維持されないと業務への影響は深刻かつ重大である
要	B	改ざんされると問題あるが業務への影響は少ない
不要	A	参照程度でしかりようされていない

③ 可用性

基 準	評価値	説 明
高	C	必要時に確実に情報が利用できないと影響は深刻かつ重大である
中	B	情報が利用できなくなると支障あるが、代替手段で業務できる
低	A	情報が利用できなくとも支障ない

（４）情報資産の保管場所

１）委員会およびシステム担当者は、情報資産ごとに保管場所を明確にし「情報資産管理台帳」の以下の「保管場所」に記載する。

２）前項の定めに拘らず、同一の目的に使用する情報資産を同一フォルダに記録する場合は、フォルダ単位で情報資産管理台帳に記載できる。

1	各種業務サーバ
2	テープ装置の常駐メディア(ＬＴＯ、ＤＡＴ等)
3	キャビネット、耐火金庫
4	各部用サーバ／PC
5	バックアップメディア(ＬＴＯ、ＤＡＴ外付けＨＤＤ、ＤＶＤ、ＭＯ、ま

	たはこれに準じるもの)
6	データメディア(外付けＨＤＤ、ＣＤ、ＤＶＤ、ＭＯ、ＦＤ、ＵＳＢメモリ、またはこれに準じるもの)

９．職務定義および雇用における標準

（１）目的

この項は、職員等（シルバーランドみつい及びシルバーランドきしの職員就業規則第４条に規定する常勤職員、済生会長野保育園職員就業規則第３条に規定する常勤職員、パート職員、派遣職員、請負業者等を含む当会管下施設の内部関係者）の職務を明確にし、もってシステム使用時の誤り、不正行為または設備の誤用のリスクを軽減することを目的とする。

（２）職員等の審査およびその個別方針

１）職員採用の際、履歴書等の応募資料を精査し、不正行為等が行われないよう留意する。

２）取扱いに慎重を要する情報にアクセスが必要な職員等は、可能な範囲で信用調査を行う。

３）派遣職員は、常勤職員の採用と同等な審査手続きができないため、派遣会社が行う審査の責任等を、派遣会社との契約に明記する。

（３）機密保持契約

１）職員および外部利用者には、情報処理設備へのアクセスを認める前に、誓約書または機密保持契約書への署名を求める。

２）機密保持契約は、雇用条件または請負契約に変更がある場合、特に職員等がその組織を離れるとき、または請負契約が終了するときは、見直しを行う。

（４）雇用条件

１）雇用条件には、情報セキュリティに関する職員等の責任について記述する。

２）情報セキュリティに関する責任は、雇用終了後も継続する。

３）職員等がセキュリティ要求事項を無視した場合にとる措置に関しても、雇用条件に含める。

１０．セキュリティ教育に関する標準

（１）目的

この項は、情報セキュリティの脅威および懸念に対する利用者の認識を確実なものとするために必要な教育等に関する事項を定め、もって職員等が通常業務の中で基本方針等の遵守を確実にすることを目的とする。

（２）教育の計画立案

情報システム担当部署は、教育対象となる職員等の理解度を把握し、適切な時期に教育計画を立案する。

１）一般説明会

情報システム担当部署は、年に１回コンピュータに携わるすべての職員等に対し、セキュリティに関する説明会を実施する。

２）再教育

情報システム担当部署は、セキュリティ違反者に対し、セキュリティの再教育を実施し、違反の再発防止に努める。

３）新入職員、中間採用者への教育

情報システム担当部署は、新入職員、中間採用者、派遣職員に対し、入職時にセキュリティ教育を実施する。

4）施設内外異動者への教育

情報システム担当部署または、各部署の情報セキュリティ担当者は、施設内外異動者に対し、異動時に、その部署の情報セキュリティに関する教育を実施する。

（3）教育の実施

情報システム担当部署は、コンピュータに携わるすべての職員等に対し、以下の教育内容について、教育資料を使用し、セキュリティの教育を実施する。

○　教育内容

・情報セキュリティの問題の持つ意味を理解
・組織や個人の情報セキュリティの重要性
・セキュリティ対策
・データ所有者の責任
・モラル

（4）教育資料

教育に用いる次の資料は、適切な教育を行うため、必要に応じて見直す。

○　教育資料

・一般説明会教育資料
・再教育資料
・新入職員教育資料
・中間採用者教育資料

（5）教育実施記録

情報システム担当部署は、教育の実施状況に関する以下の記録を作成し、保管する。

○　記録項目

・教育実施日
・教育実施者（部署）
・教育受講者
・教育内容

１１．罰則に関する標準

（1）目的

この項は、当会管下施設のセキュリティ違反に対する罰則の適用手順およびその際の遵守事項を定め、もってセキュリティ違反の防止に寄与することを目的とする。

（2）罰則案件の申し出

1）各部署の長は、罰則に相当すると思われる職員等のセキュリティ違反を確認した場合は、委員会に罰則の適用審議を求める案件として申し出る。

2）各部署の長のセキュリティ違反に関する罰則案件は、委員会の委員が申し出る。

（3）委員会での審議および決定

委員会は、申し出が行われた罰則案件について、申し出日の属する月またはその翌月に審議を行い、罰則の適用と再教育の要否、程度および内容を決定する。

（4）人事部門の罰則手続き

人事部門は、委員会の決定に基づき、該当者の就業規則に定める罰則適用に関する手続きを行う。

（５）再教育
委員会は、罰則案件の審議結果で再教育が必要と決定した該当者に対し、再教育を行う。

１２．物理的対策標準

（１）目的
この項は、敷地・建物・機器・設備等の保護に関する事項を定め、もってそれらの損傷や利用の妨害、許可されていないアクセスを防止することを目的とする。

（２）対象
情報システムに係るすべての物理的資産を対象とする。

（３）機器・設備の保護
１）機器・設備は、不正な操作やミスが起こりにくいように配慮して設置する。
２）特別な保護を必要とする機器・設備は、それ以外の機器・設備の保護レベルを上げるため、分離して設置する。
３）設置場所に応じ、機器・設備の落下や損傷の防止措置をとる。
４）機器周辺での飲食は、認めない。

（４）電源・空調の保護
１）電源および空調設備には、耐震、耐火、耐水などの防災対策を講じる。
２）電源は、安定化装置の導入、負荷変動機器との配電隔離等により、電源容量と電圧変動の安定を確保する。
３）電源は、過電流・漏電等に対する保護措置を講じる。
４）電源には、避雷設備を設置する。
５）重要度の高い機器・設備の電源には、無停電電源装置、バックアップ電源等を設置する。
６）空調設備は、機器・設備を適切に運転するために必要な能力（温度・湿度の調整能力）を確保する。
７）重要度の高い機器・設備に対する空調設備には、予備装置を確保する。

（５）ケーブルの保護
１）ケーブルは、損傷や盗聴を避けるため、保護用の電線管・カバーの使用や、敷設経路に対する配慮などの対策を講じる。
２）干渉防止のため、電源ケーブルと通信ケーブルは分離する。
３）重要度の高いケーブルは、代替経路を準備する。

１３．職場環境におけるセキュリティ標準

（１）目的
この項は、職場環境のセキュリティリスクを低減するために必要な事項を定め、もって情報漏えい等のセキュリティ事故を防止することを目的とする。

（２）対象システム
職場環境に存在するすべての情報資産を対象とする。

（３）書類・媒体等の取扱いと保管（クリアデスクポリシー）

1）使用していない書類や媒体は、机上等に放置せず、キャビネット等へ収納する。
2）重要度の高い書類や媒体は、施錠して保管する。特に必要な場合は、耐火金庫・耐熱金庫に保管する。

（4）画面に表示する情報の管理（クリアスクリーンポリシー）
不正な操作や盗み見防止のため、ＰＣ使用中に離席するときには、ログオフするか、画面およびキーボードロック等の保護機能を使用する。

（5）事務・通信機器の取扱い
1）ホワイトボード等への書き込みは、使用後に必ず削除し、放置しない。
2）コピー機、ＦＡＸ、プリンタ等の入出力書類は、放置しない。特に重要度の高い書類は、印刷および送受信の間、職員等が常に機器（ＦＡＸの場合は送受信の両側とも）に立ち会う。
3）誤送信を防止するため、ＦＡＸ送信時には、必ず宛先を確認する。

（6）搬入物の受渡し
1）搬入物の受入れを行う職員は、受入れの際に危険物持込や情報漏えい等のリスクがないかどうか点検する。
2）搬入物が、登録の必要な情報資産である場合は、受入れ後、速やかに登録作業を行う。
3）郵便物の受入れ場所には、盗み見や抜き取りの防止対策を講じる。

（7）口頭情報漏えい防止
電話、立ち話、オープンスペースの発言および会話について、盗み聞き等の防止に配慮する。

１４．ウイルス対策標準

（1）目的
この項は、ウイルスやワーム等の不正プログラムに関する対策を定め、もってこれらが引き起こす情報漏えいやシステム破壊の被害を未然に防止することを目的とする。

（2）対象システム
クライアントＰＣ、サーバを含むすべてのコンピュータおよび周辺機器を対象とする。

（3）ウイルス対策ソフトウェアの導入
1）ウイルス対策ソフトウェアは、情報システム担当部署が指定したソフトウェアを使用する。
2）ウイルス対策ソフトウェアの選択要件には、以下の機能を含む。
・定義ファイルの自動更新機能
・常時スキャン機能
（ファイルシステム、電子メール）

（4）ウイルス対策ソフトウェアの利用
1）ウイルス対策ソフトウェアは常駐設定とし、ファイルへのアクセスおよび電子メールの受信時には、自動でウイルススキャンを行うよう設定する。
2）職員等は、定期的に、すべてのファイルに対してウイルススキャンを実施する。
3）常駐設定の際、定義ファイルの自動更新機能を使用する。

（5）ソフトウェアのセキュリティ対策
職員等でＰＣを借用している者は、ＰＣに導入されているソフトウェアを「２３．ＰＣ等

におけるセキュリティ対策標準」に基づき、ソフトウェアアップデートを実施する。

（６）電子メールを介したＰＣのウイルス被害の防止
１）電子メールを使用するときは、ウイルス対策ソフトウェアの電子メール保護機能を有効にする。
２）送信元不明のメールの添付ファイル、実行形式のまま添付されたファイル等の不審な添付ファイルは、ウイルス等悪意のあるプログラムの可能性が高いため実行しない。また、添付ファイルとともにメール自体も削除する。
３）ファイルを添付してメールを送信する場合は、当該ファイルにウイルス感染が無いことを必ず確認する。
４）電子メールサービスを利用中に、ウイルスまたはウイルスと思われる症状を発見した場合は、「２８．セキュリティインシデント報告・対応標準」に基づき対応する。

（７）情報システム担当部署のウイルス対策窓口の設置
１）情報システム担当部署は、施設内のウイルス被害状況等を迅速に収集するために、ウイルス対策窓口を設置し、周知徹底する。
２）ウイルス対策窓口は、施設内のウイルス被害状況を掌握し、問題発生時の一次対応を担当する。

（８）ウイルス対策ソフトウェアがウイルスを検知した場合
１）職員等は、ウイルスを認知したときは、コンピュータをネットワークから切り離した後、ウイルス対策ソフトウェアを使用してウイルスの駆除または隔離を行う。
２）ウイルスを駆除または隔離した職員等は、情報システム担当部署に報告する。

（９）ウイルス感染の疑いがある場合
１）職員等は、ウイルス対策ソフトウェアが検知しなくとも、ウイルスに感染した疑いを持ったときは、ウイルス対策窓口に連絡する。
２）前項の連絡を受けたウイルス対策窓口は、ウイルス感染が疑われる場合は、職員等にＰＣからネットワークケーブルをはずすことを指示し、現場に急行する。
３）ウイルス対策窓口は、現場でウイルス対策ソフトウェアの定義ファイルのバージョンを確認するとともに、最新の定義ファイルを用いてＰＣのすべてのファイルに対し、ウイルススキャンを行う。
４）前項のスキャンによりウイルスが検知された場合は、そのウイルスの特性上どのような挙動を示すかを予測し、影響範囲を特定し、対策を講じる。
５）ウイルスが検知されなかった場合でも、ファイアウォールのログを確認するなど、原因を追究する。
６）ウイルス被害の影響範囲が、施設外にまで至っている場合は、「２８．セキュリティインシデント報告・対応標準」に基づき、問題の沈静化を図る。

１５．システム維持に関する標準

（１）目的
この項は、ソフトウェアアップデートおよびバックアップに関する事項を定め、もって当会管下施設システムのセキュリティレベルを維持することを目的とする。

（２）対象システム
当会管下施設の職員等が業務上使用するすべてのサーバ、クライアントＰＣ、ネットワーク機器

（3）ソフトウェアアップデートのルール

1）職員等は、「１６．セキュリティ情報収集および配信標準」に基づき情報システム担当部署の指示を受け、自分が管理または使用しているすべてのＰＣに速やかにソフトウェアアップデートを実施する。

2）情報システム担当部署は、施設内のすべてのＰＣに、前項のソフトウェアアップデートが指示通り実施されているか確認する。

3）ソフトウェアアップデートに伴うサービスの停止など他システムへの影響が大きい場合は、あらかじめ関係各部署で綿密な調整を行うとともに、施設内外への周知を確実に行う。

4）各部署で管理運営しているシステムにソフトウェアアップデートを実施する場合は、情報システム担当部署に、実施したいソフトウェアアップデートとその理由を報告する。

5）ソフトウェアアップデート中に何らかのトラブルが発生した場合は、作業者は、トラブルの内容を情報システム担当部署に報告する。

6）情報システム担当部署は、前項のトラブル報告を受けた場合は、今後同様なトラブルを防止する対応を定めた上、関係各部署へ連絡する。

（4）アップデートプログラムの取得および配付方法

ＯＳやアプリケーション等のソフトウェアおよびネットワーク機器等のハードウェアのいずれのアップデートプログラムも、システム担当者がベンダーのサイト等から取得する。

（5）ウイルス定義ファイルの更新

システム担当者は、「１４．ウイルス対策標準」に基づき、安全性が認められたウイルス定義ファイルを更新する。

１６．セキュリティ情報収集および配信標準

（1）目的

この項は、当会管下施設内で使用する製品のセキュリティ情報の収集に関する事項を定め、もってセキュリティレベルを維持することを目的とする。

（2）対象システム

当会管下施設が導入しているすべてのソフトウェアおよびハードウェア

（3）セキュリティ情報の収集

1）情報システム担当部署は、「２７．ソフトウェア／ハードウェアの購入および導入標準」に基づき作成した各管理台帳をもとに、施設内システムに導入されているすべてのハードウェアおよびソフトウェアのセキュリティ情報を、定期的に収集する。

2）セキュリティ情報は、各ベンダーのＷＥＢサイトやサポートページなどから収集する。

3）情報システム担当部署は、セキュリティ関連のメーリングリスト、セキュリティセミナーなどに参加し、情報を収集する。

4）収集した情報は、重要性、影響範囲などを考慮し、以下に分類する。

危険度　高：サーバ管理権限の奪取方法など、業務停止や利用者への悪影響の可能性が高く、即座に対応が必要な情報

中：業務停止はなく、または、利用者などに影響を与えないため、即座対応の必要はないが、定期メンテナンス時などに対処する必要がある情報

低：特殊な環境／設定でのみ発生し、施設のシステムには関係がないため、特に対処しなくともよい情報

（4）セキュリティ情報の配付

1）情報システム担当部署は、収集した情報を危険度に応じて関係者に通知する。

危険度　高：発見次第、即座に関係者全員に連絡する。
　　中：関係者全員に連絡する。
　　低：システム担当者に連絡する。

2）情報システム担当部署から通知を受けた者は、速やかにその指示に従う。ソフトウェアアップデートが必要な場合は「１５．システム維持に関する標準」、ウイルス定義ファイルを更新する場合は「１４．ウイルス対策標準」に基づいて行う。

１７．ネットワーク構築標準

（1）目的

この項は、当会管下施設のネットワーク構築をする際に、インターネット接続環境、施設内ＬＡＮ環境の遵守事項を定め、もって必要なセキュリティを確保することを目的とする。

（2）対象システム

インターネット接続環境、施設内ＬＡＮ環境

（3）共通規定

ネットワーク構築の共通規定を、以下に定める。

1）ネットワーク環境は、以下のとおり。
- ・インターネット接続環境
- ・プライベートアドレスを利用した施設内ＬＡＮ環境

2）ネットワーク構築のための機器を、以下に定める。
- ・ネットワーク機器（ルータ、スイッチングハブ、ハブ、ＶＰＮ装置等）

3）パスワードの設定が可能な機器は、「２２．ユーザ認証標準」に準拠し、パスワードを設定する。

4）アクセス制御の設定が可能な機器は、特定機器からの接続のみが可能な設定をする。

5）各機器は、設置場所・接続機器状況・管理者を明確にする。

6）セキュリティ対策上、利用できるサービスは必要最小限とする。

（4）インターネット接続環境

インターネット接続環境を、以下に定める。

インターネット接続環境は、ルータによるプロバイダ接続とする。

（5）施設内ＬＡＮ環境

施設のＬＡＮ環境を、以下に定める。

施設内ＬＡＮの構成は、スイッチングハブ等を使用した施設内のネットワークとする。

（6）ネットワーク管理

情報システム担当部署でなく、部署独自で管理するネットワーク機器を設置する場合の手順を、以下に定める。

1）設置許可申請

部署独自に設置しようとする場合は、別に定める「設置許可申請書」を、情報システム担当部署に提出する。

2）機器管理者の決定

独自に設置しようとする部署は、機器管理者を選出し、情報システム担当部署に文書で報告する。

3）機器の設置

設置するネットワーク機器は、委員会が指示するセキュリティ対策を講じる。

4）審査・設置許可

①　システム担当者は、設置申請のあったネットワーク機器について、委員会が指示す

るセキュリティ対策に関し審査する。
② 内部審査に合格しない機器は、ネットワークへの接続を認めない。
③ 設置したネットワーク機器は、許可されたネットワーク以外には接続しない。

5）監視

設置した機器は、委員会の指定した外部機関または情報システム担当部署が、ネットワーク機器の稼動状況を監視する。

6）監査の継続と切り離し

① 設置した機器は、設置後も定期・不定期的に監査する。
② 監査で発見された問題点の程度によっては、委員会の判断により、問題点の処置が完了するまでネットワークから切り離す。

１８．ＬＡＮにおけるＰＣ設置/変更/撤去の標準

（1）目的

この項は、当会管下施設ＬＡＮ環境のＰＣ接続に関する事項を定め、もって発生し得る各種の問題を未然に防ぎ、情報資産を保護することを目的とする。

（2）対象システム

施設の各フロア、関連施設等の管轄拠点に展開されるＬＡＮに接続されたすべてのシステムを対象とする。

（3）機材の設置

1）ＬＡＮに接続するＰＣは、「２７．ソフトウェア／ハードウェアの購入および導入標準」に基づいて導入されたものに限る。
○ あらかじめ委員会の許可を得た場合に限り、個人所有の情報機器の利用およびＬＡＮ接続ができる。
○ 個人所有情報機器内に個人情報が記録されている場合、施設外への持ち出しを原則禁止する。

2）ＬＡＮに接続するＰＣは、「２３．クライアント等におけるセキュリティ対策標準」に基づくセキュリティ対策を講じる。

3）職員等は、ＬＡＮ に接続するＰＣの設置、変更および期間満了前の撤去に際し、情報システム担当部署に以下の情報を申請し、承認を受ける。
・利用者情報（氏名、所属、連絡先等）
・利用目的
・利用形態（設置希望箇所、利用時間帯、利用サービス、予定期間）
・利用機器情報（管理者、連絡先、ＭＡＣアドレス等ハードウェア情報）

4）情報システム担当部署は、前項の職員等の申請を受理したときは、利用目的、利用形態を審査し、結果を申請者に連絡する。

5）情報システム担当部署は、利用申請に許諾を与える場合に、一定規則に則ってＰＣ名称（ホスト名）、ＩＰアドレスを付与する。必要に応じ、アクセス権等を設定する。

6）情報システム担当部署は、利用申請に許諾を与える場合は、接続するハブ・情報コンセント・利用ケーブル番号など、接続箇所を決定する。

7）情報システム担当部署は、以下の情報一覧（必要に応じて図を利用）を保管する。
・ＩＰアドレス利用一覧
・ＰＣ名称、ＤＮＳ登録一覧
・接続箇所利用一覧
・職員情報（氏名、所属、連絡先等）
・利用目的
・利用形態（設置箇所、利用時間帯、利用サービス、予定期間）
・利用機器情報（管理者、連絡先、ＭＡＣアドレス等ハードウェア情報、ＰＣ名称、

ＩＰアドレス、アドレス取得形態（固定ＩＰ/ＤＨＣＰ）、接続箇所情報、ＤＮＳ登録の有無、ディレクトリ登録情報）

8）情報システム担当部署は、利用申請に許諾を与える場合は、申請者に以下の情報を通知する。

・許諾された利用目的
・許諾された利用形態（設置箇所、利用時間帯、利用サービス、予定期間）
・利用機器情報（ＰＣ名称、ＩＰアドレス、アドレス取得形態（固定ＩＰ/ＤＨＣＰ）、接続箇所情報、ＤＮＳ登録の有無、ディレクトリ登録情報）

（4）ＬＡＮ接続における留意点

1）情報システム担当部署が設置した以外のネットワーク機器を導入する等の、ネットワーク形態の変更は認めない。

2）情報システム担当部署の許可が無い、使用機材の機能変更、また、許可された目的外のＬＡＮ利用は認めない。

3）情報システム担当部署は、必要に応じ、職員等のＬＡＮ接続を制限（アクセスの制御、切断など）できる。

○　緊急時には、情報システム担当部署は、職員等に指示を与える前に、ＬＡＮ接続を制限できる。

4）情報システム担当部署は、職員等の接続形態にあわせ、適切な認証機能・暗号化機能等を提供し、情報の保護に努める。

○　無線ＬＡＮを利用する場合には、認証および暗号化機能を利用する。
○　ＬＡＮ に接続する機器の通信は、「２４．施設内ネットワーク利用標準」に照らして適切な通信のみに限定する。

（5）ＬＡＮ接続情報の更新、通知手続き

1）情報システム担当部署は、職員等に許可したＬＡＮ接続形態を、許諾後２週間以内に、申請内容と照合して確認する。

○　また、半年に１度、部門ごとのＬＡＮ接続状態を確認する。

2）情報システム担当部署は、職員等に許可したＬＡＮ接続について、申請・変更時に予定した期間が満了する２週間前に、利用者に期間満了を通知する。

3）ＰＣの追加、変更、削除に際しては、周辺業務への影響を調査し、業務に支障が無いように対応する。

１９．媒体の取扱に関する標準

（1）目的

この項は、ＰＣ等の修理時および媒体の処分時に関するルールを定め、もって機密性の高い情報の漏洩を未然に防ぐことを目的とする。

（2）対象システム

当会管下施設の業務で使用するすべてのＰＣ等および媒体を対象とする。

○　媒体とは、フロッピーディスク、ＭＯ、ＣＤ、ＤＶＤ、磁気テープ、ハードディスク、ＵＳＢメモリ等、取り外しが可能で情報が保存できるものをいう。

（3）ＰＣ（ＩＴ製品）の修理

1）ＰＣ等の修理は、機密性の高い情報が保管されていないことを確認した上で依頼する。
故障の状況により、保管情報の確認や保護が実施できない場合は、ハードディスク等の情報が保管されている装置を取り外し、修理を依頼する。

2）「２７．ソフトウェア／ハードウェアの購入および導入標準」に定める標準製品の修理は、情報システム担当部署を通して行う。

○　情報システム担当部署は、標準製品の代替品を準備し、必要に応じて貸し出す。
○　標準外製品の修理は、使用部署が直接修理を依頼する。

3）情報システム担当部署および標準外製品の修理を依頼した職員等は、外部業者が施設内に立ち入って修理を行う場合は、「１２．物理的対策標準」に基づいて対応する。

（4）媒体の保管

1）機密性の高い情報を保存した媒体は、鍵のかかる場所に保管し、鍵は容易に持ち出せない場所に保管する。

2）高度なセキュリティが必要なデータは、暗号化して保管する。

（5）媒体の移動

媒体の移動は、「２６．情報および情報機器の持ち出しに関する標準」に基づいて行う。

（6）媒体の再使用

機密性の高い情報が保存されている媒体を再利用する場合は、保存されていた情報を、再生できない方法で消去する。

（7）ＰＣ（ＩＴ製品）と媒体の廃棄

1）ＰＣ（ＩＴ製品）の廃棄を行うときは、情報システム担当部署に、廃棄申請を提出する。

2）ＰＣ（ＩＴ製品）は、機密性の高い情報が保管されたハードディスク等を取り外した後、指定された場所に廃棄する。

3）取り外したハードディスク等の機密性の高い情報が保管された媒体は、情報システム担当部署が指定する場所に持ち込む。

4）機密性の高い情報が保管されているかどうかが確認できない場合は、機密性の高い情報が保管されているものとして取扱う。

5）情報システム担当部署は、機密性の高い情報が保管されたハードディスク等の媒体を、再生不能な状態に破壊して廃棄する。

6）情報システム担当部署は、機密性の高い情報が保管されたハードディスク等の媒体の処分を外部業者に委託する場合は、委員会の承認を得る。

外部業者に委託する場合は、秘密保持および処分依頼品の再利用禁止に関し、契約文書に盛り込む。

２０．電子メールサービス利用標準

（1）目的

この項は、電子メールで受け渡す情報の取扱いに関する事項を定め、もってこの安全性を確保し、利用に際して発生し得る各種の問題を未然に防ぐことを目的とする。

（2）対象システム

当会管下施設が発行する電子メールアドレスを用いてメールの送受信を行うＰＣ（ＩＴ機器）とする。

（3）電子メールサービス利用端末機器のセキュリティ

1）電子メールの送受信は、委員会が指定した電子メールソフトウェアを用いる。

○　また、委員会の指示に従い、当該ソフトウェアのバージョンアップを行う。

2）前項のソフトウェアを使用するコンピュータは、「２７．ソフトウェア/ハードウェアの購入および導入標準」に基づいて導入し、「２３．クライアント等におけるセキュリティ対策標準」に基づくセキュリティ対策を講じる。

3）電子メールアドレスは、初期パスワードとともに発行する。

○　初期パスワードは直ちに変更し、その後、最低３ヵ月に１度、定期的に変更する。
○　パスワードの設定は、「２２．ユーザ認証標準」に基づいて行う。

4）電子メールソフトウェアの起動は、ユーザ認証が必要な設定とし、パスワード等の自動入力は認めない。

（4）電子メールで送受信される情報の保護

1）施設の事業に関する情報、利用者、職員等のプライバシーに関する情報等の機密情報は、原則として、電子メールでは送信しない。

2）業務上やむを得ず機密情報を送受信する場合は、委員会の指示に従い、内容に応じて暗号化、電子署名等の保護手段を講じる。

3）電子メールを送信する際は、送信先のメールアドレスを確認の上、送信する。
○　特に初めての相手先の場合はメール送受信のテストを行う。

4）施設の行事案内等、施設外の複数のドメインが混在するメールアドレスに、１通の電子メールで同報送信する場合は、送信先メールアドレスが受信者間で閲覧できないように設定する。
○　施設の広告となりうるメール等を送信する際は、法令を遵守する。

5）電子メールを施設外の個人的なメールアドレスに自動転送する場合は、委員会の許可を要する。

（5）電子メールサービスとネットワーク保護

1）業務目的以外に、電子メールサービスは利用しない。

2）スパムメールを受信した場合は、これを転送しない。

3）施設が発行したメールアドレスを利用して外部のメーリングリストに参加する場合は、当該メーリングリストの信頼性および業務への必要性を充分考慮する。
○　参加意義が無くなった場合は、直ちに脱退する。
○　メーリングリストでの発言は、「（4）電子メールで送受信される情報の保護」を遵守するとともに、公序良俗に反する発言はしない。

4）送信可能なメールの最大サイズは、委員会が定める。
○　規定サイズ以上のメールを送信せざるを得ない場合は、分割して送信する。

5）その他、無用な電子メールの送受信は、ネットワークに負荷をかけるので認めない。
○　送信する電子メールは、原則として、HTML ではなくプレーンテキストとする。

（6）電子メールを介したウイルス被害の防止

メール送受信の際は、「１４．ウイルス対策標準」に基づき、メールのウイルスチェック等のウイルス対策を行う。

（7）電子メールの監視許可

電子メールの利用状況は、システム担当者の協力のもと、委員会が監視する。

２１．アカウント管理標準

（1）目的

この項は、アカウントを、必要最小限の権限を与えるユーザにのみ発行して管理する事項を定め、もって組織変更や異動などにも支障をおこさないよう、セキュリティ確保と業務対応の両立を図ることを目的とする。

（2）アカウントの管理

1）アカウントとは、ネットワークやシステムに接続（ログイン）する際の権利をいう。具体的には、ユーザＩＤを指す。

2）アカウントの管理は、新しいアカウントの初期登録から、情報システムおよびサービ

スへのアクセスを必要としなくなった最終的な登録削除まで、すべての段階を対象とする。
3）システムの利用者との対応付けができ、また、利用者に自分の行動に責任を負わせるため、一人の利用者に対して、一意のアカウントを付与する。
4）一つのアカウントの複数人使用は原則として認めない。
ただし、委員会の許可を得た場合に限り認めることができる。
5）メール送受信、ファイル共有、インターネットアクセス等の基本的なアクセス権限は、別に標準的なアクセス権限表を作る。

（3）新規アカウントの発行
1）各部署の長は、新規のアカウントが必要になった場合には、必要最低限のアクセス権限の範囲と共に人事責任者に申請する。
2）前項の申請を受理した人事責任者は、アカウントの必要性とそのアクセス権限の範囲を検討した上で、システム担当者に新規アカウントの発行を申請する。
3）前項の申請を受理したシステム担当者は、システムの実務管理者にアクセス権限等の妥当性を確認した上、アカウントを発行する。
4）アカウントに対応するパスワードは、「２２．ユーザ認証標準」に基づき、慎重に設定する。

（4）アカウントの変更および削除
1）アカウントに付与した権限を変更する場合は、新規アカウントの発行と同様に人事責任者を通してシステム担当者に申請する。
2）人事責任者およびシステム担当者は、情報システム利用者の役職または職務領域に変更があった場合は、対応するアカウントのアクセス権限を直ちに変更するために必要な手続きを行う。
3）職員等が異動、退職、休職などでアカウントが不要になった場合は、直ちにアカウントを削除・停止する。
4）変更および取消の管理は、抜けや処理忘れを防ぐため定期的に検査し、不整合があればアカウントを削除する。
5）未認可のアクセスを試みたり、アカウントの不正使用が検知された場合は、当該アカウントのアクセス権限を直ちに停止する。

２２．ユーザ認証標準

（1）目的
この項は、情報を守る為に使用されるユーザ認証に関する事項を定め、もってセキュリティを確保しつつ利便性を実現することを目的とする。

（2）対象システム
以下のいずれかの条件を満たす機器、システムおよびアプリケーションは、ユーザ認証を用いて情報セキュリティを確保する。
1）汎用的に使われているＯＳなどでネットワーク機能を持つ機器
2）ハードディスクなどの記憶媒体を持つ機器
3）ルータ
4）ユーザが用いるメールソフトウェア

（3）ユーザ認証を用いたセキュリティ確保
1）情報システムへのアクセスを正当な利用者のみに限定するため、情報システムは、利用者の識別と認証を行う機能を持たせる。
2）情報システムへのアクセスを行うすべての者に対しＩＤ・パスワード、IC カード、電

子証明書、生体認証等、本人の識別・認証に用いられる手段を用意し、統一的に管理する。

（4）対象システムによる認証システムの選定
システム担当者は、対象システムの重要性と、セキュリティを実現する手法の難易度を勘案し、ユーザ認証システムを構築する。

（5）パスワード
1）原則として、英数字を混在させた６文字以上の設定とする。
2）パスワードは、職員番号等の規則性があり予測できるもの、一般に使われている単語、本人の趣味、プライベートなどから、他人に推測されやすいものは認めない。
3）設定したパスワードは、少なくとも、３ヵ月に１度は、定期的に変更する。
4）システム担当者であっても、利用者のパスワードは知り得ないようにする。
5）パスワードは、紙等に記録して保管しない。ただし、セキュリティを確保して保管される場合は、その限りではない。
6）パスワードは、口外しない。
○　ヒントとなるような物品を身の回りに置かない。
7）１度使用したパスワードは、連続でなくとも、再使用しない。
8）１度使用したパスワードは、他のシステムなどに使用しない。

（6）初期設定のパスワード
1）利用者が最初に使用する初期設定のパスワードは、システム担当者が発行し、口頭もしくは書面で該当者に通知する。
2）利用者は、パスワードが発行されたときは速やかに自らログインし、パスワードを変更する。
3）システム担当者は、初期設定のパスワードを受理した利用者が、パスワードを変更したことを確認する。

（7）パスワードを忘れた場合の処置
1）利用者がパスワードを忘れた場合は、利用者の申し出により、システム担当者が新規パスワードを再発行する。
2）システム担当者が、新規パスワードを再発行する際には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載する。
3）新規パスワード再発行の申請を受理したシステム担当者は、速やかに新規パスワードを発行し、利用者に通知する。
○　利用者は、再発行のパスワードで速やかに自らログインし、パスワードを変更する。

（8）パスワード管理技術の進歩
パスワードの長さ、文字の種別、更新頻度、対象機器等は、実現方法に関する技術の進歩が著しいので、技術動向を見極めた上、この対策標準を適宜更新する。

２３．ＰＣ等のセキュリティ対策標準

（1）目的
この項は、ＰＣ上の情報セキュリティの確保に必要な事項を定め、もって発生し得る各種問題を未然に防ぐことを目的とする。

（2）対象システム
当会管下施設から支給または貸与されたＰＣ

（3）個人所有ＰＣの使用禁止
1）施設の業務処理に職員等が使用できるＰＣは、施設が支給または貸与したＰＣのみとする。
2）あらかじめ委員会の許可を得た場合に限り、個人所有の情報機器の利用およびＬＡＮ接続ができる。

（4）ＰＣに導入するソフトウェア
1）施設が支給または貸与するＰＣは、「２７．ソフトウェア／ハードウェアの購入および導入標準」に定めるソフトウェアを導入する。
○　それ以外のソフトウェアは、導入を認めない。
2）業務上やむを得ない場合は、情報システム担当部署の許可を得て、前項の指定ソフトウェア以外を導入できる。
3）導入したソフトウェアは、セキュリティに留意し、情報システム担当部署が提供するソフトウェア情報をもとに修正プログラム等を適用する。

（5）ＰＣの他者への利用制限
1）席を離れる場合には、第三者が無断でＰＣを利用できないように施錠、パスワードまたはその他の方法で保護する。
2）「２２．ユーザ認証標準」および「２６．情報および情報機器の持ち出しに関する標準」に基づき、ＰＣのパスワード管理を徹底する。

（6）ＰＣでの情報の取扱い
1）ＰＣで機密情報を取扱う場合、長期間その情報を利用する場合には、情報システム担当部署に機密情報を取扱う許可を申請し、許可を得る。
○　許可を得た機密情報は、万一の漏えいに備え、暗号化等の対策を講じる。
2）ＰＣで一時的に機密情報を取扱う場合は、取扱い後は、不必要となった情報を速やかに削除する。

（7）ウイルス対策の徹底
ＰＣを利用するすべての職員等は、「１４．ウイルス対策標準」に基づくウイルス対策を徹底する。

（8）ＰＣの移設
1）ＰＣは、システム担当者の許可がない移設は認めない。
2）ＰＣの移設が必要な場合は、システム担当者の許可を得て行う。

２４．施設内ネットワーク利用標準

（1）目的
この項は、当会管下施設内ネットワークの利用および管理に必要な事項を定め、もってネットワークの機密保持、情報資産の保護、有効活用を目的とする。

（2）対象システム
施設内ネットワークに接続し、施設内ネットワーク、インターネットへの通信を行うコンピュータおよびシステムを対象とする。

（3）施設内ネットワークおよびインターネットの業務目的以外の利用禁止
1）施設内ネットワークは施設の情報資産であり、電子メールやＷＥＢサイトの利用などは、業務目的以外の使用を禁止する。
○　インターネット利用に関しても、業務目的外使用を禁止する。

2）委員会の許可無く、施設内ネットワーク上に、電子メールサーバ、ＷＥＢサーバ、FTPサーバなどの構築は認めない。
3）他人の利用者ＩＤを用いて、施設内ネットワーク、施設外のネットワーク、インターネット上のサイトへのアクセスは認めない。
4）故意もしくは不注意を問わず、施設内外のネットワークに、許可されたアクセス権限を超えるアクセスはしない。

（4）ネットワークを利用した機密情報の送受信
1）「8．情報資産の保護」の「（3）情報資産の評価」の「1」機密性」に定める「公開」以外の情報は、施設外へ送信しない。
2）出所が不明なファイル、内容に確証の持てないファイルは、ダウンロードあるいは実行しない。
3）業務上やむを得ず機密情報を施設外へ送受信する場合は、委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を講じる。

（5）インターネットで利用可能なサービス
1）インターネットの利用は、委員会が定めるサービス以外は利用しない。
2）暗号通信を用いたインターネットへのアクセスは、委員会が認めたサイトのみ許可する。
3）ＷＥＢサービスを利用する際は、「２５．ＷＥＢサービス利用標準」を遵守する。
4）施設内ネットワークに接続したＰＣは、委員会が定めた電子メールサービス以外は利用しない。
○　やむを得ず、施設外の電子メールサービスを利用するときは、委員会の承認を得て行う。
5）システム担当者は、インターネットで利用可能なサービスを制限するため、技術的な対策を講じる。

（6）施設内ネットワークで利用可能なサービス
1）ネットワーク利用者は、施設内ネットワークで、ネットワークモニターなどのネットワーク上を流れるパケットを盗聴できる機器およびソフトウェアを使用できない。
2）ネットワーク利用者は、施設内ネットワークへのアクセス用のＩＤ、パスワード、証明書を適切に管理する。
○　特に、パスワードの選択および使用は、「２２．ユーザ認証標準」に基づき厳重に行う。

（7）施設内ネットワークへの接続時の注意事項
1）自宅や他組織のネットワークへ接続したＰＣは、ウイルス検査とセキュリティ検査を実施し、異常が発見されなかったことを各部署のセキュリティ担当者が確認した後でなければ、施設内ネットワークへの接続を認めない。
2）ネットワーク利用者は、与えられたＩＰアドレス以外のＩＰアドレスは使用できない。
3）ネットワーク利用者は、施設内ネットワークに接続中のコンピュータを、委員会が定めた通信手段以外を使用して、施設外のネットワークへ接続できない。

２５．ＷＥＢサービス利用標準

（1）目的
この項は、ＷＥＢブラウザを使用し、施設内外のサイトを利用する際の注意事項を定め、もって利用により発生し得る各種の問題を未然に防ぐことを目的とする。

（2）対象システム

施設内ネットワークに接続してＷＥＢブラウザを使用し、施設内外のＷＥＢサイトにアクセスするコンピュータ。

（３）ＷＥＢ ブラウザ利用端末機器のセキュリティ

１）職員等は、ＷＥＢサービスの利用に際しては、委員会が指定したＷＥＢブラウザを用いる。

○　システム担当者は、委員会の指示に従い、当該ソフトウェアのバージョンアップおよびソフトウェアアップデートを実施する。

２）職員等は、ＷＥＢブラウザの利用に際しては、委員会が指定した設定により行う。

３）使用するコンピュータは、「２７．ソフトウェア/ハードウェアの購入および導入」に基づいて導入し、「２３．クライアント等のセキュリティ対策標準」に基づくセキュリティ対策を講じる。

（４）ＷＥＢブラウザの利用

１）職員等は、施設内およびインターネット上のＷＥＢサーバへのアクセスは、業務上必要な場合のみ利用できる。

２）職員等は、リンクをクリックするときは、リンク先のＵＲＬを確認してからクリックする。この場合、リンク先が、信頼できないＵＲＬの場合は、クリックを認めない。

○　バナー広告に関しても、業務上必要のないバナー広告のクリックは認めない。

３）職員等は、業務上不必要なファイル、ソフトウェア、不審なファイルなどをダウンロードしない。

○　必要なファイルやソフトウェアも、ＷＥＢサイト上では実行せず、ダウンロードし、ウイルスチェックを実施した後で表示、実行する。

４）職員等は、署名の無いあるいは信頼できないサイトでの実行指示（ActiveX などのコードによる）は行わない。

５）職員等は、独自に暗号化ソフトウェアをインストールしてはならない。

○　業務上、暗号通信が必要となった場合は、所属部署の長から理由目的等を明記して委員会に申請し、承認を得た場合に情報システム担当部署に依頼して行う。

６）職員等は、通信事業者が無料で提供しているＷＥＢメールシステム等を用いた電子メールは原則として使用しない。

７）職員等は、施設内外のＷＥＢサーバに対し、攻撃等の不正なアクセスを行わない。

○　攻撃等の不正なアクセスを目的とした施設内外のシステム利用は認めない。

（５）アクセス制御されたＷＥＢサイトの閲覧

１）職員等は、パスワードによってアクセス制御されたＷＥＢサイトを閲覧する際は、パスワードをＷＥＢブラウザに記憶させる等の行為を行わない。

２）アクセス制御されたＷＥＢサイトの閲覧時に離席する際には、ＷＥＢブラウザを終了させるか、ＯＳのパスワード付スクリーンロックを実施する。

３）パスワードによってアクセス制御されたＷＥＢサイトを閲覧するときは、他人のユーザＩＤやパスワードなどを利用しない。

２６．情報および情報機器の持ち出しに関する標準

（１）目的

この項は、情報資産の施設外持ち出しに関する事項を定め、もって情報の漏えいを防ぐことを目的とする。

（２）情報資産

この項で扱う情報資産は、次のものとする。

①　情報機器

・情報端末（パソコン、ノートパソコン、ＰＤＡ、携帯電話等）
・情報記録媒体（ＵＳＢメモリ、光ディスク、その他の磁気記録装置等）
② 情報（サービス記録、ログ、ソフトウェア等）

（３）管理策
１）「８．情報資産の保護」に基づき、情報資産の把握を行い、複写して施設外に持ち出すことのできる情報およびその情報を記録する媒体を特定する。
２）情報資産の施設外持ち出しは、許可制とする。システム担当者は、記録台帳を作成し、実施者、持ち出す情報資産、目的、期間等を台帳に記載し、管理する。
３）施設管轄外の情報機器（個人所有のＵＳＢメモリ等）を用いて情報を持ち出す場合は、システム担当者の許可を要する。システム担当者は、この項で定める保護策が遵守されることを確認し、記録台帳に許可内容を記録する。
４）持ち出した情報を、施設管轄外の情報機器（個人所有のパソコン等）で取扱う場合は、システム担当者の許可を要する。システム担当者は、この項で定める保護策が遵守されることを確認し、記録台帳に許可内容を記録する。

（４）保護策
１）盗難、置き忘れ等の対策として、情報を暗号化する、アクセスパスワードを設定する等を必ず実施し、容易に内容を読み取れない措置をする。
２）情報端末には、起動パスワードを設定する。パスワードの設定は、「２２．ユーザ認証標準」に基づき、推定しやすいパスワードの利用を避け、定期的にパスワードを変更する等を徹底する。
３）情報端末は、ウイルス対策ソフトウェアの導入、パーソナルファイアウォールの導入等をし、情報漏えい、改ざん等の対象にならない対策を講じる。ウイルス対策は、「１４．ウイルス対策標準」を遵守する。
４）情報端末に、システム担当者の許可がないアプリケーションのインストールは認めない。個人所有の情報機器を業務に使用する場合は、ファイル交換ソフトウェア（Ｗｉｎｎｙ等）のインストールを禁止する。
５）外部の人の目に触れる場所で、持ち出した情報を閲覧しない。業務の都合で閲覧せざるをえない場合は、ディスプレイに覗き見防止フィルタを張る。
６）施設外に情報機器を持ち出す場合は、盗難・遺失・毀損に注意する。車両、ホテルの部屋、集会所等では、情報機器を無人の状態で放置せず、引出しに入れて施錠する等を厳守する。
７）情報機器の利用者は、情報機器を盗難された、または遺失、毀損した場合は、速やかにシステム担当者にその旨を連絡する。システム担当者は、失った情報資産のリスクに応じた対応を利用者に指示するとともに、委員会に状況と対応を報告する。
８）情報資産の施設外持ち出しを許可する場合は、「１０.セキュリティ教育に関する標準」に基づき、持ち出しに関する情報セキュリティ対策を教育する。

２７．ソフトウェア／ハードウェアの購入および導入標準

（１）目的
この項は、当会管下施設の業務で使用するソフトウェア／ハードウェアの標準製品・仕様を定めて運用管理することにより、もって統一されたセキュリティ対策の実現を容易にし、管理の効率化を図り、導入時の設定ミス等を防止することを目的とする。

（２）標準製品リストの作成
１）委員会は、施設の一般的な業務で使用する以下の標準製品を定める。

① ハードウェア
デスクトップＰＣ、ノートＰＣ、ルータ、スイッチングハブ等
② ソフトウェア
ＯＳ、文書作成、表計算、プレゼンテーション支援、ウィルス対策、電子メール、ＷＥＢブラウザ、暗号化、圧縮・解凍ソフトウェア等を含むすべての業務で使用するアプリケーション

2）業務上の正当な理由があり、委員会から標準外製品の購入／導入を承認された場合を除き、標準製品を購入／導入する。

3）委員会は、標準製品を決定する際は、以下の点を考慮する。
① 必要なセキュリティ機能、スペックを備え、サポート、ライセンス条件、価格、などの条件を考慮し、既存の情報システムと問題なく動作できるものを選択する。
② 製品のセキュリティホール情報やその他の不具合に関する情報の提供、ソフトウェアアップデート等の対応が悪い製品は、標準製品に指定しない。

（3）標準製品の購入／導入

1）情報システム担当部署は、標準製品の発注、保守契約、ライセンス、インストールメディア等を、一括管理する。

2）標準製品の購入を予定する部署は、情報システム担当部署に、購入申請書を提出する。

3）情報システム担当部署は、前項の申請を受けて標準製品を発注し、必須導入ソフトウェアのインストールと設定、ネットワーク接続の設定、各種ソフトウェアのソフトウェアアップデートを行った上、申請者指定の場所に納品する。
○ 製品購入時に既にインストールされているもの、ＯＳに付属するソフトウェアでも、標準製品として未認可のものは、排除した後に納品する。

4）情報システム担当部署は、購入し、納品した製品を「管理台帳」に登録する。

5）情報システム担当部署は、各部署の申請に基づき、再インストール等のためにライセンス上問題のないインストールメディアを貸し出す。
○ 情報システム担当部署は、貸し出し記録を作成し、管理する。

（4）標準外製品の購入／導入

1）研究、開発、その他業務上の理由で、標準外製品を購入／導入する必要がある部署は、委員会に、標準外製品を使用する理由、製品名、製品の種類、管理者等の必要事項を明記して申請する。

2）前項の申請を受理した委員会は、受理日の属する月またはその翌月に、申請の妥当性を審査し、その結果を申請者に通知する。

3）委員会の承認を得て標準外製品を使用した部署が、標準外製品の使用を停止したときは、委員会にその旨を遅滞無く報告する。

4）委員会は、使用を許可した標準外製品をシステム担当者に通知し、システム担当者は、標準外製品を管理台帳に登録する。

5）委員会は、標準外のネットワークソフトウェアの使用を許可した場合は、システム担当者に、その旨を通知する。使用停止の報告があった場合も、通知する。

6）委員会は、標準外のネットワークソフトウェアを施設内ネットワークに接続を認めない場合で、業務上必須と認められる場合は、情報システム担当部署に、施設内ネットワークから切り離した独立環境を構築して業務上の要求に応えるよう指示する。
○ 情報システム担当部署は、施設内ネットワークから切り離した環境で使用していることを、３ヵ月を超えない期間ごとに、使用部署には通知せずに確認する。
○ 独立環境を使用している部署は、その環境が不要になった場合は、速やかに委員会および情報システム担当部署に報告する。

7）標準外製品の購入／導入を行う部署は、自部署の責任において購入／導入するとともに、ライセンス、インストールメディアの管理を厳密に行う。

8）標準外製品の購入／導入を行う部署は、事前に、既存の情報システムへの影響を検討

し、セキュリティ上の安全性を確認し、情報システム担当部署のチェックを受けた後に使用する。

9）委員会は、標準外製品の接続を原因として既存システムのセキュリティ上、その他のトラブルが発生した場合は、標準外製品の購入／導入を行った部署に対し、当該製品の設定変更、施設内ネットワークからの切り離し、当該製品の使用停止等を命じる。

（5）ネットワーク機器の購入／導入

1）施設の主要なネットワーク機器の購入／導入は、情報システム担当部署が行う。ただし、各部署で購入する場合は、標準製品の使用を原則とする。

○　各部署が購入した製品は、管理台帳に登録するため、情報システム担当部署に登録申請する。

○　購入した製品は、各部署が管理する。

2）情報システム担当部署は、「１７．ネットワーク構築標準」に基づき、主要なネットワーク機器を導入する。

（6）管理台帳の作成／管理

1）情報システム担当部署は、申請された情報を元に、ＰＣ、ネットワーク機器の管理台帳を作成し、新規登録、変更、削除等を管理する。

2）管理台帳には、標準製品、標準外製品の両者を登録する。

２８．セキュリティインシデント報告・対応標準

（1）目的

この項は、セキュリティインシデントが発生した場合に必要な事項を定め、もって迅速な対応と情報システム環境の復旧が円滑に行われることを目的とする。

（2）報告事例

情報セキュリティの事象およびインシデントは、以下のものとする。

1）サービス、装置または施設の停止
2）システムの誤動作または過負荷
3）人による誤り
4）個別方針または指針の非順守
5）物理的セキュリティの取決めに対する違反
6）管理されていないシステム変更
7）ソフトウェアまたはハードウェアの誤動作
8）アクセス違反

（3）平時の準備

1）委員会は、「１０．セキュリティ教育に関する標準」に基づき、セキュリティ教育を実施し、職員のセキュリティ意識の向上に努める。

2）利用するすべてのコンピュータは、「１４．ウイルス対策標準」に基づき、適切なウイルス対策を講じる。

3）情報システム担当部署は、「１６．セキュリティ情報収集および配信標準」に基づき、施設で使用している製品のセキュリティ情報を収集し、必要なセキュリティ対策を実施してセキュリティレベルの維持に努める。

4）情報システム担当部署は、インシデント発生後のシステムの復旧作業に役立てるため、適切にバックアップを実行する。

○　バックアップ後のメディアは、サーバ設置場所と違う場所に保管する。

5）情報システム担当部署は、インシデント発生後のシステムの復旧作業に必要なリソースを検討し、確保しておく。

6）委員会は、各システムの復旧優先度を、あらかじめ定める。

○　復旧優先度の決定は、対象システムにて運用される業務の停止許容時間を観点に行う（表１参照)。

表１　システムの復旧優先度

復旧優先度	業務復旧までの許容時間
3	業務が停止することは許されない
2	24 時間以内に復旧しなければならない
1	3 日以内に復旧しなければならない
0	インシデント発生時は停止してもよい

（4）セキュリティインシデント発生時

1）職員等は、インシデントの発生と疑われる事象を発見した場合は、速やかに委員会またはシステム担当者に報告する。

○　クライアントＰＣにウイルス感染や不正アクセスの疑いがある場合は、発見後ただちに該当するクライアントＰＣをネットワークから切り離した上で報告する。

2）前項の報告を受理した委員会またはシステム担当者は、以下の観点で状況把握し、対応方法を報告者に指示する。

○　システム担当者が報告を受けた場合は、対応方法を報告者に指示するとともに、その内容を速やかに委員会に報告する。

○　システム担当者では作業が困難である場合は、速やかに委員会に申し出て、協力を依頼する。

＜観点＞

・インシデント発生の真偽
・被害を発見した日時
・被害の拡大範囲
・被害内容
・被害原因
・対応方法

3）インシデントの発生が確認された場合、委員会は、速やかに関連する部署（情報システム担当部署等)、プロバイダー、外部ベンダー等に連絡し、協力を依頼する。

○　委員会は、必要に応じ、組織横断的なタスクフォースを設け、状況把握や対応方法の指示にあたる。

4）情報システム担当部署は、インシデントの原因が解消された後、速やかにバックアップメディアを用いてシステムを正常な状態に復旧する。

○　復旧作業に際しては、（2）の2）に定める復旧優先度に基づいて作業する。

5）職員等は、インシデントの２次被害防止のため、ＯＳ、アプリケーションの入れ替えやクライアントＰＣの設定変更等の作業が必要になった場合は、委員会の指示に従い、速やかに実施する。

（5）再発防止計画

1）セキュリティインシデントの対応が完了した後、委員会およびシステム担当者は、調査結果をもとに再発防止計画を作成する。

○　再発防止計画を作成するときは、技術的側面と組織的側面の両方に留意する。

2）委員会は、発生したインシデントのうち、以下の要件を満たすものは、速やかに施設長に報告する。

＜要件＞

・施設外の第三者からのセキュリティ侵害により施設が被害者となる場合
・利用者等の施設外に対して施設が加害者となる場合

3）再発防止計画は、すべての職員等に周知し、適切に実施する。

4）委員会は、セキュリティインシデントの発生から再発防止計画作成までの一連の記録

を保存・管理する。

２９．外部と個人情報を含む情報を交換する場合の安全管理に関する標準

（１）目的

この項は、情報をネットワークを利用して外部と交換する場合、特に留意すべき項目について定め、もって確実に情報を送り届けることを目的とする。

（２）認証手段の利用

１）データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認を行う。

２）採用する通信方式や運用管理規程により、採用する認証手段を決める。

３）その他認証については、「２２．ユーザ認証標準」に基づいて行う。

（３）施設内のセキュリティ対策

１）施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとる。

２）ルータなどのネットワーク機器は、安全性が確認できる機器を利用する。安全性が確認できる機器とは、例えばIS015408に適合したもの等である。

３）その他施設内のセキュリティ対策については、「２３．アカウント管理標準」および「１８．ＬＡＮにおけるＰＣ設置／変更／撤去の標準」に基づいて行う。

（４）送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施する。

（５）責任の所在の明確化

１）施設等の間の情報通信には、施設等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社など多くの組織が関連するため、次の事項について、関連組織の責任分界点、責任の所在を契約書等で明確にする。

① サービス情報等を含む情報を、送信先の施設等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定
② 送信元の施設等がネットワークに接続できない場合の対処
③ 送信先の施設等がネットワークに接続できなかった場合の対処
④ ネットワークの経路途中が不通または著しい遅延の場合の対処
⑤ 送信先の施設等が受け取った保存情報を正しく受信できなかった場合の対処
⑥ 伝送情報の暗号化に不具合があった場合の対処
⑦ 送信元の施設等と送信先の施設等の認証に不具合があった場合の対処
⑧ 障害が起こった場合に障害部位を切り分ける責任
⑨ 送信元の施設等または送信先の施設等が情報交換を中止する場合の対処

２）施設内においても次の事項において運用管理規程等で定めておく。

① 通信機器、暗号化装置、認証装置等の管理責任の明確化。
外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。
② 利用者等に対する説明責任の明確化。
③ 事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。
④ 交換した情報等に対する管理責任および事後責任の明確化。
個人情報の取扱いに関して利用者から照会等があった場合の送信元、送信先双方の施設等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

（６）回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管

理責任の範囲や回線の可用性等の品質に関して問題がないか確認する。

（7）利用者による情報閲覧の場合
1）情報を公開しているコンピュータシステムを通じて、施設内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信の暗号化、個人認証等の技術を用いた対策を実施する。
2）情報の主体者となる~~患者~~利用者等へ危険性や提供目的の納得できる説明を実施し、ＩＴに係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にする。

３０．プライバシーに関する標準

（1）目的
この項は、サービス記録をはじめとする利用者の個人情報（以下、「個人情報」という。）を収集・維持・破棄する際の注意事項を定め、もって発生しうる問題を未然に防ぐことを目的とする。

（2）対象システム
個人を識別できる情報のすべてと、それを扱うシステムを対象とする。
○　電子化情報は、データ量が多くなる上、目視確認が困難なため、特段に配慮する。

（3）個人情報を取扱う部門の特定
1）委員会は、施設内に、個人情報を取扱う部門を特定し、その部門長に（5）から（9）の遵守事項等を徹底する。
2）前項で特定されない部門では、個人情報を取扱ってはならない。

（4）個人情報管理責任者の選任
個人情報の収集・維持・破棄を行う部門の長は、個人情報管理責任者を選任し、部門内の責任者を明確にする。

（5）個人情報保護方針の公開
1）個人情報管理責任者は、個人情報を広く一般から収集する場合、施設のＷＥＢサイト、広報誌、収集時の広告等に、施設の個人情報保護方針を明記して公開する。
2）個人情報保護方針には、（6）の遵守事項の内容および施設への連絡先を明確に記載する。

（6）個人情報収集時の遵守事項
個人情報を収集し、あるいは、取扱う者は、以下の事項を遵守する。
1）個人情報を取得するときは、あらかじめその利用目的を公表し、または本人に明示し、本人の同意を得る。
2）個人情報を書面で取得するときは、あらかじめ、本人に利用目的を明示する。
3）公表または本人に示した利用目的に使用する情報以外は、収集しない。
4）収集または取得した情報を、本人に明示した目的以外に使用するとき、または、利用目的を変更する場合は、目的外使用の理由または変更した利用目的を本人に明示し、同意を得た後でなければ使用しない。

（7）個人情報の維持
個人情報管理責任者は、以下の事項を遵守する。
1）個人情報の登録・参照・変更・削除を担当する者を明確にし、個人情報へのアクセスを制限する。
2）個人情報を利用する場合は、正確な情報を利用するものとし、そのための保護策を実

施する。
3）個人情報を記録した媒体（バックアップを含む。以下同様）は、個人情報と同様の管理策を設ける。
4）個人情報を登録された本人が、本人の個人情報に関する開示・訂正・削除の要求をした場合は、正当に拒否する理由がない限り要求に応じる。

（8）個人情報の破棄
個人情報管理責任者は、以下の事項を遵守する。
1）個人情報を破棄する場合は、第三者の目にさらされないように注意して破棄する。
2）電子媒体等を破棄する場合は、「１９．媒体の取扱いに関する標準」に基づいて実施する。

（9）本人からのクレーム処理
個人情報管理責任者は、以下の事項を遵守する。
1）施設の業務に関し、利用者本人からクレームを受けた場合は、速やかに対応する。
2）個人情報が漏えいした等、必要がある場合は委員会を開催し、施設の見解を迅速に明確にする。
3）どのようなクレームが発生した場合でも、第一報は１２時間以内に委員会へ報告し、その後の対応状況も適宜連絡する。

３１．監査標準

（1）目的
この項は、監査に関する事項を定め、もって監査の効率を高めるともに、監査の実施が利用者、システム等に悪影響を与えないよう配慮することを目的とする。

（2）共通事項
1）委員会は、監査組織を構成し、定期的に監査を実施する。
○　監査の周期は1年に1回以上とし、委員会が定める。
2）委員会は、監査の対象、目的について、監査組織と協議する。委員会は、監査組織と協議し、決定した内容に関して責任を有する。
3）監査組織は、前項の決定内容に基づいて監査を実施し、その結果を委員会へ報告する。委員会は、監査報告の指摘等を受けて、適切な是正措置を実施する。
4）監査組織は、監査の実施に際し、専門知識や技能を必要とする場合は、委員会の承認を得て、専門家の協力を得ることができる。
○　監査組織は、監査の目的を専門家に説明し、専門家の作業結果に基づいて最終的に判断する。
5）監査組織は、監査の過程で知りえた情報を、監査の目的以外に利用し、または、公開しない。
6）監査を受ける部署とその所属員は、監査の円滑な実施のため、日程調整、資料の提示、監査時の立会い等、監査組織の活動に協力する。

（3）監査計画
1）監査組織は、（2）の2）で決定した監査内容に基づいて、監査の計画を立案する。監査の目的には、次の事項を含める。
・内部統制が、正しく定められているか
・定めた内容に基づいて、効率的に運営されているか
2）監査組織は、監査計画の立案に際し、以下の内容を検討し、計画に反映する。
・内部統制として実施している活動内容
・資産およびそれらへのリスクの分析

・基本方針や対策標準等の規定の分析
・組織を取り巻く環境の変化
・内部統制を理解・徹底するためのヒアリングや観察

3）監査項目には、以下の内容を含める。
・基本方針と対策標準等の整備
・委員会の構成および運営
・情報資産を含む財産の管理
・常勤職員、非常勤職員等の扱い
・物理セキュリティ
・通信および運用
・アクセス制御
・システム開発
・事業継続計画
・法律、規制等への準拠

4）監査組織は、計画した監査項目に問題点が内在する可能性を検討し、予測される内部統制リスクを判断した上で、実施手続きや監査のサンプリング密度を決定する。

5）監査組織は、監査の実施手順および監査項目に関し、文書化して保管する。

（4）監査の実施

1）監査組織は、監査人に監査の実施を文書で指示する。

2）監査人は、あらかじめ定めた手続きに基づき、監査を実施する。

○　監査手続きには、以下を含む。
・インタビュー
・行動の観察
・証拠等の検閲
・監査人による作業手順の実施

3）監査人は、組織内で提供されているサービスの可用性を考慮する。

4）監査人は、システム監査ツールを使用する場合は、システムへの影響に細心の注意を払う。

○　システム監査は、一般へのサービスを停止させない時期を考慮する。やむを得ず停止する場合は、あらかじめ停止の時期と理由を公開する。

5）監査人は、セキュリティに関する方針等と実際のマネジメント活動を比較し、有効性を判断する。

○　判断する観点には、以下を含む。
・組織の事業内容とセキュリティ方針等との整合性
・基本方針と対策標準の整合性
・標準の実行に関し、使用中の設備費用および運用費用等のコストとその妥当性

6）監査人は、監査結果を裏付けるため、監査で得た情報を記録する。

7）監査人は、監査で得た情報を元に、内部統制リスクが予測範囲内であるかを評価し、実施手続きの妥当性を判断する。

8）監査組織は、監査人の報告から、発見した問題の量や質が予測範囲を超え、実施した監査手続きが妥当でないと判断した場合は、再度監査計画を立案して実行する。

（5）監査結果の報告

1）監査組織は、監査結果を元に監査報告書を作成し、委員会へ提出する。

○　監査報告書には、職員の不在、機密情報に関する閲覧の拒絶など、さまざまな理由によって実施できなかった監査項目を、その理由とともに明記する。

2）監査組織は、監査結果の裏付けとなる十分な根拠を提示する。

3）監査組織は、問題点の指摘事項を報告する場合は、その重大性に応じて分類する。

○　その場合、問題点を解決する改善策に関し、可能な限り監査報告書に記載する。

4）監査報告書の開示範囲は、委員会のみとする。

（6）是正措置

1）委員会は、監査組織の報告内容を検討し、必要に応じて是正措置を計画立案し、実行する。

2）前項の是正措置は、緊急性および重要性等を考慮し、適切な時期に行う。

3）是正措置の指示を受けた部署または職員等は、速やかに是正措置を行い、実施した是正内容および時期を委員会に報告する。

３２．電子保存に関する標準

（1）目的

この項は、情報を電子化して保存、管理、流通する場合に必要な事項を定め、もって情報セキュリティを確保することを目的とする。

（2）法令対応

法令により保存義務が定められている文書等に記録された情報を電子媒体に保存する場合は、真正性・見読性・保存性の「電子保存の３基準」を満たして行う。

（3）真正性の確保

真正性とは、正当な人が記録し確認された情報に関し、第三者から見て作成責任の所在が明確であり、かつ、故意または過失による虚偽入力、書き換え、消去および混同が防止されていることをいう。

この場合において、混同とは、利用者を取り違えた記録がされたり、記録された情報間での関連性を誤ることをいう。

1）作成者の識別および認証

① 利用者に、ＩＤ、パスワード等の本人認証・識別に用いる識別情報を発行し、本人しか持ち得ないまたは知り得ないように運用する。

システムは、発行されたＩＤ、パスワード等による本人認証・識別機能を有するものとする。

② システムへのすべての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定める。また、権限のある利用者以外による作成、追記、変更を防止する。

③ 業務アプリケーションが稼動可能な端末を管理し、権限を持たない者のアクセスを防止する。

2）記録手順の確立と作成責任者の識別情報の記録

① サービス記録等の作成・保存を行う場合は、システムは確定された情報が登録できる仕組みとする。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含める。

② 「記録の確定」は、作成責任者が、内容を十分確認できるようにする。

③ 確定された記録が、故意による虚偽入力、書き換え、消去および混同されることを運用も含めて防止でき、それらが検知された場合は、バックアップ等を用いて原状回復できるようする。

④ 外部から入力された情報を「参照」する場合は、その情報は正しく保存された確定記録とする。

参照元の情報が「保存された記録」でない場合は、コピー等の移動手段を経て取り込み操作を行った後に、その情報も含めた「記録の確定」を行う。

3）更新履歴の保存

① 一旦確定したサービス記録等を更新した場合は、更新履歴を保存し、必要に応じて更新前と更新後の内容を照合できるようにする。

② 更新履歴の参照（照らし合せ）は、更新前後の情報が各々物理的に独立して保存されているものの様に更新の順序に沿って参照する方法か、更新時の変更点を明示するような方法（消し込み線を表示する等）で参照できるようにする。
③ 同じサービス記録等に対して更新が複数回行われた場合にも、更新の順序性を識別して参照できるようにする。
④ アクセスログの記録を残し、そのログが改ざんされない対策を講じ、万一、記録情報の改ざん・削除が生じた場合は、その事実を検証できるようにする。

4）機器・ソフトウェアの品質管理
① システムは、どのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにし、システムの仕様を明確に定義する。
② 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを定める。

5）ルールの遵守
① 情報セキュリティ実施手順書が定める内容を遵守するため、職員等の教育とルールの遵守状況を委員会が把握する。
② ルールの改訂や職員等を登用する際は、教育を実施する。

（4）見読性の確保

見読性とは、電子媒体に保存された内容を、権限保有者の要求に基づき、必要に応じて肉眼で見読可能な状態にできることをいう。

「必要に応じて」とは、「サービス」、「利用者への説明」、「監査」、「訴訟」等に際し、それぞれの目的に支障のない応答時間やスループット、操作方法により行うことをいう。

特に、監査・訴訟の場合は、監査対象情報の内容を、直ちに書面にできることとする。

1）情報の所在管理
紙管理される情報を含め、各種媒体に分散管理された情報も、利用者ごとの情報のすべての所在は、日常的に管理する。

2）見読化手段の管理
電子媒体に保存されたすべての情報とそれらの見読化手段は、対応づけて管理する。見読手段の機器、ソフトウェア、関連情報等は、常に整備する。

3）見読目的に応じた応答時間とスループット
① 利用者への説明が生じたときは、速やかに検索表示もしくは書面に表示できるようにする。この場合の「速やかに」とは、数分以内とする。
② 監査当日に指定された利用者のサービス記録等は、監査に支障のない時間内に検索表示もしくは書面に表示できるようにする。
③ 裁判所、警察等の所定の機関から請求されたときは、指定された日までに、利用者のサービス録等を書面に表示できるようにする。
④ 保存場所が複数ある場合は、各保存場所ごとに見読手段を用意し、その操作方法を明示する。

4）システム障害対策としてのバックアップデータの保存
システムの障害対策として、日々バックアップデータを採取する。

（5）保存性の確保

保存性とは、記録された情報が、法令等が定める期間の真正性を保ち、見読可能にできる状態で保存されることをいう。

1）コンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器および媒体を管理する。

2）不適切な保管・取扱いによる情報の滅失、破壊の防止
① 記録媒体および記録機器の保管および取扱いは、情報セキュリティ実施手順書を作成し、適切な保管および取扱いを行うように関係者を教育し、周知徹底する。
② 電子的に保存されたサービス録等の情報へのアクセス履歴を残し、管理する。

③　各保存場所の情報が破損したときに、バックアップしたデータを用いて破損前の状態に戻せるようにする。もし、破損前と同じ状態に戻せない場合は、失われた範囲が容易にわかるようにする。

3）記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止
記録媒体が劣化する前に、情報を新たな記録媒体または記録機器に複写する。

4）媒体・機器・ソフトウェアの整合性不備による復元不能の防止
システムの変更に際し、旧システムで蓄積した情報の継続的利用を図る対策を講じる。
システム導入時には、契約等でシステム導入業者にデータ移行に関する情報開示条件を明確に示し、旧システムから新システムに移行する場合に、システム内のデータ構造が分からないことに起因するデータ移行の不能を防止する。
開示条件には、倒産・解散・取扱い停止などの事態にも対応できることを含める。

３３．外部保存に関する標準

（1）目的
この項は、情報を外部で保存する場合に必要な事項を定め、もって情報セキュリティを確保することを目的とする。

（2）サービス記録および諸記録を外部に保存する際の基準
1）サービス記録等の保存場所に関する基準は、次の３つに分ける。
①　電子媒体による外部保存を、磁気テープ、ＣＤ-R、ＤＶＤ-R 等の可搬型媒体で行う場合
②　紙やフィルム等の媒体で外部保存を行う場合
2）厚生労働省のガイドライン本文に準拠する。

３４．スキャナ等による電子化保存に関する標準

（1）目的
この項は、サービス記録等を、紙等の媒体で作成・運用した後、スキャナ等で電子化し、保存・運用する場合の取扱いの基準を定め、もって情報セキュリティの確保を目的とする。

（2）共通の要件
1）業務等に支障が生じないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等一定の規格・基準を満たすスキャナを用いる。
○　スキャン等を行う前に、対象書類に他の書類が重なって貼り付けられる、スキャナ等が電子化可能な範囲外に情報が存在する等で、スキャンによる電子化で情報が欠落しないように留意する。

①　一般の書類をスキャンした画像情報は、ＴＩＦＦ形式またはＰＤＦ形式の保存を原則とする。
②　非可逆的な圧縮は、画像の精度を低下させるため、非可逆圧縮を行う場合は、業務等に支障がない精度とする。
③　スキャンの対象となった紙等の破損や汚れ等の状況も、判定可能な範囲を念頭に行う。

2）スキャナによる読み取りの管理者は、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じる。
3）個人情報の保護のため、個人情報保護法を踏まえた所要の取扱いとする。
○　電子化後のもとの紙媒体やフィルムを破棄する場合は、シュレッダー等で個人識別

不可能な状態にした上で破棄する。(医療・介護関係事業者における個人情報の適切な取扱いのためのガイドラインおよび厚労省ガイドライン参照)

(3)都度スキャナ等で電子化して保存する場合の要件

改ざんを防止するため、情報を作成した後または情報を入手した後、一定期間以内にスキャンを行う。

○　一定期間とは、改ざんの機会が生じない程度の期間で、通常は遅滞なくスキャンを行う。機器が使用できない等のやむを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行う。

(4)過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合

1)電子化を行う前に、対象の利用者等に、スキャナ等で電子化する旨を掲示等で周知し、異議の申し立てがあった場合は、スキャナ等で電子化を行わない。

2)実施前に、以下の項目を含む実施計画書を作成する。

①　運用管理規程の作成と妥当性を評価する。
　評価は、外部の有識者を含む、公正性を確保した委員会等で行う(倫理委員会を用いることも可)。

②　作業責任者の特定。

③　利用者等への周知の手段と異議の申し立てに対する対応。

④　相互監視を含む実施の体制。

⑤　実施記録の作成と記録項目。(次項の監査に耐え得る記録作成とする。)

⑥　事後の監査人の選定と監査項目。

⑦　スキャン等で電子化を行ってから紙やフィルムを破棄するまでの期間、および破棄の方法。

3)保有するスキャナ等で電子化を行う場合の監査を、システム監査技術者やＩＳＡＣＡ認定等の適切な能力を持つ外部監査人によっておこなう。

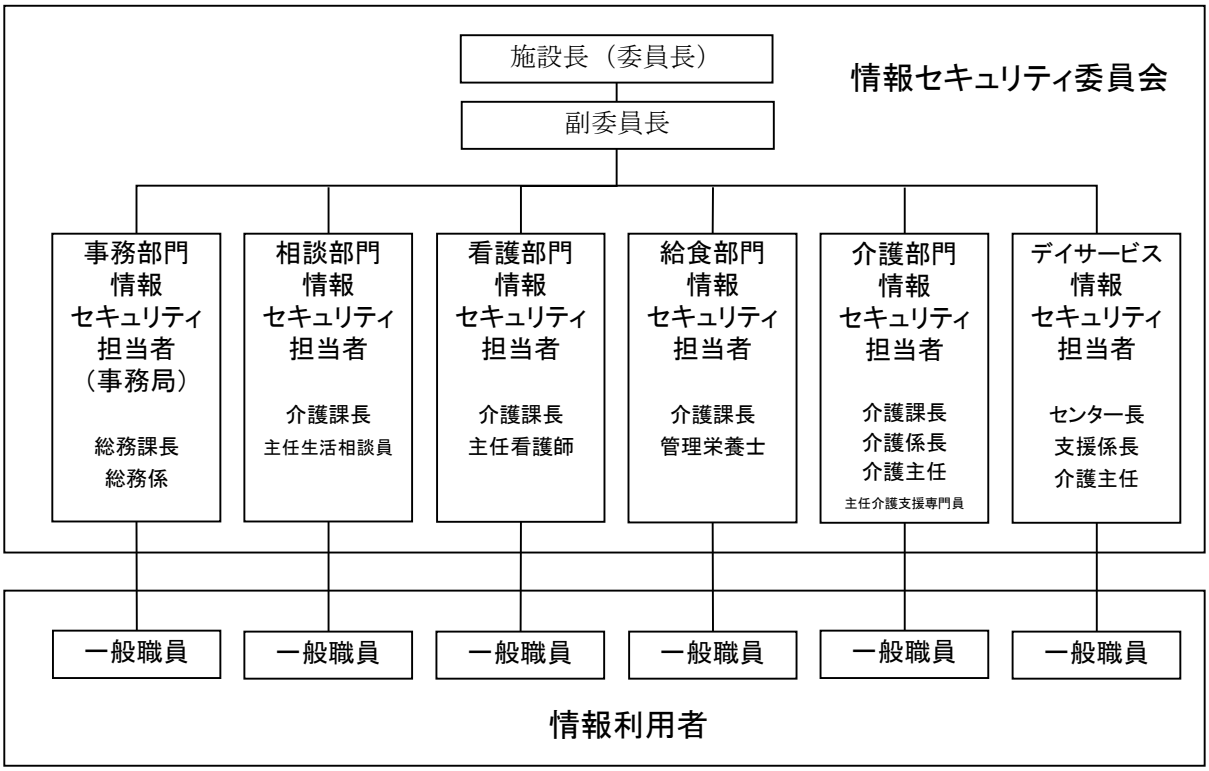
4)外部事業者に委託する場合は、「(2)共通の要件」を満たす適切な事業者を、入札等により選定する。

○　適切な事業者とは、少なくともプライバシーマークを取得し、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者とする。

○　実施に際しては、システム監査技術者やＩＳＡＣＡ認定等の適切な能力を持つ外部監査人の監査を受けることを含め、契約書に十分な安全管理を行うことを具体的に明記させる。

長野県済生会　シルバーランドみつい
情報セキュリティ実施手順

推進体制



１．　情報資産の管理方法

（１）情報資産とは

・情報システム及び記録媒体のデータ

・コンピュータから出力した紙媒体

（２）情報区分

情報区分Ⅰ　・・・　①個人情報を含むもの

②職務の適正な執行に支障を及ぼす恐れのあるもの

情報区分Ⅱ　・・・　情報区分Ⅰ以外の情報

（３）管理方法

①情報資産は情報資産管理表（資料１）に従って管理すること。

②情報は業務目的の範囲内で利用すること。

③盗難や盗み見（利用者及びその家族や業者等外来者）による情報遺漏を防ぐために、机上に個人情報に関わるものを放置しないこと。

④離席する際は、ノートパソコンのふたを閉じる。

⑤重要資産を廃棄する際は、廃棄までは施錠管理された場所で保管し、裁断、溶解等で情報が判読できないように処理をする。

⑥プリンター、コピー、FAX から出力された文書等は速やかに整理や回収並びにシュレッダー等による裁断等、適切な対応を図る。

⑦重要な情報が記載されている用紙を、裏紙として再利用しないこと。

⑧個人情報 ID・パスワード等に関する会話は、周囲に漏れることがない様十分な配慮をする。

⑨やむを得ず外部に重要な情報資産を持ち出すときは、必ず施設長の許可を得ること。また、外出時の行動については「２．情報資産の持ち出しについて」に従って行動する。
⑩ノートパソコン（私物を含む）等は、盗難による情報遺漏がないよう努める。

（資料１）情報資産管理表（情報セキュリティ対策標準８．情報資産の保護（３）情報資産の評価２）評価基準）

評価値 / 取扱	情報区分Ⅰ（４もしくは３）	情報区分Ⅱ（２もしくは１）
複写・複製・コピー（記録媒体・紙媒体）	施設長の許可が必要	主管課長に委任
送付（記録媒体・紙媒体）	・ 施設長の許可が必要 ・ 封筒に入れ､確実に封をする。可能なものは暗号化等の対策をとる ・ 利用目的及び権限の確認 ・ 管理簿を設ける	・ 主管課長に委任 ・ 利用目的及び権限の確認
施設外への持ち出し（記録媒体・紙媒体）	・ 原則禁止 ・ 職務上必要な場合、施設長の許可が必要 ・ 利用目的及び権限の確認	・ 主管課長に委任 ・ 利用目的及び権限の確認
廃棄・再利用（記録媒体・紙媒体）	・ 施設長の許可が必要 ・ 廃棄・再利用前にデータ消去 ・ 廃棄前に裁断等物理的破壊	・主管課長に委任
保管（記録媒体・紙媒体）	・施錠管理	

２．　情報資産の持ち出しについて
（１）外部に重要な情報資産を持ち出す場合は、必ず事前に施設長の許可を得る。
（２）持ち出し時は、盗難・紛失等の情報遺漏リスクを意識し、手元から離さない様注意する。
（３）記録媒体内のデータについては、パスワードを設定する等セキュリティ対策を施す。
（４）返却時は、持ち出した情報資産がすべて揃っている事を確認する。不足があることがわかった時は、直ちに施設長に報告すること。

３．　施設外で利用するパソコンについてのセキュリティ
（１）ウイルス対策ソフトをインストールし、自動アップデートを施し常に最新の状態を保つ。
（２）月１回もしくは適宜に手動で Windows Update を行うこと。自動アップデートも導入。
（３）個人情報等の重要な情報のハードディスク内保存を禁止する。
（４）ウイルススキャンを適宜に自動で行う。
（５）ファイル交換ソフト（Winny 等）がインストールされていない事を確認する。インストールされている場合は、重要な情報を扱わない。

４．　私物パソコンの持ち込みについて

（１）個人所有の情報システム機器を持ち込む場合は、必ず主管課長に申し出を行い、情報管理に関し遺漏がないよう確認と対策をとる。又、申し出を受けた主管課長は、状況報告も合わせ施設長に報告し委員会の了承を得る。

（２）ウイルス対策ソフトをインストールし、自動アップデートを施し常に最新の状態を保つ。

（３）月１回もしくは適宜に手動で Windows Update を行うこと。自動アップデートも導入。

（４）個人情報等の重要な情報のハードディスク内保存を禁止する。

（５）ウイルススキャンを適宜に自動で行う。

（６）個人情報等の重要データは、パスワード付き USB メモリに保存し、施錠できる設備で保管する。

５．　情報システム機器利用時の遵守事項

（１）ハードウェアは無断で改造したり、無断で他のネットワークに接続しない。

（２）OS やソフトウェアにはセキュリティホールという情報セキュリティ上の欠陥が発見されることがあるため、敏速に最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用する。

（３）私用の USB メモリや FD 等の移動媒体も、随時ウイルスチェックを行う。

６．　離席時の対策

（１）長時間離席する場合は、ファイルや使用ソフトを閉じること。
開いたまま離席しない。

（２）使用している USB メモリや FD 等を、忘れずに取り出してしまい込む等適切な管理を行うこと。

（３）ノートパソコン等自席のパソコンは、スクリーンセーバーの設定を施し、情報が遺漏することのないよう管理する。
特に、パソコンに重要データを表示している場合は、他者に盗み見されないよう周囲に配慮すること。

７．　ソフトウェアの取り扱い

（１）私用ソフトをインストールしない。

（２）ソフトウェアの違法コピーを行わない。

（３）施設がライセンス所有するソフトウェアを個人所有のパソコンにインストールしない。

８．　インターネット利用時における遵守事項

（１）職務に関係のないホームページの閲覧を行わない。

（２）ホームページに記載されている情報を全て信用しない。

（３）アクセスしたホームページが有料か無料かの確認を行う。

（４）インターネットからむやみにファイルのダウンロードを行わない。

（５）インターネットの掲示板等に書き込みを行わない。

９．　電子メール利用時における遵守事項

（１）施設内からの送受信は、施設長が必要と認めたパソコンのみに限定する。

（２）職務以外の目的で電子メールを使用しない。

（３）原則として、施設で定めたメールアドレス以外は使用を禁ずる。

（４）送信時には、「内容」、「宛先」の確認を確実に行う。

（５）個人加入のメールアドレスへむやみに送信しない。
（６）データ量が１MB 以上の添付ファイルを送信しない。
（７）不審なメールは、開封及び添付ファイルを実行したりせず、迷惑メールフォルダに移動するか削除すること。
（８）原則として、重要な情報はメールで送信しないこと。業務上やむを得ず送信する時は、必ず事前に主管課長に許可を得る。

10.　コンピュータウイルスに対する遵守事項

（１）ウイルス対策ソフトをインストールすること。

（２）コンピュータウイルス対策ソフトの定義ファイルは、常に最新の状態を保つこと。(自動アップデートを施すこと)
（３）身に覚えのない人から送信された電子メールファイルや添付ファイル、ダウンロードや外部から持ち込まれたプログラム等を開く場合は、開く前にウイルスチェックを行うこと。
（４）ウイルス感染被害に備え、必要に応じて日頃からバックアップを行っておくこと。
（５）ウイルス感染が発覚した場合、そのパソコンの LAN ケーブルをすぐに外し、主管課長・情報セキュリティ委員事務局・施設長に速やかに報告する。その際に使用していた USB メモリや FD 等を他で使用せずに隔離して、担当者の指示に従うこと。

11.　情報セキュリティ事故発生時の手順

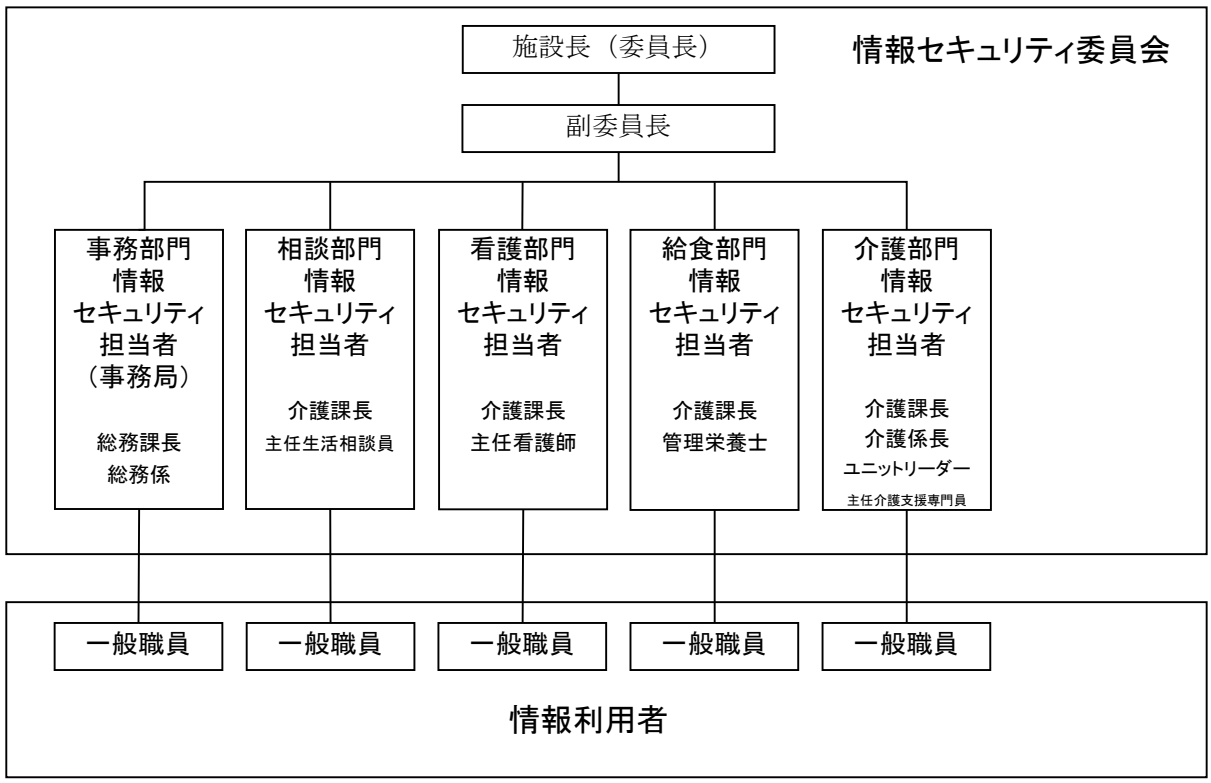
（１）情報遺漏・紛失・盗難・ウイルス感染等の情報セキュリティ事故が発生した場合は、速やかに施設長の報告すること。
（２）「事故報告書」により、施設長に報告すること。
（３）重大な個人情報等の紛失等の場合、事務局は事情を聴取し纏め、別途「事故報告書」により県及び関係市町村の担当課宛報告すること。

施設から利用者等の個人情報が、紛失、流失、遺漏した場合、施設及び法人の信用を失墜させ、場合により損害賠償の請求を受ける事があります。
又、職員は法令・条例による罰則や、就業規則による懲戒処分に課されることもあります。
私用のデータを扱っているのではなく、利用者等の大切な情報を扱っているという意識を持ち、情報セキュリティ規程等や実施手順を遵守しましょう。

参考資料：東京都板橋区　板橋第一小学校セキュリティ実施手順

長野県済生会　シルバーランドきしの
情報セキュリティ実施手順

推進体制



１．　情報資産の管理方法

（１）情報資産とは

・情報システム及び記録媒体のデータ

・コンピュータから出力した紙媒体

（２）情報区分

情報区分Ⅰ　・・・　①個人情報を含むもの

②職務の適正な執行に支障を及ぼす恐れのあるもの

情報区分Ⅱ　・・・　情報区分Ⅰ以外の情報

（３）管理方法

①情報資産は情報資産管理表（資料１）に従って管理すること。

②情報は業務目的の範囲内で利用すること。

③盗難や盗み見（利用者及びその家族や業者等外来者）による情報遺漏を防ぐために、机上に個人情報に関わるものを放置しないこと。

④離席する際は、ノートパソコンのふたを閉じる。

⑤重要資産を廃棄する際は、廃棄までは施錠管理された場所で保管し、裁断、溶解等で情報が判読できないように処理をする。

⑥プリンター、コピー、FAX から出力された文書等は速やかに整理や回収並びにシュレッダー等による裁断等、適切な対応を図る。

⑦重要な情報が記載されている用紙を、裏紙として再利用しないこと。

⑧個人情報 ID・パスワード等に関する会話は、周囲に漏れることがない様十分な

配慮をする。

⑨やむを得ず外部に重要な情報資産を持ち出すときは、必ず施設長の許可を得ること。また、外出時の行動については「２．情報資産の持ち出しについて」に従って行動する。

⑩ノートパソコン（私物を含む）等は、盗難による情報遺漏がないよう努める。

（資料１）情報資産管理表（情報セキュリティ対策標準８．情報資産の保護（３）情報資産の評価２）評価基準）

評価値 / 取扱	情報区分Ⅰ（４もしくは３）	情報区分Ⅱ（２もしくは１）
複写・複製・コピー（記録媒体・紙媒体）	施設長の許可が必要	主管課長に委任
送付（記録媒体・紙媒体）	・ 施設長の許可が必要 ・ 封筒に入れ､確実に封をする。可能なものは暗号化等の対策をとる ・ 利用目的及び権限の確認 ・ 管理簿を設ける	・ 主管課長に委任 ・ 利用目的及び権限の確認
施設外への持ち出し（記録媒体・紙媒体）	・ 原則禁止 ・ 職務上必要な場合、施設長の許可が必要 ・ 利用目的及び権限の確認	・ 主管課長に委任 ・ 利用目的及び権限の確認
廃棄・再利用（記録媒体・紙媒体）	・ 施設長の許可が必要 ・ 廃棄・再利用前にデータ消去 ・ 廃棄前に裁断等物理的破壊	・主管課長に委任
保管（記録媒体・紙媒体）	・施錠管理	

２．　情報資産の持ち出しについて

（１）外部に重要な情報資産を持ち出す場合は、必ず事前に施設長の許可を得る。

（２）持ち出し時は、盗難・紛失等の情報遺漏リスクを意識し、手元から離さない様注意する。

（３）記録媒体内のデータについては、パスワードを設定する等セキュリティ対策を施す。

（４）返却時は、持ち出した情報資産がすべて揃っている事を確認する。不足があることがわかった時は、直ちに施設長に報告すること。

３．　施設外で利用するパソコンについてのセキュリティ

（１）ウイルス対策ソフトをインストールし、自動アップデートを施し常に最新の状態を保つ。

（２）月１回もしくは適宜に手動で Windows Update を行うこと。自動アップデートも導入。

（３）個人情報等の重要な情報のハードディスク内保存を禁止する。

（４）ウイルススキャンを適宜に自動で行う。

（５）ファイル交換ソフト（Winny 等）がインストールされていない事を確認する。インストールされている場合は、重要な情報を扱わない。

４．　私物パソコンの持ち込みについて

（１）個人所有の情報システム機器を持ち込む場合は、必ず主管課長に申し出を行い、情報管理に関し遺漏がないよう確認と対策をとる。又、申し出を受けた主管課長は、状況報告も合わせ施設長に報告し委員会の了承を得る。

（２）ウイルス対策ソフトをインストールし、自動アップデートを施し常に最新の状態を保つ。

（３）月１回もしくは適宜に手動で Windows Update を行うこと。自動アップデートも導入。

（４）個人情報等の重要な情報のハードディスク内保存を禁止する。

（５）ウイルススキャンを適宜に自動で行う。

（６）個人情報等の重要データは、パスワード付き USB メモリに保存し、施錠できる設備で保管する。

５．　情報システム機器利用時の遵守事項

（１）ハードウェアは無断で改造したり、無断で他のネットワークに接続しない。

（２）OS やソフトウェアにはセキュリティホールという情報セキュリティ上の欠陥が発見されることがあるため、敏速に最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用する。

（３）私用の USB メモリや FD 等の移動媒体も、随時ウイルスチェックを行う。

６．　離席時の対策

（１）長時間離席する場合は、ファイルや使用ソフトを閉じること。
開いたまま離席しない。

（２）使用している USB メモリや FD 等を、忘れずに取り出してしまい込む等適切な管理を行うこと。

（３）ノートパソコン等自席のパソコンは、スクリーンセーバーの設定を施し、情報が遺漏することのないよう管理する。
特に、パソコンに重要データを表示している場合は、他者に盗み見されないよう周囲に配慮すること。

７．　ソフトウェアの取り扱い

（１）私用ソフトをインストールしない。

（２）ソフトウェアの違法コピーを行わない。

（３）施設がライセンス所有するソフトウェアを個人所有のパソコンにインストールしない。

８．　インターネット利用時における遵守事項

（１）職務に関係のないホームページの閲覧を行わない。

（２）ホームページに記載されている情報を全て信用しない。

（３）アクセスしたホームページが有料か無料かの確認を行う。

（４）インターネットからむやみにファイルのダウンロードを行わない。

（５）インターネットの掲示板等に書き込みを行わない。

９．　電子メール利用時における遵守事項

（１）施設内からの送受信は、施設長が必要と認めたパソコンのみに限定する。

（２）職務以外の目的で電子メールを使用しない。

（３）原則として、施設で定めたメールアドレス以外は使用を禁ずる。

（４）送信時には、「内容」、「宛先」の確認を確実に行う。

（５）個人加入のメールアドレスへむやみに送信しない。
（６）データ量が１MB 以上の添付ファイルを送信しない。
（７）不審なメールは、開封及び添付ファイルを実行したりせず、迷惑メールフォルダに移動するか削除すること。
（８）原則として、重要な情報はメールで送信しないこと。業務上やむを得ず送信する時は、必ず事前に主管課長に許可を得る。

10.　コンピュータウイルスに対する遵守事項

（１）ウイルス対策ソフトをインストールすること。

（２）コンピュータウイルス対策ソフトの定義ファイルは、常に最新の状態を保つこと。（自動アップデートを施すこと）
（３）身に覚えのない人から送信された電子メールファイルや添付ファイル、ダウンロードや外部から持ち込まれたプログラム等を開く場合は、開く前にウイルスチェックを行うこと。
（４）ウイルス感染被害に備え、必要に応じて日頃からバックアップを行っておくこと。
（５）ウイルス感染が発覚した場合、そのパソコンの LAN ケーブルをすぐに外し、主管課長・情報セキュリティ委員事務局・施設長に速やかに報告する。その際に使用していた USB メモリや FD 等を他で使用せずに隔離して、担当者の指示に従うこと。

11.　情報セキュリティ事故発生時の手順

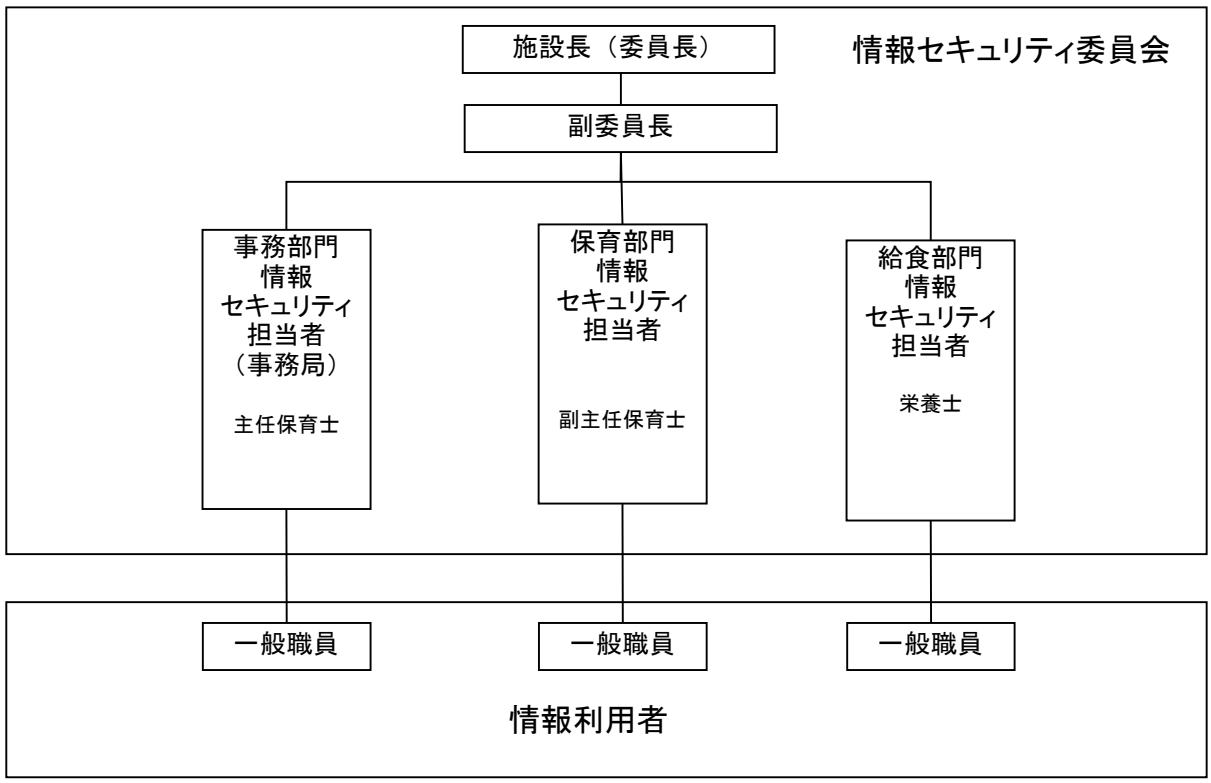
（１）情報遺漏・紛失・盗難・ウイルス感染等の情報セキュリティ事故が発生した場合は、速やかに施設長の報告すること。
（２）「事故報告書」により、施設長に報告すること。
（３）重大な個人情報等の紛失等の場合、事務局は事情を聴取し纏め、別途「事故報告書」により県及び関係市町村の担当課宛報告すること。

施設から利用者等の個人情報が、紛失、流失、遺漏した場合、施設及び法人の信用を失墜させ、場合により損害賠償の請求を受ける事があります。
又、職員は法令・条例による罰則や、就業規則による懲戒処分に課されることもあります。
私用のデータを扱っているのではなく、利用者等の大切な情報を扱っているという意識を持ち、情報セキュリティ規程等や実施手順を遵守しましょう。

参考資料：東京都板橋区　板橋第一小学校セキュリティ実施手順

長野県済生会　長野保育園
情報セキュリティ実施手順

推進体制



１．　情報資産の管理方法

（１）情報資産とは

・情報システム及び記録媒体のデータ

・コンピュータから出力した紙媒体

（２）情報区分

情報区分Ⅰ　・・・　①個人情報を含むもの
②職務の適正な執行に支障を及ぼす恐れのあるもの

情報区分Ⅱ　・・・　情報区分Ⅰ以外の情報

（３）管理方法

①情報資産は情報資産管理表（資料１）に従って管理すること。

②情報は業務目的の範囲内で利用すること。

③盗難や盗み見（利用者及びその家族や業者等外来者）による情報遺漏を防ぐために、机上に個人情報に関わるものを放置しないこと。

④離席する際は、ノートパソコンのふたを閉じる。

⑤重要資産を廃棄する際は、廃棄までは施錠管理された場所で保管し、裁断、溶解等で情報が判読できないように処理をする。

⑥プリンター、コピー、FAX から出力された文書等は速やかに整理や回収並びにシュレッダー等による裁断等、適切な対応を図る。

⑦重要な情報が記載されている用紙を、裏紙として再利用しないこと。

⑧個人情報 ID・パスワード等に関する会話は、周囲に漏れることがない様十分な

配慮をする。
⑨やむを得ず外部に重要な情報資産を持ち出すときは、必ず施設長の許可を得ること。また、外出時の行動については「２．情報資産の持ち出しについて」に従って行動する。
⑩ノートパソコン（私物を含む）等は、盗難による情報遺漏がないよう努める。

（資料１）情報資産管理表（情報セキュリティ対策標準８．情報資産の保護（３）情報資産の評価２）評価基準）

評価値 / 取扱	情報区分Ⅰ （４もしくは３）	情報区分Ⅱ （２もしくは１）
複写・複製・コピー （記録媒体・紙媒体）	施設長の許可が必要	主管課長に委任
送付 （記録媒体・紙媒体）	・ 施設長の許可が必要 ・ 封筒に入れ､確実に封をする。可能なものは暗号化等の対策をとる ・ 利用目的及び権限の確認 ・ 管理簿を設ける	・ 主管課長に委任 ・ 利用目的及び権限の確認
施設外への持ち出し （記録媒体・紙媒体）	・ 原則禁止 ・ 職務上必要な場合、施設長の許可が必要 ・ 利用目的及び権限の確認	・ 主管課長に委任 ・ 利用目的及び権限の確認
廃棄・再利用 （記録媒体・紙媒体）	・ 施設長の許可が必要 ・ 廃棄・再利用前にデータ消去 ・ 廃棄前に裁断等物理的破壊	・主管課長に委任
保管 （記録媒体・紙媒体）	・施錠管理	

２．　情報資産の持ち出しについて
（１）外部に重要な情報資産を持ち出す場合は、必ず事前に施設長の許可を得る。
（２）持ち出し時は、盗難・紛失等の情報遺漏リスクを意識し、手元から離さない様注意する。
（３）記録媒体内のデータについては、パスワードを設定する等セキュリティ対策を施す。
（４）返却時は、持ち出した情報資産がすべて揃っている事を確認する。不足があることがわかった時は、直ちに施設長に報告すること。

３．　施設外で利用するパソコンについてのセキュリティ
（１）ウイルス対策ソフトをインストールし、自動アップデートを施し常に最新の状態を保つ。
（２）月１回もしくは適宜に手動で Windows Update を行うこと。自動アップデートも導入。
（３）個人情報等の重要な情報のハードディスク内保存を禁止する。
（４）ウイルススキャンを適宜に自動で行う。
（５）ファイル交換ソフト（Winny 等）がインストールされていない事を確認する。インストールされている場合は、重要な情報を扱わない。

４．　私物パソコンの持ち込みについて

（１）個人所有の情報システム機器を持ち込む場合は、必ず主管課長に申し出を行い、情報管理に関し遺漏がないよう確認と対策をとる。又、申し出を受けた主管課長は、状況報告も合わせ施設長に報告し委員会の了承を得る。

（２）ウイルス対策ソフトをインストールし、自動アップデートを施し常に最新の状態を保つ。

（３）月１回もしくは適宜に手動で Windows Update を行うこと。自動アップデートも導入。

（４）個人情報等の重要な情報のハードディスク内保存を禁止する。

（５）ウイルススキャンを適宜に自動で行う。

（６）個人情報等の重要データは、パスワード付き USB メモリに保存し、施錠できる設備で保管する。

５．　情報システム機器利用時の遵守事項

（１）ハードウェアは無断で改造したり、無断で他のネットワークに接続しない。

（２）OS やソフトウェアにはセキュリティホールという情報セキュリティ上の欠陥が発見されることがあるため、敏速に最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用する。

（３）私用の USB メモリや FD 等の移動媒体も、随時ウイルスチェックを行う。

６．　離席時の対策

（１）長時間離席する場合は、ファイルや使用ソフトを閉じること。
開いたまま離席しない。

（２）使用している USB メモリや FD 等を、忘れずに取り出してしまい込む等適切な管理を行うこと。

（３）ノートパソコン等自席のパソコンは、スクリーンセーバーの設定を施し、情報が遺漏することのないよう管理する。
特に、パソコンに重要データを表示している場合は、他者に盗み見されないよう周囲に配慮すること。

７．　ソフトウェアの取り扱い

（１）私用ソフトをインストールしない。

（２）ソフトウェアの違法コピーを行わない。

（３）施設がライセンス所有するソフトウェアを個人所有のパソコンにインストールしない。

８．　インターネット利用時における遵守事項

（１）職務に関係のないホームページの閲覧を行わない。

（２）ホームページに記載されている情報を全て信用しない。

（３）アクセスしたホームページが有料か無料かの確認を行う。

（４）インターネットからむやみにファイルのダウンロードを行わない。

（５）インターネットの掲示板等に書き込みを行わない。

９．　電子メール利用時における遵守事項

（１）施設内からの送受信は、施設長が必要と認めたパソコンのみに限定する。

（２）職務以外の目的で電子メールを使用しない。

（３）原則として、施設で定めたメールアドレス以外は使用を禁ずる。

（４）送信時には、「内容」、「宛先」の確認を確実に行う。

（５）個人加入のメールアドレスへむやみに送信しない。
（６）データ量が１MB 以上の添付ファイルを送信しない。
（７）不審なメールは、開封及び添付ファイルを実行したりせず、迷惑メールフォルダに移動するか削除すること。
（８）原則として、重要な情報はメールで送信しないこと。業務上やむを得ず送信する時は、必ず事前に主管課長に許可を得る。

10.　コンピュータウイルスに対する遵守事項

（１）ウイルス対策ソフトをインストールすること。

（２）コンピュータウイルス対策ソフトの定義ファイルは、常に最新の状態を保つこと。(自動アップデートを施すこと)
（３）身に覚えのない人から送信された電子メールファイルや添付ファイル、ダウンロードや外部から持ち込まれたプログラム等を開く場合は、開く前にウイルスチェックを行うこと。
（４）ウイルス感染被害に備え、必要に応じて日頃からバックアップを行っておくこと。
（５）ウイルス感染が発覚した場合、そのパソコンの LAN ケーブルをすぐに外し、主管課長・情報セキュリティ委員事務局・施設長に速やかに報告する。その際に使用していた USB メモリや FD 等を他で使用せずに隔離して、担当者の指示に従うこと。

11.　情報セキュリティ事故発生時の手順

（１）情報遺漏・紛失・盗難・ウイルス感染等の情報セキュリティ事故が発生した場合は、速やかに施設長の報告すること。
（２）「事故報告書」により、施設長に報告すること。
（３）重大な個人情報等の紛失等の場合、事務局は事情を聴取し纏め、別途「事故報告書」により県及び関係市町村の担当課宛報告すること。

施設から利用者等の個人情報が、紛失、流失、遺漏した場合、施設及び法人の信用を失墜させ、場合により損害賠償の請求を受ける事があります。
又、職員は法令・条例による罰則や、就業規則による懲戒処分に課されることもあります。
私用のデータを扱っているのではなく、利用者等の大切な情報を扱っているという意識を持ち、情報セキュリティ規程等や実施手順を遵守しましょう。

参考資料：東京都板橋区　板橋第一小学校セキュリティ実施手順