新潟県市町村総合事務組合情報セキュリティ対策基準

新潟県市町村総合事務組合情報セキュリティ対策基準を次のように定め、平成20年10月1日から実施する。

1　趣旨

この基準は、新潟県市町村総合事務組合情報セキュリティ基本方針に基づき、新潟県市町村総合事務組合の情報セキュリティ対策に必要な事項を定めるものとする。

2　定義

この基準で使用する用語は、この基準で定めるもののほか、新潟県市町村総合事務組合情報セキュリティ基本方針で使用する用語の例による。

3　組織体制

(1) 情報セキュリティ責任者

① 事務局長を情報セキュリティ責任者とする。

② 情報セキュリティ責任者は、情報セキュリティ対策に関する統括的な権限及び責任を有する。

③ 情報セキュリティ責任者は、情報システムの開発、設定変更、運用、見直し等を行う統括的な権限及び責任を有する。

(2) 情報セキュリティ管理者

① 課長を情報セキュリティ管理者とする。

② 情報セキュリティ管理者は、所管する課の情報セキュリティ対策に関する権限及び責任を有する。

③ 情報セキュリティ管理者は、所管する課の情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

④ 情報セキュリティ管理者は、所管する課において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報システム管理者に連絡するとともに、情報セキュリティ責任者に報告をしなければならない。

(3) 情報システム管理者

① 総務課長を、情報システム管理者とする。

② 情報システム管理者は､情報システムのセキュリティに関する権限及び責任を有する。

③ 情報システム管理者は、情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

(4) 情報システム担当者

① 総務係長を、情報システム担当者とする。

② 情報システム担当者は、情報システム管理者の指示等に従い、情報システムのセキュリティに関する作業を行う。

③ 情報システム担当者は、情報システム管理者の指示等に従い、情報システムの開発、設定変更、運用、更新等の作業を行う。

(5) 情報セキュリティ委員会

情報セキュリティに関する重要事項を決定するため、組合に情報セキュリティ委員会

（以下この項において「委員会」という。）を置き、その組織を次に掲げるとおりとする。

① 委員会の委員は、事務局長、事務局次長及び課長とする。

② 委員会に委員長及び副委員長を置き、委員長には事務局長を、副委員長には事務局次長をもって充てる。

③ 副委員長は、委員長を補佐し、委員長に事故あるとき又は委員長が欠けたときは、その職務を代理する。

④ 委員会は、委員長が招集し、委員長が会議の議長となる。

⑤ 委員会の議事は、出席委員の過半数でこれを決し、可否同数のときは、議長が決するところによる。

⑥ 委員会の庶務は、総務係において行う。

⑦ この基準に定めるもののほか、委員会の運営に関し必要な事項は、別に定める。

4 情報資産の分類と管理

(1) 情報資産の分類

情報資産は、機密性、完全性及び可用性により、次のとおり分類し、取扱制限を行うものとする。

① 機密性による情報資産

分類	分類基準	取扱制限
機密性３	情報資産のうち、秘密文書に相当する機密性を要する情報資産	・ 私物パソコンでの作業禁止 ・ 必要以上の複製及び配付禁止 ・ 保管場所の制限及び保管場所への外部記録媒体等の持込禁止 ・ 情報の送信、情報資産の運搬、提供時における暗号化、パスワード設定等 ・ 復元不可能な処理を施しての廃棄 ・ 信頼できるネットワーク回線の選択 ・ 外部記録媒体等の施錠可能な場所への保管
機密性２	情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに、一般に公表することを前提としていない情報資産	
機密性１	機密性２及び機密性３の情報資産以外の情報資産	

② 完全性による情報資産

分類	分類基準	取扱制限
完全性２	情報資産のうち、改ざん、破損等により、事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・ バックアップ、電子署名付与等 ・ 外部記録媒体等の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

③ 可用性による情報資産

分類	分類基準	取扱制限

可用性２	情報資産のうち、滅失、紛失等により、事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・ バックアップ及び指定時間以内の復旧体制の確保 ・ 外部記録媒体等の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	

(2) 情報資産の管理

① 管理責任

ア 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

イ 情報資産が複製又は伝送された場合には、当該情報資産も(1)の分類により管理しなければならない。

② 情報の作成

ア 職員等は、業務上必要のない情報を作成してはならない。

イ 情報を作成する者は、情報の作成時に(1)の分類により当該情報の分類及び取扱制限を定めなければならない。

ウ 情報を作成する者は、作成途中の情報についても、紛失、漏えい等を防止しなければならない。

エ 情報を作成する者は、情報の作成途中で情報が不要になった場合は、当該情報を消去しなければならない。

③ 情報資産の入手

ア 情報資産を入手した者は、(1)の分類により当該情報の分類及び取扱制限を定めなければならない。

イ 情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰がなければならない。

④ 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、情報資産の分類により適切な取扱いをしなければならない。

ウ 情報資産を利用する者は、記録媒体等に情報資産の分類が異なる情報が複数記録されている場合は、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

⑤ 情報資産の保管

ア 情報セキュリティ管理者は、情報資産の分類により情報資産を適切に保管しなければならない。

イ 情報セキュリティ管理者は、情報資産を記録した外部記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ 情報セキュリティ管理者は、利用頻度が低い外部記録媒体及び情報システムのバックアップで取得したデータを記録する外部記録媒体を長期保管する場合は、自然災害を被る可能性が低い場所に保管しなければならない。

エ 情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を記録した外部記録媒体を保管する場合は、施錠可能な場所に保管しなければならない。

⑥　情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じて、暗号化又はパスワード設定を行わなければならない。

⑦　情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は、暗号化、パスワード設定等による情報資産の不正利用を防止するための措置を講じなければならない。

イ　機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑧　情報資産の廃棄

ア　機密性２以上の情報資産を廃棄する者は、記録媒体等の初期化その他情報の復元が不可能な処置をした上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得るとともに、必要に応じて、日時、担当者及び処理内容を記録しなければならない。

5　物理的セキュリティ

(1) サーバ等の管理

①　機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を受けない場所に設置し、取り外せないよう固定する等の措置を講じなければならない。

②　機器の電源

ア　情報システム管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備えて、必要に応じて、当該機器が適切に停止するまでの間に十分な電力を供給するための予備電源を備え付けなければならない。

イ　情報システム管理者は、落雷等による過電流に備えて、必要に応じて、サーバ等の機器を保護するための措置を講じなければならない。

③　通信ケーブル等の配線

ア　情報システム管理者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等の必要な措置を講じなければならない。

イ　情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合は、連携して対応しなければならない。

ウ　情報システム管理者は、ネットワーク接続口を他者が容易に接続できない場所に設置する等により適切に管理をしなければならない。

エ　情報システム管理者は、操作を認められていない者が配線を変更又は追加できないように必要な措置を施さなければならない。

④　機器の定期保守及び修理

ア　情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

イ　情報システム管理者は、記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。

ウ　イの場合において、内容を消去できないときは、修理を委託する事業者との間で、守秘義務契約の締結等の必要な措置を講じなければならない。

⑤　敷地外への機器の設置

ア　情報システム管理者は、庁舎外にサーバ等の機器を設置する場合は、情報セキュリティ責任者の承認を得なければならない。

イ　アの場合において、情報システム管理者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑥　機器の廃棄等

情報システム管理者は、機器の廃棄、返却等をする場合は、機器内部の記憶装置のすべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(2) 情報システム室の管理

①　情報システム室の構造等

ア　情報システム室とは、情報ネットワーク及び情報システムが設置され、当該情報ネットワーク及び情報システムの管理及び運用を行っている部屋等をいう。

イ　情報システム管理者は、情報システム室を地階又は１階に設けてはならない。

ウ　情報システム管理者は、情報システム室への外部からの侵入を防ぐため、無窓の外壁にしなければならない。【推奨事項】

エ　情報システム管理者は、情報システム室から外部に通じるドアは必要最小限とし、鍵、監視機能、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しなければならない。

オ　情報システム管理者は、情報システム室内には、転倒、落下等の防止のため、耐震、防火、防水等の必要な措置を講じなければならない。

カ　情報システム管理者は、情報システム室を囲む外壁等の床下開口部をすべてふさがなければならない。【推奨事項】

キ　情報システム管理者は、情報システム室に配置する消火薬剤、消防用設備等が、機器等及び記録媒体に影響を与えないようにしなければならない。

②　情報システム室の入退室管理等

ア　情報システム管理者は、情報システム室への入退室を許可された者のみに制限し、必要に応じて、ＩＣカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。【推奨事項】

イ　職員等及び外部委託事業者は、情報システム室に入室する場合は、身分証明書等を携帯し、求められたときは、提示しなければならない。【推奨事項】

③　機器等の搬入出

ア　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託業者に確認を行わせなければならない。

イ　情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

(3) 通信回線等の管理

①　情報システム管理者は、組合の通信回線及び通信回線装置を適切に管理しなければならない。

②　情報システム管理者は、①に関連する文書を適切に保管しなければならない。

③　情報システム管理者は、外部ネットワークへの接続を必要最低限に限定しなければならない。

④　情報システム管理者は、外部ネットワークに使用する回線について、伝送途上に情報の漏えい、破壊、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

(4) 職員等のパソコン等の管理

①　情報システム管理者は、パソコン等の端末について、盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。

②　情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③　情報システム管理者は、必要に応じて、BIOS パスワード、ハードディスクパスワード等を併用しなければならない。【推奨事項】

④　情報システム管理者は、必要に応じて、パスワード以外に指紋認証等の生体認証を併用しなければならない。【推奨事項】

⑤　情報システム管理者は、パソコン等の端末のディスクデータの暗号化、セキュリティチップ等の機能を有効に活用しなければならない。【推奨事項】

6　人的セキュリティ

(1) 職員等の遵守事項

①　職員等の遵守事項

ア　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守するとともに、情報セキュリティ対策について、不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

イ　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、インターネットへのアクセス等を行ってはならない。

ウ　パソコン等の端末の持ち出し及び外部における情報処理作業の制限

・　職員等は、組合のパソコン等の端末、記録媒体、情報資産及びソフトウエアを外部に持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

・　職員等は、外部で情報処理業務を行う場合は、情報セキュリティ管理者の許可を得なければならない。

エ　パソコン等の端末等の持込み

職員等は、私物のパソコン又は記録媒体を庁舎内に持ち込んではならない。ただし、業務上必要な場合であって、情報セキュリティ管理者の許可を得たときは、この限りでない。

オ　持ち出し及び持込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持込みについて、必要に応じて、記録を作成し、保管しなければならない。

カ　パソコン等の端末におけるセキュリティ機能の設定変更の禁止

職員等は、パソコン等の端末のソフトウエアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

キ　机上の端末等の管理

職員等は、パソコン等の端末や記録媒体、情報が印刷された文書等について、第三

者に使用されること又は閲覧されることを防止するため、離席時の端末ロック、記録媒体、文書等の容易に閲覧されない場所への保管その他適切な措置を講じなければならない。

ク　退職時等の遵守事項

・　職員等は、異動、退職等により業務を離れる場合は、利用していた情報資産を、返却しなければならない。

・　職員等は、業務上知り得た情報を漏らしてはならない。その職を退いた後も同様とする。

② 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

③ 外部委託事業者に対する説明

情報セキュリティ管理者は、情報ネットワーク及び情報システムの開発、保守等を外部委託事業者に発注する場合は、情報セキュリティポリシーその他外部委託事業者が守るべき内容について、説明しなければならない。

(2) 研修

① 情報セキュリティに関する研修

情報システム管理者は、定期的に情報セキュリティに関する研修を実施しなければならない。

② 研修計画の立案及び実施

ア　情報システム管理者は、職員等に対する情報セキュリティに関する研修計画を立案し、情報セキュリティ委員会の承認を得なければならない。

イ　情報システム管理者は、研修計画において、職員等は毎年度最低1回は情報セキュリティに関する研修を受講できるようにしなければならない。【推奨事項】

③ 研修への参加

職員等は、定められた情報セキュリティに関する研修に参加しなければならない。

(3) ＩＤ及びパスワード等の管理

① 職員等のＩＤの取扱い

ア　自己が利用しているＩＤは、他人に利用させてはならない。

イ　共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

② 職員等のパスワードの取扱い

ア パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

イ パスワードを記載したメモを作成してはならない。

ウ パスワードが流出したおそれがある場合は、情報システム管理者に速やかに報告しなければならない。

エ 複数の情報システムを取り扱う職員等は、同一のパスワードをシステム間で用いてはならない。

オ パソコン等の端末のパスワードの記憶機能を利用してはならない。

カ 職員等間でパスワードを共有してはならない。

7　技術的セキュリティ

(1) コンピュータ及びネットワークの管理

① バックアップの実施

情報システム管理者は、サーバ等に記録された情報について、定期的にバックアップを実施しなければならない。

② 他団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、他団体との間で情報システムに関する情報又はソフトウエアを交換する場合は、その取扱いに関する事項をあらかじめ定め、情報セキュリティ責任者及びシステム管理者の許可を得なければならない。

③ システムの管理記録及び作業確認

情報セキュリティ管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、改ざん、消去、盗難等をされないように適切に管理しなければならない。

④ 情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図及び情報システム仕様書について、業務上必要とする者以外の閲覧並びに盗難及び紛失がないように、適切に管理しなければならない。

⑤ 障害記録

情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果等を障害記録として記録し、適切に保存しなければならない。

⑥ 情報ネットワークの接続制御、経路制御等

ア 情報システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等を設定しなければならない。

イ 情報システム管理者は、不正アクセスを防止するため、情報ネットワークに適切なアクセス制御を施さなければならない。

⑦ 外部の者が利用できるシステムの分離等

情報システム管理者は、外部の者が利用できるシステムについて、必要に応じて、他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑧ 外部ネットワークとの接続制限等

ア 情報セキュリティ管理者は、所管する情報ネットワークを外部ネットワークと接続しようとする場合は、情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

イ 情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合は、情報セキュリティ責任者及び情報システム管理者に報告するとともに、速やかに、当該外部ネットワークを物理的に遮断しなければならない。

⑨ 電子メールのセキュリティ管理

ア 情報システム管理者は、大量のスパムメール等の送受信を検知した場合は、メールサーバの運用を停止しなければならない。

イ 情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。【推奨事項】

ウ 情報システム管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように、システム上の措置を行わなければならない。

【推奨事項】

⑩　電子メールの利用制限

ア　職員等は、自動転送機能を用いて電子メールを転送してはならない。

イ　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　職員等は、複数人に電子メールを送信する場合は、他の送信先の電子メールアドレスが分からないようにしなければならない。

エ　職員等は、重要な電子メールを誤送信した場合は、直ちに、情報セキュリティ管理者に報告しなければならない。

⑪　無許可ソフトウエアの導入等の禁止

ア　職員等は、パソコン等の端末に無許可でソフトウエアを導入してはならない。

イ　職員等は、業務上の必要がある場合であって、情報セキュリティ管理者及び情報システム管理者がやむを得ないものと認めたときに限り、ソフトウェアを導入することができる。

ウ　職員等は、不正にコピーしたソフトウェアを利用してはならない。

⑫　機器構成の変更の制限

ア　職員等は、パソコン等の端末を無許可で機器の改造又は増設若しくは交換を行ってはならない。

イ　職員等は、業務上の必要がある場合であって、情報セキュリティ責任者及び情報システム管理者がやむを得ないものと認めたときに限り、パソコン等の端末を機器の改造又は増設若しくは交換を行うことができる。

⑬　ネットワーク接続の禁止

職員等は、情報セキュリティ管理者の許可なくパソコン等の端末を情報ネットワークに接続してはならない。

⑭　業務以外の目的でのウェブ閲覧の禁止

ア　職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　情報セキュリティ管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ責任者及び情報システム管理者に通知し、適切な措置を求めなければならない。

(2)　アクセス制御

①　アクセス制御

ア　アクセス制御

情報システム管理者は、情報ネットワーク及び情報システムについて、アクセス権限のない職員等がアクセスできないようにシステム上の制限をしなければならない。

イ　利用者ＩＤの取扱い

・　情報システム管理者は、利用者の登録、変更、抹消等の情報管理及び職員等の異動、退職等に伴う利用者ＩＤの取扱方法を定めなければならない。

・　情報システム管理者は、利用されていないＩＤが放置されないよう点検しなければならない。

②　パスワードに関する情報の管理

情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。この場合において、オペレーティングシステム等でパスワード設定のセキュリティ強化機能があるときは、これを有効に活用しなければならない。

(3) 情報システム開発、導入、保守等

① 情報システムの調達

ア 情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ 情報システム管理者は、機器及びソフトウエアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

② 情報システムの開発

ア 情報システム管理者は、情報システム開発の責任者及び作業者を特定しなければならない。

イ 情報システム管理者は、情報システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

ウ 情報システム管理者は、情報システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。

③ 情報システム開発、保守等に関連する資料等の保管

ア 情報システム管理者は、情報システム開発、保守等に関連する資料及び文書を適切な方法で保管しなければならない。

イ 情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ 情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

④ 情報システムにおける入出力データの正確性の確保

ア 情報システム管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正文字列入力の除去機能を組み込むように情報システムを設計しなければならない。

イ 情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合は、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

⑤ 情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

⑥ 開発及び保守用のソフトウエアの更新等

情報システム管理者は、開発及び保守用のソフトウエア等の更新又はパッチの適用をする場合は、他の情報システムとの整合性を確認しなければならない。

(4) 不正プログラム対策

① 情報システム管理者の措置事項

ア 外部ネットワークから受信又は送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入又は外部への拡散を防止しなければならない。

イ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じて、職員等に対して注意喚起しなければならない。

ウ　サーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウエアを常駐させなければならない。

エ　不正プログラム対策のソフトウエア及びそのパターンファイルは、常に最新の状態に保たなければならない。

オ　インターネットに接続していないシステムにおいて、記録媒体を使う場合は、コンピュータウイルス等の感染を防止するため、組合が管理している媒体以外のものを職員等に利用させてはならない。

② 職員等の遵守事項

ア　パソコン等の端末において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

イ　外部からデータ又はソフトウエアを取り入れる場合は、必ず不正プログラム対策ソフトウエアによるチェックを行わなければならない。

ウ　差出人が不明なメール又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

エ　端末に対して、不正プログラム対策ソフトウエアによるフルチェックを定期的に実施しなければならない。

オ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行わなければならない。

カ　コンピュータウイルス等の不正プログラムに感染した場合は、ＬＡＮケーブルの取り外し及び機器の電源遮断を行わなければならない。

(5) 不正アクセス対策

① 情報システム管理者の措置事項

ア　使用されていないポートを閉鎖しなければならない。

イ　不正アクセスによるウェブページの改ざんを防止するため、データの書換えを検出するよう設定しなければならない。【推奨事項】

ウ　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】

② 攻撃の予告

情報システム管理者は、サーバ等に攻撃を受けることが明確になった場合は、システムの停止その他必要な措置を講じなければならない。

③ 記録の保存

情報システム管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）違反等の犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

④ 内部からの攻撃

情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末を利用した組合サーバ等に対する攻撃及び外部サイトに対する攻撃の有無について、監視しなければならない。【推奨事項】

⑤ 職員等による不正アクセス

情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

(6) セキュリティ情報の収集

① セキュリティホールに関する情報の収集、共有等

情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じて、関係者間で共有しなければならない。この場合において、当該セキュリティホールの緊急度に応じて、ソフトウエア更新等の対策を実施しなければならない。

② 不正プログラム等のセキュリティ情報の収及び周知

情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じて、職員等に周知しなければならない。

8 運用

(1) 情報システムの監視

① 情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 情報システム管理者は、重要なアクセスログ等を取得するため、サーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③ 情報システム管理者は､外部と常時接続するシステムを常時監視しなければならない。

【推奨事項】

(2) 情報セキュリティポリシーの遵守状況の確認

① 遵守状況の確認及び対処

ア 情報システム管理者は､情報セキュリティポリシーの遵守状況について確認を行い、問題があると認めた場合は、速やかに、情報セキュリティ責任者に報告し、発生した問題について、適切に対処しなければならない。

イ 情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合は、適切かつ速やかに対処しなければならない。

② 職員等の報告義務

職員等は、情報セキュリティポリシーに対する違反行為を発見した場合は、直ちに、情報システム管理者に報告しなければならない。

(3) 侵害時の対応

情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合は、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施しなければならない。

(4) 情報システムの外部委託

① 外部委託先の選定基準

情報セキュリティ管理者は、外部委託先の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② 契約項目

情報システムの運用等を外部委託する場合は、委託事業者との間で必要に応じて、次に掲げる事項を明記した契約を締結しなければならない。

ア 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

イ 委託先の責任者、委託内容、作業者及び作業場所の特定

ウ 提供されるサービスレベルの保証

エ 従業員に対する教育の実施

オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
カ　業務上知り得た情報の守秘義務
キ　委託業務終了時の情報資産の返還、廃棄等
ク　委託業務の定期報告及び緊急時報告義務
ケ　組合による監査又は検査
コ　組合による事故等の公表
サ　情報セキュリティポリシーが遵守されなかった場合の規定
シ　その他情報セキュリティに関する事項

③　確認、措置等

情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じて、②の契約に基づく措置をしなければならない。

(5) 例外措置

①　例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合は、情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

②　緊急時の例外措置

情報セキュリティ管理者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、当該例外措置を実施後、速やかに、情報セキュリティ責任者に報告しなければならない。

③　例外措置の申請書の管理

情報セキュリティ責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

(6) 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次に掲げる法令その他の関係法令を遵守しなければならない。

①　地方公務員法(昭和25年法律第261号)
②　著作権法（昭和45年法律第48号）
③　不正アクセス行為の禁止等に関する法律
④　行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）
⑤　新潟県市町村総合事務組合個人情報保護条例（平成18年条例第2号）

(7) 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

9　評価及び見直し

(1) 監査

①　実施方法

情報セキュリティ委員会は、情報システム担当者をして情報ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的又は必要に応じて、監査を行わせなければならない。

② 監査実施計画の立案及び実施への協力

ア 情報システム担当者は、監査を行うに当たっては、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

③ 外部委託事業者に対する監査

情報システム担当者は、外部委託事業者に委託している場合は、外部委託事業者から下請として受託している事業者も含めて情報セキュリティポリシーの遵守について、監査を定期的又は必要に応じて行わなければならない。

④ 報告

情報システム担当者は、監査結果を取りまとめ、情報セキュリティ委員会に報告しなければならない。

⑤ 保管

情報システム担当者は、監査の実施によって、収集した監査証拠又は監査報告書の作成のための監査調書を適切に保管しなければならない。

⑥ 監査結果への対応

情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。

⑦ 情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し時に活用しなければならない。

(2) 自己点検

① 実施方法

ア 情報システム管理者は、情報ネットワーク及び情報システムについて、必要に応じて、自己点検を実施しなければならない。

イ 情報セキュリティ管理者は、情報システム管理者の行う点検について、協力しなければならない。

② 報告

情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

③ 自己点検結果の活用

ア 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ 情報セキュリティ委員会は、点検結果を情報セキュリティポリシーの見直し時に活用しなければならない。

(3) 情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合は、その見直しを行うものとする。