八日市布引ライフ組合訓令第１号

八日市布引ライフ組合情報セキュリティポリシーを次のとおり制定する。

令和８年２月27日

八日市布引ライフ組合管理者　小　椋　正　清

八日市布引ライフ組合情報セキュリティポリシー

目次

第75条（障害記録）
第76条（ネットワークの接続制御、経路制御等）
第77条
第78条（外部ネットワークとの接続制限等）
第79条
第80条
第81条
第82条
第83条（複合機のセキュリティ管理）
第84条
第85条
第86条（無線LAN及びネットワークの盗聴対策）
第87条
第88条（電子メールのセキュリティ管理）
第89条
第90条（電子メールの利用制限）
第91条
第92条
第93条（電子署名及び暗号化）
第94条（無許可ソフトウェアの導入等の禁止）
第95条
第96条
第97条（機器構成の変更の制限）
第98条
第99条（業務外ネットワークへの接続の禁止）
第100条（業務以外の目的でのウェブ閲覧の禁止）
第101条（ウェブ会議サービスの利用時の対策）
第102条
第103条
第104条
第２項　アクセス制御
第105条（アクセス制御）
第106条（利用者IDの取扱い）
第107条（職員等による外部からのアクセス等の制限）

第１章　総則

（目的）

第１条　この訓令は、八日市布引ライフ組合（以下「組合」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、組合が実施する情報セキュリティ対策についての基本的な事項（以下「基本方針」という。）及び基本方針を実行に移すため

の情報セキュリティ対策の基準（以下「対策基準」という。）を定めることを目的とする。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 情報セキュリティポリシー　基本方針及び対策基準をいう。

(2) 情報資産　紙、電磁媒体、フィルム等の記録媒体に記録された全ての情報及び情報システムの総称をいう。

(3) ネットワーク　コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(4) インターネット　異なるネットワーク同士を相互に接続することにより、世界中に広がったネットワーク環境をいう。

(5) 情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(6) 情報セキュリティ　情報資産の機密性、完全性及び可用性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(7) 機密性　情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(8) 完全性　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(9) 可用性　情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

第２章　情報セキュリティ基本方針

（対象とする脅威）

第３条　情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　この訓令が適用される範囲は、それぞれ次のとおりとする。

(1) 行政機関の範囲　八日市布引ライフ組合個人情報の保護に関する法律施行条例（令和５年八日市布引ライフ組合条例第１号）第２条に規定する実施機関及び議会とする。

(2) 情報資産の範囲　次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

（職員等の遵守義務）

第５条　職員、定年前再任用短時間勤務職員、会計年度任用職員、労働派遣契約等により組合の業務に従事する者（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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を遵守しなければならない。

（情報セキュリティ対策）

第６条　組合は、第４条の脅威から情報資産を保護するために、次の各号に掲げる区分に応じ、当該各号に定める情報セキュリティ対策を講じる。

(1) 組織体制　組合の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理　組合の保有する情報資産の機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 物理的セキュリティサーバ、通信回線、職員等のパーソナルコンピュータ等の管理について、物理的な対策を講ずる。

(4) 人的セキュリティ　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講ずる。

(5) 技術的セキュリティ　コンピュータ等の管理､アクセス制御､不正プログラム対策、不正アクセス対策等の技術的対策を講ずる。

(6) 運用　情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(7) 業務委託及び外部サービス(クラウドサービス)の利用　業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。また、ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(8) 評価・見直し　情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第７条　情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８条　前条の情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直すものとする。

（対策基準の策定）

第９条　情報資産に対し情報セキュリティ対策を講じるに当たり、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、対策基準の策定に当たっては、情報セキュリティ対策を行う上で必要となる基本的な要件、実施手順の策定、監視方法や評価及び運用の見直し等の事項について明記することとする。

（情報セキュリティポリシーの公開）

第10条　情報セキュリティポリシーは、組合ホームページにおいて公開し、組合の情報セキュリティマネジメントの取り組み方を外部に表明する。なお、情報セキュリティ実施手順は、公にすることにより組合の業務運営に重大な支障を及ぼすおそれがあることから非公開とする。

第３章　情報セキュリティ対策基準

第１節　組織体制

（行政機関）

第11条　この対策基準が適用される行政機関は、八日市布引ライフ組合個人情報の保護に関する法律施行条例（令和５年八日市布引ライフ組合条例第１号）第２条に規定する実施機関及び議会とする。

（最高情報セキュリティ責任者）

第12条　管理者は､情報セキュリティ対策を推進及び管理するための組織体制を整備する。

２　管理者は、前項の組織に係る事務を総括するため、最高情報セキュリティ責任者（Chief Information Security Officer、以下「CISO」という。）を置き、八日市布引ライフ組合規約（昭和41年３月３日許可滋賀県指令地第251号）第10条第２項に規定する副管理者をもって充てる。

３　第１項の組織に関し必要な事項は、別に定める。

（総括情報セキュリティ責任者）

第13条　事務局長を総括情報セキュリティ責任者とし、CISOを補佐する。

２　総括情報セキュリティ責任者は、組合のネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

（情報セキュリティ責任者）

第14条　事務局次長を情報セキュリティ責任者とし、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約、職員等に対する必要な助言及び指示を行う。

２　情報セキュリティ責任者は、組合全般における開発、設定の変更、運用、見直し等を行う総括的な権限及び責任を有する。

３　前項の情報システムにおける開発、設定の変更、運用、見直し等は、組合の情報セキュリティポリシーに則ったものであり、他の情報システムと調和して機能を果たすものでなければならない。

４　第２項の情報システムにおける開発、設定の変更、運用、見直し等を行う場合は、情報システム管理者と協議しなければならない。

（情報セキュリティ管理者）

第15条　所属長等を情報セキュリティ管理者とし、その所管する所属等の情報セキュリティ対策が円滑に実施されるよう努めなければならない。

２　情報セキュリティ管理者は、その所掌する所属等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、総括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

（管理責任）

第16条　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。

２　情報資産が複製又は伝送された場合には、複製等された情報資産も前条の分類に基づき管理しなければならない。

（情報システム管理者）

第17条　総務課長を情報システム管理者とし、組合の情報システムを管理し、開発、設定の変更、運用、見直し等に関し必要な調整を行う権限及び責任を有する。

２　組合のネットワークに接続しないで単独で運用する情報システムにあっては、前項の規定にかかわらず、当該システムを所管する所属長を情報システム管理者とする。

（情報セキュリティ委員会）

第18条　本組合の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会を設置し、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

第２節　情報資産の分類と管理方法

（情報資産の分類）

第19条　組合における情報資産の分類は、機密性、完全性及び可用性により、別表のとおり分類し、必要に応じ取扱制限を行うものとする。

（分類の明示）

第20条　職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限事項を明示して、適切な管理を行わなければならない。

（情報の作成）

第21条　業務に係る情報を作成する者は、情報の作成時に第18条の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。

２　業務に係る情報を作成する者は、作成途上の情報についても紛失や流出等を防止し、情報の作成途上で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。

（情報資産の入手）

第22条　庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

２　庁外の者が作成した情報資産を入手した者は、前項の分類に準じ当該情報の分類と取扱制限を定めなければならない。

３　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、情報セキュリティ管理者の指示に従わなければならない。

（情報資産の利用）

第23条　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。

２　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

３　情報資産を利用する者は、電磁的記録媒体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、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（情報資産の保管）

第24条　情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

２　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的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。

３　情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や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電磁的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地域に保管しなければならない。

４　情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

（情報の送信）

第25条　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、必要に応じパスワード等による暗号化を行わなければならない。

（情報資産の運搬）

第26条　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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。

２　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。

（情報資産の提供及び公表）

第27条　機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化の設定を行わなければならない。

２　機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

３　前項の場合において、情報セキュリティ管理者は、総括情報セキュリティ責任者に当該情報資産の外部への提供に関し、協議しなければならない。

４　情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

（情報資産の廃棄）

第28条　機密性２以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

２　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

３　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なければならない。

第３節　物理的セキュリティ

（機器の取付け）

第29条　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、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（サーバの冗長化）

第30条　情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

２　情報システム管理者は、メインサーバに障害が発生した場合、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

（機器の電源）

第31条　情報システム管理者は､総括情報セキュリティ責任者及び施設管理部門と連携し、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、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容量の予備電源を備え付けなければならない。

２　情報システム管理者は、総括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、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。

（機器の定期保守及び修理）

第32条　情報システム管理者及び情報システム所管管理者は、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。

２　情報システム管理者は、電磁的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。

３　情報システム管理者及び情報システム所管管理者は、前項の場合において内容を消去できない場合、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（庁外への機器の設置）

第33条　総括情報セキュリティ責任者及び情報セキュリティ責任者は、庁外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。

２　総括情報セキュリティ責任者及び情報セキュリティ責任者は、庁外にサーバ等の機器を設置した場合、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。

（機器の廃棄等）

第34条　情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全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。

第35条　情報システム管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理し、かつ、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

第36条　総括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

第37条　総括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

第38条　総括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報の破壊、盗聴、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。

第39条　総括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択し、必要に応じ回線を冗長構成にする等の措置を講じなければならない。

第40条　情報システム管理者は、盗難防止のため、執務室等で利用するパーソナルコンピュータ、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

第41条　情報システム管理者は、情報システムへのログインに際し、パスワード、生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

第42条　情報システム管理者は、パーソナルコンピュータやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合についても、同様とする。

２　情報システム管理者は、電磁的記録媒体についてデータ暗号化機能を備える媒体を使用しなければならない。

３　情報システム管理者は、モバイル端末の庁外での業務利用の際は、遠隔消去機能を利用する等の措置を講じなければならない。

第４節　人的セキュリティ

（情報セキュリティポリシー等の遵守）

第43条　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しなければならない。

２　職員等は、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、指示を受けなければならない。

（業務以外の目的での使用の禁止）

第44条　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及びインターネットへのアクセスを行ってはならない。

（モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限）

第45条　CISOは、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

２　職員等は、本組合のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

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

（支給以外のパーソナルコンピュータ､モバイル端末及び電磁的記録媒体等の業務利用）

第46条　職員等は、支給以外のパーソナルコンピュータ、モバイル端末及び電磁的記録媒体等を原則として業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

２　職員等は、支給以外のパーソナルコンピュータ、モバイル端末及び電磁的記録媒体等を用いる場合、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

３　職員等は、機密性３の情報資産については、支給以外のパーソナルコンピュータ又はモバイル端末による情報処理を行ってはならない。

（持ち出し及び持込みの記録）

第47条　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、記録を作成し、保管しなければならない。

（パーソナルコンピュータ等におけるセキュリティ設定変更の禁止）

第48条　職員等は、パーソナルコンピュータ及びモバイル端末のソフトウェアに関するセ

キュリティ機能の設定を情報システム管理者の許可なく変更してはならない。

（机上の端末等の管理）

第49条　職員等は、パーソナルコンピュータ、モバイル端末、電磁的記録媒体及び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情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパーソナルコンピュータ、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

（退職時等の遵守事項）

第50条　職員等は、異動、退職等により業務を離れる場合、利用していた情報資産を、返却しなければならない。

２　職員等は、退職後も業務上知り得た情報を漏らしてはならない。

（情報セキュリティポリシー等の掲示）

第51条　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。

（委託事業者に対する説明）

第52条　情報セキュリティ管理者は、ネットワーク及び情報システムの開発、保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（情報セキュリティに関する研修及び訓練）

第53条　総括情報セキュリティ責任者は、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

（研修計画の策定及び実施）

第54条　CISOは、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い､情報セキュリティ委員会の承認を得なければならない。

２　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研修を受講しなければならない。

３　新規採用の職員を対象とする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。

４　研修は、総括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム担当者その他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

５　情報セキュリティ管理者は、所管する所属等の研修の実施状況を記録し、総括情報セキュリティ責任者及び情報セキュリティ責任者に対して報告しなければならない。

６　総括情報セキュリティ責任者は、研修の実施状況を分析及び評価し、CISOに情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

７　CISOは、毎年度1回、情報セキュリティ委員会に対して、職員の情報セキュリティ研修の実施状況について報告しなければならない。

（緊急時対応訓練）

第55条　CISOは、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施できるようにしなければならない。

（研修及び訓練への参加）

第56条　職員等は、定められた研修及び訓練に参加しなければならない。

（庁内からの情報セキュリティインシデントの報告）

第57条　職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

第58条　報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者、情報システム管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

第59条　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてCISO及び総括情報セキュリティ責任者に報告しなければならない。

（住民等外部からの情報セキュリティインシデントの報告）

第60条　職員等は、組合が管理する情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

２　報告を受けた情報セキュリティ管理者は、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　前項の報告を受けた情報セキュリティ責任者は、必要に応じてCISO及び総括情報セキュリティ責任者に報告しなければならない。

第61条　総括情報セキュリティ責任者は、情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（情報セキュリティインシデント原因の究明、記録、再発防止等）

第62条　総括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした部署の情報セキュリティ管理者及び情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。

２　総括情報セキュリティ責任者は、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、CISOに報告しなければならない。

第63条　CISOは、総括情報セキュリティ責任者から情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を講じなければならない。

（IDの取扱い）

第64条　職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

(1) 自己が利用している ID を他人に利用させないこと。

(2) 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こと。

（パスワードの取扱い）

第65条　職員等は、パスワードを他者に知られないように管理しなければならない。

２　職員等は、パスワードを秘密にし、関係者以外からのパスワードの照会等には一切応じてはならない。

３　職員等は、パスワードを十分な長さとし、文字列は想像しにくいものにしなければならない。

４　職員等は、パスワードが流出したおそれがある場合には、情報システム管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

５　職員等は、パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

６　職員等は、複数の情報システムを扱う場合は、同一のパスワードをシステム間で用いてはならない。

７　職員等は、仮のパスワードは、最初のログイン時点で変更しなければならない。

８　職員等は、サーバ、ネットワーク機器及びパーソナルコンピュータ等の端末にパスワードを記憶させてはならない。

９　職員等は、職員等間でパスワード（共用IDに対するパスワードを除く。）を共有してはならない。

第５節　技術的セキュリティ

（文書サーバの設定等）

第66条　情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一所属等であっても、担当職員等以外の職員等が閲覧及び使用できないようにしなければならない。

（バックアップの実施）

第67条　総括情報セキュリティ責任者及び情報システム管理者は、業務システムのデータベース、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、

必要に応じて定期的にバックアップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第68条　情報システム管理者及は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、総括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

（システム管理記録及び作業の確認）

第69条　情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

第70条　情報システム管理者は、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、詐取、改ざん等をされないように適切に管理しなければならない。

第71条　情報システム管理者は、契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２人以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書等の管理）

第72条　情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧又は紛失することがないよう適切に管理しなければならない。

（ログの取得等）

第73条　情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

第74条　情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

（障害記録）

第75条　情報システム管理者は、職員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又は問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの接続制御、経路制御等）

第76条　総括情報セキュリティ責任者は、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ェア等を設定しなければならない。

第77条　総括情報セキュリティ責任者は、不正アクセスを防止するため、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。

（外部ネットワークとの接続制限等）

第78条　情報セキュリティ責任者は、所管する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、CISOの許可を得なければならない。

第79条　情報セキュリティ責任者及び情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

第80条　情報システム管理者は､接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

第81条　総括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、次に掲げるセキュリティ対策を実施しなければならない。

(1) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用すること。

(2) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じること。

(3) 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定すること。

(4) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講ずること。

第82条　情報システム管理者は、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には、総括情報セキュリティ責任者の判断に従い、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。

（複合機のセキュリティ管理）

第83条　総括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

第84条　総括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

第85条　総括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（無線LAN及びネットワークの盗聴対策）

第86条　情報システム管理者は、所管するシステムにおいて無線LANの利用を認める場合、総括情報セキュリティ責任者の承認を得なければならない。

２　情報システム管理者は、前項の無線LANの利用においては、解読が困難な暗号化及び認

証技術の使用を義務付けなければならない。

第87条　情報システム管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）

第88条　情報システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

第89条　情報システム管理者は、大量のスパムメール等の受信又は送信を検知した場合、メールサーバの運用を停止しなければならない。

（電子メールの利用制限）

第90条　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。

第91条　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、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。

第92条　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

（電子署名及び暗号化）

第93条　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、組合が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

（無許可ソフトウェアの導入等の禁止）

第94条　職員等は、パーソナルコンピュータやモバイル端末に無断でソフトウェアを導入してはならない。

第95条　職員等は、業務上の必要がある場合は、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て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

第96条　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。

（機器構成の変更の制限）

第97条　職員等は、パーソナルコンピュータやモバイル端末に対し機器の改造、増設及び交換を行ってはならない。

第98条　職員等は、業務上、パーソナルコンピュータやモバイル端末に対し機器の改造、増設及び交換を行う必要がある場合､情報システム管理者の許可を得なければならない。

（業務外ネットワークへの接続の禁止）

第99条　職員等は、支給されたパーソナルコンピュータ、モバイル端末等を、情報システ

ム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

（業務以外の目的でのウェブ閲覧の禁止）

第100条　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。

（ウェブ会議サービスの利用時の対策）

第101条　総括情報セキュリティ責任者は、ウェブ会議を適切に利用するための利用手順を定めなければならない。

第102条　職員等は、組合の定める利用手順に従い、ウェブ会議の参加者及び取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

第103条　職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

第104条　職員等は、外部からウェブ会議に招待される場合は、組合の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

（アクセス制御）

第105条　情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

（利用者IDの取扱い）

第106条　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、職員等の異動、出向、退職者に伴う利用者IDの取扱い等の方法を定めなければならない。

２　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、総括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

３　総括情報セキュリティ責任者及び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、人事管理部門と連携し、点検しなければならない。

（職員等による外部からのアクセス等の制限）

第107条　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合、情報システム管理者又は情報システム所管管理者の許可を得なければならない。

２　総括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

３　総括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

４　総括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

５　情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与

する場合、セキュリティ確保のために必要な措置を講じなければならない。

6　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得て、又は情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

7　総括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（自動識別の設定）

第108条　情報システム管理者及び情報システム所管管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（認証情報の管理）

第109条　情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

2　情報システム管理者及び情報システム所管管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

3　情報システム管理者及び情報システム所管管理者は、認証情報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。

（情報システムの調達）

第110条　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。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

2　情報システム管理者及び情報システム所管管理者は、機器及びソフトウェ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。

（システム開発における責任者及び作業者の特定）

第111条　情報システム管理者は、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。

（システム開発に用いるハードウェア及びソフトウェアの管理）

第112条　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

２　情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（アプリケーション及びコンテンツの開発時の対策）

第113条　情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

（開発環境と運用環境の分離及び移行手順の明確化）

第114条　情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

２　情報システム管理者及び情報システム所管管理者は、システム開発、保守及びテスト環境からシステム運用環境への移行について、システム開発、保守計画の策定時に手順を明確にしなければならない。

３　情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

４　情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

（テスト）

第115条　情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

２　情報システム管理者は、個人情報及び機密性の高いデータをテストデータに使用する場合、テスト後のデータの消去を職員に確認させなければならない。

３　情報システム管理者は、開発したシステムについて受入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

４　情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

（機器等の納入時又は情報システムの受入れ時）

第116条　情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認及び検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

２　情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（情報システムの基盤を管理又は制御するソフトウェア導入時の対策）

第117条　情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じなければならない。

（情報システムの基盤を管理又は制御するソフトウェア運用時の対策）

第118条　情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用又は保守する場合は、次に掲げるセキュリティ対策を実施しなければならない。

(1) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

(2) 脅威及び情報セキュリティインシデントを迅速に検知し、対応するための対策

２　情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

（システム開発又は保守に関連する資料等の整備及び保管）

第119条　情報システム管理者は、システム開発又は保守に関連する資料及びシステム関連文書を適切に整備し、かつ、保管しなければならない。

２　情報システム管理者及び情報システム所管管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について総括情報セキュリティ責任者に報告しなければならない。

３　情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次に掲げる内容を含む情報システム関連文書を整備しなければならない。

(1) 情報システムを構成するサーバ装置及び端末関連情報

(2) 情報システムを構成する通信回線及び通信回線装置関連情報

４　情報システム管理者及び情報システム所管管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次に掲げる内容を含む実施手順を整備しなければならない。

(1) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(2) 情報セキュリティインシデントを認知した際の対処手順及び情報システムが停止した際の復旧手順

５　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。

６　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。

第120条　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。

（開発及び保守用のソフトウェアの更新等）

第121条　情報システム管理者は、開発又は保守用のソフトウェア等の更新又はパッチの適用をする場合、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。

（システム更新又は統合時の検証等）

第122条　情報システム管理者は、システム更新又は統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。

（情報システムについての対策の見直し）

第123条　情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、組合内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。この場合において、見直しの結果については、総括情報セキュリティ責任者へ報告しなければならない。

（総括情報セキュリティ責任者の措置事項）

第124条　総括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 外部ネットワークから受信したファイルは、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を防止すること。

(2) 外部ネットワークに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不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止すること。

(3) 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、必要に応じ職員に対して注意喚起すること。

(4) 所掌するサーバ及びパーソナルコンピュータ等の端末に、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ェアを常駐させること。

(5) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。

(6) 不正プログラム対策のソフトウェアは、常に最新の状態に保つこと。

(7) 業務で利用するソフトウェアは、パッチ、バージョンアップ等の開発元のサポートが終了したソフトウェアを利用しないこと。また、当該製品の利用を予定している期

間中にパッチ、バージョンアップ等の開発元のサポートが終了する予定がないことを確認すること。

（情報システム管理者の措置事項）

第125条　情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(1) 所掌するサーバ及びパーソナルコンピュータ等の端末に、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ェアを常駐させること。

(2) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。

(3) 不正プログラム対策のソフトウェアは、常に最新の状態に保つこと。

(4) インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、組合が管理している媒体以外を職員等に利用させないこと。

(5) 不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施すること。

(6) 不正プログラム対策ソフトウェア等の設定の変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならないこと。

（職員等の遵守事項）

第126条　職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

(1) パーソナルコンピュータやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合、当該ソフトウェアの設定を変更しないこと。

(2) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行うこと。

(3) 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除すること。

(4) 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施すること。

(5) ファイルが添付され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ェアでチェックを行うこと。また、インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN接続系に取り込む場合は、無害化すること。

(6) 総括情報セキュリティ責任者が提供するウイルス情報を常に確認すること。

(7) 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又は感染が疑われる場合

は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行うこと。また、初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外し、通信を行わない設定への変更等を実施すること。

（専門家の支援体制）

第127条　総括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（総括情報セキュリティ責任者の措置事項）

第128条　総括情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。

(1) 使用されていないポートを閉鎖すること。

(2) 不要なサービスについて、機能を削除又は停止すること。

(3) 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し、情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定すること。

(4) 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すること。

２　総括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応等を実施できる体制並びに連絡網を構築しなければならない。

（攻撃への対処）

第129条　CISO及び総括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。この場合において、関係機関と連絡を密にして情報の収集に努めなければならない。また、総務省、都道府県、市町等と連絡を密にして情報の収集に努めなければならない。

（記録の保存）

第130条　CISO及び総括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、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。

（内部からの攻撃）

第131条　総括情報セキュリティ責任者及び情報システム管理者は、職員等及び委託事業者が使用しているパーソナルコンピュータ等の端末からの庁内のサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。

（職員等による不正アクセス）

第132条　総括情報セキュリティ責任者及び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、当該職員等が所属する所属等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。

（サービス不能攻撃）

第133条　総括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）

第134条　総括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）及び内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

（セキュリティホールに関する情報の収集、共有及びソフトウェアの更新等）

第135条　総括情報セキュリティ責任者及び情報システム管理者は、サーバ装置、端末、通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。

２　総括情報セキュリティ責任者及び情報システム管理者は、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（不正プログラム等のセキュリティ情報の収集及び周知）

第136条　総括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）

第137条　総括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第６節　運用

（情報システムの運用及び保守時の対策）

第138条　総括情報セキュリティ責任者及び情報システム管理者は、情報システムの運用及び保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運

用しなければならない。

2　総括情報セキュリティ責任者及び情報システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

3　総括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

（情報システムの監視機能）

第139条　総括情報セキュリティ責任者及び情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

2　総括情報セキュリティ責任者及び情報システム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

3　総括情報セキュリティ責任者及び情報システム管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象及び手法を定期的に見直さなければならない。

4　総括情報セキュリティ責任者及び情報システム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

（情報システムの監視）

第140条　総括情報セキュリティ責任者及び情報システム管理者は、情報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　総括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得する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　総括情報セキュリティ責任者及び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。

4　総括情報セキュリティ責任者及び情報システム管理者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

（遵守状況の確認及び対処）

第141条　総括情報セキュリティ責任者及び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、問題を認めた場合、速やかにCISO及び総括情報セキュリティ責任者に報告しなければならない。

2　CISOは、発生した問題について、適切かつ速やかに対処しなければならない。

3　総括情報セキュリティ責任者及び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、問題が発生した場合には適切かつ速やかに対処しなければならない。

（パーソナルコンピュータ、モバイル端末、電磁的記録媒体等の利用状況調査）

第142条　CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパーソナルコンピュータ、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（職員等の対処義務）

第143条　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、直ちに総括情報セキュリティ責任者及び情報セキュリティ管理者に報告しなければならない。

２　職員等は、違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると総括情報セキュリティ責任者が判断した場合、緊急時対応計画に従って適切に対処しなければならない。

（緊急時対応計画の策定）

第144条　CISOは、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において、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するため、緊急時対応計画を定め、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（緊急時対応計画に盛り込むべき内容）

第145条　緊急時対応計画には、次の内容を定めなければならない。

(1) 関係者の連絡先

(2) 発生した事案に係る報告すべき事項

(3) 発生した事案への対応措置

(4) 再発防止措置の策定

（業務継続計画との整合性確保）

第146条　CISO又は情報セキュリティ委員会は、自然災害、大規模又は広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（緊急時対応計画の見直し）

第147条　CISO又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（例外措置の許可）

第148条　情報セキュリティ管理者及び情報システム管理者は、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、行政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には、CISOの許可を得て、例外措置を取ることができる。

（緊急時の例外措置）

第149条　情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合において、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

（例外措置の申請書の管理）

第150条　CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

第151条　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、次の法令のほか関係法令を遵守し、これに従わなければならない。

(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（平成11年法律第128号）

(4) 個人情報の保護に関する法律（平成15年法律第57号）

(5) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）

(6) サイバーセキュリティ基本法（平成26年法律第104号）

（懲戒処分）

第152条　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。

（違反時の対応）

第153条　職員等の情報セキュリティポリシーに違反する行動を確認した場合、職員等は、所属する情報セキュリティ責任者に違反内容を報告しなければならない。

２　前項の報告を受けた情報セキュリティ責任者は、違反者が属する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　総括情報セキュリティ責任者が違反を確認した場合、総括情報セキュリティ責任者は、当該職員等が所属する所属等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

４　情報システム管理者が違反を確認した場合、違反を確認した者は、速やかに総括情報セキュリティ責任者及び当該職員等が所属する所属等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

５　総括情報セキュリティ責任者は、情報セキュリティ管理者の指導によっても改善され

ない場合、当該職員等のネットワーク又は情報システムを使用する権利を停止し、又は剥奪することができる。

6　総括情報セキュリティ責任者は、前項の規定に基づき職員等の権利を停止し、又は剥奪したときは、CISO及び当該職員等が所属する所属等の情報セキュリティ管理者にその旨を通知しなければならない。

7　第１項の場合において、情報セキュリティ責任者が違反者であったときは、総括情報セキュリティ責任者に報告するものとする。

第７節　業務委託及び外部サービス（クラウドサービス）の利用

（業務委託に係る運用規程の整備）

第154条　総括情報セキュリティ責任者は、業務委託に係る次に掲げる内容を含む運用規程を整備しなければならない。

(1) 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準(以下「委託判断基準」という。)

(2) 委託事業者の選定基準

（外部委託実施前の対策）

第155条　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、次に掲げる内容を含む事項を実施しなければならない。

(1) 委託する業務内容の特定

(2) 委託事業者の選定条件を含む仕様の策定

(3) 仕様に基づく委託事業者の選定

（契約項目）

第156条　情報システム管理者は、情報システムの運用、保守等を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。

(1) 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

(2) 委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定

(3) 提供されるサービスレベルの保証

(4) 委託事業者にアクセスを許可する情報の種類及び範囲、アクセス方法の明確化等、情報のライフサイクル全般での管理方法

(5) 委託事業者の従業員に対する教育の実施

(6) 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

(7) 業務上知り得た情報の守秘義務

(8) 再委託に関する制限事項の遵守

(9) 委託業務終了時の情報資産の返還、廃棄等

(10) 委託業務の定期報告及び緊急時報告義務
(11) 組合による監査及び検査
(12) 組合による情報セキュリティインシデント発生時の公表
(13) 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（損害賠償等）

（秘密保持契約）

第157条　委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）を締結しなければならない。

２　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、次に掲げる内容を含む事項の実施を委託事業者に求めなければならない。

(1) 仕様に準拠した提案
(2) 契約の締結
(3) 委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

（業務委託実施期間における対策）

第158条　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、次に掲げる内容を含む対策を実施しなければならない。

(1) 委託判断基準に従った重要情報の提供
(2) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
(3) 総括情報セキュリティ責任者（重要度に応じ、CISO）へ措置内容の報告
(4) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断等の必要な措置を含む契約に基づく対処の要求

２　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、次に掲げる内容を含む対策の実施を委託事業者に求めなければならない。

(1) 情報の適正な取扱いのための情報セキュリティ対策
(2) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
(3) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における委託事業の一時中断等の必要な措置を含む対処

（業務委託終了時の対策）

第159条　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、次に掲げる内容を含む対策を実施しなければならない。

(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含

む検収

(2) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

2　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、次に掲げる内容を含む対策の実施を委託事業者に求めなければならない。

(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(2) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

（情報システムに関する業務委託における共通的対策）

第160条　情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに組合の意図しない変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

（情報システムの構築を業務委託する場合の対策）

第161条　情報システム管理者は、情報システムの運用又は保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

2　情報システム管理者は、情報システムの運用及び保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めなければならない。

（本組合向けに情報システムの一部の機能を提供するサービスを利用する場合の対策）

第162条　情報システム管理者又は情報セキュリティ管理者は、外部の一般の者が本組合向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

2　情報システム管理者又は情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

3　情報システム管理者又は情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的かつ客観的に評価し判断しなければならない。

4　情報システム管理者又は情報セキュリティ管理者は、業務委託サービスを利用する場合には、総括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。

5　総括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利

用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

6　総括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

（外部サービスの選定に係る運用規定の整備）

第163条　総括情報セキュリティ責任者は、機密性２以上の情報を取り扱う場合、次に掲げる外部サービス（クラウドサービス）（以下「クラウドサービス」という。）の選定に関する規定を整備しなければならない。

(1) クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「クラウドサービス利用判断基準」という。）

(2) クラウドサービス提供者の選定基準

(3) クラウドサービスの利用申請の許可権限者及び利用手続

(4) クラウドサービス管理者の指名及びクラウドサービスの利用状況の管理

（クラウドサービスの選定）

第164条　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従ってクラウドサービスの利用を検討しなければならない。

2　情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定しなければならない。この場合において、次に掲げる内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

(1) クラウドサービスの利用を通じて組合が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

(2) クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制

(3) クラウドサービスの提供に当たり、クラウドサービス提供者又はその従業員、再委託先その他の者によって、組合の意図しない変更が加えられないための管理体制

(4) クラウドサービス提供者の資本関係、役員等の情報並びにクラウドサービス提供に従事する者の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報提供並びに調達仕様書による施設の場所及びリージョンの指定

(5) 情報セキュリティインシデントへの対処方法

(6) 情報セキュリティ対策その他の契約の履行状況の確認方法

(7) 情報セキュリティ対策の履行が不十分な場合の対処方法

3　情報セキュリティ責任者は、クラウドサービスの中断及び終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。

4　情報セキュリティ責任者は、クラウドサービスの利用を通じて組合が取り扱う情報の

格付等を勘案し、必要に応じて次に掲げる内容をクラウドサービス提供者の選定条件に含めなければならない。

(1) 情報セキュリティ監査の受入れ

(2) サービスレベルの保証

5　情報セキュリティ責任者は、クラウドサービスの利用を通じて組合が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて組合の情報が取り扱われる場所並びに契約に定める準拠法及び裁判管轄を選定条件に含めなければならない。

6　情報セキュリティ責任者は、クラウドサービス提供者がその役務内容の一部を再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を組合に提供し、組合の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

7　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定しなければならない。また、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。

8　情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めなければならない。

9　総括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定及び認証制度の適用状況等から、クラウドサービス提供者の信頼性が十分であることを総合的及び客観的に評価し判断しなければならない。

（クラウドサービスの利用に係る調達及び契約）

第165条　情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

2　情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

（クラウドサービスを利用した情報システムの導入及び構築時の対策）

第166条　総括情報セキュリティ責任者は、クラウドサービスの特性、責任分界点に係る考え方等を踏まえ、次に掲げる内容を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

(1) 不正なアクセスを防止するためのアクセス制御

(2) 取り扱う情報の機密性保護のための暗号化

(3) 開発時におけるセキュリティ対策

(4) 設計及び設定時の誤りの防止

２　クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状況を確認及び記録しなければならない。

（クラウドサービスを利用した情報システムの運用及び保守時の対策）

第167条　総括情報セキュリティ責任者は、クラウドサービスの特性及び責任分界点に係る考え方を踏まえ、次に掲げる内容を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

(1) クラウドサービス利用方針の規定

(2) クラウドサービス利用に必要な教育

(3) 取り扱う資産の管理

(4) 不正アクセスを防止するためのアクセス制御

(5) 取り扱う情報の機密性保護のための暗号化

(6) クラウドサービス内の通信の制御

(7) 設計及び設定時の誤りの防止

(8) クラウドサービスを利用した情報システムの事業継続

２　情報セキュリティ責任者は、クラウドサービスの特性及び責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

３　クラウドサービス管理者は、前２項において定める規定に対し、運用及び保守時に実施状況を定期的に確認及び記録しなければならない。

（クラウドサービスを利用した情報システムの更改及び廃棄時の対策）

第168条　総括情報セキュリティ責任者は、クラウドサービスの特性及び責任分界点に係る考え方を踏まえ、次に掲げる内容を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

(1) クラウドサービスの利用終了時における対策

(2) クラウドサービスで取り扱った情報の廃棄

(3) クラウドサービスの利用のために作成したアカウントの廃棄

２　クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認及び記録しなければならない。

第８節　評価及び見直し

（実施方法）

第169条　CISOは、情報セキュリティ監査責任者を指名し、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、毎年度及び必要に応じて監査を行わせなければならない。

（監査を行う者の要件）

第170条　情報セキュリティ監査責任者は、監査を実施する場合、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

２　監査を行う者は、監査及び情報セキュリティに関する専門知識を有するものでなければならない。

（監査実施計画の立案及び実施への協力）

第171条　情報セキュリティ監査責任者は、監査を行うに当たって、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。

２　被監査部門は、監査の実施に協力しなければならない。

（外部委託事業者に対する監査）

第172条　外部委託事業者に監査を委託している場合、情報セキュリティ監査責任者は外部委託事業者から下請け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。

（報告）

第173条　情報セキュリティ監査責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

（保管）

第174条　情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第175条　CISO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。

２　CISOは、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

３　CISOは、庁内で横断的に改善が必要な事項については、総括情報セキュリティ責任者

に対し、当該事項への対処を指示しなければならない。

（情報セキュリティポリシー及び関係規程等の見直し等への活用）

第176条　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及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（実施方法）

第177条　総括情報セキュリティ責任者、情報システム管理者及び情報システム所管管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

２　情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する課における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（報告）

第178条　総括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、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。

（自己点検結果の活用）

第179条　職員等は、前条の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。

２　情報セキュリティ委員会は、前条の自己点検結果を情報セキュリティポリシー及び関係規程等の見直しその他情報セキュリティ対策の見直し時に活用しなければならない。

第180条　情報セキュリティ委員会は、情報セキュリティ監査及び第201条の自己点検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、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。この場合において、横断的に改善が必要となる情報セキュリティ対策の運用の見直しについては、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてCISOに報告しなければならない。

第４章　その他

（その他）

第181条　この訓令の施行に関し必要な事項は、管理者が別に定める。

附　則

この訓令は、令和８年４月１日から施行する。

別表（第19条関係）

１　機密性による情報資産の分類

分類	分類基準	取扱制限

機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給された端末以外での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬又は提供時における暗号化、パスワード設定及び鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、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又は機密性３の情報資産以外の情報資産	

２　完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政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 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体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の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のう	・バックアップ、指定する時間以

	ち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政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	内の復旧 ・電磁的記録媒体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	