水戸市議会情報セキュリティ対策基準

１　目的

水戸市議会情報セキュリティ基本方針に位置づけた情報セキュリティ対策等を実行に移すため、水戸市議会情報セキュリティ対策基準（以下「対策基準」という。）を定めるものである。

なお、対策基準において、以下で使用する用語の定義は、水戸市議会情報セキュリティ基本方針の例によるものとする。

２　組織体制

(1) 最高情報セキュリティ責任者（CISO: Chief Information Security OffiCer、以下「CISO」という。）

ア　議長をCISOとする。CISOは、議会における情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　CISOは、最高情報セキュリティ副責任者(以下「副CISO」という。)１名を必要に応じて置くことができる。副CISOは、CISOを助けて本市議会における情報セキュリティに関する事務を整理し、CISOの命を受けて本市議会の情報セキュリティに関する事務を統括する。

ウ　CISOは、対策基準に定められた自らの担務を、副CISOその他の対策基準に定める責任者に担わせることができる。

(2) 情報セキュリティ責任者

ア　議会事務局長を情報セキュリティ責任者とする。情報セキュリティ責任者は、CISO及び副CISOを補佐しなければならない。

イ　情報セキュリティ責任者は、議会の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。

ウ　情報セキュリティ責任者は、議会が管理する情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

エ　情報セキュリティ責任者は、議会が管理する情報システムについて、緊急時等における連絡体制の整備、水戸市議会情報セキュリティポリシー（以下「セキュリティポリシー」という。）の遵守に関する意見の集約並びに議員及び職員に対する教育、訓練、助言及び指示を行う。

(3) 情報セキュリティ管理者

ア　議会事務局総務課長を情報セキュリティ管理者とする。

イ　情報セキュリティ管理者は、議会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。

ウ　情報セキュリティ管理者は、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。

(4) 情報システム管理者

ア　各情報システムを所管する課の課長補佐を情報システム管理者とする。

イ　情報システム管理者は、所管する情報システムの開発、設定の変更、運用、見直し等を

行う権限及び責任を有する。

ウ　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に関する権限及び責任を有する。

エ　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持及び管理を行う。

(5) 情報システム担当者

ア　各情報システムを所管する課の担当係長を情報システム担当者とする。

イ　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、設定の変更、運用、更新等の作業を行う。

(6) 兼務の禁止

ア　情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ　情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(7) 水戸市議会 CSIRT の設置・役割

ア　CISO は、セキュリティポリシーの適用範囲に関わる情報セキュリティインシデントに迅速かつ適切に対処するための体制として水戸市議会 CSIRT※（以下「議会 CSIRT」という。）整備し、その役割を明確化しなければならない。

イ　議会 CSIRT の設置及び運営に関し必要な事項は、CISO が別に定める。

ウ　CISO は、議会 CSIRT に所属する職員等を選任し、その中から議会 CSIRT 責任者を置かなければならない。また、議会 CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

エ　CISO は、情報セキュリティに関する窓口を議会事務局総務課に設置する。

オ　CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

カ　情報セキュリティインシデントを認知した場合には、CISO、市長公室デジタルイノベーション課等へ報告しなければならない。

キ　情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知又は公表等の対応を行わなければならない。

ク　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

※CSIRT：Computer Security Incident Response Team

３　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、必要に応じて取り扱いを制限するものとする。

ア　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３Ａ	情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・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・提供時における暗号化・パスワード設定や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３Ｂ	情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報	
機密性３Ｃ	情報資産のうち、機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
機密性２	情報資産のうち、機密性３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	―

イ　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	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議会運営に支障（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の情報資産以外の情報資産	―

ウ　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	情報資産のうち、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議会の安定的な運営に支障（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、指定する時間以内の復旧 ・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	－

(2) 情報資産の管理

ア　管理責任

(ｱ) 情報セキュリティ管理者は、情報資産について管理責任を有する。

(ｲ) 情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

(ｳ) 情報セキュリティ管理者は、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(1)の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

議員及び職員は、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についても明示する等適正な管理を行わなければならない。

ただし、機密性、完全性及び可用性の全てにおいて１に分類されるものは、この限りでない。

ウ　情報の作成

(ｱ) 議員及び職員は、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)の分類に基づき、当該情報の分類と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、作成途上の情報についても、紛失や流出等を防止しなければならない。また、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。

エ　情報資産の入手

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に判断を仰がなければならない。

オ　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、情報資産の分類に応じ、適正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、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。

カ　情報資産の保管

(ｱ) 情報セキュリティ管理者及び情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

(ｲ) 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。

(ｳ) 情報セキュリティ管理者及び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。

キ　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、パスワード等による暗号化を行わなければならない。

ク　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、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。

(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。

ケ　情報資産の提供・公表

(ｱ) 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を行わなければならない。

(ｲ) 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。

(ｳ) 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。

コ　情報資産の廃棄等

(ｱ) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(ｲ) 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者の氏名及び処理内容を記録しなければならない。

(ｳ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

４　情報システム全体の強靭性の向上

(1) マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナ

ンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

イ　情報のアクセス及び持ち出しにおける対策

(ｱ) 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

(ｲ) 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(2) LGWAN 接続系

ア　LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。

なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

(ｱ) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

(ｲ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(ｳ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3) インターネット接続系

ア　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

イ　インターネット接続系に議員及び職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

５　物理的セキュリティ

5-1　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、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正に固定する等、必要な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、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、当該機器が適正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。

イ　情報システム管理者は、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。

(3) 通信ケーブル等の配線

ア　情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、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必要な措置を講じなければならない。

イ　情報セキュリティ責任者及び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、連携して対応しなければならない。

ウ　情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口(ハブのポート等)を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

エ　情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

(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、電磁的記録媒体を内蔵する機器を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。内容を消去できない場合、情報システム管理者は、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。

(5) 庁外への機器の設置

情報セキュリティ責任者及び情報システム管理者は、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。また、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。

5-2　管理区域（情報システム室等）の管理

(1) 管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ　情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区

域から外部に通ず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立入りを防止しなければならない。

ウ　情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

(2) 管理区域の入退室管理等

ア　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿により、入退室管理を行うものとする。

イ　委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ　情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

(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事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。

5-3　通信回線及び通信回線装置の管理

(1) 情報セキュリティ責任者は、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、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

(2) 情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

(3) 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。

(4) 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、適正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。

(5) 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、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

(6) 情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

(7) 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なければならない。また、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。

5-4　議員及び職員の利用する端末や電磁的記録媒体等の管理

(1) 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ソコンのワイヤーによる固定、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。

(2) 情報システム管理者は、所管する情報システムへのログインに際し、パスワード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。

６　人的セキュリティ

6-1　議員及び職員の遵守事項

(1) 議員及び職員の遵守事項

ア　セキュリティポリシー等の遵守

議員及び職員は、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。また、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

議員及び職員は、業務以外の目的で情報資産の外部への持ち出し、議会が管理する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。

ウ　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

(ｱ) CISOは、機密性２以上、可用性２、完全性２のいずれかの区分に該当する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。

(ｲ) 議員及び職員は、議会が管理するモバイル端末、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。

(ｳ) 議員及び職員は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

エ　パソコン、モバイル端末等の業務利用

(ｱ) 議員及び職員は、原則として、議長が指定したパソコン、モバイル端末等（以下「指定端末」という。）を業務に使用するものとする。ただし、業務上必要な場合は、情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得て、指定端末以外のパソコン、モバイル端末等を使用することができる。

(ｲ) 議員及び職員は、指定端末以外のパソコン、モバイル端末等を用いる場合には、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に関する規定を遵守しなければならない。

オ　セキュリティ設定の変更禁止

議員及び職員は、議会が管理するパソコンや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セキュリティ管理者の許可なく変更してはならない。

カ　机上の端末等の管理

議員及び職員は、離席時にパソコン、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、適正な措置を講じなければならない。

キ　退職時等の遵守事項

議員及び職員は、異動、退職、任期満了等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

(2) セキュリティポリシー等の閲覧

情報セキュリティ管理者は、議員及び職員が常に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しなければならない。

(3) 委託事業者に対する説明

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・保守等を事業者に発注する場合、再委託事業者も含めて、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事項を説明しなければならない。

6-2　研修・訓練

(1) 情報セキュリティに関する研修・訓練

CISO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。

なお、職員を対象とする研修については、市長公室デジタルイノベーション課が主催する研修への参加に代えることができるものとする。

(2) 研修計画の策定及び実施

ア　CISOは、議員及び職員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うものとする。

イ　情報セキュリティ管理者は、初当選の議員及び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。

ウ　研修は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者、議員及び職員に対して、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。

エ　情報セキュリティ管理者は、研修の実施状況を記録し、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。

オ　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研修の実施状況について、CISOに報告しなければならない。

(3) 緊急時対応訓練

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、また、効果的に実施できるようにしなければならない。

(4) 研修及び訓練への参加

議員及び職員は、定められた研修及び訓練に参加しなければならない。

6-3 情報セキュリティインシデントの報告

(1) 情報セキュリティインシデントの報告

ア　議員及び職員は、情報セキュリティインシデントを認知した場合又は住民等外部から報告を受けた場合、速やかに情報セキュリティ管理者及び市長公室デジタルイノベーション課に報告しなければならない。

イ　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、CISO、情報セキュリティ責任者及び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。

ウ　情報セキュリティインシデントにより、個人情報又は特定個人情報の漏えい等が発生した場合、必要に応じて水戸市議会個人情報保護推進委員会へ報告しなければならない。

(2) 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

ア　議会 CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

イ　議会 CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。

ウ　議会 CSIRT は、情報セキュリティインシデントであると評価した場合、情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

エ　議会 CSIRT は、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。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

オ　CISO は、議会 CSIRT 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指示しなければならない。

6-4 ID 及びパスワードの管理

(1) ID の取扱い

議員及び職員は、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。

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) パスワードの取扱い

議員及び職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

エ　パスワードが流出したおそれがある場合には、情報セキュリティ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。

オ　複数の情報システムを扱う議員及び職員は、同一のパスワードをシステム間で用いてはならない。

カ　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

キ　サーバ、ネットワーク機器及びパソコン等の端末に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

ク　議員及び職員間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く）。

7　技術的セキュリティ

7-1　コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

ア　情報システム管理者は、議員及び職員が使用できる文書サーバの容量を設定し、議員及び職員に周知しなければならない。

イ　情報システム管理者は、文書サーバを会議又は課等の組織で構成し、権限のない議員及び職員がフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。

ウ　情報システム管理者は、住民の個人情報、人事記録等、特定の議員及び職員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、会議の構成員又は同一の組織であっても、権限のない議員及び職員が閲覧及び使用できないようにしなければならない。

(2) バックアップの実施

ア　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やファイルサーバ等に記録された情報について、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。

イ　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サーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

ウ　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を構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(3) 他団体との情報システムに関する情報等の交換

情報システム管理者は、所管する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、情報セキュリティ責任者の許可を得なければならない。

(4) システム管理記録及び作業の確認

ア　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。

イ　情報システム管理者は、所管する情報システムにおいて、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正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

ウ　情報システム管理者及び情報システム担当者並びに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名以上で作業し、互いにその作業を確認しなければならない。

(5) 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、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したり、紛失等がないよう、適正に管理しなければならない。

(6) ログの取得等

ア　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、１か月程度保存しなければならない。

イ　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、適正にログを管理しなければならない。

ウ　情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

情報セキュリティ責任者及び情報システム管理者は、議員及び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、適正に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

ア　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。

イ　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、ネットワークに適正なアクセス制御を施さなければならない。

ウ　情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

(9) 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、電子申請の受付システム等、外部の者が利用できるシステムについて、必要に応じ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。

(10) 外部ネットワークとの接続制限等

ア　情報システム管理者は、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には、CISO 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。

イ　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、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。

ウ　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。

エ　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、次のセキュリティ対策を実施しなければならない。

(ｱ) 議会が管理するネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

(ｲ) 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しなければならない。

(ｳ) 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なければならない。

(ｴ) 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しなければならない。

オ　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、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。

(11) 複合機のセキュリティ管理

ア　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及び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、適正なセキュリティ要件を策定しなければならない。

イ　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正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。

ウ　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する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。

(12) IoT 機器を含む特定用途機器のセキュリティ管理

情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(13) 無線 LAN のセキュリティ対策及びネットワークの盗聴対策

ア　情報セキュリティ責任者は、無線 LAN の利用を認める場合、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。

イ　情報セキュリティ責任者は、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。

(14) 電子メールのセキュリティ管理

ア　情報セキュリティ責任者は、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）ができないよう、電子メールサーバの設定を行わなければならない。

イ　情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　情報セキュリティ責任者は、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。

エ　情報セキュリティ責任者は、議員及び職員が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を議員及び職員に周知しなければならない。

(15) 電子メールの利用制限

ア　議員及び職員は、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　議員及び職員は、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　議員及び職員は、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。

エ　議員及び職員は、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。

(16) 電子署名・暗号化

ア　議員及び職員は、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、CISO が定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

イ　議員及び職員は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO が定めた方法で暗号のためのパスワードを管理しなければならない。

ウ　CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

ア　議員及び職員は、議会が管理するパソコンやモバイル端末にソフトウェアを導入してはならない。

イ　議員及び職員は、業務上の必要がある場合に限り、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、議会が管理するパソコンやモバイル端末にソフトウェアを導入することができる。

　なお、当該ソフトウェアを導入する際は、情報システム管理者が、ソフトウェアのライセンスを管理しなければならない。

ウ　議員及び職員は、不正にコピーしたソフトウェアを利用してはならない。

(18) 機器構成の変更の制限

ア　議員及び職員は、議会が管理するパソコンやモバイル端末に対し機器の改造及び増設又は交換を行ってはならない。

イ　議員及び職員は、業務上、議会が管理するパソコンやモバイル端末に機器の改造及び増設又は交換を行う必要がある場合には、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。

(19) 業務外ネットワークへの接続の制限

情報セキュリティ管理者は、議会が管理するパソコンやモバイル端末について、端末に搭載されたOSのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(20) 業務以外の目的でのウェブ閲覧の禁止

ア　議員及び職員は、業務以外の目的でウェブを閲覧してはならない。

イ　情報セキュリティ責任者は、議員及び職員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、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

(21) ウェブ会議サービスの利用時の対策

ア　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。

イ　議員及び職員は、議会の定める利用手順に従い、ウェブ会議の参加者や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。

ウ　議員及び職員は、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。

エ　議員及び職員は、外部からウェブ会議に招待される場合は、議会の定める利用手順に従い、必要に応じて利用申請を行い、情報システム担当者の承認を得なければならない。

(22) ソーシャルメディアサービスの利用

ア　情報セキュリティ管理者は、議会が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ｱ) 議会のアカウントによる情報発信が、実際に議会のものであることを明らかにするために、議会の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施しなければならない。

(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USBメモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施しなければならない。

イ　機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

ウ　情報セキュリティ管理者は、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なければならない。

エ　情報セキュリティ管理者は、アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

オ　可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市議会の自己管理ウェブサイトに当該情報を掲載して参照可能な状態にしなければならない。

7-2　アクセス制御

(1) アクセス制御等

ア　アクセス制御

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議員及び職員がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者 ID の取扱い

(ｱ) 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、議員及び職員の異動、出向、退職、任期満了に伴う利用者 ID の取扱い等の方法を定めなければならない。

(ｲ) 議員及び職員は、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、情報システム管理者に通知しなければならない。

(ｳ) 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。

(ｴ) 情報システム管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

ウ　管理者権限を付与された ID の管理等

(ｱ) 情報システム管理者は、管理者権限を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

(ｲ) 情報システム管理者は、管理者権限の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。

(ｳ) 情報システム管理者の権限を代行する者は、情報セキュリティ責任者が指名し、CISO が認めた者でなければならない。

(ｴ) CISO は、(ｳ)の代行者を認めた場合、速やかに情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

(ｵ) 情報システム管理者は、管理者権限を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

(ｶ) 情報システム管理者は、管理者権限を付与された ID 及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等のセキュリティ機能を強化しなければならない。

(ｷ) 情報システム管理者は、管理者権限を付与された ID を初期設定以外のものに変更しなければならない。

(2) 議員及び職員による外部からのアクセス等の制限

ア　議員及び職員が外部から議会が管理するネットワーク又は情報システムにアクセスする場合、情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

イ　情報セキュリティ責任者は、議会が管理する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。

ウ　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。

エ　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。

オ　情報セキュリティ責任者は、外部からのアクセスに利用するモバイル端末を議員及び職員に貸与する場合、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。

カ　議員及び職員は、持ち込んだ又は外部から持ち帰ったモバイル端末を議会が管理する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るか、もしく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。

キ　情報セキュリティ責任者は、議会が管理するネットワーク及び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、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）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。

(3) 認証情報の管理

ア　情報システム管理者は、議員及び職員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、OS 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。

イ　情報システム管理者は、議員及び職員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、初回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。

ウ　情報システム管理者は、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。

(4) 管理者権限の行使による接続時間の制限

情報システム管理者は、管理者権限を行使したネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

7-3　システム開発、導入、保守等

(1) 機器等の調達に係る協議

情報セキュリティ管理者は、機器等を調達する場合、事前に市長公室デジタルイノベーション課長に協議の上、機器の選定,納入時の確認を行わなければならない。

(2) 機器等及び情報システムの調達

ア　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　情報セキュリティ責任者及び情報システム管理者は、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。

(3) 情報システムの開発

ア　システム開発における責任者及び作業者の特定

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。

イ　システム開発における責任者及び作業者の ID の管理

(ｱ) 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 ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(ｲ) 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のアクセス権限を設定しなければならならない。

ウ　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

(ｱ) 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、それ以外のものを利用させてはならない。

(ｲ) 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。

エ　アプリケーション・コンテンツの開発時の対策

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、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。

(4) 情報システムの導入

ア　開発環境と運用環境の分離及び移行手順の明確化

(ｱ) 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。

(ｲ) 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。

(ｳ) 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。

イ　運用テストの実施

(ｱ) 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運用テストを行わなければならない。

(ｲ) 情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ｳ) 情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(ｴ) 情報システム管理者は、開発したシステムについて受け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。

(ｵ) 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。

ウ　機器等の納入時又は情報システムの受入れ時

(ｱ) 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・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。

(ｲ) 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。

(5) 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

ア　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・保守する場合は、以下の全てのセキュリティ対策を実施しなければならない。【推奨事項】

(ｱ) 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

(ｲ) 脅威や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

イ　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、定期的に確認し、必要に応じてこれを見直さなければならない。

(6) システム開発・保守に関連する資料等の整備及び保管

ア　情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備し、保管しなければならない。

(ｱ) 情報システム管理者は、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、その内容について情報セキュリティ責任者に報告しなければならない。

(ｲ) 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、以下を全て含む実施手順を整備しなければならない。

・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

・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

・情報システムが停止した際の復旧手順

イ　情報システム管理者は、運用テストの実施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正な方法で保管しなければならない。

(7) 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、所管する情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する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、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(ｱ) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等の改善に努めること。

(ｲ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じること。

(ｳ) ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報の改ざん又は漏えいのおそれがある場合に、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すること。

ウ　情報システム管理者は、所管する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。

(8) 情報システムの変更管理

情報システム管理者は、所管する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。

(9) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を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。

(10) システム更新又は統合時の検証等

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。

(11) 情報システムについての対策の見直し

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適切に見直さなければならない。

なお、措置の結果については、情報セキュリティ責任者へ報告しなければならない。

7-4 不正プログラム対策

(1) 情報セキュリティ責任者の措置事項

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。

ア　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。

イ　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。

ウ　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、必要に応じ議員及び職員に対して注意喚起すること。

エ　議会が管理する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ェアを常駐させること。

オ　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たれていること。

カ　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たれていること。

キ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなど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。

(2) 情報システム管理者の措置事項

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。

ア　所管する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

策ソフトウェアをシステムに常駐させること。

イ　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たれていること。

ウ　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たれていること。

エ　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、議会が管理する媒体以外を議員及び職員に利用させないこと。

オ　不正プログラム対策ソフトウェア等の設定変更に係る権限については、一括管理し、情報システム管理者が許可した職員のみに当該権限を付与すること。

(3) 議員及び職員の遵守事項

議員及び職員は、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。

ア　パソコン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は、当該ソフトウェアの設定を変更しないこと。

イ　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。

ウ　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。

エ　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。

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ェアでチェックを行うこと。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。

カ　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。

キ　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。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や、通信を行わない設定への変更などを実施すること。

(4) 専門家の支援体制

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。

7-6　不正アクセス対策

(1) 情報セキュリティ責任者の措置事項

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

ア　使用されていないポートを閉鎖すること。

イ　不要なサービスについて、機能を削除又は停止すること。

ウ　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に、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。

エ　市長公室デジタルイノベーション課と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築すること。

(2) 攻撃への対処

CISO 及び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リスクがある場合は、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。また、市長公室デジタルイノベーション課等の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。

(3) 記録の保存

CISO 及び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。

(4) 内部からの攻撃

情報システム管理者は、議員及び職員並びに委託事業者が使用しているパソコン等の端末からの議会が管理するサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 議員及び職員による不正アクセス

情報システム管理者は、議員及び職員による不正アクセスを発見した場合は、情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(6) サービス不能攻撃

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。

(7) 標的型攻撃

情報システム管理者は、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）や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。

7-6　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、ソフトウェアの更新等

情報システム管理者は、サーバ装置、端末及び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。また、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。

(2) 不正プログラム等のセキュリティ情報の収集・周知

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、対応方法について議員及び職員に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

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、必要に応じて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は、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。

8　運用

8-1　情報システムの監視

(1) 情報システムの運用・保守時の対策

ア　情報システム管理者は、所管する情報システムの運用・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。

イ　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。

ウ　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。

(2) 情報システムの監視機能

ア　情報システム管理者は、所管する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。

イ　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、所管する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。

ウ　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、所管する情報システムにおける監視の対象や手法を定期的に見直さなければならない。

エ　情報システム管理者は、所管する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。

(3) 情報システムの監視

ア　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、所管する情報システムを常時監視するための措置を講じるとともに、監視の強化に不断に努めなければならない。

イ　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。

ウ　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するための措置を講じるとともに、監視の強化に不断に努めなければならない。

8-2　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　情報セキュリティ管理者は、セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにCISOに報告しなければならない。

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

ウ　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には適正かつ速やかに対処しなければならない。

(2) 利用状況の調査

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、議員及び職員が使用しているパソコン、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。

(3) 議員及び職員の報告義務

ア　議員及び職員は、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を行わなければならない。

イ　当該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情報セキュリティ責任者が判断した場合において、議員及び職員は、緊急時対応計画に従って適正に対処しなければならない。

8-3　侵害時の対応等

(1) 緊急時対応計画の策定

CISO は、情報セキュリティインシデント、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正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

(3) 業務継続計画との整合性確保

情報セキュリティ責任者は、セキュリティポリシーと議長が別に定める業務継続計画との整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

CISO 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見直しを行わなければならない。

8-4　例外措置

(1) 例外措置の許可

情報セキュリティ管理者は、セキュリティポリシーを遵守することが困難な状況で、議会運営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する、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、例外措置を講じることができる。

(2) 緊急時の例外措置

情報セキュリティ管理者は、議会運営の遂行に緊急を要する等の場合であって、例外措置を講じることが避けられないときは、事後速やかにCISOに報告しなければならない。

(3) 例外措置の申請書の管理

CISOは、例外措置を講じるに至った経緯に係る資料を適正に保管し、定期的にその状況を確認しなければならない。

8-5 違反時の対応

議員及び職員のセキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

ア　情報セキュリティ責任者が違反を確認した場合は、情報セキュリティ管理者に通知し、適正な措置を求めること。

イ　情報システム管理者等が違反を確認した場合は、速やかに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通知し、適正な措置を求めること。

ウ　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、情報セキュリティ責任者は、当該議員及び職員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あるいは剥奪することができる。その後速やかに、情報セキュリティ責任者は、議員及び職員の権利を停止あるいは剥奪した旨をCISO及び情報セキュリティ管理者に通知すること。

9 業務委託と外部サービスの利用

(1) 業務委託

ア　委託事業者の選定基準

情報セキュリティ管理者は、委託事業者の選定にあたり、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。

イ　業務委託実施前の対策

情報セキュリティ管理者は、データの処理、情報システムの運用・保守等に係る委託契約の締結をしようとするときは、水戸市情報システムの管理運営に関する規則第28条第2項各号及び第35条各号に掲げる事項を契約書等に記載しなければならない。

ウ　業務委託実施期間中の対策

情報セキュリティ管理者は、委託事業者において、契約書等に定める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、必要に応じて措置を講じなければならない。また、その重要度に応じて、その結果を情報セキュリティ責任者に報告しなければならない。

エ　業務委託終了時の対策

情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

(ｱ) 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

(ｲ) 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) 外部サービス（クラウドサービス）の利用

ア　外部サービスの利用に関する基準の整備

情報セキュリティ責任者は、以下を含む外部サービスの利用に関する基準（以下「外部サービス利用基準」という。）を整備しなくてはならない。

(ｱ) 外部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の判断に関すること。

(ｲ) 外部サービス提供者の選定に関すること。

(ｳ) 外部サービスの利用申請に関すること。

(ｴ) 外部サービスの利用状況の管理に関すること。

(ｵ) 外部サービスを利用する際のセキュリティ対策に関すること。

(ｶ) 外部サービスの利用終了時における取り扱った情報及びアカウントの廃棄に関すること。

(ｷ) 外部サービスの利用中断及び終了時におけるデータの移行に関すること。

(ｸ) 外部サービスにおけるサービスレベルの保証に関すること。

(ｹ) 外部サービス提供者に対する情報セキュリティ監査に関すること。

(ｺ) 外部サービスにおける準拠法及び管轄裁判所に関すること。

(ｻ) 再委託実施時の条件及び外部サービス提供者の責務に関すること。

(ｼ) 外部サービス提供者の信頼性に関すること。

イ　外部サービスの調達・契約

(ｱ) 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス利用基準及び外部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。

(ｲ) 情報セキュリティ管理者は、外部サービスを調達する場合は、当該サービス及び外部サービス提供者が調達仕様を満たすことを契約事務の開始前までにに確認し、情報セキュリティ責任者の承認を得なければならない。

ウ　外部サービスの利用申請

(ｱ) 情報セキュリティ管理者は、契約締結後、外部サービスの利用を開始する場合、情報セキュリティ責任者へ利用申請を行わなければならない。

(ｲ) 情報セキュリティ責任者は、外部サービスの利用申請があった場合、その内容を審査し、利用の可否を決定しなければならない。また、外部サービスの利用申請を承認した場合は情報システム台帳に記載しなければならない。

エ　外部サービスの構築・運用時における対策

(ｱ) 情報セキュリティ管理者は、外部サービスの運用開始前までに以下の内容を全て含む実施手順を整備しなければならない。

・外部サービスにおける情報セキュリティ維持に関する手順

・外部サービスの運用中の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

・外部サービスが停止、利用できなくなった際の復旧手順

(ｲ) 情報セキュリティ管理者は、実施手順に記載したセキュリティ対策の実施状況を確認し、記録しなければならない。

(ｳ) 情報セキュリティ管理者は、利用している外部サービスについて、新たな脅威に対応するため、セキュリティ対策を適時見直し、必要な措置を講じなければならない。

オ　外部サービスを利用した情報システムの利用終了時の対策

情報セキュリティ管理者は、外部サービス利用基準に定められた、外部サービスの利用終了時における情報セキュリティ対策を実施するとともに、実施状況を確認・記録しなければならない。

10　評価・見直し

10-1　監査

(1) 実施方法

CISOは、情報セキュリティ監査統括責任者を市長公室デジタルイノベーション課長に指名し、情報資産の情報セキュリティ対策状況について、毎年度監査を行わせなければならない。

(2) 監査を行う者の要件

ア　情報セキュリティ監査統括責任者は、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。

イ　監査を行う者は、情報セキュリティに関する専門知識を有する者でなければならない。

(3) 委託事業者に対する監査

事業者に業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対し、セキュリティポリシーの遵守について、監査を定期的に行わなければならない。

(4) 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、CISOに報告する。

(5) 保管

情報セキュリティ監査統括責任者は、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正に保管しなければならない。

(6) 監査結果への対応

ア　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（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

イ　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。

(7) 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

情報セキュリティ責任者は、監査結果を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。

10-2　自己点検

(1) 実施方法

ア　情報システム管理者は、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。

イ　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、セキュリティポリシーに沿った情報セキュリティ対策の実施状況について、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。

(2) 自己点検結果の活用

ア　議員及び職員は、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　情報セキュリティ責任者は、この点検結果をセキュリティポリシー、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。

10-3　セキュリティポリシー及び関係規程等の見直し

情報セキュリティ責任者は、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、セキュリティポリシー等について毎年度及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、改善を行うものとする。