大津市議会情報セキュリティポリシー

令和８年４月１日施行

つなぐ、つくる、みらいへ
大津市議会
Otsu City Council

第１章　情報セキュリティ基本方針

第２章　情報セキュリティ対策基準

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、本市議会が保有する情報資産の機密性及び可用性を維持するため、本市議会が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

⑴　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。

⑵　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。

⑶　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

⑷　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

⑸　機密性

情報にアクセスすることを認められた者だけが、必要な時にアクセスできる状態を確保することをいう。

⑹　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。

⑺　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑻　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３　対象とする脅威

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

⑴　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、重要情報の搾取、内部不正等

⑵　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、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備、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

⑶　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

⑷　大規模・広範囲にわたる疾病による要因不足に伴うシステム運用の機能不全等

4　適用範囲

本基本方針の適用範囲は、次に掲げるものとする。

⑴　対象者の範囲

本市議会の情報資産を取扱うすべての者（以下、「情報資産取扱者」という。）

⑵　情報資産の範囲

①ネットワーク並びにこれらに関する設備及び電磁的記録媒体

②ネットワークで取り扱う情報（これを印刷した文書を含む。）

5　議員及び議会局職員等の遵守義務

議員及び議会局職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって情報セキュリティポリシーを遵守しなければならない。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

⑴　組織体制

本市議会の情報資産について、情報セキュリティ対策を推進する体制を確立する。

⑵　情報資産の分類と管理

本市議会の保有する情報資産を機密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。

⑶　物理的セキュリティ

通信回線及び職員が使用するパソコン・タブレット端末等の管理について、物理的な対策を講じる。

⑷　人的セキュリティ

情報セキュリティに関し、議員及び議会局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じる。

⑸　技術的セキュリティ

コンピュータ・タブレット端末等の管理、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じる。

⑹　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、情報資産に対するセキュリティ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。

⑺　業務委託と外部サービスの利用

業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結し、受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する。

⑻　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、定期的又は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。

７　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は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。

８　情報セキュリティポリシーの見直し

情報セキュリティ監査又は自己点検の結果、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となった場合には、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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を定める。

１０　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政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。

１１　その他

議会局職員等が取り扱う大津市の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及び取り扱う情報（これらを印刷した文書を含む。）に関する情報セキュリティ対策については、大津市情報セキュリティポリシーによることとする。

第２章 情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、本議会における情報資産に関する情報セキュリティ対策の基準を定めたものである。

１　組織体制

(1)　最高情報統括責任者（CIO、以下「CIO」という。）

① CIOは議長の職にある者をもって充てる

② CIOは本議会における全てのネットワーク、情報システム等の情報資産の管理の最終決定権限及び責任を有する。

(2)　副最高情報統括責任者（副CIO、以下「副CIO」という。）

① 副CIOは副議長の職にある者をもって充てる

② 副CIOはCIOと連携を図り、本議会の情報資産の管理及び情報セキュリティ対策に関する指導及び助言を行う権限を有する。

(3)　最高情報セキュリティ責任者（CISO、以下「CISO」という。）

① CISOは議会局長の職にある者をもって充てる

② CISOは、本議会における全てのネットワーク、情報システム等の情報資産の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。

③ CISOは情報セキュリティインシデントに対処するための体制を整備し、役割を明確化する。

(4)　情報セキュリティ責任者

① 議会局次長の職にある者をもって充てる

② 情報セキュリティ責任者はCISOを補佐しなければならない

③ 情報セキュリティ責任者は本議会の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④ 情報セキュリティ責任者は情報セキュリティ管理者、情報セキュリティ担当者、情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤ 情報セキュリティ責任者は緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

⑥ 情報セキュリティ責任者は情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてCISOにその内容を報告しなければならない。

(5)　情報セキュリティ管理者

① 情報セキュリティ管理者は、議会総務課長及び議事課長の職にある者をもって充てる。

② 情報セキュリティ管理者は、所管する課等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、所管する課等で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。

(6)　情報セキュリティ担当者

情報セキュリティ管理者の指示に従い、対策基準の順守について、職員等に対する教育、訓練

等を行う者を情報セキュリティ担当者とする。

(7)　情報システム担当者

情報セキュリティ管理者の指示等に従い、情報システムの設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

(8)　情報セキュリティ対策の実施状況の確認

本議会の情報セキュリティ対策を統一的に実施するため、議会運営委員会において、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とともに、毎年情報セキュリティ対策の実施状況について確認を行う。

2　情報資産の分類と管理

(1) 情報資産の分類

本市議会における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
議会機密性A	議会事務で取り扱う情報資産のうち、個人情報等漏洩が生じた際に権利利益の侵害に繋がる恐れのある情報資産	・市から支給された端末及び議会局で調達した端末以外での作業の原則禁止。 ・必要以上の複製及び配布禁止 ・保管場所の制限 ・信頼のできるネットワーク回線の選択。
議会機密性B	議会機密性Aの情報資産以外の情報資産	―

可用性による情報資産の分類

分類	分類基準	取扱制限
議会可用性A	議会事務で取り扱う情報資産のうち、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個人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
議会可用性B	議会可用性B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。

② 情報の作成

（ア） 議会局職員は、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、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、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。

（イ） 議会局職員以外の者が作成した情報資産を入手した者は、（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。

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、情報資産の分類に応じ、適正な取扱いをしなければならない。

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議会機密性A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。

⑦ 情報資産の提供・公表

（ア） 自治体機密性A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） 自治体機密性A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。

⑧ 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。

3　情報システム全体の強靭性の向上

(1) インターネット接続

① 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不適正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。

4　物理的セキュリティ

(1) 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、議会局内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。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、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。

(2) 議会局職員の利用する端末や電磁式記録媒体等の管理

① 情報セキュリティ管理者は、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 情報セキュリティ管理者は、情報システムへのログインに際し、パスワード等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。

③ 情報セキュリティ管理者は、パソコン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、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についても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。

5　人的セキュリティ

(1) 議員、議会局職員等の遵守事項

① 情報セキュリティポリシー等の遵守

議員、議会局職員等は、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。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。

② 業務以外の目的での使用の禁止

議員、議会局職員は、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。

③ 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）議会局職員等は、本市のモバイル端末、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。

（イ）議会局職員等は、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。

④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア）議会局職員は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則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。

（イ）議員は、自身のパソコン、モバイル端末を用い議会局のネットワークに接続する場合には、安全管理措置に関する規定を遵守しなければならない。

⑤ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

議会局職員は、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。

⑥ 机上の端末等の管理

議会局職員は、パソコン、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。

⑦ 退職時等の遵守事項

議会局職員は、異動、退職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) 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保守等を委託事業者に発注する場合、再委託事業者も含めて、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。

(3) 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・訓練を実施しなければならない。

(4) 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。

(5) 議会における情報セキュリティインシデントの報告

① 議員、議会局職員は、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。

② 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 及び情報セキュリティ責任者に報告しなければならない。

③ 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場

合、必要に応じて個人情報保護委員会へ報告しなければならない。

(6) ID 、パスワードの取扱い

① IDの取扱い

議員、議会局職員等は、自己の管理するIDは、他人に利用させてはならない。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、議会局職員等は、自己の管理するパスワードに関し、他者に知られないように管理するとともに、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。

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

③ パスワードが流出した際の取扱い

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。

6　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 システム管理作業の確認

情報セキュリティ責任者及び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、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。

② 障害記録

情報セキュリティ責任者及び情報セキュリティ管理者は、議員、議会局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。

③ ネットワークの接続制御

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。

④ 外部ネットワークとの接続制限等

情報セキュリティ管理者は、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。

⑤ 無線LAN 及びネットワークの盗聴対策

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。また、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。

⑥ 電子メールの利用制限

議会局職員は、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。また、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。

議会局職員は、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。

⑦ 無許可ソフトウェアの導入等の禁止

議会局職員等は、パソコン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。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セキュリティ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が、導入する際は、情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

⑧ 機器構成の変更の制限

議会局職員は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。業務上、パソコンやモバイル端末に対し機器の改造及び増設・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セキュリティ管理者の許可を得なければならない。

⑨ 業務外ネットワークへの接続の禁止

議会局職員は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報セキュリティー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。

⑩ 業務以外の目的でのウェブ閲覧の禁止

議会局職員等は、業務以外の目的でウェブを閲覧してはならない。

⑪ Web 会議サービスの利用時の対策

議会局職員は、Web 会議に無関係の者が参加できないよう対策を講ずるとともに、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すること。

⑫ ソーシャルメディアサービスの利用

情報セキュリティ管理者は、本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）本議会のアカウントによる情報発信が、実際の本議会のものであることを明らかにするために、本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すること。

（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すること。

（ウ）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。

⑬ AIサービスの利用

議会局職員は、AIサービスを利用する場合は、大津市生成AIの利用ガイドラインを遵守しなければならない。

(2) アクセス制御

① アクセス制御等

（ア）アクセス制御等

情報セキュリティ責任者又は情報セキュリティ管理者は、所管するネットワークごとにアクセスする権限のない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

議会局職員は、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、情報セキュリティ責任者又は情報セキュリティ管理者に通知しなければならない。情報セキュリティ責任者又は情報セキュリティ管理者利用者はシステム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。

② 議会局職員等による外部からのアクセス等の制限

（ア）議会局職員等が外部から内部のネットワークにアクセスする場合は、情報セキュリティ責任者及び情報セキュリティ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、内部のネットワークに対する外部からのアクセスを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、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。

(3) システム導入、保守等

① 機器等の調達

情報セキュリティ責任者及び情報セキュリティ管理者は、情報機器の導入、保守等の調達にあたっては、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、当該情報機器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 情報システムの導入

情報セキュリティ管理者は、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。

③ 情報セキュリティ管理者は、新たに情報機器もしくは情報システムを導入する場合、既に稼動している情報システムに接続する前に十分な試験を行うとともに、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、確実に検証を実施しなければならない。

④ 調達仕様書等に定められた検査手続に従い、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。

(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しなければならない。

（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しなければならない。
（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、必要に応じ議会局職員に対して注意喚起しなければならない。
（エ）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なければならない。
（オ）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なければならない。
（カ）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しなければならない。

② 情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、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）セキュリティ管理者は、その所管する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なければならない。
（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なければならない。
（ウ）不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報セキュリティ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。

③ 議会局職員の遵守事項

議会局職員は、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てはならない。
（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わなければならない。
（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、速やかに削除しなければならない。
（エ）情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
（オ）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わなければならない。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しなければならない。

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、外部の専門家や大津市の情報システム管理当局から支援を受けられるようにして

おかなければならない。

(5) 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）不要なサービスについて、機能を削除又は停止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セキュリティ管理者へ通報するよう、設定しなければならない。

（ウ）情報セキュリティに関して大津市と連携し、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しなければならない。

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、総務省、滋賀県、大津市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 議員、議会局職員による不正アクセス

情報セキュリティ責任者及び情報セキュリティ管理者は、議員、議会局職員等による不正アクセスを発見した場合は、適正な処置を行わなければならない。

(6) セキュリティ情報の収集

① 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、職員に周知しなければならない。

② 情報セキュリティに関する情報の収集及び共有

情報セキュリティ責任者及び情報セキュリティ管理者は、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。

7　運用

(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）情報セキュリティ責任者及び情報セキュリティ管理者は、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）情報セキュリティ責任者及び情報セキュリティ管理者は、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。

(2) 情報システムの監視機能

① 情報セキュリティ責任者及び情報セキュリティ管理者は、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 情報セキュリティ責任者及び情報セキュリティ管理者は、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や手法を定期的に見直さなければならない。

(3) 情報システムの監視

① 情報セキュリティ責任者及び情報セキュリティ管理者は、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。

(4) 情報セキュリティポリシーの遵守状況の確認及び対処

① 情報セキュリティ責任者及び情報セキュリティ管理者は、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、問題を認めた場合には、速やかにCISO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、適正かつ速やかに対処しなければならない。

③ 情報セキュリティ責任者及び情報セキュリティ管理者は、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には適正かつ速やかに対処しなければならない。

(5) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

① 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、議会局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。

(6) 議員、議会局職員の報告義務

① 議員、議会局職員は、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。

② 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、議会局職員は、適正に対処しなければならない。

(7) 侵害時の対応等

① 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正に対処しなければならない。

(8) 法令遵守

議員、議会局職員は、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（昭和二十五年十二月十三日法律第二百六十一号）

②著作権法（昭和四十五年法律第四十八号）

③不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）

④個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）

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28 年法律第31 号）

⑦大津市個人情報保護法施行条例（令和四年十二月二十二日条例第四十三号）

(9) 処分等

① 情報セキュリティポリシーに違反した議会局職員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、処分の対象とする。

② 議員、議会局職員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、当該職員が所属する課室等の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。

（イ）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、当該議会局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、職員の権利を停止あるいは剥奪した旨をCISO 及び当該職員が所属する課室等の情報セキュリティ管理者に通知しなければならない。

8　業務委託と外部サービス（クラウドサービス）の利用

(1) 業務委託

① 業務委託に係る規程の整備

情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む規程を整備しなければならない。

（ア）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。）

（イ）委託事業者の選定基準

② 業務委託実施前の対策

情報セキュリティ管理者は、業務委託の実施までに、以下の全てを含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務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。

・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

・個人情報漏えい防止のための技術的安全管理措置に関する取り決め

・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

・提供されるサービスレベルの保証

・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・情報セキュリティインシデント発生時の公表
・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）

③ 情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア）仕様に準拠した提案

（イ）契約の締結

④ 業務委託実施期間中の対策

（ア）情報セキュリティ管理者は、業務委託の実施期間において、以下の全てを含む対策を実施しなければならない。
・委託判断基準に従った重要情報の提供
・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
・統括情報セキュリティ責任者へ措置内容の報告（重要度に応じてCISO に報告）
・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などの必要な措置を含む、契約に基づく対処の要求

（イ）情報セキュリティ管理者は、業務委託の実施期間において、以下の全て含む対策の実施を委託事業者に求めなければならない。
・情報の適正な取扱いのための情報セキュリティ対策
・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
・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などの必要な措置を含む対処

⑤ 業務委託終了時の対策

（ア）情報セキュリティ管理者は、ここまで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。
・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
・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

（イ）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の実施を委託事業者に求めなければならない。

・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

・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

(2) 情報システムに関する業務委託

① 情報システムに関する業務委託における共通的対策

情報セキュリティー管理者は、情報システムに関する業務委託の実施までに、情報システムに本議会の意図せざる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。

② 情報システムの構築を業務委託する場合の対策

情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）情報システムのセキュリティ要件の適切な実装

（イ）情報セキュリティの観点に基づく試験の実施

（ウ）情報システムの開発環境及び開発工程における情報セキュリティ対策

③ 情報システムの運用・保守を業務委託する場合の対策

（ア）情報セキュリティ管理者は、情報システムの運用・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。

（イ）情報セキュリティ管理者は、情報システムの運用・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、委託事業者に速やかな報告を求めなければならない。

(3) 外部サービス（クラウドサービス）の利用

① クラウドサービスの選定に係る規程の整備

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、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規程を整備しなくてはならない。

（ア）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り扱いを許可する場所を判断する基準

（イ）クラウドサービス提供者の選定基準

（ウ）クラウドサービスの利用申請の許可権限者と利用手続

（エ）クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

② クラウドサービスの利用に係る規程の整備

統括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、以下を含むクラウドサービスの利用に関する規程を整備しなければならない。

（ア）情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を規程として整備しなければならない。

（イ）情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を規程として整備しなければならない。

（ウ）情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下の全て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の基本方針を規程として整備しなければならない。

・クラウドサービスの利用終了時における対策

・クラウドサービスで取り扱った情報の廃棄

・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

③ クラウドサービスの選定

（ア）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、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

（イ）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すること。さらに、以下の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。

・クラウドサービスの利用を通じて本議会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

・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

・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若しくはその従業員、再委託先又はその他の者によって、本議会の意図しない変更が加えられないための管理体制

・クラウドサービス提供者の資本関係・役員等の情報、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やリージョンの指定

・情報セキュリティインシデントへの対処方法

・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

・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

（ウ）情報セキュリティ責任者または情報セキュリティ管理者は、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、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

（エ）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本市が取り扱う情報の格付等を勘案し、必要に応じて以下の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。

・情報セキュリティ監査の受入れ

・サービスレベルの保証

（オ）情報セキュリティ責任者または情報セキュリティ管理者は、クラウドサービスの利用を通じて本市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、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

（カ）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を一部再委託する場合は、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本市に提供し、本市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ること。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。

（キ）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情報セキュリティ要件を定め、クラウドサービスを選定すること。また、クラウドサービスの情報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。

（ク）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、以下を全て含む情報セキュリティ要件を定めなければならない。

・クラウドサービスに求める情報セキュリティ対策
・クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法
・クラウドサービスに求めるサービスレベル

（ケ）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・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・客観的に評価し判断しなければならない。

9　評価・見直し

(1) 監査

① 実施方法

CISO は、情報セキュリティ責任者に対して、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。

② 監査を行う者の要件

（ア）情報セキュリティ責任者は、監査を実施する場合には、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、監査及び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 監査実施計画の立案及び実施への協力

（ア）情報セキュリティ責任者は、監査を行うに当たって、監査実施計画を立案し、議会運営委

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。

④ 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、情報セキュリティ責任者は委託事業者（再委託事業者を含む。）に対して、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に又は必要に応じて行わなければならない。

⑤ 報告

情報セキュリティ責任者は、監査結果を取りまとめ、CIOに報告する。

⑥ 保管

情報セキュリティ責任者は、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。

⑦ 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。また、議会内で横断的に改善が必要な事項については、情報セキュリティ責任者に対し、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。なお、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。

⑧ 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

議会運営委員会は、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。

(2) 自己点検

① 実施方法

（ア）情報セキュリティ責任者は、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、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。

② 報告

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、議会運営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）議会運営委員会はこの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。

(3) 情報セキュリティポリシー及び関係規程等の見直し

議会運営委員会は、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、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。なお、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見直しについて、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。