一般社団法人つくばスマートシティ協議会情報セキュリティポリシー

令和６年４月１日制定

目次

第１章　基本方針

（目的）

第１条　一般社団法人つくばスマートシティ協議会情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は、一般社団法人つくばスマートシティ協議会（以下「本協議会」という。）が保有する情報資産について高度な情報セキュリティを確立することを目的とする。

（定義）

第２条　情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　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。

ア　機密性　情報にアクセスすることを許可された者だけが、確実に情報にアクセスできることをいう。

イ　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。

ウ　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。

（２）　事務局　本協議会の事務局をいう。

（３）　職員　事務局長、事務局次長及び書記をいう。

（４）　職員等　職員、本協議会から業務を受託し、若しくは請け負った事業者の従業員で当該業務に従事する者又は労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律（昭和 60 年法律第 88 号）に基づき本協議会に派遣された者で当該派遣業務に従事する者及び情報管理者が情報セキュリティポリシー上職員として取り扱われるべき者と判断した者をいう。

（５）　端末　職員等が利用するパーソナルコンピュータ等のほか、これに類する機能を持つ携帯電話等のことをいう。

（６）　電磁的記録媒体　磁気テープ、ハードディスク、CD・DVD 及びフラッシュメモリ等の電子情報を記録可能な媒体をいう。

（７）　外部デバイス　電磁的記録媒体以外の物であって、マウス、キーボード、ディスプレイ、プリンタ及びスキャナ等端末等に接続して使用する機器をいう。

（８）　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及びその構成機器（ハードウェア及びソフトウェアをいう。）をいう。

（９）　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るものであって、情報処理を行う仕組みをいう。

（１０）　業務情報　本協議会の業務執行に係る情報で、かつ、情報システムで取り扱うものをいう。

（１１） 情報資産　業務情報及び情報システムをいう。
（１２） 外部ネットワーク　本協議会以外の者が管理するネットワークをいう。
（１３） 情報セキュリティ事故等　情報システムの停止（メンテナンス等による計画停止を除く。）、コンピュータウイルス等不正プログラムへの感染、不正アクセスその他サイバー攻撃、情報資産の盗難又は紛失等が発生した事故等をいう。
（１４） クラウドサービス　データ、ソフトウェア及びハードウェア等をネットワーク経由で利用者に提供するサービスをいう。
（１５） Web 会議サービス　専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて対面せずに会議を行えるサービスをいう（テレビ会議システムを除く。）。
（１６） 外部サービス　クラウドサービスや Web 会議サービス、SNS、ホスティングサービス等の本協議会以外の者が情報システムの一部又は全部の機能を提供するサービスをいう。
（１７） 約款による外部サービス　外部サービスうち、事業者等が不特定多数の利用者に対して、画一的な約款や規約等への同意及び簡易なアカウントの登録により当該機能を提供するサービスをいう。

（対象とする脅威）
第３条　情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を講じる。
（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　情報セキュリティポリシーは、職員等及び本協議会の保有する情報資産に適用する。

（具体的な手順等の定め）
第５条　情報セキュリティポリシーによる情報セキュリティ対策を講じるための個別具体

的な手順等を定めるため、次に掲げる要項及び計画を策定する。

（１） 一般社団法人つくばスマートシティ協議会 CSIRT 設置要項

（２） 一般社団法人つくばスマートシティ協議会情報セキュリティ緊急時対応計画

（情報セキュリティ対策）

第６条　第３条に掲げる脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

（１） 組織体制（第２章）　本協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ための組織体制を確立する。

（２） 情報資産の分類と管理（第３章）　本協議会の保有する情報資産を重要度に応じて分類し、当該分類により情報セキュリティ対策を講じる。

（３） 物理的セキュリティ（第４章）　情報資産の管理について、物理的な対策を講じる。

（４） 技術的セキュリティ（第５章）　情報システムの管理、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な対策を講じる。

（５） 人的セキュリティ（第６章）　情報セキュリティについて、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。

（６） 運用（第７章）　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及び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し、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切に対応するため、緊急時対応計画を策定する。

（７） 業務委託と外部サービスの利用（第８章）　業務委託については、委託事業者と情報セキュリティ要件を明記した契約を締結し、取り扱う情報資産の重要度に応じ必要なセキュリティ対策が当該委託事業者において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ものとし、外部サービス等の利用については、利用に係る規定を整備し対策を講じる。

（８） 評価・見直し（第９章）　情報セキュリティポリシーの遵守状況を検証するため、定期的に自己点検を実施し、運用改善を行い情報セキュリティの向上を図るとともに、必要に応じて、情報セキュリティポリシーの見直しを行う。

第２章　組織体制

（最高情報セキュリティ責任者）

第７条　情報セキュリティを統括する最高責任者として、最高情報セキュリティ責任者（以下「CISO」という。）を置き、代表理事をもってこれに充てる。

２　CISO は、情報セキュリティに関する専門的な知識及び経験を有した専門家をアドバイザーとして置くことができる。

３　CISO は、本協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。

４　CISO は、情報セキュリティを阻害しない範囲内において、情報通信技術を用いたサービスの向上に努めなければならない。

（CSIRT）

第８条　CISO は、情報セキュリティ事故等に対処するための体制（Computer Security Incident Response Team （以下「CSIRT」という。））を整備し、役割を明確化しなければならない。

２　CISO は、CSIRT に所属する職員を選任し、その中から CSIRT 責任者及び CSIRT 内の業務統括及び外部との連携等を行う職員を定めるものとする。

３　CISO は、情報セキュリティ事故等の統一的な窓口を整備し、情報セキュリティ事故等の報告を受けた場合は、その状況を確認し、必要に応じて自らへの報告が行われる体制を整備しなければならない。

４　CSIRT の設置に関する詳細は、別に定める。

（統括情報セキュリティ責任者）

第９条　CISO を補佐するために、統括情報セキュリティ責任者を置き、事務局長をもってこれに充てる。

２　統括情報セキュリティ責任者は、情報管理者が、情報セキュリティポリシーの目的や趣旨に則した判断を行うよう、必要かつ適切な監督を行わなければならない。

３　統括情報セキュリティ責任者は、前項の監督を行うため、情報管理者に対し、情報セキュリティに関する報告を求めることができる。

４　第２項及び前項の場合において、統括情報セキュリティ責任者は、情報管理者の判断が情報セキュリティポリシーの目的や趣旨に反することが明らかなときには、是正するよう命令することができる。

（情報管理者）

第１０条　情報セキュリティの適正な運用及び管理を行うために、情報管理者を置き、事務

局次長をもってこれに充てる。

２　情報管理者は、職員等に対し情報セキュリティポリシーについて啓発に努めるとともに、情報セキュリティに関する研修及び必要に応じて緊急時対応訓練を実施しなければならない。

（情報セキュリティ委員会）

第１１条　情報セキュリティについて協議するため、情報セキュリティ委員会（以下「委員会」という。）を設置する。

２　委員会は、委員長、副委員長及び委員をもって構成する。

３　委員長は、CISO をもってこれに充てる。

４　副委員長は、統括情報セキュリティ責任者をもってこれに充てる。

５　委員は、理事をもってこれに充てる。

６　委員長は、委員会の会務を総理する。

７　副委員長は、委員長を補佐し、委員長が不在の際は、その職務を代理する。

８　委員会の庶務は、書記において処理する。

９　委員会は、必要に応じて委員長が招集する。

10　委員会は、適用範囲における情報資産を洗い出し、情報資産に関わる脅威及び脆弱性を分析評価し、毎年度、リスクアセスメントを実施する。

（兼務の禁止）

第１２条　情報セキュリティ対策の実施において、や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。

２　情報セキュリティ監査の実施において、や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。

第３章　情報資産の分類と管理

（情報資産の分類）

第１３条　情報セキュリティが侵害された場合の影響等を考慮し、本協議会の情報資産について、当該情報資産の重要度により、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。この場合において、取り扱う情報資産がどの重要度に分類されるかは、情報管理者が判断するものとする。

重要度による情報資産の分類

分類	分類基準
重要度１	個人番号利用事務に係る個人番号を含む情報資産
重要度２	重要度１に該当しない情報資産で、次に掲げるもの ア　当該情報資産に係る個別の法令等により守秘義務又は情報漏えい等に対する安全管理措置等（以下「守秘義務規定等」という。）が課されているもの イ　個人情報の保護に関する法律（平成 15 年法律第 57 号）第２条第３項に規定する要配慮個人情報を含むもの ウ　情報管理者の判断により重要度２として取り扱うべきとされたもの
重要度３	重要度１及び重要度２の情報資産に該当しない個人情報並びに次に掲げる情報資産 ア　当該業務情報を扱う事務局以外に知られることが不適当なもの イ　漏えいした場合に本協議会に対する信頼を著しく害するおそれのあるもの ウ　機密性、完全性又は可用性が侵害されることにより、業務の安定的な遂行に支障を及ぼすおそれがあるもの
重要度４	重要度１、重要度２及び重要度３に該当しない情報資産

（取り扱うことができる情報資産）

第１４条　重要度１、重要度２及び重要度３の情報資産については、外部ネットワークで取り扱うことができない。ただし、情報管理者が認めたものについては、この限りでない。

（情報資産の管理責任）

第１５条　情報管理者は、所管する情報資産について管理責任を有する。

２　情報管理者は、次条から第 26 条までの規定が遵守されるよう、管理しなければならない。

３　職員等は、情報資産の取扱いに当たっては、情報管理者の指示に従わなければならない。

（情報資産の分類の表示）

第１６条　職員等は、所管する情報資産について、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、必要に応じて取扱制限についても明示する等適切な管理に努めなければならない。

（情報資産の作成）

第１７条　職員等は、情報資産の作成に当たり、次に掲げる事項を遵守しなければならない。

（１）　業務上必要のない情報資産を作成してはならないこと

（２）　作成した情報資産又は作成途上の情報資産について、第 13 条に掲げる分類により適切に取り扱うものとすること

（３）　作成途上の情報資産について、作成途上で不要になった場合は、当該情報資産を消去しなければならないこと

（情報資産の入手）

第１８条　職員等は、外部の者が作成した情報資産を入手したときは、情報管理者の指示に基づき、第 13 条に掲げる分類により、当該情報資産の分類と取扱制限を定めなければならない。

（情報資産の利用）

第１９条　職員等は、情報資産の利用に当たり、次に掲げる事項を遵守しなければならない。

（１）　情報資産は、業務以外の目的に利用してはならないこと

（２）　外部の者が作成した情報資産は、許可された利用目的以外に利用してはならないこと

（３）　情報資産は、第 13 条に掲げる分類に応じ、適切な取扱いをしなければならないこと

（４）　情報資産の分類が異なる情報が複数記録されている電磁的記録媒体は、最高度の分類に従って取り扱わなければならないこと

（情報資産の保管）

第２０条　職員等は、情報資産の保管に当たり、次に掲げる事項を遵守しなければならない。

（１）　情報資産は、紛失・破損等を防止するため、第 13 条に掲げる分類に従い、適切に保管しなければならないこと

（２）　重要度１、重要度２又は重要度３の情報資産を記録した電磁的記録媒体は、当該情報資産の機密性、完全性及び可用性の確保の必要性に応じ、情報管理者若しくはその代

理人が常時監視できる場所、施錠できる部屋（入退室を情報管理者又はその代理人が管理するものに限る。）又は施錠できる保管庫等への収納並びに耐火、耐熱、耐水及び耐湿等の対策を講じた場所に保管しなければならないこと

（３） 重要度１、重要度２又は重要度３の情報資産を含むファイルは、求められる機密性の確保の必要性に応じ、パスワードを設定するなど、職務上無関係な者の閲覧を制限しなければならないこと。ただし、ネットワーク又はファイルを保管する機器自体が、職務上無関係な者の閲覧を制限している場合は、この限りでない。

（４） 情報資産の紛失・破損等は、発生後速やかにその旨を情報管理者に報告しなければならないこと

（情報資産の複写及び複製）

第２１条　職員等は、重要度１、重要度２又は重要度３の情報資産を複写又は複製する場合は、情報管理者の許可を得なければならない。

２　職員等は、前項の規定により重要度１、重要度２又は重要度３の情報資産を複写又は複製する場合は、必要以上に複写又は複製してはならない。

３　職員等は、情報資産が複写又は複製された場合は、複写又は複製された情報資産も第 13 条に掲げる分類と取扱制限により管理しなければならない。

（情報資産の持ち出し）

第２２条　職員等は、重要度１、重要度２又は重要度３の情報資産を持ち出す場合は、情報管理者の許可を得なければならない。

２　情報管理者は、前項の規定により許可をした場合は、安全管理について措置を講じなければならない。

３　職員等は、第１項の規定により情報資産を持ち出す場合は、所要事項を記録するものとする。

４　職員等は、第１項の規定により情報資産を持ち出す場合は、必要に応じてパスワード等による暗号化を行わなければならない。

（情報資産の外部への提供）

第２３条　職員等は、重要度１、重要度２又は重要度３の情報資産を外部に提供する場合は、情報管理者に許可を得なければならない。

２　情報管理者は、前項の規定により許可をした場合は、安全管理について措置を講じなければならない。

３　職員等は、第１項の規定により情報資産を外部に提供する場合は、提供先、日時、提供内容等の所要事項を記録し、保管するものとする。

４　職員等は、第１項の規定により情報資産を外部に提供する場合は、必要に応じてパスワ

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２４条　職員等は、重要度１、重要度２又は重要度３の情報資産を運搬する場合は、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など盗難又は紛失時におけ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。

（情報資産の送信）

第２５条　職員等は、重要度１、重要度２又は重要度３の情報資産を電子メール等により送信する場合は、情報管理者に許可を得なければならない。

２　情報管理者は、前項の規定により許可をした場合は、安全管理について措置を講じなければならない。

３　職員等は、第１項の規定により送信する場合は、必要に応じ、電子署名の付与又はパスワード等による暗号化等の措置を講じた上で、送信しなければならない。

（情報資産の廃棄）

第２６条　情報管理者は、重要度１、重要度２又は重要度３の情報資産を記録している電磁的記録媒体が不要になった場合又はリース返却等を行う場合は、電磁的記録媒体の情報を復元できないように消去を行うなどの必要な措置を講じるものとする。

２　職員等は、前項の規定による措置を行う場合は、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。

第４章　物理的セキュリティ

（機器の取付け）

第２７条　情報管理者は、サーバ等の機器の取付けを行う場合は、当該サーバ等を火災、水害、埃、振動、温度及び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など必要な措置を講じなければならない。

（サーバの冗長化）

第２８条　情報管理者は、本協議会が独自で所管する重要な機器の冗長化を図る等、同一データの保持に努めなければならない。

２　情報管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動する等、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２９条　情報管理者は、本協議会が独自で所管する重要な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　情報管理者は、落雷等による過電流に対して、本協議会が独自で所管する重要な機器を保護するための措置を講じなければならない。

（通信ケーブル等の配線）

第３０条　情報管理者は、本協議会が独自で所管するネットワークで使用する通信ケーブル及び電源ケーブル等（以下「ケーブル等」という。）を管理するものとする。

２　職員等は、情報管理者が管理するケーブル等を増設、移設又は撤去してはならない。

３　職員等は、情報管理者が管理するケーブル等の増設、移設又は撤去が必要な場合は、情報管理者と協議するものとする。

４　情報管理者は、本協議会が独自で管理するネットワークに係るケーブル等の損傷等を防止するために、必要な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３１条　情報管理者は、本協議会が独自で所管するサーバ等の機器について、当該サーバ等で取り扱う情報の重要度や故障時等のサービスへの影響等を考慮し、必要に応じて定期保守を実施しなければならない。

２　情報管理者は、外部の事業者にサーバ機器の故障を修理させるに当たり、当該サーバ等で取り扱う情報に重要度１、重要度２又は重要度３の情報が含まれる場合は、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。

（外部に設置する装置）

第３２条　情報管理者は、本協議会の管理が及ばない施設等にサーバ等の機器を設置する場合は、情報セキュリティポリシーに適合しているかどうか、確認しなければならない。

２　情報管理者は、定期的に前項に規定する機器への情報セキュリティ対策に関する情報について確認しなければならない。

（機器の廃棄等）

第３３条　情報管理者は、機器を廃棄、リース返却等をする場合は、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。

（設置場所への立入り制限）

第３４条　情報管理者は、本協議会が所管する重要な機器の設置場所（以下「設置場所」という。）への職員等以外の者の入室を許可した場合は、入退室の記録、職員等による立会い等必要な措置を講じるものとする。

２　情報管理者は、設置場所から外部に通ずるドアの数は必要最小限とするとともに、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。

３　情報管理者は、設置場所内の機器等に、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。

４　情報管理者は、設置場所に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（設置場所の入退室管理等）

第３５条　情報管理者は、設置場所への入退室を、許可した者のみに制限し、IC カード又は生体情報による認証及び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。

２　設置場所に入室する者は、身分証明書等を携帯するものとし、情報管理者の求めにより提示しなければならない。

３　外部からの訪問者が設置場所に入室する場合は、必要に応じて立入区域を制限した上で、設置場所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。

４　情報管理者は、設置場所への入室について、入室目的に関連しない物品の持ち込みについて制限するなど必要な措置をとらなければならない。

（機器等の搬入出）

第３６条　情報管理者は、設置場所の機器等の搬入出について、職員等を立ち会わせなければならない。

（ネットワークの稼働等）

第３７条　情報管理者は、本協議会が独自で所管するネットワークについて、通年終日稼働するよう努めなければならない。

２　前項の規定にかかわらず、情報管理者は、運用上又は技術上の理由により、本協議会が独自で所管するネットワークの運用を必要に応じて停止することができる。

３　情報管理者は、前項の規定により本協議会が独自で所管するネットワークの一部又は全部の運用を停止する場合は、関係する利用者等に対してその内容及び停止期間等を事前に周知しなければならない。

４　情報管理者は、本協議会が独自で所管するネットワークの運用について、セキュリティ上の異常が認められ、緊急を要する場合は、前項の規定にかかわらず、事前の予告なしに所管するネットワークを停止することができる。

（通信設備等の管理）

第３８条　情報管理者は、本協議会が独自で所管する通信設備等を適正に管理しなければならない。

２　情報管理者は、本協議会が独自で所管する通信設備等について次に掲げる資料を作成しなければならない。

（１）　通信設備の一覧表

（２）　通信設備の IP アドレス等を管理する資料

（３）　通信設備の配置を管理する資料

（４）　通信設備の構成を管理する資料

（５）　管理者権限等のユーザ情報を管理する資料

（６）　電源を管理する資料

３　情報管理者は、前項に規定する資料を適正に管理しなければならない。

４　情報管理者は、本協議会が独自で所管するネットワークを管理するに当たり、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。

５　情報管理者は、本協議会が独自で所管する重要度１、重要度２又は重要度３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は、必要なセキュリティ水準を検討の上、専用線等、適正な回線を選択し、必要に応じて送受信される情報の暗号化を行わなければならない。

６　情報管理者は、本協議会が独自で所管する主要な箇所の通信設備等について、保守及び

点検を行わなければならない。

7　情報管理者は、本協議会が独自で所管する通信設備等について、管理しやすい場所で、かつ、目立たない場所に設置するものとする。

（端末及び電磁的記録媒体等の管理）

第３９条　情報管理者は、執務室内に常時設置する端末等について、ワイヤー等による固定及び施錠等により盗難防止に努めなければならない。

2　情報管理者は、ノート型端末及び電磁的記録媒体等について、施錠保管の徹底を求めること等により、盗難防止に努めなければならない。

3　職員等は、ノート型端末及び電磁的記録媒体について、使用時以外は施錠可能な場所に保管しなければならない。

第５章　技術的セキュリティ

（情報システムの開発）

第４０条　情報管理者は、情報システムの開発を行う場合は、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。

２　情報管理者は、システム開発の責任者及び作業者のアクセス権限を必要最小限の範囲で設定しなければならない。

３　情報管理者は、情報システムを開発する場合は、情報システムの仕様書、ネットワーク構成図等を必要に応じて整備しなければならない。

（情報システムの導入）

第４１条　情報管理者は、システム開発、保守及びテスト環境からの運用環境への移行について、システム導入計画の策定時に手順を明確にしなければならない。

２　情報管理者は、開発したシステムへデータを移行する場合は、移行前の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。

３　情報管理者は、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。

４　情報管理者は、開発したソフトウェアを情報システムに取り入れる場合は、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わなければならない。

５　情報管理者は、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してはならない。

（情報システム完成図書等の管理）

第４２条　情報管理者は、本協議会が独自で所管するネットワークに係るネットワーク構成図、情報システム完成図書や開発に係るテスト結果等の情報システム関連文書について、記録媒体にかかわらず、職務上必要とする者以外の者による閲覧や、紛失等がないよう、適正に管理しなければならない。

（情報システムの作業記録簿）

第４３条　情報管理者は、本協議会が独自で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。

２　情報管理者は、本協議会が独自で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、詐取又は改ざん等をされないように適正に管理しなければならない。

３　情報管理者は、本協議会が独自で所管する情報システムにおいてシステム変更等の作

業を行う場合は、２名以上で作業を行い、互いにその作業内容について確認するように努めなければならない。

（情報システムの保守及び更新）

第４４条　情報管理者は、情報セキュリティに重大な影響を及ぼす情報システムについては、適切な保守を行い、その不具合については、速やかに修正等の対応を行わなければならない。

２　情報管理者は、情報システムのソフトウェアの更新等については、計画的に実施しなければならない。

（情報システムの変更管理）

第４５条　情報管理者は、情報システムを追加、変更又は廃棄等した場合は、その際の設定及び構成等の履歴を記録又は保存し、必要な場合には復旧できるようにしなければならない。

（バックアップの実施）

第４６条　情報管理者は、本協議会が独自で所管するネットワーク及び情報システムにおける情報資産の完全性及び可用性を確保するため、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。

（ログの取得等）

第４７条　情報管理者は、本協議会が独自で所管するネットワーク及び情報システムに係る各種ログ並びに情報セキュリティの確保に必要な記録を取得し、３年以上保存しなければならない。

２　情報管理者は、前項の規定により取得した記録が、改ざん又は消去されないように必要な措置を講じなければならない。

３　情報管理者は、第１項の規定により取得した記録を必要に応じて分析しなければならない。

４　情報管理者は、第１項の規定により取得した記録又は前項の規定により分析した情報資産について、重要度１、重要度２又は重要度３の情報資産を削除又は解読が不能な状態に加工した上で、他の機関に提供することができる。ただし、致命的な不具合等の問題解決に必要であると情報管理者が認めた場合は、この限りでない。

（情報システムの障害記録）

第４８条　情報管理者は、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。

（ネットワークの接続制御、経路制御等）

第４９条　情報管理者は、本協議会が独自で所管するネットワークにおいて、フィルタリング又はルーティングにおける設定の不整合が発生しないように、ファイアウォール又はルータ等を設定しなければならない。

２　情報管理者は、本協議会が独自で所管するネットワークで使用される機器について、必要に応じて電子証明書による端末認証や、接続する機器の IP アドレス、MAC アドレス等の認証等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。

（無線 LAN 及びネットワークのセキュリティ対策）

第５０条　情報管理者は、本協議会が独自で所管するネットワークで無線 LAN を利用する場合は、次に掲げるセキュリティ対策を講じなければならない。

（１）　SSID 及びパスワードによる認証

（２）　解読が困難な暗号化

（３）　取り扱う情報資産の重要度に応じた証明書や認証サーバによる接続の制御等

（外部ネットワークとの接続制限等）

第５１条　情報管理者は、本協議会が独自で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は、通信経路の限定（IP アドレス、MAC アドレス等による制御）及びアプリケーションプロトコルの限定（ポート番号による制御）を行わなければならない。

２　情報管理者は、前項の規定により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。

３　情報管理者は、第１項の規定にかかわらず、本協議会が独自で所管するネットワーク上にある機器に対し、外部からの遠隔操作等によるアクセスを行わせてはならない。

４　前項の規定にかかわらず、保守等を実施する業者の所在地が遠隔地にある等やむを得ない場合は、この限りでない。ただし、遠隔操作による保守等を実施する場合は、必要な安全管理措置を講じるものとする。

５　情報管理者は、ウェブサーバ等をインターネットに公開する場合は、本協議会が独自で所管するネットワークへの侵入を防止するために、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なければならない。

６　情報管理者は、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、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。

７　情報管理者は、不正アクセスを防止するため、本協議会が独自で所管するネットワーク

に適正なアクセス制御を施さなければならない。

８　情報管理者は、情報システムに不正な侵入や利用があった場合に探知等ができるよう、適切な対策に努めなければならない。

（権限によるアクセス制御）

第５２条　情報管理者は、本協議会が独自で所管するネットワーク及び情報システムにおいて、アクセスする権限のない者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。

２　情報管理者は、本協議会が独自で所管するネットワークにおける職員等以外の者が利用できる情報システムについて、情報セキュリティ対策について特に強固な対策を取らなければならない。

（利用者アカウントの管理）

第５３条　情報管理者は、利用者アカウント等における登録、変更及び抹消等の情報管理について、職員等の異動、出向、退職等（以下「人事異動等」という。）に伴う取扱いを適切に行わなければならない。

（情報システムの認証等）

第５４条　情報管理者は、情報システムへのログインに際し、パスワード、IC カード又は生体情報による認証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。

２　情報管理者は、必要に応じて、端末に、BIOS パスワード及びハードディスクパスワード等を設定するものとする。

３　情報管理者は、必要に応じて、端末及び電磁的記録媒体等におけるデータの暗号化等の機能を利用するものとする。

（認証情報に関する情報の管理）

第５５条　情報管理者は、認証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、認証情報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、必要性に応じて、これを有効に活用しなければならない。

２　情報管理者は、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、初回ログイン後直ちに仮のパスワードを変更できるよう、必要な措置を講じるものとする。

３　情報管理者は、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　情報管理者は、職員等によるパスワードの利用に当たり、職員等の人事異動等の状況に応じ、適切に変更が行われるよう、必要な措置を講じなければならない。

（特権を付与されたアカウントの管理等）

第５６条　情報管理者は、管理者権限等の特権を付与されたアカウントを利用する者を必要最小限にし、当該アカウント及びパスワードの漏えい等が発生しないよう、当該アカウント及びパスワードを厳重に管理しなければならない。

２　情報管理者は、特権を付与されたアカウントに係るパスワードを初期設定以外のものに変更しなければならない。

３　情報管理者は、特権を付与されたアカウントに係るパスワードについて、職員等の人事異動等があった場合は、変更しなければならない。ただし、運用上又は技術上の理由等から変更が難しい場合は、この限りでない。

４　情報管理者は、前項の規定によりパスワードの変更を行う場合は、一定の規則性に基づいたものにしない等変更前のパスワードから類推することが困難なパスワードとしなければならない。

５　情報管理者は、第２項又は第３項の規定によりパスワードを設定する際は、長さが８文字以上かつ英数字を組合せたもの以上の複雑さを持つものとしなければならない。

６　情報管理者は、特権による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

（不要な情報システム等の削除又は停止）

第５７条　情報管理者は、不要な情報システム及び情報システム上の機能がある場合は、当該システム又は当該機能について、可能な限り削除又は停止しなければならない。

（不正プログラム対策）

第５８条　情報管理者は、次に掲げる不正プログラム対策を講じなければならない。

（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）　本協議会が独自で所管するサーバ、端末及びネットワーク機器等に、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

（４）　不正プログラム対策ソフトウェアの設定変更権限については、一括管理し、職員等に当該権限を付与しないこと

（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。ただし、ネットワークに接続しない端末においては、必要に応じて最新のパター

ンファイルへ更新すること

（６） 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等の開発元のサポートが終了したものを利用しないものとし、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等の開発元のサポートが終了しないことを確認すること。ただし、やむを得ないと情報管理者が認める場合は、この限りでない。

（７） 情報管理者が配布する端末で電磁的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に、情報管理者が許可した媒体以外を職員等に利用させないこと

（外部デバイス及び電磁的記録媒体の接続制限）

第５９条　情報管理者は、本協議会が独自で所管する端末等で、情報管理者が配布したもの又は情報管理者の許可を得て職員等が独自に導入したもの以外の外部デバイス又は電磁的記録媒体を接続することができないように設定しなければならない。

２　情報管理者は、前項の場合において、業務上やむを得ない事由等により必要がある場合は、特定の外部デバイス及び電磁的記録媒体を特定の端末等で使用可能な状態に設定することができる。

（ソフトウェアのインストール制限）

第６０条　情報管理者は、本協議会が独自で所管する端末等で、情報管理者が認めていない設定変更又はソフトウェアのインストールをできないように設定しなければならない。

２　情報管理者は、前項の場合において、業務上やむを得ない事由等により必要がある場合は、ソフトウェアを特定の端末等にインストールをすることができる。

（内部から外部への攻撃の監視）

第６１条　情報管理者は、本協議会が独自で所管するネットワークにおいて、不正プログラム等に感染した端末等で、職員等及び委託事業者が使用しているものからの、所管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。

（職員等による不正アクセスの監視）

第６２条　情報管理者は、職員等による不正アクセスを監視し、発見した場合は、適切な処置を求めなければならない。

（攻撃への対処）

第６３条　情報管理者は、本協議会が独自で所管するサーバ等に攻撃を受けた場合若しくは攻撃を受けるリスクがある場合又は不正プログラム等への感染により内部から外部への攻撃が確認された場合若しくは外部へ攻撃するリスクがある場合は、情報システムの

停止を含む必要な措置を講じなければならない。

２　情報管理者は、前項の攻撃への対処として次に掲げる対策を講じなければならない。

（１）　標的型攻撃による組織内部への侵入を低減する対策

（２）　内部に侵入した攻撃を早期検知して対処する対策

（３）　侵入範囲の拡大の困難度を上げる対策

（４）　外部との不正通信を検知して対処する対策

（記録の保存）

第６４条　情報管理者は、本協議会が独自で所管する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）に違反するなど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。

（電子メールのセキュリティ管理）

第６５条　情報管理者は、本協議会が独自で所管する電子メールのセキュリティ対策に関し、次に掲げる事項を遵守しなければならない。

（１）　権限のない者により、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うこと

（２）　大量のスパムメール等の受信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するなど必要な措置を講じること

（３）　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すること

（４）　職員等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職員等に周知すること

（５）　システム開発や運用、保守等のため委託事業者の作業員による電子メールアドレスの利用について、委託事業者との間で利用方法を取り決めること

（６）　なりすまし等への対策のため、送信ドメイン認証技術（SPF、DKIM 等）によって対策を行うこと

（７）　職員等が不審メールを受信しないよう措置を講じること

（８）　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できないように添付ファイルの監視等のシステム上の措置を講じること

２　情報管理者は、電子メール用のアカウントを職員等に利用させることができる。

３　情報管理者は、前項の規定により職員等が利用するアカウントについて、当該アカウントを利用しなくなったことを確認した場合は、当該アカウントを利用できないよう措置を講じなければならない。

４　情報管理者は、運用上又は技術上の理由により、必要に応じて所管する電子メールの利

用を停止することができる。

5　情報管理者は、前項の規定により電子メールの利用の一部又は全部を停止させる場合は、職員等に対して事前にその内容及び停止期間等を通知しなければならない。

6　情報管理者は、端末等にウイルス感染等の異常が認められた場合又は電子メールを経由して当該異常が拡大するおそれがあると認められた場合は、前項の規定にかかわらず、予告なく電子メールの利用を停止させることができる。

（ウェブサイト）

第６６条　情報管理者は、本協議会が独自で所管する外部に向けて公開するウェブサイトの情報セキュリティに関し、次に掲げる事項を遵守しなければならない。

（１）　原則として、利用者がアクセス可能なページは SSL 等の暗号化通信でアクセスできるようにすること

（２）　管理画面やデータベース等第三者からアクセスされるべきでない情報へのアクセスは、取り扱う情報資産の重要度及び選択した通信回線の種類に応じて、ID 及びパスワード等による認証、通信経路の限定（IP アドレス、MAC アドレス等による制御）及びアプリケーションプロトコルの限定（ポート番号による制御）等必要な情報セキュリティ対策を講じること

（３）　不正アクセスによるウェブページの改ざん対策に努めること

（４）　ウェブサイトで利用していたドメインを廃止する場合は、旧ドメインがなりすまし等に利用されないよう、利用者に対して廃止前後において、十分な期間を設けて周知するものとし、利用者の旧ドメインへのアクセス状況等に応じて、利用をしなくなってから相当の期間、旧ドメインを所有すること

（フィルタリング）

第６７条　情報管理者は、本協議会が独自で所管するネットワークにおけるインターネットの閲覧において、業務に関係のないサイト又はウイルス感染や情報漏えいの危険性を含むサイト等の閲覧ができないようフィルタリング等の防止措置を講じなければならない。

2　職員等は、業務上閲覧が必要なウェブサイトがフィルタリングされている場合は、情報管理者に閲覧の許可を得なければならない。

（インターネットの利用停止）

第６８条　情報管理者は、運用上又は技術上の理由により、必要に応じて本協議会が独自で所管するネットワークにおけるインターネットの利用を停止させることができる。

2　情報管理者は、前項の規定によりインターネットの利用の一部又は全部を停止させる場合は、職員等に対して事前にその内容及び停止期間等を通知しなければならない。

３　情報管理者は、端末等にウイルス感染等の異常が認められた場合又はインターネットを経由して当該異常が拡大するおそれがあると認められた場合は、前項の規定にかかわらず、予告なくインターネットの利用を停止させることができる。

（セキュリティ情報の収集）

第６９条　情報管理者は、セキュリティホール、不正プログラム及びサイバー攻撃等の情報セキュリティに関する情報について、国及び関係団体、民間事業者等から適宜情報を収集しなければならない。

２　情報管理者は、セキュリティホール、不正プログラム及びサイバー攻撃等の情報セキュリティに関する情報について、必要に応じ、関係者間で共有及び職員等に周知しなければならない。

３　情報管理者は、セキュリティホールに関する情報を得た場合は、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講じなければならない。

４　情報管理者は、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。

（ファイルサーバの設定等）

第７０条　情報管理者は、本協議会が独自で所管するファイルサーバについて、職員等が使用できる容量を設定し、事務局に通知しなければならない。

（特定用途機器のセキュリティ管理）

第７１条　情報管理者は、監視カメラシステムや FAX システム等特定の用途に利用する機器を導入する場合は、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。

第６章　人的セキュリティ

（情報セキュリティポリシーの遵守等）

第７２条　情報管理者は、職員等が常に情報セキュリティポリシーを閲覧できるように提示しなければならない。

２　情報管理者は、職員等に対し、情報セキュリティポリシーを理解させ、遵守させるための措置を講じなければならない。

３　職員等は、情報セキュリティポリシーの理解に努めなければならない。

４　職員等は、情報セキュリティポリシーを遵守しなければならない。

５　職員等は、情報セキュリティポリシーに関して不明な点がある場合又は遵守に困難な点がある場合は、情報管理者に相談し、指示を受けなければならない。

６　情報管理者は、情報セキュリティポリシーの遵守状況及び運用上の支障の有無について適宜確認を行うものとし、情報セキュリティポリシーの遵守に困難な点があると判断した場合は、統括情報セキュリティ責任者と協議するものとする。

（業務以外の目的での利用禁止）

第７３条　職員等は、業務以外の目的で情報システムへのアクセス、電子メールの利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。

（端末等の管理）

第７４条　職員等は、第三者による不正閲覧や盗難等の防止のため、情報管理者が配布する端末においては離席時のログオフ、電磁的記録媒体については机上放置をしない等適正な措置を講じなければならない。

２　職員等は、情報管理者が配布する端末及び電磁的記録媒体の利用に当たり、退庁時や出張時等長時間利用を行わない場合は、施錠できる場所に保管しなければならない。

（端末等の障害報告）

第７５条　職員等は、情報管理者が配布する端末等に障害（破損等を含む。）が発生した場合は、障害の状況を確認し、速やかに情報管理者に報告しなければならない。

（端末等の外部への持ち出し）

第７６条　職員等は、情報管理者が配布する端末等を外部に持ち出す場合は、情報管理者と安全管理措置について協議した上で、その許可を得なければならない。

２　職員等は、前項の規定により持ち出した端末の管理に当たっては、盗難や破損、情報漏えい等がないように、必要なセキュリティ対策を講じるものとする。

（個人所有端末の持込み及び利用）

第７７条　職員等は、携帯電話又はスマートフォンによる通話、メッセージサービス等必要最低限の利用を除き、個人所有の端末を業務で使用してはならない。ただし、業務上やむを得ない場合は、情報管理者の許可を得て、使用することができる。

２　職員等が前項の許可を得て、個人所有の端末を業務で使用する場合は、必要な情報セキュリティ対策を講じなければならない。

３　個人所有の端末では、重要度１、重要度２又は重要度３の情報資産は取り扱ってはならない。

（機器構成の変更の制限）

第７８条　職員等は、情報管理者が配布する端末に対し、機器の改造、増設及び交換並びに情報管理者が指示又は案内するもの以外の設定変更を行ってはならない。

（無許可でのネットワーク接続の禁止）

第７９条　職員等は、情報管理者が配布する端末を、情報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。

２　職員等は、情報管理者が許可したもの以外の端末、外部デバイス、電磁的記録媒体又はネットワーク機器を本協議会が所管するネットワークに接続してはならない。

（電磁的記録媒体等の利用）

第８０条　職員等は、情報管理者が配布したもの以外の外部デバイス又は電磁的記録媒体を情報管理者が配布した端末に接続してはならない。ただし、記憶領域を持たない、マウス、キーボード、イヤホン、ヘッドホン及びディスプレイに限り、業務の効率化に寄与すると情報管理者が認める場合は、この限りでない。

２　職員等は、前項ただし書に掲げる場合以外であって、業務上やむを得ず、情報管理者が配布したもの以外の外部デバイス又は電磁的記録媒体を情報管理者が配布した端末等に接続する必要がある場合は、情報管理者の許可を得なければならない。

３　職員等は、前項の規定により認められた外部デバイス又は電磁的記録媒体を利用するに当たり、許可を得た用途以外の利用を行ってはならない。

（ソフトウェアのインストール）

第８１条　職員等は、情報管理者の許可なく、情報管理者が所管するネットワークにおける情報システムに新たなソフトウェアのインストールをしてはならない。ただし、端末等の動作に影響を与えないことが明らかである等の軽微なものに関しては、この限りでない。

２　職員等は、前項ただし書以外の場合であって、業務上の必要により情報管理者から配布された端末にソフトウェアのインストールを行いたい場合は、情報管理者の許可を得な

ければならない。ただし、前条第２項の規定による申請で許可を得た外部デバイス又は電磁的記録媒体を利用するためのソフトウェアのインストールについては、この限りでない。

３　前項の規定による端末へのソフトウェアのインストール作業は、情報管理者が実施するものとする。ただし、インストール作業に専門的な知識を要する場合で、情報管理者がやむを得ないと認める場合に限り、当該委託業者がインストール作業を実施することができるものとする。

（離職後の守秘義務）

第８２条　職員等は、人事異動等により職務を離れる場合は、利用していた情報資産を返却するものとし、知り得た業務情報を守秘しなければならない。

（インターネットの利用）

第８３条　職員等は、次に掲げる端末等を使用してインターネットを利用することができる。

（１）　情報管理者が配布した端末等及びシステム

（２）　第 77 条第１項により情報管理者が使用を承認した個人端末であって、情報管理者が整備したネットワークを利用するもの

２　職員等は、インターネットの利用において、次に掲げる行為をしてはならない。

（１）　第三者の名誉を傷つけること

（２）　第三者のプライバシーを侵害すること

（３）　情報の改ざん、滅失、き損、漏えい等の行為及び故意に虚偽の情報を提供すること

（４）　本協議会の風評を害する内容を提供すること

（５）　法令又は公序良俗に反して利用すること

（６）　第三者の著作権その他知的財産所有権を侵害する行為又は侵害するおそれのある行為をすること

（７）　情報セキュリティポリシーの規定に反すること

３　情報管理者は、前項各号に該当する行為を確認した場合は、当該職員等に対してインターネットの利用中止を命ずることができる。この場合において、中止の命令に従わない職員等に対しては、インターネット閲覧設定の解除や回線の切断等の措置を講じることができる。

４　情報管理者は、インターネットの適正な利用を図るため、職員等の指導及び監督を行うものとする。

５　職員等は、インターネット上で重要度１、重要度２又は重要度３の情報資産を取り扱ってはならない。ただし、重要度２又は重要度３の情報資産について、第 14 条に規定する場合は、この限りでない。

（電子メールの利用）

第８４条　職員等は、電子メールの利用において、次に掲げる行為をしてはならない。

（１）　業務上必要のない電子メールを送信すること

（２）　第三者の名誉を傷つけること

（３）　第三者のプライバシーを侵害すること

（４）　情報の改ざん、滅失、き損、漏えい等の行為及び故意に虚偽の情報を提供すること

（５）　個人情報の保護に関する法律の趣旨に反して、個人情報に係る内容を提供すること

（６）　本協議会の風評を害する内容を提供すること

（７）　法令又は公序良俗に反して利用すること

（８）　第三者の著作権その他知的財産権を侵害する行為又は侵害するおそれのある行為をすること

（９）　情報セキュリティポリシーの規定に反すること

２　情報管理者は、前項各号に該当する行為を確認した場合は、当該職員等に対して電子メールの利用中止を命ずることができる。この場合において、中止の命令に従わない職員等に対しては、電子メール利用の解除等の措置を講じることができる。

３　職員等は、複数人に電子メールを送信する場合は、必要がある場合を除き、BCC 機能等により他の送信先の電子メールアドレスが、受信者側で分からないようにしなければならない。

４　職員等は、差出人が不明なメール若しくは不自然なファイルが添付されたメールを受信した場合若しくは自らが不審メールを開封した場合又は他の職員等が不審メールを開封した形跡を発見した場合は、速やかに情報管理者に報告し、判断を仰がなければならない。

５　情報管理者は、電子メールの適正な利用を図るため、職員等の指導及び監督を行うものとする。

６　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。ただし、情報管理者が認めた場合は、この限りでない。

（職員等による不正プログラム対策）

第８５条　職員等は、不正プログラム対策に関し、次に掲げる事項を遵守しなければならない。

（１）　情報管理者から配布された端末において、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こと

（２）　外部からデータを取り入れる場合は、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） 情報管理者が提供する不正プログラムに関する情報を常に確認すること
（４） ウイルス対策ソフトのパターンファイルが最新であることを常に確認すること

（職員等におけるアカウントの利用）
第８６条　職員等は、自己の利用するアカウントについては、次に掲げる事項を遵守しなければならない。
（１） 自己の利用しているアカウントを他人に利用させないこと
（２） 共用アカウントを利用している場合は、共用している利用者以外に利用させないこと

（パスワードの管理）
第８７条　職員等は、自己の管理するパスワードを厳重に管理し、次に掲げる事項を遵守しなければならない。
（１） パスワードは、他人に知られないようにすること
（２） 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ないこと
（３） パスワードは、長さが８文字以上かつ英数字を組合せたもの以上の複雑さをもつものとすること
（４） パスワードは、漏えいの可能性が懸念される場合は、速やかにパスワードの変更を行うこと
（５） 前号の規定によりパスワードの変更を行う場合は、一定の規則性に基づいたものにしない等変更前のパスワードから類推することが困難なものとすること
（６） ログイン情報は、保存機能を有効にする等端末にパスワードを記憶させないこと
（７） 仮のパスワード（初期パスワード等）は、速やかに変更すること
（８） 共用 ID に対するパスワード以外は、職員等間で共有しないこと
２　情報管理者は、共用 ID 等のパスワードについて、次に掲げる事項を遵守しなければならない。
（１） パスワードは、職員等以外の者に知られないようにすること
（２） パスワードは、秘密にし、職員以外の者からのパスワードの照会等には一切応じないこと
（３） パスワードは、長さが８文字以上かつ英数字を組合せたもの以上の複雑さをもつものとすること
（４） パスワードは、漏えいの可能性が懸念される場合又は人事異動等があった場合は、速やかに変更すること
（５） 前号の規定によりパスワードの変更を行う場合は、一定の規則性に基づいたものにしない等変更前のパスワードから類推することが困難なものとすること
（６） ログイン情報は、保存機能を有効にする等端末にパスワードを記憶させないこと

（７） 仮のパスワード（初期パスワード等）は、速やかに変更すること

（不正アクセスの禁止等）

第８８条　職員等は、他人の ID を使用するなどして情報システムの機器に不正にアクセスをしてはならない。

２　職員等は、離席する際は、情報システムからログオフする等他人に情報システムの不正操作又は不正な閲覧をされないようにしなければならない。

（Web 会議サービスの利用時の対策）

第８９条　職員等は、Web 会議サービスを利用する場合は、情報セキュリティ対策に関する次に掲げる事項を遵守しなければならない。

（１） 重要度１、重要度２又は重要度３の情報を含む会話、資料等の画面共有、ファイルのアップロード等は行わないこと

（２） 会議とは無関係の重要な映像又は音声が入り込まない場所で利用すること

（３） Web 会議を主催する場合は、機密性の高い会議には利用しないこと

（４） Web 会議を主催する場合は、会議に無関係の者が参加できないように対策を講じること

２　前項第１号及び第３号の規定にかかわらず、第 102 条第４項の規定によるサービスを利用する場合は、この限りでない。

第７章　運用

（情報システムの監視義務）

第９０条　情報管理者は、自己が所管する情報システム及びネットワークの動作状況及び通信状況を適時監視するとともに、事故等に対して注意を払わなければならない。

２　情報管理者は、前項の監視により、情報システムに異常があると思慮する場合は、調査しなければならない。

（情報セキュリティポリシー遵守の例外措置）

第９１条　情報管理者は、情報セキュリティポリシーを遵守することが困難な状況で、業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、統括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　情報管理者は、業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、事後速やかに統括情報セキュリティ責任者に報告しなければならない。この場合において、特に重要であるものについては、統括情報セキュリティ責任者は、CISO に報告しなければならない。

（違反時の対応）

第９２条　情報管理者は、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は、当該職員等に対し、速やかに適正な措置を講じるよう命じなければならない。

２　前項の場合において、適正な措置が講じられない場合は、該当する情報システムの使用権限をその使用状況にかかわらず、停止することができる。ただし、改善が認められ、かつ、他の職員等に影響がないことが確認できた場合は、使用を再開しなければならない。

３　職員等は、情報セキュリティポリシーに違反した事実を発見した場合は、直ちに情報管理者に報告しなければならない。

（端末及び電磁的記録媒体等の利用状況調査）

第９３条　CISO が指名した者及び情報管理者は、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使用状況を調査することができる。

（情報セキュリティ緊急時対応計画）

第９４条　CISO は、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に、「一般社団法人

つくばスマートシティ協議会情報セキュリティ緊急時対応計画」（以下「緊急時対応計画」という。）を策定し、情報セキュリティの侵害時には、当該計画に従って適切に対処しなければならない。

２　緊急時対応計画には、次に掲げる事項を定めなければならない。

（１）　対象とするインシデント

（２）　インシデントハンドリングの概要及び具体的手順

（３）　平常時の事前準備及び予防等

（４）　再発防止措置の策定

（５）　訓練及び演習

（６）　評価及び見直し

３　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規定を見直さなければならない。

（情報セキュリティ事故等への対応）

第９５条　職員等は、情報セキュリティポリシーに係る情報セキュリティ事故等が発生したことを認知した場合又は外部から報告を受けた場合は、直ちに情報管理者に報告しなければならない。

２　情報管理者は、前項の規定により情報セキュリティ事故等について報告を受け、又は認知した場合は、緊急時対応計画に従い適正に対処しなければならない。

３　情報管理者は、緊急時対応計画で対象とする情報セキュリティ事故等が発生した場合において、本協議会若しくは本協議会以外の者の情報資産又は本協議会以外の者に対して重大な影響を及ぼすおそれがあるときは、速やかに統括情報セキュリティ責任者及び CISO に報告し、指示を受けなければならない。

４　CISO 及び情報管理者は、重大な情報セキュリティ事故等が発生した場合は、情報セキュリティ委員会を適宜開催し、状況を報告しなくてはならない。

（不正プログラムへの感染等への対応）

第９６条　職員等は、情報セキュリティ事故等を認知し、又は外部から報告を受けた場合において、コンピュータウイルス等不正プログラムへの感染、不正アクセス又はサイバー攻撃の発生又は発生が疑われるときは、直ちに LAN ケーブルの取り外し、無線 LAN の切替スイッチによる切断、無線 LAN 通信を行わない設定への変更等通信が行われないように適切に対処しなければならない。

２　情報管理者は、前条第１項の規定により報告を受け、又は認知した情報セキュリティ事故等において、コンピュータウイルス等不正プログラムへの感染、不正アクセス又はサイバー攻撃の発生若しくは発生が疑われる場合は、当該情報システムの利用状況にかかわらず、情報システムを強制的に停止することができる。

３　情報管理者は、本協議会の情報資産又は外部及び外部の情報資産に対して、重大な影響を及ぼすおそれのある事故等が発生した場合は、情報システムの停止、外部ネットワークの遮断等を含む必要な措置を講じなければならない。

（障害時の措置）

第９７条　情報管理者は、所管する情報システムに障害が発生した場合は、直ちに対策を講じ復旧に努めなければならない。

２　前項の場合において、障害が職員等の業務に影響を及ぼす場合は、職員等に対し障害情報及び復旧情報を通知しなければならない。

第８章　業務委託と外部サービスの利用

（業務委託）

第９８条　情報管理者は、所管する情報システムに係る委託事業者の選定に当たり、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。

（外部委託事業者に対する管理）

第９９条　情報管理者は、委託事業者に対し、守秘義務又はそれに準ずる事項を盛り込んだ契約を締結するとともに、委託業務遂行に関する情報セキュリティ上の遵守すべき事項を理解させなければならない。

２　情報管理者は、前項の規定による契約の範囲内において、委託事業者に情報管理者が配布した端末を使用させることができる。

（業務委託事業者への確認、措置等）

第１００条　情報管理者は、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、前条の規定による契約内容に基づき措置しなければならない。

（外部サービスの利用）

第１０１条　情報管理者は、クラウドサービス等の外部サービス（約款による外部サービスを除く。）を利用する場合は、次の各号に掲げる区分に応じ、当該各号に定める事項を遵守しなければならない。

（１）　インターネット上における外部サービスを利用する場合　重要度１、重要度２又は重要度３の情報資産は取り扱わないこと。ただし、重要度２又は重要度３の情報資産について、第 14 条に規定する場合は、この限りでない。

（２）　インターネット以外の環境で外部サービスを利用する場合　当該サービスで取り扱う情報資産の重要度は、情報管理者と協議し決定すること

（３）　重要度１、重要度２又は重要度３の情報資産を取り扱う場合　情報管理者は、外部サービス事業者の選定にあたり、委託する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すること

（４）　重要度１、重要度２又は重要度３の情報資産を取り扱う場合　データセンター等サービスに関する設備で日本国外にあるものを使用するサービスを利用しないこと

（５）　取り扱う情報資産の重要度に応じて、専用線や VPN の利用等適切な通信回線を選択することとし、高い可用性が求められる情報資産を取り扱う場合　回線やサーバの冗長化等の対策を行うこと

（６）　重要度１、重要度２又は重要度３の情報資産を取り扱う場合　情報漏えい等への

対策として、通信の暗号化等を行うこと

（７） 外部サービスの構築時　管理画面やデータベース等第三者からアクセスされるべきでない情報へのアクセスは、取り扱う情報資産の重要度及び選択した通信回線の種類に応じて、ID 及びパスワード等による認証、通信経路の限定（IP アドレス、MAC アドレス等による制御）及びアプリケーションプロトコルの限定（ポート番号による制御）等必要な情報セキュリティ対策を講じるとともに、当該セキュリティ対策の設定に誤り等がないか確認を行うこと

（８） 外部サービスの終了時　取り扱う情報資産の重要度に応じて、外部サービスで取り扱った情報資産の廃棄及び作成したアカウントの廃棄が実施されていることを確認すること

（９） サービス提供事業者との間で契約を締結する場合　取り扱う情報資産の重要度に応じて、当該サービス提供事業者との間で守秘義務又はそれに準ずる事項を盛り込んだ契約を締結するとともに、外部サービスに関する情報セキュリティ上の遵守すべき事項を理解させること

（約款による外部サービスの利用）

第１０２条　職員等は、約款による外部サービスを利用してはならない。ただし、情報管理者が必要と認めた場合は、この限りでない。

２　職員等は、前項ただし書の規定により利用を認められた約款による外部サービスを利用する場合は、認められた用途以外で利用してはならない。

３　情報管理者は、第１項ただし書の規定により認めた利用目的以外の用途に利用されていないか定期的に確認しなければならない。

４　職員等は、第１項ただし書の規定により情報管理者の許可を得て約款による外部サービスを利用する場合は、当該約款による外部サービスにおいて重要度１、重要度２及び重要度３の情報資産を取り扱ってはならない。ただし、次に掲げる約款による外部サービスは、この限りでない。

（１） 政府情報システムのためのセキュリティ評価制度（ISMAP）のクラウドサービスリストに掲載されているサービス、国等の公的機関が構築したシステム又は LGWAN-ASP サービス等十分に安全性が確保されていると情報管理者が認めたもの

（２） 約款による外部サービスでの情報の取扱いについて当該情報に係る利用者の同意を得た場合であって、安全性について情報管理者と協議を実施し、やむを得ないと認められたもの

５　前項の規定は、職員等が利用登録等のために約款に基づいて当該外部サービス提供者に自己の個人情報を提供していることをもって当該約款による外部サービスの利用を妨げるものではない。ただし、当該個人情報を利用する目的で当該約款による外部サービスを利用してはならない。

第９章　評価及び見直し

（自己点検）

第１０３条　情報管理者は、事務局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、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。

（自己点検結果の報告）

第１０４条　情報管理者は、自己点検の実施結果に不適切な状況があった場合は、その改善策を統括情報セキュリティ責任者に速やかに報告しなければならない。

（自己点検結果の活用）

第１０５条　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。

２　情報管理者は、自己点検の結果に基づき、必要に応じ改善措置を講じなければならない。

（情報セキュリティ監査）

第１０６条　統括情報セキュリティ責任者は、第 104 条の規定に基づき報告を受けた自己点検の結果及び近年に起きたインシデント等の状況により、情報セキュリティリスクがあると判断した場合は、監査を行うよう情報管理者へ指示することができる。

２　情報管理者が前項の規定により監査を行う場合は、監査実施計画を立案し、統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。

（評価及び見直し）

第１０７条　CISO は、情報セキュリティポリシーについて評価及び見直しが必要となる事象が発生した場合は、必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

附　則

この情報セキュリティポリシーは、令和６年４月１日から施行する。