本庄市情報セキュリティ対策基準

平成１８年　１月１０日　策　　定
平成１９年　４月　１日　一部改定
平成２３年　４月　１日　全部改定
平成２５年　４月　１日　一部改定
平成２７年　４月　１日　一部改定
平成２７年　９月　１日　全部改定
平成３０年　４月　１日　一部改定
平成３１年　４月　１日　一部改定
令和　３年　６月　２日　一部改定
令和　８年　４月　１日　一部改定

（目次）

本庄市情報セキュリティ対策基準

１　総則

（１）目的

本対策基準は、本庄市情報セキュリティ基本方針の規定に基づき、本市の情報セキュリティ対策を実施するために必要となる統一的な基準を定めることにより、本市の情報資産を組織として適切に保護することを目的とする。

（２）用語の定義

本対策基準において用いる用語の意義は、本庄市情報セキュリティ基本方針の定義による。

２　組織体制

（１）最高情報セキュリティ責任者

①副市長を、最高情報セキュリティ責任者（CISO:Chief Information Security Officer、以下「CISO」という。）とする。

②CISOは、本市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。

③CISO 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（CSIRT:Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

④CISOは、CISOを助けて本市における情報セキュリティに関する事務を整理し、CISOの命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副CISO」という。）１人を必要に応じて置く。

⑤CISO は、本情報セキュリティポリシーに定められた自らの担務を、副CISO、その他本情報セキュリティポリシーに定める責任者に担わせることができる。

（２）統括情報セキュリティ責任者

①企画財政部長を、CISO直属の統括情報セキュリティ責任者とする。

②統括情報セキュリティ責任者は、CISO及び副CISOを補佐するとともに、CISO及び副CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行うものとする。

（３）情報セキュリティ責任者

①市長事務部局の部局長、教育委員会事務局長、議会事務局長及び上下水道部長を情報セキュリティ責任者とする。

②情報セキュリティ責任者は、当該部局等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。なお、当該部局等の範囲については、別表第１のとおりとする。

（４）情報セキュリティ管理者

①市長事務部局の課長、室長及び次長、教育委員会事務局の課長、図書館長、監査委員事務局長、農業委員会事務局長、議会事務局長並びに地方公営企業部局の課長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課室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。

（５）統括システム管理者

①情報システム課長を統括システム管理者とする。

②統括システム管理者は、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。

（６）システム管理者

①各情報システムの担当課長等を、当該情報システムに関するシステム管理者とする。

②システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

③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・管理を行う。

（７）情報セキュリティ担当者

①各課等に情報セキュリティ担当者を置く。

②情報セキュリティ担当者は、本庄市情報システム管理運営規程（平成２３年本庄市訓令第３号）第５条に規定する情報システム推進担当者をもって充てる。

③情報セキュリティ担当者は、情報セキュリティ管理者の指示等に従い、その所属する課等の情報セキュリティに関する対策の向上を図らなければならない。

（８）情報セキュリティ委員会

①本市の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、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。

②委員会は、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、統括システム管理者をもって組織する。

③委員会の庶務は、企画財政部情報システム課において処理する。

（９）CSIRT の設置・役割

①CISO は、CSIRT を整備し、その役割を明確化しなければならない。

②CISOは、CSIRTに所属する職員を選任し、その中からCSIRT責任者を置かなければならない。また、CSIRT内の業務統括及び外部との連携等を行う職員を定めなければならない。

③CISOは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、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。

④CISO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。

⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。

⑥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・公表対応を行わなければならない。

⑦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。

3　情報資産の分類と管理方法

3．1　情報資産の分類

本市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
自治体機密性３Ａ	行政事務で取り扱う情報資産のうち、「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（自治体機密性３の情報資産に対して） ・必要以上の複製及び配付の禁止 ・保管場所の制限 ・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
自治体機密性３Ｂ	行政事務で取り扱う情報資産のうち、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資産	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
自治体機密性３Ｃ	行政事務で取り扱う情報資産のうち、自治体機密性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	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性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	
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	－

完全性による情報資産の分類

分類	分類基準	取扱制限
自治体完全性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
自治体完全性１	自治体完全性２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

自治体可用性2	行政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、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	・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
自治体可用性1	自治体可用性2の情報資産以外の情報資産	－

３．２　情報資産の管理

（１）管理責任

①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３．１の分類に基づき管理しなければならない。

（２）情報資産の分類の表示

情報資産を取り扱う職員等（以下「職員等」という。）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・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、情報資産の分類を必要に応じて表示しなければならない。

（３）情報資産の利用

①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。

（４）情報資産の保管

①情報セキュリティ管理者又はシステム管理者は、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システム管理者は、自治体機密性２以上、自治体完全性２又は自治体可用性２の情報を記録した電磁的記

録媒体を保管する場合、施錠可能な場所に保管するとともに、可能な限り耐火、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。

（５）情報の送信

電子メール等により自治体機密性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。

（６）情報資産の運搬

①車両等により自治体機密性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自治体機密性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。

（７）情報資産の提供又は公表

①自治体機密性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。

②自治体機密性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。

（８）情報資産の廃棄等

①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。

②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。

③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

①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。

②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　情報の持ち出しの不可設定

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

①LGWAN 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

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 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。

②都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

③業務の効率化・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産を LGWAN 接続系に配置する場合、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。

また、業務の効率化・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や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

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。

（2）サーバの冗長化

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。また、メインサーバに障害が発生した場合には、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。

（3）機器の電源

①システム管理者は、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システム管理者は、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。

（4）通信ケーブル等の配線

①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。

②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切に管理しなければならない。

（5）機器の定期保守及び修理

①システム管理者は、所管する機器の定期保守を必要に応じて実施しなければならない。

②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、事業者に故障を修理させるにあたり、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などを行わなければならない。

（６）庁外への機器の設置

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、統括情報セキュリティ責任者及び統括システム管理者の許可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。

（７）機器の廃棄等

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　管理区域の管理

（１）管理区域の構造等

①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や電磁的記録媒体の保管庫をいう。

②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。

（２）管理区域の入退室管理等

①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、IC カード及び入退室管理簿の記載等による入退室管理を行わなければならない。

②職員等及び外部委託事業者は、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。

（３）機器等の搬入出

①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した業者に確認を行わせなければならない。

②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）通信回線及び通信回線装置の管理

①統括システム管理者は、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切に保管しなければならない。

②統括システム管理者は、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。

③統括システム管理者は、本庄市情報システム管理運営規程（平成２３年本庄市訓令第３号）第２条に規定する基幹系システム及び内部情報系システムのネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

④統括システム管理者は、自治体機密性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。

５．４　職員等のパソコン等の管理

（１）職員等のパソコン等の管理

①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等、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、スマートカード、或いは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。

③システム管理者は､マイナンバー利用事務系では「知識」､「所持」、「存在」を利用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）を行うよう設定しなければならない。

６　人的セキュリティ

６．１　職員等の遵守事項

（１）職員等の遵守事項

①職員等は、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。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。
③職員等は、本市のパソコン等の端末、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。
④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。
⑤職員等は、支給以外のパソコン等の端末及び電磁的記録媒体を原則業務に使用してはならない。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。
⑥職員等は、電磁的記憶媒体を使用する場合には、情報セキュリティ管理者の許可を得なければならない。
⑦職員等は、自治体機密性２以上、自治体可用性２又は自治体完全性２の情報資産を外部で処理する場合は、CISOが定める安全管理措置に関する規定を遵守しなければならない。
⑧職員等は、パソコン等の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システム管理者の許可なく変更してはならない。
⑨職員等は、パソコン等の端末や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。
⑩職員等は、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）会計年度任用職員等への対応
①情報セキュリティ管理者は、会計年度任用職員等に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。
②情報セキュリティ管理者は、会計年度任用職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求め、それを統括システム管理者へ提出しなければならない。
③情報セキュリティ管理者は、会計年度任用職員等にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにし

なければならない。

（３）情報セキュリティポリシー等の掲示

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

（４）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、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。

６．２　研修・訓練

（１）研修・訓練

①CISO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。

②CISOは、新規採用の職員等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。

③情報セキュリティ管理者は、所管する課等の研修の実施状況を記録し、統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。

④統括情報セキュリティ責任者は、研修の実施状況を分析、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。

⑤CISO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。

⑥全ての職員等は、定められた研修・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）職員等からの情報セキュリティインシデントの報告

①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。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者、統括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。

③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及び情報セキュリティ責任者に報告しなければならない。

④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。

（２）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

①職員等は、本市が管理するネットワーク及び情報システム等の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、速やかに統括情報セキュリティ責任者及び統括システム管理者に報告しなければならない。

③情報セキュリティ管理者は、当該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原因の究明・記録、再発防止等

①CSIRT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。

②CSIRT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。

③CSIRTは、情報セキュリティインシデントに関係する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。

④CSIRTは、これらの情報セキュリティインシデントの原因を究明し、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。

⑤CISOは、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及びパスワード等の管理

（１）ICカード等の取扱い

①職員等は、認証に用いるICカード等を、職員等間で共有してはならない。

②職員等は、業務上必要のないときは、ICカード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。

③職員等は、ICカード等を紛失した場合には、速やかにシステム管理

者に通報し、指示に従わなければならない。

④システム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

（２）ID の取扱い

職員等は、自己の利用する ID を他人に利用させてはならない。また、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。

（３）パスワードの取扱い

①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、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（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）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。

⑤職員等は、仮のパスワード（初期パスワード含む）を最初のログイン時点で変更しなければならない。

⑥職員等は、サーバ、ネットワーク機器及びパソコン等の端末のパスワード記憶機能を利用してはならない。

⑦職員等は、自己の利用するパスワードを他人に利用させてはならない。また、共用パスワードを利用する場合は、共用パスワードの利用者以外に利用させてはならない。

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

①統括システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

②統括システム管理者は、文書サーバを課等の単位で構成し、職員等が他の課等の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。

③システム管理者は、特定の職員等しか取扱えない情報資産がある場合は、別途ディレクトリを作成する等の措置を講じ、同一課等であっても、担当職員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。

（２）バックアップの実施

システム管理者は、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。

（３）他団体との情報システムに関する情報等の交換

システム管理者は、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、統括情報セキュリティ責任者、情報セキュリティ責任者及び統括システム管理者の許可を得なければならない。

（４）情報システム仕様書等の管理

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、記録媒体に関わらず、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、適切に管理しなければならない。

（５）ログの取得等

①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。

②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。

（６）ネットワークの接続制御、経路制御等

①システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②システム管理者は、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。

③システム管理者は、外部の者が利用できるシステムについて、必要に応じ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。

④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、統括情報セキュリティ責任者及び統括システム管理者の許可を得なければならない。

⑤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。

⑥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。

⑦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、庁内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。

⑧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、統括システム管理者の判断に従い、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。

（７）複合機のセキュリティ管理

①統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、適切なセキュリティ要件を策定しなければならない。

②統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。

③統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。

（８）IoT機器を含む特定用途機器のセキュリティ管理

統括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実施しなければならない。

（９）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

①統括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。

②統括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。

（１０）電子メールのセキュリティ管理

①統括システム管理者は、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。

②統括システム管理者は、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。

③統括システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④統括システム管理者は、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しなければならない。

（１１）電子メールの利用制限

①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。

②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。

③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。

④職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

（１２）電子署名、暗号化

①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、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。

②職員等は､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鍵を管理しなければならない。

③CISO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。

（１３）無許可ソフトウェアの導入等の禁止

①職員等は、パソコン等の端末に無断でソフトウェアを導入してはならない。

②職員等は、業務上の必要がある場合は、統括システム管理者及び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。

③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。

（１４）機器構成の変更の制限

職員等は、業務上、パソコン等の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には、統括システム管理者及びシステム管

理者の許可を得なければならない。

（１５）無許可でのネットワーク接続の禁止

職員等は、パソコン等の端末を有線・無線を問わず、その端末を接続して利用するよう統括システム管理者及び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。

（１６）業務以外の目的でのウェブ閲覧の禁止

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。

（１７）Web 会議サービスの利用時の対策

①統括システム管理者は、Web 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。

②職員等は、本市の定める利用手順に従い、Web 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。

③職員等は、Web 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ずること。

④職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従って利用すること。

（１８）ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本市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　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市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。

②自治体機密性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。

③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。

④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。

７．２　アクセス制御等

（１）アクセス制御

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。

（２）利用者 ID の取扱い

①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 の取扱いを適切に行わなければならない。

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、システム管理者に通知しなければならない。

③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。

（３）特権を付与された ID の管理等

①システム管理者は、管理者権限等の特権を付与された 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。

②システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

（４）職員等による外部からのアクセス等の制限

①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は、統括システム管理者の許可を得なければならない。

②統括システム管理者は、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統括システム管理者は、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統括システム管理者は、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統括システム管理者は、外部からのアクセスに利用するパソコン等の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、外部から持ち帰ったパソコン等の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、統括システム管理者の許可を得るか、もしくは統括システム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統括システム管理者は、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、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。

（５）パスワードに関する情報の管理

①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。

②システム管理者は、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。

７．３　システム開発、導入、保守等

（１）情報システムの調達

①情報セキュリティ管理者又はシステム管理者は、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。

②情報セキュリティ管理者又はシステム管理者は、機器及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの導入

①情報セキュリティ管理者又はシステム管理者は、システム開発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情報セキュリティ管理者又はシステム管理者は、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。

③情報セキュリティ管理者又はシステム管理者は、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情報セキュリティ管理者又はシステム管理者は、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。

⑤情報セキュリティ管理者又はシステム管理者は、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。

⑥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。

（３）機器等の納入時又は情報システムの受入れ時

①情報セキュリティ管理者又はシステム管理者は、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、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情報セキュリティ管理者又はシステム管理者は、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。

（４）システム開発・保守に関連する資料等の整備・保管

情報セキュリティ管理者又はシステム管理者は、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切に整備・保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①情報セキュリティ管理者又はシステム管理者は、情報システムに入力されるデータについて、範囲、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。

②情報セキュリティ管理者又はシステム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

７．４　不正プログラム対策

（１）不正プログラムに対する措置事項

①システム管理者は、外部ネットワークから受信したファイルに対して、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。

②システム管理者は､外部ネットワークに送信するファイルに対して、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。

③統括システム管理者は、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、必要に応じ職員等に対して注意を喚起しなければならない。

④システム管理者は、所掌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なければならない。

⑤システム管理者は、不正プログラム対策ソフトウェアのパターンファイルを、常に最新の状態に保たなければならない。

⑥システム管理者は、不正プログラム対策のソフトウェアを、常に最新の状態に保たなければならない。

⑦システム管理者は、インターネットに接続していないシステムについて、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しなければならない。

⑧システム管理者は、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一括管理し、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。

⑨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。

（２）職員等の遵守事項

①職員等は、外部からデータ等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。

②職員等は、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。

③職員等は、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しなければならない。

④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わなければならない。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しなければならない。

⑤職員等は、統括システム管理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。

⑥職員等は、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。

７．５　不正アクセス対策

（１）統括情報セキュリティ責任者の措置事項

①不正アクセス対策として使用されていないポートを閉鎖しなければならない。

②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及び統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、埼玉県等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及び統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。

（４）サービス不能攻撃

統括情報セキュリティ責任者及びシステム管理者は、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。

（５）標的型攻撃

統括情報セキュリティ責任者及びシステム管理者は、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）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。

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

①システム管理者は、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。

②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

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

②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。

８．２　情報セキュリティポリシーの遵守状況の確認

（１）遵守状況の確認及び対処

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及び情報セキュリティ実施手順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及び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。

②CISO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統括システム管理者及びシステム管理者は、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及び情報セキュリティ実施手順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切かつ速やかに対処しなければならない。

（２）端末及び電磁的記録媒体等の利用状況調査

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、職員等が使用しているパソコン等の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。

８．３　障害等の報告

（１）障害等の報告

①職員等は、情報セキュリティ基本方針に想定する脅威等による情報資産への障害（以下「障害等」という。）が発生した場合又は発生するおそれがある場合、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報告を受けた情報セキュリティ管理者は、当該障害等が情報システムに関連する場合、速やかに、統括システム管理者及びシステム管理者に報告しなければならない。

③情報セキュリティ管理者は、当該障害等について、必要に応じてCISO、統括情報セキュリティ責任者、情報セキュリティ責任者に報告しなければならない。

④情報セキュリティ管理者は、統括システム管理者及びシステム管理者と連携し､当該障害等を分析し､記録を保存しなければならない。

８．４　緊急時対応計画

（１）緊急時対応計画の策定

CISO又は情報セキュリティ委員会は、重大な障害等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、緊急時対応計画を定めておかなければならない。

（２）緊急時対応計画の見直し

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。

８．５　例外措置

（１）例外措置の許可

情報セキュリティ管理者又はシステム管理者は、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、例外措置を取ることができる。

（２）緊急時の例外措置

情報セキュリティ管理者又はシステム管理者は、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、例外措置の申請書及び審査結果を適切に保管しなければならない。

８．６　違反時の対応

（１）違反時の対応

①統括情報セキュリティ責任者は、情報セキュリティポリシー又は情報セキュリティ実施手順に違反する行動を確認した場合、当該職員等が所属する課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。

②システム管理者等は、情報セキュリティポリシー又は情報セキュリティ実施手順に違反する行動を確認した場合、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

③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、統括情報セキュリティ責任者は、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あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨をCISO及び当該職員等が所属する課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。

９　業務委託と外部サービス（クラウドサービス）の利用

９．１　業務委託

（１）委託事業者の選定基準

①情報セキュリティ管理者又はシステム管理者は、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。

②情報セキュリティ管理者又はシステム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

（２）業務委託実施前の対策

①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要件を明記した契約を締結しなければならない。

ア　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

イ　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

ウ　委託事業者の責任者、委託内容、作業者、作業場所の特定

エ　提供されるサービスレベルの保証

オ　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

カ　委託事業者の従業員に対する教育の実施

キ　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

ク　業務上知り得た情報の守秘義務

ケ　再委託に関する制限事項の遵守

コ　委託業務終了時の情報資産の返還、廃棄等

サ　委託業務の定期報告及び緊急時報告義務

シ　市による監査、検査

ス　市による情報セキュリティインシデント発生時の公表

セ　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）

ソ　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）の締結

②指定管理者を含む委託事業者（以下「委託事業者等」という。）がLGWAN を利用する場合には、委託事業者等との間で次の要件を明記した契約又は協定を締結しなければならない。

ア　情報セキュリティポリシー及び情報セキュリティ実施手順の順守

イ　委託する業務内容に限定した利用

ウ　業務上知り得た情報の守秘義務

エ　委託事業者等の従業員に対する教育

オ　再委託に関する制限事項の遵守

カ　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）

キ　LGWAN の利用については、地方公共団体情報システム機構が定める条件も遵守

（３）業務委託実施期間中の対策

①情報セキュリティ管理者又はシステム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

ア　契約に基づき委託事業者に実施され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

イ　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）

ウ　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

②情報セキュリティ管理者又はシステム管理者は、業務委託の実施期間において、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。

ア　情報の適正な取扱いのための情報セキュリティ対策

イ　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

ウ　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

（４）業務委託終了時の対策

①情報セキュリティ管理者又はシステム管理者は、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情報セキュリティ管理者又はシステム管理者は、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。

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報告を含む検収の受検

イ　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

９．２　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

情報セキュリティ管理者又はシステム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市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又はシステム管理者は、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。

①情報システムのセキュリティ要件の適切な実装

②情報セキュリティの観点に基づく試験の実施

③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

①情報セキュリティ管理者又はシステム管理者は、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。

②情報セキュリティ管理者又はシステム管理者は、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。

（４）本市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

①情報セキュリティ管理者又はシステム管理者は、外部の一般の者が本市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情報セキュリティ管理者又はシステム管理者は、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情報セキュリティ管理者又はシステム管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

９．３　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）

（１）クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、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。）の選定に関する規定を整備しなくてはならない。

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手続

④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運用規程の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

①統括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運用規程として整備しなければならない。

②統括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運用規程として整備しなければならない。

③統括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、以下を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運用規程として整備しなければならない。

ア　クラウドサービスの利用終了時における対策

イ　クラウドサービスで取り扱った情報の廃棄

ウ　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

①情報セキュリティ管理者又はシステム管理者は、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。

②情報セキュリティ管理者又はシステム管理者は、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。また、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。

ア　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クラウドサービス提供者における目的外利用の禁止

イ　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

ウ　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、本市の意図しない変更が加えられないための管理体制

エ　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

オ　情報セキュリティインシデントへの対処方法

カ　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

キ　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情報セキュリティ管理者又はシステム管理者は、クラウドサービスの中断や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情報セキュリティ管理者又はシステム管理者は、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。

ア　情報セキュリティ監査の受入れ

イ　サービスレベルの保証

⑤情報セキュリティ管理者又はシステム管理者は、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。

⑥情報セキュリティ管理者又はシステム管理者は、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情報セキュリティ管理者又はシステム管理者は、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、以下を全て含むセキュリティ要件を定めなければならない。

ア　クラウドサービスに求める情報セキュリティ対策

イ　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

ウ　クラウドサービスに求めるサービスレベル

⑧統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・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。

（４）クラウドサービスの利用に係る調達・契約

①情報セキュリティ管理者又はシステム管理者は、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情報セキュリティ管理者又はシステム管理者は、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。

（５）クラウドサービスの利用についての事前相談

①情報セキュリティ管理者又はシステム管理者は、クラウドサービスの利用を検討している段階から、統括システム管理者へクラウドサービスの利用について事前相談を行わなければならない。

②統括システム管理者はクラウドサービスの利用について事前相談を受けた場合は、クラウドサービスの特性や責任分界点に係る考え方等について助言し、運用規程の遵守を求めなければならない。

（６）クラウドサービスを利用した情報システムの導入・構築時の対策

①統括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、以下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。

ア　不正なアクセスを防止するためのアクセス制御

イ　取り扱う情報の機密性保護のための暗号化

ウ　開発時におけるセキュリティ対策

エ　設計・設定時の誤りの防止

②情報セキュリティ管理者又はシステム管理者は、情報システムにおいてクラウドサービスを利用する際には、情報セキュリティ責任者及び統括システム管理者へ報告しなければならない。

③情報セキュリティ管理者又はシステム管理者は、クラウドサービス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、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

ア　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

イ　クラウドサービスを利用した情報システムの運用・監視中における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

ウ　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

④情報セキュリティ管理者又はシステム管理者は、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・記録しなければならない。

（７）クラウドサービスを利用した情報システムの運用・保守時の対策

①統括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。

ア　クラウドサービス利用方針の規定

イ　クラウドサービス利用に必要な教育

ウ　取り扱う資産の管理

エ　不正アクセスを防止するためのアクセス制御

オ　取り扱う情報の機密性保護のための暗号化

カ　クラウドサービス内の通信の制御

キ　設計・設定時の誤りの防止

ク　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情報セキュリティ管理者又はシステム管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合は、情報セキュリティ責

任者及び統括システム管理者へ報告しなければならない。

③情報セキュリティ管理者又はシステム管理者は、クラウドサービス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。

④情報セキュリティ管理者又はシステム管理者、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。

⑤情報セキュリティ管理者又はシステム管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

（８）クラウドサービスを利用した情報システムの更改・廃棄時の対策

①統括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。

ア　クラウドサービスの利用終了時における対策

イ　クラウドサービスで取り扱った情報の廃棄

ウ　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情報セキュリティ管理者又はシステム管理者は、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・記録しなければならない。

９．４　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱わない場合）

（１）クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱わない場合、以下を含むクラウドサービスの利用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の範囲

②クラウドサービスの利用手続

③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

④クラウドサービスの利用の運用手順

（２）クラウドサービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で自治体機密

性２以上の情報を取り扱わない場合のクラウドサービスの利用を情報セキュリティ管理者又はシステム管理者に申請しなければならない。また、情報セキュリティ管理者又はシステム管理者、当該クラウドサービスの利用において適切な措置を講じなければならない。

②情報セキュリティ管理者又はシステム管理者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスを記録しなければならない。

１０　評価及び見直し

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、定期的に又は必要に応じて監査を行わせなければならない。

（２）監査を行う者の要件

①情報セキュリティ監査統括責任者は、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。

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者でなければならない。

（３）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、情報セキュリティ委員会に報告しなければならない。

（４）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切に保管しなければならない。

（５）監査結果への対応

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。また、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。なお、庁内で横断的に改善が必要な事項については、統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。

（６）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

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。

１０．２　自己点検

（１）実施方法

①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、定期的に又は必要に応じ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、所管する部局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、定期的に又は必要に応じ自己点検を行わなければならない。

（２）自己点検結果に基づく改善

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。

１０．３　情報セキュリティポリシー及び関係規程等の見直し

（１）情報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ふまえ、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。

ただし、緊急を要する場合又は軽微な変更については、CISOの判断で改定を行い、事後速やかに情報セキュリティ委員会に報告するものとする。

別表第１

部局等名称	部局等の範囲
企画財政部	秘書課、企画課、シティプロモーション推進課、財政課、情報システム課、資産マネジメント推進課
総務部	行政管理課、課税課、収納課、会計課、監査委員事務局
市民生活部	市民活動推進課、危機管理課、市民課、支所総務課、支所市民福祉課
福祉部	地域福祉課、生活支援課、障害福祉課、高齢者福祉課、介護保険課
保健部	保険課、健康推進課、子育て支援課、こども家庭センター、保育課
経済環境部	環境推進課、商工観光課、農政課、産業開発室、支所環境産業課、農業委員会事務局
都市整備部	道路管理課、道路整備課、都市計画課、建築開発課、営繕住宅課、市街地整備室
教育委員会事務局	教育総務課、学校教育課、教育環境整備課、生涯学習課、文化財保護課、スポーツ推進課、図書館
議会事務局	議会事務局
上下水道部	経営管理課、施設工務課