みやこ町情報セキュリティ対策基準

令和２年７月１日策定

令和８年３月６日改定

みやこ町情報セキュリティ対策基準

目次

第１章　総則（第１条）
第２章　組織体制（第２条―第９条）
第３章　情報資産の分類及び管理（第１０条―第２０条）
第４章　情報システム全体の強靭性の向上（第２１条―第２３条）
第５章　物理的セキュリティ
　第１節　サーバ等の管理（第２４条―第２９条）
　第２節　管理区域（サーバ室等）の管理（第３０条―第３２条）
　第３節　通信回線及び通信回線装置の管理（第３３条）
　第４節　職員の利用する端末又は電磁的記録媒体等の管理（第３４条）
第６章　人的セキュリティ
　第１節　職員の遵守事項（第３５条―第３８条）
　第２節　研修及び訓練（第３９条―第４２条）
　第３節　情報セキュリティインシデントの報告（第４３条―第４５条）
　第４節　ID及びパスワード等の管理（第４６条―第４８条）
第７章　技術的セキュリティ
　第１節　コンピュータ及びネットワークの管理（第４９条―第７０条）
　第２節　アクセス制御（第７１条―第７５条）
　第３節　システムの開発、導入、保守等（第７６条―第８７条）
　第４節　不正プログラム対策（第８８条―第９１条）
　第５節　不正アクセス対策（第９２条―第９８条）
　第６節　セキュリティ情報の収集（第９９条―第１０１条）
第８章　運用
　第１節　情報システムの監視（第１０２条―第１０４条）
　第２節　情報セキュリティポリシーの遵守状況の確認（第１０５条―第１０７条）
　第３節　侵害時の対応等（第１０８条―第１１１条）
　第４節　例外措置（第１１２条―第１１４条）
　第５節　法令遵守（第１１５条）

第６節　懲戒処分等（第１１６条・第１１７条）
第９章　業務委託と外部サービス（クラウドサービス）の利用
第１節　業務委託（第１１８条―第１２１条）
第２節　情報システムに関する業務委託（第１２２条―第１２５条）
第３節　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）（第１２６条―第１３３条）
第４節　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）（第１３４条・第１３５条）
第１０章　評価及び見直し
第１節　監査（第１３６条―第１４３条）
第２節　自己点検（第１４４条―第１４６条）
第３節　情報セキュリティポリシー及び関係規程等の見直し（第１４７条）
附則

第１章　総則

（趣旨）

第１条　みやこ町情報セキュリティ対策基準は、みやこ町情報セキュリティ基本方針（令和２年みやこ町訓令第９号）を実行に移すための、本町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るものとする。

第２章　組織体制

（最高情報セキュリティ責任者）

第２条　副町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。CISOは、本町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。

２　CISOは、必要に応じ、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最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

（統括情報セキュリティ責任者）

第３条　行政経営課長をCISO直属の統括情報セキュリティ責任者とする。統括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。

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

3　統括情報セキュリティ責任者は、本町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。

4　統括情報セキュリティ責任者は、次条第１項に規定する情報セキュリティ責任者及び第５条第１項に規定する情報システム管理者に対して、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　統括情報セキュリティ責任者は、本町の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、CISOの指示に従い、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権限及び責任を有する。

6　統括情報セキュリティ責任者は、本町の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持及び管理を行う権限及び責任を有する。

7　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、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、情報システム管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

8　統括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。

9　統括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。

（情報セキュリティ責任者）

第４条　町長部局、公営企業、教育委員会、選挙管理委員会、監査委員事務局、農業委員会事務局、固定資産評価審査委員会及び議会事務局の所属課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、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。

3　情報セキュリティ責任者は、その所管する課室等において所有してい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、情報セキュリティポリシーの遵守に

関する意見の集約並びに職員に対する教育、訓練、助言及び指示を行う。

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

（情報システム管理者）

第５条　各情報システムの担当課長を当該システムに関する情報システム管理者とする。

２　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

３　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。

（情報システム担当者）

第６条　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者を情報システム担当者とする。

（みやこ町DX推進本部）

第７条　本町の情報セキュリティ対策を統一的に行うため、みやこ町DX推進本部において、情報セキュリティポリシー等の情報セキュリティに関する重要な事項を決定する。

（兼務の禁止）

第８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。

（CSIRTの整備及び役割）

第９条　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（CSIRT：Computer Security Incident Response Team。以下「CSIRT」という。）を整備し、その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。

３　CISO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

トについて課室等から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。

4　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、その内容を関係課室等に提供しなければならない。

5　CSIRTは、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、福岡県等へ報告しなければならない。

6　CSIRTは、情報セキュリティインシデントを認知した場合には、その重要度又は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は、委託事業者等との情報共有を行わなければならない。

第３章　情報資産の分類及び管理

（情報資産の分類）

第１０条　本町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

<table>
<tr><th>分類</th><th>分類基準</th><th>取扱制限</th></tr>
<tr><td>自治体機密性３Ａ</td><td>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</td><td rowspan="3">・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、保管場所への必要以上の電磁的記録媒体等の持込禁止
・情報の送信、情報資産の運搬及び提供時における暗号化及びパスワードの設定並びに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</td></tr>
<tr><td>自治体機密性３Ｂ</td><td>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</td></tr>
<tr><td>自治体機密</td><td>行政事務で取り扱う情報資産のう</td></tr>
</table>

性３Ｃ	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	・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、又は行政事務の安定的な遂行に支障（軽微	・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

	なものを除く。）を及ぼすおそれがある情報資産	
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	－

（情報資産の管理責任）

第１１条　情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

２　情報セキュリティ責任者は、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。

３　情報セキュリティ責任者は、情報資産が複製され、又は伝送された場合には、複製等された情報資産も前条の表に規定する情報資産の分類に基づき管理しなければならない。

（情報資産の分類の表示）

第１２条　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・フッター等を含む。）、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。

（情報の作成）

第１３条　職員は、業務上必要のない情報を作成してはならない。

２　情報を作成する者は、情報の作成時に第１０条の表に規定する情報資産の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。

３　情報を作成する者は、作成途上の情報についても、紛失、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。

（情報資産の入手）

第１４条　庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

２　庁外の者が作成した情報資産を入手した者は、第１０条の表に規定する情報資産の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。

３　情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリ

ティ責任者に判断を仰がなければならない。

（情報資産の利用）

第１５条　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

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

３　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合は、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（情報資産の保管）

第１６条　情報セキュリティ責任者又は情報システム管理者は、情報資産の分類に従って、情報資産を適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又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書き込み禁止の措置を講じなければならない。

３　情報セキュリティ責任者又は情報システム管理者は、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は、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

（情報の送信）

第１７条　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。

（情報資産の運搬）

第１８条　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、情報セキュリティ責任者に許可を得なければならない。

（情報資産の提供及び公表）

第１９条　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、情報セキュリティ責任者に許可を得なければならない。

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

（情報資産の廃棄等）

第２０条　機密性２以上の情報資産を廃棄やリース返却等をする者は、情報を記録している電磁的記録媒体について、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、情報セキュリティ責任者の許可を得なければならない。

第４章　情報システム全体の強靭性の向上

（マイナンバー利用事務系と他の領域との分離）

第２１条　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。ただし、マイナンバー利用事務系と他の領域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。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を、次のとおり実施しなければならない。

（１）　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、２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、業務ごとに専用端末を設置することが望ましい。

（２）　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。

（LGWAN接続系とインターネット接続系の分割）

第２２条　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。

（１）　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

（２）　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

（３）　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

（インターネット接続系）

第２３条　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及び対処並びにLGWANへの不適正なアクセス等に対する監視等の情報セキュリティ対策を行わなければならない。

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、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。

第５章　物理的セキュリティ

第１節　サーバ等の管理

（機器の取付け）

第２４条　情報システム管理者は、サーバ等の機器の取付けを行う場合は、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。

（機器の電源）

第２５条　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適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。

２　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（通信ケーブル等の配線）

第２６条　統括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。

２　統括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は、連携して対応しなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（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。

４　統括情報セキュリティ責任者及び情報システム管理者は、自ら若しくは情報システム担当者又は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し、又は追加できないように必要な措置を施さなければならない。

（機器の定期保守及び修理）

第２７条　情報システム管理者は、自治体可用性２の情報資産を取り扱うサーバ等の機器の定期保守を実施しなければならない。

２　情報システム管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合は、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は、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。

（庁外への機器の設置）

第２８条　統括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は、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。

（機器の廃棄等）

第２９条　情報システム管理者は、機器の廃棄、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。

第２節　管理区域（サーバ室等）の管理

（管理区域の構造等）

第３０条　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「サーバ室等」という。）並びに電磁的記録媒体の保管庫をいう。

２　統括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。

３　統括情報セキュリティ責任者及び情報システム管理者は、サーバ室等内の機器等に、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　統括情報セキュリティ責任者及び情報システム管理者は、管理区域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。

（管理区域の入退室管理等）

第３１条　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、ICカード、指紋認証等の生体認証又は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　職員及び委託事業者は、管理区域に入室する場合は、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　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、必要に応じて立入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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

４　情報システム管理者は、自治体機密性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。

（機器等の搬出入）

第３２条　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。

２　情報システム管理者は、サーバ室等の機器等の搬出入について、職員を立ち会わせなければならない。

第３節　通信回線及び通信回線装置の管理

（通信回線等の管理）

第３３条　統括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　統括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　統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

4　統括情報セキュリティ責任者は、行政系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。

5　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、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。

6　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上で情報に破壊、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。

7　統括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。

8　統括情報セキュリティ責任者は、自治体可用性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。

第４節　職員の利用する端末又は電磁的記録媒体等の管理

（職員の利用する端末又は電磁的記録媒体等の管理）

第３４条　情報システム管理者は、盗難防止のため、執務室等で利用するパ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、情報システムへのログインパスワード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２つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

第６章　人的セキュリティ

第１節　職員の遵守事項

（職員の遵守事項）

第３５条　職員は、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責任者に相談し、指示を仰がなければならない。

２　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　モバイル端末又は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を、次のとおり実施する。

（１）　CISOは、自治体機密性２以上、自治体可用性２及び自治体完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（２）　職員は、本町のモバイル端末、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、情報セキュリティ責任者の許可を得なければならない。

（３）　職員は、外部で情報処理業務を行う場合には、情報セキュリティ責任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については次のとおりとする。

（１）　職員は、原則として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業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ責任者の許可を得て利用することができる。

（２）　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用いる場合には、情報セキュリティ責任者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

５　情報セキュリティ責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

６　職員は、パソコン又は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責任者の許可なく変更してはならない。

７　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責任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、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。

８　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。

（会計年度任用職員への対応）

第３６条　情報セキュリティ責任者は、職員のうち、地方公務員法（昭和２５年法律第２６１号）第２２条の２第１項に規定する会計年度任用職員（以下「会計年度任用職員」という。）に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員が守るべき内容を理解させ、実施させ、及び遵守させなければならない。

２　情報セキュリティ責任者は、会計年度任用職員の採用の際、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るものとする。

３　情報セキュリティ責任者は、会計年度任用職員にパソコン又はモバイル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は、これを利用できないようにしなければならない。

（情報セキュリティポリシー等の掲示）

第３７条　情報セキュリティ責任者は、職員が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（委託事業者に対する説明）

第３８条　情報セキュリティ責任者は、ネットワーク及び情報システムの開発、保守等を委託事業者に発注する場合は、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を遵守させ、及びその機密事項を説明しなければならない。

第２節　研修及び訓練

（情報セキュリティに関する研修及び訓練）

第３９条　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。

（研修計画の策定及び実施）

第４０条　CISOは、幹部を含め全ての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及びその実施体制の構築を定期的に行い、みやこ町DX推進本部の承認を得なければならない。

２　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。

３　研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者、情報システム担当者及びその他職員に対して、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。

４　CISOは、毎年度１回、みやこ町DX推進本部に対して、職員の情報セキュリティ研修の実施状況について報告しなければならない。

（緊急時対応訓練）

第４１条　CISOは、緊急時の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。

２　訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施できるようにしなければならない。

（研修及び訓練への参加）

第４２条　幹部を含めた全ての職員は、定められた研修及び訓練に参加しなければならない。

第３節　情報セキュリティインシデントの報告

（庁内での情報セキュリティインシデントの報告）

第４３条　職員は、情報セキュリティインシデントを認知した場合は、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に関する統一的な窓口に報告しなければならない。

２　前項の場合において、報告を受けた情報セキュリティ責任者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

３　情報セキュリティ責任者は、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、個人情報又は特定個人情報の漏えい等が発生した場合は、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。

（住民等外部からの情報セキュリティインシデントの報告）

第４４条　職員は、本町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は、情報セキュリティ責任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責任者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

３　情報セキュリティ責任者は、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に報告しなければならない。

（情報セキュリティインシデント原因の究明、記録、再発防止等）

第４５条　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。

２　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。

３　CSIRT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。また、CSIRTは、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。

４　CSIRT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。

５　CISO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。

第４節　ID及びパスワード等の管理

（ICカード等の取扱い）

第４６条　職員は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。

（１）　認証に用いるICカード等を、職員間で共有してはならない。

（２）　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）　ICカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、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。

３　統括情報セキュリティ責任者及び情報システム管理者は、ICカード等を切り替える場合は、切替え前のカードを回収し、破砕する等復元不可能な処理を行った上で廃棄しなければならない。

（IDの取扱い）

第４７条　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。

（１）　自己が利用しているIDは、他人に利用させてはならない。

（２）　共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

（パスワードの取扱い）

第４８条　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。

（１）　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。

（２）　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）　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（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）　パスワードが流出したおそれがある場合には、情報セキュリティ責任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）　複数の情報システムを扱う職員は、同一のパスワードを異なるシステム間で用いてはならない。

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

（７）　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。

（８）　職員間でパスワードを共有してはならない。

第７章　技術的セキュリティ

第１節　コンピュータ及びネットワークの管理

（文書サーバの設定等）

第４９条　情報システム管理者は、職員が使用できる文書サーバの容量を設定し、職員に周知しなければならない。

２　情報システム管理者は、文書サーバを課室等の単位で構成し、職員が他課室等のフォルダ及びファイルを閲覧し、及び使用できないように設定しなければならない。

３　情報システム管理者は、住民の個人情報、人事記録等、特定の職員しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員が閲覧し、及び使用できないようにしなければならない。

（バックアップの実施）

第５０条　統括情報セキュリティ責任者及び情報システム管理者は、業務システムのデータベースや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の有無にかかわらず、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。

２　統括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱う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。

３　統括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱う情報システム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、及び保管しなければならない。

（他団体との情報システムに関する情報等の交換）

第５１条　情報システム管理者は、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は、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の許可を得なければならない。

（システム管理記録及び作業の確認）

第５２条　情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成又は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。

３　統括情報セキュリティ責任者、情報システム管理者、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がシステム変更等の作業を行う場合は、２人以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書等の管理）

第５３条　統括情報セキュリティ責任者は、ネットワーク構成図、情報システム仕様書について、記録媒体の如何にかかわらず、業務上必要とする者以外の者の閲覧、紛失等がないよう、適正に管理しなければならない。

（ログの取得等）

第５４条　統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

２　統括情報セキュリティ責任者は、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。

３　統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検し、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。

（障害記録）

第５５条　統括情報セキュリティ責任者及び情報システム管理者は、職員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５６条　統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

２　統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

３　統括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。

（外部の者が利用できるシステムの分離等）

第５７条　情報システム管理者は、電子申請の汎用受付システム等、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。

（外部ネットワークとの接続制限等）

第５８条　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及び統括情報セキュリティ責任者の許可を得なければならない。

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

３　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。

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

（１）　庁内の全ての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。

（２）　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。

（３）　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。

（４）　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。

５　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、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（複合機のセキュリティ管理）

第５９条　統括情報セキュリティ責任者は、複合機を調達する場合は、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正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正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は、複合機の持つ電磁的記録媒体の全ての情報を抹消し、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。

（IoT機器を含む特定用途機器のセキュリティ管理）

第６０条　統括情報セキュリティ責任者は、IoT機器を含む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。

（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）

第６１条　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は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

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。

（電子メールのセキュリティ管理）

第６２条　統括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。

３　統括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。

４　統括情報セキュリティ責任者は、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職員に周知しなければならない。

５　統括情報セキュリティ責任者は、システムの開発、運用、保守等のため庁舎内に常駐している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なければならない。

（電子メールの利用制限）

第６３条　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。

２　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。

３　職員は、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、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。

４　職員は、重要な電子メールを誤送信した場合は、情報セキュリティ責任者に報告しなければならない。

（電子署名及び暗号化）

第６４条　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。

２　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鍵を管理しなければならない。

３　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。

（無許可ソフトウェアの導入等の禁止）

第６５条　職員は、パソコン又は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。

２　職員は、業務上の必要がある場合は、統括情報セキュリティ責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際、情報セキュリティ責任者又は情報システム管理者は、当該ソフトウェアのライセンスを管理しなければならない。

３　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。

（機器構成の変更の制限等）

第６６条　職員は、パソコン又はモバイル端末に対し機器の改造、増設及び交換を行ってはならない。

２　職員は、業務上、パソコン又はモバイル端末に対し機器の改造、増設又は交換を行う必要がある場合には、統括情報セキュリティ責任者の許可を得なければならない。

（業務外ネットワークへの接続の禁止）

第６７条　職員は、支給された端末を、有線又は無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

２　情報セキュリティ責任者は、支給した端末について、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。

（業務以外の目的でのウェブ閲覧の禁止）

第６８条　職員は、業務以外の目的でウェブを閲覧してはならない。

２　統括情報セキュリティ責任者は、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、情報セキュリティ責任者に通知し適正な措置を求めなければならない。

（ウェブ会議サービスの利用時の対策）

第６９条　統括情報セキュリティ責任者は、ウェブ会議を適切に利用するための利用手順を定めなければならない。

２　職員は、本町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。

３　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。

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

（ソーシャルメディアサービスの利用）

第７０条　情報セキュリティ責任者は、本町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。

（１）　本町のアカウントによる情報発信が、実際の本町のものであることを明らかにするために、本町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。

（２）　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。

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。

５　自治体可用性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、本町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しなければならない。

第２節　アクセス制御

（アクセス制御等）

第７１条　統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとに、アクセスする権限のない職員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。

２　統括情報セキュリティ責任者又は情報システム管理者は、IDの取扱いについて、次に定める措置を講じなければならない。

（１）　統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員の異動、出向、退職者に伴う利用者IDの取扱い等の方法を定めなければならない。

（２）　職員は、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、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

（３）　統括情報セキュリティ責任者及び情報システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。

（４）　統括情報セキュリティ責任者及び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。

３　CISO、統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与されたID及びパスワードの管理について、次に定める措置を講じなければならない。

（１）　統括情報セキュリティ責任者及び情報システム管理者は、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）　統括情報セキュリティ責任者及び情報システム管理者は、管理者権限の特権

を持つ主体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並びに内部からの不正操作及び誤操作を防止するための措置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及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISOが認めた者でなければならない。

（４）　CISOは、前号に規定する代行者を認めた場合は、速やかに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情報システム管理者に通知しなければならない。

（５）　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたID及びパスワードの変更について、委託事業者に行わせてはならない。

（６）　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された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。

（７）　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

(職員による外部からのアクセス等の制限)

第７２条　職員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。

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

３　統括情報セキュリティ責任者は、外部からのアクセスを認める場合は、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は、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　統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員に貸与する場合は、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　職員は、持ち込み、又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと及びパッチの適用状況等を確認し、情報セキュリティ責任者の許可を得るか、又は情報セキュリティ責任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　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報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。

（ログイン時の表示等）

第７３条　情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員がログインしたことを確認することができるようシステムを設定しなければならない。

（認証情報の管理）

第７４条　統括情報セキュリティ責任者又は情報システム管理者は、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、オペレーティングシステム等に認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

２　統括情報セキュリティ責任者又は情報システム管理者は、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、ログイン後、直ちに仮のパスワードを変更させなければならない。

３　統括情報セキュリティ責任者又は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。

（特権による接続時間の制限）

第７５条　情報システム管理者は、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。

第３節　システムの開発、導入、保守等

（機器等の調達に係る運用規程の整備）

第７６条　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。なお、必要に応じて、選定基準の１つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認及び検査手続を整備しなければならない。

（機器等及び情報システムの調達）

第７７条　統括情報セキュリティ責任者及び情報システム管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

２　統括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。

（情報システムの開発）

第７８条　情報システム管理者は、システムの開発の責任者及び作業者を特定しなければならない。また、システムの開発のための規則を確立しなければならない。

２　情報システム管理者は、システムの開発の責任者及び作業者が使用する開発用IDを管理し、開発の完了後、当該開発用IDを削除しなければならない。

３　情報システム管理者は、システムの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い。

４　情報システム管理者は、システムの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。

５　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は、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。

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

（情報システムの導入）

第７９条　情報システム管理者は、システムの開発及び保守並びにテスト環境からシス

テム運用環境への移行について、システム開発及び保守計画の策定時に手順を明確にしなければならない。

2　情報システム管理者は、前項の移行の際、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。

3　情報システム管理者は、導入するシステム又は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　情報システム管理者は、新たに情報システムを導入する場合は、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　情報システム管理者は、運用テストを行う場合は、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　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。

7　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は、開発した組織及び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。

8　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。

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

１０　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。

（情報システムの基盤を管理又は制御するソフトウェア導入時の対策）

第８０条　情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する際は、利用するソフトウェアの特性を踏まえ、次の全ての実施手順を整備しなければならない。

（１）　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

（２）　情報システムの基盤を管理又は制御するソフトウェアで発生した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

（情報システムの基盤を管理又は制御するソフトウェア運用時の対策）

第８１条　情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用･保守する場合は､次の全てのセキュリティ対策を実施しなければならない。

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

（２）　情報システムの基盤を管理又は制御するソフトウェアに対する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

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

（システムの開発及び保守に関連する資料等の整備及び保管）

第８２条　情報システム管理者は、システムの開発及び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、及び保管しなければならない。

２　情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について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。

３　情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次の全ての実施手順を整備しなければならない。

（１）　情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

（２）　情報セキュリティインシデントを認知した際の対処手順

（３）　情報システムが停止した際の復旧手順

４　情報システム管理者は、テスト結果を一定期間保管しなければならない。

５　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。

（情報システムにおける入出力データの正確性の確保）

第８３条　情報システム管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに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　情報システム管理者は、ウェブアプリケーション及び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。

（１）　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を見直ししなければならない。

（２）　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なければならない。

（３）　ウェブアプリケーション及びウェブコンテンツにおいて、情報システム管理者は、故意又は過失により情報が改ざんされ、又は漏えいする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しなければならない。

３　情報システム管理者は、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。

（情報システムの変更管理）

第８４条　情報システム管理者は、情報システムを変更した場合は、プログラム仕様書等の変更履歴を作成しなければならない。

（開発及び保守用のソフトウェアの更新等）

第８５条　情報システム管理者は、開発及び保守用のソフトウェア等を更新し、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（システム更新又は統合時の検証等）

第８６条　情報システム管理者は、システムの更新又は統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。

（情報システムについての対策の見直し）

第８７条　情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本町内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括情報セキュリティ責任者へ報告しなければならない。

第４節　不正プログラム対策

（統括情報セキュリティ責任者の措置事項）

第８８条　統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措

置しなければならない。

（１）　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

（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の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）　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員に対して注意喚起しなければならない。

（４）　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）　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。

（６）　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

（７）　業務で利用するソフトウェアは、パッチ又はバージョンアップ等の開発元のサポートが終了したソフトウェアを利用してはならない。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。

（情報システム管理者の措置事項）

第８９条　情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

（１）　情報システム管理者は、その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システムに常駐させなければならない。

（２）　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

（３）　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

（４）　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う

場合は、コンピュータウイルス等の感染を防止するために、本町が管理している媒体以外を職員に利用させてはならない。また、不正プログラムの感染又は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のパターンファイルの更新を実施しなければならない。

（５）　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、情報システム管理者が許可した職員を除く職員に当該権限を付与してはならない。

(職員の遵守事項)

第９０条　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。

（１）　パソコン又は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。

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

（３）　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

（４）　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

（５）　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、当該ファイルを無害化しなければならない。

（６）　統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

（７）　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行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。

(専門家の支援体制)

第９１条　統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかな

ければならない。

第５節　不正アクセス対策

（統括情報セキュリティ責任者の措置事項）

第９２条　統括情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。

（１）　使用されていないネットワークポートを閉鎖しなければならない。

（２）　不要なサービスについて、機能を削除し、又は停止しなければならない。

（３）　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括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、設定しなければならない。

（４）　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正な対応等を実施できる体制並びに連絡網を構築しなければならない。

（攻撃への対処）

第９３条　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、都道府県等と連絡を密にして、情報の収集に努めなければならない。

（記録の保存）

第９４条　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）に違反する等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（内部からの攻撃）

第９５条　統括情報セキュリティ責任者及び情報システム管理者は、職員及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃又は外部のサイトに対する攻撃を監視しなければならない。

（職員による不正アクセス）

第９６条　統括情報セキュリティ責任者及び情報システム管理者は、職員による不正アクセスを発見した場合は、当該職員が所属する課室等の情報セキュリティ責任者に通知し、適正な処置を求めなければならない。

（サービス不能攻撃）

第９７条　統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からのサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）

第９８条　統括情報セキュリティ責任者及び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。

第６節　セキュリティ情報の収集

（セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等）

第９９条　統括情報セキュリティ責任者及び情報システム管理者は、サーバ装置、端末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。

（不正プログラム等のセキュリティ情報の収集及び周知）

第１００条　統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について職員に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）

第１０１条　統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境又は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。

第８章　運用

第１節　情報システムの監視

（情報システムの運用・保守時の対策）

第１０２条　統括情報セキュリティ責任者及び情報システム管理者は、情報システムの

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

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

（情報システムの監視機能）

第１０３条　統括情報セキュリティ責任者及び情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

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

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

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

（情報システムの監視）

第１０４条　統括情報セキュリティ責任者及び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、情報システムを常時監視しなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

第２節　情報セキュリティポリシーの遵守状況の確認

（遵守状況の確認及び対処）

第１０５条　情報セキュリティ責任者は、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。

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　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には、適正かつ速やかに対処しなければならない。

（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）

第１０６条　CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために、職員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。

（職員の報告義務）

第１０７条　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は、直ちに統括情報セキュリティ責任者及び情報システム管理者に報告を行わなければならない。

２　前項の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統括情報セキュリティ責任者が判断した場合において、職員は、次条に規定する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。

第３節　侵害時の対応等

（緊急時対応計画の策定）

第１０８条　CISO又はみやこ町DX推進本部は、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。

（緊急時対応計画に盛り込むべき内容）

第１０９条　緊急時対応計画には、次の内容を定めなければならない。

（１）　関係者の連絡先

（２）　発生した事案に係る報告すべき事項

（３）　発生した事案への対応措置

（４）　再発防止措置の策定

（業務継続計画との整合性の確保）

第１１０条　自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、みやこ町DX推進本部は、当該計画との情報セキュリティポリシーの整合性を確保しなければならない。

（緊急時対応計画の見直し）

第１１１条　CISO又はみやこ町DX推進本部は、情報セキュリティを取り巻く状況の変化、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。

第４節　例外措置

（例外措置の許可）

第１１２条　情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ関係規程を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得て、例外措置を取ることができる。

（緊急時の例外措置）

第１１３条　情報セキュリティ責任者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、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。

（例外措置の申請書の管理）

第１１４条　CISOは、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

第５節　法令遵守

（法令遵守）

第１１５条　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

（２）　著作権法（昭和４５年法律第４８号）

（３）　不正アクセス行為の禁止等に関する法律

（４）　個人情報の保護に関する法律（平成１５年法律第５７号）

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

（６）　サイバーセキュリティ基本法（平成２６年法律第１０４号）

（７）　みやこ町個人情報保護法施行条例（令和５年みやこ町条例第２号）

第６節　懲戒処分等

（懲戒処分）

第１１６条　情報セキュリティポリシーに違反した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、地方公務員法による懲戒処分の対象とする。

（違反時の対応）

第１１７条　職員の情報セキュリティポリシーに対する違反行為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。

（１）　統括情報セキュリティ責任者が違反行為を確認した場合は、統括情報セキュリティ責任者は、当該職員が所属する課室等の情報セキュリティ責任者に通知し、適正な措置を求めなければならない。

（２）　情報セキュリティ責任者等が違反行為を確認した場合は、違反を確認した者は、速やかに統括情報セキュリティ責任者に通知し、適正な措置を求めなければならない。

（３）　情報セキュリティ責任者の指導によっても違反行為が改善されない場合は、統括情報セキュリティ責任者は、当該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し、又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、職員の権利を停止し、又は剥奪した旨をCISO及び当該職員が所属する課室等の情報セキュリティ責任者に通知しなければならない。

第９章　業務委託と外部サービス（クラウドサービス）の利用

第１節　業務委託

（業務委託に係る運用規程の整備）

第１１８条　統括情報セキュリティ責任者は、業務委託に係る次の内容を全て含む運用規程を整備しなければならない。

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

（２）　委託事業者の選定基準

（業務委託実施前の対策）

第１１９条　情報セキュリティ責任者又は情報システム管理者は、業務委託の実施までに、次に掲げる全ての事項を実施しなければならない。

（１）　委託する業務内容の特定

（２）　委託事業者の選定条件を含む仕様の策定

（３）　仕様に基づく委託事業者の選定

（４）　情報セキュリティ要件を明記した契約の締結

（５）　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　前項第４号に規定する契約に明記する情報セキュリティ等に係る要件は、次のとおりとする。

（１）　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

（２）　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

（３）　委託事業者の責任者、委託内容、作業者及び作業場所の特定

（４）　提供されるサービスレベルの保証

（５）　委託事業者にアクセスを許可する情報の種類及び範囲並びに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

（６）　委託事業者の従業員に対する教育の実施

（７）　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

（８）　業務上知り得た情報の守秘義務

（９）　再委託に関する制限事項の遵守

（１０）　委託業務終了時の情報資産の返還、廃棄等

（１１）　委託業務の定期報告及び緊急時報告義務

（１２）　本町による監査、検査

（１３）　本町による情報セキュリティインシデント発生時の公表

（１４）　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　情報セキュリティ責任者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、次に掲げる全ての事項の実施を委託事業者に求めなければならない。

（１）　仕様に準拠した提案

（２）　契約の締結

（３）　委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

（業務委託実施期間中の対策）

第１２０条　情報セキュリティ責任者又は情報システム管理者は、業務委託の実施期間において、次に掲げる全ての対策を実施しなければならない。

（１）　委託判断基準に従った重要情報の提供

（２）　契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

（３）　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）

（４）　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員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　情報セキュリティ責任者又は情報システム管理者は、業務委託の実施期間において、次に掲げる全ての対策の実施を委託事業者に求めなければならない。

（１）　情報の適正な取扱いのための情報セキュリティ対策

（２）　契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

（３）　委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

（業務委託終了時の対策）

第１２１条　情報セキュリティ責任者又は情報システム管理者は、業務委託の終了に際して、次に掲げる全ての対策を実施しなければならない。

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

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

２　情報セキュリティ責任者又は情報システム管理者は、業務委託の終了に際して、次に掲げる全ての対策の実施を委託事業者に求めなければならない。

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

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

第２節　情報システムに関する業務委託

（情報システムに関する業務委託における共通的対策）

第１２２条　情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本町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。

（情報システムの構築を業務委託する場合の対策）

第１２３条　情報システム管理者は、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、次に掲げる全ての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

（情報システムの運用・保守を業務委託する場合の対策）

第１２４条　情報システム管理者は、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。

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

第１２５条　情報システム管理者又は情報セキュリティ責任者は、外部の一般の者が本町向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

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

３　情報システム管理者又は情報セキュリティ責任者は、委託事業者の信頼性が十分で

あることを総合的及び客観的に評価し判断しなければならない。

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

5　統括情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

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

第３節　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）

（クラウドサービスの選定に係る運用規程の整備）

第１２６条　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には、次の内容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（以下第９章第３節において「クラウドサービス利用判断基準」という。）

（２）　クラウドサービス提供者の選定基準

（３）　クラウドサービスの利用申請の許可権限者と利用手続

（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

（クラウドサービスの利用に係る運用規程の整備）

第１２７条　統括情報セキュリティ責任者は、クラウドサービスにおいて自治体機密性２以上の情報を取り扱う場合には、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、次の内容を含むクラウドサービスの利用に関する運用規程を整備しなければならない。

（１）　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

（２）　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

（３）　次の内容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

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

（クラウドサービスの選定）

第１２８条　情報セキュリティ責任者は、取り扱う情報の格付及び取扱い制限を踏まえ、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い制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定しなければならない。また、次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。

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

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

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

（４）　クラウドサービス提供者の資本関係・役員等の情報、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

（５）　情報セキュリティインシデントへの対処方法

（６）　情報セキュリティ対策その他の契約の履行状況の確認方法

（７）　情報セキュリティ対策の履行が不十分な場合の対処方法

３　情報セキュリティ責任者は、クラウドサービスの中断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　情報セキュリティ責任者は、クラウドサービスの利用を通じて本町が取り扱う情報の格付等を勘案し、必要に応じて次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。

（1）　情報セキュリティ監査の受入れ

（2）　サービスレベルの保証

5　情報セキュリティ責任者は、クラウドサービスの利用を通じて本町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、必要に応じて本町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町に提供し、本町の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

7　情報セキュリティ責任者は、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、次の内容を全て含むセキュリティ要件を定めなければならない。

（1）　クラウドサービスに求める情報セキュリティ対策

（2）　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

（3）　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。

（クラウドサービスの利用に係る調達・契約）

第１２９条　情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウ

ドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

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

（クラウドサービスの利用承認）

第１３０条　情報セキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

２　利用申請の許可権限者は、職員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。

３　利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

（クラウドサービスを利用した情報システムの導入・構築時の対策）

第１３１条　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、次の内容を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

（１）　不正なアクセスを防止するためのアクセス制御

（２）　取り扱う情報の機密性保護のための暗号化

（３）　開発時におけるセキュリティ対策

（４）　設計及び設定時の誤りの防止

２　クラウドサービス管理者は、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、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告しなければならない。

３　クラウドサービス管理者は、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次の全ての実施手順を整備しなければならない。

（１）　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

（２）　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

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

（クラウドサービスを利用した情報システムの運用・保守時の対策）

第１３２条　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、次の内容を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

（１）　クラウドサービス利用方針の規定

（２）　クラウドサービス利用に必要な教育

（３）　取り扱う資産の管理

（４）　不正アクセスを防止するためのアクセス制御

（５）　取り扱う情報の機密性保護のための暗号化

（６）　クラウドサービス内の通信の制御

（７）　設計・設定時の誤りの防止

（８）　クラウドサービスを利用した情報システムの事業継続

２　クラウドサービス管理者は、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には、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合には、統括情報セキュリティ責任者へ報告しなければならない。

３　クラウドサービス管理者は、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、運用及び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　クラウドサービス管理者は、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し、及び記録しなければならない。

（クラウドサービスを利用した情報システムの更改・廃棄時の対策）

第１３３条　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、次の内容を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

（１）　クラウドサービスの利用終了時における対策

（２）　クラウドサービスで取り扱った情報の廃棄

（３）　クラウドサービスの利用のために作成したアカウントの廃棄

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

第４節　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）

（クラウドサービスの利用に係る規定の整備）

第１３４条　統括情報セキュリティ責任者は、次の内容を含む外部サービス（機密性２以上の情報を取り扱わない場合）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申請の許可権限者と利用手続

（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

（クラウドサービスの利用における対策の実施）

第１３５条　職員は、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申請しなければならない。また、承認時に指名されたクラウドサービス管理者は、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　情報セキュリティ責任者は、職員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。

第１０章　評価及び見直し

第１節　監査

（実施方法）

第１３６条　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、毎年度及び必要に応じて監査を行わせなければならない。

（監査を行う者の要件）

第１３７条　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。

（監査実施計画の立案及び実施への協力）

第１３８条　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、みやこ町DX推進本部の承認を得なければならない。

２　被監査部門は、監査の実施に協力しなければならない。

（委託事業者に対する監査）

第１３９条　事業者に業務委託を行っている場合は、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。

（報告）

第１４０条　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、みやこ町DX推進本部に報告する。

（保管）

第１４１条　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。

（監査結果への対応）

第１４２条　CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ責任者に対し、当該指摘事項への対処（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。

２　CISOは、指摘事項を所管していない情報セキュリティ責任者に対しても、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、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（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。

（情報セキュリティポリシー及び関係規程等の見直し等への活用）

第１４３条　みやこ町DX推進本部は、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。

第２節　自己点検

（実施方法）

第１４４条　統括情報セキュリティ責任者及び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。

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

（報告）

第１４５条　統括情報セキュリティ責任者、情報システム管理者は、自己点検の結果と自己点検の結果に基づく改善策を取りまとめ、みやこ町DX推進本部に報告しなければならない。

（自己点検の結果の活用）

第１４６条　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。

２　みやこ町DX推進本部は、自己点検の結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

第３節　情報セキュリティポリシー及び関係規程等の見直し

（見直し）

第１４７条　みやこ町DX推進本部は、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は、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は、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてCISO に報告しなければならない。

附　則

この訓令は、公表の日から施行する。