北九州市情報セキュリティ対策基準

制定日：平成３１年２月２８日

施行日：令和７年４月１日

北九州市

改訂履歴

施行年月日	版番号	改定理由・内容
平成31年4月1日	第1.0版	初版発行（平成31年2月6日決裁、2月28日通知）
令和2年4月1日	第1.1版	見直し（令和2年3月9日決裁、3月11日通知）
令和3年4月1日	第1.2版	組織改正によるもの
令和5年4月1日	第1.3版	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う改定（令和5年3月2日決裁、3月29日通知）
令和6年4月1日	第1.4版	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う改定（令和6年3月1日決裁、3月5日通知）
令和7年4月1日	第1.5版	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う改定（令和7年3月3日決裁、3月17日通知）
令和7年4月1日	第1.6版	組織改正によるもの

目次

北九州市情報セキュリティ対策基準

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

本対策基準の適用範囲は、北九州市情報セキュリティ基本方針に定める行政機関の適用範囲とする。ただし、教育委員会のうち、小学校、中学校、特別支援学校及び高等学校を除く。

具体的な運用は各行政機関が実施手順に定めるものとする。

１　組織体制

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

① 政策局長をCISOとする。CISO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。

② 各行政機関の長は情報セキュリティの組織体制を定める。

（２）兼務の禁止

① 情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

② 監査を受ける者とその監査を実施する者は、止むを得ない場合を除き、同じ者が兼務してはならない。

（３）CSIRT の設置・役割

CISO は、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）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、役割を明確化しなければならない。

CSIRT の対応体制等については、別に定める北九州市情報セキュリティ事故に関する対応要綱によるものとする。

2　情報資産の分類と管理

（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。

区 分	種 別	分 類 基 準
機 密 性の基準	第１種	・個人情報（北九州市情報公開条例第７条第１号で定める個人に関する情報に限り、行政手続における特定の個人を識別するための番号の利用等に関する法律第２条で定める特定個人情報を含む。） ・行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産
	第２種	・不開示情報（北九州市情報公開条例第７条で定める不開示情報をいう。）のうち個人情報を除くもの ・行政事務で取り扱う情報資産のうち、秘密文書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
	第３種	上記第１種及び第２種以外の情報資産
完 全 性の基準	第１種	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（生命、財産、プライバシー）が侵害されるおそれがある情報資産
	第２種	情報資産が改ざん、誤びゅう又は破損により、企業、国及び他の自治体に影響が及ぶもの
	第３種	情報資産が改ざん、誤びゅう又は破損により、市内部の事務に影響が及ぶもの
	第４種	上記第１種から第３種以外の情報資産
可 用 性の基準	第１種	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で、情報システムが停止した場合、当該情報システムの利用ができないことを許容しうる時間が１分以内のもの
	第２種	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で、情報システムが停止した場合、当該情報システムの利用ができないことを許容しうる時間が１分を超え１時間以内のもの
	第３種	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で、情報システムが停止した場合、当該情報システムの利用ができないことを許容しうる時間が１時間を超え１日以内のもの
	第４種	上記第１種から第３種以外の情報資産

（２）情報資産の管理

① 管理責任

（ア）各課（課に準ずる組織を含む。以下同じ。）の長（以下「所属長」という。）は、その所管する情報資産について管理責任を有する。

（イ）所属長は、所管する情報資産に対して、当該情報資産のセキュリティ要件に係る事項について、台帳を整備しなければならない。

（ウ）所属長は、情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

（エ）所属長は、機密性の基準第１種又は第２種の情報資産を取り扱う場所を明確にし、取扱区域として指定しなければならない。

② 情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③ 情報資産の入手

（ア）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。

（イ）庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、所属長に判断を仰がなければならない。

④ 情報資産の利用

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

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

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

⑤ 情報資産の保管

（ア）所属長は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）所属長は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）所属長は、機密性の基準第１種又は第２種、完全性の基準第１種、第２種又は第３種、可用性の基準第１種、第２種又は第３種の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑥ 情報の送信

電子メール等により情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑦ 情報資産の運搬

（ア）車両等により情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）機密性の基準第１種又は第２種の情報資産を運搬する者は、所属長に許可を得なければならない。

⑧ 情報資産の提供・公表

（ア）情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）機密性の基準第１種又は第２種の情報資産を外部に提供する者は、所属長に許可を得なければならない。

（ウ）所属長は、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。

⑨ 情報資産の廃棄等

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

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

（ウ）情報資産の廃棄やリース返却等を行う者は、所属長の許可を得なければならない。

3　情報システム全体の強靭性の向上

（1）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

① LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

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

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

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

（3）インターネット接続系

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等とともに、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 業務の効率性・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、又は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は、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。

４　人的セキュリティ

４．１　職員等の遵守事項

（１）職員等の遵守事項

① 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに所属長に相談し、指示を仰がなければならない。

② 業務以外の目的での使用の禁止

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 パソコン、モバイル端末及び電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア）情報資産を外部で処理する場合は庁内における対策基準に加え、安全管理のための必要な措置を確認したうえで、実施手順を定めなければならない。

（イ）職員等は、本市のパソコン、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、所属長の許可を得なければならない。

（ウ）職員等は、外部で情報処理業務を行う場合には、所属長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

職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をCISOが行い、利用可となった場合であって、業務上必要な場合は、所属長の許可を得て利用することができる。

⑤ 持ち出しの記録

所属長は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

⑥ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定をシステム管理部門又は所属長の許可なく変更してはならない。

⑦ 机上の端末等の管理

職員等は、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所属長の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

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）非常勤及び臨時職員等への対応

① 情報セキュリティポリシー等の遵守

所属長は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時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 インターネット接続及び電子メール使用等の制限

所属長は、非常勤及び臨時職員等にパソコンや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、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

所属長は、職員等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。

（4）委託事業者に対する説明

所属長は、ネットワーク及び情報システムの開発・保守並びにその他情報資産に関する業務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。

4．2　研修・訓練

（1）情報セキュリティに関する研修・訓練

各行政機関は、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。

（2）研修計画の策定及び実施

① 各行政機関は、職員等に対する情報セキュリティに関する研修計画を策定しなければならない。

② 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 研修は、職員等に対して、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 所属長は、所管する課室等の研修の実施状況を記録し、CISO に対して、報告しなければならない。

（3）研修・訓練への参加

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。

４．３　情報セキュリティインシデントの報告

CISOは、情報セキュリティインシデント発生時の報告手順を定め、所属長は、情報セキュリティインシデントが発生した場合、報告手順に従って速やかに報告を行わなければならない。

４．４　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、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。

（ア）認証に用いるICカード等を、職員等間で原則共有してはならない。

（イ）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。

（ウ）ICカード等を紛失した場合には、速やかにICカード発行部署及び所属長に通報し、指示に従わなければならない。

② ICカード発行部署は、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 ICカード発行部署は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕するなど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。

（２）IDの取扱い

職員等は、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。

（３）パスワードの取扱い

職員等は、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、所属長に速やかに報告し、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等は、同一のパスワードをシステム間で用いてはならない。

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

⑦ サーバ、ネットワーク機器及びパソコン等の端末に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

⑧ 職員等間でパスワードを共有してはならない（ただし、共用IDに対するパスワードは除く）。

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

各行政機関のシステム管理部門（以下「システム管理部門」という。）及び業務システム所管課は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。また、パソコン等の機器を設置する場合、ディスプレイに表示される情報が他者から覗き見されないような措置を講じなければならない。

（2）機器の電源

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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。

（3）通信ケーブル等の配線

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③ システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（4）機器の定期保守及び修理

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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、システム管理部門及び業務システム所管課は、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等を行わなければならない。

（5）庁外への機器の設置

システム管理部門及び業務システム所管課は、庁外に業務システムのサーバ等の機器を設置する場合、CISOの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（6）機器の廃棄等

システム管理部門及び業務システム所管課は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

5．2　管理区域（情報システム室等）の管理

（1）管理区域の構造等

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（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

④ システム管理部門及び業務システム所管課は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

（2）管理区域の入退室管理等

① システム管理部門及び業務システム所管課は、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や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 職員等及び委託事業者は、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 システム管理部門及び業務システム所管課は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④ システム管理部門及び業務システム所管課は、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、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（3）機器等の搬入出

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門は、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 システム管理部門は、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 システム管理部門は、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 システム管理部門は、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 システム管理部門は、情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑥ システム管理部門は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

⑦ システム管理部門は、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 システム管理部門は、情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

5．4　職員等の利用する端末や電磁的記録媒体等の管理

① 所属長は、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 システム管理部門及び業務システム所管課は、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、ある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 システム管理部門及び業務システム所管課は、マイナンバー利用事務系（個人

番号利用事務に関わる情報システム及びデータ）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。

５．５　取扱区域の管理

① 所属長は、取扱区域における情報資産の盗難又は紛失等を防止しなければならない。

② 所属長は、外部からの訪問者が取扱区域に入る場合には、必要に応じて職員が付き添うなど、担当者以外のものが容易に閲覧等できないようにしなければならない。

6　技術的セキュリティ

6．1　情報システム全体のあり方

複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響をあたえるリスクが想定されるため、機密性、完全性及び可用性の確保に十分配慮した攻撃に強い情報システムにしなければならない。

6．2　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 システム管理部門は、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 システム管理部門は、文書サーバを課室等の単位で構成し、職員等が他課室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 システム管理部門は、住民の個人情報、人事記録等、特定の職員等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

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し、保管しなければならない。

（3）システム管理記録及び作業の確認

① 業務システム所管課は、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 システム管理部門及び業務システム所管課は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

③ システム管理部門、業務システム所管課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、原則として、2 名以上で作業し、互いにその作業を確認しなければならない。

（４）情報システム仕様書等の管理

システム管理部門及び業務システム所管課は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者の閲覧や、紛失等がないよう、適正に管理しなければならない。

（５）ログの取得等

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（６）障害記録

システム管理部門及び業務システム所管課は、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。

（７）ネットワークの接続制御、経路制御等

① システム管理部門は、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 システム管理部門は、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 システム管理部門は、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。

（８）外部の者が利用できるシステムの分離等

システム管理部門は、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。

（９）外部ネットワークとの接続制限等

① 業務システム所管課は、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、システム管理部門の許可を得なければならない。

② 業務システム所管課は、システム管理部門と連携し、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 業務システム所管課は、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 システム管理部門及び業務システム所管課は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

（ア）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。

（イ）脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

（ウ）ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

（エ）業務システム所管課は、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 業務システム所管課は、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、システム管理部門と連携し、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。

（１０）複合機のセキュリティ管理

① 所属長は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ対策を講じなければならない。

② 所属長は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ 所属長は、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。

（１１）IoT 機器を含む特定用途機器のセキュリティ管理

システム管理部門は、特定用途機器（ネットワークカメラシステム等の通信又は電磁的記録媒体を内蔵する機器）について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（１２）無線 LAN の盗聴対策

① システム管理部門は、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 システム管理部門は、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。

（１３）電子メールのセキュリティ管理

① システム管理部門は、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 システム管理部門は、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 システム管理部門は、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 システム管理部門は、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。

⑤ システム管理部門は、システム開発や運用、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。

（１４）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、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。

④ 職員等は、重要な電子メールを誤送信した場合、所属長に報告しなければならない。

⑤ 職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等において私的な個人アカウント等を原則使用してはならない。

（１５）電子署名・暗号化

① 職員等は、情報資産の分類に応じて、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、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 所属長は、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。

（１６）無許可ソフトウェアの導入等の禁止

① 職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

② 職員等は、業務上の必要がある場合は、情報資産を管理している部門の長の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、所属長は、ソフトウェアのライセンスを適切に管理しなければならない。

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。

（１７）機器構成の変更の制限

① 職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

② 職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報資産を管理している部門の長の許可を得なければならない。

（１８）業務外ネットワークへの接続の禁止

① 職員等は、支給された端末（各所属で調達した端末を含む）を、有線・無線を問わず、その端末を接続して利用するようシステム管理部門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 システム管理部門は、支給した端末について、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。

（１９）業務以外の目的でのウェブ閲覧の禁止

① 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。

② システム管理部門は、職員等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、所属長に通知し適正な措置を求めなければならない。

（２０）ウェブ会議サービスの利用時の対策

① CISO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 職員等は、本市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すること。

（２１）ソーシャルメディアサービスの利用

① 所属長は、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、次の情報セキュリティ対策を行わなければならない。

（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 機密性の基準第１種又は第２種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 可用性の基準第１種及び第２種の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理ウェブサイト等に当該情報を掲載して参照可能とすること。

６．３　アクセス制御

（１）アクセス制御等

① アクセス制御

システム管理部門又は業務システム所管課は、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 利用者IDの取扱い

（ア）システム管理部門及び業務システム所管課は、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の取扱い等の方法を定めなければならない。

（イ）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、システム管理部門又は業務システム所管課に通知しなければならない。

（ウ）システム管理部門及び業務システム所管課は、利用されていないIDが放置されないよう、点検しなければならない。

（エ）システム管理部門及び業務システム所管課は、利用者に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 特権を付与されたIDの管理等

（ア）システム管理部門及び業務システム所管課は、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。

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

（ウ）システム管理部門及び業務システム所管課の特権を代行する者は、システム管理部門の長及び業務システム所管課の長が認めた者でなければならない。

（エ）システム管理部門及び業務システム所管課は、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。

（オ）システム管理部門及び業務システム所管課は、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。

（カ）システム管理部門及び業務システム所管課は、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。

（２）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、システム管理部門及び当該情報システムを管理する業務システム所管課の許可を得なければならない。

② システム管理部門は、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 システム管理部門は、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 システム管理部門は、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 システム管理部門及び業務システム所管課は、外部からのアクセスに利用するモバイル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、持ち込んだ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、パッチの適用状況等を確認し、システム管理部門の許可を得るか、もしくはシステム管理部門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。ただし、閉域網で仮想化技術を用いて庁内のネットワークに接続しているモバイル端末は除く。

⑦ システム管理部門は、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、止むを得ず接続を許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）自動識別の設定

CISO及びシステム管理部門は、ネットワークで使用される端末について、端末固有情報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。

（４）ログイン時の表示等

業務システム所管課は、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等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。

（５）認証情報の管理

① システム管理部門又は業務システム所管課は、職員等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で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

② システム管理部門又は業務システム所管課は、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させなければならない。

③ システム管理部門又は業務システム所管課は、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。

６．４　システム開発、導入、保守等

（１）機器等の調達に係る運用規程の整備

① システム管理部門は、機器等の選定基準を定めなければならない。必要に応じて、選定基準の一つとして、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 システム管理部門及び業務システム所管課は、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・検査手続を整備しなければならない。

（２）機器等及び情報システムの調達

① システム管理部門及び業務システム所管課は、情報システム開発、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。

② システム管理部門及び業務システム所管課は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（３）情報システムの開発

① システム開発における責任者及び作業者の特定

業務システム所管課は、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。また、システム開発のための方針手順等を決定し、開発に適用しなければならない。

② システム開発における責任者、作業者のIDの管理

（ア）システム管理部門及び業務システム所管課は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

（イ）業務システム所管課は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③ システム開発に用いるハードウェア及びソフトウェアの管理

（ア）業務システム所管課は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。

（イ）業務システム所管課は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

④ アプリケーション・コンテンツの開発時の対策

業務システム所管課は、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。

（4）情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

（ア）業務システム所管課は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（イ）業務システム所管課は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（ウ）業務システム所管課は、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。

（エ）業務システム所管課は、所管する情報システムの保守及び点検を定期的に実施しなければならない。

② テスト

（ア）業務システム所管課は、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。

（イ）業務システム所管課は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）業務システム所管課は、個人情報及び機密性の高い生データを、テストデータに原則使用してはならない。

（エ）業務システム所管課は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（オ）業務システム所管課は、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。

③ 機器等の納入時又は情報システムの受入れ時

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

（イ）業務システム所管課は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（5）情報システムの基盤を管理又は制御するソフトウェア導入時の対策

利用するソフトウェアの特性を踏まえ、以下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

（6）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

業務システム所管課は、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。

（7）システム開発・保守に関連する資料等の整備・保管

① 業務システム所管課は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

（ア）業務システム所管課は、情報システムを新規に構築し、又は更改する際には、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CISOに報告しなければならない。

（イ）業務システム所管課は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

・情報セキュリティインシデントを認知した際の対処手順

・情報システムが停止した際の復旧手順

② 業務システム所管課は、テスト結果を一定期間保管しなければならない。

③ 業務システム所管課は、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。

（8）情報システムにおける入出力データの正確性の確保

① 業務システム所管課は、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 業務システム所管課は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

（ア）利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

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

（ウ）ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる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 業務システム所管課は、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。

（9）情報システムの変更管理

業務システム所管課は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（１０）開発・保守用のソフトウェアの更新等

業務システム所管課は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（１１）システム更新又は統合時の検証等

業務システム所管課は、システム更新・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・統合後の業務運営体制の検証を行わなければならない。

（１２）情報システムについての対策の見直し

業務システム所管課は、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、本市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、システム管理部門へ報告しなければならない。

６．５　不正プログラム対策

（1）システム管理部門の措置事項

システム管理部門は、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、必要に応じ職員等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原則利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

（2）業務システム所管課の措置事項

業務システム所管課は、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 業務システム所管課は、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、コンピュータウイルス等の感染を防止するために、市が管理している媒体以外を職員等に利用させてはならない。また、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。
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等に当該権限を付与してはならない。

（3）職員等の遵守事項

職員等は、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 パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
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。
⑥ システム管理部門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。

（4）専門家の支援体制

システム管理部門は、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。

6．6　不正アクセス対策

（1）システム管理部門の措置事項

システム管理部門は、不正アクセス対策として、以下の事項を措置しなければならない。

① 使用されていない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、業務システム所管課へ通報するよう、設定しなければならない。

④ システム管理部門は、情報セキュリティインシデントに対処するための体制と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2）攻撃への対処

システム管理部門は、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。

（3）記録の保存

システム管理部門は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃

システム管理部門及び業務システム所管課は、職員等及び外部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や外部のサイトに対する攻撃を監視しなければならない。

（5）職員等による不正アクセス

システム管理部門及び業務システム所管課は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の所属長に通知し、適正な処置を求めなければならない。

（6）サービス不能攻撃

システム管理部門及び業務システム所管課は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（7）標的型攻撃

システム管理部門及び業務システム所管課は、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。

6．7　セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

システム管理部門及び業務システム所管課は、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

システム管理部門は、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、職員等に周知しなければならない。

（3）情報セキュリティに関する情報の収集及び共有

システム管理部門及び業務システム所管課は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7　運用

7．1　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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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。

④ システム管理部門及び業務システム所管課は、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。

（3）情報システムの監視

① システム管理部門及び業務システム所管課は、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 システム管理部門及び業務システム所管課は、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。

7．2　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 各行政機関は、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、速やかに関係各所に報告しなければならない。

② 各行政機関は、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 各行政機関は、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。

（2）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

各行政機関は、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、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（3）職員等の報告義務

① 職員等は、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、定められた手続きにより直ちに報告を行わなければならない。

② 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると各行政機関の長が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

7．3　侵害時の対応等

（1）緊急時対応計画の策定

各行政機関は、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切に実施するために、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切に対処しなければならない。

（2）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

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

（3）業務継続計画との整合性確保

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、各行政機関は当該計画と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。

（4）緊急時対応計画の見直し

各行政機関は、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。

7．4　例外措置

（1）例外措置の許可

各行政機関は、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、各行政機関の長の許可を得て、例外措置を講じることができる。

（２）緊急時の例外措置

各行政機関は、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、事後速やかに各行政機関の長に報告しなければならない。

７．５　法令遵守

（１）法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

① 地方公務員法(昭和25 年法律第261号)
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（平成11 年法律第128号）
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律（平成25年法律第27号）
⑥ サイバーセキュリティ基本法（平成26年法律第104号）
⑦ 北九州市個人情報の保護に関する法律施行条例（令和5年条例第2号）

（２）マイナンバーガイドライン

マイナンバーを扱う個人番号利用事務及び個人番号関係事務は、個人情報保護委員会が定める「特定個人情報の適正な取扱いに関するガイドライン」を遵守しなければならない。

７．６　違反時の対応

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には、速やかに次の措置を講じなければならない。

① CISO が違反を確認した場合は、CISO は当該職員等が所属する課室等の所属長に通知し、適正な措置を求めなければならない。
② 指導によっても改善されない場合、CISO 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。

8　業務委託とクラウドサービスの利用

8．1　業務委託

（1）委託事業者の選定基準

所属長は、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）業務委託実施前の対策

所属長は、業務委託の実施までに、以下を全て含む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

重要な情報資産を取り扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。

・ 情報セキュリティポリシー等の遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・ 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・ 提供されるサービスレベルの保証
・ 委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・ 委託事業者の従業員に対する教育の実施
・ 提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・ 業務上知り得た情報の守秘義務
・ 再委託に関する制限事項の遵守
・ 委託事業者のデータの保管に関する事項
・ データの複写及び複製の禁止に関する事項
・ データの授受及び搬送に関する事項
・ 委託業務終了時の情報資産の返還、廃棄等の報告義務
・ 委託業務の定期報告、完了報告及び緊急時報告義務
・ 市による監査、検査
・ 市による情報セキュリティインシデント発生時の公表
・ 特定個人情報を取り扱う従事者の明確化に関する事項
・ 漏えい事案等が発生した場合の委託先の責任に関する事項
・ 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に関する事項
・ 委託事業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、情報システムに地方公共団体の意図せざる変更が加えられないための管理体制に関する事項

・ 委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）・実績及び国籍に関する情報提供
・ 情報システムのセキュリティ要件の適切な実装に関する事項
・ 情報セキュリティの観点に基づく試験の実施に関する事項
・ 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に関する事項
・ 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関する事項
・ 情報システムの変更内容についての委託事業者からの速やかな報告に関する事項
・ その他データの保護に関し必要な事項
・ 前記各事項の定めに違反した場合における契約解除等の措置及び損害賠償に関する事項

（3）確認・措置等

所属長は、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、（2）の契約に基づき確認・措置を実施しなければならない。

8．2　クラウドサービスの利用

事業者等の本市の外部の組織が、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（以下「クラウドサービス」という。）の利用については、CISO が別途整備する利用基準に基づいて行うこととする。

9　監査・自己点検

9．1　監査

（1）情報セキュリティ監査

① 各行政機関は、情報セキュリティ監査を実施しなければならない。
② 各行政機関は、情報セキュリティ監査の体制及び計画を定めなければならない。

（2）委託事業者に対する監査

事業者に業務委託を行っている場合、所属長は委託事業者（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、定期的に又は必要に応じて監査を行わなければならない。

９．２　自己点検

（１）実施方法

① システム管理部門及び業務システム所管課は、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 各行政機関は、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、毎年度及び必要に応じて自己点検を行わなければならない。

（２）自己点検結果の活用

① 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 各行政機関は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．３　情報セキュリティポリシー及び関係規程等の見直し

各行政機関は、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置した結果について CISO に報告しなければならない。