那須塩原市情報セキュリティ対策基準

平成２８年９月策定
令和　３年５月改訂
令和　６年９月改訂
令和　８年３月改訂

那須塩原市デジタル推進課

目次

はじめに

本対策基準は、那須塩原市情報セキュリティ規則（以下「規則」という。）の規定を実行に移すため、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。なお、本対策基準における用語の定義及び適用範囲は、別段の定めがない限り、規則で定めるところによる。

第１章 組織体制

１.１ 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。）

⑴ 規則第８条に規定するCISOは、次に掲げる職務を所掌する。

① 情報セキュリティ対策に関する総合的な管理運営に関すること。

② 情報セキュリティの確保及び個人情報の安全管理に関すること。

⑵ CISOは、企画部に属する事務を所掌する副市長をもって充てる。

⑶ 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、役割を明確化する。

⑷ CISOは、本市における情報セキュリティに関する事務についてCISOを補佐し、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(DISO：Deputy chief Information Security Officer、以下「DISO」という。)を一人任命することができる。

⑸ CISOは、本対策基準に定められた自らの担務を、DISOその他の本対策基準に定める責任者に担わせることができる。

２　各実施機関の代表者

⑴ 各実施機関（市長を除く。以下同じ。）の代表者は、情報セキュリティポリシーを遵守し、その所管する情報資産及び情報セキュリティを管理しなければならない。

⑵ 各実施機関の代表者は、CISO及びDISOとの連携を密にし、各実施機関の情報セキュリティ責任者とともに、情報セキュリティ対策を推進しなければならない。

３　統括情報セキュリティ責任者

⑴ CISO及びDISOを補佐する者として、統括情報セキュリティ責任者(以下「統括責任者」という。)を置く。

⑵ 統括責任者は、企画部長をもって充てる。

⑶ 統括責任者は、本市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。

⑷ 統括責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

⑸ 統括責任者は、本市の情報資産に対する情報セキュリティインシデントが発生し、又はそのおそれがある場合において、CISO又はDISOの指示に従うとともに、CISO及びDISO

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。

⑹　統括責任者は、本市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。

⑺　統括責任者は、情報セキュリティインシデントが発生したときは、直ちにCISO及びDISOに報告を行うとともに、情報資産の回復のための対策を講じなければならない。

⑻　統括責任者は、情報セキュリティ責任者、情報セキュリティ管理者に対して、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。

⑼　統括責任者は、情報セキュリティインシデント発生時等の円滑な情報共有を図るため、CISO、DISO、統括責任者、統括管理者、セキュリティ責任者、セキュリティ管理者を網羅する 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。この場合において、各実施機関の代表者に対しても必要に応じて適切に情報の共有が図ることができるよう、各実施機関のセキュリティ責任者に対し連絡体制の構築を求めなければならない。

⑽　統括責任者は、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把握し、必要に応じてCISO及びDISOにその内容を報告しなければならない。

⑾　統括責任者は、情報セキュリティ監査に関する計画の策定、その実施及び結果の承認について権限及び責任を有する。

4　統括情報セキュリティ管理者

⑴　情報セキュリティ及び情報システムに関する専門的な観点から統括責任者を補佐する者として、統括情報セキュリティ管理者(以下「統括管理者」という。)を置く。

⑵　統括管理者は、企画部デジタル推進課長をもって充てる。

⑶　統括管理者は、本市のセキュリティ対策の実施状況について取りまとめなければならない。

⑷　統括管理者は、本市のネットワーク及び情報システムの適正な管理及び運営を取りまとめなければならない。

⑸　統括管理者は、職員に対しセキュリティ教育を実施しなければならない。

⑹　統括管理者は、情報セキュリティインシデント等に関する情報を収集し、必要に応じて関係する組織に周知しなければならない。

5　情報セキュリティ責任者

⑴　各実施機関の部及び事務局におけるセキュリティ対策を実施する者として、部長等及び会計管理者を情報セキュリティ責任者(以下「セキュリティ責任者」という。)とする。

※部局等：各部及び各事務局(会計課を含む。)

※部長等：庁議等規則第３条第１号に掲げる部長等

⑵　セキュリティ責任者は、その所掌する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。

⑶　セキュリティ責任者は、その所掌する部局等において所管している情報システムにおける導入、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

⑷　セキュリティ責任者は、所掌する部局等において所有している情報システムについて、情報セキュリティインシデント発生時等における連絡体制の整備並びに職員に対し、情

報セキュリティに関する教育、訓練、助言及び指示を行うものとする。

6　情報セキュリティ管理者

⑴　セキュリティ責任者を補佐する者として課長等を情報セキュリティ管理者(以下「セキュリティ管理者」という。)とする。ただし、施設にあっては施設長をセキュリティ管理者とする。

※課長等：庁議等規則第３条第２号に掲げる課長等

⑵　セキュリティ管理者は、その所掌する課、室又は施設(以下「課等」という。)におけるセキュリティ対策に関する権限及び責任を有する。

⑶　セキュリティ管理者は、その所掌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。

⑷　セキュリティ管理者は、その所掌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。

⑸　セキュリティ管理者は、その所掌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。

⑹　セキュリティ管理者は、その所掌する課等において使用している情報システムについて、情報セキュリティインシデント発生時等における連絡体制を整備する。

⑺　セキュリティ管理者は、その所掌する課等において、情報資産に対する情報セキュリティインシデントが発生し、又はそのおそれがある場合には、速やかにCISO、DISO、統括責任者、統括管理者及びセキュリティ責任者に報告を行い、指示を仰がなければならない。

7　デジタル推進課

デジタル推進課は、情報セキュリティの総合的な管理及び運営に関する事務を円滑に行う。

8　情報セキュリティタスクフォースの設置

⑴　市の情報セキュリティに関する重要事項を協議し、総合的な調整を行うため、情報セキュリティタスクフォース（以下「対策本部」という。）を設置する。

⑵　対策本部には、本部長、副本部長を置き、部長等及び会計管理者をもって組織する。

⑶　本部長はCISOが兼ねるものとし、副本部長は本部長が指名する。

⑷　本部長は、対策本部を統括し、会議の結果を市長へ報告する。

⑸　本部長に事故があるとき、又は本部長が欠けたときは、副本部長がその職務を代理する。

⑹　対策本部の会議は、必要に応じて本部長が招集する。

⑺　本部長は、必要があると認めるときは、学識経験者その他の者に会議への出席を求め、必要な資料を提出させ、又はその意見を聴くことができる。

⑻　情報セキュリティ対策を総合的かつ統一的に行い、特定の事項を調査、研究及び検討するため、情報セキュリティ対策専門部会を置くことができる。

9　兼務の禁止

⑴　情報セキュリティ対策の実施において、特に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。

⑵　監査を受ける者とその監査を実施する者は、特にやむを得ない場合を除き、同じ者が兼務してはならない。

10　CSIRTの設置・役割

⑴　CISOは、CSIRTを整備し、その役割を明確化しなければならない。

⑵　CISOは、CSIRTに所属する職員等を選任し、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等を定めなければならない。

⑶　CISOは、情報セキュリティに関する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。

⑷　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、第７章に規定する緊急時対応計画に沿ってCISO、総務省、都道府県等へ報告しなければならない。

⑸　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。

⑹　CSIRTは、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、外部委託事業者等との情報共有を行わなければならない。

第２章 情報資産の分類と管理方法

２．１ 情報資産の分類

１　情報資産の重要度区分

本市における情報資産は、重要度により、次のとおり区分し、必要に応じ取扱制限を行うものとする。

重要度区分		内容
最重要情報	個人情報	個人に関する情報 １　個人情報の保護に関する法律(平成15年法律第57号)第2条第1項に規定する個人情報 ２　那須塩原市情報公開条例(平成20年那須塩原市条例第31号)第6条第2号に規定する個人に関する情報 ３　行政手続き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5月31日法律第27号)第2条第8項に規定する特定個人情報（以下「特定個人情報」という。）
	個人情報以外	１　情報が脅威にさらされた場合に、個人又は法人に損失及び不利益を与える情報 ア　法令又は条例の規定により非公開とする情報 イ　法人又は個人の権利、競争上の地位等、正当な利益を害するおそれのある情報 ウ　公正かつ円滑な人事の確保に支障が生ずるおそれのある人事情報(勤務成績、人事評定等) エ　監査、検査、試験等に係る事務に関し、正確な事実の把握を困難にするおそれのある情報 ２　情報が脅威にさらされた場合に、事務又は事業の遂行に著しく支障を与える情報、公正かつ能率的な遂行を不当に阻害するおそれのある要領、内規、運用及び管理手順書並びに調査研究情報(未発表の研究情報等) ３　その他セキュリティ管理者が必要と認める情報（那須塩原市情報公開条例で公開しないことができると考えられる情報等）
重要情報		行政事務で取り扱う情報のうち、秘密文書に相当する機密性は有しないが、直ちに一般に公表することを前提としていない情報
一般情報		最重要情報、重要情報に該当しない情報

2　情報システムの区分

本市における情報システムを次のとおり区分する。

システム区分	内容
1	1　侵害及び破壊等が、個人若しくは法人に重大な損害及び不利益を与える情報システム 2　侵害及び破壊等が、事務又は事業の遂行に著しく支障を及ぼすおそれのある情報システム 3　法令又は条例の規定により公開することができないとされている
2	情報を取り扱う情報システム システム区分１以外の情報システム

2．2 情報資産の管理方法

1　情報資産の管理責任

⑴　統括管理者及び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。

⑵　情報システムを所管するセキュリティ管理者は、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。

⑶　セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産についても「２．１ 情報資産の分類 １ 情報資産の重要度区分」に基づき管理しなければならない。

⑷　職員は、作成・入手した情報を「１ 情報資産の重要度区分」に従って取り扱わなけれならない。ただし、情報の区分が不明確な場合はセキュリティ管理者を通じてセキュリティ責任者に相談の上、判断するものとする。

⑸　セキュリティ管理者は、クラウドサービスの環境に保存される情報資産についても「２．１ 情 報資産の分類 １ 情報資産の重要度区分」に基づき管理しなければならない。また、情報資産におけるライフサイクル(作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等)の取扱いを定めるとともに、クラウドサービスを更改する際の情報資産の移行及びクラウドサービス の利用を終了する際の情報資産の削除について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

2　情報資産へのアクセス制限

⑴　統括管理者又はセキュリティ管理者は、最重要情報へのアクセスを業務上知る必要がある 職員に限定しなければならない。

⑵　統括管理者及びセキュリティ管理者は、重要情報へのアクセスを職員に限定しなければならない。

3　情報資産の保管

⑴　職員は、個人所有の機器(パソコン、スマートフォン、タブレット等)や電磁的記録媒体等へ情報資産を保存してはならない。

⑵　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セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑶　セキュリティ管理者は、最重要情報が含まれる帳票に関して、使用時以外はロッカー、キャビネット等で常時施錠保管しなければならない。

⑷　セキュリティ管理者は、重要情報が含まれる帳票を第三者の目に触れない場所に保管しなければならない。

⑸　セキュリティ管理者は、電磁的記録媒体等に関して、重要度区分に関係なく、使用時以外はロッカー、キャビネット等で施錠保管しなければならない。また、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。

⑹　職員は、重要情報以上の情報資産について、デジタル推進課が管理するオンラインストレージ又はファイルサーバ等と同等のアクセス制限等のセキュリティ対策が講じられた場所に格納しなければならない。ただし、最重要情報のうち特定個人情報に該当するものは、マイナンバー利用事務系の領域又は同等のアクセス制限等のセキュリティ対策が講じられた場所に格納することとし、オンラインストレージへの格納は禁止とする。

⑺　セキュリティ管理者は、「２．１　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。

⑻　セキュリティ管理者は、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。

⑼　セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、安全な場所に保管しなければならない。

4　情報資産の印刷、複製及び複写

⑴　最重要情報の印刷、複製(電子データのコピー等)及び複写(紙のコピー等)は、業務上やむを得ない場合を除き、禁止とする。

⑵　重要情報の印刷、複製及び複写は必要最低限とする。

5　情報資産の電子メール送信

⑴　最重要情報を外部にメール送信することは原則禁止とする。ただし、業務上やむを得ない場合は、セキュリティ管理者の許可の下、データの暗号化又はパスワード設定をした上で送信しなければならない。

⑵　重要情報を外部にメール送信する場合は、セキュリティ管理者の判断の下、パスワードの設定及びセキュリティ管理者への同報等の必要な措置を講じた上で送信しなければならない。

6　情報資産のFAX送信

最重要情報は、FAXでの送信を原則禁止とする。ただし、業務上やむを得ない場合はセキュリティ管理者の許可を得て送信すること。その場合、送信先の事前確認及び到着確認を行わなければならない。

7　情報資産の郵送等

⑴　最重要情報を含む帳票及び電磁的記録媒体は、郵送等を原則禁止とする。ただし、業務上やむを得ない場合はセキュリティ管理者の許可を得て送付すること。その場合、特定記録 郵便等の追跡可能な送付方法を講じた上で親展表示などのセキュリティ対策を実施しなければならない。また電磁的記録媒体に関しては、データの暗号化又はパスワード設定をした上で送付しなければならない。

⑵　重要情報を含む帳票及び電磁的記録媒体を郵便等で送付する場合には、書留相当で送付すること。また電磁的記録媒体に関しては、データの暗号化又はパスワード設定をした上で送付しなければならない。

8　オンラインストレージサービスを利用した情報資産の送信

⑴　最重要情報をオンラインストレージサービス経由で送信することは原則禁止とする。ただし、業務上やむを得ない場合はセキュリティ管理者の許可の下、原則としてデジタル推進課が管理するオンラインストレージサービスにより、データの暗号化又はアクセス制限等のセキュリティ対策を講じた上で送信しなければならない。

⑵　重要情報をオンラインストレージサービス経由で送信する場合は、セキュリティ管理者の判断の下、パスワード設定及びセキュリティ管理者への同報等の必要な措置を講じた上で送信しなければならない。

9　情報資産の運搬

⑴　車両等により最重要情報又は重要情報に該当する情報資産を運搬する場合には、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。

⑵　最重要情報又は重要情報に該当する情報資産を運搬する場合には、セキュリティ管理者に許可を得なければならない。

10　情報資産の廃棄

⑴　情報資産の廃棄やリース返却等を行う場合には、セキュリティ管理者の許可を得て、記録されている情報の機密性に応じ、記載内容が判読できない状態で廃棄しなければならない。

⑵　廃棄する帳票・電磁的記録媒体等を集積する場合は、施錠できる場所に保管しなければならない。

⑶　情報資産の廃棄やリース返却等を行う場合は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

⑷　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了に際して、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならな い。

第３章 情報システム全体の強靭性の向上

３．１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

⑴ マイナンバー利用事務系と他の領域との通信は原則禁止とする。

⑵ マイナンバー利用事務系と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との通信の必要がある場合は、通信経路の限定(MACアドレス、IPアドレス等)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った特定通信とする。

⑶ 国等の公的機関が構築したシステム等との特定通信においては、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は可能とする。

２ 情報のアクセス及び持ち出しにおける対策

⑴ 正規の利用者かどうかを判断するため、パスワード、ICカード、或いは生体認証等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。

⑵ 電磁的記録媒体による情報資産の持出しは原則禁止とする。ただし、電磁的記録媒体の利用がやむを得ない場合は、電磁的記録媒体管理実施手順書により利用しなければならない。

３ マイナンバー利用事務系と接続するガバメントクラウド上の情報システムの取扱いマイナンバー利用事務系のパソコン・サーバ等と専用回線により接続するガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、他の領域とはネットワークを分離しなければならない。

４ マイナンバー利用事務系と接続されるガバメントクラウド上の情報資産の取扱い

⑴ マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

⑵ クラウドサービスを利用する場合、クラウドサービス事業者が実施する暗号に関する対策やその内容について情報を入手し、理解に努め、必要な措置を行わなければならない。

３．２ 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。

２ インターネット接続系との通信の無害化

⑴ インターネット環境で受信したメールをLGWAN接続系に取り込む場合は、本文のみを転送するメールテキスト化等の方法により無害化しなければならない。

⑵ LGWAN接続系のパソコン等からインターネット環境にアクセスする場合は、仮想化したインターネット接続系のサーバ等からの画面転送等の方法により通信を無害化しなければならない。

⑶　インターネット接続系からLGWAN接続系にデータを取り込む場合は、危険因子をファイルから除去するサニタイズ処理等の方法によりデータを無害化しなければならない。

3　LGWAN接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をLGWAN接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

3.3インターネット接続系

1　インターネット接続系のセキュリティ対策

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。

第４章 物理的セキュリティ

４．１物理的セキュリティ対策の実施

１　物理的セキュリティ対策の適用

⑴　統括責任者及び統括管理者並びにシステム区分１の情報システムを所管するセキュリティ責任者及びセキュリティ管理者は、システム区分１に分類される情報システムの物理的セキュリティ対策について、本章に規定する対策を全て適用しなければならない。

⑵　統括責任者及び統括管理者並びにシステム区分２の情報システムを所管するセキュリティ責任者及びセキュリティ管理者は、システム区分２に分類される情報システムの物理的セキュリティ対策について、本章に規定する対策に準ずるよう努めなければならない。ただし、情報セキュリティ対策専門部会がシステム区分２であっても重要情報以上の情報を取り扱うシステムと判断した場合は、本章に規定する対策を全て適用しなければならない。

４．２サーバ等の管理

１　機器の取付け

統括管理者及び情報システムを所管するセキュリティ管理者は、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

統括管理者及び情報システムを所管するセキュリティ管理者は、重要情報以上の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、同一データを保持するよう努めなければならない。

３　機器の電源

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、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。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、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

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、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、可能な限り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。

⑵　情報システムを所管するセキュリティ管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて損傷が発生した場合には、速やかにデジタル推進課に報告しなければならない。

⑶　統括管理者及び情報システムを所管するセキュリティ管理者は、ネットワーク接続口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。

⑷　統括管理者及び情報システムを所管するセキュリティ管理者は、デジタル推進課及び契約により操作を認められた外部委託事業者等以外の者に配線を変更させたり、追加させたりしてはならない。

5　機器の定期保守及び修理

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、サーバ等の機器の定期保守を実施しなければならない。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、電磁的記録媒体等を内蔵する機器を外部委託事業者等に修理させる場合、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、統括管理者又は情報システムを所管するセキュリティ管理者は、外部委託事業者等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、秘密保持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。

6　庁外への機器の設置

ハウジングサービスの利用等により庁外にサーバ等の機器を設置する場合、本章の規程と同等以上のセキュリティ対策を満たすことを確認し、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の実施状況について確認しなければならない。

7　機器の廃棄等

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器に内蔵する電磁的記録媒体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。また、外部委託事業者等に委託する場合には、秘密保持契約を締結するほか、情報の消去等に関する証明書を提出させなければならない。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、クラウドサービス事業者が利用する機器等の廃棄の手順について、セキュリティが確保されているか確認しなければならない。なお、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を確認すること。

4.3電算室の管理

1　電算室の構造等

⑴　電算室とは、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をいう。

⑵　統括管理者は、電算室を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。

⑶　統括管理者は、施設管理部門と連携して、電算室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。

⑷　統括管理者は、電算室内の機器等に、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。

⑸　統括管理者は、電算室を囲む外壁等の床下開口部を全て塞がなければならない。
⑹　統括管理者は、電算室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　電算室の入退室管理等
⑴　統括管理者は、施設管理部門と連携し、電算室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。
⑵　職員及び外部委託事業者等は、電算室に入室する場合、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。
⑶　統括管理者は、外部委託事業者等が電算室に入る場合には、電算室への入退室を許可された職員が監督し、外見上職員と区別できる措置を講じなければならない。
⑷　職員は、当該情報システムに関連しないパソコン、モバイル端末、通信回線装置、電磁的記録媒体等を電算室に持ち込む場合には、統括管理者に許可を得なければならない。
３　機器等の搬入出
⑴　職員は、電算室に搬入する機器等が、既存の情報システムに与える影響について、あらかじめ外部委託事業者等に確認を行わせなければならない。
⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、外部委託事業者等による電算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。

４．４ 通信回線等の管理
１　通信回線及び通信回線装置の管理
⑴　統括管理者は、庁内ネットワークの通信回線及び通信回線装置を適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。
⑵　統括管理者は、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。
⑶　統括管理者及びセキュリティ管理者は、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。
⑷　統括管理者及びセキュリティ管理者は、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十分なセキュリティ対策を実施しなければならない。
⑸　統括管理者及びセキュリティ管理者は、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。

４．５ パソコン等の管理
１　職員等の利用するパソコン等や電磁的記録媒体等の管理
⑴　セキュリティ管理者は、マイナンバー利用事務系に属するパソコン等及び特定個人情報に該当する情報資産を取り扱うパソコン等は、ワイヤーによる固定等の盗難防止措置を講じなければならない。

⑵　統括管理者又は情報システムを所管するセキュリティ管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等の認証情報の入力を必要とするように設定しなければならない。なお、取り扱う情報の重要度に応じて多要素認証の利用を検討しなければならない。
⑶　統括管理者又は情報システムを所管するセキュリティ管理者は、パソコン等の電源起動時のパスワード等(BIOSパスワード、ハードディスクパスワード等)を設定しなければならない。
⑷　統括管理者又は情報システムを所管するセキュリティ管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。パソコン等にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。
⑸　セキュリティ管理者は、電磁的記録媒体等についてもデータ暗号化機能を備える媒体を使用するよう努めなければならない。
⑹　セキュリティ管理者は、電磁的記録媒体等を台帳にて管理しなければならない。

第５章 人的セキュリティ

５．１ 職員の遵守事項

１　情報セキュリティポリシー等の遵守

⑴ 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。

⑵ セキュリティ管理者は、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、速やかに統括管理者に相談し、指示を仰がなければならない。

２　業務以外の目的での使用の禁止

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　IDの取扱い

⑴ 職員は、自己の管理するIDを、他人に利用させてはならない。

⑵ 職員は、共用IDを利用する場合は、必要最小限の範囲で利用しなければならない。

４　ICカード等の取扱い

⑴ 統括管理者及びICカード等を利用する課のセキュリティ管理者は、ICカード毎に利用者を明確にしなければならない。

⑵ 統括管理者及びICカード等を利用する課のセキュリティ管理者は、紛失・盗難などに備えてICカード等を管理しなければならない。

⑶ 職員は、ICカード等を使用する場合には、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、利用者間で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若しく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、情報セキュリティインシデント発生時の対応手順に沿って報告・対応しなければならない。

⑷ 統括管理者及びICカードを利用する課のセキュリティ管理者は、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。

⑸ 統括管理者及びICカードを利用する課のセキュリティ管理者は、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。

５　情報システム機器の持ち出し及び庁外における情報処理作業の制限

⑴ 統括責任者は、情報システム機器の持ち出し及び庁外における情報処理作業に関する安全管理措置を定めなければならない。

⑵ 職員は、原則として配備されたパソコン等を庁外に持ち出してはならない。ただし、業務上必要な場合には、統括管理者の許可を得て持ち出すことができる。

⑶ 職員は、原則として独自に導入したパソコン等を庁外に持ち出す場合には、セキュリティ管理者の許可を得なければならない。

⑷　セキュリティ管理者は、配備されたパソコン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。
⑸　職員は、情報システム機器を持ち出す場合及び庁外で情報処理作業を行う場合には、統括責任者の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。

6　パスワードの取扱い
⑴　職員は、自己の管理するパスワードに関し、他者に知られないように管理しなければならな い。
⑵　職員は、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。
⑶　職員は、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。
⑷　職員は、パスワードが流出したおそれがある場合には、第７章に規定する緊急時対応計画に従い、セキュリティ管理者に速やかに報告しなければならない。
⑸　職員は、パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
⑹　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。
⑺　職員は、新規のパスワードを最初のログイン時点で変更しなければならない。
⑻　職員は、共有IDを除き、職員間でパスワードを共有してはならない。また、共有IDに紐付くパスワードは人事異動等が発生した場合には、速やかにパスワードを変更しなければならない。

7　個人所有の機器の取り扱い
⑴　職員は、原則として個人所有機器(パソコン、スマートフォン、タブレット等)を業務に利用してはならない。ただし、業務上必要な場合には、統括責任者の定める実施手順に従い利用すること。
⑵　職員は、個人所有機器(パソコン、スマートフォン、タブレット等)を庁内ネットワークに接続してはならない。

8 情報システム機器の取扱い
⑴　職員は、配備されたパソコン等を業務以外の目的で利用してはならない。
⑵　職員は、情報システムへ業務以外の目的でアクセスしてはならない。
⑶　職員は、離席時はパソコン等の画面ロックを実施しなければならない。
⑷　職員は、ソフトウェアに関するセキュリティ機能の設定を変更してはならない。
⑸　職員は、機器の改造及び増設・交換を行う必要がある場合には、統括管理者及び情報システムを所管するセキュリティ管理者の許可を得なければならない。
⑹　職員は、プリンタの設定、ネットワーク機器の設定を変更してはならない。

9　退職時等の遵守事項 職員は、異動、退職等により業務を離れる場合には、利用している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。

10　電子メールの利用

⑴　職員は、業務上付与された電子メールアドレスを業務以外の目的に使用してはならない。

⑵　職員は、外部の複数人に対して電子メールを送信する場合には、個人情報の流出を防ぐために原則として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。

⑶　職員は、電子メールアドレス及びオンラインストレージサービスについては、デジタル推進課が管理するサービスを利用するものとし、それ以外の同種サービスを原則として利用してはな らない。

⑷　職員は、電子メールを個人所有のメールアドレス等に転送してはならない。

⑸　職員は、重要な電子メールを誤送信した場合、セキュリティ管理者に報告しなければならな い。

11　インターネットの利用

⑴　職員は、業務においてソーシャルメディアサービス等を利用する場合は、セキュリティ管理者の許可を得なければならない。

⑵　職員は、インターネット上に掲載されている写真、イラスト、文章、ソフトウェア、プログラムを 利用する場合は知的財産権等に十分留意しなければならない。

⑶　職員は、私用で利用しているソーシャルメディアサービス等において、業務上知り得た情報　及び自己又は他人の社会的評価を低下させ、本市の信用を失墜させる可能性のある情報は書き込んではならない。

12　無許可ソフトウェアのダウンロード及びインストール等の禁止

⑴　職員は、配備されたパソコン等に無断でソフトウェアを導入してはならない

⑵　職員は、業務上必要がある場合は、統括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。なお、セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

⑶　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。

13　日常のセキュリティ対策

⑴　職員は、離席時は文書の内容が容易に閲覧されないようにしなければならない。

⑵　職員は、プリンタ、複写機、FAX機等から出力された文書・帳票は速やかに回収しなければならない。

14　不正プログラム対策

⑴　職員は、外部からデータを取り込む場合又はソフトウェアを導入する場合には、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。

⑵　職員は、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には、速やかにデジタル推進課に報告し、指示に従わなければならない。

⑶　職員は、配備されたパソコン等に対して、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。

⑷ 職員は、添付ファイルが付いた電子メールを送受信する場合には、メールソフトウェア内のウィルス対策機能又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。また、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。

⑸ 職員は、統括管理者が提供するウイルス情報を確認しなければならない。

⑹ 職員は、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、第７章に規定する緊急時対応計画に従い、セキュリティ管理者に速やかに報告しなければならない。

15　情報セキュリティポリシー等の掲示

統括管理者は、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。

16　外部委託事業者等に対する説明

統括管理者及び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導入・保守等を外部委託事業者等に発注する場合、外部委託事業者等から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者等が遵守するべき内容を説明しなければならない。

17　職員の報告義務　職員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括管理者及びセキュリティ管理者に報告を行わなければならない。

５.２ 研修・訓練

１　情報セキュリティに関する研修・訓練

⑴ 統括責任者は、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。

⑵ 統括責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

２　研修計画の策定及び実施

⑴ 統括責任者は、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とその実施体制の構築を定期的に行い、CISOの承認を得なければならない。

⑵ 統括責任者は、研修計画において、職員が毎年度最低１回は情報セキュリティ研修を受講する機会を与えなければならない。

⑶ 統括責任者は、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。

⑷ 統括責任者は、研修の内容をセキュリティ責任者、セキュリティ管理者及びその他職員等に対して、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。

⑸ 統括管理者は、研修の実施状況を記録し、統括責任者に対して報告しなければならない。

⑹　統括責任者は、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。
⑺　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。

3　緊急時対応訓練

統括責任者は、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。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、また、効果的に実施できるようにしなければならない。

5.3 情報セキュリティインシデントの報告

1　庁内からの情報セキュリティインシデントの報告

⑴　職員は、情報セキュリティインシデントを認知した場合、速やかにセキュリティ管理者及びデジタル推進課に報告しなければならない。
⑵　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、速やかに統括管理者、セキュリティ責任者及び情報システムを所管するセキュリティ管理者に報告しなければならない。
⑶　統括管理者は、報告のあった情報セキュリティインシデントについて、統括責任者に報告しなければならない。
⑷　統括責任者は、報告のあった情報セキュリティインシデントについて、必要に応じてCISO及びDISOに報告しなければならない。
⑸　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。
⑹　セキュリティ責任者は、クラウドサービスで発生した情報セキュリティインシデントについて、クラウドサービス事業者を含む関係者に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

⑴　職員は、本市が管理する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、速やかにセキュリティ管理者に報告しなければならない。
⑵　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、速やかにセキュリティ責任者、統括管理者及び情報システムを所管するセキュリティ管理者に報告しなければならない。
⑶　統括管理者は、報告のあった情報セキュリティインシデントについて、統括責任者に報告しなければならない。
⑷　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、必要に応じて CISO及びDISOに報告しなければならない。
⑸　統括管理者及びセキュリティ管理者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や原因の究明・記録、再発防止に係る実施体制を契約等で取り決めなければならない。
⑹　CISOは、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るための窓口を設置し、当該窓口への連絡手段を公表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

⑴　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。

⑵　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及びDISOに速やかに報告しなければならない。

⑶　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セキュリティ管理者へ確認 を指示しなければならない。

⑷　CSIRTは、情報セキュリティインシデントを引き起こした部門のセキュリティ管理者と連携し、これらの情報セキュリティインシデント原因を究明し、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結果から、再発防止策を検討し、CISO及びDISOに報告しなければならない。

⑸　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６章 技術的セキュリティ

６．１技術的セキュリティ対策の実施

１　技術的セキュリティ対策の適用

⑴　統括責任者及び統括管理者並びにシステム区分１の情報システムを所管するセキュリティ責任者及びセキュリティ管理者は、システム区分１に分類される情報システムの技術的セキュリティ対策について、本章に規定する対策を全て適用しなければならない。

⑵　統括責任者及び統括管理者並びにシステム区分２の情報システムを所管するセキュリティ責任者及びセキュリティ管理者は、システム区分２に分類される情報システムの物理的セキュリティ対策について、本章に規定する対策に準ずるよう努めなければならない。ただし、情報セキュリティ対策専門部会がシステム区分２であっても重要情報以上の情報を取り扱うシステムと判断した場合は、本章に規定する対策を全て適用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　ファイルサーバの設定等

⑴　統括管理者は、職員が使用できるオンラインストレージサービス及びファイルサーバの容量を設定し、セキュリティ管理者は職員に定期的にオンラインストレージサービス及びファイル サーバの情報整理を行わせなければならない。

⑵　統括管理者は、オンラインストレージサービス及びファイルサーバを課等の単位で構成し、職員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、アクセス権限を設 定しなければならない。

⑶　統括管理者は、セキュリティ管理者が特定の職員しか取り扱えないと判断するデータについて、同一の課等であっても別途アクセス権限を設定する等の措置を講じることができる。

２　バックアップの実施

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、オンラインストレージサービス及び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。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、その仕様が本市の求める要求事項を満たすことを確認しなければならない。

⑶　統括管理者及び情報システムを所管するセキュリティ管理者は、クラウドサービス事業者のバックアップ機能が要求事項を満たさない場合やバックアップ機能を利用しない場合は、自らの責任の下、情報資産のバックアップを行わなければならない。

３　システム管理記録及び作業の確認

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、所管する情報システムの運用において実施した定期的なメンテナンスや修繕等の作業について、作業記録を作成しなければならない。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、所管する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、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。

⑶　統括管理者、セキュリティ管理者又は契約により操作を認められた外部委託事業者等がシステム変更等の作業を行う場合は、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

統括管理者及び情報システムを所管するセキュリティ管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧したり、紛失したりすること等がないよう、適正に管理しなければならない。

5　ログの取得等

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、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。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、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、適正にログを管理しなければならない。

⑶　統括管理者及び情報システムを所管するセキュリティ管理者は、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。

⑷　統括管理者及び情報システムを所管するセキュリティ管理者は、クラウドサービス事業者が収集し、保存するログの管理及び保護等の対策が適正に実施されているか確認しなければならない。

⑸　統括管理者及び情報システムを所管するセキュリティ管理者は、クラウドサービス事業者から提供されるログ等の情報について、監査及びデジタルフォレンジックに係る本市の要求事項を満たさない場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

6　障害記録

統括管理者及び情報システムを所管するセキュリティ管理者は、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。

7　ネットワークの接続制御、経路制御

⑴　統括管理者は、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。

⑵　統括管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

⑶　統括管理者は、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。

8　外部の者が利用できるシステムの分離

情報システムを所管するセキュリティ管理者は、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又は論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

⑴　情報システムを所管するセキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、統括管理者の許可を得なければならない。

⑵　情報システムを所管するセキュリティ管理者は、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、デジタル推進課に報告しなければ ならない。

⑶　情報システムを所管するセキュリティ管理者は、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。

⑷　情報システムを所管するセキュリティ管理者は、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。

10　複合機のセキュリティ管理

⑴　統括管理者は、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、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。

⑵　統括管理者は、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。

11　IoT機器を含む特定用途機器のセキュリティ管理

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、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講じなければならない。

⑵　情報システムを所管するセキュリティ管理者は、特定用途機器を庁内ネットワークに接続する場合には、統括管理者の許可を得なければならない。

12　無線LAN及びネットワークの盗聴対策

統括管理者は、無線LANのネットワークを整備する場合、情報の盗聴等を防ぐため、解読が困難な暗号化及び認証技術の使用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

⑴　統括管理者は、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。

⑵　統括管理者は、大量のスパムメール等の受信、又は内部からスパムメール等が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。

⑶　統括管理者は、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。

⑷　統括管理者は、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。

⑸　統括管理者は、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。

⑹　統括管理者は、職員が電子メールの送信等による情報資産の無断での外部持ち出しを抑止するため、添付ファイルの監視等によるシステム上の対策措置を行わなければならない。

14　電子署名・暗号化

⑴　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、統括責任者が定めた電子署名、パスワード等による暗号化等の方法を用いて送信しなければならない。

⑵　職員は、暗号化を行う場合に統括責任者が定める以外の方法を用いてはならない。また、統括責任者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。

⑶　統括責任者は、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。

15　業務外ネットワークへの接続の禁止

⑴　職員は、配備されたパソコン等を、有線・無線を問わず、そのパソコン等を接続して利用するよう統括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。

⑵　統括管理者は、配備したパソコン等について、パソコン等に搭載されたOSのポリシー設定等により、パソコン等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しなければならない。

16　業務以外の目的でのウェブ閲覧の禁止

⑴　職員は、業務以外の目的でウェブ閲覧をしてはならない。

⑵　統括管理者は、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、セキュリティ管理者に通知し適正な措置を求めなければならない。

17　Web会議サービスの利用時の対策

⑴ 統括管理者は、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。

⑵ 職員は、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しなければならない。
⑶ 職員は、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じなければならない。
⑷ 職員は、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わなければならない。

6.3 アクセス制御

1 アクセス制御等

統括管理者又は情報システムを所管するセキュリティ管理者は、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しなければならない。

2 利用者IDの取扱い

⑴ 統括管理者又は情報システムを所管するセキュリティ管理者は、利用者の登録、変更、抹消等の情報を管理し、職員等の異動、出向、退職に伴う利用者IDの取扱い等の方法を定めなければならない。
⑵ 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、統括管理者又は情報システムを所管するセキュリティ管理者に通知しなければならない。
⑶ 統括管理者又は情報システムを所管するセキュリティ管理者は、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。
⑷ 統括管理者及び情報システムを所管するセキュリティ管理者は、職員に必要以上の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

⑴ 統括管理者又は情報システムを所管するセキュリティ管理者は、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。
⑵ 統括管理者及び情報システムを所管するセキュリティ管理者は、管理者権限の特権を付与されたID及びパスワードが、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。
⑶ 統括管理者及び情報システムを所管するセキュリティ管理者の特権を代行する者は、統括管理者及び情報システムを所管するセキュリティ管理者が指名した者でなければならない。
⑷ 統括管理者及び情報システムを所管するセキュリティ管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者等に行わせてはならない。
⑸ 統括管理者及び情報システムを所管するセキュリティ管理者は、特権を付与されたID及びパスワードについて、定期変更、入力回数制限等により高いセキュリティ水準を維持しなけれ ばならない。
⑹ 統括管理者及び情報システムを所管するセキュリティ管理者は、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。

4　職員による外部からのアクセス等の制限

⑴　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、統括管理者及び当該情報システムを所管するセキュリティ管理者の許可を得なければならない。

⑵　統括管理者は、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認める場合は、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。

⑶　統括管理者は、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。

⑷　統括管理者は、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。

⑸　公衆通信回線(公衆無線LAN等)から内部のネットワーク又は情報システムに接続することは原則として禁止とする。

5 自動識別の設定

統括管理者及び情報システムを所管するセキュリティ管理者は、ネットワークで使用される機器について、機器固有情報等によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

6　ログイン時の表示等

情報システムを所管するセキュリティ管理者は、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できるよう設定しなければならない。

7　パスワードに関する情報の管理

⑴　統括管理者又は情報システムを所管するセキュリティ管理者は、職員のパスワードに関する情報を厳重に管理しなければならない。パスワードを不正利用から保護するため、OS等でパ スワード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。

⑵　統括管理者又は情報システムを所管するセキュリティ管理者は、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、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。

⑶　統括管理者又は情報システムを所管するセキュリティ管理者は、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。

8　特権による接続時間の制限 情報システムを所管するセキュリティ管理者は、特権を付与されたID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。

６．４システム導入、保守等

１ 情報システムの調達

⑴ セキュリティ管理者は、個別にシステムを導入する場合、本章に規定するセキュリティ対策を検討し、デジタル推進課と事前に協議しなければならない。

⑵ 統括管理者及びセキュリティ管理者は、情報システムの導入、保守等の調達に当たっては、必要とする技術的なセキュリティ機能を調達仕様書に明記しなければならない。

⑶ 統括管理者及びセキュリティ管理者は、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、本市の求める要求事項を満たすことを確認しなければならない。

２ システム導入における責任者、作業者のIDの管理

⑴ 情報システムを所管するセキュリティ管理者は、システム導入の責任者及び作業者を特定しなければならない。また、システム導入のための規則を確立しなければならない。

⑵ 情報システムを所管するセキュリティ管理者は、システム導入の責任者及び作業者のIDを 管理し、導入完了後、導入時に使用したIDを削除しなければならない。

⑶ 情報システムを所管するセキュリティ管理者は、システム導入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。

３ システム導入に用いるハードウェア及びソフトウェアの管理

⑴ 情報システムを所管するセキュリティ管理者は、システム導入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なければならない。

⑵ 情報システムを所管するセキュリティ管理者は、利用を認めていない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 テスト環境と運用環境の分離及び移行手順の明確化

⑴ 情報システムを所管するセキュリティ管理者は、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。

⑵ 情報システムを所管するセキュリティ管理者は、テスト環境からシステム運用環境への移行について、あらかじめ手順を明確にしなければならない。

⑶ 情報システムを所管するセキュリティ管理者は、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。

⑷ 情報システムを所管するセキュリティ管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

５ 新たな情報システム導入時における稼働テストの実施

⑴ 情報システムを所管するセキュリティ管理者は、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。

⑵ 情報システムを所管するセキュリティ管理者は、運用テストを行う場合、あらかじめテスト環境 による操作確認を行わなければならない。

⑶ 情報システムを所管するセキュリティ管理者は、重要情報以上の情報資産をテストデータに使用してはならない。

⑷　情報システムを所管するセキュリティ管理者は、導入するシステムの受入テストを行う場合、導入する組織と受け入れる組織がそれぞれ独立したテストを行うよう指示をしなければならない。

6　システム導入・保守に関連する資料等の整備・保管

⑴　情報システムを所管するセキュリティ管理者は、システム導入・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。

⑵　情報システムを所管するセキュリティ管理者は、テスト結果を一定期間保管しなければならない。

⑶　情報システムを所管するセキュリティ管理者は、情報システムに係るソースコードを適切な方 法で保管しなければならない。

7　情報システムにおける入出力データの正確性の確保

⑴　情報システムを所管するセキュリティ管理者は、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情報システムを設計しなければならない。

⑵　情報システムを所管するセキュリティ管理者は、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。

①　アプリケーション及びウェブコンテンツが情報セキュリティ水準の低下を招かぬようあらかじめ確認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。

⑶　情報システムを所管するセキュリティ管理者は、故意又は過失による情報の改ざん又は漏えいのおそれがある場合に、これを検出できるよう情報システムを設計しなければならない。

⑷　情報システムを所管するセキュリティ管理者は、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、出力されるよう情報システムを設計しなければならない。

8　情報システムの変更管理　情報システムを所管するセキュリティ管理者は、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。

9　導入・保守用のソフトウェアの更新等　情報システムを所管するセキュリティ管理者は、導入・保守用のソフトウェア等の更新又はパッチ適用をする場合、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。

10　システム更新又は統合時の体制等　情報システムを所管するセキュリティ管理者は、システム更新・統合時の移行基準の明確化及びリスク管理体制の構築並びに更新・統合後の業務運営体制の構築をしなければならない。

６．５ 不正プログラム対策

１　統括管理者の措置事項 統括管理者は、コンピュータウイルス等の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。

⑴　外部から受信したファイルについて、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、コンピュータウイルス等の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。

⑵　外部に送信するファイルについて、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、コンピュータウイルス等の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。

⑶　コンピュータウイルス等の不正プログラムの情報を収集し、必要に応じ職員に対して注意喚起しなければならない。

⑷　所管するサーバ及びパソコン等は、不正プログラム対策ソフトウェアが常駐又は同等以上の機能が搭載されたものとしなければならない。

⑸　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。

⑹　不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。

⑺　業務で利用するソフトウェアは、パッチやバージョンアップ等により開発元のサポートが終了したもの又は業務期間中に終了する予定のものを利用してはならない。

⑻　サーバ等を構築する際に不正プログラムへの対策(必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施)を確実に実施しなければならない。SaaS型を利用する場合は、これらの対策がクラウドサービス事業者側でされているか確認しなければならない。

２　情報システムを所管するセキュリティ管理者の措置事項

情報システムを所管するセキュリティ管理者は、コンピュータウイルス等の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。

⑴　所管するサーバ及びパソコン等は、不正プログラム対策ソフトウェアが常駐又は同等以上の機能が搭載されたものとしなければならない。

⑵　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。

⑶　不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。

⑷　不正プログラム対策ソフトウェア等の設定変更権限を統一的に管理し、情報システムを所管するセキュリティ管理者が許可した職員を除く職員等に当該権限を付与してはならない。

⑸　所管するソフトウェアについて、パッチやバージョンアップ等により開発元のサポートが終了したもの又は業務期間中に終了する予定のものを利用してはならない。

３　専門家の支援体制

統括責任者は、外部の専門家との連絡体制を構築し、不正プログラム感染時等に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　統括管理者及び情報システムを所管するセキュリティ管理者の措置事項

統括管理者及び情報システムを所管するセキュリティ管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

⑴　使用されていないポートを閉鎖しなければならない。

⑵　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。

⑶　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 括管理者又は情報システムを所管するセキュリティ管理者へ通報するよう、設定しなければな らない。

⑷　クラウドサービスの利用について、情報セキュリティポリシーにおけるアクセス制御に関する事項を満たすことを確認しなければならない。

⑸　クラウドサービスの利用について、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させなければならない。

⑹　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が情報セキュリティポリシーを満たすことを確認しなければならない。

2 攻撃への対処

CISO、DISO及び統括責任者は、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、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、DISO及び統括責任者は、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　内部からの攻撃

統括管理者及び情報システムを所管するセキュリティ管理者は、職員及び外部委託事業者等が使用しているパソコン等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　職員による不正アクセス

統括管理者及び情報システムを所管するセキュリティ管理者は、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セキュリティ管理者に通知し、適切な処置を求めなければならない。

6　サービス不能攻撃

統括管理者及び情報システムを所管するセキュリティ管理者は、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。

7　標的型攻撃

統括管理者及び情報システムを所管するセキュリティ管理者は、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入口対策、内部に侵入した攻撃の早期検知や侵入範囲の拡大抑止等の内部対策及び外部との不正通信検知等の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

⑴　統括管理者及び情報システムを所管するセキュリティ管理者は、サーバ、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に対する対応の緊急性に応じて、ソフトウェア更新等の対策を実施しなければならない。

⑵　統括管理者及び情報システムを所管するセキュリティ管理者は、利用するクラウドサービスにおける技術的な脆弱性について、本市の情報資産への影響範囲を特定し、リスク評価、対応の優先順位付け等の管理手順について事業者に確認しなければならない。

2　情報セキュリティに関する情報の収集及び共有

統括管理者及びセキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、職員及び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、セキュリティインシデントの発生を未 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７章 運用

７．１ 情報システムの監視

１　情報システムの監視

⑴　情報システムの運用・保守時の対策

①　統括管理者及び情報システムを所管するセキュリティ管理者は、情報システムの運用・保守において、当該情報システムのセキュリティ機能を適切に運用しなければならない。

②　統括管理者及び情報システムを所管するセキュリティ管理者は、新たな脅威の出現、運用、監視等の状況により情報システムの情報セキュリティ対策を定期的に見直し、必要な措 置を講じなければならない。

③　統括管理者及び情報システムを所管するセキュリティ管理者は、重要情報以上の情報資産を取り扱う情報システムについて、障害発生時のアラート発報等の対策を講じなければ ならない。

⑵　情報システムの監視機能

①　統括管理者及び情報システムを所管するセキュリティ管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

②　統括管理者及び情報システムを所管するセキュリティ管理者は、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　統括管理者及び情報システムを所管するセキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

⑶　統括管理者及び情報システムを所管するセキュリティ管理者は、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。また、利用するクラウドサービスにおける時刻の同期についても適切になされているのか確認しなければならない。

⑷　統括管理者及び情報システムを所管するセキュリティ管理者は、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。

⑸　統括管理者及び情報システムを所管するセキュリティ管理者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

⑹　統括管理者及び情報システムを所管するセキュリティ管理者は、必要となるリソースの容量・ 能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウド サービスにおいて、リソースやアプリの使用状況及び設定値などを監視し、業務が維持できる ように努めなければならない。

⑺　統括管理者及び情報システムを所管するセキュリティ管理者は、イベントログ取得に関する ポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認しなければならない。

⑻　統括管理者及び情報システムを所管するセキュリティ管理者は、次の重要な操作に関して、重大なインシデントにつながるおそれがあるため、誤操作等がないよう手順化しなければならない。

①　サーバ、ネットワーク、ストレージなどの仮想化されたデバイスに対するインストール、変更 及び削除

②　クラウドサービス利用の終了手順

③　バックアップ及び復旧

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

⑴　セキュリティ責任者及びセキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括責任者及び統括管理者に報告しなければならない。

⑵　統括責任者は、発生した問題について、必要に応じてCISO及びDISOに報告しなければならない。

⑶　統括責任者又はCISO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。

⑷　統括管理者及び情報システムを所管するセキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

2　パソコン等の利用状況調査

CISO及び統括責任者は、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　違反行為への対処

統括責任者は、情報セキュリティポリシーに対する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判断した場合、第７章に規定する緊急時対応計画に従って適切に対処しなければならない。

7.3 情報セキュリティインシデント発生時の対応等

1　緊急時対応計画の策定

⑴　CISOは、情報セキュリティポリシーの違反等により情報資産に対するセキュリティインシデントが発生した場合における連絡、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、緊急時対応計画を策定し、セキュリティインシデント発生時には 当該計画に従って適切に対処しなければならない。

⑵　CISOは、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にした緊急時対応計画を定めておき、セキュリティインシデント発生時には当該 計画に従って適正に対処しなければならない。

2　緊急時対応計画に盛り込むべき内容

CISOは、緊急時対応計画において、以下の内容を定めなければならない。

⑴　関係者の連絡先
⑵　発生した事案に係る報告すべき事項
⑶　発生した事案への対応措置
⑷　再発防止措置の策定

3　業務継続計画との整合性の確保

CISOは、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、情報セキュリティ対策専門部会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

CISOは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて 緊急時対応計画の規定を見直さなければならない。

7.4　例外措置

1　例外措置の許可

セキュリティ管理者は、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。

2　緊急時の例外措置

セキュリティ管理者は、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　例外措置の状況確認

CISOは、例外措置の内容等に係る資料を適切に保管し、定期的に措置状況を確認しなければならない。

7.5 法令遵守

1　法令等の遵守

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、次の法令等のほか関係法令等を遵守し、これに従わなければならない。

⑴　地方公務員法(昭和25年法律第261号)
⑵　著作権法(昭和45年法律第48号)
⑶　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)
⑷　個人情報の保護に関する法律(平成15年法律第57号)

⑸　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)
⑹　サイバーセキュリティ基本法(平成28年法律第31号)
⑺　那須塩原市個人情報の保護に関する法律施行条例(令和4年12月16日条例第37号)
⑻　利用するソフトウェアのライセンス規約

７．６　違反時の対応

１　違反時の対応

職員の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

⑴　統括管理者が違反を確認した場合は、統括管理者は当該職員が所属する課等の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。
⑵　情報システムを所管するセキュリティ管理者が違反を確認した場合は、速やかに統括管理者及び当該職員が所属する課等の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。
⑶　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、統括責任者は、当該職員の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、統括責任者は、職員の権利を停止あるいは剥奪した旨をCISO及び当該職員が所属するセキュリティ管理者に通知しなければならない。

２　懲戒処分

情報セキュリティポリシーに違反した職員等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。

第８章 業務委託と外部サービス(クラウドサービス)の利用

８．１　外部委託

１　外部委託事業者等の選定基準

⑴　セキュリティ責任者は、外部委託事業者等の選定にあたり、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。

⑵　セキュリティ責任者は、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、事業者を選定しなければならない。

２　契約項目

セキュリティ管理者は、情報システムの運用、保守等を外部委託する場合には、外部委託事業者等との間で取り交わす契約書において、必要に応じて次の情報セキュリティ要件を明記しなければならない。

⑴　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
⑵　外部委託事業者等の責任者、委託内容、作業者、作業場所の特定
⑶　提供されるサービスレベルの保証
⑷　外部委託事業者等にアクセスを許可する情報の種類と範囲、アクセス方法
⑸　外部委託事業者等の従業員に対する教育の実施
⑹　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
⑺　業務上知り得た情報の守秘義務
⑻　再委託に関する制限事項の遵守
⑼　委託業務終了時の情報資産の返還、廃棄等
⑽　委託業務の定期報告及び緊急時報告義務
⑾　市による監査、検査
⑿　再委託先に対する市による監査、検査
⒀　市による情報セキュリティインシデント発生時の公表
⒁　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　確認・措置等

⑴　セキュリティ管理者は、外部委託事業者等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なければならない。

⑵　セキュリティ対策が確保されていないと認められる場合は、契約に基づき是正を要求し、その内容をセキュリティ責任者、統括管理者及び統括責任者に報告するとともに、その重要度 に応じてDISO及びCISOに報告しなければならない。

４　情報システムに関する業務委託

⑴　情報システムに関する業務委託における共通的対策

情報システムを所管するセキュリティ管理者は、情報システムに関する業務委託の際には、契約書等に本市の意図しない変更が加えられないよう必要な措置を講じなければならない。

⑵　情報システムの構築を業務委託する場合の対策

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

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

⑶　情報システムの運用・保守を業務委託する場合の対策

①　情報システムを所管するセキュリティ管理者は、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、契約書等に基づき、委託事業者に実施を求めなければならない。

②　情報システムを所管するセキュリティ管理者は、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、契約書等に基づき、委託事業者に速やかな報告を求めなければならない。

⑷　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　情報システムを所管するセキュリティ管理者は、外部事業者が情報システムの一部の機能を提供するサービス(ホスティングサービス又はインターネット回線接続サービスを含む。また、クラウドサービスを除く。)(以下「業務委託サービス」という。)を利用し、重要情報以 上の情報資産を取り扱う業務委託を実施する場合は、業務委託サービス特有の選定条件 を加えなければならない。

②　情報システムを所管するセキュリティ管理者は、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　情報システムを所管するセキュリティ管理者は、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。

8.2 クラウドサービスの利用

1　クラウドサービスの定義

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理 的又は仮想的なリソースにネットワーク経由でアクセスし、利用者によって自由にリソースの設 定・管理が可能な次のサービスをいう。

⑴　SaaS(Software as a Service)クラウド上のソフトウェア／アプリケーションを利用するサービ スであり、利用者にはクラウドサービスプロバイダの基盤上で稼動しているアプリケーション サービスプロバイダ由来のアプリケーションが提供されるもの

⑵　PaaS(Platform as a Service)クラウド上のOSやミドルウェアなどのプラットフォームを利用す るサービスであり、利用者にはOS、ミドルウェア、演算機能、ストレージ、ネットワークその他の 基礎的コンピューティングリソースが提供されるもの

⑶　IaaS(Infrastructure as a Service)クラウド上のネットワーク、CPU、メモリ、ストレージなどの コンピューティングリソースを提供する基盤を利用するサービスであり、利用者には演算機 能、ストレージ、ネットワークその他の基礎的コンピューティングリソースの基盤が提供されるも の

2　クラウドサービスの選定に関する運用規程の整備

統括責任者は、重要情報以上の情報資産を取り扱う場合、次の事項を含むクラウドサービスの選定に関する規程を整備しなければならない。

⑴　クラウドサービスを利用可能な業務、機器、接続方法及び庁外での利用可否等に係る判断基準(以下「クラウドサービス利用判断基準」という。)

⑵　クラウドサービス提供者の選定基準

⑶　クラウドサービスの利用申請の許可権限者と利用手続

⑷　クラウドサービスの利用状況の管理

3　クラウドサービスの利用に関する運用規程の整備

統括責任者は、重要情報以上の情報資産を取り扱う場合、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、次の事項を含むクラウドサービスの利用に関する規程を整備しなければならない。

⑴　クラウドサービスを利用した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

⑵　クラウドサービスを利用した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

⑶　クラウドサービスの利用終了に係る次の事項を含むセキュリティ対策の基本方針

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

8.3 ソーシャルメディアサービスの利用

1　ソーシャルメディアサービスの利用

⑴　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、次の事項を遵守しなければならない。

①　市が管理するウェブサイトにアカウント情報を掲載して参照可能とする等の方法でなりすまし対策を行うこと。

②　認証情報を適切に管理し、不正アクセス対策を行うこと。

③　重要情報以上の情報を発信しないこと。

④　なりすまし又は不正アクセス等を確認した場合には、被害の最小化措置を講じること。

⑵　統括責任者は、利用するソーシャルメディアサービスごとに管理責任者を定めなければならない。

第９章 評価・見直し

９．１ 監査

１　実施方法

CISOは、監査責任者を指名し、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の実施状況について、毎年度及び必要に応じて監査を行わせなければならない。

２　監査を行う者の要件

⑴　監査責任者は、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。

⑵　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

３　監査実施計画の立案及び実施への協力

⑴　監査責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティタスクフォースの承認を得なければならない。

⑵　被監査部門は、監査の実施に協力しなければならない。

４　外部委託事業者等に対する監査

⑴　監査責任者は、外部委託事業者等(下請け事業者も含む。)に対し、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。

⑵　監査責任者は、クラウドサービス事業者が実施する情報セキュリティに関する対策状況について、定期的に監査を行わなければならない。なお、クラウドサービス事業者を直接監査することが困難な場合は、クラウドサービス事業者が実施する第三者による監査証明書や監査報 告書等の確認をもって監査に代えることができる。

５　報告

監査責任者は、監査結果を取りまとめ、情報セキュリティタスクフォースに報告する。

６　保管

監査責任者は、監査により収集した監査証拠や監査調書を適切に保管しなければならない。

７　監査結果への対応

⑴　CISOは、監査結果を踏まえ、指摘事項を所掌するセキュリティ管理者に対し、当該事項への対処(改善計画の策定等)を指示しなければならない。また、措置が完了していないものについては、定期的に進捗状況の報告を指示しなければならない。

⑵　CISOは、庁内で横断的に改善が必要な指摘事項については、関係する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、措置が完了していないものについては、定期的に進捗状況の報告を指示しなければならない。

8　情報セキュリティポリシー及び関係規程等の見直し等への活用 情報セキュリティタスクフォースは、監査結果を情報セキュリティポリシー、関係規程等の見直し時に活用しなければならない。

9.2 自己点検

1　実施方法

⑴ 統括管理者及び情報システムを所管するセキュリティ管理者は、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。

⑵ セキュリティ責任者は、セキュリティ管理者と連携して、所掌する部局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の実施状況について、毎年度及び必要に応じて 自己点検を行わなければならない。

2　報告

統括責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティタスクフォースに報告しなければならない。

3　自己点検結果の活用

⑴ 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。

⑵ 情報セキュリティタスクフォースは、自己点検結果を情報セキュリティポリシー、関係規程等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

情報セキュリティタスクフォースは、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。