

関ヶ原町情報セキュリティ対策基準

第1 趣旨

この対策基準は、関ヶ原町情報セキュリティ基本方針に規定する対策等の実施について、必要な事項を定めるものとする。

第2 定義

この対策基準における用語の意義は、関ヶ原町情報セキュリティ基本方針第2条に規定する用語の定義を準用する。

第3 対象範囲

- 1 この対策基準が対象とする資産（以下「対象資産」という。）は、関ヶ原町情報セキュリティ基本方針第1条に規定する「対象資産」のうち、学校の用に供する教育財産を除いたものとする。
- 2 この対策基準の適用範囲は、関ヶ原町（以下「本町」という。）が保有する対象資産、対象資産に関する事務に携わる全ての職員及び委託事業者とする。

第4 組織体制及び役割

- 1 情報セキュリティ対策を実施するための組織体制は、以下のとおりとする。

役職名	職名
総括保護管理者	副町長
監査責任者	総務課長
保護管理者	各課・室の長
保護担当者	保護管理者が指定する者
職員及び委託事業者	職員及び委託事業者

- 2 各組織の役割は以下のとおりとする。

役職名	役割・権限等
総括保護管理者	<ol style="list-style-type: none">1 本町における全ての対象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 総括保護管理者は、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ことができる。
監査責任者	<ol style="list-style-type: none">1 総括保護管理者を補佐する。2 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。3 保護管理者に対して、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。4 本町の共通的な対象資産に関する情報セキュリティ実施手順の策定及び維持・管理を行う権限及び責任を有する。5 監査責任者は、本町の情報資産に対するセキュリティ侵害が発

	<p>生じた場合又はセキュリティ侵害のおそれがある場合に、総括保護管理者の指示に従い、総括保護管理者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。</p> <p>6 監査責任者は、緊急時等の円滑な情報共有を図るため、総括保護管理者、監査責任者、保護管理者、保護担当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。</p> <p>7 監査責任者は、緊急時には総括保護管理者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。</p>
保護管理者	<p>1 所管する課室等及び情報システム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。</p> <p>2 監査責任者の指示に従い、所管する対象資産に係る情報セキュリティ実施手順の策定及び更新を行う。</p> <p>3 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。</p> <p>4 保護管理者は、その所掌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、監査責任者及び総括保護管理者へ速やかに報告を行い、指示を仰がなければならない。</p>
保護担当者	<p>保護管理者の指示等に従い、その所属する課室及び施設等の情報セキュリティに関する対策の向上を図る。</p>
職員及び委託事業者	<p>情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守する。</p>

3 兼務の禁止

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

4 情報セキュリティに関する統一的な窓口の設置（CSIRT）

- (1) 総括保護管理者は、情報セキュリティの事件・事故等の情報セキュリティインシデント（以下、「情報セキュリティインシデント」という。）の統一的な窓口としてCSIRTを設置し、情報セキュリティインシデントについて課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する。
- (2) CSIRTは、総括保護管理者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、その内容を関係課等に提供する。
- (3) CSIRTは、情報セキュリティに関して、外部の事業者等との情報共有を行う。
- (4) CSIRTは、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られるための連絡手段を公表するものとする。

5 クラウドサービス利用における組織体制

総括保護管理者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を

確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

第5 情報資産の分類と管理方法

1 情報資産の分類

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、当該分類に応じた取扱制限を行うものとする。

(1) 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	1 関ヶ原町情報公開条例第7条に規定する非公開情報のうち、特定の職員又は組織等、業務上必要とする最小限の者のみが扱う情報 2 特定個人情報	1 分類2に掲げる対策のほか以下に掲げる事項 ・暗号化やパスワード設定 2 特定個人情報においては、上記に掲げる対策のほか以下に掲げる事項 ・法令で定める以外の事務での取扱いの禁止 ・インターネットに接続したコンピュータへの作成・保管・複製
機密性2	関ヶ原町情報公開条例第7条に規定する非公開情報のうち、上記以外の情報資産	1 許可された者以外による閲覧の制限 2 適切なネットワーク回線の選択 3 必要以上の複製及び配付禁止 4 情報資産の送信・運搬・提供時における暗号化、パスワード設定、鍵付きケースへの格納等 5 外部記録媒体の施錠可能な場所への保管 6 復元不可能な処理を施しての廃棄
機密性1	上記以外の情報資産	

(2) 完全性による情報資産の分類

分類	分類基準	取扱制限
完全性2	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	1 許可された者以外による編集の制限 2 バックアップの作成、保管 3 外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所への保管
完全性1	上記以外の情報資産	

(3) 可用性による情報資産の分類

分類	分類基準	取扱制限
----	------	------

可用性 2	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。）及ぼすおそれがある情報資産	1 サーバやネットワーク等の冗長化 2 バックアップの作成、保管及び相当時間以内の復旧 3 外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設可能な場所への保管
可用性 1	上記以外の情報資産	

2 情報資産の管理

(1) 管理責任

ア 保護管理者は、その所管する情報資産について管理責任を有する。

イ 保護管理者は、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も 1 の分類に基づき管理しなければならない。

ウ 保護管理者は、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 1 の分類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。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、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) 情報の作成及び消去

ア 職員は、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、当該情報が作成途上であっても、1 の分類に基づき管理しなければならない。

ウ 情報を消去する者は、情報が不要になった場合は、当該情報を速やかに消去しなければならない。

(3) 情報資産の入手

自己以外の者が作成した情報資産を入手した者は、1 の分類に基づいた取扱いをしなければならない。

(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、適切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、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 保護管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

イ 保護管理者は、情報資産を記録した外部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 保護管理者は、利用頻度が低い外部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外部記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

エ 保護管理者は、機密性2以上、完全性2又は可用性2の情報資産を記録した外部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設可能な場所に保管しなければならない。

(6) 情報資産の運搬

ア 機密性2以上の情報資産を運搬する者は、保護管理者に許可を得なければならない。

イ 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、暗号化し、又はパスワードを設定する等、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。

(7) 情報資産の提供又は公表

ア 機密性2以上の情報資産を外部に提供する者は、保護管理者に許可を得なければならない。

イ 保護管理者は、機密性2以上の情報資産の外部提供を許可する場合は、当該情報資産の外部提供が関ヶ原町個人情報保護条例及びその他関連する規定に抵触しないことを確認しなければならない。

ウ 機密性2以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

エ 保護管理者は、住民に提供又は公表する情報資産について、完全性を確保しなければならない。

(8) 情報資産の廃棄

ア 機密性2以上の情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、物理的に破壊又はデータ消去ソフト等を利用し、情報を復元できないように処置した上で廃棄しなければならない。

イ 機密性2以上の情報資産の廃棄を行う者は、保護管理者の許可を得なければならない。

ウ 機密性2以上の情報資産の廃棄を行う者は、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。また、廃棄を委託した場合も同様とし、必要に応じて証明書等の提出を求めなければならない。

エ 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時期を確認し、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6 物理的セキュリティ

1 サーバ等の管理

(1) 機器の取付け

保護管理者は、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

保護管理者は、所管するサーバに格納している情報の重要性、可用性、停止することによる業務への影響度等を勘案し、必要に応じて冗長化を施し、サービスや業務を停止させないよう努めなければならない。

(3) 機器の電源

ア 保護管理者は、監査責任者及び施設管理部門と連携し、所管する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可能な限り備え付けなければならない。

イ 保護管理者は、監査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、所管するサーバ等の機器を保護するための措置を可能な限り講じなければならない。

(4) 通信ケーブル等の配線

ア 保護管理者は、施設管理部門と連携し、所管する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。

イ 保護管理者は、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、連携して対応しなければならない。

ウ 保護管理者は、ネットワークの接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

エ 保護管理者は、自ら又は操作を認めた者以外の者が、配線を変更、追加できないように必要な措置を施さなければならない。

(5) 機器の定期保守及び修理

ア 保護管理者は、所管するサーバ等の機器の定期保守を必要に応じて実施しなければならない。

イ 保護管理者は、電磁的記録媒体を内蔵する機器を外部の事業者修理させる場合、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、保護管理者は、外部の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、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) 庁舎外への機器の設置

保護管理者は、庁舎外に所管するサーバ等の機器を設置する場合、総括保護管理者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。

(7) 機器の廃棄等

保護管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

2 管理区域の管理

(1) 管理区域の構造等

ア 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、当該機器等の管理並びに運用を行うための部屋や電磁的記録媒体の保管庫をいう。

イ 監査責任者及び保護管理者は、施設管理部門と連携して、可能な限り管理区域を地階又は1階に設けてはならない。また、無窓の外壁にする等可能な限り外部からの侵入が容易にできないようにしなければならない。

ウ 保護管理者は、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。

エ 保護管理者は、施設管理部門と連携して、可能な限り管理区域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。

オ 保護管理者は、施設管理部門と連携して、可能な限り管理区域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。

カ 保護管理者は、施設管理部門と連携して、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。

(2) 管理区域の入退室管理等

ア 保護管理者は、施設管理部門と連携して、管理区域への入退室を許可された者のみに制限し、磁気又はID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。

イ 職員及び委託事業者は、管理区域に入室する場合、入室許可証及び身分証明書等を見やすい位置に着用しなければならない。

ウ 保護管理者は、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。

(3) 機器等の搬入出

ア 保護管理者は、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を確認を行わせなければならない。

イ 保護管理者は、管理区域の機器等の搬入出について、職員を立ち合わせなければならない。

3 通信回線及び通信回線装置の管理

(1) 監査責任者は、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、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

(2) 監査責任者は、本町の管轄外のネットワーク（以下「外部ネットワーク」という。）との接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

(3) 監査責任者は、情報システム全体の強靱性の向上のために、情報システム全体に対し、次の三段階の対策を講じなければならない。

ア マイナンバー利用事務系においては、原則として他の領域との通信をできないようにして、端末からの情報持ち出し不可設定や端末への二要素認証の導入等により、住民情報の流出を防ぐ。

イ LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムと通信経路の分割をする。

ウ インターネット接続系においては、不正通信監視機能強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、自治体情報セキュリティクラウドを導入する。

(4) 監査責任者は、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

(5) 監査責任者は、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。

(6) 監査責任者は、機密性2以上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、回線を冗長化する等の措置を講じなければならない。

4 職員のパソコン等の管理

- (1) 保護管理者は、執務室等のパソコン等の端末について、盗難による情報資産の流出を防止するため、ワイヤーによる固定等の措置を講じなければならない。ただし、情報資産を蓄積しないプリンタ、スキャナ、クライアント端末等は除く。
- (2) 保護管理者は、マイナンバー利用事務系パソコン等の端末及び情報システムを使用するためには、ID、パスワード、生体認証等複数の認証が必要となるよう設定しなければならない。

第7 人的セキュリティ

1 職員の遵守事項

(1) 職員の遵守事項

ア 情報セキュリティポリシー等の遵守

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、情報セキュリティに関する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、速やかに保護管理者に報告し、指示を仰がなければならない。

イ 業務以外の目的での使用の禁止

職員は、業務以外の目的で対象資産を使用してはならない。

ウ 対象資産の持ち出し及び外部における情報処理作業の制限

- ① 職員は、対象資産を外部に持ち出す場合には、保護管理者の許可を得なければならない。また、保護管理者は、その記録を作成し、保管しなければならない。
- ② 職員は、外部で情報処理業務を行う場合には、保護管理者の許可を得なければならない。
- ③ 職員は、外部で情報処理作業を行う際、本町が管理する以外のパソコンを用いる場合には、保護管理者の許可を得た上で、保護管理者が定めた実施手順を遵守しなければならない。

エ 私物機器の使用制限

- ① 職員は、本町が管理する以外の電磁的記録媒体やパソコン等の機器を対象資産に読み込み又は接続してはならない。ただし、業務上必要な場合で、監査責任者の許可を得た場合はこの限りでない。
- ② 保護管理者は、私物機器の使用について、記録を作成し、保管しなければならない。

オ 情報システムにおけるセキュリティ設定変更の禁止

職員は、情報システムに関するセキュリティ機能の設定を保護管理者の許可なく変更してはならない。

カ 机上の対象資産の管理

- ① 職員は、机上のパソコン等の端末を第三者に使用されること、又は保護管理者の許可なく情報を閲覧されることがないように、離席する際にはIDカードを取り外し、端末をロックすることにより、情報資産を保全しなければならない。
- ② 職員は、IDカードによる運用対象外の情報システムについては、離席する際には、アプリケーションの終了、パスワードによるロックをかけたスクリーンセーバー、ログオフ等の手段を複合的に用いることにより、情報資産を保全しなければならない。
- ③ 職員は、机上の記録媒体、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、又は保護管理者の許可なく情報を閲覧されることがないように、離席する際には、記録媒体や文書等を容易に閲覧されない場所へ保管する等、適切な措置を講じなければならない。

キ 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、利用していた対象資産を、保護管理者に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への対応

ア 情報セキュリティポリシー等の遵守

保護管理者は、非常勤及び臨時職員に対し、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。

イ 情報セキュリティポリシー等の遵守に対する同意

保護管理者は、非常勤及び臨時職員の採用の際、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についての署名を求めるものとする。

ウ インターネット接続及び電子メール使用等の制限

保護管理者は、非常勤及び臨時職員にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) 委託事業者に対する説明

保護管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者が発注する場合、委託事業者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委託事業者が守るべき内容を理解させ、これを遵守させなければならない。

2 研修・訓練

(1) 情報セキュリティに関する研修・訓練

総括保護管理者は、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) 研修計画の立案及び実施

ア 総括保護管理者は、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を定期的に立案しなければならない。

イ 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。

ウ 研修は、保護管理者及びその他職員に対して、それぞれの役割等に応じたものに行われなければならない。

(3) 緊急時対応訓練

総括保護管理者は、定期的又は必要に応じて緊急時対応を想定した訓練を実施しなければならない。訓練計画は、ネットワーク及び情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

職員は、定められた研修・訓練に参加しなければならない。

3 事故、欠陥等の報告及び対処

(1) 事故、欠陥等の報告

職員は、情報セキュリティに関する事故並びに情報システムの欠陥及び誤動作を発見した場合又は住民等外部から報告を受けた場合、速やかに保護管理者に報告しなければならない。

(2) 事故、欠陥等の対処

保護管理者は、報告のあった事故等について、緊急時対応計画に従い適切に対処しなければならない。

4 ID及びパスワード等の管理

(1) ID等の取扱い

保護管理者及び職員は、ID等について関係実施手順に基づき適切に取扱わなければならない。

(2) IDの取扱い

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。

ア 自己が利用しているIDは、他人に利用させてはならない。

イ 共用IDを利用する場合は、共用IDの利用を許可された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。

ア 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。

イ 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。

ウ 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。

エ パスワードが流出したおそれがある場合には、保護管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

オ 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。

カ 複数の情報システムにおいて、同一のパスワードを用いてはならない。

キ 初期パスワード又は仮のパスワードは、最初のログイン時点で変更しなければならない。

ク パソコン等の端末のパスワードの記憶機能を利用してはならない。

ケ 職員間でパスワードを共有してはならない。

第8 技術的セキュリティ

1 情報システム及びネットワークの管理

(1) 情報システムの設定等

ア 保護管理者は、情報システムを設置する場合、他課室等の許可していない職員が情報資産を閲覧及び使用できないように、アクセス制御の設定をしなければならない。

イ 保護管理者は、課室内の特定の職員しか取扱えない情報資産がある場合は、別領域を作成しアクセス制御の措置を講じる等、同一課室内であっても、担当職員以外の職員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

ア 監査責任者及び保護管理者は、必要に応じて情報資産のバックアップを実施しなければならない。

イ 監査責任者及び保護管理者は、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、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が関ヶ原町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。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

(3) 他団体との情報システムに関する情報等の交換

保護管理者は、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、必要に応じてその取扱いに関する事項をあらかじめ定め、総括保護管理者の許可を得なければならない。

(4) システム管理記録及び作業の確認

ア 保護管理者は、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。

イ 保護管理者は、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、窃取、改ざん等をされないように適切に管理しなければならない。

ウ 保護管理者は、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う場合は、必要に応じて2名以上で作業させ、互いにその作業を確認させなければならない。

(5) 情報システム仕様書等の管理

保護管理者は、所管する情報システムのネットワーク構成図、仕様書等の情報資産について、業務上必要とする者以外の者が閲覧、紛失等がないよう、適切に管理しなければならない。

(6) ログの取得等

ア 保護管理者は、所管する情報システムの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。

イ 保護管理者は、ログ等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

ウ 保護管理者は、所管する情報システムから自動出力したログ等について、必要に応じ、外部記録媒体にバックアップしなければならない。

エ 保護管理者は、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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

オ 監査責任者及び保護管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、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。

(7) 障害記録

監査責任者及び保護管理者は、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、適切に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

ア 監査責任者は、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、ネットワークを設定しなければならない。

イ 監査責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

(9) 外部の者が利用できるシステムの分離等

保護管理者は、所管する情報システムにおいて、外部の者が利用できる場合、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

ア 保護管理者は、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、総括保護管理者及び監査責任者の許可を得なければならない。

イ 保護管理者は、接続しようとする外部ネットワークに係るセキュリティ技術等を詳細に調査し、庁内の全ての対象資産に影響が生じないことを確認しなければならない。

ウ 保護管理者は、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、必要に応じて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。

エ 監査責任者及び保護管理者は、ウェブサーバ等の情報システムをインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。

オ 保護管理者は、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、対象資産に脅威が生じることが想定される場合には、監査責任者の判断に従い、速やかに当該外部ネットワークを遮断しなければならない。

(11) 複合機のセキュリティ管理

ア 監査責任者は、プリンタ・ファクシミリ・イメージスキャナ・コピー機等の機能が一つにまとめられている機器（以下「複合機」という。）を調達する場合、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、適切なセキュリティ要件を策定しなければならない。

イ 監査責任者又は複合機を調達した保護管理者は、複合機が備える機能について適切な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ 監査責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消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。

(12) 特定用途機器のセキュリティ管理

ア 監査責任者は、IP電話システム、ネットワークカメラシステム等の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。

(13) 無線LANの利用

ア 保護管理者は、無線LANを利用するときは、監査責任者の許可を得なければならない。

イ 監査責任者は、無線LANの利用を認める場合、情報の破壊、盗聴、改ざん、消去等が生じないように暗号化及び認証技術、その他十分なセキュリティ対策の実施を義務づけなければならない。

(14) 電子メールのセキュリティ管理

ア 監査責任者は、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。

イ 監査責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

ウ 監査責任者は、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。

エ 監査責任者は、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。

オ 監査責任者は、システム開発や運用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、委託先との間で利用方法を取り決めなければならない。

(15) 電子メールの利用制限

ア 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。

イ 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。

ウ 職員は、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。

エ 職員は、重要な電子メールを誤送信した場合、保護管理者に報告しなければならない。

(16) 電子署名・暗号化

ア 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、総括保護管理者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

イ 職員は、暗号化を行う場合に総括保護管理者が定める以外の方法を用いてはならない。また、総括保護管理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。

ウ 総括保護管理者は、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。

(17) 無許可ソフトウェアの導入等の禁止

ア 職員は、情報システムに業務上の必要がないソフトウェアを導入してはならない。

イ 職員は、業務上の必要がある場合に限り、監査責任者及び当該情報システムを所管する保護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。

ウ 職員は、不正にコピー、改ざん等されたソフトウェアを利用してはならない。

エ 保護管理者は、所管する課室等で利用するソフトウェアについて、不正にコピー、改ざん等されたものを利用することや、保有するライセンス数を超えて利用すること等を防止するため、ライセンスを管理しなければならない。

(18) 機器構成の変更の制限

職員は、情報システムに対し機器の改造及び増設・交換を行ってはならない。ただし、業務上の必要がある場合は、監査責任者及び当該情報システムを所管する保護管理者の許可を得

て、これを行うことができる。

(19) 無許可でのネットワーク接続の禁止

職員は、監査責任者の許可なく情報システムをネットワークに接続してはならない。

(20) 業務以外の目的でのウェブサイトへのアクセス制限

ア 職員は、ネットワーク等に障害を発生させるおそれがあるため、業務以外の目的でウェブを閲覧してはならない。

イ 監査責任者は、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、保護管理者に通知し適切な措置を求めなければならない。

2 アクセス制御等

(1) アクセス制御等

ア アクセス制御

監査責任者又は保護管理者は、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、システム上制限しなければならない。

イ 利用者ID等の取扱い

① 監査責任者又は保護管理者は、所管する情報システムに係る利用者の登録、変更、抹消等の情報管理、職員の異動、出向、退職に伴う利用者ID等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、当該情報システムを所管する保護管理者に報告しなければならない。

③ 監査責任者又は保護管理者は、所管する情報システムについて、利用されていないID等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。

ウ 特権を付与されたID等の管理等

① 監査責任者及び保護管理者は、所管する情報システムに係る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等を厳重に管理しなければならない。

② 監査責任者又は保護管理者の管理者権限等の特権を付与されたID等を利用する者は、監査責任者又は保護管理者が認めた者でなければならない。

③ 監査責任者及び保護管理者は、管理者権限等の特権を付与されたID等の変更について、委託事業者に行わせてはならない。

④ 監査責任者及び保護管理者は、管理者権限等の特権を付与されたID等について、職員の端末等のパスワードよりもセキュリティ機能を強化しなければならない。

⑤ 監査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。

(2) 職員による外部からのアクセス等の制限

ア 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、監査責任者及び当該情報システムを所管する保護管理者の許可を得なければならない。

イ 監査責任者及び当該情報システムを所管する保護管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

ウ 監査責任者は、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。

エ 監査責任者は、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。

オ 監査責任者及び当該情報システムを所管する保護管理者は、外部からのアクセスに利用するパソコン等の端末に、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。

カ 職員は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

キ 監査責任者は、公衆通信回線（公衆無線LAN等）の庁外通信回線を庁内ネットワークに接続することは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及びこれを記録した媒体（IDカード等）による認証に加えて通信内容の暗号化等の措置を講ずる等、情報セキュリティの確保に努めるものとする。

(3) 自動識別の設定

監査責任者及び情報システム管理者は、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できるよう努めるものとする。

(4) ログイン時の表示等

保護管理者は、所管する情報システムについて、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情報システムを設定しなければならない。

(5) パスワードに関する情報の管理

ア 監査責任者又は情報システムを所管する保護管理者は、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。

イ 監査責任者又は情報システムを所管する保護管理者は、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。

(6) 特権による接続時間の制限

監査責任者又は情報システムを所管する保護管理者は、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。

3 システム開発、導入、保守等

(1) 情報システムの調達

ア 監査責任者及び情報システムを所管する保護管理者は、情報システムの開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ 監査責任者及び情報システムを所管する保護管理者は、情報システムの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2) 情報システムの開発

ア 情報システムの開発における責任者及び作業者の特定

情報システムを所管する保護管理者は、情報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。

イ 情報システムの開発における責任者、作業者のIDの管理

- ① 情報システムを所管する保護管理者は、情報システムの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。
- ② 情報システムを所管する保護管理者は、情報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。

ウ 情報システムの開発に用いるハードウェア及びソフトウェアの管理

- ① 情報システムを所管する保護管理者は、情報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なければならない。
- ② 情報システムを所管する保護管理者は、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、必要に応じて当該ソフトウェアを情報システムから削除しなければならない。

(3) 情報システムの導入

ア 開発環境と運用環境の分離及び移行手順の明確化

- ① 情報システムを所管する保護管理者は、情報システムの開発・保守及びテスト環境から情報システムの運用環境への移行について、情報システムの開発・保守計画の策定時に手順を明確にしなければならない。
- ② 情報システムを所管する保護管理者は、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し、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。

イ テスト

- ① 情報システムを所管する保護管理者は、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。
- ② 情報システムを所管する保護管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
- ③ 開発したシステムについて受け入れテストを行う場合、システムを所管する部署及び情報政策課がそれぞれ独立したテストを行わなければならない。

(4) システム開発・保守に関連する資料等の整備・保管

ア 情報システムを所管する保護管理者は、情報システムの開発・保守に関連する資料及びシステム関連文書を適切な方法で整備・保管しなければならない。

イ 情報システムを所管する保護管理者は、テスト結果を一定期間保管しなければならない。

(5) 情報システムにおける入出力データの正確性の確保

ア 情報システムを所管する保護管理者は、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。

イ 情報システムを所管する保護管理者は、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。

ウ 情報システムを所管する保護管理者は、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。

(6) 情報システムの変更管理

情報システムを所管する保護管理者は、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。

(7) 開発・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保護管理者は、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。

(8) システム更新又は統合時の検証等

保護管理者は、所管する情報システムの更新・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。

4 不正プログラム対策

(1) 監査責任者の措置事項

監査責任者は、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。

ア 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、不正プログラムの情報システムへの侵入を防止しなければならない。

イ 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。

ウ 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。

エ 所管する情報システムに、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。

オ 所管する情報システムに対して、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実施しなければならない。

カ 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。

キ 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。

(2) 保護管理者の措置事項

情報システムを所管する保護管理者は、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。

ア 所管する情報システムに、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。

イ 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。

ウ 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。

エ 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、町が管理している媒体以外を利用させてはならない。

オ インターネットに接続していない情報システムにおいて、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定

期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

カ 仮想マシンを設定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、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者へ報告を求めなければならない。

(3) 職員の遵守事項

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。

ア パソコン等の端末において、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。

イ 外部から情報資産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。

ウ 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。

エ パソコン等の端末に対して、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。

オ 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。

カ 監査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。

キ コンピュータウイルス等の不正プログラムに感染したと思われる場合は、緊急時対応計画に従い適切に対処しなければならない。

5 不正アクセス対策

(1) 監査責任者の措置事項

監査責任者は、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。

ア 使用されていないポートを閉鎖しなければならない。

イ 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。

ウ 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するよう設定しなければならない。

エ 重要な情報システムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ 監査責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応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。

カ 本町が定めた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が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者へ確認しなければならない。

キ クラウドサービスを利用する際に、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、クラウドサービスにアクセスさせなければならない。

(2) 攻撃の予告

総括保護管理者及び監査責任者は、情報システムに攻撃を受けることが明確になった場合、情報システムの停止を含む必要な措置を講じなければならない。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

総括保護管理者及び監査責任者は、所管する情報システムに攻撃を受け、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

監査責任者及び情報システムを所管する保護管理者は、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

監査責任者及び保護管理者は、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保護管理者に通知し、緊急時対応計画による対処を求めなければならない。

(6) サービス不能攻撃

監査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

監査責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

6 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

ア 監査責任者及び情報システムを所管する保護管理者は、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。

イ 監査責任者及び保護管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、関ヶ原町の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認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

監査責任者は、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。

(3) 情報セキュリティに関する情報の収集及び共有

監査責任者及び保護管理者は、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、セキュリティ侵害等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9 運用

1 情報システムの監視

- (1) 監査責任者及び情報システムを所管する保護管理者は、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) 監査責任者及び情報システムを所管する保護管理者は、重要なアクセスログ等を取得する情報システムの正確な時刻設定及び情報システム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で使用す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。
- (3) 監査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。
- (4) 監査責任者及び情報システムを所管する保護管理者は、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の使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。
- (5) 監査責任者及び情報システムを所管する保護管理者は、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、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうか検討しなければならない。
- (5) 監査責任者及び情報システムを所管する保護管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

ア 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のインストール、変更及び削除

イ クラウドサービス利用の終了手順

ウ バックアップ及び復旧

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
 - ア 保護管理者は、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、問題を認められた場合には、速やかに総括保護管理者及び監査責任者に報告しなければならない。
 - イ 総括保護管理者は、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。
 - ウ 監査責任者及び情報システムを所管する保護管理者は、ネットワーク及びサーバ等の情報システムの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) パソコン等の端末及び電磁的記録媒体等の利用状況調査

総括保護管理者が指名した者は、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等の端末、電磁的記録媒体のログ、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) 職員の報告義務
 - ア 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、直ちに監査責任者及び保護管理者に報告を行わなければならない。
 - イ 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場合と監査責任者が判断した場合は、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。

3 侵害時の対応

(1) 緊急時対応計画の策定

ア 総括保護管理者は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により対象資産への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、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。

イ 総括保護管理者は、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、これらを踏まえてクラウドサービスの障害時を想定した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。

ア 発生した事案に応じた報告先

イ 発生した事案に係る報告すべき事項

ウ 発生した事案への対応措置

エ 再発防止措置の策定

(3) 業務継続計画との整合性確保

本町が自然災害等に備えて業務継続計画を策定する場合、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

総括保護管理者は、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、緊急時対応計画の規定を見直し、必要に応じて改定しなければならない。

4 委託

(1) 外部委託事業者の選定基準

ア 保護管理者は、委託先の選定にあたり、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。

イ 保護管理者は、個人番号利用事務等の全部又は一部を委託する場合には、外部委託事業者（委託の要素を含む賃貸借・修繕等についても同じ）において、番号法に基づく安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。

ウ 保護管理者は、機密性2以上の情報資産を委託する場合には、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、事業者を選定するよう努めるものとする。

エ 保護管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

(2) 契約項目

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

ア 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

イ 委託先の責任者、委託内容、作業者、作業場所の特定

ウ 提供されるサービスレベルの保証

- エ 従業員に対する教育の実施
- オ 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
- カ 業務上知り得た情報の守秘義務
- キ 再委託に関する制限事項の遵守
- ク 委託業務終了時の情報資産の返還、廃棄等
- ケ 委託業務の定期報告及び緊急時報告義務
- コ 町による監査、検査（委託内容に応じた情報セキュリティ対策確保のための実地調査を含む。）
- サ 町による情報セキュリティインシデント発生時の公表
- シ 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）
- ス 特定個人情報の持ち出しの原則禁止

(3) 確認・措置等

保護管理者は、外部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、契約に基づき措置しなければならない。

(4) 再委託の承認

個人番号利用事務等の全部又は一部の委託を受けた者が再委託をする際には、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断しなければならない。

5 ソーシャルメディアサービスの利用

(1) 保護管理者は、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る等、情報セキュリティ対策を講じることとする。

ア 発信する情報が、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行うこと。

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（IDカード等）等を適切に管理する等の方法で、不正アクセス対策を行うこと。

(2) 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。

6 例外措置

(1) 例外措置の許可

保護管理者は、情報セキュリティポリシーを遵守することが困難な状況で、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、総括保護管理者の許可を得て、例外措置を取ることができる。

(2) 緊急時の例外措置

保護管理者は、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、事後速やかに総括保護管理者に報告しなければならない。

(3) 例外措置の申請書の管理

総括保護管理者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

7 法令遵守

(1) 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。

ア 地方公務員法（昭和25年法律第261号）

イ 著作権法（昭和45年法律第48号）

ウ 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）

エ 個人情報の保護に関する法律（平成15年法律第57号）

オ 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）

(2) 監査責任者及び情報システムを所管する保護管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

8 違反に対する対応

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。

(1) 監査責任者が違反を確認した場合は、監査責任者は当該職員が所属する課室等の保護管理者に通知し、適切な措置を求めなければならない。

(2) 情報システムを所管する保護管理者が違反を確認した場合は、速やかに監査責任者及び当該職員が所属する課室等の保護管理者に通知し、適切な措置を求めなければならない。

(3) 保護管理者の指導によっても改善されない場合、監査責任者は、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あるいは剥奪することができる。その後速やかに、監査責任者は、職員の権利を停止あるいは剥奪した旨を総括保護管理者及び当該職員が所属する課室等の保護管理者に通知しなければならない。

第10 評価・見直し

1 監査

(1) 実施方法

総括保護管理者は、情報セキュリティ対策状況について、定期的に又は必要に応じて監査をしなければならない。

(2) 監査実施計画の立案及び実施への協力

ア 総括保護管理者は、監査を行うに当たって、監査実施計画を立案しなければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

(3) 外部委託事業者に対する監査

保護管理者は、情報セキュリティ対策を要する業務を外部委託する場合は、委託事業者及び再委託を認める場合の再委託先事業者において、必要な情報セキュリティ対策が確保されていることを確認するために、定期的に又は必要に応じて監査を実施しなければならない。

(4) 報告

総括保護管理者は、監査結果を取りまとめ、必要があると認めるときは、町長に報告する。

(5) 保管

総括保護管理者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

(6) 監査結果への対応

総括保護管理者は、監査結果を踏まえ、指摘事項を所管する保護管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない保護管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

(7) 情報セキュリティポリシー及び関係規定等の見直し等への活用

総括保護管理者は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、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。

2 自己点検

(1) 実施方法

ア 監査責任者及び保護管理者は、所管する対象資産に係る情報セキュリティ対策状況について、定期的に又は必要に応じ自己点検を実施しなければならない。

イ 保護管理者は、保護管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的に又は必要に応じ自己点検を行わなければならない。

(2) 報告

監査責任者及び保護管理者は、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、総括保護管理者に報告しなければならない。

(3) 自己点検結果の活用

ア 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。

イ 総括保護管理者は、この点検結果を情報セキュリティポリシー及び関係規定等の見直し、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。

3 情報セキュリティポリシー及び関係規定等見直し及び改定

総括保護管理者は、情報セキュリティポリシー及び関係規定等について情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、定期的に見直しを行い、必要があると認めた場合、その改定を行うものとする。

附 則

この基準は、平成27年10月5日から施行する。

附 則

この基準は、平成29年4月1日から施行する。

附 則

この基準は、令和2年4月1日から施行する。

附 則

この基準は、令和6年5月15日から施行する。