厚岸町
情報セキュリティポリシー

令和元年９月１日策定

厚　岸　町

目　次

第１章　総則

１　厚岸町情報セキュリティポリシー

厚岸町情報セキュリティポリシーとは、厚岸町の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

情報セキュリティポリシーは、厚岸町が所掌する情報資産に関する業務に携わる全職員（非常勤及び臨時職員含む。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。また、情報の処理技術や通信技術等の進歩、新たな脅威等に対応すべく、情報セキュリティポリシーの評価・見直しを行い、情報セキュリティ対策の実効性を確保する必要がある。

２　厚岸町における情報セキュリティの考え方

厚岸町は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを提供している。また、町の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、ＬＧＷＡＮ等のネットワークにより相互に接続しており、発生したＩＴ障害がネットワークを介して連鎖的に拡大する可能性は否定できない。

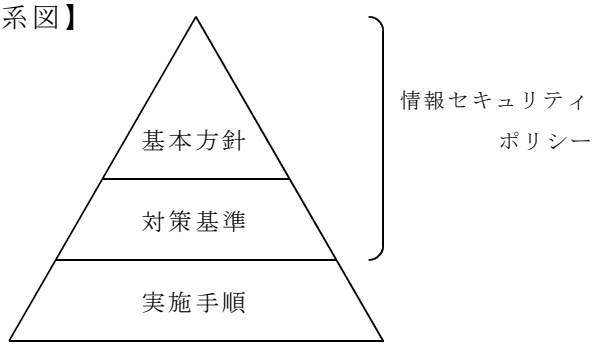
これらの事情から、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

３　情報セキュリティポリシーの構成

情報セキュリティポリシーの体系は、下図に示す階層構造となっている。

厚岸町の情報セキュリティ対策における基本的な考え方を定めるものが、「基本指針」である。この基本指針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めるものが「対策基準」である。この「基本指針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「対策基準」を、具体的なシステムや手順、手続きに展開して個別の実施事項を定めるものが「実施手順」である。

【情報セキュリティポリシーに関する体系図】



第２章　厚岸町情報セキュリティ基本方針

１　目的

この基本方針は、町が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下「対象資産」という。）について、町が実施する情報セキュリティに関する基本的な事項を定めることを目的とする。

２　定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

(2) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(3) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(4) 情報資産

情報システムで取り扱う情報で、開発及び運用に係るものを含む全ての情報をいう。

(5) 情報セキュリティ

対象資産の機密性、完全性及び可用性を維持することをいう。

(6) 情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

(7) 機密性

対象資産にアクセスすることを認められた者だけが、対象資産にアクセスできる状態を確保することをいう。

(8) 完全性

対象資産が破壊、改ざん、消去又は不正なデータがない状態を維持し、データの正当性、正確性、一貫性を確保することをいう。

(9) 可用性

対象資産にアクセスすることを認められた者が、必要なときに中断されることなく、対象資産にアクセスできる状態を確保することをいう。

(10) 特定個人情報

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（以下「番号法」という。）第２条に規定する個人番号をその内容に含む個人情報ファイルをいう。

(11) 個人番号利用事務

番号法第２条に規定する個人番号を利用して処理する事務をいう。

３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 人による脅威（故意）

不正アクセスやウイルス攻撃等のサイバー攻撃、機器の盗難、対象資産の不正な操

作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等

(2) 人による脅威（過失）

対象資産の管理不備、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備等の過失による情報資産の漏えい・破壊・消去等

(3) 災害による脅威

地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消失等

(4) 必要資源の不足、故障等による脅威

災害の影響又はその他の原因による電力、通信、水道の途絶、交通機能の麻痺や大規模・広範囲にわたる疾病の蔓延による要員の不足、機器の故障等によるサービスや業務の停止、システム運用の機能不全等

4　適用範囲

この基本方針の適用範囲は、町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、非常勤職員、臨時職員（以下「職員等」という。）及び委託事業者とする。

5　遵守義務

職員等及び委託事業者は、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しなければならない。

6　情報セキュリティ対策

上記３の脅威から対象資産を保護するために、以下の情報セキュリティ対策を講じるものとする。

(1) 組織体制

情報セキュリティ対策を推進する全庁的な組織体制の確立

(2) 情報資産の分類と管理

町の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づく情報セキュリティ対策

(3) 物理的セキュリティ

対象資産の設置方法又は保管施設の管理についての物理的な対策

(4) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策

(5) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策

(6) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際の情報セキュリティの確保等、情報セキュリティポリシーの運用面の対策、対象資産への侵害が発生した場合等に、迅速かつ適切に対応するための緊急時対応計画の策定

7　情報セキュリティに関する監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティに関する監査及び自己点検を実施する。

8　情報セキュリティポリシーの見直し及び改定

情報セキュリティに関する監査及び自己点検の結果又は情報セキュリティに関する状況の変化に対応するため、定期的に情報セキュリティポリシーの見直しを行い、必要に応じて改定する。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

なお、情報セキュリティ実施手順については、公にすることにより町の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

11　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３章　厚岸町情報セキュリティ対策基準

１　趣旨

この対策基準は、厚岸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。

２　定義

この対策基準における用語の定義は、厚岸町情報セキュリティ基本方針の２に規定する用語の定義を準用する。

３　対象範囲

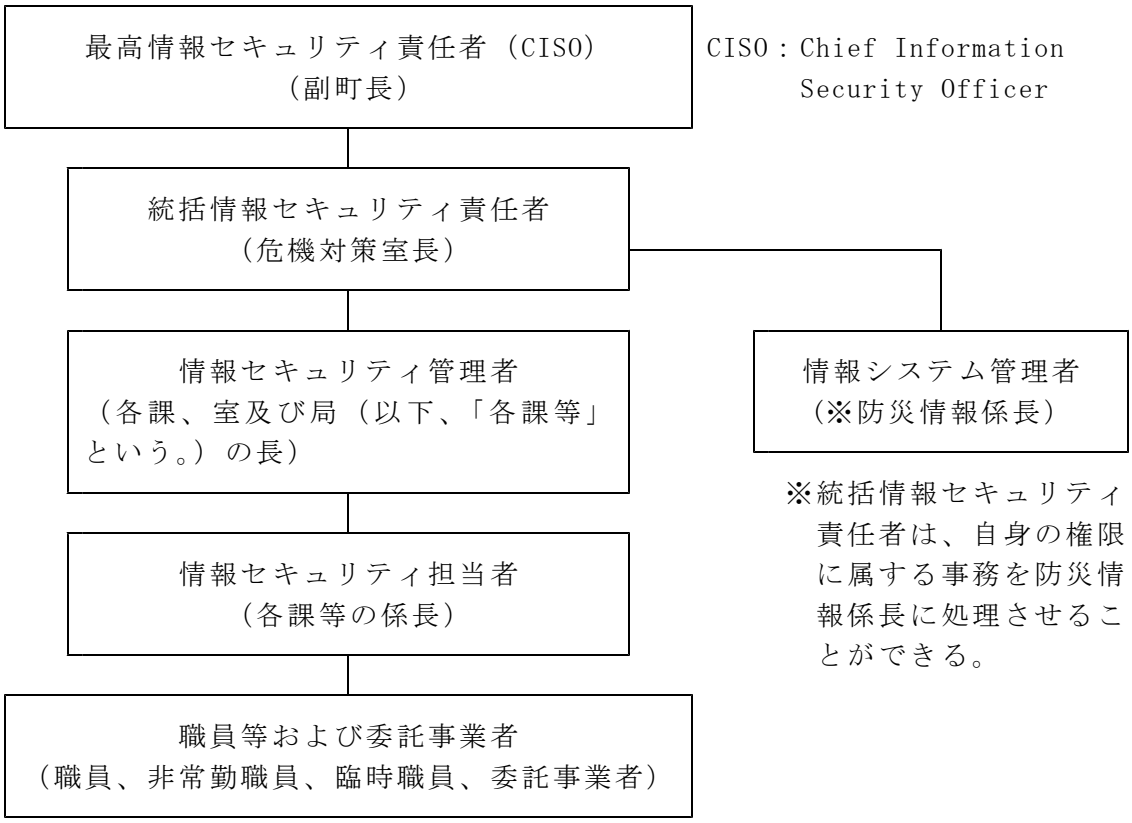
(1) この対策基準が対象とする資産（以下「対象資産」という。）は、厚岸町情報セキュリティ基本方針の１に規定する「対象資産」のうち、厚岸町病院事業に供するもの及び学校の用に供する教育財産を除いたものとする。

(2) この対策基準の適用範囲は、厚岸町病院事業及び教育財産を除く本町（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、非常勤職員、臨時職員（以下「職員等」という。）及び委託事業者とする。

４　組織体制及び役割

(1) 組織体制

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。



(2) 組織の構成員と役割

各組織の構成員及びその役割は以下のとおりとする。

組織・役職名	対象者・構成員	役割・権限等
厚岸町情報化推進委員会	「厚岸町情報処理規則」に基づく 委員長：副町長 副委員長：教育長 委員：危機対策室長、総合政策課長、町民課長、保健福祉課長、出納室長	本町の情報セキュリティ対策を統一的に行うため、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。
最高情報セキュリティ責任者（CISO）	副町長	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　最高情報セキュリティ責任者に事故あるとき、又は最高情報セキュリティ責任者が欠けたときは、統括情報セキュリティ責任者がその職務を代理する。 3　最高情報セキュリティ責任者は、必要に応じて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。
統括情報セキュリティ責任者	危機対策室長	1　最高情報セキュリティ責任者を補佐する。 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　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。 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　統括情報セキュリティ責任者は、本町の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任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。

		6　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ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。 7　統括情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任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。 8　自身の権限に属する事務を、防災情報係長に処理させることができる。
情報セキュリティ管理者	各課等の長	1　所管する課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。 2　所管する課等の情報セキュリティ実施手順を作成する。なお、作成にあたっては、統括情報セキュリティ責任者に意見を求めなければならない。 3　所管する課等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。 4　情報セキュリティ管理者は、その所掌する課等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、統括情報セキュリティ責任者及び最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。
情報セキュリティ担当者	各課等の係長	情報セキュリティ管理者の指示等に従い、その所属する課等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。
職員等及び委託事業者	職員、非常勤職員、臨時職員及び委託事業者	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。

(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

① 最高情報セキュリティ責任者は、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。）の統一的な窓口を整備し、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 情報セキュリティに関する統一的な窓口は、最高情報セキュリティ責任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、その内容を関係部局等に提供する。

③ 情報セキュリティに関する統一的な窓口は、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 情報セキュリティに関する統一的な窓口は、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るための連絡手段を公表するものとする。

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
3	厚岸町情報公開条例第７条に規定する非開示情報のうち、特定の職員等または組織など、業務上必要とする最小限の者のみが扱う情報	分類２に掲げる対策のほか、次に掲げる事項 ・暗号化又はパスワード設定
3	特定個人情報	特定個人情報においては、上記に掲げる対策のほか、次に掲げる事項 ・法令で定める以外の事務での取り扱いの禁止 ・インターネットに接続したコンピュータへの作成・保管・複製の禁止
2	厚岸町情報公開条例第７条に規定する非開示情報のうち、上記以外の情報資産	・許可された者以外による閲覧の制限 ・適切なネットワーク回線の選択 ・必要以上の複製及び配布禁止 ・情報資産の送信・運搬・提供時における暗号化又はパスワード設定、鍵付きケースへの格納等 ・外部記録媒体の施錠可能な場所への保

		管 ・復元不可能な処理を施しての廃棄
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
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	・許可された者以外による編集の制限 ・バックアップの作成、保管 ・外部記憶媒体の耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所への保管
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
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。）を及ぼすおそれがある情報資産	・サーバやネットワーク等の冗長化 ・バックアップの作成、保管及び相当時間以内の復旧 ・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
1	上記以外の情報資産	

(2) 情報資産の管理

① 管理責任

ア 情報セキュリティ管理者は､その所管する情報資産について管理責任を有する。

イ 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。

② 情報の作成及び消去

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、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、情報が不用になった場合は、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、外部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、当該外部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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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、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　情報セキュリティ管理者は、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錠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、情報セキュリティ管理者の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、情報セキュリティ管理者の許可を得なければならない。

イ　情報セキュリティ管理者は、機密性２以上の情報資産の外部提供を許可する場合、当該情報資産の外部提供が厚岸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　情報セキュリティ管理者は、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、情報セキュリティ管理者の許可を得なければならない。

イ　機密性２以上の情報資産の廃棄を行う者は、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、情報を復元不可能な状態に措置を施した上で廃棄しなければならない。

ウ　機密性２以上の情報資産の廃棄を行う者は、行なった処理について、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。

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

統括情報セキュリティ責任者は、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

統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、施設管理部門と連携し、落雷等による過電流に対して、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、電磁的記録媒体を内蔵する機器を外部の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。ただし、内容を消去できない場合は、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

統括情報セキュリティ責任者は、庁舎外に所管するサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、当該機器への情報セキュリティ対策状況について、定期的に確認しなければならない。

⑦　機器の廃棄等

情報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 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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ち入りを防止しなければならない。

エ 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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ＩＣカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。

イ 職員等及び委託事業者は、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 統括情報セキュリティ責任者は、外部からの訪問者が管理区域に入室する場合には、必要に応じて立ち入りを制限した上で、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。

③ 機器等の搬入出

ア 統括情報セキュリティ責任者は、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、あらかじめ職員等又は委託事業者に確認を行わせなければならない。

イ 統括情報セキュリティ責任者は、管理区域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。

(3) 通信回線及び通信回線装置の管理

① 統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

② 統括情報セキュリティ責任者は、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 統括情報セキュリティ責任者は、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、必要に応じて送受信される情報の暗号化を行わなければならない。

④ 統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途

上に情報が破壊、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。

⑤　統括情報セキュリティ責任者は、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、必要に応じて回線を冗長化する等の措置を講じなければならない。

(4) 職員等のパソコン等の管理

①　情報セキュリティ管理者は、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、シンクライアント端末等はこの限りでない。

②　情報セキュリティ管理者は、その所管する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、ＩＣカード、パスワード又はその他の認証方法を組み合わせた複数の認証が必要となるよう設定しなければならない。

7　人的セキュリティ

(1) 職員等の遵守事項

①　職員等の遵守事項

ア　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、速やかに情報セキュリティ管理者に報告し、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

職員等は、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

(ｱ) 職員等は、対象資産を外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。また、情報セキュリティ管理者は、その記録を作成し、保管しなければならない。

(ｲ) 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

(ｳ) 職員等は、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、情報セキュリティ管理者の許可を得た上で、情報セキュリティ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

(ｱ) 職員等は、本町が管理する以外の外部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、統括情報セキュリティ責任者の許可を得た場合はこの限りでない。

(ｲ) 統括情報セキュリティ責任者は、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

職員等は、情報システムに関するセキュリティ機能の設定を統括情報セキュリティ責任者の許可なく変更してはならない。

カ　机上の対象資産の管理

(ｱ) 職員等は、机上のパソコン等の端末を第三者に使用されること、又は情報セ

キュリティ管理者の許可なく情報を閲覧されることがないよう、離席する際にはＩＣ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。

(ｲ) 職員等は、ＩＣカードによる運用対象外の情報システムについて、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。

(ｳ) 職員等は、机上の外部記録媒体、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、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないよう、離席する際には外部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、利用していた対象資産を情報セキュリティ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

情報セキュリティ管理者は、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、実施及び遵守させなければならない。

イ　インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員にパソコン等の操作による業務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

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、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

最高情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、全ての職員等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、最高情報セキュリティ責任者の承認を得なければならない。

イ　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。

ウ　研修は、情報セキュリティ管理者及びその他職員等に対して、それぞれの役割等に応じたものにしなければならない。

エ　統括情報セキュリティ責任者は、最高情報セキュリティ責任者に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

③　緊急時対応訓練

最高情報セキュリティ責任者は、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

職員等は、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

職員等は、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、速やかに情報セキュリティ管理者に報告しなければならない。

②　事故、欠陥等の対処

情報セキュリティ管理者は、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　ＩＣカード等の取扱い

情報セキュリティ管理者及び職員等は、ＩＣカード等について情報セキュリティ実施手順に基づき適切に取り扱わなければならない。

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。

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。

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、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

オ　パスワードは定期的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記憶機能を利用してはならない。

ケ　職員等間でパスワードを共有してはならない。

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　情報セキュリティ管理者は、情報システムを設置する場合、他課等の許可していない職員等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

行わなければならない。

イ　情報セキュリティ管理者は、課等内の特定の職員等しか取り扱えない情報資産がある場合、別領域を作成しアクセス制御の措置を講じる等、同一課等内であっても、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

統括情報セキュリティ責任者及び情報セキュリティ管理者は、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。

③ 他団体との情報システムに関する情報等の交換

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

④ システム管理記録及び作業の確認

ア　情報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作業について、作業記録を作成しなければならない。

イ　情報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う場合は、必要に応じて２人以上で作業させ、互いにその作業を確認させなければならない。

ウ　情報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、窃取、改ざん等をされないよう適切に管理しなければならない。

⑤ 情報システム仕様書等の管理

情報セキュリティ管理者は、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したり、紛失等がないよう、適切に管理しなければならない。

⑥ ログの取得等

ア　情報セキュリティ管理者は、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、一定期間保存しなければならない。

イ　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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、必要に応じて外部記録媒体にバックアップしなければならない。

エ　情報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、必要に応じて悪意の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。

⑦ 障害記録

統括情報セキュリティ責任者及び情報セキュリティ管理者は、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　統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないよう、ネットワークを設定しなければならない。

イ　統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適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

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

イ　情報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セキュリティ技術等を詳細に調査し、庁内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　情報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、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　統括情報セキュリティ責任者及び情報セキュリティ管理者は、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上で接続しなければならない。

⑪　複合機のセキュリティ管理

ア　統括情報セキュリティ責任者は、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て適切なセキュリティ要件を策定しなければならない。

イ　統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消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

統括情報セキュリティ責任者は、ＩＰ告知放送システム、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　情報セキュリティ管理者は、無線ＬＡＮを利用するときは、統括情報セキュリティ責任者の許可を得なければならない。

イ　統括情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合、情報の破壊、盗聴、改ざん、消去等が生じないよう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付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　統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

イ　統括情報セキュリティ責任者は、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　統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上

限を超える電子メールの送受信を不可能にしなければならない。

エ　統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑮　電子メールの利用制限

ア　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。

イ　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。

ウ　職員等は、複数人に電子メールを送信する場合は、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

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

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

⑯　電子署名・暗号化

ア　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、最高情報セキュリティ責任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　職員等は、暗号化を行う場合に最高情報セキュリティ責任者が定める以外の方法を用いてはならない。また、最高情報セキュリティ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。

ウ　最高情報セキュリティ責任者は、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。

⑰　無許可ソフトウェアの導入等の禁止

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

イ　職員等は、業務上必要がある場合に限り、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ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　職員等は、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　情報セキュリティ管理者は、所管する課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

職員等は、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、業務上必要がある場合は、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得て、これを行うことができる。

⑲　無許可でのインターネット接続の禁止

職員等は、統括情報セキュリティ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　職員等は、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サイトを閲覧してはならない。

イ　統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係ないサイトを閲覧していることを発見した場合は、情報セキュリティ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

統括情報セキュリティ責任者又は情報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権限のない職員等がアクセスできないように、システム上制限しなければならない。

イ 利用者ＩＤ等の取扱い

(ｱ) 統括情報セキュリティ責任者又は情報セキュリティ管理者は、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、職員等の異動、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。

(ｲ) 職員等は、業務上必要がなくなった場合、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情報セキュリティ管理者に報告しなければならない。

(ｳ) 統括情報セキュリティ責任者又は情報セキュリティ管理者は、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

(ｱ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、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。

(ｲ) 統括情報セキュリティ責任者又は情報セキュリティ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、統括情報セキュリティ責任者若しくは情報セキュリティ管理者が認めた者でなければならない。

(ｳ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、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。

(ｴ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤ等について、職員等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。

(ｵ) 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与されたＩＤを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

ア 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者の許可を得なければならない。

イ 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、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 統括情報セキュリティ責任者は、外部からのアクセスを認める場合、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 統括情報セキュリティ責任者は、外部からのアクセスを認める場合、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 統括情報セキュリティ責任者及び当該情報システムを所管する情報セキュリティ管理者は、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 職員等は、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　統括情報セキュリティ責任者は、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（ＩＣ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など、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

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク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

情報セキュリティ管理者は、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等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　統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、職員等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。また、パスワード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。

イ　統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

⑥　特権による接続時間の制限

統括情報セキュリティ責任者又は情報システムを所管する情報セキュリティ管理者は、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　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報システム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。

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情報セキュリティ管理者は、情報システムの開発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責任者、作業者のＩＤの管理

(ｱ) 情報システムを所管する情報セキュリティ管理者は、情報システムの開発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) 情報システムを所管する情報セキュリティ管理者は、情報システムの開発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

(ｱ) 情報システムを所管する情報セキュリティ管理者は、情報システムの開発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。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、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

(ｱ) 情報システムを所管する情報セキュリティ管理者は、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。

(ｲ) 情報システムを所管する情報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。

(ｳ) 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

(ｱ) 情報システムを所管する情報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、既に稼動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) 情報システムを所管する情報セキュリティ管理者は､運用テストを行う場合、あらかじめ擬似環境による動作確認を行わなければならない。

(ｳ) 開発したシステムについて受入れテストを行う場合、システムを所管する部署及び防災情報係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情報セキュリティ管理者は、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情報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。

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情報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情報セキュリティ管理者は、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は、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情報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情報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。

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情報セキュリティ管理者は、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・統合時の検証等

情報セキュリティ管理者は、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　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

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、必要に応じ職員等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に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　情報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情報セキュリティ管理者は、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　外部記録媒体を利用する場合、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。

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。

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　統括情報セキュリティ責任者が提供するコンピュータウイルス等の不正プログラム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　統括情報セキュリティ責任者の措置事項
統括情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。
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　統括情報セキュリティ責任者は、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　攻撃の予告
最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、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
最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、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
統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、職員等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　職員等による不正アクセス
統括情報セキュリティ責任者及び情報セキュリティ管理者は、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等の情報セキュリティ管理者に通知し、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
統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスでき

る情報システムに対して、第三者から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

統括情報セキュリティ責任者及び情報システム管理者は、情報システム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、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

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じて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

統括情報セキュリティ責任者は､不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員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

統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じて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。

9　運用

(1) 情報システムの監視

①　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、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。

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

(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　情報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、速やかに最高情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。

イ　最高情報セキュリティ責任者は、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　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、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

最高情報セキュリティ責任者及び最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等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 職員等の報告義務

ア 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、直ちに統括情報セキュリティ責任者及び情報セキュリティ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と統括情報セキュリティ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

厚岸町情報化推進委員会又は最高情報セキュリティ責任者は、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。

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、次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、厚岸町情報化推進委員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

厚岸町情報化推進委員会又は最高情報セキュリティ責任者は、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て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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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して、事業者を選定するよう努めるものとする。

エ　情報セキュリティ管理者は、クラウドサービスを利用する場合には、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

情報セキュリティ管理者は、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、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

情報セキュリティ管理者は、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措置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　情報セキュリティ管理者は、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など、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（ICカード等）を適切に管理するなどの方法で、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

情報セキュリティ管理者は、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、最高情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

② 緊急時の例外措置

情報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、事後速やかに最高情報セキュリティ責任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

最高情報セキュリティ責任者は、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

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 厚岸町個人情報保護条例（平成17年条例第12号）

(8) 違反に対する対応

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 統括情報セキュリティ責任者が違反を確認した場合は、当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
② 情報システムを所管する情報セキュリティ管理者が違反を確認した場合は、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
③ 情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知しなければならない。

10 評価・見直し

(1) 監査

① 実施方法

最高情報セキュリティ責任者は、情報セキュリティ監査統括責任者を指名し、情報セキュリティ対策状況について、定期的又は必要に応じて監査を行わせなければならない。

② 監査を行う者の要件

ア 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

イ 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

ア　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、最高情報セキュリティ責任者の承認を得なければならない。

イ　被監査部門は、監査の実施に協力しなければならない。

④　外部委託事業者に対する監査

情報セキュリティ管理者は、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には、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、定期的又は必要に応じて監査を実施しなければならない。

⑤　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、最高情報セキュリティ責任者に報告する。

また、必要に応じて厚岸町情報化推進委員会に報告するものとする。

⑥　保管

情報セキュリティ監査統括責任者は、監査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。

⑦　監査結果への対応

最高情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

⑧　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

厚岸町情報化推進委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、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　統括情報セキュリティ責任者及び情報セキュリティ管理者は、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、定期的又は必要に応じて自己点検を実施しなければならない。

イ　統括情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する課等における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的又は必要に応じて自己点検を行わなければならない。

②　報告

統括情報セキュリティ責任者及び情報セキュリティ管理者は、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､最高情報セキュリティ責任者に報告する。

また、必要に応じて厚岸町情報化推進委員会に報告するものとする。

③　自己点検結果の活用

ア　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。

イ　厚岸町情報化推進委員会は、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の見直し及び改定

厚岸町情報化推進委員会は、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踏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。ただし、緊急を要する場合又は軽微な改定については、最高情報セキュリティ責任者の判断で改定を行い、事後速やかに厚岸町情報化推進委員会に通知するものとする。