大木町情報セキュリティポリシー

平成 15 年８月　策定
平成 30 年２月　全部改定

内容

序　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とは、組織内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、大木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（以下、「職員等」という。）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。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、第１章　情報セキュリティ基本方針及び第２章　情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として第３章　情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
	情報セキュリティ実施手順	ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第１章　情報セキュリティ基本方針

1.　目的

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

大木町は町民の個人情報や行政運営上重要な情報などの重要な情報を多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、町民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、大木町には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

そのため、大木町の情報資産の機密性、完全性及び可用性を維持するための対策(情報セキュリティ対策)を整備するために大木町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については大木町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

2.　定義

（１）ネットワーク

大木町の執行機関、大木町の議会若しくはこれらに置かれる機関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）及び記録媒体で構成され、処理を行う仕組みをいう。

（２）情報システム

業務系の電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（３）情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

（４）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（５）情報セキュリティポリシー

本基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順をいう。

（６）機密性

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

（７）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（８）可用性

情報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、情報にアクセスできる状態を確保することをいう。

第２章　情報セキュリティ対策基準

3.1.　対象範囲

（１）行政機関の範囲

本対策基準が適用される機関は、大木町の執行機関、大木町の議会若しくはこれらに置かれる機関とする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

3.2.　組織体制

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

①副町長を、CISO とする。CISO は、本町における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

（２）　統括情報セキュリティ責任者

①情報処理主管課長を、CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は CISO を補佐しなければならない。

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

③統括情報セキュリティ責任者は、本町の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。

④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、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、本町の情報資産に対するセキュリティ侵

害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

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

⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム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。

⑧統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。

（３）情報セキュリティ管理者

①各課長を、情報セキュリティ管理者とする。

②情報セキュリティ管理者は所管す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は、所管する課等において、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 CISO へ速やかに報告を行い、指示を仰がなければならない。

（４）情報システム管理者

①各課長を、所管する情報システムに関する情報システム管理者とする。

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

③情報システム管理者は、所管する情報システムに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。

④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（５）情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。

（６）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。

（7）情報セキュリティに関する統一的な窓口の設置
①CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて各課長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。
②CISO 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。
④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、外部の事業者等との情報共有を行う。

3.3. 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、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 ※各課フォルダに格納されている情報資産	・支給以外の端末での作業の禁止 ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パス

機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 ※共有フォルダに格納されている情報資産	ワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・電磁的記録媒体の施錠可能な場所への保管
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産 ※各課フォルダ・共有フォルダに格納されている情報資産	・バックアップ、電子署名付与 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害され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	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管

	それがある情報資産 ※各課フォルダ・共有フォルダに格納されている情報資産	
可用性1	可用性2の情報資産以外の情報資産	

（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

（ア）職員等は、業務上必要のない情報を作成してはならない。

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

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

③情報資産の入手

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

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

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

④情報資産の利用

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

（イ）情報資産を利用する者は、情報資産の分類に応じ、適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、電磁的記録媒体に情報資産の分類が異なる

情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑤情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適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又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書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又は情報システム管理者は、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、自然災害を被る可能性が低い場所に保管しなければならない。

（エ）情報セキュリティ管理者又は情報システム管理者は、機密性２、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑥情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑦情報資産の運搬

（ア）車両等により機密性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の設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）機密性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に許可を得なければならない。

⑧情報資産の提供・公表

（ア）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。

（イ）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に許可を得なければならない。

（ウ）情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑨情報資産の廃棄

（ア）機密性２以上の情報資産を廃棄する者は、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、電磁的記録媒体の初期化等、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）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。

（ウ）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。

3.4. 物理的セキュリティ

3.4.1. サーバ等の管理

（１）機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、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

①情報システム管理者は、重要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、同一データを保持しなければならない。

②情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

（３）機器の電源

①情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適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。

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

（４）通信ケーブル等の配線

①統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。
②統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。
③統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。
④統括情報セキュリティ責任者、情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

（５）機器の定期保守及び修理
①情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。
②情報システム管理者は、電磁的記録媒体を内蔵する機器を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。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

（６）庁外への機器の設置
統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７）機器の廃棄等
情報システム管理者は、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。

3.4.2.　管理区域（電算室）の管理
（１）管理区域の構造等
①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、

当該機器等の管理並びに運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ責任者及び情報システム管理者は、管理区域を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な対策を講じなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、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。

⑤統括情報セキュリティ責任者及び情報システム管理者は、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

①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載による入退室管理を行わなければならない。

②職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

①情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託した業者に確認を行わせなければならない。

②情報システム管理者は、電算室の機器等の搬入出について、職員等を立ち会わせなければならない。

3.4.3.　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、 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。

③統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

④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、送受信される情報の暗号化を行わなければならない。

⑤統括情報セキュリティ責任者は、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統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

3.4.4.　職員等のパソコン等の管理

①情報システム管理者は、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。

③情報システム管理者は、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。端末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。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

3.5.　人的セキュリティ

3.5.1.　職員等の遵守事項

（１）職員等の遵守事項

①情報セキュリティポリシー等の遵守

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

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア）職員等は、本町のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

（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、私物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、安全管理措置（第３章　情報セキュリティ実施手順　3.利用者の責務（３））を遵守しなければならない。また、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア）　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

（イ）職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置（第３章　情報セキュリティ実施手順　3.利用者の責務（３））を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

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

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は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、適切な措置を講じなければならない。

⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（２）非常勤及び臨時職員への対応

①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、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、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書への署名を求めるものとする。

③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やモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（３）情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（４）外部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・保守等を外部委託事業者に発注する場合、外部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外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

3.5.2.　研修・訓練

（１）情報セキュリティに関する研修・訓練

CISO は、必要に応じて、情報セキュリティに関する研修・訓練を実施しなければならない。

（２）研修計画の策定及び実施

①CISO は、必要に応じて、幹部を含め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の策定とその実施体制の構築を実施しなければならない。

②新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③研修は、統括情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当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。

（３）緊急時対応訓練

CISO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。

（４）研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

3.5.3.　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

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

③情報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、必要に応じてCISO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

①職員等は、本町が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

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

③情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じてCISOに報告しなければならない。

④CISO 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

①統括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を引き起こした部門の情報セキュリティ管理者、情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、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に報告しなければならない。

②CISO は、統括情報セキュリティ責任者から、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。

3.5.4.　ID及びパスワード等の管理

（１）ICカード等の取扱い

①職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。

（ア）認証に用いるICカード等を、職員等間で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、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、IC カード等を

切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２）IDの取扱い

職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

①自己が利用しているIDは、他人に利用させてはならない。

②共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

（３）パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

①パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④パスワードが流出したおそれがある場合には、情報セキュリティ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。

⑤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。

⑥複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑦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。

⑧パソコン等の端末にパスワードを記憶させてはならない。

⑨職員等間でパスワードを共有してはならない。

3.6. 技術的セキュリティ

3.6.1. 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

①情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

②情報システム管理者は、ファイルサーバを課等の単位で構成し、職員等が他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、設定しなければならない。

③情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか

取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（２）バックアップの実施

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、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関わらず、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。

（３）他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者の許可を得なければならない。

（４）システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた外部委託事業者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。

（５）情報システム仕様書等の管理

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、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、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

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、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、適切にログを管理しなければならない。

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

（７）障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員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

①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適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

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（１０）外部ネットワークとの接続制限等

①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

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

③情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償

責任を契約上担保しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、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。

⑤情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（１１） 複合機のセキュリティ管理

①統括情報セキュリティ責任者は、複合機を調達する場合、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。

②統括情報セキュリティ責任者は、複合機が備える機能について適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。

③統括情報セキュリティ責任者は、複合機の運用を終了する場合、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、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 及びネットワークの盗聴対策

①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、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（１４）電子メールのセキュリティ管理

①統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

②統括情報セキュリティ責任者は、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。
③統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
④統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。
⑤統括情報セキュリティ責任者は、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外部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、外部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。

（１５）電子メールの利用制限
①職員等は、自動転送機能を用いて、電子メールを転送してはならない。
②職員等は、業務上必要のない送信先に電子メールを送信してはならない。
③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
④職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。
⑤職員等は、ウェブで利用できるフリーメール等を使用してはならない。

（１６）電子署名・暗号化
①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、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
②CISO 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
①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、

ソフトウェアのライセンスを管理しなければならない。

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１８）機器構成の変更の制限

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

②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

（１９）無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末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閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

②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のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適切な措置を求めなければならない。

3.6.2.　アクセス制御

（1）アクセス制御

①アクセス制御等

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

②利用者 ID の取扱い

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

（イ）職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

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

③特権を付与されたIDの管理等

（ア）統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。

（イ）統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISOが認めた者でなければならない。

（ウ）CISOは、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知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システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

（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、特権を付与されたID及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

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

（２）職員等による外部からのアクセス等の制限

①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

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

③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネッ

トワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦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、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）自動識別の設定

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されるようシステムを設定しなければならない。【推奨事項】

（４）ログイン時の表示等

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

（５）パスワードに関する情報の管理

①統括情報セキュリティ責任者又は情報システム管理者は、職員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。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。

②統括情報セキュリティ責任者又は情報システム管理者は、職員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

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

3.6.3.　システム開発、導入、保守等

（１）情報システムの調達

①統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

①システム開発における責任者及び作業者の特定

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

②システム開発における責任者、作業者のＩＤの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、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。

（３）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は、システム開発、保守及び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。【推奨事項】

（イ）情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ）情報システム管理者は、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。

（エ）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。

②テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ）情報システム管理者は、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。

（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

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

（４）システム開発・保守に関連する資料等の整備・保管

①情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適切な方法で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

①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（６）情報システムの変更管理

情報システム管理者は、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

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

3.6.4. 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。

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

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

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

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

（2）情報システム管理者の措置事項

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

①情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに

常駐させなければならない。

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

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

④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、町が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

（３）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

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

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

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

⑤添付ファイルが付いた電子メールを送受信する場合は、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。

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

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

（ア）パソコン等の端末の場合

LAN ケーブルの即時取り外しを行わなければならない。

（イ）モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

（４）専門家の支援体制

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

3.6.5. 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、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

④重要な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。【推奨事項】

⑤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

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、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 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス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管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員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、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。

3.6.6.　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。

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

3.7. 運用

3.7.1. 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管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

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

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

3.7.2. 情報セキュリティポリシーの遵守状況の確認

（１）遵守状況の確認及び対処

①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 CISO 及び統括情報セキュリティ責任者に報告しなければならない。

②CISO 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。

③統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）職員等の報告義務

①職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、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。

②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。

3.7.3.　侵害時の対応等

（１）緊急時対応計画の策定

CISO は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先
②発生した事案に係る報告すべき事項
③発生した事案への対応措置
④再発防止措置の策定

（３）業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、CISO 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。

3.7.4.　例外措置

（１）例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、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

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、

事後速やかにCISOに報告しなければならない。

3.7.5.　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(昭和二十五年十二月十三日法律第二百六十一号)
②著作権法（昭和四十五年五月六日法律第四十八号）
③不正アクセス行為の禁止等に関する法律（平成十一年八月十三日法律第百二十八号）
④個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）
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（平成二十五年五月三十一日法律第二十七号）
⑥大木町個人情報保護条例（平成二十七年九月十日法律第十四号）

3.7.6.　懲戒処分等

（１）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。

（２）違反時の対応

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

①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員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情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者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CISO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。

3.8.　外部サービスの利用

3.8.1.　外部委託

（１）外部委託事業者の選定基準

①情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②情報セキュリティ管理者は、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。

③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。

・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
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・町による監査、検査
・町による情報セキュリティインシデント発生時の公表
・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

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、（２）の契約に

基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

3.8.2.　約款による外部サービスの利用

（１）約款による外部サービスの利用に係る規定の整備

①情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報が取扱われないように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲

（イ）業務により利用する約款による外部サービス

（ウ）利用手続及び運用手順

（２）約款による外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

3.8.3.　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、本町が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア）本町のアカウントによる情報発信が、実際の本町のものであることを明らかにするために、本町の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

（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）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。

3.9. 評価・見直し

3.9.1. 監査

（１）実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

（２）監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（３）監査実施計画の立案及び実施への協力

①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、CISO の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（４）外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（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、CISO に報告する。

（６）保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（７）監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、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程等の見直し等への活用

CISO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。

3.9.2.　自己点検

（１）実施方法

①統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

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

（２）報告

統括情報セキュリティ責任者及び情報システム管理者は、自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、CISO に報告しなければならない。

（３）自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②CISO は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3.9.3.　情報セキュリティポリシー及び関係規程等の見直し

CISO 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ふまえ、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。

第３章　情報セキュリティ実施手順

1.　目的

この実施手順は、「大木町情報セキュリティポリシー」に基づき、大木町（出先機関を含む）のネットワーク及び情報システム（以下「大木町情報資産」という。）の適正かつ効率的な整備及び管理運営を行うことと共に情報セキュリティの確保及びその向上を図ることを目的とする。

2.　適用対象者

利用者の具体的な区分は以下のとおりとする。

（１）セキュリティ責任者

情報処理主管課長

（２）システム管理者

情報処理主管課長及び情報システム担当職員

（３）利用者

上記（１）以外の職員（非常勤及び臨時職員を含む）

（４）システム事業者

大木町情報資産の保守委託業者

3.　利用者の責務

利用者は、大木町情報資産を利用する場合に、大木町情報セキュリティポリシーに定められた事項を遵守するほか、次に掲げる事項を遵守すること。

（１）大木町情報資産を利用して以下の行為を行うことを禁止する。

①利用者の所属する組織の業務以外を目的とした利用
②第三者を誹謗中傷する行為
③著作権等の法令に定める権利の侵害
④他者のプログラムやデータ等を改変し、又は破壊する行為
⑤自己の営利を目的とした行為
⑥サーバ、通信回線等のネットワーク資源を不当に占有又は浪費する行為
⑦大木町情報資産の運営に支障を及ぼすような行為
⑧他人を詐称するような行為
⑨その他、法令又は社会慣行に反する行為

（２）本町から付与された主体認証情報（IC カード付き職員証）の管理は、次に掲げる事項を遵守すること。

①自己に交付されたＩＣカード以外は利用しないこと。

②IC カードを第三者に譲渡又は貸与しないこと。

③IC カードを第三者に使用されるような状態で放置しないこと。

④IC カードを紛失しないこと。また、万が一紛失した場合は、セキュリティ管理者に紛失理由を添えて報告すること。

⑤IC カードが不要になった場合は、セキュリティ管理者に速やかに返却すること。

（３）大木町情報資産の不正アクセス・不正プログラム対策のため、次に掲げる事項を遵守すること。

①PC 等について情報及び資産が不正プログラムに感染しないよう十分な注意を払うこと。

②PC 等にメーカサポートの切れた OS は使用しないこと。また、可能な限り新しいバージョンの OS やアプリケーションソフトウェアを導入するとともに、自動更新等の機能により、常に最新の修正プログラムを入手し、適用すること。

③OS やブラウザ等のアプリケーションソフトウェアのセキュリティ機能を活用し、セキュリティレベルを適切に設定すること。

④PC 等にはウイルス対策ソフトウェアを導入し、常に最新のウイルス定義ファイルに更新すること。

⑤ウイルス対策ソフトウェア等により定期的に全ての電子ファイルに対して、不正プログラムの有無を確認すること。

⑥外部からデータやソフトウェアを PC 等に取り込む場合、又は外部にデータやソフトウェアを提供する場合は、ウイルス対策ソフトウェアにより感染の有無を確認すること。また、ウイルス対策ソフトウェアにより不正プログラムとして検知された実行ファイルの実行、データファイルのアプリケーションソフトウェア等による読み込みを行わないこと。

⑦電子メールの利用に当たっては、以下の点に注意すること。

不用意にメールアカウントを外部に公開しないこと。

メール受信において、件名や内容が不審な場合、既知の差出人であっても不用意に開封せずに削除すること。

⑧離席時には、PC 等のパスワードによるロック等により、第三者による不正操作から保護すること。

4. 情報の管理

（１）ウイルス等の被害に備えるため情報についてのバックアップの必要性の有無を検討し、必要があると認めたときは、そのバックアップを取得し適切に保管すること。

（２）情報が記録されたPC等を廃棄する場合にその内容が復元できないようにする。また、不要になった情報はPC等から速やかに消去する等、情報は適切に管理すること。

（３）本町が、障害や不正アクセス、大木町情報資産の不正利用等が発生した場合の原因究明等に用いるため必要に応じて行う、各種利用ログの取得について、利用者の所属組織への開示に同意すること。

（４）利用者区分による責務

利用者のうち、以下の区分に該当する者は、前項（１）から（３）に定められた事項と併せてそれぞれの責務を遵守すること。

①利用者

（ア）閲覧が規制されているインターネットサイトについて、業務上閲覧必要がある場合は、システム管理者に申請すること。
ただし、Web サイトが誤って閲覧規制の対象となっていると想定される場合は、電子メールによりシステム管理者に確認を依頼すること。

（イ）PC 等の管理は、利用者が責任を持って行い、不正アクセス・不正プログラム対策のため、次に掲げる事項を遵守すること。
PC等のパスワードは､大木町情報資産のパスワードと同様に厳重に管理すること。

②セキュリティ責任者

（ア）利用者がパスワードを忘失した場合は、利用者の所属を確認のうえ、速やかに再発行の申請を行うこと。

（イ）自機関の利用者に対し、情報セキュリティ対策に関する注意喚起等の周知、対策状況の確認等を実施すること。

③システム管理者

（ア）システム管理者としての権限は、セキュリティ責任者の指示に基づき

大木町情報資産の運用管理に限定して使用すること。

（イ）大木町情報資産に係る権限管理を適切に行い、管理者権限の付与は、必要最小限の者に限定すること。

各システムのアクセス制御情報を設定または変更する際は、セキュリティ責任者の承認を得ること。

（ウ）システム管理者は、管理する利用者について、以下の事項を遵守すること。

システム管理者が主体認証のために取得した利用者情報については本人から事前に同意を得た目的以外に使用しないこと。

利用者のパスワード奪取等の危険が発生したことを知った時には、直ちに大木町情報資産の使用を停止する等、必要な措置を講じる。

（エ）システムの管理については以下の事項を遵守すること。

(a) 要保護情報を取り扱う情報機器の設置及び管理

要保護情報を取り扱う情報機器を設置する場合は、外部から容易に侵入できない区域（電算室等）に設置すること。

移動可能な機器は、盗難防止策を行うこと。

(b) 情報機器等の搬出入

要保護情報が収録された電子計算機（記録媒体含む）を搬出入する場合は、あらかじめ当該電子計算機について安全性を確認してから行うこと。

業者が電子計算機等を搬出入する場合、必ず職員等が立ち会う等の措置を講じるとともに、搬出入記録を保存すること。

(c) 電子計算機等の取り付け及び接続

電子計算機等の取り付けを行う場合は、火、水、埃、振動等の影響を可能な限り排除した場所に設置し、必要に応じ容易に取り外せないよう固定等の適切な措置を講じること。

管理者以外の者が電子計算機等を容易に操作できないよう、主体認証情報の設定等の措置を講じること。

長期間利用しない機器は、ネットワークに接続しないこと。

(d) 電源

電子計算機の電源については、必要に応じて、当該電子計算機を適切に停止するまでの間に十分な電力が供給できる容量の予備電源（UPS）を備え付けること。

必要に応じて落雷等による過電流から、電子計算機を保護するための措置を講じること。

(e) 配線

配線は、傍受又は損傷等を受けることがないように可能な限り必要な措置を講じること。

主要な箇所の配線については、安定かつ円滑な運用を図るため、定期的に点検を行うこと。

基幹的な通信回線装置に接続する電子計算機は、配線の変更、追加等が容易にできないような措置を講じること。

(f) 記録媒体の管理

取り外しが可能な記録媒体については、盗難等を避けるための管理措置を講じること。

(g) システムの調達

情報システムの調達にあたっては、調達仕様書にシステム導入前の検査要求事項、守秘義務等の情報セキュリティ確保の規定を必ず盛り込むこと。また、業務遂行の必要に応じて資格証明等の提出を盛り込むこと。

開発・保守を外部の事業者に委託する場合は、委託先事業者（下請けを行う事業者も含む。）に対して、セキュリティポリシーのうち委託先事業者が遵守すべき事項を調達仕様書等に明記するとともに、誓約書等の提出を求めるなどの措置を講じた上で、契約を行うこと。

契約書にセキュリティポリシーの遵守に関する事項を規定すること。

応用ソフトウェアの開発、変更及び運用についての手順等を定めること。

電子計算機及びソフトウェアを購入等する場合、当該製品が情報セキュリティ上問題にならないかを確認すること。

電子計算機及びソフトウェアの導入、保守および撤去についての手順を定めること。

(h) システムの変更処理

重要なシステム設定等を追加、変更、廃棄した場合は、その際の設定、構成等の履歴を記録し、厳重に管理すること。

(i) システムの開発 システム開発及び保守時の事故・不正行為対策のため、次の事項を定めること。

責任者及び監督者を置くこと。

作業者及び作業範囲を明確にすること。

システム開発及び保守等の事故・不正行為に係るリスク分析を行うこと。

開発・保守するシステムは、可能な限り運用システムと切り離すこと。
開発・保守に際しては、可能な限りソースコードの提出を求めること。
開発・保守に際しては、セキュリティ上問題となるおそれのあるソフトウェアは使用しないこと。
開発・保守に際しては、完成したWebアプリケーションソフトウェア等に既知の脆弱性が生じないよう、機器の設定及びシステムの設計に必要な対策を取り入れることを開発業者に求めること。
開発・保守の際のアクセス制御を明確にすること。
機器の搬出入はシステム管理者が立ち会い、その内容を確認すること。
開発・保守記録の提出を義務づけること。
マニュアル等は、定められた場所に保管すること。
開発・保守を行った者の主体認証情報を当該開発・保守終了後速やかに抹消すること。

(j) システムの導入

新たに情報システムを導入する場合は、原則として既に稼働しているシステムに接続する前に十分な試験を行う。ただし、導入前に十分な試験を行うことが困難な場合はリスク分析を行い、その結果を踏まえ対処方針を決定すること。
試験に使用したデータ及びその結果は厳重に保管すること。

(k) システムの保守及び更新

ソフトウェア（独自開発ソフトウェア、汎用ソフトウェア）を更新、又は一部修正プログラムを組み込む場合は、不具合、他のシステムとの相性等の確認を行うこと。
情報セキュリティに重大な影響を及ぼす不具合に対処した修正プログラムについては、速やかに組込むこと。また、更新することによって、従来に増して強固なセキュリティ対策ができる場合は、速やかに導入すること。
ソフトウェアの脆弱性対応に関する管理台帳を整備すること。

(l) 情報機器の修理及び廃棄等

情報が記録された機器を外部の事業者に修理させる場合は、前項に準じた調達仕様書を作成し、契約を行うこと。
情報が記録された機器を廃棄する場合は、その内容が復元できないようにすること。ただし、委託先事業者（リース返却先事業者、

交換契約による下取り処分先事業者を含む。）に委託する場合は、記録された情報が復元できない方法を用いて削除することを調達仕様書等に明記するとともに、その方法等を審査し、契約を行うこと。

(m) システム関連ファイルの記録

システム関連のファイルは、利用者がアクセスできないように管理すること。

（オ）システム運用については、以下の事項を遵守すること。

(a) ログ管理

障害や不正アクセス、大木町情報資産の不正利用等が発生した場合の原因究明等に用いるため、必要なログを取得し、管理すること。

取得したログは、定期的に利用頻度、サービス毎、時間毎等の分析をすること。

ログ及びバックアップされた媒体は、改竄、破壊等から保護すること。

取得したログは定期的にバックアップ媒体に記録するとともに、最低３か月間保存すること。

(b) ネットワークの監視

不正侵入検知システムを導入すること。

コンピュータウイルスの感染及び拡散を最小限に押さえるため、メールサーバ及び Web アクセスの通信経路にウイルス対策システムを導入し、常時監視、または定期検査を行うこと。

不正プログラム定義ファイルは常に最新のものに保つこと。

5. システム事業者の責務

5.1. システム管理

（１）システムの変更等処理

重要なシステム設定等を追加、変更、破棄等した場合は、その際の設定、構成等を記録し、厳重に管理すること。

（２） システムの開発

大木町情報資産の開発及び保守時における事故・不正行為対策等のため、次に定める事項を実施すること。

①責任者及び監督者を置くこと。

②作業者及び作業範囲を明確にすること（時間、場所等）。

③システム開発及び保守等の事故・不正行為に係るリスク分析を行うこと。
④開発・保守するシステムは、可能な限り運用システムとは切り離すこと。
⑤開発・保守に際しては、可能な限りソースコードを大木町に提出すること。
⑥開発・保守に際しては、セキュリティ上問題となりうるおそれのあるソフトウェアは使用しないこと。
⑦開発・保守の際のアクセス制御を明確にすること。
⑧機器の搬出入はシステム管理者の立ち会い、内容確認の下で実施すること。
⑨開発・保守記録を大木町に提出すること。
⑩開発・保守を行った者の主体認証情報等は当該開発・保守終了後速やかに抹消すること。

（３） システムの導入

新たな情報システムを導入する場合は、原則として既に稼働しているシステムに接続する前に十分な試験を行うこと。ただし、導入前に十分な試験を行うことが困難な場合はリスク分析を行い、その結果を踏まえ対処方針を決定すること。

試験に使用したデータ及びその結果を厳重に保管すること。

（４） ソフトウェアの保守及び更新

ソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）を更新する場合又は一部修正のプログラムを導入する場合は、あらかじめ他の情報システムと不具合等が発生しないか確認を行うこと。

情報セキュリティに重大な影響を及ぼす不具合が生じた場合は、当該不具合に対処した修正プログラムを速やかに導入すること。また、更新することによって、従来に増して強固なセキュリティ対策ができる場合は、早期かつ計画的に更新すること。

ソフトウェアの導入に当たっては、販売者又は配付責任者の連絡先及び更新情報が明確なものを導入すること。

ソフトウェアの脆弱性対応に関する管理台帳を整備すること。

（５）システムの廃棄

情報が記録された情報及び資産を廃棄する場合は、その内容を復元できない方法で行うこと。

5.2.　運用管理

①保守を行う要員の業務範囲及び責任範囲を明確にすること。

②システム管理者との連絡体制を確立すること。なお、保守対象時間外であっても緊急時には、連絡の取れる体制とすること。

③ネットワーク構成等の重要な情報は、公開しないこと。

④利用者の情報は、厳重に管理すること。

⑤業務上知り得た情報のうち、システム管理者が情報の格付けに従い外部への公表を禁じたものについては、外部に漏らさないこと。

6.　障害・事故等への対応

（１）2.の対象に該当する者は、障害・事故等が発生並びに発生するおそれがある場合には、所属組織の定めた対処手順により、その影響が拡大することを防ぐとともに復旧を適切に実施すること。

（２）2.の対象に該当する者は、発生した障害・事故等が大木町情報資産に原因があり、大木町情報資産に影響を与える可能性があると判断した場合、あるいは大木町情報資産側で対処が必要と判断した場合は、速やかにシステム管理者に報告すること。

（３）システム管理者は、以下の事項に対処すること。

①障害・事故等への対処の訓練を行う等、緊急時に備えること。

②必要に応じて、情報セキュリティ検査を実施すること。なお、検査はなるべく外部事業者に委託すること。

③関係機器のアクセス記録及び内容並びに経過について整理し保存しておくこと。また、再発防止の措置を検討し速やかに対策を講じること。

④障害発生及び情報セキュリティが侵害された可能性のある事案を発見した際等の緊急時には、必要に応じ一時的に大木町情報資産の停止措置を講じること。

（４）システム事業者は、以下の事項に対処すること。

情報システムに障害等を発見した場合は、直ちにシステム管理者に連絡するとともに、速やかに原因の究明に努めるものとする。

事案に係る関係機器のアクセス記録及び事案内容並びに経過について整理し、保存しておくこと。また、事案に係る再発防止の措置を検討し、速やかに対策を講じること。

7. 教育

（１）2.の対象に該当する者は、情報セキュリティ対策に関する講習会を積極的に受講し、情報セキュリティ上の問題が生じないように努めること。

（２）システム管理者は、大木町情報資産に係る利用者及びシステム関係事業者に対し、情報セキュリティ対策に関する啓発を実施すること。

8. 違反者への措置

セキュリティ責任者は、システム管理者、利用者、システム事業者が、それぞれの守るべき事項に違反した場合、発生した事柄の状況に応じて本実施手順に基づき、大木町情報資産の利用の制限又は、利用の停止、管理者の交代、保守要員の交代等の措置を講ずることができる。

9. 評価・見直し

（１）2.の対象に該当する者は、この実施手順に課題及び問題点が認められる場合は、利用者はシステム管理者、また、それ以外の者にあっては所属組織を経由してシステム管理者に報告すること。

（２）システム管理者は、以下の場合は、本実施手順等の改善計画を作成し、セキュリティ責任者に提案すること。
障害発生等の事案のリスク分析を実施し、必要と認められた場合
利用者から課題及び問題点が認められる旨の報告を受けた場合

（３）セキュリティ責任者は、システム管理者からの提案により、実施手順の見直しを検討のうえ必要と判断した場合は、実施手順を改訂すること。