# 三股町電子情報保護指針

（情報セキュリティポリシー）

【更 新 日】平成25年6月25日
【　版　　】１．３１　版
【文書取扱】三股町総務課情報システム係

～ 目 次 ～

# 第1章　情報セキュリティ基本方針

## 1　目的

本基本方針は、三股町が保有する情報資産の機密性、完全性及び可用性を維持するため、三股町が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

## 2　定義

(1)　ネットワーク
コンピューター等の情報機器を相互に接続するための通信網、その構成機器（ソフトウェアを含む）をいう。

(2)　システム
コンピューター、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。

(3)　情報セキュリティ
情報資産の機密性、完全性及び可用性を維持することをいう。

(4)　情報セキュリティポリシー
本基本方針と情報セキュリティ対策基準をあわせたものをいう。

(5)　アクセス
記録された情報に対してシステムを利用することにより、閲覧・更新・複製の取得・削除のうちいずれかを行うことをいう。

(6)　情報
情報セキュリティポリシーにおいては、コンピューター等の電子情報機器および媒体（電子情報としてアクセスできるものに限る）に記録された電子情報をいう。

(7)　個人情報
情報のうち三股町個人情報保護条例により規定された種類の情報をいう。

(8)　情報資産
情報、システムおよびそれらの管理運用体制をあわせたものをいう。

(9)　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。

(10)　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。

(11)　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。

3　対象とする脅威と事象

情報資産に対する脅威として、以下の(1)～(4)の脅威を想定し、(5)の事象を防ぐため情報セキュリティ対策を実施する。

(1)　外部不正

- 部外者の侵入
- 不正アクセス
- ウイルス攻撃
- サービス不能攻撃

(2)　内部不正

- 情報資産の無断持ち出し
- 無許可ソフトウェアの使用等の規定違反

(3)　管理不全

- 設計・開発の不備
- プログラム上の欠陥
- メンテナンス不備
- 外部委託管理の不備
- 内部・外部監査機能の不備

(4)　事故災害

- 地震
- 落雷
- 火災
- 電力供給の途絶
- 通信の途絶
- 機器故障
- 操作・設定の誤り

(5)　結果の事象

- 情報の漏えい・破壊・改ざん・消去
- 重要情報の詐取
- 情報資産の破壊
- 行政サービス提供の停滞

## 4　適用範囲

### (1)　行政機関の範囲

情報セキュリティポリシーが適用される行政機関は、町長部局、教育委員会、各行政委員会、議会事務局及び地方公営企業とする。

### (2)　情報の範囲

情報セキュリティポリシーが対象とする情報は、次のとおりとする。

① 行政機関が管理する情報資産で取り扱う情報
② 行政機関が管理するシステムから個人情報を含む情報を紙媒体に印刷したもの
③ 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（これらを印刷した紙媒体を含む）

## 5　職員等の遵守義務

行政機関の職員、非常勤職員及び臨時職員（以下「職員等」という。）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の脅威から情報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。

### (1)　組織体制

三股町の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

### (2)　情報資産の分類と管理

三股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、当該分類に基づき情報セキュリティ対策を行う。

### (3)　物理的セキュリティ

サーバ、サーバルーム、電算室、通信回線及び職員使用のパソコン端末等の管理について、物理的な対策を講じる。

### (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を講じる。

### (5)　技術的セキュリティ

コンピューター等の管理、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を講じる。

### (6)　運用

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セキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

(7)　計画

情報資産への侵害が発生した際に迅速かつ適切に対応するため、緊急時対応計画を策定する。また、大規模災害や火災などにより情報資産に壊滅的な打撃を受けた場合を想定して、事業継続計画（BCP）を策定する。

7　情報セキュリティ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

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

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

セキュリティ責任者は、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ものとする。

なお、情報セキュリティ実施手順は、公にすることにより情報セキュリティや三股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。

# 第2章　情報セキュリティ対策基準

## 1　組織体制

### (1)　最高情報統括責任者（次項よりCIOと表記する）

① 副町長を最高情報統括責任者とする。最高情報統括責任者は、三股町における全ての情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

② 最高情報統括責任者は、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アドバイザーとして置くことができる。

### (2)　情報セキュリティ責任者（次項よりセキュリティ責任者と表記する）

① 情報システム担当課長を、CIO直属の情報セキュリティ責任者とする。情報セキュリティ責任者はCIOを補佐しなければならない。また、CIOが不在の場合には、CIOの代理を務めなければならない。

② 情報セキュリティ責任者は、三股町の全ての情報資産において次の権限及び責任を有する。

- 情報セキュリティを目的とした開発、設定の変更、運用・管理手法の見直し等を行うこと。
- 情報セキュリティ実施手順の策定・維持・管理を行うこと。
- 情報システム管理者及び担当者に対して、情報セキュリティに関する指導及び助言を行うこと。

③ 情報セキュリティ責任者は、三股町の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、CIO の指示に従い必要かつ十分な措置を行う権限及び責任を有する。

④ 情報セキュリティ責任者は、円滑な情報共有を図るため、CIO、情報セキュリティ責任者、情報システム管理者、担当者を網羅する連絡体制を整備しなければならない。

### (3)　情報システム管理者（次項よりシステム管理者と表記する）

① 町長部局の課長、教育委員会の担当課長、行政委員会事務局の長、地方公営企業の長、議会事務局長を情報システム管理者とする。

② 情報システム管理者は、その所管する部局等及び所管するシステムについて、次の権限及び責任を有する。

- 情報セキュリティポリシーの遵守に関して、職員等に教育・訓練・助言及び指示を行うこと。
- 情報セキュリティを目的とした設定の変更、運用・管理手法の見直し等を行うこと。
- 情報セキュリティ実施手順の実施を監督すること。
- 緊急時等における連絡体制を整備すること。
- 情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、セキュリティ責任者及びCIOへ速やかに報告を行い、指示を仰ぐこと。

(4)　情報システム担当者（次項より担当者と表記する）

① 情報システム担当者は、システム管理者が所管する部局等における職員等のうち、システムにアクセスする権限を付与された全ての職員等とする。

② 情報システム担当者は、次のことを行うにあたっては、システム管理者の指示等に従わなければならない。

- システムの運用、情報の更新等のシステム作業を行うこと。
- システムより個人情報を含む情報を取得し、個々の使用するパソコン等で二次的な加工を行うこと。

(5)　情報セキュリティ委員会（次項より委員会と表記する）

① 三股町電子計算組織運営委員会をもって情報セキュリティ委員会にあてる。

② 三股町の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、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。

③ 情報セキュリティ委員会は、年度毎に情報セキュリティ対策の実施状況を確認しなければならない。

④ 情報セキュリティ委員会は、必要に応じて三股町における情報セキュリティ対策の改善を図らなければなければならない。

(6)　兼務の禁止

① 情報セキュリティ対策の実施において、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。ただし、セキュリティ責任者がシステム管理者である場合など、やむを得ない場合を除く。

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。

## 2　情報資産の分類と管理方法

### 2-1 情報資産の分類

三股町における情報資産は、機密性、完全性及び可用性により、表2－1、表2－2及び表2－3のとおり分類し、必要に応じ取扱制限を行うものとする。なお、表示の通り上位の区分は下位の取扱い制限を内包するものとする。

〈〈表2－1〉〉

機密性による情報資産の分類

<table>
<tr><td colspan="2">分類レベル</td><td>機密性 1</td><td>機密性 2</td><td>機密性 3</td><td>機密性 4</td></tr>
<tr><td colspan="2">分 類 基 準</td><td>機密性2～4に相当しない情報資産</td><td>機密性3～4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もの</td><td>・機密性4には該当しないが、個人情報であるもの<br>・漏えい等により行政事務の安定的な遂行に著しく支障を及ぼすもの</td><td>・漏えい等により著しく個人の権利を侵害する恐れのある個人情報<br>・秘密文書に相当する機密性を要する情報資産</td></tr>
<tr><td rowspan="8">取扱制限</td><td>アクセス</td><td></td><td colspan="2">アクセス権限を部局で制限</td><td>アクセス権限を職位・部局で制限（少人数）</td></tr>
<tr><td>印刷・複製</td><td></td><td></td><td>本人への通知・交付等以外の印刷・複製の制限</td><td>必要以上の印刷・複製の禁止</td></tr>
<tr><td>交付・配布</td><td></td><td></td><td>印刷時に取扱を明記</td><td>原則として印刷・複製の配付禁止（回収）</td></tr>
<tr><td>紙媒体の保管</td><td></td><td></td><td>鍵付き倉庫・書庫への格納</td><td>鍵付きケースへの格納</td></tr>
<tr><td>記録媒体の保管</td><td></td><td></td><td colspan="2">施錠可能な場所への保管</td></tr>
<tr><td rowspan="2">ネットワーク送信</td><td></td><td></td><td>信頼のできる回線の選択</td><td>ネットワークを使った外部送信の禁止</td></tr>
<tr><td></td><td></td><td colspan="2">情報の送信、情報資産の運搬・提供時における暗号化</td></tr>
<tr><td>外部委託</td><td></td><td></td><td>安全管理措置の規定・明文化</td><td>庁外における情報処理の禁止</td></tr>
<tr><td>破棄</td><td></td><td colspan="3">復元不可能な処理を施しての廃棄</td></tr>
</table>

〈〈表2－2〉〉

完全性による情報資産の分類

| 分類レベル | | 完全性 1 | 完全性 2 |
|---|---|---|---|
| 分類基準 | | 完全性2に相当しない情報資産 | 改ざん、誤びゅう又は破損により<br>・住民の権利が侵害されるもの<br>・行政事務の安定的な遂行に支障を及ぼすもの（軽微なものを除く） |
| 取扱制限 | データバックアップ | | 高頻度に実施 |
| | 外部委託 | | 安全管理措置を規定 |
| | 記録媒体の保管 | | 施錠可能な場所への保管 |

〈〈表2－3〉〉

可用性による情報資産の分類

| 分類レベル | | 可用性 1 | 可用性 2 | 可用性 3 | 可用性 4 |
|---|---|---|---|---|---|
| 分類基準 | | 可用性2～4に相当しない情報資産 | 滅失、紛失又は利用不可能により<br>・住民の権利が侵害されるもの<br>・行政事務の安定的な遂行に支障を及ぼすもの | 滅失、紛失又は利用不可能により<br>・住民の生命・財産が侵害されるもの<br>・行政サービスの提供に重大な支障を及ぼすもの | 大規模自然災害時に利用することが想定され、利用不可能な状態が住民の生命に直結する重要なもの。 |
| 取扱制限 | システム障害への備え | | | | システムの二重化などによる災害耐性の確保 |
| | | | | 障害時の代替システムもしくは代替可能な運用方法の準備 | |
| | | | システム復旧時間を規定 | | |
| | 従来ネットワーク破損への備え | | | | 代替接続の準備確認 |
| | | | ネットワーク接続の状態を管理 | | |
| | 紙媒体の保管 | | | 必要に応じて印刷して利用を確保 | 印刷して利用を確保 |
| | 記録媒体の保管 | | | | 災害耐性の高い媒体・形式で保存 |
| | データバックアップ | | | 外部記録媒体の安全な場所への保管 | 災害時の緊急対応が可能な場所への保管 |
| | | | データバックアップを定期的に実施 | | |

2-2 情報資産の管理

(1) 責任

① システム管理者は、その所管する情報資産について管理責任を有する。ただし、ネットワーク機器等の全庁的な管理が行われているものを除く。

② 情報が複製された場合には、複製された情報についても同様に管理しなければならない。

(2) 情報資産の分類の表示

① 職員等は、情報資産について次のような情報資産の分類を表示するよう努めなければならない。

- ファイル名もしくはファイルの属性(プロパティ)
- ヘッダー・フッター等(印刷時)
- 格納する記録媒体(媒体のラベル等)

② 必要に応じて文書の隅・スタンプ表示などで取扱制限についても明示すること。

(3) 情報の作成

① 職員等は業務に必要のない情報を作成してはならない。

② 職員等は情報を作成するにあたって、つぎのことを遵守しなければならない。

- 2-1 の分類に基づき、当該情報の分類と取扱制限を定めること。
- 機密性4もしくは可用性4に該当することが明らかなもの、あるいは該当しないことが明らかでないものについては、システム管理者に判断を仰ぐこと。
- 作成途上の情報についても紛失や流出等を防止すること。
- 作成途上で不要になった場合は、当該情報を消去すること。

(4) 情報資産の入手

① 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。

② 庁外の者が作成した情報資産を入手した者は、つぎのことを遵守しなければならない。

- 2-1 の分類に基づき、当該情報の分類と取扱制限を定めること。
- 機密性4もしくは可用性4に該当することが明らかなもの、あるいは該当しないことが明らかでないものについては、システム管理者に判断を仰ぐこと。

(5) 情報資産の利用

① 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。

② 情報資産を利用する者は、つぎのことを遵守しなければならない。

- 情報資産の分類に応じ適切な取扱いをすること。
- 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は、最高度の分類に従って当該記録媒体を取り扱うこと。

(6) 所管外情報資産の利用

① システム管理者及び担当者は、機密性3以上の情報について、自身の所属する課室等

が所管する以外の情報にアクセスしてはならない。

② 上記①の禁止事項については、業務遂行上の効率性および必要性に基づき、例外措置として行うことができる。

③ 上記②の実施にあたって、システム結合やシステム参照により定常的に行う場合には、情報を所管するシステム管理者、情報を利用するシステム管理者、セキュリティ責任者の3者による協議書を3通作成し、それぞれが1通づつ保管する。協議書の管理については例外処置申請書に習って取り扱うものとする。

④ 上記②の実施にあたって、一時的にデータを取得して情報処理に利用する場合には、情報を所管するシステム管理者に対し、情報を利用するシステム管理者が申請書をもって申請を行い、許可を得なければなければならない。

⑤ 上記④の場合において、申請書は実際にデータを取得し処理を行った担当者が所属する課室等のシステム管理者が、例外処置申請書に倣って管理するものとする

(7) 情報資産の保管

① 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。

② システム管理者は、情報資産の保管にあたって、つぎのことを遵守しなければならない。

- 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ること。

③ セキュリティ責任者は、情報資産の保管にあたって、つぎのことを遵守しなければならない。

- 可用性3以上の情報を保存した外部記録媒体をバックアップ目的で長期保管する場合は、三股町から物理的距離が離れており、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。

(8) 情報の送信

① 電子メール等により機密性2の情報を送信する場合は、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。

② ネットワークを利用して機密性3の情報を送信する場合は、送信相手を特定したうえで第三者が介在できない手段を選ばなければならない。また、可能である限り暗号化を行わなければならない。

(9) 情報資産の運搬

① 機密性3以上の情報資産を運搬する者は、システム管理者に許可を得なければならない。

② 車両等により機密性3以上の情報資産を運搬する場合は、つぎのことを遵守しなければならない。

- 鍵付きのケース等に格納して運搬すること。
- 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こと。
- 情報量などの必要性に応じて複数名で運搬すること。

③ 車両等により機密性4の情報資産を運搬する場合は、つぎのことを遵守しなければならない。

- 必ず複数名で運搬すること。

(10) 情報資産の提供・公表

① 機密性3の情報資産を外部に提供する場合は、セキュリティ責任者に許可を得なければならない。ただし、個人情報を提供する場合は、三股町個人情報保護条例の定めによらなければならない。

② 機密性4の情報資産を外部に提供する場合は、CIO に許可を得なければならない。ただし、個人情報を提供する場合は、三股町個人情報保護条例の定めによらなければならない。

③ システム管理者は、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。

(11) 情報資産の廃棄

① 機密性2もしくは可用性2に該当する情報資産を廃棄する場合は、システム管理者の許可を得なければならない。

② 機密性3以上もしくは可用性3以上の情報資産を廃棄する場合は、CIO の許可を得なければならない。

③ 機密性3以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、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。

④ 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。

⑤ 廃棄を業務委託する場合は、上記②が実施されたことを保証する文書・写真等を取得しなければならない。

## 3　物理的セキュリティ

### 3-1 サーバ等の管理

(1)　機器の取付け

① サーバ等の情報を集約して処理する機器は、セキュリティ責任者の指定する専用の場所に取り付けることとし、庁内各部署への設置を行ってはならない。ただし、以下の場合を除くものとする。

- 情報システムの構築・更新にともなう作業場所を確保するため、一時的に簡易的な設置を行う場合。
- 機密性2以下かつ可用性1である情報資産に該当するサーバ機器等で簡易なもの。
- 庁外で行う業務を主目的として構築されたサーバ機器等で、相応のセキュリティ対策が講じられたもの。
- 法律等で設置場所に定めがあるもの。

② セキュリティ責任者は、サーバ等の機器を取付ける場所について、次のことに配慮しなければならない。

- 地震、風水害などの自然災害に対して十分に備えること。
- 火災、水漏れなどの事故を未然に防ぎ、発生時の対策を備えること。
- 埃、振動、温度、湿度等の影響を可能な限り排除すること。
- 生体認証鍵などを施し入退室記録などで人の出入りを管理すること。
- サーバ機器を容易に取り外せないよう適切に固定できる設備を有すること。

(2)　サーバの冗長化

① システム管理者は、情報資産の分類による必要性に応じて、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 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 システム管理者は、情報システム管理部門と連携し、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対し、十分な容量の無停電電源装置を備え付けなければならない。

② システム管理者は、情報システム管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

③ セキュリティ責任者は、庁舎全体の電源について停電等による電源供給の停止に備え、一定期間の自家発電が可能な装置を備え付けたうえで、必要最小限な情報資源の運用が確保できるよう図らなければならない。

(4)　通信ケーブル等の配線

① セキュリティ責任者及びシステム管理者は、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 セキュリティ責任者、施設管理部門及び情報システム管理部門は、庁内の主要な箇所の通信ケーブル及び電源ケーブルについて、連携して管理し保全しなければならない。
③ 情報システム管理部門は、末端部分の通信ケーブル及び電源ケーブルについて損傷等の報告があった場合、対応しなければならない。
④ セキュリティ責任者及びシステム管理者は、ネットワーク接続口の設置場所について適切に管理しなければならない。
⑤ システム管理者は、情報システム管理部門もしくは契約により作業を認められた外部委託事業者でない者が、配線を変更・追加することのないよう管理しなければならない。

(5) 機器の定期保守及び修理
① システム管理者は、可用性2以上のサーバ等の機器について定期保守を実施しなければならない。
② システム管理者は、記録媒体を内蔵する機器を庁外の場所で修理させる場合、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他、秘密保持体制の確認などを行わなければならない。

(6) 敷地外への機器の設置
① 庁舎の敷地外にサーバ等の機器を設置する場合、CIO の承認を得なければならない。ただし、個人情報を保管する機器の場合は、三股町電子計算組織に係る個人情報の保護に関する条例の定めによらなければならない。
② 庁舎の敷地外にサーバ等の機器を設置する場合、システム管理者は次のことを遵守しなければならない。
- 管理を委託する事業者との間で、セキュリティ対策や守秘義務等の必要な事項を明記した契約を締結すること。
- 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すること。

(7) 機器の廃棄等
機器を廃棄もしくはリース返却等をする場合は、システム管理者は機器内部の記憶装置からすべての情報を消去のうえ、復元不可能な状態にする措置を講じなければならない。

3-2 管理区域(サーバルーム等)の管理
(1) 管理区域の構造等
① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋(以下「サーバルーム」という。)や電磁的記録媒体の保管庫をいう。
② セキュリティ責任者及びシステム管理者は、管理区域を地階もしくは浸水の恐れのある1階に設けてはならない。また、外部からの侵入が容易にできないように措置を施さなくてはならない。
③ セキュリティ責任者及びシステム管理者は、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 セキュリティ責任者及びシステム管理者は、サーバルーム内の機器等に、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 セキュリティ責任者及びシステム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部をすべて塞がなければならない。

⑥ セキュリティ責任者及びシステム管理者は、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 セキュリティ責任者は、サーバルームへの入退室を IC カード、指紋認証等の生体認証等により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 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。

③ 非常勤職員、臨時職員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。

④ システム管理者は、非常勤職員、臨時職員及び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行政機関の職員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

① 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、あらかじめ職員又は委託した業者に確認を行わせなければならない。

② システム管理者は、サーバルーム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。

3-3 通信回線及び通信回線装置の管理

① 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 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 セキュリティ責任者は、機密性3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。

④ 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。

3-4 職員等のパソコン等の管理

① セキュリティ責任者は、職員等が業務で使用するパソコン等の端末について、盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。

② セキュリティ責任者及びシステム管理者は、職員等が業務で使用するパソコン等の固有の記録装置と端末について、盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。
③ システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。
④ システム管理者は、BIOS パスワード、ハードディスクパスワード等を併用しなければならない。
⑤ システム管理者は、パスワード以外に指紋認証等の生体認証鍵を併用しなければならない。
⑥ システム管理者は、パソコン等の端末のディスク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。

## 4　人的セキュリティ

### 4-1 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

① 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。

② 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、速やかにシステム管理者に相談し、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)　パソコン等端末固有記録装置への記録

① セキュリティ責任者及びシステム管理者は、職員等が業務で使用するパソコン等の固有の記録装置に、機密性3以上の情報を記録させてはならない。

② 上記①の禁止事項については、行政事務の遂行のため一時的な記録を行う場合にかぎり、セキュリティ責任者の許可を得て例外措置として行うことができる。

③ 職員等は、職員等が業務で使用するパソコン等の固有の記録装置に、機密性3以上の情報を記録させる場合において、当該記録の用途が終了した際には速やかに記録を消去しなければならない。

④ 上記③の遵守事項の実行はシステム管理者が確認しなければならない。

(4)　パソコン等の端末の持ち出し及び外部における情報処理作業の制限

① CIO は、機密性3以上、可用性3以上、完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

② 職員等は、三股町のパソコン等の端末、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、セキュリティ責任者の許可を得なければならない。

③ 職員等は、外部で情報処理業務を行う場合には、セキュリティ責任者の許可を得なければならない。

④ 職員等は、外部で機密性2以下の情報処理作業を行う際、私物パソコン等の三股町で管理していない情報処理機器を用いる場合には、システム管理者の許可を得たうえで、安全管理措置を遵守しなければならない。

⑤ 機密性3以上の情報資産については、私物パソコン等の三股町で管理していない情報処理機器による情報処理を行ってはならない。

(5)　パソコン等の端末等の持込

職員等は、私物のパソコン等の情報処理装置及び記録媒体を庁舎内に持ち込んではならない。ただし、業務上必要な場合は、セキュリティ責任者の許可を得て、例外措置としてこれらを持ち込むことができる。

(6)　持ち出し及び持ち込みの記録

セキュリティ責任者は、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。

(7)　パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の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セキュリティ責任者の許可なく変更してはならない。

(8)　机上の端末等の管理

職員等は、パソコン等の端末や記録媒体等について、第三者に使用されること、又はシステム管理者の許可なく情報を閲覧されることがないように、離席時の端末のロックや記録媒体の保管等、適切な措置を講じなければならない。

(9)　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。

4-2　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

システム管理者は、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

システム管理者は、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

システム管理者は、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、外部ネットワーク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。

(4)　情報セキュリティポリシー等の掲示

セキュリティ責任者は、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。

4-3　外部委託事業者に対する説明

セキュリティ責任者及びシステム管理者は、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。

4-4　研修・訓練

(1)　情報セキュリティに関する研修・訓練

CIO は、定期的又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)　研修計画の立案及び実施

① CIO は、幹部を含めすべ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又は必要に応じて立案し、委員会の承認を得なければならない。

② セキュリティ責任者は、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、可能な限り速やかに実施しなければならない。

③ 研修は、セキュリティ責任者、システム管理者、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。

④ CIO は、定期的に又は必要に応じて、委員会に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

CIO は、緊急時対応を想定した訓練を定期的に又は必要に応じて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

幹部を含めたすべての職員等は、業務に支障の無い範囲において、定められた研修・訓練に参加しなければならない。

4-5　事故、欠陥等の報告

(1)　庁内からの事故等の報告

① 職員等は、情報システム運用に関わる事故、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかにシステム管理者に報告しなければならない。

② 事故の報告を受けたシステム管理者は、速やかにセキュリティ責任者及び CIO に報告しなければならない。

③ システム上の欠陥もしくは誤動作の報告を受けたシステム管理者は、速やかにセキュリティ責任者に報告しなければならない。

④ システム管理者は、報告のあったシステム上の欠陥もしくは誤動作について、必要に応じて CIO に報告しなければならない。

(2)　住民等外部からの事故等の報告

① 職員等は、三股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事故、欠陥について、住民等外部から報告を受けた場合、システム管理者に報告しなければならない。

② 報告を受けたシステム管理者は、速やかにセキュリティ責任者に報告しなければならない。

③ セキュリティ責任者は、当該事故等について、必要に応じてCIOに報告しなければならない。

④ CIO は、情報システム等の情報資産に関する事故、欠陥について、必要に応じ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)　事故等の分析・記録等

セキュリティ責任者は、事故等を引き起こした部門のシステム管理者と連携し、これらの事故等を分析し、記録を保存しなければならない。

4-6　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、速やかにセキュリティ責任者及びシステム管理者に報告し、指示に従わなければならない。

② セキュリティ責任者及びシステム管理者は、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 セキュリティ責任者及びシステム管理者は、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。また、余人の目の届く範囲に記述を残してはならない。

② パスワードを秘密にし、例え CIO からの問い合わせであっても、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、文字列は自己の情報から類推できな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、システム管理者に報告し、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複数の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。

## 5　技術的セキュリティ

### 5-1 コンピュータ及びネットワークの管理

(1)　文書サーバの設定等

① セキュリティ管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

② セキュリティ管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③ セキュリティ管理者は、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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

④ セキュリティ責任者は、課室等及び係の単位で使用できるフォルダ容量の上限を設定し、現在の使用容量を定期的に職員等に周知しなければならない。

(2)　バックアップの実施

セキュリティ責任者及びシステム管理者は、文書サーバ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

システム管理者は、他の団体とネットワーク及び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必要がある場合、その取扱いに関する事項をあらかじめ定め、CIO の承認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 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、必要に応じて作業記録を作成しなければならない。

② セキュリティ責任者及びシステム管理者は、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、必要に応じて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 セキュリティ責任者または契約により操作を認められた外部委託事業者が、可用性3以上の情報システムについて変更等の作業を行う場合は、2 名以上で作業を行い互いにその作業を確認するか、あるいは2名のうち1名が行った作業の結果を他方が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

セキュリティ責任者及びシステム管理者は、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情報資産として適切に管理しなければならない。

(6)　アクセス記録の取得等

① セキュリティ責任者及びシステム管理者は、各種アクセス記録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 セキュリティ責任者及びシステム管理者は、アクセス記録等が詐取、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。

③ セキュリティ責任者及びシステム管理者は、システムから自動出力したアクセス記録等について、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。

(7) 障害記録

セキュリティ責任者及びシステム管理者は、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 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 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

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もしくは論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 セキュリティ責任者及びシステム管理者は、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、CIO 及び委員会の承認を得なければならない。

② セキュリティ責任者及びシステム管理者は、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、庁内のすべてのネットワーク、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 セキュリティ責任者及びシステム管理者は、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 セキュリティ責任者及びシステム管理者は、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うえで接続しなければならない。

⑤ セキュリティ責任者及びシステム管理者は、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、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) 無線 LAN 及びネットワークの盗聴対策

① セキュリティ責任者は、音声データによる通信を除き、機密性3以上の情報について無線 LAN を通じて送受信させてはならない。ただし、行政事務の遂行のため一時的な通信を行う場合にかぎり、解読が困難な暗号化及び認証技術の使用を義務づけたうえで、無線 LAN の利用を例外的に許可することができる。

② セキュリティ責任者は、機密性4の情報を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。

(12) 電子メールのセキュリティ管理

① 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 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 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 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 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、委託先との間で利用方法を取り決めなければならない。

⑥ セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように、添付ファイルの監視等によりシステム技術的な措置を講じなければならない。

(13) 電子メールの利用制限

① 職員等は、端末個別に自動転送機能を設定して、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、機密性3以上の情報を記載または添付した電子メールを送信してはならない。ただし、業務遂行上必要な場合は、セキュリティ責任者の許可を得て例外措置として行うことができる。

④ 職員等は、重要な電子メールを誤送信した場合、システム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。ただし、業務遂行上必要な場合は、セキュリティ責任者の許可を得て例外措置として行うことができる。

⑥ 職員等は、ウェブで利用できるネットワークストレージサービス等を使用する場合は、所属する課室等のシステム管理者の許可を得て、機密性2以下の情報についての利用に限り行うことができる。

(14) 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、CIO 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。

② 職員等は、暗号化を行う場合に CIO が定める以外の方法を用いてはならない。また、CIO 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。

(15) 無許可ソフトウェアの導入等の禁止

① 職員等は、パソコン等の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、セキュリティ責任者及び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。
③ ソフトウェアを導入する際において、セキュリティ責任者又はシステム管理者は、ソフトウェアのライセンスを管理しなければならない。
④ 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。

(16) 外部記憶装置の制限
① 職員等は、パソコン等の端末に無断で外部記憶装置を接続してはならない。
② セキュリティ責任者は、パソコン等の端末に外部記憶装置が接続できないよう適切に処置しなければならない。
③ 職員パソコン等の端末に外部記憶装置を接続して作業を行うことが業務遂行上必要な場合は、セキュリティ責任者の許可を得て例外措置として行うことができる。

(17) 機器構成の変更の制限
① 職員等は、パソコン等の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、パソコン等の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、セキュリティ責任者及びシステム管理者の許可を得なければならない。

(18) 無許可でのネットワーク接続の禁止
職員等は、セキュリティ責任者の許可なくパソコン等の端末をネットワークに接続してはならない。

(19) 業務以外の目的でのウェブ閲覧の禁止
① 職員等は、就業時間中にあっては、業務以外の目的でウェブを閲覧してはならない。
② 職員等は、就業時間外であっても、業務用ネットワークシステムで閲覧するにあたって、明らかに不適切なサイトを閲覧してはならない。

5-2 アクセス制御と ID の管理
(1) アクセス制御
セキュリティ責任者又はシステム管理者は、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
① セキュリティ責任者及びシステム管理者は、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。
② 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、セキュリティ責任者又はシステム管理者に通知しなければならない。
③ セキュリティ責任者及びシステム管理者は、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て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

① セキュリティ責任者及びシステム管理者は、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。
② セキュリティ責任者及びシステム管理者の特権を代行する者は、セキュリティ責任者及びシステム管理者が指名し、CIO が認めた者でなければならない。
③ CIO は、代行者を認めた場合、速やかにセキュリティ責任者及びシステム管理者に通知しなければならない。

(4) 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、セキュリティ責任者及び当該情報システムを管理するシステム管理者の許可を得なければならない。
② 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 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 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、機密性3以上の情報システムにあっては、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 セキュリティ責任者及びシステム管理者は、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、セキュリティ責任者に検査を依頼しなければならない。
⑦ セキュリティ責任者は、持ち込んだ又は外部から持ち帰ったパソコン等の端末がコンピュータウイルスに感染していないこと、及びパッチの適用状況等を確認しなければならない。

(5) 自動識別の設定
セキュリティ責任者及びシステム管理者は、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を自動的に識別する技術的な措置を講じるよう努めなければならない。

(6) ログイン時の表示等
セキュリティ責任者及びシステム管理者は、ログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、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、管理する情報システムで技術的に可能な範疇において、設定し管理なければならない。

(7) パスワードに関する情報の管理
① セキュリティ責任者又はシステム管理者は、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 セキュリティ責任者又はシステム管理者は、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。

(8) 特権による接続時間の制限

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。

5-3 システムの調達と開発

(1) 情報システムの調達

① セキュリティ責任者及びシステム管理者は、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。

② セキュリティ責任者及びシステム管理者は、機器及びソフトウェア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

① 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。

② 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。

③ 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。

④ 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。

⑤ 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。

5-4 システムの導入と保守

(1) 開発環境と運用環境の分離及び移行手順の明確化

① 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。

② 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。

③ 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。

(2)　テスト

① 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。

② 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。

③ システム管理者は、機密性4以上の実在データを、テストデータに使用してはならない。

(3)　システム開発・保守に関連する資料等の保管

① 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文書を適切な方法で保管しなければならない。

② 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 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。

(4)　情報システムにおける入出力データの正確性の確保

① 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 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 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。

(5)　情報システムの変更管理

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。

(6)　開発・保守用のソフトウェアの更新等

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。

(7)　システム更新又は統合時の検証等

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。

5-5　不正プログラム対策

(1)　セキュリティ責任者の措置事項

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。

(2) システム管理者の措置事項

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 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 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、ネットワーク接続や外部記録媒体の使用がなく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。
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又は必要に応じて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 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、もしくは疑わしき兆候、挙動を確認した場合は、LAN ケーブルを即時取り外したうえで、速やかにセキュリティ責任者に報告しなければならない。

(4)　専門家の支援体制

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。

5-6 不正アクセス対策

(1)　セキュリティ責任者の措置事項

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、セキュリティ責任者及び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。

③ 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。

(2)　攻撃の予告

CIO 及び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

CIO 及び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

セキュリティ責任者及びシステム管理者は、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

セキュリティ責任者及びシステム管理者は、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室等のシステム管理者に通知し、適切な処置を求めなければならない。

5-7 セキュリティ情報の収集

(1)　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

セキュリティ責任者及びシステム管理者は、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

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

セキュリティ責任者及びシステム管理者は、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。

## 6　運用

### 6-1　情報システムの監視

① セキュリティ責任者及びシステム管理者は、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できる技術的な措置を行わなければならない。

② セキュリティ責任者及びシステム管理者は、重要なアクセス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 セキュリティ責任者及びシステム管理者は、外部と常時接続するシステムを常時監視できる技術的な措置を行わなければならない。

### 6-2　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 システム管理者は、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、速やかにセキュリティ責任者に報告しなければならない。

② セキュリティ責任者は必要に応じて CIO に報告し、CIO は、発生した問題について適切に対処しなければならない。

③ セキュリティ責任者及びシステム管理者は、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、定期的に又は必要に応じて確認を行い、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)　端末及び記録媒体等の利用状況調査

CIO 及び CIO が指名した者は、外部不正、内部不正及び管理不全の調査のために、職員等が使用しているパソコン等の端末、記録媒体へのアクセス記録、外部ネットワークとの通信記録、インターネットの閲覧記録、電子メールの送受信記録等の利用状況を閲覧することができる。

(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、直ちにセキュリティ責任者もしくはシステム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。

### 6-3　侵害時の対応

(1)　緊急時対応計画の策定

CIO 又は委員会は、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情報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、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

三股町が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、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

CIO 又は委員会は、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。

(5) 緊急時対応計画の公開

緊急時対応計画は、公にすることにより情報セキュリティや三股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。

6-4 外部委託

(1) 外部委託先の選定基準

① セキュリティ責任者及びシステム管理者は、外部委託先の選定に当たり、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 セキュリティ責任者及びシステム管理者は、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、事業者を選定するよう努めなければならない。

(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、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
- 委託先の責任者、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
- 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
- 町による事故時等の公表
- 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

システム管理者は、所管する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 CIO に報告しなければならない。

6-5 例外措置

(1) 例外措置の許可

システム管理者は、情報セキュリティ関係規程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、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) 例外措置申請の判断

セキュリティ責任者は、情報セキュリティ関係規程に係る例外措置申請の内容が、重大もしくは広範囲な影響が懸念されると判断したときは、CIO に報告したうえで委員会の判断をあおぐことができる。この場合において、例外処置申請内容の実施は、委員会の承認が得られるまで保留される。

(3) 緊急時の例外措置

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、例外措置申請を実施することが不能なときは、情報セキュリティ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ができる。その場合、事後速やかに CIO に報告しなければならない。

(4) 例外措置の申請書の管理

① セキュリティ責任者は、例外措置申請書を適切に処理し管理しなければならない。
② 例外措置の有効期限は、最長で当該申請書の申請年月日の属する年度の末日とする。
③ 例外措置の申請書及び審査結果は、例外措置の有効期限が消滅した後、5年経過するまで適切に保管しなければならない。

6-6 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 三股町電子計算組織に係る個人情報の保護に関する条例(平成三年九月三十日条例第二十一号)

6-7 違反時の対応等

(1) 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

行動をとらなければならない。

① 違反を確認したセキュリティ責任者は、当該職員等が所属する課室等のシステム管理者に通知し、適切な措置を指示しなければならない。

② システム管理者が違反を確認した場合は、速やかにセキュリティ責任者に通知し、適切な措置を求めなければならない。

③ その他の違反を確認した者は、速やかに当該職員等が所属する課室等のシステム管理者に通知し、適切な措置を求めなければならない。

(2) 違反時の権限

① システム管理者の指導によっても違反状態が改善されない場合、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。

② セキュリティ責任者が職員等の権利を停止あるいは剥奪した場合、速やかに CIO に報告し、当該職員等が所属する課室等のシステム管理者に通知しなければならない。

(3) 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ことができる。

## 7　評価・見直し

### 7-1 監査

(1)　実施方法

委員会は、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、定期的に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

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、委員会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、委員会に報告する。

(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

CIO は、監査結果を踏まえ、指摘事項を所管するシステム管理者に対し、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システム管理者に対しても、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の見直し等への活用

委員会は、監査結果を情報セキュリティポリシーの見直し、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。

### 7-2 自己点検

(1)　実施方法

① セキュリティ責任者及びシステム管理者は、所管するネットワーク及び情報システムについて、定期的に又は必要に応じて自己点検を実施しなければならない。
② システム管理者は、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的に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

セキュリティ責任者及びシステム管理者は、自己点検結果とそれに基づく改善策を取りまとめ、委員会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。
② 委員会は、この点検結果を情報セキュリティポリシーの見直し、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。

7-3 情報セキュリティポリシーの見直し

委員会は、情報セキュリティポリシー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、定期的に又は必要に応じて評価を行い、必要があると認めた場合は改善を行うものとする。