情報セキュリティポリシー

太子町

平成１６年３月

平成 25 年 7 月 1 日一部改訂
平成 29 年 3 月 31 日一部改訂

＊目　　次＊

情報セキュリティ基本方針

情報セキュリティ対策基準

情報セキュリティ基本方針

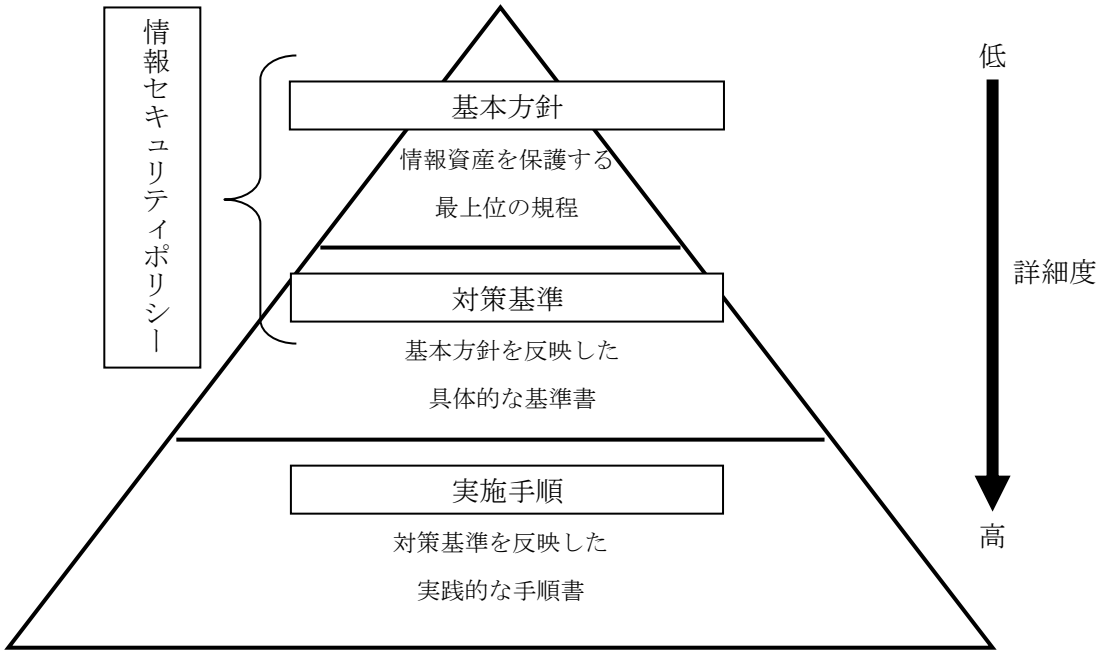
1　目的

太子町の保有する情報資産には、住民の個人情報のみならず行政の運営上重要な情報等が多く含まれており、これらの情報が部外者に漏えいした場合、極めて重大な結果を招くことが考えられる。

近年は不正アクセスやコンピュータウイルス等、サイバー攻撃の脅威は多様化、高度化しており、これらに対する情報セキュリティ対策も含め、情報資産に対して発生し得る、人的脅威や災害・事故等を未然に防止し、また、脅威が発生した場合にも被害を最小限にすることが可能な総合的かつ効果的な情報セキュリティ対策の強化、拡充が急務である。ついては、本町の情報資産の機密性、完全性、可用性を維持することを目的とし、本町の情報セキュリティポリシーを定めることとする。

2　位置付け

情報セキュリティポリシーは、組織における最上位の規程と位置付けられる。策定された情報セキュリティポリシーを反映させるため、より具体的な対策基準を策定し、さらに業務の実態に見合った実施手順を策定し、これを継続的に活用する。これらの関係を図示すると次のようになる。



3　対象範囲

対象範囲は、次のとおりとする。

（1）組織の範囲

町の業務を取扱うすべての部署

（2）人の範囲

町の保有する情報資産を取扱う職員等及び外部委託事業者等を対象とする。

ア　職員等

特別職、一般職員（再任用職員含む）、その他職員（特別職非常勤職員、臨時職員、嘱託職員等）

イ　外部委託事業者等

町と雇用関係を持たない者のうち、契約等によって定められた範囲内での町の業務を支援する者

（3）情報資産の範囲

ア　情報

町の保有する次の情報を対象とする。

・印刷情報

(イ) 情報システムから出力された印刷情報

(ロ) 情報システムの開発・運用のための資料

・電子情報

情報を記録するために用いるフロッピーディスク、磁気ディスク、光ディスク等の記録媒体に保存されているデータ及びネットワークを転送されるデータ等

イ　情報システム

町の保有する電子情報の作成・流通・保管の基盤となるコンピュータシステム及びネットワークを対象とする。

4　職員等の義務

職員等は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては情報セキュリティポリシーを遵守するものとする。

5　情報セキュリティ管理体制

本町の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

6　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じた情報セキュリティ対策を行うものとする。

7　情報資産への脅威

情報セキュリティポリシーを講ずるうえで、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

認識すべき脅威は以下のとおりである。

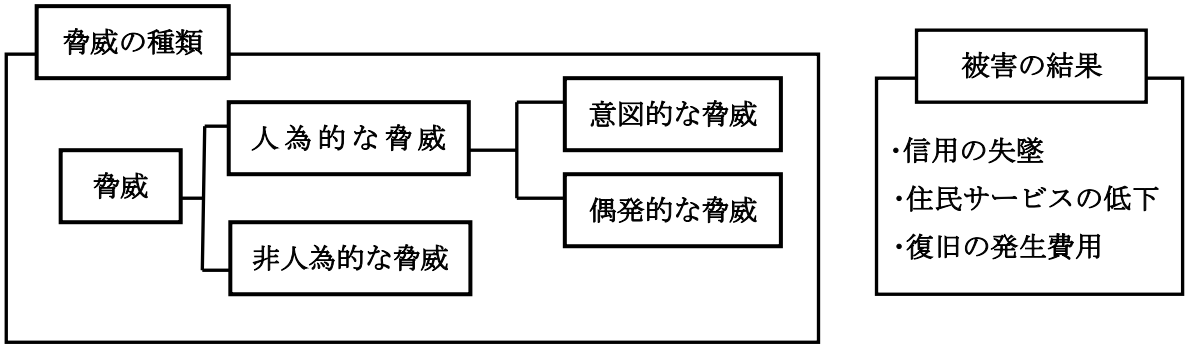
ア　サイバー攻撃をはじめとする部外者の進入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の搾取、内部不正等

イ　情報資産の無断持ち出し、無許可ソフトウエアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

ウ　地震、落雷、火災等の災害によるサービス及び業務の停止等

エ　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

オ　電力供給の途絶、通信の途絶等の提供サービスの障害からの波及等



8　情報セキュリティ対策

本町の情報資産を前記７の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

ア　人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに、すべての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育・研修を行う。

イ　物理的セキュリティ対策

情報センターへの不正な立入り等を防ぐため入退室や、機器の転倒防止等物理的な対策を講ずる。

ウ　技術的セキュリティ対策

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を講じる。

エ　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。また、情報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、緊急時対応計画を策定する。

9　情報セキュリティ対策基準の策定

本町の情報資産について、前記８の情報セキュリティ対策を講ずるにあたっては、職員等が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

１０　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくために、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、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、公開することにより本町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１１　評価・見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを実施するものとする。

用語一覧

情　報　セ　キ　ュ　リ　テ　ィ　基　本　方　針	
用　　語	用　語　の　解　説
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。
情報セキュリティ対策	脅威に対して適切に対応するための方法。
機　密　性	情報へのアクセスは、権限を持つ者に限定し、許可された者だけが行えることを保障すること。
完　全　性	情報・処理方法の正確な状態を維持することで、情報の完全性（正確性）を確保すること。
可　用　性	許可された者が、必要なときに情報、及び情報システムにアクセスできること。
情 報 資 産	情報そのものや情報を処理するシステム、情報を流通するネットワークなどがある（データ・プログラム等）。情報システムの所有権が無くても、使用している情報システムがある場合、その情報システムも保護の対象となる。
情報セキュリティポリシー	基本方針＋対策基準 組織全体で情報資産の脅威に対する抑止、予防、検知、回復についての取組むための方針。 脅威に対して、どの程度対応すべきかを決定することをいう。
基 本 方 針	情報セキュリティ上の指針となるもの。 情報セキュリティに関する自治体の責務・体制を明文化する。
対 策 基 準	個別システムに依存せず、共通に使用できる具体的な情報セキュリティ管理策をまとめたもの。

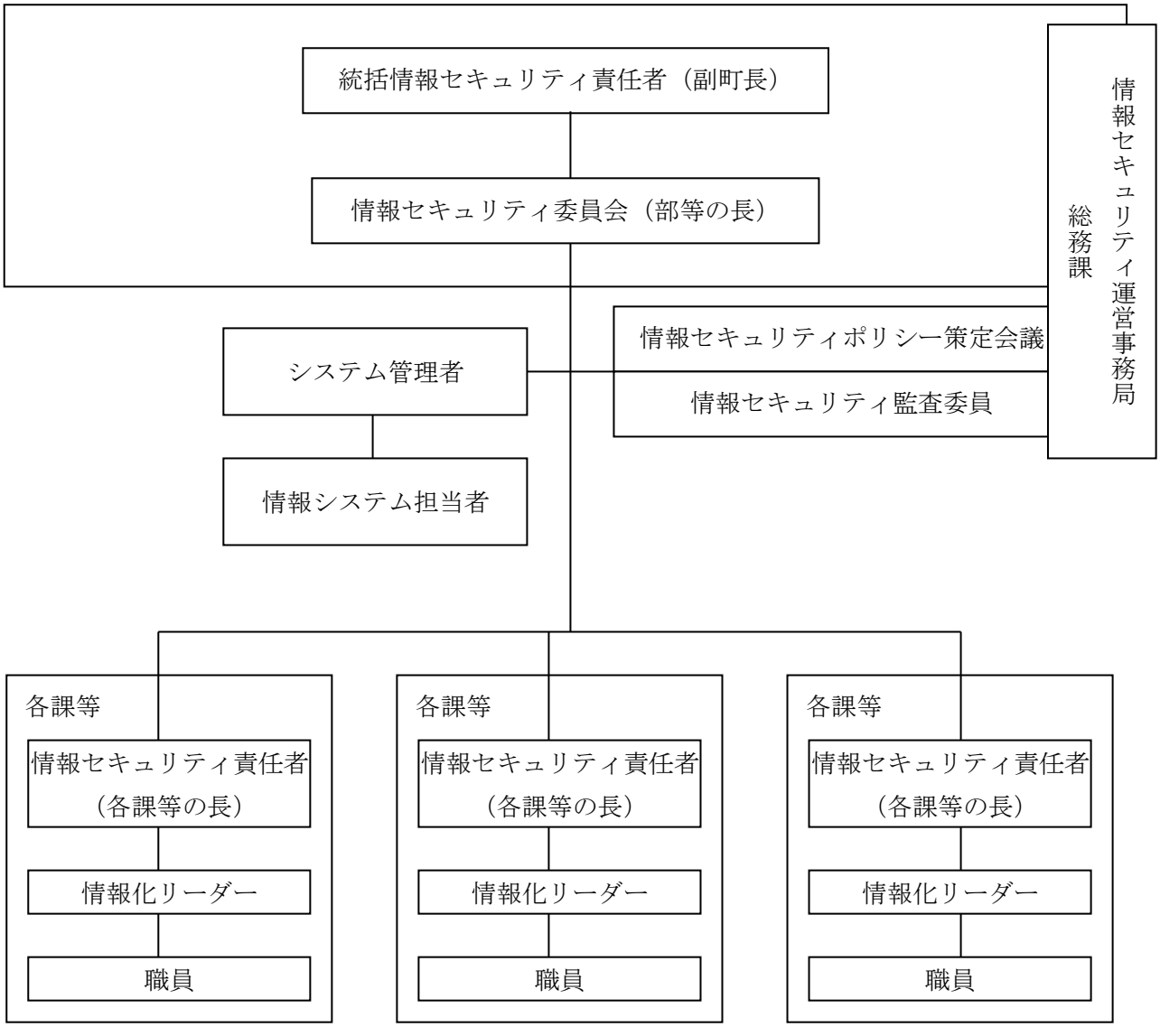
情報セキュリティ対策基準

第１　情報セキュリティ組織体制

１　目的

情報セキュリティ対策の推進及びセキュリティ侵害への迅速な対応のため、情報セキュリティに関する組織体制を確立することを目的とする。

ア　情報セキュリティの円滑な推進のため、次のような体制を確立する。



イ　情報セキュリティ運営関係者の役割

情報セキュリティ組織体制の中で、誰が何をするのかを明確にする。

組織体制役割一覧

名　　称	該当する組織又は役職	主　な　役　割
統括情報セキュリティ責任者	副　町　長	○情報セキュリティに関する全ての責任及び権限を有する。 ○情報セキュリティ委員会を開催し、その委員長を務める。
情報セキュリティ委員会	部　　長 次　　長 (太子町高度情報化施策推進本部)	○情報セキュリティに関する重要事項についての協議及び承認／否する。 ○情報セキュリティ侵害、監査結果に対する改善策を協議する。 ○情報セキュリティポリシーの内容を審議し、必要に応じて改訂を情報セキュリティポリシー策定会議に指示する。
情報セキュリティ運営事務局	総　務　課	○情報セキュリティポリシーの運営を行う。 ○情報セキュリティポリシーの普及・教育を推進する。 ○情報セキュリティ委員会の決定事項を実施する。 ○情報セキュリティポリシー策定事項を情報セキュリティ委員会に報告する。
システム管理者	総務課長	○庁内ネットワークの開発、導入、保守を管理する。 ○各情報システムが、適正に運用されているかを管理する。 ○不正プログラム対策の徹底、情報セキュリティ侵害の監視を行う。 ○情報セキュリティを収集し、必要に応じて、庁内ネットワークへの対処及び各課への周知を行う。
情報システム担当者	総務課情報係	○情報システム管理者の指示の下、庁内における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。
情報セキュリティポリシー策定会議	情報化リーダー会議で指名された者	○情報セキュリティ委員会の指示の下、情報セキュリティポリシーの改訂を行う。
情報セキュリティ監査委員		○庁内における情報セキュリティポリシーの遵守状況を監査する。 ○各情報システムの情報セキュリティレベルを監査する。 ○監査結果を情報セキュリティ委員会に報告する。
情報セキュリティ責任者	課 等 の 長	○課等の情報セキュリティに関する責任及び権限を有する。 ○課等で開発・運営している情報システムの管理に責任及び権限を有する。 ○課等において、情報セキュリティポリシーの普及及び指導を行い、遵守の徹底を図る。 ○情報セキュリティ侵害について、所管内に対応を指示し、情報セキュリティ運営事務局へ侵害内容、状況等を報告する。
情報セキュリティ担当者	課等の長より指名された者 (情報化リーダー)	○情報セキュリティ責任者の指示の下、所管内の情報セキュリティ対策を実施する。 ○情報セキュリティ侵害時には、情報セキュリティ責任者の指示の下、速やかに対処する。

第２　情報の分類と管理

１　目的

情報の重要性とその取扱いについて明らかにし、情報の管理責任を明確にすることを目的とする。

ア　情報管理関係者の役割

情報の管理における関係者の役割は次のとおりとする。

情報管理における関係者の役割一覧

名　　称	対　象　者	該　当　者	役　　割　　概　　要
情報管理責任者	情報の内容に関して責任を有する者	課等の長	○情報に対して情報分類、開示範囲を指定する。 ○情報の業務目的外利用(提供)への漏えい、改ざん、破壊がないように情報を適正に管理する。 ○情報の重要度の推移に応じて適宜、情報分類・開示範囲を変更する。
情 報 管 理 者	情報保有している課から承認を受けた者	課等の長	○情報管理責任者が付与した情報の漏えい、改ざん、破壊等が生じないように管理し、利用状況についても把握する。
情 報 利 用 者	情報管理者から情報を利用して業務を遂行する特定の職員	職　　員	○情報管理責任者が付与した情報分類に基づいて、情報を適切に取扱~~いを行~~わなければならない。

２　情報の分類

情報は、情報管理責任者、情報管理者及び情報利用者が、適正な取扱いを行えるようにするため、重要性に応じて分類をする。

情報分類

情　報　の　重　要　性	
重要性分類Ⅰ	個人情報並びに職員に関する業務上必要とする最小限の者のみが扱う情報
重要性分類Ⅱ	開示することを予定していない情報
重要性分類Ⅲ	外部に提供する情報のうち業務上重要な情報
重要性分類Ⅳ	上記以外の情報

３　情報の管理及び取扱い

重要性分類Ⅰ・Ⅱの行政情報の不用意な複製や、送付・送信を行ってはならない。

ア　職員等は、業務上必要な場合には、情報管理責任者の許可を得た上で情報の複製・送付・送信を行わなければならない。

イ　重要性分類Ⅰ・Ⅱの情報を送信・運搬する者は、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。

4　記録媒体の管理

職員等は、重要性分類Ⅰ・Ⅱの情報を記録した取り外し可能な記録媒体は、使用の際は施錠可能な安全な場所に保管し、情報管理責任者に報告しなければならない。

5　記録媒体の処分

記録媒体が不要となった場合は、当該媒体に記録されている重要性分類Ⅰ・Ⅱの情報をいかなる方法によっても復元できないように消去等を行った上で廃棄しなければならない。

ア　記録媒体の廃棄を行う者は、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。

イ　情報資産の廃棄を行う者は、情報セキュリティ責任者の許可を得なければならない。

第3　人的セキュリティ

1　目的

業務に携わる職員等が、情報セキュリティに対する意識高揚を図るため、情報セキュリティ対策の実施を確実にすることを目的とする。

2　職員等

ア　職員等は、情報セキュリティ責任者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行わなければならない。

イ　職員等は、情報セキュリティ実施手順に定めている事項を遵守しなければならない。

ウ　職員等は、情報セキュリティ実施手順について不明な点、遵守することが困難な点がある場合には、速やかに情報セキュリティ責任者に報告し、指示を仰がなければならない。

エ　職員等は、パソコン等の端末や記録媒体、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責任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、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。

オ　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。

3　教育・訓練

ア　統括情報セキュリティ責任者は、職員等に対し情報セキュリティポリシーについて啓発に努めるとともに、職員等を対象とした情報セキュリティポリシーに関する教育の機会を設けなければならない。

イ　情報システムを所管する情報セキュリティ責任者は、情報システムの運用に支障を来さない範囲において緊急時対応を想定した訓練を職員等に行わせなければならない。

ウ　職員等は、情報セキュリティポリシーに関する研修を受講し、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理解し、情報セキュリティ上の問題が生じないようにしなければならない。

4　外部委託に関する管理

情報セキュリティ責任者が、情報システムの開発・保守・運用管理を外部委託事業者等に委託する場合は、情報セキュリティが確保できる外部委託事業者等を選定のうえ、遵守すべき事項及び守秘義務を明記した契約を締結し、当該セキュリティポリシーが遵守されるよう管理しなければならない。

5　パスワード等の管理

ア　職員等は、自己の保有するパスワードについて、不用意にメモを作ったりしないようにするなど、パスワードの秘密保持に努めなければならない。

イ　職員等は、パスワード設定について、他者に類推されることない複雑な内容としなければならない。

6　個人所有機器の利用禁止

職員等は、個人が所有するパソコン、モバイル端末及びＵＳＢメモリを業務に利用してはならない。ただし、業務上特別の理由がある場合は、情報セキュリティ責任者の許可を得て、使用することができる。

7　特別職、一般職員以外の者による情報資産の利用

情報セキュリティ責任者は、その他職員、外部委託事業者等の雇用及び委託契約時に必ず、その他職員が守るべき内容を遵守させるなど、適切な指導を行わなければならない。

8　事故・欠陥等の報告

ア　職員等は、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、速やかに情報セキュリティ責任者に報告しなければならない。

イ　報告を受けた情報セキュリティ責任者は、当該事故等が情報システムに関連する場合、速やかに統括情報セキュリティ責任者及びシステム管理者に報告しなければならない。

ウ　情報セキュリティ責任者は、報告のあった事故等について、必要に応じて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。

エ　統括情報セキュリティ責任者は、事故等を引き起こした部門の情報セキュリティ責任者及び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。

第４　物理的セキュリティ

1　目的

情報資産を収容する情報管理室、サーバ室及び各事務室から情報の漏えい、盗難等に対して物理的な対策を実施することを目的とする。

2　情報管理室及びサーバ室の入退室管理

職員等の情報管理室及びサーバ室への入退室は事前に許可された者のみとし、外部委託事業者等の入退室する際には入退室管理簿に必要事項を記載しなければならない。また身分証明書を携帯し、求めにより提示しなければならない。

3　機器等の搬入場所

情報管理室及びサーバ室への機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性についてシステム管理者の確認を行い、搬入時には、そのシステム管理者が同行するなどの必要な措置を施さなければならない。

4　機器の取付け等

サーバ、ネットワーク機器及び端末等を取付ける場合は、火災、水害、ほこり、振動、湿度、温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な固定等必要な措置を施さなければならない。

5　電源

システム管理者は、停電及び電圧異常によりデータ等が破壊されるのを防ぐため、業務処理に支障をおよぼすおそれのある情報システム機器等の電源に、予備電源（無停電電源装置等）を備え付ける等の措置を講じなければならない。

6　配線

システム管理者は、傍受又は損傷等を受けることがないよう可能な限り必要な措置を講じなければならない。

7　サーバ室外へのサーバ機器等の設置

サーバ室外にサーバ機器等の機器を設置する場合は、システム管理者と協議した結果を情報セキュリティ運営委員会に諮り、使用方法を定め、統括情報セキュリティ責任者の承認を受けなければならない。

8　本町が管理するネットワーク及び施設外への機器等の持出し

情報システム機器等を本町が管理するネットワーク及び施設外（以下「外部」という。）に持ち出すことを原則禁止する。ただし、業務上必要なものである場合には、情報セキュリティ責任者は外部に持ち出す許可を与えることができる。

第５　技術的セキュリティ

1　目的

職員等が、情報セキュリティ対策を実践し、それを管理する上で情報資産を必要なときに容易に継続して利用できるよう維持管理することを目的とする。

2　システム管理記録及び作業確認

システム管理者及び情報セキュリティ責任者は、情報システムの変更等の処理について、記録を作成し、適切に管理しなければならない。

3　障害記録

システム管理者は、職員等から報告があった情報については、システムの障害に対する処理又は問題等を、障害記録として体系的に記録し、常に活用できるように保存しなければならない。

4　バックアップの取得

システム管理者及び情報セキュリティ責任者は、重要性分類Ⅰ・Ⅱの情報については、記録媒体へのバックアップを取り、施錠等のできる安全な場所へ保管しなければならない。

5　ソフトウエアの導入に関する注意

ア　職員等は、正規のライセンスのないソフトウエアを導入してはならない。

イ　職員等は、業務上不必要なソフトウエア及び出所不明なソフトウエア等安全性が確認されないソフトウエアを導入してはならない。

ウ　ソフトウェアのライセンス管理を徹底しなければならない。

エ　職員等は、業務上必要な場合は、システム管理者へソフトウエアのインストールを依頼しなければならない。

6　電子メールの送受信等

ア　職員等は、電子メールを用いて、業務上不必要な者へ職場の電子メールを送信してはならない。

イ　職員等は、重要性分類Ⅰ・Ⅱの情報に該当する添付ファイルのある電子メールを送信する必要がある場合には、事前に情報セキュリティ責任者の承認を得なければならない。

ウ　職員等は、差出人が不明又は不自然に添付されたファイルを受信した場合は、開封せず、直ちにシステム管理者へ報告を行うとともにシステム管理者の指示に従い適切に処理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、情報セキュリティ責任者に報告しなければならない。

7　業務目的外利用の禁止

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。

8　アクセス制限及び記録等の取得

システム管理者は、許可された職員等のみが情報資産を利用できるように、アクセス制限の設定をしなければならない。また、定期的にアクセス記録等を分析し、一定期間保存しなければならない。

9　外部ネットワークとの接続制限等

ア　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、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　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。

ウ　統括情報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。

エ　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。

１０　電子署名

職員等は、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、太子町電子署名規程に基づき、送信しなければならない。

１１　ＩＣカード等の取扱い

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　ＩＣカード等を紛失した場合、速やかに情報システム管理者に報告し、指示に従わなければならない。

ウ　情報システム管理者は、ＩＣカード等の紛失等の報告があった場合、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。

エ　情報システム管理者は、ＩＣカード等の返却や切り替え等があった場合、当該ＩＣカードを回収し、破砕する等復元不可能な処理を行ったうえで廃棄しなければならない。

第６　情報システムの開発・導入・保守

１　目的

情報資産のセキュリティ対策は、情報システムの開発時点から適用することが求められるため、その情報セキュリティ要件を分析し、その対応策を実施管理することを目的とする。

２　情報システムの開発・導入

ア　情報セキュリティ責任者は、情報システムのソフトウエアを開発・導入する場合は、情報セキュリティ上に問題がないかどうか等をシステム管理者に確認しなければならない。

イ　情報セキュリティ責任者は、開発したソフトウエアを情報システムに取り入れる場合には、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。

３　情報システムの変更管理

システム管理者及び情報セキュリティ責任者は、重要なシステムを追加、変更、廃棄等した場合は、その際の設定・構成等の履歴を記録・保存し、必要な場合には復旧できるようにしなければならない。

４　機器の修理及び廃棄

システム管理者及び情報セキュリティ責任者は、記録媒体の含まれる機器を貸借期限終了に外部委託事業者等に返却・廃棄する場合は、すべての情報を消去しなければならない。外部委託事業者

等に修理又は返却・廃棄させる際、情報を消去することが難しい場合は、修理又は返却・廃棄する外部委託事業者等から情報を消去した書面を入手しなければならない。

第７　不正プログラム対策

１　目的

コンピュータウイルス等不正プログラムによって、情報資産の損失、損傷、不正アクセス等による業務妨害のリスクを回避するため、その利用方法を定め、適切に保護管理することを目的とする。

２　システム管理者及び情報セキュリティ責任者が実施する事項

システム管理者及び情報セキュリティ責任者は､次の事項を実施しなければならない。

ア　情報システムのサーバ及び必要な機器に不正プログラム対策ソフトを導入すること。

イ　不正プログラムチェック用のパターンファイルは常に最新のものを保つこと。

ウ　定期的に新種の不正プログラムに関する情報収集や情報システム内部の感染状況等について情報を収集すること。

エ　不正プログラム情報について、職員等に対する注意喚起を行うこと。

オ　不正プログラムについて、職員等に対して必要な啓発活動を行うこと。

３　職員等が遵守する事項

職員等は、次の事項を遵守しなければならない。

ア　外部からデータ又はソフトウエアを取り入れる場合及び外部に持ち出す場合には、必ず不正プログラムチェックを行うこと。

イ　不正プログラムチェックの実行を途中で止めないこと。

ウ　添付ファイルのあるメールを送受信する場合は、不正プログラムチェックを行うこと。

エ　端末に対して、不正プログラム対策ソフトウエ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　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は、LANケーブルの即時取り外しを行わなければならない。

第８　運用

１　目的

情報セキュリティ対策を実施すると、日常業務に浸透する反面、慣れにより違反が生じる可能性もあるため､その利用方法を定め、適切に保護管理することを目的とする。

２　情報システムの監視

システム管理者及び情報セキュリティ責任者は、情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

３　情報セキュリティポリシーの遵守状況の確認

システム管理者及び情報セキュリティ責任者は、情報セキュリティポリシーの遵守状況について、運用上支障が生じていないかについて確認を行わなければならない。

4　情報セキュリティ障害時の対応

情報セキュリティ障害が発生した場合には、システム管理者及び情報セキュリティ責任者は速やかに対応するとともに、再発防止の措置を講じなければならない。また、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、障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。

5　情報部門における業務継続計画との整合性の確保

本町が自然災害、大規模・広範囲にわたる疾病等に備えて情報部門における業務継続計画を策定する場合、情報セキュリティ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。

6　懲戒等処分

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、地方公務員法等に照らして、懲戒等処分の対象とする。

第9　評価・見直し等

1．目的

情報セキュリティポリシーは頻繁に更新されるものでないが、業務の形態の変更や技術革新、情報システムの再構築等によって改変される状況が予想されるため、見直し等の実施を確実にすることを目的とする。

2．改善措置

ア　システム管理者及び情報セキュリティ責任者は、当該部署の情報セキュリティが確保されていることを確認するため監査を実施し，その結果を受けて必要に応じ改善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、評価及び見直しが必要となる事象が発生した場合には、必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

用語一覧

情　報　セ　キ　ュ　リ　テ　ィ　対　策　基　準	
用　　語	用　　語　　の　　解　　説
無停電電源装置	瞬間的な電源電圧の低下(瞬断)や、突然の停電でデータの消失及び機器が損傷することを防ぐ予備電源装置。
USB メモリ	コンピュータに周辺機器を接続するための規格である USB 企画に準拠したものであって、USB コネクタに接続して使用する、持ち歩き可能な記録媒体。
ＩＣカード	個人認証や権限データをＩＣチップ（集積回路）に組み込んだカード。
目的外利用(提供)	・情報公開及び個人情報保護に関する条例第１４条により個人情報が適正に収集されていても収集の目的を超えた利用及び提供は、個人の尊厳の確保と町民の基本的人権の擁護に反するおそれがあるため原則として禁止するものであるが効率的な行政運営や町民のサービス向上のためにやむをえない場合があるので例外として認めている。 ・個人情報の目的を超えて、課内で利用することをいい、実施機関が明らかにした個人情報取扱事務の目的以外に当該実施機関内で別の事務の遂行のために利用することをいう。
外　部　提　供	他の課、国又は地方公共団体などに、個人情報を提供することをいう。
パターンファイル	不正プログラム対策ソフトが不正プログラムを発見するために使うファイル。
ライセンス	ソフトハウスがユーザーに与えるソフトウエアの利用許可。
バックアップ	プログラムやデータが壊れたり紛失する場合に備えて、同じファイルを作成したり、予備のディスク装置や磁気テープ記録装置にプログラムやデータを複写しておくこと。
アクセス	情報や情報システムに接触又は接続すること。
ソフトウエア	プログラムとほぼ同じ意味。プログラム以外にもコンピュータが扱うデータ（音楽、映像など）までを含めてソフトウエアと呼ぶこともある。
不正プログラム	データを壊したり、ほかのパソコンに勝手に侵入して危害を加えたり、大量のメールを送信して迷惑をかけるなど悪意のあるプログラム。「マルウエア」とも言う。
プログラム	コンピュータ（ハードウェア）を作動させるための手順・命令をコンピュータが理解できる形式で記述したもの。