市川三郷町情報セキュリティポリシー

平成　17 年　10 月　 1 日　　策定
平成　20 年　10 月　 1 日 全部改定
平成　27 年　10 月　 1 日 一部改定
平成　29 年　10 月　10 日 一部改定
令和　 3 年　 9 月　 6 日 一部改定
令和　 7 年　10 月　 6 日 一部改定

市川三郷町情報化推進委員会　了承

IT 社会の進展により情報の共有化、集積化、ネットワーク化が進み、市川三郷町(以下「本町」という。)においても情報システムは、効率的な行政運営や住民サービス提供の基盤となっています。

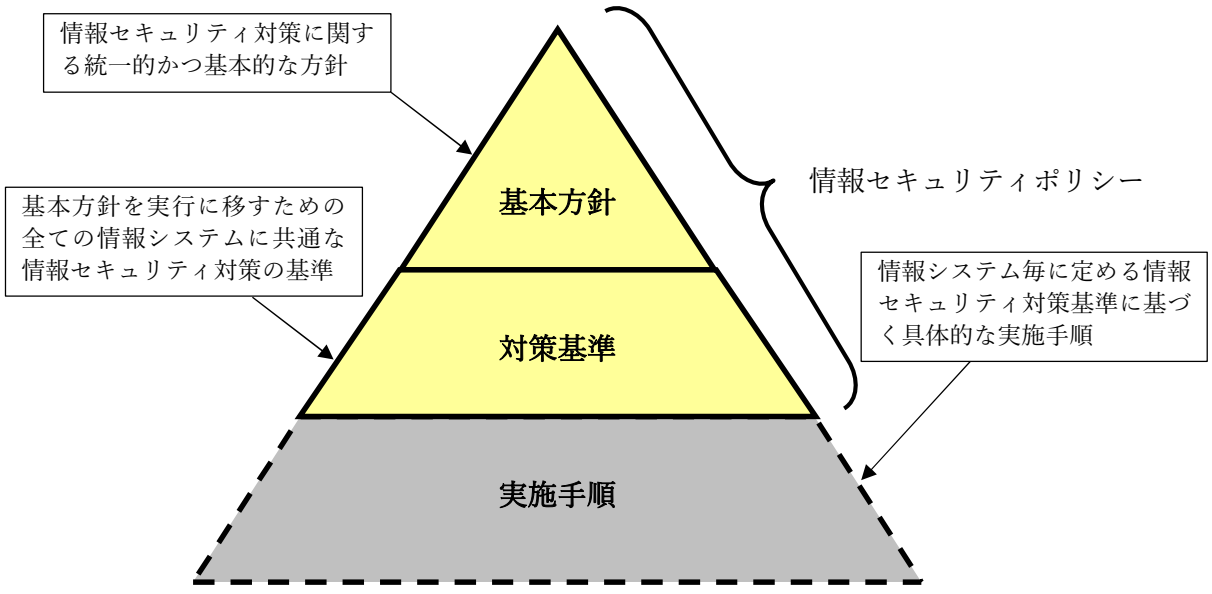
しかしながら、情報システムを利用した不正アクセスやマルウェア被害が大きな社会問題となっており、また同時に組織内部における不正操作や油断による情報の流出等のセキュリティ事故が発生する危険性も潜んでいます。

このような危険から、町民の貴重な個人情報や行政運営上の重要な情報及び情報システム(プログラム及び情報機器)等の情報資産を守るため、市川三郷町情報セキュリティポリシー(以下「本ポリシー」という。)を策定しました。

本ポリシーは、本町の情報セキュリティに対する統一的な行動基準を明確にするとともに、各職員が共通の正しい認識を持つことを目的としています。

本ポリシーは、情報セキュリティ基本方針と情報セキュリティ対策基準で構成されます。本ポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策として情報セキュリティ実施手順を策定します。(下図参照)

本ポリシー、情報セキュリティ対策基準、情報セキュリティ実施手順については、本町の現状分析を基に、個々具体的に対策を示したものであり、公開することにより情報セキュリティが脆弱になる恐れがあるため非公開とします。



本ポリシーは、高いセキュリティ水準を確保するため、継続的な運用を行い、更に評価・見直しを繰り返し、発展させていきます。

目　次

第１章　情報セキュリティ基本方針

1.　目的

本町の各情報システムが取扱う情報には、町民の個人情報、行政運営上重要な情報等、外部への漏えい、消失、破壊、改ざん、情報システムの停止等が発生した場合、極めて重大な結果を招くものが含まれている。

これらの情報及び情報を取り扱うシステムを様々な脅威から防御することは、事務の安定的な運営を図り、町民の財産、プライバシー等を守るため不可欠である。

また、情報技術の進歩に伴い、より高度で広範囲な行政の情報化が進められている。

本町がこれに対応していくためには、全ての情報システムの運用に対して十分な安全性を維持していくことが求められる。

この要求に答えるため、本町職員等が情報資産を安全に取り扱うための方針である情報セキュリティ基本方針(以下、「基本方針」という。)を定める。

基本方針は、これを職員等に浸透、普及、定着を図ることにより、取り扱われる情報資産の安全性を高め、町民からの信頼の維持向上に寄与するためのものである。

なお、基本方針は本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、本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。

(2)　情報システム

コンピュータ、ネットワーク及び電磁的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

本基本方針及び情報セキュリティ対策基準をいう。

(5)　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。

(6)　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。

(7)　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。

(8)　マイナンバー利用事務系(個人番号利用事務系)

個人番号利用事務(社会保障、地方税若しくは防災に関する事務)又は戸籍事務等に関わる情報システム及びデータをいう。

(9)　LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう(マイナンバー利用事務系を除く。)。

(10)　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11)　通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12)　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

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)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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

(2)　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、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、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

(3)　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

(4)　大規模・広範囲にわたる疾病による要因不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道共有の途絶等のインフラの障害からの波及等

4.　適用範囲

(1)　行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、地方公営企業、児童福祉施設とする。

(2)　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
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

5. 職員等の遵守義務

町長をはじめ、職員、非常勤職員及び臨時職員等(以下、「職員等」という。)及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって本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

本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

本町の所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実施する。

(3) 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN接続系においては、LGWANと接続する業務用システムとインターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、山梨県及び市町村のインターネットとの通信を集約した上で、山梨県情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ、サーバ室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリテイに関し、職員等及び外部委託事業者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。

(6)　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を講じる。

(7)　運用

　情報システムの監視、本ポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、本ポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8)　業務委託と外部サービス(クラウドサービス)の利用

　業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

　外部サービス(クラウドサービス)を利用する場合には、利用に係る規定を整備し対策を講じる。

　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

(9)　評価・見直し

　本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し、運用改善を行い、情報セキュリティの向上を図る。本ポリシーの見直しが必要な場合は、適宜本ポリシー及び情報セキュリティ実施手順の見直しを行う。

7.　情報セキュリティ監査及び自己点検の実施

　本ポリシーの遵守状況を検証するために、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、本ポリシー及び情報セキュリティ実施手順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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、本ポリシー及び情報セキュリティ実施手順を見直す。

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。

なお、情報セキュリティ対策基準は、公にすることにより本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。

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本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。