第１　東金市情報セキュリティ基本方針

1.1. 宣言

今日、市民生活の場に情報通信技術が急速に普及し、電子メールのやり取りや、ホームページの閲覧、電子商取引などが広く行われるようになり、経済面や生活面において様々な変化が起きています。

一方で、情報通信技術の利用に係る事故や犯罪、操作ミス、さらには、自然災害による情報システムの障害が発生すれば市民生活に多大な影響を与えます。

本市でも、行政サービスを提供するため、多くの業務において情報通信技術を活用しており、個人情報や行政運営上重要な情報などの多数の情報資産を保有しています。

これらの情報資産を様々な脅威から防ぐことは、市民の権利及び利益を守り、行政サービスを継続して提供するために必要不可欠です。

そこで、本市は、情報セキュリティ対策に次のとおり取り組むことを宣言します。

①情報セキュリティを確保するため、全庁的な組織体制を整備します。

②情報セキュリティ対策の統一的な基準として「東金市情報セキュリティ対策基準」を定め、それぞれの情報システムごとに「東金市情報セキュリティ実施手順」を定めます。

③保有する情報資産について、管理者を定め、適切に管理します。

④情報セキュリティ対策の重要性を認識させるため、職員に対して必要な教育を行います。

⑤情報セキュリティに関する事故が発生した場合又はそのおそれがあった場合に速やかに対応するため、緊急時対応計画を定めます。

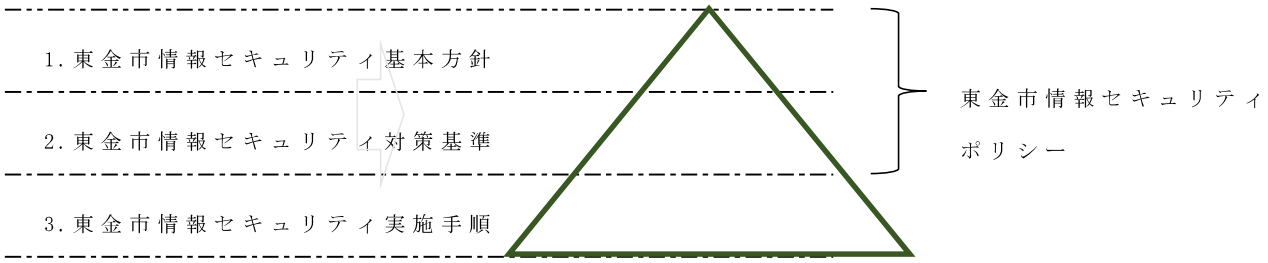
⑥情報セキュリティポリシーが遵守されていることを検証するため、監査及び自己点検を行います。

⑦情報セキュリティを取り巻く状況の変化及び監査結果を踏まえて、情報セキュリティポリシーを見直します。

⑧職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行において、情報セキュリティの関係法令並びに東金市情報セキュリティ基本方針、東金市情報セキュリティ対策基準及び東金市情報セキュリティ実施手順を遵守します。

1.2. 体系

東金市情報セキュリティポリシーの体系図



1.3. 情報セキュリティポリシーの公開範囲

本情報セキュリティポリシーは、公にすることにより本市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第１　東金市情報セキュリティ基本方針を除き非公開（守秘義務契約を締結した委託事業者を除く。）とする。

1.4. 情報セキュリティポリシーの目的

本情報セキュリティポリシーは、本市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、本市が実施する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。

1.5. 定義

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　マイナンバー系

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。※その他の文書等においてＭＮＢ系、マイナンバー利用事務系、個人番号利用事務系と表記されることもある。

⑹　ＬＧＷＡＮ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。）。※その他の文書等においてＬＧＷＡＮ接続系と表記されることもある。

⑺　インターネット系

インターネットメール等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。※その他の文書等においてＩＴＮ系、インターネット接続系と表記されることもある。

⑻　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。

⑼　Ｗｅｂ会議サービス

専用のアプリケーションやＷｅｂブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器同士で通信を行うもの（テレビ会議システム等）は含まない。

⑽　外部サービス（クラウドサービス）

外部の事業者等本市以外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において本市の情報が取り扱われる場合に限る。

⑾　クラウドサービス提供者

クラウドサービスを提供する事業者をいう。なお、クラウドサービスを利用して本市に向けて独自のサービスを提供する事業者は含まない。

⑿　情報セキュリティ対策

情報セキュリティの実現を目的として行う対策をいう。

⒀　情報セキュリティインシデント

情報セキュリティを脅かす、又は脅かすおそれのある事象をいう。

⒁　法令等

法令、条例又はこれらに基づく規則（地方自治法（昭和２２年法律第６７号。）第１３８条の４第２項に規定する規程及び地方公営企業法（昭和２７年法律第２９２号）第１０条に規定する企業管理規程を含む。）をいう。

⒂　電磁的記録媒体

電磁的方式で作られた記録に係る記録媒体をいう。

⑯　可搬記憶媒体

電磁的記録媒体の一つであって、電子計算機から容易に取り外すことのできる記憶媒体（光ディスク等（光ディスク、磁気ディスク又は磁気テープをいう。）、ＵＳＢメモリ又は外付けハードディスクドライブその他これに類するものをいう。

⑰　パソコン等

パソコン、サーバ、モバイル端末及び電磁的記録媒体その他の機器により構成される電子計算機をいう。

⑱　サーバ等

ネットワークを介して、パソコンからの命令による情報システムの利用やデータ共有等の特定の機能やデータを提供する側の電子計算機及びその周辺機器をいう。

⑲　多要素認証

情報システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。

1.6. 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を行う。

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、重要情報の詐取、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員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、水道供給の途絶等のインフラの障害からの波及等

1.7. 適用範囲

本情報セキュリティポリシーを適用する対象範囲は次のとおりとする。

⑴　対象となる機関

市長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、公営企業管理者及び議会（以下「対象機関」という。）とする。

⑵　対象となる職員

地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職に属する市の職員とする。

⑶　対象となる事業者

対象機関の情報資産に係る業務を委託する場合又は地方自治法（昭和２２年法律第６７号）第２４４条の２第３項に規定する指定管理者に行わせる場合の委託事業者又は指定管理者とする。

委託事業者及び指定管理者については、本セキュリティポリシーのうち「職員」とあるものを当該者の委託及び指定管理の内容に応じて読み替えて適用するものとする。

⑷　対象となる情報資産

本セキュリティポリシーが対象とする情報資産は次のとおりとする。ただし、教育情報セキュリティポリシーに関するガイドライン（平成２９年１０月１８日策定、文部科学省）に定める情報資産に該当するものは除く。

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、情報システム及びクラウドサービスで取り扱う情報（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

1.8.職員の義務

職員は、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。

1.9.情報セキュリティ対策

脅威から情報資産を保護するために、次の情報セキュリティ対策を行うものとする。

(1)組織体制

東金市の情報資産について、 情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

(2)情報資産の分類と整理

東金市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実施する。

(3) 情報システム全体の強靭性の向上

情報システムに対し、次の対策を講じる。

ア　マイナンバー系においては、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。

イ　ＬＧＷＡＮ系の情報システムと、インターネット系の情報システムとの通信経路を分離した上で、安全が確保された通信を必要最低限許可する。

ウ　インターネット系においては、情報セキュリティ対策として、千葉県が構築する自治体情報セキュリティクラウドを利用する。

(4)物理的セキュリティ

サーバ、情報システム室、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。

(6) 技術的セキュリティ

コンピュータ等の管理、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、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。この場合において、情報資産に対するセキュリティ侵害発生時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

ア　業務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ずる。

イ　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。

ウ　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。

1.10. 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。

1.11. 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、情報セキュリティポリシーの見直しを行う。

1.12. 情報セキュリティ対策基準の策定

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ものとする。

1.13. 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。