葛城市情報セキュリティ基本方針

平成 16 年 10 月 1 日　制定

令和 8 年 3 月 31 日　改定

葛城市

1 目的

(1) 葛城市(以下「本市」という。)の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。従って、これらの情報及び情報を取り扱う情報システムが高度な安全性を有することは、住民の財産やプライバシー等を守ると共に、住民への行政サービスの安定的かつ効率的な提供のためにも必要不可欠である。そのため、本市の情報資産の機密性、完全性及び可用性の維持を目的とし、内部部局、行政委員会、議会事務局及び各地方公営企業が共同して情報セキュリティポリシーを定めることとする。

(2) 情報セキュリティポリシーを構成する情報セキュリティ基本方針は、本市の情報資産に関する情報セキュリティ対策を策定する指針として、情報セキュリティポリシーの維持・管理に関する基本的な考え方、情報セキュリティ対策の基本原則等を定めるものとする。

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。なお、本市が利用するクラウドサービスを含む。

(3) 情報資産

ネットワーク、情報システム及びこれらで取り扱う全ての情報、関連文書等をいう。

(4) 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。

(5) 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。

(6) 職員等

本基本方針が適用される組織が所掌する情報資産に関する業務に携わる全ての常勤、非常勤及び臨時等を含む職員をいう。

(7) 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。

(8) 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。

(9) 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。

（10） 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。

（11） LGWAN接続系

人事給与、財務会計及び文書管理等 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。）。

（12） 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。

（13） 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。

（14） 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。

（15） クラウドサービス

クラウドコンピューティング技術を用いた、インターネット等のネットワークを経由して提供されるサービスをいう。

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

（6） サプライチェーン（業務委託先やクラウドサービス提供者等）を経由したサイバー攻撃や障害等

4 適用範囲

(1) 行政機関の範囲

① 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、議会事務局及び各地方公営企業とする。

② 情報セキュリティポリシーは、①で規定する各行政機関に関する業務に従事する全ての職員等及び委託事業者に適用する。

(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し、(1)で規定する各行政機関が所掌する全ての情報資産に適用する。

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

(1) 市長及び各行政機関の長をはじめとする職員等及び委託事業者は、情報セキュリティの重要性について共通の認識を持つと共に、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。

(2) 職員等及び委託事業者は、情報システムの企画、開発、運用及び利用において、事故や障害が発生しないよう十分注意する義務を負う。

(3) 職員等及び委託事業者は、情報システムの企画、開発、運用及び利用に際して知り得た情報などを業務上必要な場合を除き、第三者に開示・提供・漏洩してはならない義務を負う。

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

本市の情報資産について、情報セキュリティ対策を継続的に推進・管理するための全庁的な組織体制を確立する。また、最高情報セキュリティ責任者(CISO)を設置し、情報セキュリティ対策に関する権限及び責任を明確にする。

(2) 情報資産の分類と管理

本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。

② LGWAN 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、無害化通信等の安全な通信を実施する。

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、奈良県自治体情報セキュリティクラウドの導入を実施する。

（4） 物理的セキュリティ

情報システムを設置する施設への不正な立ち入り、情報資産の盗難、損傷等からこれらを保護するために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、全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等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

情報資産を外部からの不正アクセス等の脅威から適切に保護するため、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、情報セキュリティ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、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し、緊急時対応体制（CSIRT）を整備する。

（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、利用にかか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

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行

う。

7 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、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を見直す。

8 罰則

(1) 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に対して、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) 情報セキュリティポリシーに違反した委託業者に対しては、情報資産の利用制限、又は別途定めるところにより当該委託業者と協議し適切な処置を講じるものとする。

9 情報セキュリティ対策基準の策定

上記６及び７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市の行政運営に重大な支障を及ぼす恐れがある情報で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非公開とする