葛城市議会情報セキュリティ基本方針

1　目的

この基本方針は、葛城市議会(以下「本市議会」という。)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、必要な事項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、本市議会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)　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)　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、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)　適用対象の範囲

①　この基本方針が適用される対象は、本市議会が保有する情報資産の利用者（以下「利用者」という。）とする。ただし、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）の適用範囲となるものは除く。

(2)　情報資産の範囲

この基本方針が対象とする情報資産は次のとおりとする。ただし、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）の適用範囲となるものは除く。

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　利用者の遵守義務

(1)　利用者は、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関係法令、この基本方針、本市議会が定める規程等を遵守しなけれ

ばならない。

(2)　利用者は、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)　利用者は、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)　情報資産の分類と管理

本市議会の保有する情報資産について機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類し、当該分類に応じた情報セキュリティ対策を講じる。

(2)　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、対策を講じる。

(3)　物理的セキュリティ

情報システムを設置する場所への不正な立ち入りの禁止等、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。

(4)　人的セキュリティ

情報セキュリティに関し、利用者が遵守すべき事項を定めるとともに、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

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。

(6)　運用

情報システムの監視、この基本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等、この基本方針の運用面の対策を講じるものとする。

(7)　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、利用に関するルールを整理し対策を講じる。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する。

(8)　評価・見直し

この基本方針の遵守状況を検証するため、定期的又は必要に応じて自己点検等を実施し、運用改善を行い、情報セキュリティの向上を図る。この基本方針の見直しが必要な場合は、適宜この基本方針の見直しを行う。

7　情報セキュリティ基本方針の見直し

自己点検等の結果、この基本方針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、この基本方針を見直す。

附　則

この基本方針は、令和８年６月２４日から施行する。