第１章　情報セキュリティ基本方針

１．目的

この基本方針は、本市が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下「対象資産」という。）について、機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティに関する基本的な事項を定めることにより、行政の適正かつ円滑な運営を図り、もって市政に対する市民の信頼を確保することを目的とする。

２．定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

(2)　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。

(3)　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(4)　情報資産

情報システムで取扱う情報で、開発及び運用に係るものを含むすべての情報をいう。

(5)　情報セキュリティ

対象資産の機密性、完全性及び可用性を維持することをいう。

(6)　情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

(7)　機密性

対象資産にアクセスすることを認められた者だけが、対象資産にアクセスできる状態を確保することをいう。

(8)　完全性

対象資産が破壊、改ざん、消去又は不正なデータがない状態を維持し、データの正当性、正確性、一貫等を確保する事をいう。

(9)　可用性

対象資産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、対象資産にアクセスできる状態を確保することをいう。

(10) 特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第２条に規定する、個人番号をその内容に含む個人情報ファイルをいう。

(11) 個人番号利用事務

番号法第２条に規定する、個人番号を利用して処理する事務をいう。

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。この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　人による脅威（故意）

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対象資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2)　人による脅威（過失）

対象資産の無断持ち出し、無許可ソフトウェアの使用等の規程違反、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対象資産の漏えい・破壊・消去等

(3)　災害による脅威

地震、落雷、火災等の災害によるサービス及び業務の停止、対象資産の消失等

(4)　必要資源の不足、故障等による脅威

災害の影響又はその他の原因による電力、通信、水道の途絶、交通機能の麻痺や大規模・広範囲にわたる疾病の蔓延による要員の不足、機器の故障等によるサービスや業務の停止、システム運用の機能不全等

４．適用範囲

(1)　行政機関及び職員の範囲

この基本方針の適用範囲は、内部部局、教育委員会、選挙管理委員会、公平委員会、監査委員会、農業委員会、固定資産評価審査委員会、上下水道事業管理者及び議会事務局（以下「天理市」という。）が保有する対象資産、対象資産に関する事務に携わる全ての職員、非常勤職員、臨時職員、労働者派遣事業により本市の事務に携わる者（以下「職員等」という。）及び委託事業者とする。

(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。

ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

イ　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）。

ウ　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

エ　職員が職務上作成又は取得し、保有している文書、図面及び電磁的記録

オ　対象資産のうち、学校の用に供する教育財産は除く

５．遵守義務

上記４に規定する者は、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。

６．情報セキュリティ対策

上記３の脅威から対象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ものとする。

(1)　組織体制

情報セキュリティ対策を推進する全庁的な組織体制の確立する。

(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、当該分類に基づく情報セキュリティ対策を行う。

(3)　物理的セキュリティ

保管施設、通信回線、コンピュータ等の管理について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、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。

(5)　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。

(6)　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情報セキュリティの確保等、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。対象資産へのセキュリティ侵害が発生した場合等に、迅速かつ適切に対応

するための緊急時対応計画を策定する。

７．情報セキュリティに関する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、必要に応じて情報セキュリティに関する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及び改訂

情報セキュリティに関する監査及び自己点検の結果又は情報セキュリティに関する状況の変化に対応するため、定期的に情報セキュリティポリシーの見直しを行い、必要に応じて改定する。

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。

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、情報セキュリティに関する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。

なお、情報セキュリティ実施手順は、セキュリティ確保のため非公開とする。

１１．違反規定

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、地方公務員法第29条に規定する懲戒処分の対象となるほか、情報資産の利用に制限を加えることができる。

附　則

この基本方針は、平成 16 年 7 月 1 日から施行する。

この基本方針は、平成 20 年 6 月 1 日から施行する。

この基本方針は、平成 23 年 3 月 2 日から施行する。

この基本方針は、平成 27 年 12 月 28 日から施行する。