鹿沼市セキュリティポリシー基本方針

1　目的

地方自治体は、その責務を果たすために必要な情報の収集・保有・利用において、その安全性を確保し、適切に保護しなければならない。この目的を達成するため、鹿沼市情報セキュリティポリシー（以下「ポリシー」という。）を策定する。

2　定義

(1)「情報セキュリティポリシー」とは、本基本方針及び情報セキュリティ対策基準をいう。

(2)「情報システム」とは、コンピュータ及びその周辺機器、ソフトウェア、ネットワーク等で構成され、これらの組合せにより業務処理を行うものをいう。

(3)「ネットワーク」とは、情報を共有又は送受信するための通信網及びその機器構成をいう。

(4)「情報資産」とは、次のものをいう。

ア　情報システム上で取扱う情報及びこれらを印刷した文書、記録媒体

イ　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

ウ　情報システムに関する設備、記録媒体

(5)「情報セキュリティ」とは、情報の「機密性」、「完全性」及び「可用性」が確保されている状態をいう。

ア「機密性」とは、情報にアクセスすることを認められたものだけが、情報にアクセスできる状態を確保することをいう。

イ「完全性」とは、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。

ウ「可用性」とは、許可された利用者が、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。

(6)「脅威」とは、情報セキュリティを脅かす様々な危険性（リスク）をいう。

3　適用範囲及び対象者

ポリシーは、本市の全ての情報システム及び情報資産を適用範囲とし、それを取り扱う全ての者を対象者とする。

4　組織及び管理体制

ポリシーの適正な管理と推進のため、鹿沼市情報セキュリティ対策委員会（以下「委員会」という。）を設置する。委員会の所掌業務は、次のとおりとする。

(1) 情報セキュリティ対策の立案に関すること

(2) 情報セキュリティ対策の遵守状況の確認に関すること

(3) 情報セキュリティ研修に関すること

(4) 情報セキュリティ監査に関すること

5　管理職員及び職員等の役割

(1) 本市の管理職員は、自らの責任と権限において率先して情報セキュリティ対策を推進するための体制を確立し、又はその取組に協力する。

(2) 職員等は、情報セキュリティの重要性について共通の認識を持ち、ポリシー及び関係法令等を遵守し、情報セキュリティの確保に努める。

6　外部委託

本市の情報システム及び情報資産の管理や処理業務を業者等に委託する際は、ポリシーの遵守を義務付けなくてはならない。

7　情報セキュリティ対策

情報セキュリティの維持を妨げる脅威から情報資産を保護するために、以下の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講じる。

(2)物理的セキュリティ対策

サーバ等、情報システム室等、通信回線等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。

(3)技術的セキュリティ対策

情報資産をコンピュータウィルスや不正アクセス、改ざん行為等から保護するため、ウィルス対策ソフトの導入やアクセス制御など、技術的対策を講じる。

(4) 人的セキュリティ対策

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、十分な教育及び訓練を行う等の人的な対策を講じる。

(5) 運用セキュリティ対策

情報システム利用状況の監視や分析、ポリシー遵守状況の確認、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における対策を講じる。

(6) 緊急時対策

システム障害や情報漏えい事故等の緊急事態が発生した際は、迅速かつ適切な対応を行う。

8　監査及び自己点検

ポリシーの遵守の状況及び基準の検証を行うため、委員会は定期又は必要に応じた情報セキュリティ監査及び自己点検を実施する。

9　ポリシーの見直し

委員会は、情報セキュリティ監査及び自己点検等の結果等に基づき、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新たな課題や状況への対応が必要となった場合、ポリシーの見直しを行う。

10　情報セキュリティ対策基準の策定

上記７、８及び９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については、公にすることにより本市のセキュリティ対策の実施に重大な支障を及ぼすおそれがあるため、原則非公開とする。

11　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。なお、情報セキュリティ実施手順については、公にすることにより本市のセキュリティ対策の実施に重大な支障を及ぼすおそれがあるため、原則非公開とする。