鎌ケ谷市情報セキュリティ基本方針

第１　目的

本基本方針の目的は、鎌ケ谷市が保有する情報資産のセキュリティを確保する上で必要となる対策の基本的な方針を定めることである。

なお、本基本方針は、鎌ケ谷市におけるセキュリティ対策の根幹であり、本基本方針に基づき定めたあらゆる規程は、本基本方針の定めに違反してはならない。

第２　位置付け

本基本方針は、鎌ケ谷市が所管する情報資産に関するセキュリティ対策について、総合的かつ体系的に取りまとめたものであり、セキュリティ対策の頂点に位置するものである。

第３　対象とする脅威

情報資産に対する次の脅威を想定し、セキュリティ対策を実施する。

１　情報資産の意図的取扱いを要因とするもの

不正アクセス、不正プログラムによる攻撃、サービス不能攻撃等のサイバー攻撃並びにセキュリティ管理区域及び執務スペースへの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、改ざん、破壊、削除、否認、なりすまし等。

２　情報資産の非意図的取扱いを要因とするもの

情報資産の許可なき持出し等の規定違反、設計又は開発の不備、プログラム上の欠陥、設定又は操作の誤り、保守対応の不備、内部監査又は外部監査の不備、委託管理の不備、誤った取扱いによる機器の損壊、その他総合的管理体制の欠陥等、非意図的要因による情報資産の漏えい、改ざん、破壊、削除等。

３　インフラ障害を要因とするもの

経年劣化等による機器の故障並びに電気、通信等のインフラからの障害の波及等。

４　災害を要因とするもの

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。

５　組織体制の不備又は不足を要因とするもの

大規模、広範囲にわたる疾病等による人員不足に伴うシステム運用の機能不全等。

第４　適用範囲

１　行政機関の範囲

本基本方針が適用される行政機関は、本市の市長部局、議会、行政委員会及び消防本部とする。

２　利用者等の遵守義務

利用者等は、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本基本方針を遵守しなければならない。また、情報セキュリティ対策基準及び情報セキュリティ実施手順が策定されている場合は、併せてその規定を遵守しなければならない。

第５　セキュリティ対策

対象とする脅威から情報資産を保護するために、次のセキュリティ対策を講じる。

１　組織体制

鎌ケ谷市の情報資産について、セキュリティ対策を推進する全庁的な組織体制を確立する。

なお、緊急時対応計画を策定し、これに基づき、情報資産に対する被害が発生した場合等に迅速かつ的確に対応する。

２　情報資産の分類と管理

鎌ケ谷市の保有する情報資産を、機密性、完全性及び可用性を踏まえ、対象とする脅威による被害を受けた場合に想定される影響の大きさに基づき分類し、当該分類に基づき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

情報システム全体を構成する三層の分類毎に、次の対策を講じる。

個人番号利用事務系は、原則として、LGWAN 接続系、インターネット接続系等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、情報資産の漏えいを防ぐ。

LGWAN 接続系は、原則として、インターネット接続系と通信できないようにした上で、端末からの電子データの持出しを制限する。なお、LGWAN 接続系及びインターネット接続系間で通信する場合には、必要な通信のみを許可し、電子データに対して無害化処理を施す。

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、高度なセキュリティ対策を実施する。都道府県と市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

4　物理的安全管理措置

サーバー等重要機器に対する温度、湿度、災害等の影響の除去、ネットワーク機器に対する被覆保護、端末の盗難防止、セキュリティ管理区域の入退室管理等により、物理的な対策を講じる。

5　人的安全管理措置

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　技術的安全管理措置

情報資産管理、アクセス制御、アクセス権設定、不正プログラム対策、不正アクセス対策等の技術的な対策を講じる。

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、委託及び外部サービスの利用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を運用する上で必要となる対策を講じる。

8　委託等

委託を行う場合、外部サービスを利用する場合等は、原則として、情報セキュリティポリシーに基づきセキュリティ要件を明記した契約を締結し、委託の相手方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。

ソーシャルメディアサービスを利用する場合等、文書による契約の締結が困難な場合は、職員等に責任者を定め、情報セキュリティポリシーに基づき、そのサービスの利用に関する規程を整備する。

第6　評価及び見直し

1　監査及び自己点検

情報セキュリティポリシーの遵守状況を検証するため、監査及び自己点検を実施し、その結果を踏まえて改善活動を行い、セキュリティの向上を継続する。

2　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の見直し

監査又は自己点検の結果、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の見直しが必要となった場合及びセキュリティに関する状況の変化に対応するため新たな対策が必要になった場合には、これを見直す。

第７ 情報セキュリティ対策基準の策定

本基本方針に基づき、上記のセキュリティ対策を実施するための具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準を必要に応じて策定する。

第８ 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、セキュリティ対策を実施するためにその具体的な手順を明示する必要がある場合は、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、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。