大崎市情報セキュリティ基本方針

平成18年3月31日　策定

大崎市

大崎市情報セキュリティ基本方針

目次

大崎市情報セキュリティ基本方針

平成18年３月31日

序　大崎市情報セキュリティポリシーの構成

大崎市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は，本市が所掌する情報資産に関する情報セキュリティ対策について，総合的，体系的かつ具体的に取りまとめたものであり，情報セキュリティ対策の頂点に位置付けられるものである（図１参照）。

情報セキュリティポリシーは，本市が所掌する情報資産に関する業務に携わる職員等に浸透，普及，定着されるものであり，安定的な規範であることが求められる。しかしながら一方では，技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。

このようなことから，情報セキュリティポリシーを一定の普遍性を備えた部分と情報資産を取り巻く状況の変化に依存する部分に分けて策定することとした。

具体的には，情報セキュリティポリシーを「大崎市情報セキュリティ基本方針」及び「大崎市情報セキュリティ対策基準」の２階層に分け，それぞれを策定することとする。また，大崎市情報セキュリティ対策基準に基づき，情報システム毎の具体的な情報セキュリティ対策の実施手順として「大崎市情報セキュリティ実施手順」を策定することとする。

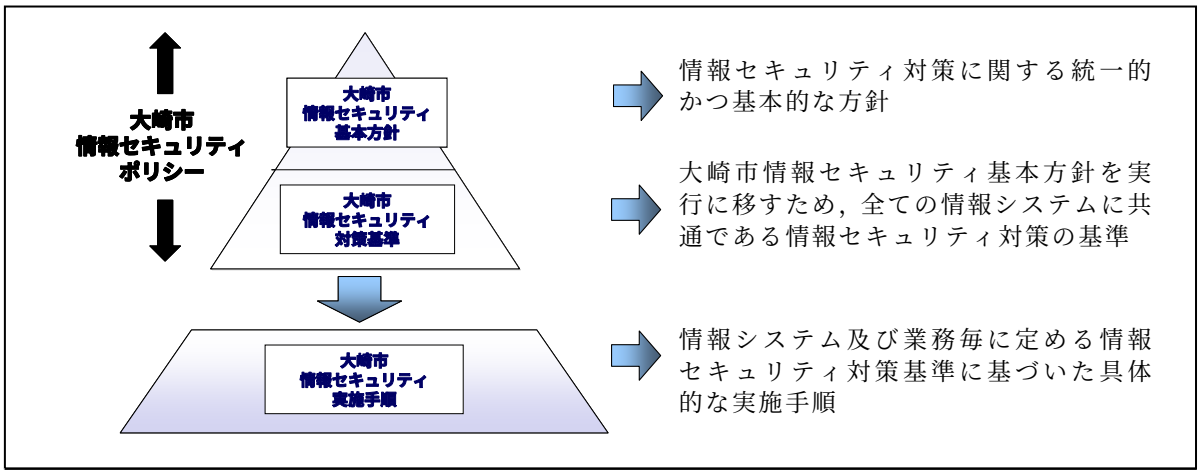

図１　大崎市情報セキュリティポリシーの位置付け

大崎市情報セキュリティ基本方針

１　目的

本市が取り扱う情報には，市民の個人情報をはじめとして，行政運営上重要な情報等，漏洩や破壊等が発生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。

したがって，情報技術を活用した業務が増加している中で，本市の情報資産を様々な脅威から防御することが，市民の財産・プライバシー等を守るためにも，また，行政の安定的な運営のためにも必要不可欠である。ひいては，このことが市民に対する信頼の確保に寄与するものである。

また，近年のいわゆるＩＴ革命の進展により，電子商取引の発展や電子自治体の構築が現実のものとなっており，本市が電子自治体を構築するためにも，情報システムが高度な安全性を有することが不可欠である。

このため，本市の情報セキュリティポリシーを定め，情報資産の機密性，完全性及び可用性（※注）を維持するための対策（情報セキュリティ対策）を講ずる。

このうち，大崎市情報セキュリティ基本方針においては，本市の情報セキュリティ対策の統一的かつ基本的な方針として，情報セキュリティポリシーの対象，位置付け等を定めるものとする。

（注）　国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）

・機密性（confidentiality）

情報にアクセスすることが許可された者だけがアクセスできることを確実にすること。

・完全性（integrity）

情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

・可用性（availability）

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

（１）　情報資産

情報システムで取り扱う全ての情報及び機器をいう。

ただし，情報の重要性に鑑み，紙等の有体物に出力された情報を含む。

（２）　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。

（３）　情報システム

電子計算機（ネットワーク，ハードウェア及びソフトウェア）及び記録媒体で構成され，処理を行う仕組みをいう。

（４）　ネットワーク

電子計算機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）及び記録媒体で構成され，処理を行う仕組みをいう。

（５）　通信回線装置

情報システムのうち，ネットワークを構成するケーブル及びその構成機器（ハードウェア及びソフトウェア）をいう。

（６）　ハードウェア

電子的にデータを処理する機能を持ち，事務処理に使用する機器をいう。

（７）　ソフトウェア

ハードウェア上で稼働するプログラム等をいう。

（８）　記録媒体

電子計算機に使用される光ディスク，磁気ディスク，磁気テープその他これらに類するものをいう。

（９）　サーバ

情報システムのうち，ネットワーク上においてファイル管理，印刷等の機能を提供するために設置される機器をいう。

（10）　アクセス権限

情報資産を利用することのできる範囲をいう。

（11）　行政情報

職員が職務上作成又は取得した情報で，その記録媒体の形態に関わらず組織的に管理しているものをいう。

（12）　個人情報

行政情報のうち，個人に関する情報で，特定の個人が識別され，又は識別され得るものをいう。

３　対象範囲

情報セキュリティポリシーの対象範囲は，次に掲げるものとする。

（１）　対象となる組織

市長，公営企業管理者，教育委員会，選挙管理委員会，公平委員会，監査委員，農業委員会，固定資産評価審査委員会及び議会とする。

（２）　対象となる情報

（１）に定める組織において取り扱う情報資産とする。

（３）　対象者

（１）に定める組織に属する職員（非常勤職員及び臨時職員を含む。以下「職員」という。）及び（２）に定める対象となる情報資産の取り扱いを委託された者（以下「外部委託事業者」という。）とする。

（４）　他の制度との調整

対象となる情報について，他の法令又は条例の定めるところにより，取扱いが別に定められている場合は，当該法令又は条例に基づき取り扱うものとする。

４　職員及び外部委託事業者の義務

職員及び外部委託事業者は，情報セキュリティの重要度について共通の認識を持つとともに，業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

５　情報セキュリティ管理体制

本市の情報資産について，適切に情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

６　情報資産の分類

情報資産をその重要度に応じて分類し，それに応じた情報セキュリティ対策を行うものとする。

７　情報セキュリティ対策

（１）　情報資産への脅威

情報セキュリティポリシーを講ずる上で，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると，特に認識すべき脅威は次のとおりである。

ア　部外者の侵入による情報資産の破壊・盗難，不正アクセス又は不正操作による情報資産の破壊・盗聴・改ざん・消去等

イ　職員又は外部委託事業者による情報資産の持ち出し，誤操作，アクセスのための認証情報（ID及びパスワード等）の不適切管理，不正アクセス又は不

正行為による破壊・盗聴・改ざん・消去等，搬送中の事故等による情報資産の盗難又は規定外の端末接続によるデータ漏洩等

ウ　コンピュータウイルス，地震，落雷，火災等の災害並びに事故，故障等による行政サービス及び業務の停止

（２）　情報セキュリティ対策の実施

（１）で示した脅威から情報資産を保護するために，次の情報セキュリティ対策を講ずるものとする。

ア　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り，情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

イ　人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに，全ての職員及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底するために，十分な教育及び啓発に必要な対策を講ずる。

ウ　技術的セキュリティ対策

情報資産を不正アクセス等から適切に保護するため，情報資産へのアクセス制御，ネットワーク管理等の技術面の対策を講ずる。

エ　運用

システム開発等の外部委託，ネットワークの監視，情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。また，緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

８　情報セキュリティ対策基準の策定

大崎市情報セキュリティ基本方針を実行に移すため，遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。

そのため，大崎市情報セキュリティ基本方針を実行に移す上で，全ての情報システムに共通する情報セキュリティ対策の基準を策定する。

９　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を実施するために，情報システム及び業務毎に実施手順を具体的に定めていく必要がある。そのため，情報セキュリティ対策基準に基づき，情報資産に対する脅威及び情報資産の重要度に対応する，大崎市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のある機密情報を含むことから非公開とする。

10　法令等の遵守

職員及び外部委託事業者は，職務の遂行において，情報セキュリティに関係する法令等を遵守しなければならない。

11　情報セキュリティポリシーの違反行為時における対応

情報セキュリティポリシーの違反行為に対しては，その重大性，発生した事件，事故等の状況等に応じて各関連法令等の罰則の対象となるものとする。

12　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守され，情報セキュリティが維持されていることを検証するため，定期的に情報セキュリティ監査を実施するものとする。

13　評価及び見直しの実施

情報セキュリティ監査の結果等により，情報セキュリティポリシーに定める事項及び情報セキュリティ対策の有効性等について評価するとともに，情報セキュリティを取り巻く状況の変化に対応するため，適宜情報セキュリティポリシーの見直しを実施するものとする。