岡崎市情報セキュリティポリシー

序　岡崎市情報セキュリティポリシーの構成

岡崎市情報セキュリティポリシー（以下「セキュリティポリシー」という。）とは、本市が保有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る。

セキュリティポリシーは、本市が所掌する情報資産を取り扱う職員（会計年度任用職員を含む。）及び委託事業者（従事者及び派遣労働者を含む。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。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へ柔軟に対応することも必要である。

このようなことから、セキュリティポリシーを、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「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、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」を策定することとする。（下表参照）

セキュリティポリシーの構成

文　書　名		内　容
セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づく情報セキュリティ対策を実施するための具体的な手順

第１章　情報セキュリティ基本方針

１　目的

この情報セキュリティ基本方針は、本市が保有する情報資産を様々な脅威から防御し、その機密性、完全性及び可用性（※注）を確保するため、組織的かつ計画的に取り組むための統一的な方針であり、情報セキュリティを実践するにあたっての基本的な考え方及び方策を定め、市民の財産、プライバシー等を守り、また、業務を継続的に安全に行うことで市民からの信頼の維持向上に寄与することを目的とする。

（※注）：国際標準化機構（ISO）が定めるもの（IS07498－２：1989）

機密性（confidentiality）	情報にアクセスすることが認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　用語の定義

⑴　ネットワーク

コンピュータを相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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。

⑶　情報資産

情報システム及び情報システムの開発と運用に係る全ての情報並びに情報システムにより取り扱われる全ての情報をいう。

⑷　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　職員の義務

本市が所掌する情報資産に関する業務に携わる職員（会計年度任用職員を含む。以下同じ。）は、情報セキュリティの重要性について共通の認識をもつとともに、業務の遂行に当たってセキュリティポリシーを遵守する義務を負う。

４　管理体制

情報資産の統一的な情報セキュリティを確保するため、全庁的な組織体制を整備する。

5　情報資産の管理

情報資産については、内容に応じて適切な管理を行う。

6　情報資産への脅威

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や発生した場合の影響を考慮するものとする。特に認識すべき脅威は以下のとおりである。

⑴　権限のない者の故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し、盗難、改ざん、消去、機器及び電磁的記録媒体の盗難等

⑵　職員及び委託事業者による意図しない操作、故意の不正アクセス又は不正操作によるデータ及びプログラムの持ち出し、盗難、改ざん、消去、機器及び電磁的記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏えい等

⑶　地震、落雷、火災等の災害や事故、故障等

7　情報セキュリティ対策

本市の情報資産を情報資産への脅威（上記６）から保護するため以下の対策を講ずるものとする。

⑴　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及び遵守すべき事項を定め、職員に対する周知徹底を図るため、教育及び啓発を行う。

⑵　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、情報資産への損傷及び利用の妨害等から保護するために物理的な対策を講ずる。

⑶　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・暗号化処理等の技術的な対策を講ずる。

⑷　運用等におけるセキュリティ対策

情報システムの監視、情報セキュリティ対策の遵守状況の確認等の対策を実施する。また、緊急事態において迅速な対応を可能とするための対策を講ずる。

8　情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づき、情報セキュリティ対策を実施するに当たって必要となる基本的な要件を明記した情報セキュリティ対策基準を定める。

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基準に基づき、主要な情報システム等について情報セキュリティ対策を具体的に実施するために、情報セキュリティ実施手順を定める。

10　情報セキュリティ監査及び自己点検の実施

セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

11　評価及び見直しの実施

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評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜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を実施する。