逗子市情報セキュリティ基本方針

（目的）

1　逗子市情報セキュリティ基本方針（以下「基本方針」という。）は、市が所管する情報資産の機密性、完全性及び可用性を確保するため、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針並びに情報資産の安全管理対策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、市における情報資産の管理を徹底することを目的とする。

（適用範囲）

2　この基本方針の適用範囲は、市長部局、消防、議会、教育委員会（学校を除く。）、選挙管理委員会及び監査委員とする。

（対象者）

3　この基本方針の対象者は、市の機関に配置されるすべての者（以下「職員等」という。）及び市の事務事業の委託を受けた者（以下「受託者」という。）とする。

（用語の定義）

4　この基本方針において次に掲げる用語の意義は、次のとおりとする。

⑴　情報資産　市が所管する情報及び情報システムをいう。

⑵　情報　市が所管するすべての情報をいう。

⑶　情報システム　ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、情報処理を行う仕組みをいう。

⑷　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及びその構成機器をいう。

⑸　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。

⑹　機密性　情報にアクセスすることが認められた者だけがアクセスできることを確実にすることをいう。

⑺　完全性　情報及び処理の方法が正確であること及び完全であることを保護することをいう。

⑻　可用性　アクセスの権限のある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をいう。

（管理体制）

5　市が所管する情報資産を保護するため、情報セキュリティ対策を推進及び管理するための組織体制を確立する。

（情報資産の分類及び管理）

6　情報資産については情報の機密性、完全性及び可用性を踏まえた情報資産の分類を行い、その重要性に応じて、適切な管理を行うものとする。

（情報資産への脅威）

7　情報資産に対して想定される脅威は、その発生度合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。

⑴　部外者による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、盗聴、改ざん、消去並びに機器及び記録媒体の盗難、破壊等

⑵　職員等及び受託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、盗聴、改ざん及び消去並びに機器及び媒体の盗難、破壊等

⑶　地震、落雷、火災等の災害、事故及び故障による行政サービス及び業務の停止

（情報セキュリティ対策）

8　前項の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ものとする。

⑴　物理的セキュリティ対策　情報システムの設置場所、情報の保管場所等への不正な立入り、情報資産への損害及び利用の妨害等から保護するための物理的な対策を講じる。

⑵　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、職員等及び受託者に対する周知及び徹底を図るとともに、十分な教育及び啓発が行われるよう必要な対策を講じる。

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、ネットワーク管理等の技術的対策を講じる。

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及び情報セキュリティ対策の遵守状況の確認等の運用面の対策を講じる。

⑸　緊急時におけるセキュリティ対策　緊急事態が発生した場合に、迅速かつ適切な対応が可能となるような危機管理対策を講じる。

（情報セキュリティ対策基準の策定）

9　前項の情報セキュリティ対策を講じるに当たり、遵守すべき事項及び判断等の統一的な基準として、情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

（情報セキュリティ実施手順の策定）

10　基本方針及び対策基準に基づき、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（以下「実施手順」という。）を定めるものとする。

（法令等の遵守）

11　職員等及び受託者は、情報資産の利用に当たり、関係法令を遵守しなければならない。

（職員等及び受託者の義務）

12　職員等及び受託者は、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、対策基準及び実施手順を遵守しなければならない。

（情報セキュリティ対策に違反した職員等及び受託者への対応）

13　情報セキュリティ対策に違反した職員等及び受託者については、その重大性、発生した事案の状況等に応じて厳正に対応する。

（情報セキュリティ監査の実施）

14　情報セキュリティ対策が遵守されていることを検証するため、定期的に監査を実施するものとする。

（評価及び見直し）

15　情報セキュリティ監査の結果等に基づき、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、基本方針、対策基準及び実施手順の見直しを実施するものとする。

（その他）

16　この基本方針の適用範囲以外であっても、必要に応じて教育及び啓発等を行うことができるものとする。