名張市情報セキュリティポリシー
(基本方針)

平成16年8月12日　策定

名張市情報セキュリティポリシー

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、名張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を総称する。情報セキュリティポリシーは、当市が保有する情報資産に関する業務に携わる全ての職員及び外部委託事業者に浸透、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（基本方針）と情報資源を取り巻く状況の変化に依存する部分（対策基準）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、

1. 情報セキュリティポリシー基本方針
2. 情報セキュリティポリシー対策基準

の2階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づきネットワーク及び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「情報セキュリティ実施手順」を策定することとする。

情報セキュリティポリシーの構成

文　書　名		内　　容
情報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ネットワーク及び情報システム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		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順

情報セキュリティ基本方針

1．目的

名張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など外部への漏洩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、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは市民の財産・プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが当市に対する市民からの信頼の維持向上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いる。当市が電子自治体を構築するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、当市の情報資産の機密性、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)を整備するため名張市情報セキュリティポリシーを定めることとし、このうち情報セキュリティ基本方針については、当市の情報セキュリティ対策の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認可されたもの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完全防護すること。
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）ネットワーク

名張市における全ての部（事務局及びこれらに相当する組織を含む。以下「部等」という。）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。

（2）情報システム

業務系のコンピュータ（業務系におけるネットワーク、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。

(3) 情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報、ならびにネットワーク及び情報システムで取り扱う全ての情報をいう。なお、情報資産には紙等の有機物に出力された情報も含むものとする。

ただし、学術分野における情報システム及び市立小･中学校における教育分野に関するシステムを除く。

(4) 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. 情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、名張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り、情報セキュリティ対策の頂点に位置するものである。

したがって、名張市長をはじめとして当市が保有する情報資産に関する業務に携わる全ての職員（以下、「職員等」という。）及び外部委託事業者は、情報セキュリティの重要性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。

4. 情報セキュリティ管理体制

名張市の情報資産について、幹部が率先して情報セキュリティ対策を推進･管理するための体制を確立するものとする。

5. 情報資産の分類

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

6. 情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威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以下のとおりである。

(1) 部外者の侵入による機器又は情報資産の破壊･盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊･盗聴･改ざん･消去等

(2) 職員等又は外部委託事業者による機器又は情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の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機器又は

情報資産の盗難、規定外の端末接続によるデータ漏洩等

(3) コンピュータウィルスの感染や、地震、火災等の災害並びに事故、故障等によるサービス及び業務の停止

7. 情報セキュリティ対策

上記 6 で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1) 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ち入り、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。

(2) 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、職員等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等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3) 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正な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、また、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

名張市の様々な情報資産について、上記 7 の情報セキュリティ対策を講ずるに当たっては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、情報セキュリティ対策を行う上で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策定するものとする。

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基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等を定めていく必要がある。そのため、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情報セキュリティ対策基準の基本的な要件に基づき、部等の長が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準の一部及び情報セキュリティ実施手順は、公開す

ることにより名張市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

10. 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ていることを検証するため、定期的に監査を実施する。

11. 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評価を実施するとともに、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に、情報セキュリティポリシーの見直しを実施する。