

香芝市情報セキュリティ基本方針

平成17年3月28日

目次

はじめに.....	1
1 目的.....	2
2 用語の定義.....	2
3 適用範囲.....	2
4 職員の義務.....	3
5 委託事業者の管理及び義務.....	3
6 情報の区分.....	3
7 情報セキュリティ対策.....	3
8 情報セキュリティ対策基準.....	4
9 情報セキュリティ実施手順.....	4
10 情報セキュリティ管理体制.....	4
11 情報セキュリティ監査の実施.....	4
12 情報セキュリティの見直し.....	4
13 法令等の遵守.....	4
14 違反への対応.....	4
附則.....	4

はじめに

インターネットを中心とした情報通信技術は、世界規模でめざましい発展を遂げ、日々、社会の情報化が進み、私たちの生活にも様々な影響をもたらしています。

本市におきましても、市民生活を豊かにするまちづくりのために情報技術を積極的に取り入れ、市民サービスの質を向上させるとともに事務の効率化を進めているところです。また、ここ数年来インターネット等を利用した行政サービスの提供や情報の受発信など推進するために、電子自治体の実現に向けた取り組みが推し進められています。

しかし一方では、情報化の進展とともに、不正アクセスやコンピュータウィルスによるデータの改ざん、個人情報の漏えい等の被害が発生して大きな社会問題となっています。また地震、火災等の自然災害や組織内部における情報機器の不正操作等による情報セキュリティ事故が発生する危険も潜んでいます。

本市が保有している個人情報や重要な行政情報等の情報資産をこのような脅威から防御することは、市民の財産を守るためにも、行政の安定的な運営のためにも必要不可欠であり、特に個人情報保護については、プライバシーを中心とした個人権利利益の侵害を予防するため、平成16年4月に香芝市個人情報保護条例を制定し、また、国においても平成17年4月には一定数以上の個人情報を取り扱う事業者を対象に個人情報保護法が完全実施されるところであります。

そこで、情報資産全般についての「機密性」、「完全性」及び「可用性」を確保し、本市のコンプライアンスプログラムを示す「香芝市情報セキュリティポリシー」を制定いたします。

平成17年3月28日

香芝市長 先山昭夫

注)

「機密性」

権限のない者への重要な情報の漏えいを防止すること。

「完全性」

情報の改ざん、破壊による被害を防止すること。

「可用性」

権限のある者に対し、いつでも情報の利用を可能とすること。

「コンプライアンスプログラム」

CP = 自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム

1 目的

香芝市情報セキュリティ基本方針（以下「基本方針」という。）は、情報セキュリティに対する基本的な指針を記述し、香芝市（以下「市」という。）が保有する情報資産を適切に保護することを目的とする。

2 用語の定義

この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 情報

職員が職務上作成し、又は取得したコンピュータ及び記憶媒体に記録されたデータをいう。

(2) 情報システム

コンピュータシステム（ハードウェア、ソフトウェア、ネットワーク及び記憶媒体）をいう。

(3) 情報資産

情報及び情報システムをいう。

(4) 脅威

自然の脅威（地震、火災、風水害等）、情報システムの脅威（情報システムの故障、誤動作等）及び人的な脅威（不正行為、誤操作等）をいう。

(5) 情報セキュリティ

脅威から市が保有する情報資産を保護し、情報資産の「機密性」、「完全性」及び「可用性」を確保することをいう。

イ「機密性」：権限のない者への重要な情報の漏えいを防止すること。

ロ「完全性」：情報の改ざん、破壊による被害を防止すること。

ハ「可用性」：権限のある者に対し、いつでも情報の利用を可能とすること。

(6) 情報セキュリティ対策

情報セキュリティを維持するための管理策をいう。

(7) 職員

市及び市の関係機関に勤務し、市が保有する情報資産を職務で利用する者の総称をいう。

(8) 委託事業者

契約に基づいて市の情報資産に接する者の総称をいう。

3 適用範囲

この基本方針の適用範囲は、次に定めるところによる。

(1) 適用対象者

この基本方針の適用対象者は、職員及び委託事業者とする。

(2) 適用資産

市が保有するすべての情報資産とする。

4 職員の義務

職員は、地方公務員法に基づく守秘義務及び香芝市個人情報保護条例(以下、「条例」という。)に基づき次の義務を負う。

- (1) この基本方針を遵守し、情報セキュリティ対策を有効に機能させなければならない。
- (2) 職務上知り得た秘密を漏らしてはならない。その職を退いた後も同様とする。

5 委託事業者の管理及び義務

職員は、条例、契約及び管理規則等に基づき、4と同様の内容を委託事業者に対しても義務づけ、管理するものとする。受託事業者は、個人情報を取り扱う業務にあっては、条例の規定に基づき職員と同様の義務を負い、その他の場合にあっては契約に基づく守秘義務を負う。

6 情報の区分

市が保有する情報資産は、その重要度に応じて区分し、その区分に応じた情報セキュリティ対策を講ずるものとする。

7 情報セキュリティ対策

市が保有する情報資産を脅威から保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

(1) 情報資産に関する対策

すべての情報資産について、情報の漏えい、改ざん、破壊などの脅威から保護して管理するために、情報区分に応じて機器や施設に対して必要な対策を講ずる。

(2) 人員に関する対策

職員及び委託事業者に対して情報セキュリティの重要性を認識させ、情報セキュリティの啓発に有効と考えられる教育活動等、必要な対策を講ずる。

(3) 情報システムの設計・開発に関する対策

情報システムの誤作動、不正利用、情報漏えい等から情報資産を保護するために、設計・開発環境、品質保持に必要な対策を講ずる。

(4) 情報システムの運用に関する対策

情報システムに対して運用ミスや情報漏えい等から情報資産を保護するために、情報システムの運用、保守、監視等の必要な対策を講ずる。

(5) ネットワークに関する対策

ネットワーク障害、不正アクセス等から情報資産を保護するために、ネットワークの可用性確保、ネットワーク監視等の必要な対策を講ずる。

(6) 情報セキュリティ事故に関する対策

情報セキュリティ事故発生時に迅速に対応し、被害の拡大を防止するとともに再発を未然に防止するために必要なセキュリティ対策を講ずる。

(7) 情報セキュリティ監査に関する対策

情報セキュリティ対策の実施状況を確認し、情報セキュリティ対策の形骸化を防止するために必要となる情報セキュリティ監査に関する対策を講ずる。

8 情報セキュリティ対策基準

市における情報セキュリティ対策の統一基準となる情報セキュリティ対策基準（以下「対策基準」という。）を定め、想定される脅威に対応するための対策要件を規定する。

この基本方針と対策基準を総称して情報セキュリティポリシーという。

9 情報セキュリティ実施手順

この基本方針、対策基準に従い、情報セキュリティ対策に関する手法、手順の詳細となる情報セキュリティ実施手順（以下「実施手順」という。）を作成するものとする。なお、この対策基準及び実施手順は、公にすることにより市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

10 情報セキュリティ管理体制

この基本方針及び対策基準に規定された情報セキュリティ対策の推進・管理にあたり、以下の組織・体制を置くものとする。

- (1) 情報セキュリティ委員会
- (2) 情報セキュリティ統括責任者
- (3) 情報セキュリティ責任者
- (4) 情報セキュリティ委員会事務局
- (5) 情報セキュリティ管理者

11 情報セキュリティ監査の実施

この基本方針及び対策基準が遵守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。

12 情報セキュリティの見直し

情報セキュリティ監査の実施結果又は情報資産を取り巻く環境の変化に対応するため、必要に応じ見直しを実施するものとする。

13 法令等の遵守

すべての適用対象者は、職務遂行において、関連法令等に従わなければならない。

14 違反への対応

この基本方針に定められた情報セキュリティ対策に違反した場合はその重大性及び発生した事象の状況に応じ、地方公務員法及び条例等の罰則規定の適用対象となる。

附則

この基本方針は、平成17年3月28日から施行する。