# 尼崎市情報セキュリティ基本方針

## 1　目的

本基本方針は、本市が実施する情報セキュリティ対策について基本的な事項を定めることにより、本市が保有する情報資産の機密性、完全性及び可用性を維持することを目的とする。

## 2　定義

(1)　職員

地方公務員法(昭和 25 年法律第 261 号)第 3 条第 2 項に規定する一般職に属する本市の職員並びに市長、副市長、教育長、公営企業管理者、常勤の監査委員及び同条第 3 項第 3 号に掲げる職に属する本市の職員をいう。

(2)　情報

事実、事象、事物、過程、着想等の対象物に関して知り得たことであって、概念を含み、一定の文脈中で特定の意味をもつものをいう。

(3)　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。

(4)　情報資産

資産としての価値がある情報をいう。

(5)　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。

(6)　情報セキュリティポリシー

本情報セキュリティ基本方針をはじめとする情報セキュリティに関する関係法令等をいう。

(7)　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(8)　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(9)　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(10)　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（ハードウェア及びソフトウェア）をいう。

(11)　マイナンバー利用事務系ネットワーク

情報資産分類１の情報資産(但し職員又は職員に類する者の特定個人情報を含む情

報資産を除く)を扱うネットワークをいう。

(12)　ＬＧＷＡＮ接続系ネットワーク

情報資産分類２の情報資産及び、職員又は職員に類する者の特定個人情報を含む情報資産を扱うネットワーク又はＬＧＷＡＮ（総合行政ネットワーク）と接続するネットワークをいう。但し、統括情報セキュリティ責任者が許可した情報資産分類２の情報資産を扱うウェブサーバ等をインターネットに接続するネットワークは除く。

(13)　インターネット接続系ネットワーク

インターネットに接続したネットワークをいう。

(14)　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(15)　本市

本基本方針が適用される行政機関をいう。

3　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

(4)　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　本基本方針の適用範囲

本基本方針が適用される行政機関は、市長部局、議会事務局、消防局、公営企業局及び行政委員会とする。

5　職員の遵守義務

職員は、情報セキュリティの重要性について共通の認識を持ち、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しなければならない。

6　情報セキュリティ対策

上記３の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じる。

(1)　組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2)　情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性等を総合的に勘案して分類し、当該分類に基づき情報セキュリティ対策を行う。

(3)　情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

ア　マイナンバー利用事務系ネットワークにおいては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等により、住民情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系ネットワークにおいては、インターネット接続系ネットワークとの通信環境を分離する。なお、両ネットワーク間で通信する場合には、無害化通信を行う。

ウ　インターネット接続系ネットワークにおいては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を行う。高度な情報セキュリティ対策として、市町のインターネット接続口を集約する兵庫県情報セキュリティクラウドの導入等を行う。

(4)　物理的セキュリティ

情報システム機器、ネットワーク及び職員等のパソコン等の管理について、物理的な対策を講じる。

(5)　人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6)　技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7)　運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際の情報セキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じる。

また、情報資産に対する情報セキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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。

## 8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

## 9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。なお、情報セキュリティ対策基準は、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があることから非公開として運用する。

## 10　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、各所属毎の状況に応じた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ものとする。

なお、情報セキュリティ実施手順においても、情報セキュリティ対策基準同様非公開とし、運用する。