小田原市情報セキュリティポリシー

小田原市情報セキュリティ基本方針

小 田 原 市

目　次

小田原市情報セキュリティ基本方針

1　趣旨

この基本方針は、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、完全性及び可用性を維持するため、組織的かつ体系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当たっての基本的な考え方及び方策を定めるものとする。

2　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、当該各号に定めるところによる。

(1) 行政情報　職員が職務上作成し、又は取得した電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録であって、コンピュータによる情報処理の用に供されるものをいう。以下同じ。）であって、本市が保有しているものをいう。

(2) 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回線網及び構成機器をいう。

(3) 情報システム　ハードウェア、ソフトウェア、ネットワーク、記録媒体等により構成され、データを電子的に処理するための仕組みをいう。

(4) 情報資産　行政情報及びそれを扱う情報システムをいう。

(5) 情報セキュリティ　情報資産の機密性（情報資産の利用を許可された者だけが、情報資産を利用することができることを確実にすることをいう。）、完全性（情報及びその処理方法が、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。）及び可用性（情報資産の利用を許可された者が、必要なときに情報資産を利用することができることを確実にすることをいう。）を維持することをいう。

3　適用範囲

この基本方針は、本市の情報資産及び職員（情報資産を取り扱う非常勤職員及び臨時職員を含む。以下同じ。）に適用する。

4　情報セキュリティ管理体制

本市の情報セキュリティ対策を推進し、及び管理するため、次に掲げる管理者、責任者及び委員会を置き、その職務は、当該各号に定めるところによる。

(1) 最高情報セキュリティ管理者

本市におけるすべての情報資産の情報セキュリティを統括する。

(2) 情報セキュリティ管理者

ア　最高情報セキュリティ管理者を補佐する。

イ　情報セキュリティ管理者を補佐するため、副情報セキュリティ管理者を置くことができる。

(3) 情報システム責任者

個別の情報システムにおける情報セキュリティに関する権限及び責任を有する。

(4) 小田原市情報セキュリティ委員会

本市の情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティに関する重要な事項を審議する。

5　情報セキュリティ対策基準

(1) 最高情報セキュリティ管理者は、この基本方針に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき行為、判断等の基準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。

(2) 情報セキュリティ対策基準は、公開することにより本市の行政運営に支障を及ぼす可能性がある情報であることから非公開とする。

6　情報セキュリティ実施手順

(1) 情報システム責任者は、情報セキュリティ対策基準に基づき、必要に応じて情報システムに関する情報セキュリティ対策の手順等を明記した情報セキュリティ実施手順を策定するものとする。

(2) 情報セキュリティ実施手順は、公開することにより本市の行政運営に支障を及ぼす可能性がある情報であることから非公開とする。

7　職員の義務

(1) 職員は、情報資産を適正に管理し、及び利用し、情報資産を取り巻く様々な脅威から保護しなければならない。

(2) 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つとともに、業務の遂行に当たってこの基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順（以下「情報セキュリティポリシー」という。）を遵守する義務を負うものとする。

8　情報セキュリティ対策

職員は、様々な脅威から情報資産を保護するため、情報セキュリティポリシーに基づき、情報セキュリティ対策を実施するものとする。

9　事件・事故への対応

職員は、情報セキュリティを侵害する事件及び事故が発生した場合は、被害の拡大防止に努めるとともに、早期解決に向けて迅速かつ適切に対応しなければならない。

１０　情報セキュリティ監査

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、定期的及び臨時に情報セキュリティ監査を実施するものとする。

１１　評価及び見直し

(1) 最高情報セキュリティ管理者は、情報セキュリティ監査の結果等により、この基本方針及び情報セキュリティ対策基準の評価を実施し、必要に応じて見直しを行うものとする。

(2) 情報システム責任者は、情報セキュリティ実施手順の評価を実施し、必要に応じて見直しを行うものとする。

１２　違反に対する措置

(1) 最高情報セキュリティ管理者は、情報セキュリティポリシーに違反した職員並

びに当該職員の所属する課、室及びこれらに準ずるところの長に対し、情報セキュリティを確保するために必要な措置を講ずるものとする。

(2) 最高情報セキュリティ管理者は、必要と認めるときは、違反した職員の氏名、所属名及び違反した内容を市長に報告するものとする。

(3) 情報セキュリティポリシーに違反した職員については、その重大性、発生した事案の状況等に応じて、懲戒処分等の対象とする。

附　則

この基本方針は、平成１６年４月１日から施行する。