茅野市情報セキュリティ対策基準

1　趣旨

茅野市情報セキュリティ基本方針（以下「基本方針」という。）第７の規定に基づき、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。

2　適用範囲

(1) 行政機関の範囲

この対策基準が適用される行政機関（以下「行政機関」という。）は、基本方針に定めるところによる。

(2) 情報資産の範囲

この対策基準が適用される情報資産は、基本方針に定めるところによる。

3　組織体制

(1) 最高情報統括責任者

① 市長を、最高情報統括責任者とする。

② 最高情報統括責任者は、市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定の権限及び責任を有する。

③ 最高情報統括責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家をアドバイザーとして置くものとする。

(2) 情報統括責任者

① 副市長及び教育長を、情報統括責任者とする。

② 情報統括責任者は、最高情報統括責任者を補佐する。

③情報統括責任者は、最高情報統括責任者に事故があるときは、その職務を代理する。

(3) 情報セキュリティ統括責任者

① 企画部長を、情報セキュリティ統括責任者とする。

②情報セキュリティ統括責任者は、市の全てのネットワークにおける情報セキュリティを管理し、ネットワークの開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③情報セキュリティ統括責任者は、市の情報資産に対する侵害が発生した場合又は侵害の恐れがある場合は、最高情報統括責任者へ速やかに報告を行い、その指示に従い必要な措置を講ずるものとする。

④情報セキュリティ統括責任者は、緊急時の円滑な情報共有を図るため、最高情報統括責任者、情報統括責任者、情報セキュリティ統括責任者、情報セキュリティ責任者、情報セキュリティ統括管理者、情報セキュリティ管理者及び情報システム管理者を網羅する連絡体制を整備しなければならない。

(4) 情報セキュリティ責任者

① 市長部局の部長、行政委員会事務局の部長又は事務局長等を、情報セキュリティ責任者とする。

②情報セキュリティ責任者は、その所管する部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部局等における情報システムの開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、その所管する部局等において、情報資産に対する侵害が発生した場合又は侵害の恐れがある場合は、情報セキュリティ統括責任者へ速やかに報告を行い、指示を仰がなければならない。

(5) 情報セキュリティ統括管理者

① 地域戦略課長を、情報セキュリティ統括管理者とする。

②情報セキュリティ統括管理者は、本市の全てのネットワーク及び情報システムにおける開発、設定の変更、運用、見直し等に関する指導及び助言を行う権限を有するほか、情報セキュリティ対策に関する指導及び助言を行う権限を有する。

③情報セキュリティ統括管理者は、市の情報資産に対する侵害が発生した場合又は侵害の恐れがある場合は、情報セキュリティ統括責任者の指示に従い、情報システム管理者とともに必要な措置を講ずるものとする。

④情報セキュリティ統括管理者は、情報セキュリティ統括責任者の下、基本方針及び対策基準（以下「情報セキュリティポリシー」という。）等の遵守に関する権限及び責任を有する。

(6) 情報セキュリティ管理者

①市長部局の課室長、市長部局の出張所等出先機関の長、行政委員会事務局の課室長及び地方公営企業の課室長を、情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、その所管する課室等において、情報資産に対する侵害が発生した場合又は侵害の恐れがある場合は、情報セキュリティ責任者、情報セキュリティ統括管理者及び情報システム管理者へ速や

かに報告を行い、指示を仰がなければならない。

④情報セキュリティ管理者は、その所管する課室等において、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練及び指示を行う。

(7) 情報システム管理者

①各情報システムの担当課室長等を、当該情報システムに関する情報システム管理者とする。

②情報システム管理者は、所管する情報システムにおける情報セキュリティを管理し、当該システムの軽微な開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③情報システム管理者は、所管する情報システムにおいて、情報資産に対する侵害が発生した場合又は侵害の恐れがある場合は、情報セキュリティ責任者及び情報セキュリティ統括管理者へ速やかに報告を行い、指示を仰がなければならない。

④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順（以下「実施手順」という。）を作成し、維持・管理を行う。

4　情報資産の管理及び責任

(1) 管理及び責任

情報セキュリティ管理者は、所管する情報資産を重要性区分に従い分類し、情報資産を適正に管理しなければならない。また、すべての職員等は、情報資産の分類に従い、情報資産を適正に取り扱わなければならない。

(2) 管理方法

① 情報資産の分類

情報資産の分類は、機密性、完全性及び可用性の３つの点を踏まえ、次の重要性区分に分類し適正な管理を行うものとする。

重　要　性　区　分
Ⅰ　情報セキュリティに対する脅威が、市民の生命、財産及びプライバシーへ重大な影響を及ぼすもの。
Ⅱ　情報セキュリティに対する脅威が、行政事務の執行に重大な影響を及ぼすもの。
Ⅲ　情報セキュリティに対する脅威が、行政事務の執行に軽微な影響を及ぼすもの。
Ⅳ　影響をほとんど及ぼさないもの。

② 管理台帳の整備

(ｱ) 情報セキュリティ管理者は、その所管する情報資産のうち、重要性区分Ⅱ以上の情報資産については、それらを管理するための台帳を作成し、情報資産の所在、情報資産の重要性区分、管理責任等を明確にしなければならない。

(ｲ) 情報セキュリティ管理者は、作成した管理台帳について、適宜見直しを行い、適正に管理しなければならない。

③ 情報の作成

(ｱ) 職員等は、業務上必要のない情報を作成してはならない。

(ｲ) 情報を作成する者は、情報の作成時に①の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ) 情報を作成する者は、作成途上の情報についても、紛失、流出等を防止しなければならない。情報が作成途上で不要になった場合は、当該情報を消去しなければならない。

④ 情報資産の入手

(ｱ) 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(ｲ) 庁外の者が作成した情報資産を入手した者は、①の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

⑤ 情報資産の利用

(ｱ) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

(ｳ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報資産が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥ アクセス制御等

情報システム管理者は、情報資産の重要性区分に従いアクセス権を定めるなど、適正に管理しなければならない。

特に、重要性区分Ⅰの情報資産は、生体認証等によるアクセス管理をしなければならない。

⑦ 職員等による重要性区分Ⅱ以上の情報資産の取扱い

(ｱ) 施錠可能な場所に保管するなど適正に管理しなければならない。
(ｲ) 貸出し及び複製は、行ってはならない。ただし、特別な理由がある場合は、情報セキュリティ管理者の許可を得て、目的、日時、情報資産の内容、担当者等を記録し、実施するものとする。
(ｳ) 情報を記録している電磁的記録媒体が不要になった場合は、当該電磁的記録媒体の初期化等により、情報を復元できないように処置した上で廃棄しなければならない。
(ｴ) 廃棄する場合は、情報セキュリティ管理者の許可を得て、廃棄の日時、担当者及び処理方法等を記録し、実施するものとする。
ただし、コンピュータ等機器を廃棄する場合は、情報システム管理者の許可を得て、6 技術的セキュリティ対策(4)情報システムの調達、導入、保守等⑤コンピュータ等の修理及び廃棄により、行うものとする。
(ｵ) 完結した情報を保存した電磁的記録媒体は、書込禁止等の措置を行わなければならない。

5　人的セキュリティ対策

(1) 職員等が遵守すべき事項

① ＩＤ、パスワード等の取扱い

情報システムは、定められた識別・認証方法（パスワード、IC カード、生体認証等）により使用するものとする。その識別・認証に用いるユーザＩＤ、パスワード等は、次の事項を守り第三者に使用されることがないよう厳格に管理しなければならない。

(ｱ) 自己が利用しているＩＤ等は、他人に利用させてはならない。
(ｲ) 共用ＩＤ等を利用する場合は、共用ＩＤ等の利用者以外に利用させてはならない。
(ｳ) パスワードは、個人的な秘密事項として扱い、照会等には一切応じてはならない。
(ｴ) パスワードの設定にあたっては、類推されやすいものは避けること。
(ｵ) パスワードは、随時変更を行うこと。

② 情報資産の送信制限

情報セキュリティ管理者の許可なく、重要性区分Ⅱ以上の情報資産を外部のネットワークに対して電子メール等を使用して送信してはならない。また、重要性区分Ⅱ以上の情報資産を送信する場合は、目的、日時、情報資産の内容、担当者等を記録し、暗号化やパスワード設定等の措置を講じた上で、送信するものとする。

③ 電子メール等の使用制限

(ｱ) 情報セキュリティ統括管理者の許可を得た場合を除き、メールソフトの自動転送機能を用いて、職場のメールを転送してはならない。
(ｲ) 複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスがわからないようにしなければならない。
(ｳ) ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。ただし、最高情報統括責任者が使用を認めたものについては、この限りでない。

④ 事故等の報告

情報セキュリティに関する事故、情報システム上の欠陥、誤作動等を発見した場合は、速やかに情報システム管理者及び情報セキュリティ管理者に報告し、指示に従い必要な措置を講じなければならない。

⑤ 机上の端末等の管理

パソコン等の端末、電磁的記録媒体等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末のシャットダウン、電磁的記録媒体等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑥ 業務目的以外での利用の禁止

業務目的以外の情報システムへのアクセス、電子メールの使用及びインターネットの利用を行ってはならない。

⑦ 退職時等の遵守事項

異動、退職等により業務を離れる場合は、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

⑧ 無許可ソフトウェアの導入等の禁止

標準実装以外のソフトウェアをコンピュータへインストールしてはならない。

ただし、職員等が業務上必要なソフトウェアがある場合は、そのコンピュータを所管する情報システム管理者の許可を得て、インストールできるものとする。

⑨ 機器構成の変更の制限

情報システム管理者の許可なくコンピュータ及びネットワークの改造、増設及び交換を行ってはならない。

⑩ 外部持ち出しの制限

情報セキュリティ管理者の許可なく重要性区分Ⅱ以上の情報資産を外部へ持ち出してはならない。また、重要性区分Ⅱ以上の情報資産を持ち出す場合は、目的、日時、情報資産の内容、担当者等を記録し、暗号化やパスワード設定等の措置を講じた上で、持ち出すものとする。

⑪ パソコン等の持ち込みの禁止

個人所有のパソコン、電磁的記録媒体等を業務上使用すること及びネットワークへの接続は行ってはならない。

⑫ 関係法令等の遵守

職務の遂行において使用する情報資産の取り扱いについては、関係法令等を遵守し、これに従わなければならない。

(2) 教育及び訓練

① 教育及び研修の実施

(ｱ) 情報セキュリティ統括責任者及び情報セキュリティ統括管理者は、職員等に対し、情報セキュリティに関する指導及び教育を行うとともに、必要な研修を受講させなければならない。

(ｲ) 情報セキュリティ管理者は、その所管する課室等の職員等に対し、情報セキュリティに関する指導及び教育を行わなければならない。

(ｳ) 情報セキュリティ管理者は、その所管する課室等の嘱託職員、非常勤職員及び臨時職員並びに協定又は覚書に基づく派遣職員に対し、採用時に情報セキュリティポリシー等の内容を理解させ、遵守させなければならない。

② 訓練の実施

情報セキュリティ統括責任者及び情報セキュリティ統括管理者は、所管する情報資産に重大な障害が発生した場合に備え、緊急時対応を想定した訓練を実施しなければならない。

6　物理的セキュリティ対策

(1) 情報システム室の管理

重要性区分Ⅱ以上の情報資産を取り扱う情報システムの基幹機器を設置し、管理し、又は運用する専用の部屋（情報システム室）は、その部屋を管理している者が適切な施設管理及び確実な入退室管理を行わなければならない。

(2) サーバ等の管理

情報システム管理者は、次の措置を講ずるとともに、障害発生時に迅速に対応可能な措置を講じなければならない。

① 機器の取付け

情報システム機器は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、転倒及び落下を防止するため、固定等の必要な措置を講じなければならない。

② 定期保守の実施

重要性区分Ⅱ以上の情報資産を取り扱う情報システムは、定期的に保守を行い、その作業記録を保管しなければならない。

③ 機器の電源

情報システムの主要な機器の電源は、停電等の電源異常時において、当該機器を適切に停止するまでの間、十分な電力を供給できる容量の予備電源を備えつける等、情報資産を保護するための措置を講じなければならない。

④ 通信回線等の管理

(ｱ) 通信回線は、傍受又は損傷がないように必要な措置を講じ、主要な箇所の通信回線については、定期的に点検を行わなければならない。

(ｲ) 情報セキュリティ統括責任者及び情報システム管理者は、外部ネットワークとの物理的接続を必要なものに限定する等、適切に管理しなければならない。

⑤ 行政機関以外への機器の設置

行政機関以外へ情報システムを設置する場合は、情報セキュリティポリシーと同等のセキュリティ対策を、実施していることを確認しなければならない。

(3) 施錠等の措置

情報システム機器等の盗難防止のため、これらを設置している部屋等は、必要に応じて施錠等の措置を講じなければならない。

7　技術的セキュリティ対策

(1) 情報システムの管理

① アクセス記録等

(ｱ) 情報システム管理者は、所管する情報システムについて、情報セキュリティの確保に必要な記録（以下「アクセス記録等」という。）を取得し、一定の期間保存しなければならない。
(ｲ) 情報システム管理者は、アクセス記録等が窃取、改ざん、消去等されないようにアクセス権の設定、複製保存等の必要な措置を講じなければならない。

② 管理内容及び作業内容の記録

情報システム管理者は、情報システムの変更等の処理及び作業内容について、記録を作成しなければならない。

③ 仕様書等の管理

(ｱ) 情報システム管理者は、構成図、設定書及び仕様書（以下「仕様書等」という。）について、記録媒体に関わらず業務上必要とする者のみが閲覧できる場所を定め、保管しなければならない。
(ｲ) 情報システム管理者は、所管する情報システムに修正又は変更を行った場合は、その仕様書等について改訂を行い、仕様書等を常に最新の状態で管理しなければならない。

④ 情報及びソフトウェアの管理

重要性区分Ⅲ以上の情報資産を取り扱う情報システムに関する情報及びソフトウェアを、当該情報システム利用者以外に提供する場合は、条例その他の規程に定められた取扱い方法に従い、当該権者の許可を得なければならない。

⑤ 情報資産の複製保存（バックアップ）

情報システム管理者は、情報資産について定期的にバックアップを行い、適正な管理のもとバックアップデータを保持しなければならない。

⑥ 電子メール

情報システム管理者は、電子メールで送受信できる容量を定め、許容量を超えたメールは、送受信を不可能としなければならない。また、メールボックスの容量を定め、許容量を超えた場合は適正な処置を講じなければならない。

⑦ ファイルサーバ

情報システム管理者は、職員等が使用できるファイルサーバについて、課等の単位でフォルダを構成し、他の課等のフォルダ及びファイルを閲覧及び使用できないよう設定しなければならない。

⑧ インターネット接続、電子メール使用等の制限

情報セキュリティ管理者は、嘱託職員、非常勤職員及び臨時職員並びに協定又は覚書に基づく派遣職員にパソコン等の端末による作業を行わせる場合において、インターネットへの接続、電子メールの使用等が不要な場合、これを利用できないようにしなければならない。

⑨ 外部の者が利用できるシステム

情報システム管理者は、外部の者が利用できる情報システムについて、必要に応じ他の情報システムと物理的に分ける等の措置を講じなければならない。

(2) アクセス制御

① アクセス権限

(ｱ) 情報セキュリティ管理者は､情報システムに対してアクセスできる者を、情報システム管理者へ申請するものとする。

(ｲ) 情報セキュリティ統括責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとに、アクセスする権限のない職員等がアクセスできないように、システム上制限するとともに、設定したアクセス権限を定期的に見直さなければならない。

特に、重要性区分Ｉの情報資産を取り扱う情報システムにアクセスできる者は、必要最小限にしなければならない。

② 特権を付与されたＩＤの管理等

情報セキュリティ統括責任者及び情報システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

③ 特権による接続時間の制限

情報セキュリティ統括責任者及び情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を、必要最小限に制限しなければならない。

(3) ネットワークの管理

① ネットワークの接続制御、経路制御等

(ｱ) 情報セキュリティ統括責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

(ｲ) 情報セキュリティ統括責任者は、不正アクセス及び内部からの情報漏えいを防止するため、通信プロトコルの制御等、ネットワークに適切なアクセス制御をしなければならない。

② 外部ネットワークとの接続

(ｱ) 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合は、既存ネットワーク及び既存情報システムに影響がないことを確認するとともに、最高情報統括責任者の許可を得なければならない。

(ｲ) 情報システム管理者は、外部からのアクセスの許可を、必要最低限にしなければならない。

(ｳ) 情報システム管理者は、外部と常時接続する情報システムについては、ファイアウォールを設置するなど、外部からの侵入防止対策をとらなければならない。

(ｴ) 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合は、速やかに当該外部ネットワークを物理的に遮断しなければならない。

③ 無線ＬＡＮの盗聴対策

情報セキュリティ統括責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

(4) 情報システムの調達、導入、保守等

① 情報システムの調達

(ｱ) 情報システム管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

(ｲ) 情報システム管理者は、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

(ｳ) 情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題がないことを確認しなければならない。

② 情報システムの導入等

(ｱ) 情報システム管理者は、新たな情報システムを導入し、並びに既存情報システムを変更し、及び廃棄する場合は、既存ネットワーク又は既に稼動している情報システムに､影響がないことを確認しなければならない。

(ｲ) 情報システム管理者は、情報システムを変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。

③ 情報システムの調達及び導入に係る情報セキュリティ統括管理者の承認

情報システム管理者は、情報システムの調達及び導入にあたり、事前に計画書、仕様書等を情報セキュリティ統括管理者に提出し、承認を得なければならない。

④ ソフトウェアの保守

(ｱ) 情報システム管理者は、情報システムの機密性・完全性・可用性を確保するため、必要に応じソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）の更新又は修正を行わなければならない。

(ｲ) 情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合を発見又は探知した場合は、修正プログラムを適用するなど、速やかに対応を行わなければならない。

⑤ コンピュータ等の修理及び廃棄

(ｱ) 情報システム管理者は、コンピュータ及びネットワーク機器について、業者に修理をさせる場合は、重要性区分Ⅲ以上の情報資産が完全に消去された状態で行わせなければならない。ただし、情報を完全に消去することが困難な場合において、業者が秘密保持を文書等により確約している場合は、この限りでない。

(ｲ) 情報システム管理者は、コンピュータ及びネットワーク機器を廃棄する場合は、保存されていた情報が復元不可能な状態にして、廃棄の日時、担当者、処理方法等を記録し、廃棄を行わなければならない。

(5) 不正プログラム対策

① 不正プログラム対策ソフトウェアの導入等

情報システム管理者は、コンピュータ及びネットワークへのコンピュータウィルス等の不正プログラム対策ソフトウェアの導入、コンピュータウィルス等の不正プログラムのチェックの実施、職員等への注意喚起など、以下の点に留意した対策を講じなければならない。

(ｱ) 不正プログラム対策ソフトウェア及びそのパターンファイルは、常に最新の状態にすること。

(ｲ) 外部から持ち込まれ、又は外部へ持ち出す情報資産については、事前に不正プログラムのチェックを行うこと。

②感染時等の対応

コンピュータ及びネットワークに不正プログラムの感染又は感染の恐れがある場合は、情報システム管理者は、管理ネットワークへの接続禁止、情報システムの停止等必要な措置を講じなければならない。

8　運用セキュリティ対策

(1) 情報システムの監視

情報システム管理者は、所管する情報システムの監視を行い、その記録を適正に管理及び保存するとともに、定期的に情報システムの安全性を確認しなければならない。

(2) セキュリティ情報の収集

情報セキュリティ統括管理者及び情報システム管理者は、情報セキュリティに関する情報を収集し、関係課等に通知するとともに、情報セキュリティ対策上必要な措置を講じなければならない。

(3) 情報セキュリティポリシーの遵守状況の確認

①情報セキュリティ管理者及び情報システム管理者は、情報セキュリティポリシーの遵守状況及び問題発生状況について常に確認等を行い、問題が発生していた場合は、速やかに情報セキュリティ統括責任者に報告し、必要に応じて最高情報統括責任者に報告しなければならない。

②情報セキュリティ統括責任者は、発生した問題に速やかに対処しなければならない。

③職員等は、情報セキュリティポリシー違反を発見した場合は、直ちに情報セキュリティ管理者及び情報システム管理者に報告しなければならない。

(4) 危機管理体制の整備

① 事件事故等の発見及び調査

(ｱ)職員等は、情報資産に対する侵害若しくは侵害の恐れ又は事故・故障（以下「事件事故等」という。）を発見した場合は、速やかに情報セキュリティ管理者、情報システム管理者及び情報セキュリティ統括管理者に報告し、必要に応じて情報セキュリティ責任者及び情報セキュリティ統括責任者に報告しなければならない。

(ｲ)情報セキュリティ管理者、情報システム管理者及び情報セキュリティ統括管理者は、事件事故等の報告を受けた場合、詳細な調査を行うとともに、最高情報統括責任者に報告し、必要に応じて影響を及ぼす関係機関のほか、それぞれ定められた連絡先へ連絡しなければならない。

② 事件事故等への対処

(ｱ)情報システム管理者は、事件事故等が発生し、情報資産の防護及び被害拡大防止のために情報システムの停止がやむを得ないと判断した場合は、情報システムを停止するなどの措置を講ずるものとする。

(ｲ)職員等は、個々のコンピュータを管理ネットワークから切断する場合、情報システム管理者の許可を得なければならない。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合は、事後報告とすることができる。
(ｳ)情報システム管理者は、事件事故等に係る情報システムのアクセス記録が残されている場合は、記録の保存に努めるものとする。また、当該事件事故等が不正アクセス行為の禁止等に関する法律違反等犯罪の可能性がある場合は、警察及び関係機関との緊密な連携に努めなければならない。
(ｴ)職員等による不正アクセス等があった場合は、情報システム管理者は、当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。
(ｵ)最高情報統括責任者は、当該事件事故等が市民生活に重大な影響を及ぼす場合又は及ぼす恐れがある場合は、速やかに当該事件事故等の状況、影響等について、市民等に対する情報提供を行うものとする。
(ｶ)情報システム管理者及び事件事故等を引き起こした部門の情報セキュリティ管理者は、事件事故等に対処した経過を記録しなければならない。
(ｷ)情報システム管理者は、事件事故等に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討しなければならない。
(ｸ)情報システム管理者は､再発防止の暫定措置を速やかに講ずるとともに、情報システムを復旧しなければならない。

(5) 再発防止の措置

情報セキュリティ統括管理者及び情報システム管理者は､当該事件事故等に係るリスクの分析を実施し､その再発防止措置に準拠して実施手順の改訂を図るものとする。

(6) 緊急時対応計画

最高情報統括責任者は､事件事故等発生時における次の事項を含めた緊急時対応計画を策定しなければならない。

① 関係者の連絡先
② 発生事案に係る報告すべき事項
③ 発生した事案への対応措置
④ 再発防止措置の策定

(7) 運用管理における留意点

情報システム管理者は､アクセス記録､メール等個人のプライバシーに係る情報を閲覧できる権限を有する職員を実施手順に定めなければならない。ただし､法令で定められた個人情報の保護に関係する情報の閲覧に関しては、

当該法令に定められた手続に従うものとする。

(8) 委託業者との契約

情報システムの開発、保守、運用等を外部業者に委託する場合は、当該委託契約書に、次の事項を明記しなければならない。

① 情報セキュリティポリシーの遵守
② 情報資産の秘密保持、目的外使用及び受託者以外の者への提供の禁止に関する事項
③ 業務上知り得た情報の守秘義務に関する事項
④ 再委託に関する制限事項の遵守
⑤ 情報資産の複写及び複製に関する事項
⑥ 委託業務終了時の情報資産の返還、廃棄等
⑦ 委託業務の定期報告及び緊急時報告義務
⑧ 市による事件事故等の公表
⑨ これらの定めに違反した場合の措置及び損害賠償等に関する事項

(9) 委託業者への確認・措置等

情報システム管理者は、委託業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(8)の契約に基づき、必要な措置を講じなければならない。

9 実施手順の策定及び実施状況の検証

(1) 実施手順の作成

情報システム管理者は、具体的なセキュリティ対策を実施するための実施手順を定め、当該システムの使用者に対し、周知するものとする。

(2) 遵守状況の確認

① 情報セキュリティ管理者は、各課等における情報セキュリティポリシー、実施手順等の遵守状況を定期的に確認し、遵守されていない事項については、速やかに適切な措置を講じなければならない。
② 情報セキュリティ統括責任者及び情報セキュリティ責任者は、各部局等における情報セキュリティポリシー等の遵守状況を定期的に確認し、遵守されていない事項については、速やかに適切な措置を講じなければならない。また、必要に応じ、情報セキュリティ管理者、情報システム管理者等に対して、情報セキュリティポリシー等の遵守状況の報告を求めるものとする。
③ 最高情報統括責任者は、必要に応じ、情報セキュリティ統括責任者に対して、情報セキュリティポリシー等の遵守状況の報告を求め、情報セキュリ

ティ実施状況の検証結果、情報セキュリティを取り巻く状況の変化等に対応し、情報セキュリティポリシーの見直しを適宜行うものとする。

10　他の法令との調整

この対策基準の規定は、他の法令等の規定に基づき情報セキュリティ対策ができる場合については、その限りにおいて適用しない。