

# 個別施策7 セキュリティ対策及び 個人情報等の適正な取扱い スケジュール

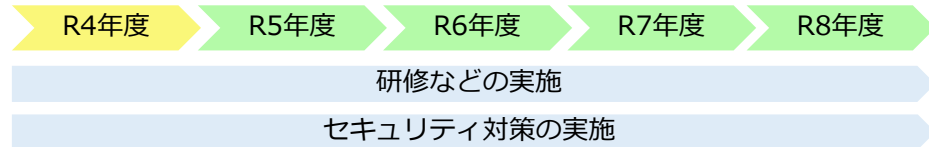


## 施策概要

市では、法令などに基づき、住民の個人情報など、重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供していることから、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続していくことが必要です。

今後、各種手続のオンライン利用の本格化や情報システムの高度化など、電子自治体が進展することにより、情報システムの停止などが発生した場合、重大な支障が生じる可能性も高まります。また、マルウェア※感染、DDoS攻撃※、不正アクセスの増加などサイバーセキュリティ上の脅威は増大しています。

これらの事情から、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要です。さらに、未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止や迅速な復旧、再発防止の対策を引き続き講じていきます。



## 現状

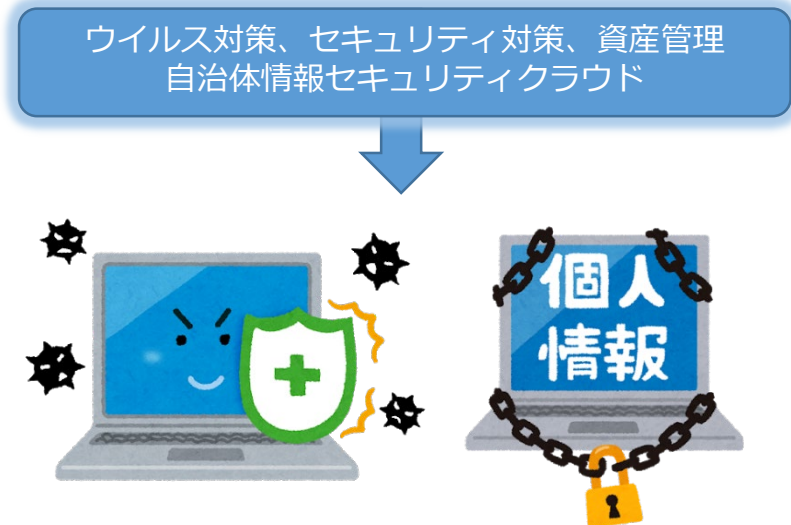
現在、本市で取り組んでいるセキュリティ対策は以下のとおりです。

- ・全職員を対象としたセキュリティチェックの実施
- ・所属のセキュリティ管理者、担当者を対象としたセキュリティ研修の実施
- ・情報セキュリティポリシー※の制定
- ・CSIRT※の設置（情報セキュリティインシデントに対応するための体制）

※CSIRT : Computer Security Incident Response Team

## 課題

全職員が、情報セキュリティの知識を持ち、市民の個人情報等を適正に取り扱うスキルを高める必要があります。

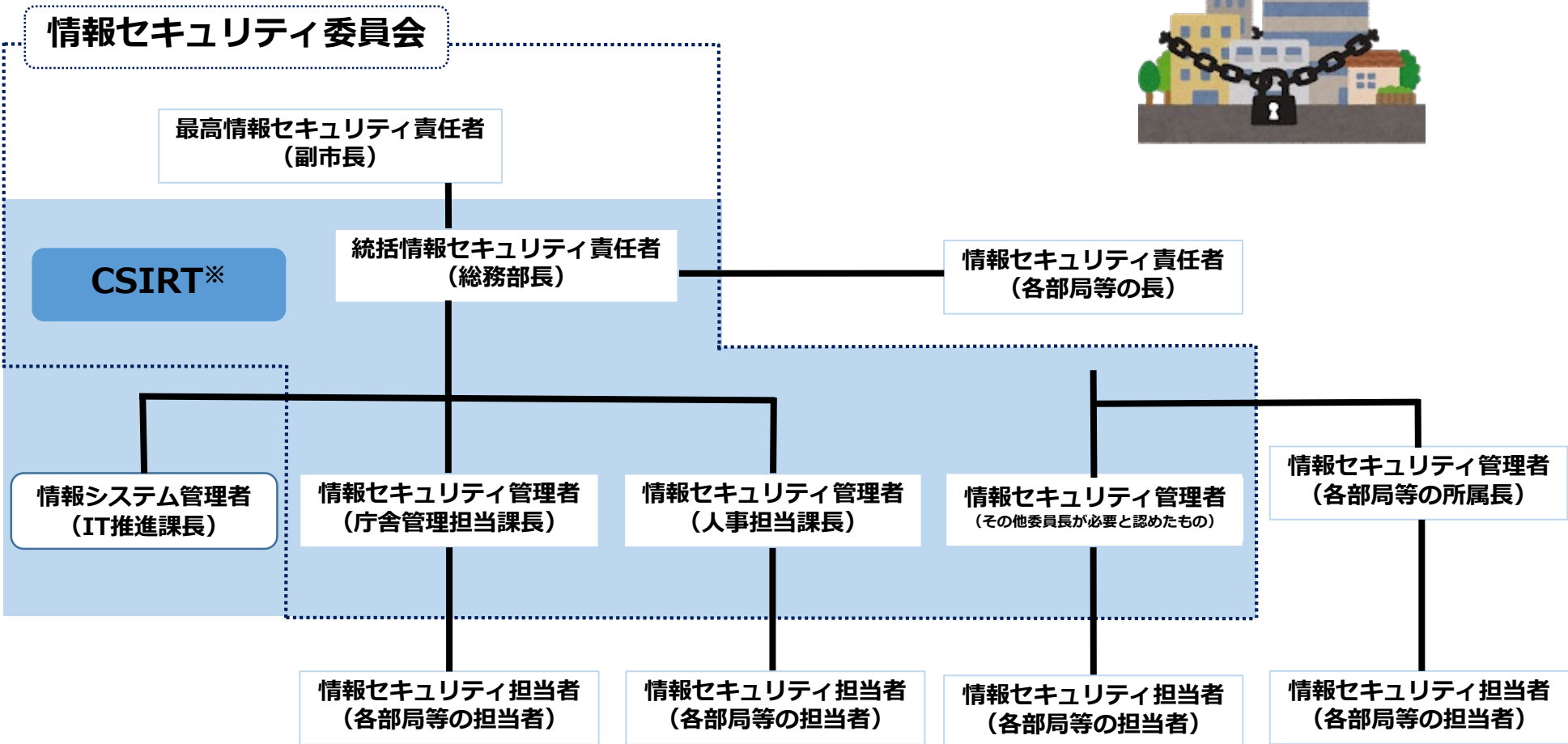


本文中に※印がある用語は巻末の用語集に解説があります。

# 個別施策7 セキュリティ対策及び 個人情報等の適正な取扱い



## 上尾市情報セキュリティ体制図



# 個別施策7 セキュリティ対策及び 個人情報等の適正な取扱い



## 情報セキュリティ委員会

- ・情報セキュリティに関する重要な事項の決定
- ・研修計画の承認、実施状況の受理
- ・監査責任者の指名、監査の実施及び監査結果の受理
- ・自己点検結果、自己点検結果に基づく改善策の受理
- ・事務局はIT推進課

## 情報セキュリティ委員会の委員

- (1) 統括情報セキュリティ責任者（総務部長）
- (2) 庁舎管理担当課長（総務課長）
- (3) 人事担当課長（職員課長）
- (4) その他委員長が必要と認めた者（行政経営課長、市民税課長、福祉総務課長、市民課長、経営総務課長、消防総務課長、教育総務課長）



## CSIRT※（情報インシデントへの対応）

情報セキュリティ委員会の委員と情報システム管理者で構成

- ・情報セキュリティインシデントであるか評価
- ・最高情報セキュリティ責任者への報告（情報セキュリティインシデントの場合）
- ・被害の拡大防止などを図るための応急措置の実施及び復旧に係る指示
- ・情報セキュリティインシデントの原因を究明し、記録を保存

# 個別施策7 セキュリティ対策及び 個人情報等の適正な取扱い



## 情報セキュリティ初心者のための三原則

### 原則1 ソフトウェア※の更新

OS※（基本ソフト）やWebブラウザ※などのソフトウェア※では、脆弱性（ぜいじゃくせい）と呼ばれる情報セキュリティ上の問題（弱点）が発見されることがあります。この問題を解決するためには、ソフトウェア※メーカーなどから提供される修正プログラムを定期的に適用して、できる限りソフトウェア※を最新の状態に保つように心がけなければなりません。

代表的なソフトウェア※では、修正プログラムが提供された場合に、「ソフトウェア※の更新が必要です」という形で通知が表示されることが多くなっています。通知が表示されたら、忘れず更新しましょう。

### 原則2 ウイルス対策ソフト（ウイルス対策サービス）の導入

ウイルスに感染しないようにすることは、情報セキュリティ対策の基本です。そのためには、コンピュータにウイルス対策ソフトを導入したり、インターネットサービスプロバイダ※によるウイルス対策サービスを利用したりすることが重要です。

最近ではウイルス対策のほか、パーソナルファイアウォール※やフィルタリング※などの機能を備えた総合セキュリティ対策ソフトが提供されています。これらの機能は、不正アクセス防止や、フィッシング詐欺※サイトへのアクセス防止などの対策に有効です。

### 原則3 IDとパスワードの適切な管理

IDやパスワードは、パソコンなどの情報機器や各種インターネットサービスを利用する際に必要となる情報です。この情報が他人に奪われてしまうと、自分自身になりすまされて、情報機器や各種インターネットサービスを勝手に利用されてしまうおそれがあります。そのような被害に遭わないよう、IDやパスワードは適切に管理しなければなりません。

具体的には、パスワードは他人に容易に想像されないものを作成する、複数のインターネットサービスで同じパスワードを使い回さないなどの対策が必要です。また、フィッシング詐欺※などのIDとパスワードを盗み取る犯罪に注意する、IDやパスワードをメモをした場合は他人の目につきにくいところに大切に保管する、などの対策も重要です。