



# 情報 セキュリティ

小冊子

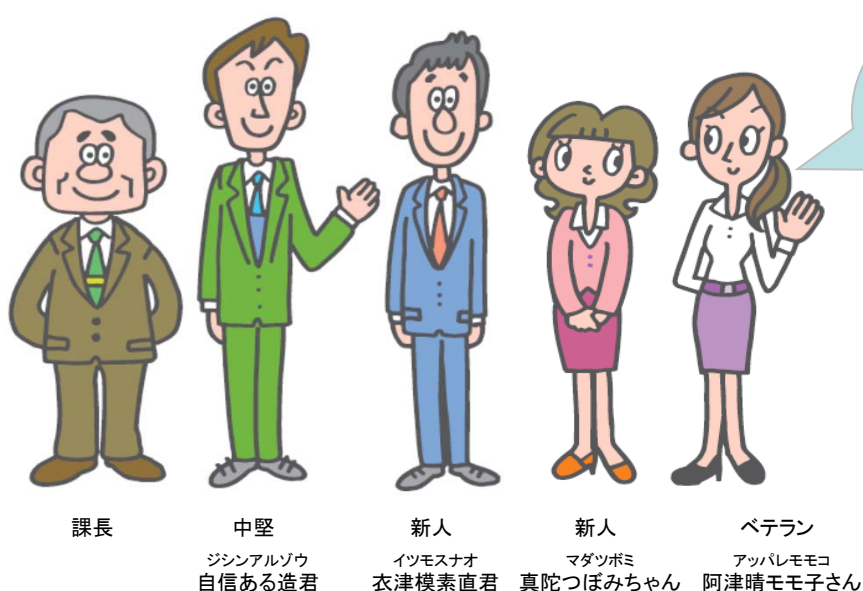




## 本小冊子の目的

本冊子は、「政府機関の情報セキュリティ対策のための統一基準(平成26年度版)」の遵守事項のうち、一般職員が普段の業務を行うに当たり、情報セキュリティ対策を適切に遵守するための主要事項について、テーマ及びユースケースごとに整理したものです。

代表的な業務シーンや過去の事例、対策のポイント等について、イラストを用いてわかり易い解説としましたので、職員の皆さんは、普段から本冊子に目を通して情報セキュリティ対策についての理解を深めるとともに、どうすればいいのか迷ったときの参考としてください。



# 目次

## ■ 第1章 情報の取扱い

- 1 格付及び取扱制限の明示等
- 2 情報を利用・保存するときは
- 3 情報を提供・公表するときは
- 4 情報を持ち運ぶときは
- 5 情報を消去・廃棄するときは

## ■ 第2章 情報システム利用時の注意点

- 1 パソコンを利用するときは(その1)
- 2 パソコンを利用するときは(その2)
- 3 IDやパスワード等の取扱いは
- 4 電子メールを利用するときは
- 5 ウェブサイトを利用するときは

## ■ 第3章 外部委託・外部サービスの利用など

- 1 委託先事業者における情報の取扱い
- 2 フリーメールサービス等の外部サービスの利用について

## ■ 第4章 こんなときには

- 1 モバイルパソコンを庁舎外に持ち出して使いたい
- 2 私物の端末を使いたいが……
- 3 USBメモリを利用するときは
- 4 不審な電子メールを受信した
- 5 端末がウイルスに感染してしまった、感染したかもしれない
- 6 パソコン等の端末を紛失してしまった、盗まれたかもしれない
- 7 その他、困ったことがあったら

## ■ 付録

- 1 情報の格付区分について
- 2 水飲み場型攻撃
- 3 標的型メール攻撃

A lined memo page with a decorative border. The page features 15 horizontal lines for writing. The top right corner is decorated with a cartoon cat wearing a hat and holding a pencil, with the word "MEMO" written below it. The page is also adorned with several pink paw prints scattered across the top and right sides, and a cluster of yellow paw prints in the bottom left corner.



# 第1章



# 情報の取扱い

## 1章-1

### 格付及び取扱制限の明示等



情報を作成又は入手した場合は、  
**「格付」、「取扱制限」**を明示しましょう。



#### 参考:セキュリティ事故事例や社会動向 等

##### ■「機密性2」と表示された資料

政府機関がインターネット上のホームページ等で公表している資料の中に、機密性2と表示された資料が掲載されていたことがネットで話題となった。

資料を公表する際は、「格付」「取扱制限」の見直しに留意する必要があります。

ここがポイント！

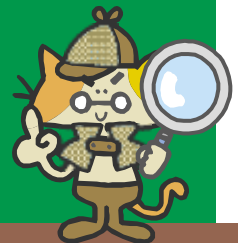
- 格付は、「機密性」、「完全性」、「可用性」の3種類。  
※巻末付録を参照

全ての情報の利用者が格付を認識できるように明示等すること。

※用語解説欄参照

- 格付のみで情報の取扱いを制限できない場合は、取扱制限を活用すること。

例) 「〇〇担当者限り」: 参照者の制限  
「複製禁止」: 複製の制限  
「転送禁止」: 転送の制限



## 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

### P19 3.1.1(3) 情報の格付及び取扱制限の決定・明示等

- 行政事務従事者は、情報の作成時及び府省庁外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。
- 行政事務従事者は、情報を機密性3情報と決定した場合には、機密性3情報として取り扱う期間を明示等すること。
- 行政事務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。
- 行政事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者(決定を引き継いだ者を含む。)又は決定者の上司(以下この項において決定者等という。)に確認し、その結果に基づき見直すこと。

### 用語解説等

#### 明示等:

情報の格付の区分を取り扱う者がすぐに理解できるよう表示すること。  
明示等の方法は、格付の区分を文章のヘッダーやファイル名に記載するなどがあります。  
なお、規程等であらかじめ決めておき、明示を省略することが可能な場合もあります。



## 1章-2

### 情報を利用・保存するときは



格付及び取扱制限に従って、  
情報を適切に取り扱きましょう。



#### 参考:セキュリティ事故事例や社会動向 等

##### ■2013年7月

インターネット上でメールを共有できる米グーグルの無料サービス「グループ」で個人情報や中央官庁の内部情報等が誰でも閲覧できる状態になっていた。

##### ◆ 個人情報漏えいの原因

・管理ミス	59.0%
・誤操作	20.1%
・紛失・置き忘れ	8.0%
・盗難	3.7%

2013年度情報セキュリティインシデントに対する調査報告書  
(NPO日本ネットワークセキュリティ協会)

ここがポイント！

- ・情報の利用は、業務上必要な範囲に限定すること。
- ・情報の取扱いに関する組織のルールを知って、守ること。  
※用語解説欄参照
- ・格付や取扱制限が不明なら、上司や同僚に相談、確認すること。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P19 3.1.1(2) 情報の目的外での利用等の禁止

(a) 行政事務従事者は、自らが担当している行政事務の遂行のために必要な範囲に限って、情報を利用等すること。

P20 3.1.1(4) 情報の利用・保存

(a) 行政事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

P12 2.2.1(2) 違反への対処

(a) 行政事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュリティ責任者にその旨

用語解説等

#### 組織のルール:

府省庁の情報セキュリティ関係規程や所属する組織が定めた個別の実施手順等のこと。手順が分からないときに、すぐに参照できるよう、規程文書の所在を知っておくことも重要です。

## 1章-3

### 情報を提供・公表するときは



部外者へ提供してよい情報ですか？  
公表資料に、公表してはならない情報  
が含まれていませんか？  
念のため確認しましょう。



#### 参考：セキュリティ事故事例や社会動向 等

##### ■2015年3月：政府機関

「政府機関の新人研修資料がインターネット上に流出していたことがわかった。資料には「機密性2」と記されていたが、既に知られた情報であり、秘匿すべき情報はないとしている。」との内容が報道された。

## ここがポイント！

- 部外者に情報を提供する場合は、責任者の許可を得た上で、提供先で格付に応じて取り扱われるようにすること。
- 要保護情報を提供する場合は、安全な提供手段を用いること。

### \* 要保護情報を提供する際の安全な手段の例

- 電磁的記録を暗号化した上で、組織が指定した電子メールサービスにより提供先に送信する。
- 電磁的記録を暗号化した上で、外部電磁的記録媒体に出力して運搬する。(組織が指定したセキュアな運送サービスを利用する方法も考えられる)



## 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

### P20 3.1.1(5) 情報の提供・公表

- 行政事務従事者は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認すること。
- 行政事務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。
- 行政事務従事者は、機密性3情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。
- 行政事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録の付加記録(更新の履歴、文書のプロパティ等をいう。)等からの不用意な情報漏えいを防止するための措置を講ずること。

### 用語解説等

#### 要保護情報:

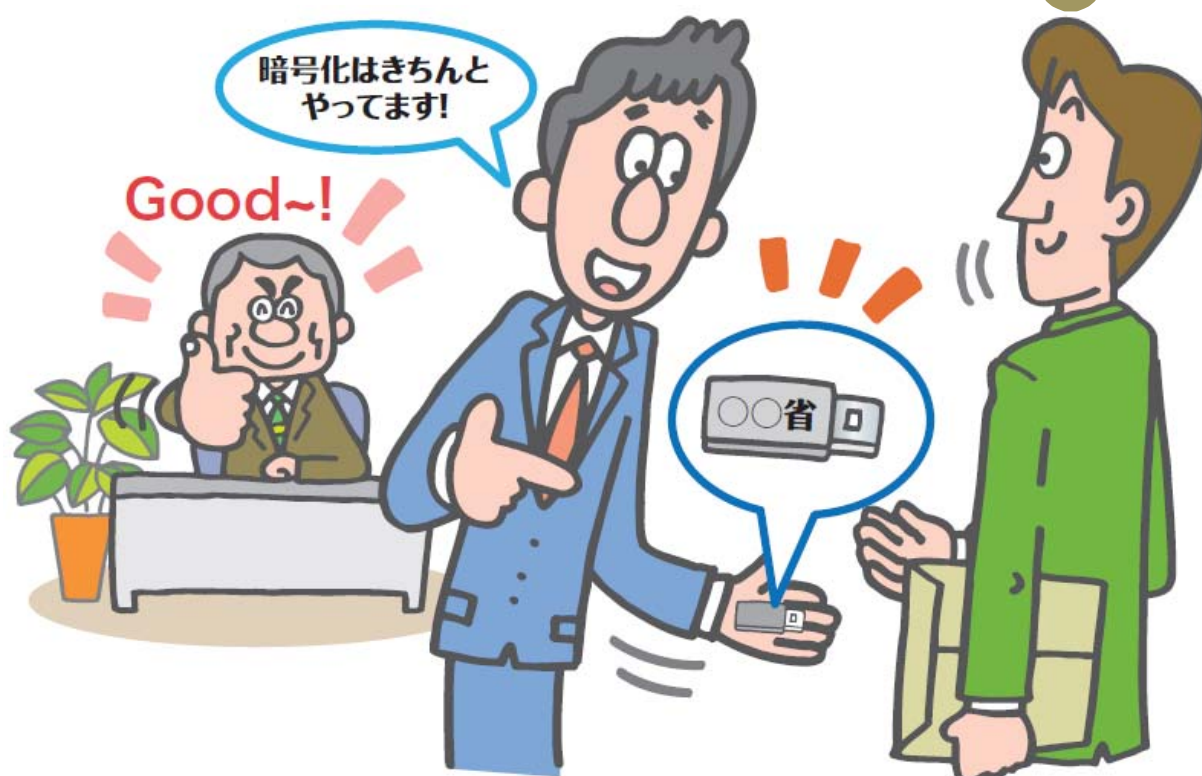
要機密情報、要保全情報及び要安定情報のいずれかに該当する情報のことをいいます。  
(※巻末付録を参照)

## 1章-4

### 情報を持ち運ぶときは



要保護情報を庁舎外に持ち出す際は、  
**盗難・紛失に注意**しましょう。



参考:セキュリティ事故事例や社会動向 等

情報の運搬時に、盗難・紛失の危険はつきもの。  
万が一の際の被害を最小限に食い止められるよう、万全の準備を!

- ◆ 個人情報漏えい媒体、経路
- ・紙媒体 58.7%
- ・USB等記憶媒体 25.9%
- ・電子メール 5.5%
- ・インターネット 5.0%

2013年度情報セキュリティインシデントに対する調査報告書  
(NPO日本ネットワークセキュリティ協会)

## ここがポイント！

- 要保護情報を庁舎外に持ち出す場合は、組織で決められた手順をとること。
- USBメモリは組織が許可したものを使用すること。

府省庁によっては、主体認証機能や暗号化機能が備わった電磁的記録媒体(USBメモリなど)を利用するように手順が定められています。外部電磁的記録媒体を利用する際は、必ず自府省庁の手順を確認しましょう。(4章-3も参照)



### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

#### P20 3.1.1(6) 情報の運搬・送信

- (a) 行政事務従事者は、機密性3情報、要保全情報又は要安定情報を、要管理対策区域外に持ち出し他の場所に運搬する場合又は府省庁外通信回線を使用して送信する場合には、課室情報セキュリティ責任者の許可を得ること。
- (b) 行政事務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。ただし、他府省庁の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域と見なすことができる。
- (c) 行政事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

## 1章-5

### 情報を消去・廃棄するときは



**不要となった情報は、  
パソコン等から速やかに消去しましょう。**



参考: セキュリティ事故事例や社会動向 等

■2012年5月

リサイクルショップで購入したワープロ内部に、政府機関において作成したと思われる個人情報を含む職務上の情報が残存しているとの情報提供があった。

ここがポイント！

- パソコンやUSBメモリを廃棄する場合は、勝手に廃棄せず、組織で決められた手順に従い処置すること。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

##### P21 3.1.1(7) 情報の消去

- (a) 行政事務従事者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。
- (b) 行政事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。
- (c) 行政事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。





A series of 15 horizontal pink lines for writing, spanning the width of the page.



## 第2章



# 情報システム利用時の 注意点

## 2章-1

### パソコンを利用するときは(その1)



情報システムは業務に必要な最低限の範囲に限り利用が原則！ 離席時はスクリーンロック、利用後はログアウトを忘れずに！



#### 参考:セキュリティ事故事例や社会動向 等

■IPA:組織内部者の不正行為によるインシデント調査:2012年7月  
・内部不正を誘発すると考えられる要因に関するアンケート調査結果

環境・機会	1位	職場で頻繁にルール違反が繰り返されている	8.8%
	2位	社内ルールや規則を違反した際、罰則がない	8.7%
	3位	システム管理がずさんで、顧客情報を簡単に持ち出せることを知っている	8.4%

ルール違反が情報セキュリティ事故を誘発します。

ここがポイント！

- 許可された通信回線以外にパソコンを接続しないこと。
- 私物パソコン等を勝手に府省庁LANに接続しないこと。  
※用語解説欄参照
- パソコンの設定を勝手に変更しないこと。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P54 8.1.1(3) 情報システムの利用時の基本的対策

- (a) 行政事務従事者は、行政事務の遂行以外の目的で情報システムを利用しないこと。
- (b) 行政事務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に府省庁の情報システムを接続しないこと。
- (c) 行政事務従事者は、府省庁内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。
- (e) 行政事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

## 2章-2

### パソコンを利用するときは(その2)



利用が認められてるソフトウェア以外は  
**勝手にインストールしてはダメ!**



#### 参考:セキュリティ事故事例や社会動向 等

- 2014年2月:〇〇病院  
パソコン2台が動画再生ソフト「GOMプレーヤー」をアップデートした際にウイルスに感染していたことが判明した。
- 2013年12月:政府機関、〇〇大学など  
パソコンにおいて、入力した全ての文字情報が「百度(バイドゥ)」のサーバに送信される日本語入力ソフト(Baidu IME)がインストールされていた。

ここがポイント！

- 許可されていないソフトウェアを勝手にパソコンへインストールしないこと。
- 利用が認められているかどうか不明な場合は、府省庁LANのヘルプデスクに相談すること。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P54 8.1.1(3) 情報システム利用時の基本的対策

- (d) 行政事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。

P54 (8.1.1(7))

- (a) 行政事務従事者は、不正プログラム感染防止に関する措置に努めること。  
(b) 行政事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

## 2章-3

### IDやパスワード等の取扱いは



パスワードは、他者に知られないよう、**厳重に管理**しましょう。



#### 参考:セキュリティ事故事例や社会動向 等

- 2012年2月:〇〇地検  
使用権限のないID やパスワードを使って組織内の人事情報を閲覧したとして、男性  
検察事務官が戒告処分を受けた。

ここがポイント！

- IDは、自分に付与されたもののみを利用すること。
- パスワードは容易に推測されない複雑なものを設定し、他者に知られないよう、厳重に管理すること。
- パスワードの使い回しをしないこと。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P54 (8.1.1(5))

- (a) 行政事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。
- (b) 行政事務従事者は、自己に付与された識別コードを適切に管理すること。
- (c) 行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。
- (d) 行政事務従事者は、自己の主体認証情報の管理を徹底すること。



## 2章-4

### 電子メールを利用するときは



決められた電子メールサービスを利用しましょう。

電子メールを送信する前に、宛先や添付ファイルの確認を！



#### 参考：セキュリティ事故事例や社会動向 等

##### ■2013年10月：政府機関

「公益通報相談窓口」を通じて内部告発してきた通報者の電子メールについて、政府機関職員が内容を確認する返信メールを送信する際に、別の案件の通報者に誤送信した。

## ここがポイント！

- 要保護情報を電子メール等で送信する場合は、暗号化等の安全管理措置を講ずること。※用語解説欄参照
- 電子メールを送信する際は、宛先や添付ファイルの誤りが無いよう、送信前の確認を徹底するなど、最大限の注意を払うこと。

※ 不審な電子メールを受信した場合の対処について、4章-4で解説しています。併せて参考にしましょう。



### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

#### P20 3.1.1(6) 情報の運搬・送信

- (c) 行政事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

#### P54 8.1.1(4) 電子メール・ウェブの利用時の対策

- (a) 行政事務従事者は、要機密情報を含む電子メールを送受信する場合には、それぞれの府省庁が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。
- (b) 行政事務従事者は、府省庁外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合は除く。
- (c) 行政事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

#### 用語解説等

##### (電子メールの)暗号化:

ネットワークやシステムで情報をやり取りする際、通信途中で第三者にのぞき見られたり書き換えられたりしないようデータを変換すること。

## 2章-5

### ウェブサイトを利用するときは



不審なウェブサイトにご注意しましょう。  
怪しいサイトにアクセスしてしまった場合は  
**直ちに報告窓口に連絡を!**



#### 参考: セキュリティ事故事例や社会動向 等

- 2013年8月~9月: 政府関連機関を狙った水飲み場型攻撃 ※用語解説欄参照  
中央省庁や大手企業の少なくとも20機関を狙った標的型サイバー攻撃(標的組織のIPアドレスからのサイト訪問者だけが感染するもの)が発生した。
- 2014年9月19日: ○○銀行  
○○銀行をかたるフィッシング詐欺。偽画面では、本物のログイン画面と同様の「偽画面にご注意!」といった警告画像を貼り、ユーザーをだまそうとしていた。画面構成なども、本物のログイン画面と酷似していた。

## ここがポイント！

- 業務に関係がないウェブサイトを開覧しないこと。
- ウェブサイトにパスワード等を入力する場合は、暗号化(ブラウザに錠アイコンが表示)されていることを確認すること。



### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P54 8.1.1(4) 電子メール・ウェブの利用時の対策

- (d) 行政事務従事者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。
- (e) 行政事務従事者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。
- (f) 行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。
  - (ア) 送信内容が暗号化されること
  - (イ) 当該ウェブサイトが送信先として想定している組織のものであること

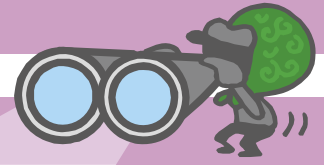
#### 用語解説等

##### 水飲み場型攻撃:

対象組織が通常閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータにマルウェアを自動的に導入させる攻撃手法。(※巻末付録を参照)



# 第3章



## 外部委託・サービスの利用など

### 3章-1

## 委託先事業者における 情報の取扱い



### 委託先事業者に要保護情報を提供する

※用語解説欄参照

場合は、委託先で適切にセキュリティが確保されるようにしましょう。



#### 参考：セキュリティ事故事例や社会動向 等

■2013年9月：東京都〇〇建設事務所

物件調査を委託した業者が個人情報に記載した用地取得事務資料を紛失。物件調査書5部、電子データ(CD)1枚、および原図で、これらには15名分の氏名、住所、電話番号、工作物等を示した図面が含まれていた。

■2015年2月：東京都〇〇区

「健康長寿若返り教室」の委託先事業者が、参加者の個人情報を紛失。打ち合わせ終了後に同社内の鍵付きキャビネットに保管することになっていたが、保管したかどうかの確認もできない状況であった。

ここがポイント！

- 委託先で要保護情報が漏えいしないよう、守秘義務を契約に盛り込むとともに、適切なセキュリティ管理を委託先（再委託先を含む。）に実施させること。
- 委託事業で情報セキュリティに関する事件、事故が発生した場合は、直ちに報告窓口へ連絡すること。



政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P23 4.1.1(4) 外部委託における情報の取扱い

(a) 行政事務従事者は、委託先への情報の提供等において、以下の事項を遵守すること。

(ア) 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

(ウ) 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。

用語解説等

委託先事業者:

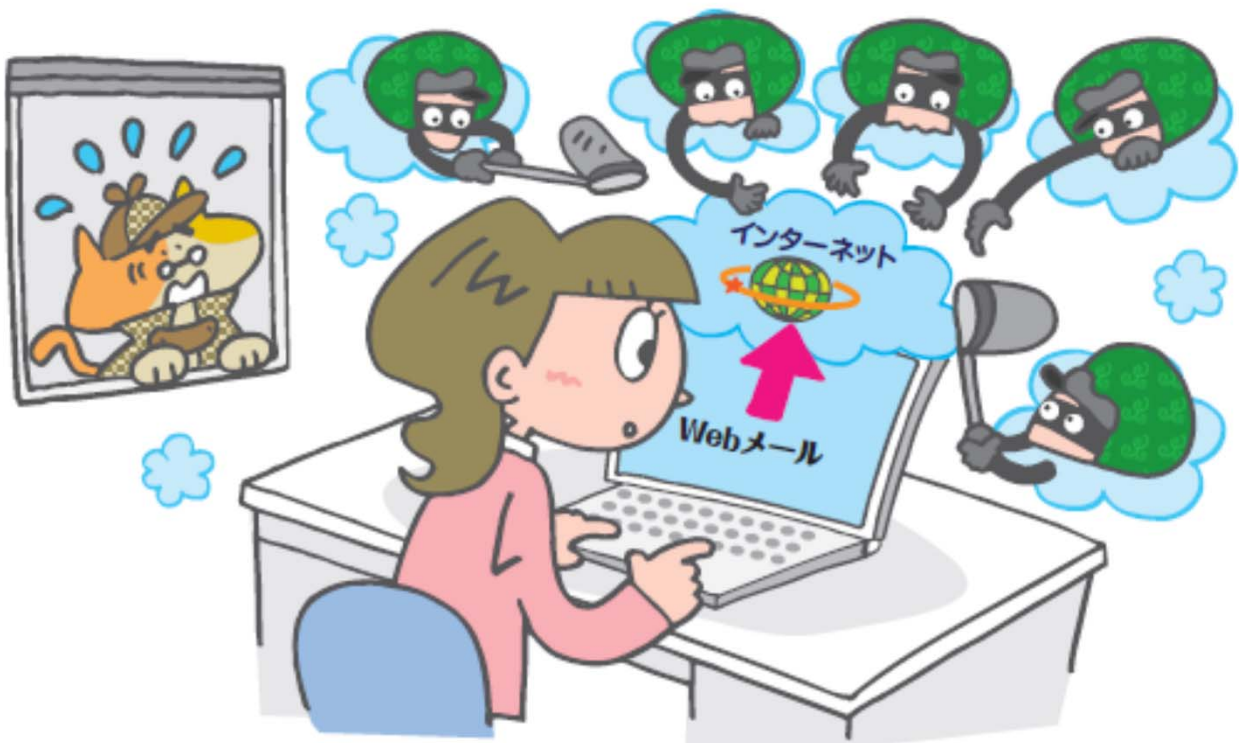
情報システムの構築・運用、情報処理業務等の実施を契約により委ねた民間等の事業者。



## 3章-2 フリーメールサービス等の 外部サービスの利用について



フリーメールやファイルストレージサービスを許可なく**業務に利用しない！**  
**要機密情報の取扱いは絶対禁止！**



### 参考：セキュリティ事故事例や社会動向 等

#### ■2012年7月：政府機関

インターネット上でメールを共有できる米グーグルの無料サービス「グーグルグループ」で個人情報や中央官庁の内部情報等が誰でも閲覧できる状態になっていた。

#### ■2013年8月：〇〇大学

「グーグルグループ」に保存していた留学生センターに所属する学生の成績評価案等の個人情報がインターネット上で閲覧可能な状態になっていた。

ここがポイント！

- インターネット上で提供されているフリーメールやファイルストレージサービス等の約款による外部サービスは、

※用語解説欄参照

原則として業務に利用しないこと。

※組織で使用が認められているものは除く。

- やむを得ず業務利用する場合であっても、要機密情報を取り扱わないようにし、約款、利用規約、利用条件等を事前に十分確認すること。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P25 4.1.2(2) 約款による外部サービスの利用における対策の実施

- (a) 行政事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

用語解説等

約款による外部サービス:

民間事業者等がインターネット上で不特定の利用者(主として一般消費者)に対して提供している、フリーメールやファイルストレージ、グループウェア等のサービスのこと。無料のサービスが多い。



# 第4章



こんなときは

## 4章-1 モバイルパソコンを庁舎外に 持ち出して使いたい



持ち出しに関する申請手続等のルールに従うとともに、持ち出し先での**セキュリティ管理**を徹底しましょう。

※用語解説欄参照



### 参考：セキュリティ事故事例や社会動向 等

- 2012年12月：〇〇大学  
工学研究科の教員が、学生に関する個人情報が含まれているパソコンを学外に持ち出し、紛失した。
- 2015年2月：〇〇大学医学部付属病院  
同病院に関連する医師が、患者の個人情報含むノートパソコンなどを電車内に置き忘れ、一時紛失していたことがわかった。

ここがポイント！

- 要保護情報を取り扱うモバイルパソコンを庁舎外に持ち出す場合は、持ち出しの手続に加え、情報の持ち出しに係る必要な手続も忘れずに行うこと。
- 液晶モニターの“のぞき見”や、モバイルパソコンの盗難・紛失等に注意すること。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P54 8.1.1(3) 情報システムの利用時の基本的対策

- (e) 行政事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。
- (f) 行政事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。
- (g) 行政事務従事者は、機密性3情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。

用語解説等

(パソコンの持ち出し先での)セキュリティ管理:  
盗難・紛失、画面ののぞき見等による情報窃取のリスクに備えた管理を行うこと。



私物等の府省庁支給以外の端末

※用語解説欄参照

(スマートフォンなどを含む)は、**許可なく業務に利用しない**ようにしましょう！



参考：セキュリティ事故事例や社会動向 等

■2014年3月：〇〇医科大学

同大学院生が同大学付属病院の患者の個人情報を含むファイルを個人所有のコンピューターに入れて無断で学外に持ち出し、電子メールで誤送信した。

ここがポイント！

- 府省庁支給以外の端末は、原則使用しないこと。
- 府省庁支給以外の端末をやむを得ず業務利用する場合は、定められた手順に従い、責任者の許可を得た上で利用すること。
- 府省庁支給以外の端末は、府省庁LANに勝手に接続しないこと。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P54 8.1.1(3) 情報システムの利用時の基本的対策

(c) 行政事務従事者は、府省庁内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。

P57 8.2.1 府省庁支給以外の端末の利用時の対策

(a) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、遵守事項8.2.1(1)(c)で定める責任者の許可を得ること。

(b) 行政事務従事者は、要機密情報を府省庁支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

(c) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、府省庁にて定められた手続及び安全管理措置に関する規定に従うこと。

(d) 行政事務従事者は、情報処理の目的を完了した場合は、要機密情報を府省庁支給以外の端末から消去すること。

用語解説等

府省庁支給以外の端末:

自府省庁以外の組織が調達したものや個人所有のパソコンやスマートフォンなどのこと。





要保護情報を保存したUSBメモリは、**厳重に管理**しましょう。

小さいので**紛失には特に注意!**



参考:セキュリティ事故事例や社会動向 等

- 2012年2月:政府機関  
〇〇局麻薬取締部の麻薬取締官が、麻薬事件の容疑者1人の供述内容など捜査情報が入ったUSBメモリを紛失した。
- 2013年12月:〇〇研究センター  
職員ががん検診を受けた9,121人の氏名や判定結果など個人情報の入ったUSBメモリを紛失した。
- 2009年2月:〇〇病院  
職員が業務用パソコンに接続した職員のUSBメモリがウイルス感染しており、ネットワークを通じて1,000台以上に感染が拡大し、大規模なシステム障害が発生した。

ここがポイント！

- 組織で許可されたUSBメモリ等を使用すること。

※用語解説欄参照

- 要保護情報を保存したUSBメモリ等を放置しないこと。
- 要保護情報を保存する場合は、情報を暗号化するなどのセキュリティ対策を講ずること。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P20 3.1.1(4) 情報の利用・保存

- (b) 行政事務従事者は、機密性3情報について要管理対策区域外で情報処理を行う場合は、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。
- (c) 行政事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。
- (e) 行政事務従事者は、USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。

用語解説等

組織で許可されたUSBメモリ等:

府省庁や所属する組織が購入・管理し、職員に利用を許可しているUSBメモリやSDカード等のこと。

## 4章-4

### 不審な電子メールを受信した



**不審な電子メールを受信した場合は、**

※用語解説欄参照

**直ちに報告窓口に連絡しましょう。**



#### 参考：セキュリティ事事故事例や社会動向 等

- 2012年11月：〇〇研究開発機構  
「研究開発活動に係る不正行為に関する告発」を行うメールアドレス宛てメールでPC3台ウイルス感染、内2台のPCから情報の漏洩があった。
- 2013年8月：〇〇研究所  
職員が不審なメールを開いてアカウントが盗用され大量のメールが送信された。
- 2013年12月：独立行政法人(2か所)  
両事務所のメールアドレスを不正に使用したメールが送信された。

ここがポイント！

- 不審な電子メールを受信したことに気が付いた場合は、報告窓口へ連絡し、指示に従う。
- 不審な電子メールの添付ファイルの開封、URLをクリックしない。



#### 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P55 8.1.1(4) 電子メール・ウェブの利用時の対策

(c) 行政事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

用語解説等

#### 不審な電子メール:

府省庁の職員や、業務で関係する委託先事業者等をかたり、重要情報等を窃取する等の不正行為を目的として送信された電子メールのこと。そのような不正行為を標的型メール攻撃と呼ぶこともある。(※巻末付録を参照)

## 4章-5 端末がウイルスに感染してしまった、 感染したかもしれない



パソコンがウイルス等に感染したおそれがあると思ったら、**直ちにLANケーブルを抜き、利用を取りやめましょう！**



### 参考：セキュリティ事故事例や社会動向 等

- 2014年1月：〇〇開発機構  
原発関連施設で、職員用のパソコン1台がウイルス感染し、メールなどの情報が外部に漏れた可能性があるとして発表した。
- 2015年1月：〇〇新聞  
社内パソコン17台がマルウェアに感染し、社内データなどが外部へ流出した。

ここがポイント！

- ウイルス等に感染したおそれがある場合は、勝手に措置せずに、組織で定められた手順（以下に例示）に従うこと。

<例>

- 直ちにLANケーブルを抜く。

※用語解説欄参照

- 端末の電源を切ったり、再起動させたりせず、そのままの状態を保存する。
- 直ちに報告窓口連絡し、指示を受ける。



## 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P14 2.2.4(2) 情報セキュリティインシデントの認知時における報告・対処

- (a) 行政事務従事者は、情報セキュリティインシデントを認知した場合には、府省庁の報告窓口へ報告し、指示に従うこと

用語解説等

### LANケーブルを抜く:

他のコンピュータとネットワークを通じたやり取りをできなくすることを目的に、パソコンに接続されているLAN通信のためのケーブルを抜くこと。無線LANで接続されている場合は、無線LANスイッチを切ったりして、同様に通信機能を停止させる必要がある。

## 4章-6 パソコン等の端末を紛失してしまった、盗まれたかもしれない



府省庁から支給されているパソコン等が  
**紛失**又は**盗難**に遭った場合

(可能性がある場合を含む)、**直ちに報告窓口**  
**に連絡**しましょう。



### 参考:セキュリティ事故事例や社会動向 等

#### ■「個人情報漏えい」原因の比率 上位5位

・誤操作	34.9%	・盗難	5.5%
・管理ミス	32.3%	・不正アクセス	4.7%
・紛失・置忘れ	14.3%		

2013年情報セキュリティインシデントに関する調査報告書  
(NPO日本ネットワークセキュリティ協会)

#### ■遺失/拾得物件数(平成25年度)

携帯電話:  
14万3千件超 (全体の4.5%)

警視庁統計

ここがポイント！

- 盗難・紛失が確定していない場合も、必ず報告窓口へ連絡し、指示に従うこと。
- 遠隔ロックや遠隔データ消去等の端末  
※用語解説欄参照  
のセキュリティ機能が利用できる場合は、実施すること。  
(組織で予め手順が定められている場合は、当該手順に従うこと。)



## 政府機関の情報セキュリティ対策のための統一基準(平成26年度版)

P14 2.2.4(2) 情報セキュリティインシデントの認知時における報告・対処

(a) 行政事務従事者は、情報セキュリティインシデントを認知した場合には、府省庁の報告窓口へ報告し、指示に従うこと

### 用語解説等

#### 遠隔ロック、遠隔データ消去:

モバイル端末の管理ツール(MDM)や通信事業者のサービスにより、ネットワークを通じて端末を利用できないようにしたり、端末に保存された情報を抹消したりする(機能のこと)。





**まずは  
報告、連絡、相談を！**





「ごつち」相談しにおいて



CSIRTとは  
 企業や行政機関において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査を行う体制。

◆あなたが真っ先に報告、相談すべき人は



(責任者名)

(電話番号)

課室情報セキュリティ責任者等の連絡先を入れておきましょう

◆府省庁LANのヘルプデスクやCSIRT窓口等の  
 連絡先を入れておきましょう



※府省庁LANヘルプデスク

(責任者名)

(電話番号)

※CSIRT窓口

(責任者名)

(電話番号)

## ■付録

### 1 情報の格付区分について

#### ●機密性についての格付の定義

格付の区分	分類の基準
機密性3情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性2情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性1情報	公表済みの情報、公表しても差し支えない情報等、機密性2情報又は機密性3情報以外の情報

なお、機密性2情報及び機密性3情報を「要機密情報」という。

#### ●完全性についての格付の定義

格付の区分	分類の基準
完全性2情報	行政事務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性1情報	完全性2情報以外の情報（書面を除く。）

なお、完全性2情報を「要保全情報」という。

#### ●可用性についての格付の定義

格付の区分	分類の基準
可用性2情報	行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性1情報	可用性2情報以外の情報（書面を除く。）

なお、可用性2情報を「要安定情報」という。

また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

## 2 水飲み場型攻撃

### 脅威の概要

- 標的組織がよく閲覧するWebサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
- ブラウザの未知の脆弱性を悪用した攻撃(ゼロデイ攻撃)の場合もあり、未然防止は困難。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

#### <最近の事例>

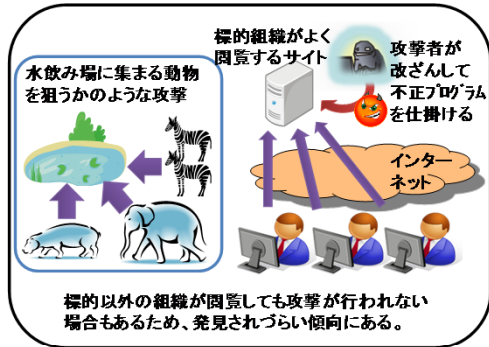
- 2013年8月～9月 中央省庁や大手企業の少なくとも20機関を狙った標的型サイバー攻撃(標的組織のIPアドレスからのサイト閲覧者だけが感染するもの)が発生

### 主な対策

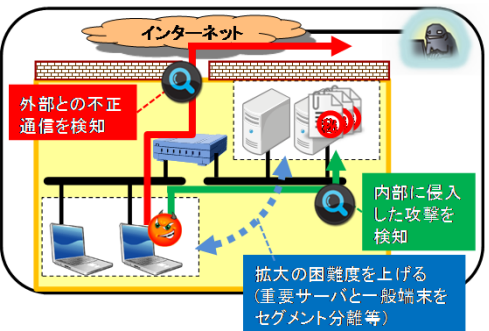
- 感染の未然防止は困難であるため、組織内部へ侵入されることを前提に内部対策を実施。
- 内部対策としては、以下が挙げられる。
  - 内部に侵入した攻撃を早期検知して対処
  - 侵入範囲の拡大の困難度を上げる
  - 外部との不正通信を検知して対処

- <統一基準群(平成26年度版)における対策事項>
- 6.2.4項 標的型攻撃対策 等

### 水飲み場型攻撃(イメージ)



### 対策の概要(例)



## 3 標的型メール攻撃

### 脅威の概要

- 特定の組織を狙って職員等になりすましたメールを送付し、添付ファイルやURLを開かせることによって不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

#### <最近の事例>

- 2012年11月 一部の独立行政法人が「なりすましメール」による不正プログラムに感染し、情報漏えいした可能性があることが判明

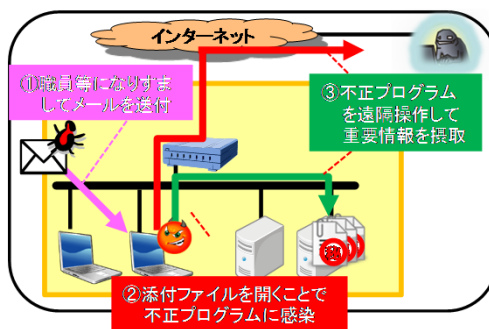
### 主な対策

- 不審なメールを検出する仕組みの整備、対応能力を向上する(SPFの検証、教育・訓練、等)。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

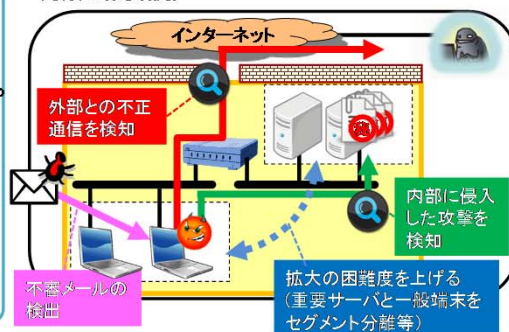
#### <統一基準群(平成26年度版)における対策事項>

- 6.2.4項 標的型攻撃対策
- 6.2.1項 ソフトウェアに関する脆弱性対策
- 7.2.1項 電子メール 等

### 標的型メール攻撃のイメージ



### 対策の概要(例)





情報セキュリティ小冊子

