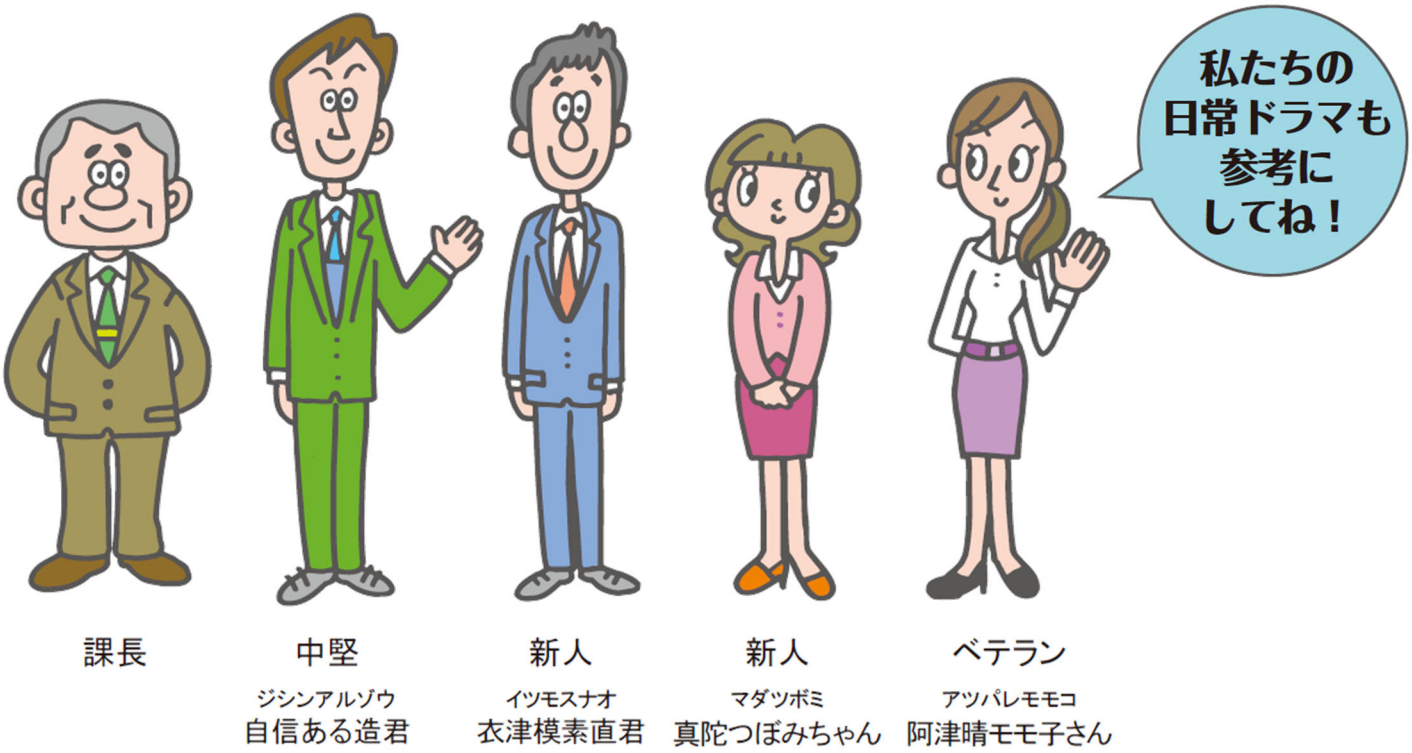
サイバー
セキュリティ

小冊子

本小冊子の目的

本冊子は、「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」の遵守事項のうち、国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）の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　業務委託・外部サービスの利用など**

1　委託先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
3　Web会議の利用について

■**第4章　こんなときには**

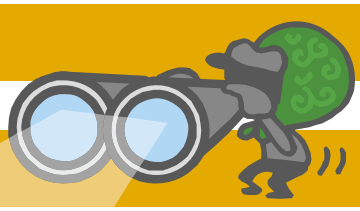
1　モバイルパソコンを施設外に持ち出して使いたい
2　私物の端末を使いたいが・・・・
3　USBメモリを利用するときは
4　不審な電子メールを受信した
5　端末がウイルスに感染してしまった、感染したかもしれない
6　パソコン等の端末を紛失してしまった、盗まれたかもしれない
7　テレワークを実施するときは
8　その他、困ったことがあったら

■**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


MEMO

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：情報セキュリティインシデント事例や社会動向 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）「○○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

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P21　3.1.1(3) 情報の格付及び取扱制限の決定・明示等

(a) 職員等は、情報の作成時及び機関等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。

(b) 職員等は、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。

(c) 職員等は、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（以下本款において「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定めておき、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いましょう。

参考：情報セキュリティインシデント事例や社会動向 等

■2017年４月：○○機構
　同機構のポータルサイトにおいて、登録ユーザーの個人情報が、他の登録ユーザーにより閲覧できる状態になっていた。

◆ 個人情報漏えいの原因
- ・紛失・置き忘れ　26.2%
- ・誤操作　24.6%
- ・不正アクセス　20.3%
- ・管理ミス　12.2%

2018年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～
（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、情報の作成者や入手先に確認又は相談すること。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P13　2.2.1(2) 違反への対処
(a) 職員等は、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を報告すること。

P21　3.1.1(2) 情報の目的外での利用等の禁止
(a) 職員等は、自らが担当している業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。

P22　3.1.1(4) 情報の利用・保存
(a) 職員等は、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。

用語解説等

組織のルール：
自組織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。

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：情報セキュリティインシデント事例や社会動向 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、提供先で格付及び取扱制限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。
  ※用語解説欄参照

＊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）

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P22　3.1.1(5) 情報の提供・公表

(a) 職員等は、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。

(b) 職員等は、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。

(c) 独立行政法人及び指定法人における職員等は、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。

(d) 職員等は、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に一つでも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

要保護情報を施設外に持ち出す際は、
盗難・紛失に注意しましょう。

参考：情報セキュリティインシデント事例や社会動向 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 29.8%
- ・インターネット 26.6%
- ・電子メール 21.4%
- ・USB等記録媒体 12.6%

2018年 情報セキュリティインシデントに関する調査報告書
～個人情報漏えい編～ （NPO日本ネットワークセキュリティ協会）

ここがポイント！

- **要保護情報を施設外に持ち出す場合は、組織で決められた手続をとること。**
- **USBメモリ等は組織が使用を認めたものを使用すること。**

※用語解説欄参照

組織によっては、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、必ず自組織の手順を確認しましょう。（４章-３も参照）

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P22　3.1.1(6) 情報の運搬・送信

(a) 職員等は、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。独立行政法人及び指定法人における職員等が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等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みなすことができる。

(b) 職員等は、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。独立行政法人及び指定法人における職員等が、機密性３情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。

用語解説等

組織が使用を認めたUSBメモリ等：
機関等や所属する組織が購入・管理し、職員等に利用できるものとして定めているUSBメモリやSDカード等のこと。
また、情報の取扱いの遵守を機関等との間で取り決めた機関等外の組織から受け取ったUSBメモリやSDカード等のこと。

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：情報セキュリティインシデント事例や社会動向 等

■2016年７月：民間企業
　顧客情報の保存されているPCを、適正にデータ消去せずに売却し、約400人分の顧客情報が流出していたと発表した。

■2018年6月：XX高専
　廃棄紙の一時保管場所から個人情報20人分が記載されている資料が持ち出される事象が発生。

ここがポイント！

- パソコンやUSBメモリ等を廃棄する場合は、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。
- 要機密情報を含む書類を破棄する場合は、シュレッダーでの裁断等を行うこと。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P23　3.1.1(7) 情報の消去

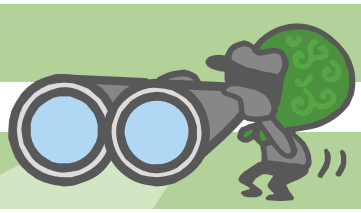
(a) 職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

(b) 職員等は、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) 職員等は、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。


MEMO

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って利用が原則！　離席時はロック、利用後はサインアウトを忘れずに！

参考：情報セキュリティインシデント事例や社会動向 等

■IPA：内部不正による情報セキュリティインシデント実態調査　2016年3月

◆内部不正経験者が起こした内部不正の詳細

・うっかりミスや不注意によるルールや規則の違反	66.5%
・顧客情報等の職務で知り得た情報の持ち出し	58.5%
・個人情報を売買するなど職務で知り得た情報の目的外利用	40.5%
・システムの破壊・改ざん	36.5%
・上記以外の何らかのルールや規則の違反	23.0%

URL：https://www.ipa.go.jp/security/fy27/reports/insider/

ルール違反が情報セキュリティインシデントを誘発します。

ここがポイント！

- 許可された通信回線以外の回線にパソコンを接続しないこと。
- 私物パソコン等を勝手に自組織のLANに接続しないこと。
- パソコンの設定を勝手に変更しないこと。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P64　8.1.1(3) 情報システムの利用時の基本的対策

(a) 職員等は、業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) 職員等は、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機関等の情報システムを接続しないこと。

(c) 職員等は、機関等内通信回線に、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) 職員等は、接続が許可されていない機器等を情報システムに接続しないこと。

(f) 職員等は、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：情報セキュリティインシデント事例や社会動向 等

■2014年2月：○○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、○○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、LANのヘルプデスクに相談すること。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P64　8.1.1(3) 情報システムの利用時の基本的対策

(d) 職員等は、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。

P65 8.1.1(7) 不正プログラム感染防止

(a) 職員等は、不正プログラム感染防止に関する措置に努めること。

(b) 職員等は、情報システム（支給外端末を含む）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（支給外端末を含む）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やパスワードの取扱いは

IDは自分のもののみを使用しましょう。

パスワードは、推測されないものを設定し、他者に知られないよう、厳重に管理しましょう。

推測されないパスワードを設定すればいいの？

それも大事だけど、
システムを跨いで同じパスワード
を設定することは良くないよ

参考：情報セキュリティインシデント事例や社会動向 等

■政府機関等の対策基準策定のためのガイドライン（令和3年度版）

・解説　基本対策事項8.1.1(5)-2 d)「『推測されないもの』について」　（要約）
パスワードに利用者の名前や利用者個人に関連する情報から簡単に派生させたもの等、容易に推測されるものを用いず、十分に長い文字列を用い、推測されないパスワードを設定すること。
パスワードに長い文字列を使用できないシステムの場合は、複雑な文字列を用いること。

> ※複雑な文字列…アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜるなどして、可能な限りランダム生成に近い文字列

・解説　基本対策事項6.1.1(1)-3「『利用者に主体認証情報の定期的な変更を求める場合』について」　（要約）
パスワードを定期的に変更することの情報セキュリティ上の効果は、情報システムの運用方法や認証技術の方式により異なるものであり、必ずしも明らかでなく、利用者にパスワードの定期的な変更を求めるか否かは、その効果と逆効果を勘案して判断する必要がある。

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。
- パスワードは十分に長い文字列とし、推測されないものを設定すること。
- パスワードは、他者に知られないよう厳重に管理すること。
- 異なるシステムで同じパスワードを使い回さないこと。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P65　8.1.1(5) 識別コード・主体認証情報の取扱い

(a) 職員等は、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) 職員等は、自己に付与された識別コードを適切に管理すること。

(c) 職員等は、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) 職員等は、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：情報セキュリティインシデント事例や社会動向 等

■ 2017年１月：政府機関
　職員約30人の人事異動案を、担当者が誤って全職員宛てにメールで一斉送信していた。

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。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P22　3.1.1(6) 情報の運搬・送信

(b) 職員等は、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。独立行政法人及び指定法人における職員等が、機密性３情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。

P64　8.1.1(4) 電子メール・ウェブの利用時の対策

(a) 職員等は、要機密情報を含む電子メールを送受信する場合には、それぞれの機関等が運営し、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) 職員等は、機関等外の者と電子メールにより情報を送受信する場合は、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。（以下、略）

(c) 職員等は、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：情報セキュリティインシデント事例や社会動向 等

■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。

■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。

ここがポイント！

- 業務に関係がないウェブサイトを閲覧しないこと。
- 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。
- オートコンプリート機能を用いると、認証情報が端末上に保存され、攻撃者に窃取されてしまう可能性があるので、オートコンプリート機能は使用しないこと！

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P64　8.1.1(4) 電子メール・ウェブの利用時の対策

(d) 職員等は、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) 職員等は、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) 職員等は、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

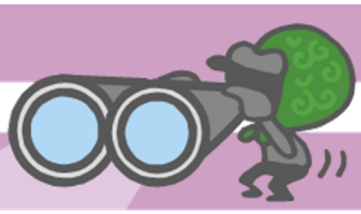
(イ) 当該ウェブサイトが送信先として想定している組織のものであること

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）


MEMO

第3章



業務委託
外部サービスの利用など

3章-1

委託先における情報の取扱い

業務委託する委託先に機関等の情報を
※用語解説欄参照
提供する場合は、業務委託先で適切に
セキュリティが確保されるようにしましょう。

参考：情報セキュリティインシデント事例や社会動向 等

■2018年2月：日本年金機構
日本年金機構が業務委託先に委託していたデータ入力を委託先が無断で中国企業に再委託していた。

ここがポイント！

- 委託先で機関等の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。
- 委託業務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。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P26　4.1.1(4) 業務委託における情報の取扱い

(a) 職員等は、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は、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。

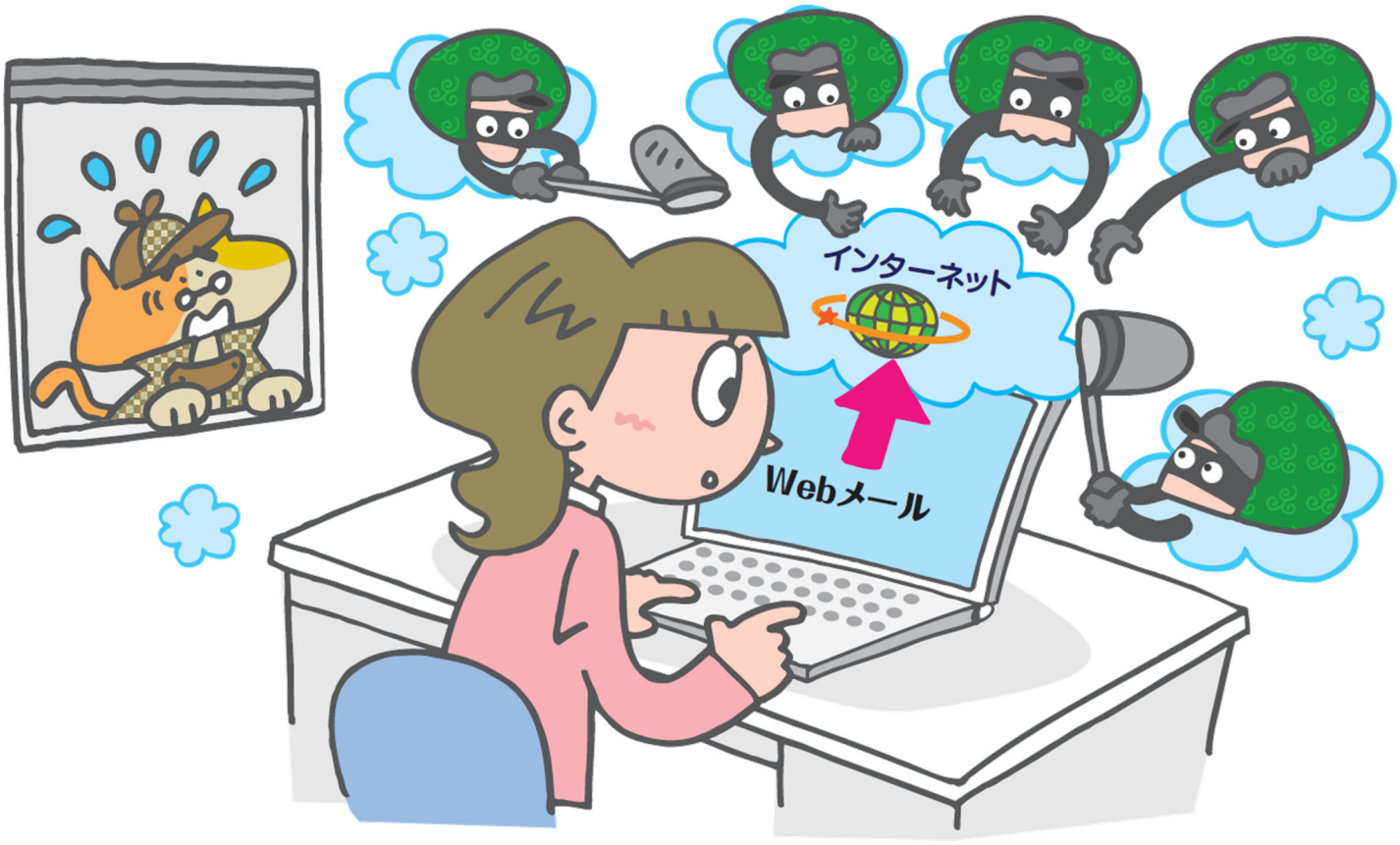
(ウ) 委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。

用語解説等

業務委託：
機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。
「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。
ただし、当該業務において機関等の情報を取り扱わせる場合に限る。

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：情報セキュリティインシデント事例や社会動向 等

■2021年4月：〇〇県警
職務上知りえた運転免許証の個人情報や拾得物情報を元同僚にLINEにて漏えいしていた。

■2021年2月：〇〇医科大学
業務連絡のために開設したGoogle個人アカウントでのGoogleグループの閲覧設定が「ウェブ上のすべてのユーザー」になっており、業務連絡メールなどが第三者より閲覧可能になっていた。

ここがポイント！

- フリーメールやファイルストレージサービスなどの許可を得ない外部サービスの利用においては、情報が適正に取扱われることを直接確認することや必要十分なセキュリティ要件を満たすことが一般的に困難なため、許可なく業務に利用しないこと。

- 外部サービス※用語解説欄参照を利用する際、要機密情報を取り扱わない場合に利用を認められている外部サービスや、要機密情報を取り扱う場合の外部サービスの利用について、各機関の情報セキュリティポリシーを確認すること。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P32　4.2.2(2)　外部サービスの利用における対策の実施

(a) 職員等は、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要機密情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

用語解説等

外部サービス：
機関等外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。
ただし、当該機能において機関等の情報が取り扱われる場合に限る。

3章-3 Web会議の利用について

会議に無関係な人が参加しないように
会議室に<u>パスワード等</u>をかけましょう。

また、不審な参加者がいたら会議室から
退出させましょう。

参考：情報セキュリティインシデント事例や社会動向 等

意図しない者が会議に参加することにより、会議進行の妨害、機密情報の漏えいが発生します。意図しない者の会議へ参加を防ぐためには、会議案内メールの安全な経路での配付と共に、会議参加者の確認・認証方式の選定が重要です。

「Web会議サービスを使用する際のセキュリティ上の注意事項」
（独立行政法人情報処理推進機構）

ここがポイント！

- **Web会議サービス**を利用する際は、
※用語解説欄参照
機密性の高い資料の画面共有を控えるなど、取り扱う情報に応じたセキュリティ対策を実施しよう。

- **Web会議サービスが用意している機能を活用し、会議に無関係の人が参加できないよう対策をしよう。**

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

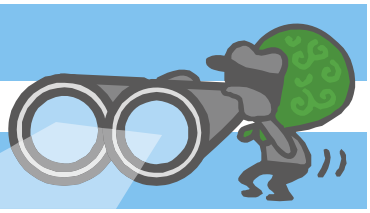
P65 8.1.1(8) Web会議サービスの利用時の対策
(a) 職員等は、機関等の定める利用手順に従い、Web会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。
(b) 職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

用語解説等

Web会議サービス：
専用のアプリケーションやウェブブラウザを利用し、映像または音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。


MEMO

第4章



こんなときには～

4章-1 モバイルパソコンを施設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<u>セキュリティ管理</u>を徹底しましょう。

※用語解説欄参照

参考：情報セキュリティインシデント事例や社会動向 等

■2015年2月：○○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。

■2015年9月：政府機関
　政府機関の職員が、帰途中の電車内で業務用PC、個人情報を記録したUSBメモリ、会議資料等の入った鞄を網棚に置き忘れた。

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施設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。
- モバイルパソコンの盗難・紛失等に注意すること。
- 持ち出し時にインターネットに接続したモバイルパソコンを施設内で機関等LANに接続する場合は、自組織での接続可否についての判断に従うこと。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P64　8.1.1(3) 情報システムの利用時の基本的対策

(f)　職員等は、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。

(g)　職員等は、機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。

(h)　職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

(ア)　機関等が支給する端末（要管理対策区域外で使用する場合に限る）　機密性３情報、要保全情報又は要安定情報

(イ)　機関等支給以外の端末　要保護情報

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・紛失等による情報窃取のリスクに備えた管理を行うこと。

4章-2

私物の端末を使いたいが・・・・

私物等の端末（スマートフォンなどを含む。）
※用語解説欄参照
は、**許可なく業務に利用しない**ように
しましょう！

参考：情報セキュリティインシデント事例や社会動向 等

■2021年4月　〇〇大学医学部付属病院
　病院で許可されていないクラウドサービスに586名の個人情報を保存して使用していたところ、フィッシングメールにより当該サービスのID/PWが盗み取られ、個人情報を閲覧できる状態になっていた。

ここがポイント！

- 支給以外の端末は、原則業務に使用しないこと。なお、支給以外の端末を利用する場合は、自組織での利用の可否の判断に従うこと。
- 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。
- 支給以外の端末は、自組織のLANに勝手に接続しないこと。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P53　7.1.1(5)機関等支給以外の端末の導入及び利用時の対策

(j)　職員等は、機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。

(k)　職員等は、情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去すること。

P64　8.1.1(3) 情報システムの利用時の基本的対策

(c)　職員等は、機関等内通信回線に、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。

用語解説等

私物等の端末：
個人所有のパソコンやスマートフォンなどのほか、他組織から支給された端末も含む。

4章-3

USBメモリを利用するときは

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：情報セキュリティインシデント事例や社会動向 等

■2019年11月：○○大学
　教員が出張先で業務を行うためUSBメモリを利用しデータを持ち出し、出張から帰宅後紛失が判明。43人の氏名、学籍番号等が保存されていた。暗号化や、パスワード設定の処置はされていなかった。同学では個人情報の学外への持ち出しを制限しているが当該教員は保護管理者の許可を得ずにファイルを持ち出した。

ここがポイント！

- 組織が使用を認めたUSBメモリ等を使用すること。
- USBメモリを利用する場合は、利用内容を貸出簿等に記録すること。
- 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。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P22　3.1.1(4) 情報の利用・保存

(b) 職員等は、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、課室情報セキュリティ責任者の許可を得ること。

(c) 職員等は、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) 職員等は、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。

P63　8.1.1(1) 情報システムの利用に係る規定の整備

(b) 統括情報セキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。当該手順には、以下の事項を含めること。

(ア) 職員等は、国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体を使用すること。

(イ) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。

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：情報セキュリティインシデント事例や社会動向 等

警察庁が令和２年に約8100事業者等間を通じて把握した標的型メール攻撃の件数は4,119件であった。

「令和２年におけるサイバー空間をめぐる脅威の情勢等について」
（令和３年３月４日警察庁広報資料）

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。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P64　8.1.1(4) 電子メール・ウェブの利用時の対策
(c)　職員等は、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：
自組織の職員や、業務で関係する委託先等をかたり、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：情報セキュリティインシデント事例や社会動向 等

■2017年３月：○○病院
　ログ解析用ソフトを用いて同病院の医療用端末を解析したところ、患者の個人情報が保存された医療用端末がウイルスに感染し、外部との通信を行っていたことがわかった。

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＞

- 直ちに報告窓口に連絡し、指示を受ける。
- 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。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P16　2.2.4(2) 情報セキュリティインシデントへの対処

(a) 職員等は、情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口に報告し、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

自組織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：情報セキュリティインシデント事例や社会動向 等

■「個人情報漏えい」原因の比率（件数）

・管理ミス	34.0%	・紛失・置忘れ	13.0%
・誤操作	15.6%	・不正な情報持出	6.8%
・不正アクセス	14.5%	・盗難	5.3%

2016年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～
（NPO日本ネットワークセキュリティ協会）

ここがポイント！

- 盗難・紛失が確定していない場合も、必ず報告窓口に連絡し、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。）

※用語解説欄参照

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

P16　2.2.4(2) 情報セキュリティインシデントへの対処

(a) 職員等は、情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口に報告し、指示に従うこと。

P64 8.1.1(3) 情報システムの利用時の基本的対策

(g) 職員等は、機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。

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。

4章-7

テレワークを実施するときは

画面の<u>のぞき見等を防止</u>できるよう実施場所を選定しよう。

また、<u>セキュリティ対策が施されている回線</u>を利用して行いましょう！

参考：情報セキュリティインシデント事例や社会動向 等

■2021年4月

半分以上の委託元がテレワークに関する社内規定・規則・手順が守られていることを確認していないとの調査結果あり。

規定や手順が取り決められていても、遵守状況を確認できていないことにより、内部不正の機会の増加や、気づかないうちに規定に違反していることが原因でセキュリティインシデントが発生する恐れがある。

「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査」
（独立行政法人情報処理推進機構）

ここがポイント！

- 画面ののぞき見や盗み聞きを防止できるようにプライバシーフィルターやイヤホンを活用したり、テレワークの実施場所も選定すること。
  また、自宅以外でテレワークを実施する時は、離席時の盗難に注意すること。

- 公衆無線LAN等の利用については、
  ※用語解説欄参照
  各機関の情報セキュリティポリシーにおいて利用が認められている回線であるか確認すること。

政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）

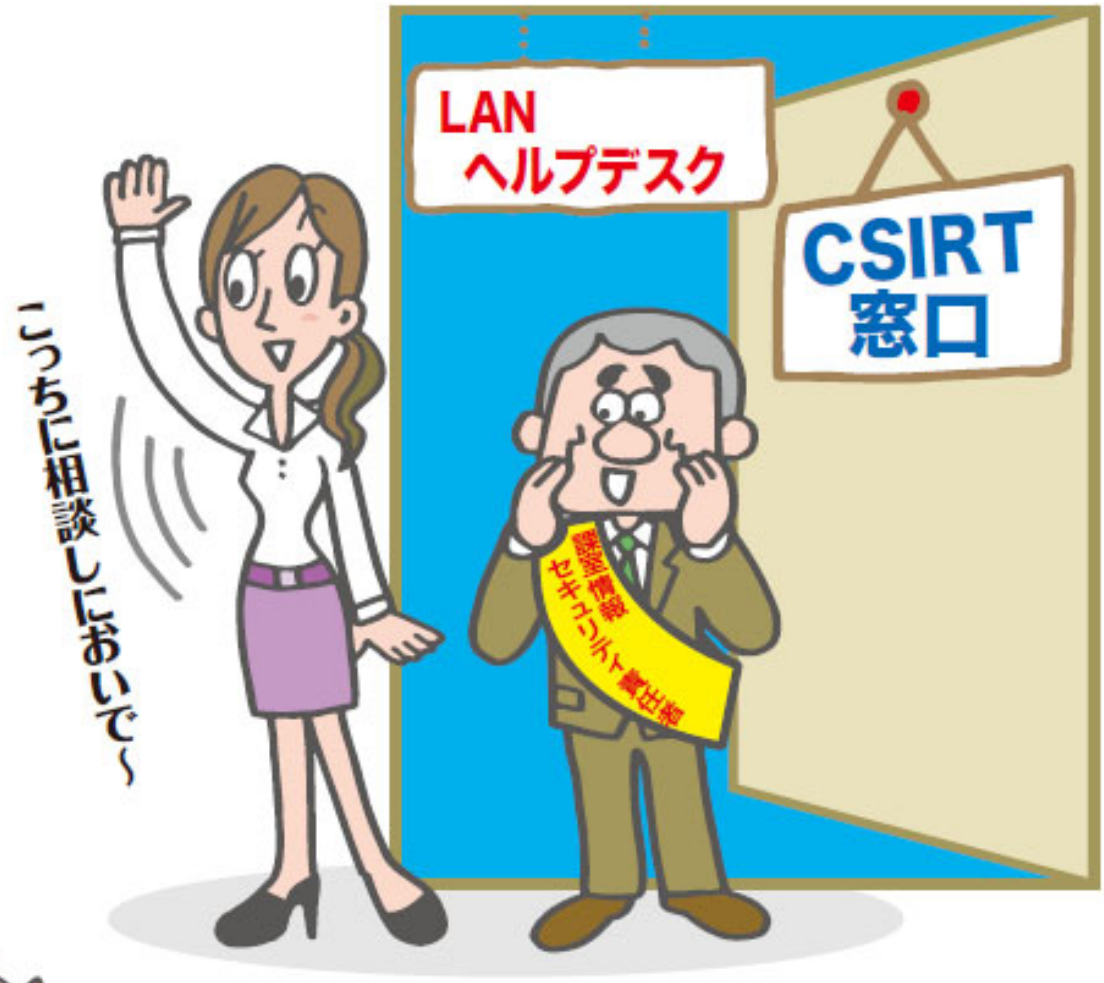
P67 8.1.3(3) 実施時における対策
(b) 職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意すること。
(c) 職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な機関等外通信回線を利用してテレワークを行わないこと。

用語解説等

公衆無線LAN：
ホテル等の施設や町中で提供される無線LANサービス。一般的に、フリーWi-Fi 、無料Wi-Fiなどと呼ばれる。

その他、困ったことがあったら

まずは
報告、連絡、相談を！



ＣＳＩＲＴとは
　最高情報セキュリティ責任者等の幹部の指揮の下、情報セキュリティインシデントへの対処を一元的に管理し、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う機能を有する体制

◆あなたが真っ先に報告、相談するべき人は

（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

◆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

※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	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取り扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性２情報	国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性１情報	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報

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	業務で取り扱う情報（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業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	業務で取り扱う情報（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業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、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「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

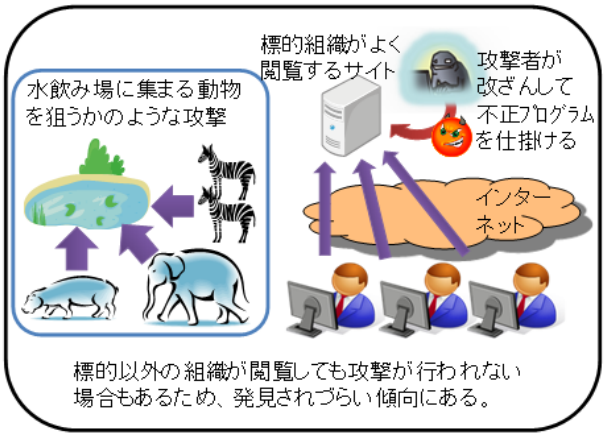
主な対策

- 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、以下があげられる。
  - 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

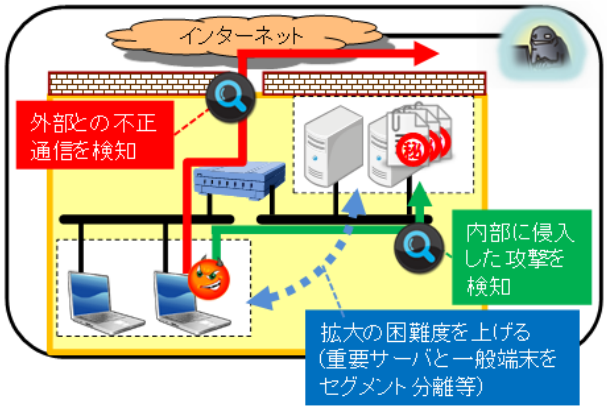
<統一基準群(令和3年度版)における対策事項>

- 6.2.4　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>

- 2015年５月　○○機構に対して4度にわたる執ような標的型メール攻撃が行われ、31台の端末が不正プログラムに感染し、125万件の個人情報が流出するという事案が発生

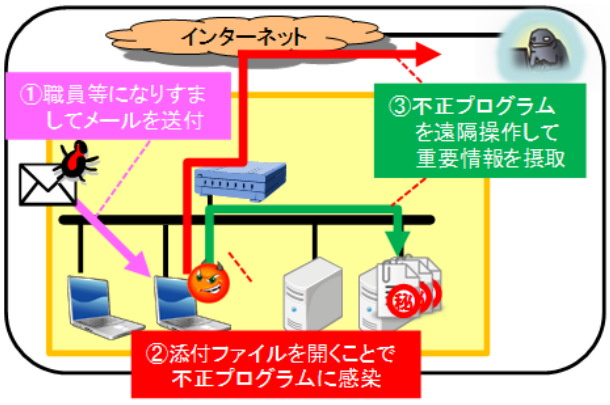
主な対策

- 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（送信ドメイン認証技術の活用、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。

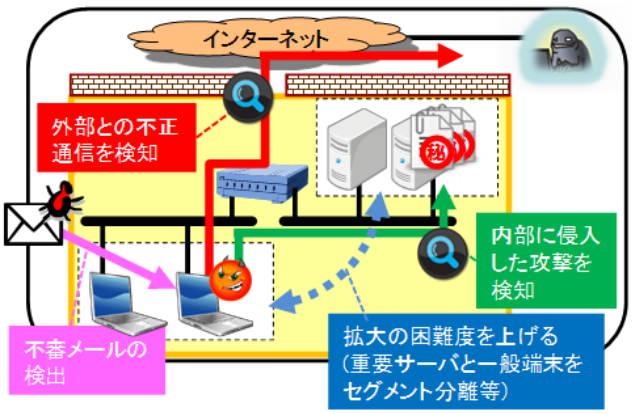
<統一基準群（令和3年度版）における対策事項>

- 6.2.4　標的型攻撃対策
- 6.2.1　ソフトウェアに関する脆弱性対策
- 7.2.1　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)



サイバーセキュリティ小冊子