# 個人情報保護ハンドブック

＜JISQ15001＞

株式会社アンスール

# 個人情報保護マネジメントシステムの基本

# プライバシーマーク制度　用語の確認

プライバシーマーク制度とは、JISQ15001に適合した社内の仕組み（マネジメントシステム）を構築し、個人情報の取扱いを適正に実施している事業者に対し、付与機関であるJIPDECが定めるロゴマーク（Pマーク）の使用を許諾する公的制度です。一回の使用許諾期間は2年で、更新毎に審査を受ける必要があります。

## JISQ15001

日本産業規格で定める「個人情報保護マネジメントシステム－要求事項」。

## 一般財団法人　日本情報経済社会推進協会（JIPDEC）

プライバシーマークの付与機関。

企業等の組織

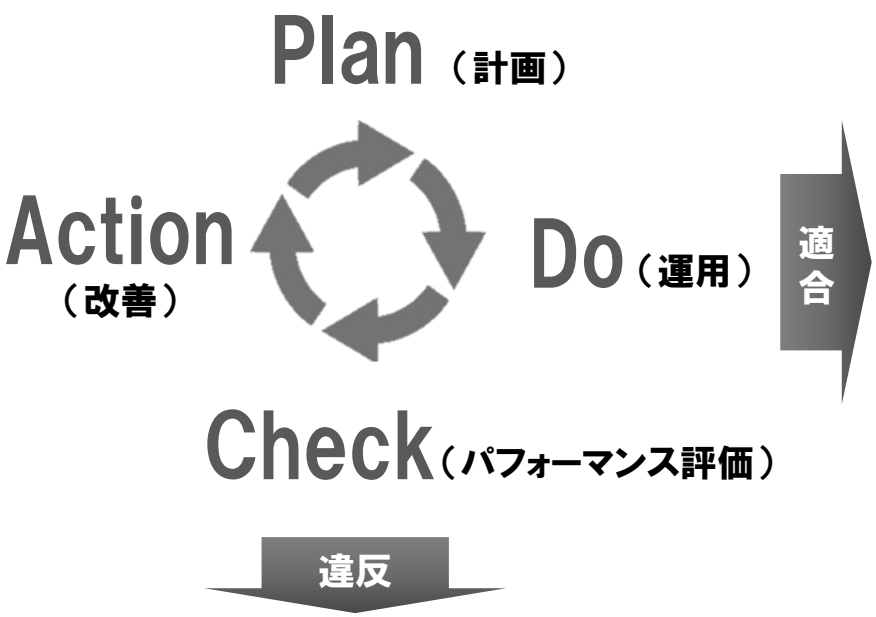
## 個人情報保護マネジメントシステム　＝ PMS（Personal Information Protection Management Systems）

個人情報を適切に管理するための仕組みのこと。

＜参考＞JISQ15001:2017　0.1概要

「個人情報保護マネジメントシステムの採用は、組織の戦略的決定である。組織の個人情報保護マネジメントシステムの確立及び実施は、その組織のニーズ及び目的、個人情報保護の要求事項、組織が用いているプロセス、並びに組織の規模及び構造によって影響を受ける。影響をもたらすこれらも要因全ては、時間とともに変化することが見込まれる。」

# PMS運用のメリットと違反した場合の結果




## PMSに適合することの重要性及び利点

### 事業への好影響

| | |
|---|---|
| 社会的信用の確立 | お客様、取引先からの信頼が得られます |
| 従業者の意識向上 | 従業員の情報保護に対する意識が高まります |
| 個人情報に関する事故リスクの低減 | 情報漏えいなどのリスクを低減できます |

## PMSに違反した際に予想される結果（情報漏えいなど）

**本人への迷惑**

一度漏えいした情報は取り返すことができません。詐欺被害にあう可能性など、ご本人に多大な迷惑をおかけしてしまいます。

**損害賠償責任**

個人情報を漏洩させた会社に対して損害賠償の支払を命じる判決が出されています。漏らしてしまった情報の件数が多ければ多いほど多額の損害賠償を支払わなければなりません。

**会社のイメージダウン**

個人情報の漏洩事件は、新聞・テレビなどのメディアで大きく報道され、会社の信用を失うことになります。

**罰則・ペナルティー**

故意に個人情報を漏洩させた法人若しくは従業者は、法律による罰則に加えて、会社の規程により懲戒の対象になります。

# 個人情報保護の組織体制（PMSに適合するための役割および責任）

| 個人情報保護体制上の役割 | 責任 |
| --- | --- |
| トップマネジメント | 当社PMSの最高責任者として、管理責任者、監査責任者を指名し、PMSを実施させる。 |
| 個人情報保護管理者 | 当社PMSの統括責任者として、PMSの構築、維持および個人情報取扱いの管理全般について責任を負う。 |
| 個人情報保護監査責任者 | 全部門の監査を計画、実行し、代表者に報告する。 |
| 苦情相談窓口責任者 | 保有個人データに関する問合せや各種依頼への対応、及び個人情報取扱についての苦情相談等に対応する。 |
| 情報システム管理者 | 情報システムに関して、PMSを維持するための安全管理対策を実施する。 |
| 特定個人情報等事務取扱責任者 | 個人番号を含む個人情報の取扱いについて、特定個人情報取扱いの管理全般について責任を負う。 |
| 特定個人情報等事務取扱担当者 | 個人番号を含む個人情報の取扱いについて、特定個人情報等事務取扱責任者の指示を受けて適切な取得、利用、保管を実施する。 |

# 個人情報保護方針（内部向け個人情報保護方針及び外部向け個人情報保護方針）

制定年月日　2022年10月5日
最終改正年月日　2022年10月5日
株式会社アンスール
代表取締役 澤田　旺

当社は、当社が取り扱う全ての個人情報の保護について、社会的使命を十分に認識し、本人の権利の保護、個人情報に関する法規制等を遵守します。また、以下に示す方針を具現化するための個人情報保護マネジメントシステムを構築し、最新のＩＴ技術の動向、社会的要請の変化、経営環境の変動等を常に認識しながら、その継続的改善に、全社を挙げて取り組むことをここに宣言します。

ａ）個人情報は、ソフトウェア企画、開発、サポート支援、保守小学校受験に関するサイト運営ホームページの制作、更新、保守、SEO人材育成業務業務における当社の正当な事業遂行上並びに従業員の雇用、人事管理上必要な範囲に限定して、取得・利用及び提供をし、特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（目的外利用）を行いません。また、目的外利用を行わないための措置を講じます。

ｂ）個人情報保護に関する法令、国が定める指針及びその他の規範を遵守致します。

ｃ）個人情報の漏えい、滅失、き損などのリスクに対しては、合理的な安全対策を講じて防止すべく事業の実情に合致した経営資源を注入し個人情報セキュリティ体制を継続的に向上させます。また、個人情報保護上、問題があると判断された場合には速やかに是正措置を講じます。

ｄ）個人情報取扱いに関する苦情及び相談に対しては、迅速かつ誠実に、適切な対応をさせていただきます。

ｅ）個人情報保護マネジメントシステムは、当社を取り巻く環境の変化を踏まえ、適時・適切に見直してその改善を継続的に推進します。

以上

**【お問合せ窓口】**

個人情報保護方針に関するお問合せにつきましては、下記窓口で受付けております。

株式会社アンスール　個人情報問合せ窓口
〒103-0014 東京都中央区日本橋蛎殻町１丁目-20-10
TEL：03-6222-8295 FAX：03-6222-8296 MAIL：info@ansurs.co.jp
受付時間：9:00～18:00 （土・日曜日、祝日、年末年始は除く）

# セキュリティ対策の基本

# 情報セキュリティ上の脅威のトレンド

昨年から継続してランサムウェアによる被害や標的型攻撃によるリスクが高いことがレポートされており、引き続き注意が必要です。セキュリティ対策が脆弱な取引先などを経由したサプライチェーン攻撃の脅威も高まっています。

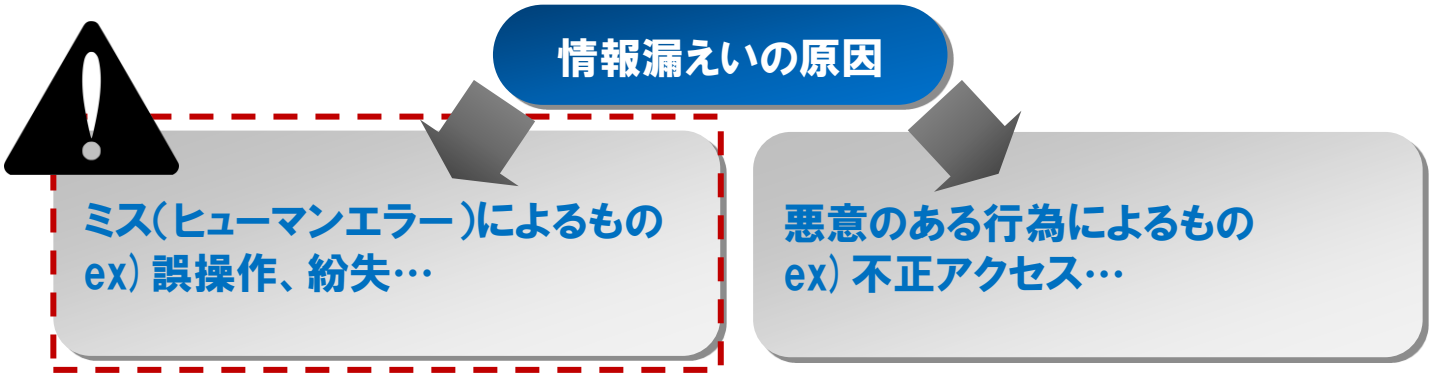
IPA「情報セキュリティ10大脅威 2022」の組織に対する脅威の上位5位までを抜粋

| 順位 | 組織 | 昨年順位 |
|---|---|---|
| 1位 | ランサムウェアによる被害 | 1位 |
| 2位 | 標的型攻撃による機密情報の窃取 | 2位 |
| 3位 | サプライチェーンの弱点を悪用した攻撃 | 4位 |
| 4位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 3位 |
| 5位 | 内部不正による情報漏えい | 6位 |

IPA「情報セキュリティ10大脅威 2022」より

# セキュリティ事故の防止はヒューマンエラーをなくすことから

セキュリティ事故の原因は大きく、「ミスによるもの」、「悪意のある行為によるもの」に分類されます。実は、漏えい事故の多くはミスにより発生しているのです。ミスにより流出した情報は必ず悪用されるとは限りません。しかし、情報が漏れたことで、ご本人に不安を与え、ひいては会社の信頼を失うことにつながります。




ミスは情報を移送するタイミングで多く発生します。基本的なことですが、以下の点に留意して業務を行いましょう。

| 業務 | リスク | 対策 |
|---|---|---|
| メールを送信する/郵送する/FAXを送る | ・宛先を間違える<br>・送る情報を間違える | 宛先や送る情報を2重に確認する |
| デバイス、メモリ等を社外に持ち出す | ・置忘れる<br>・紛失する | ・手放さないように徹底<br>・持出す際は許可を得る |

# ソーシャルエンジニアリング対策

ソーシャルエンジニアリングには物理的な対策が有効です。オフィスでの作業環境には情報漏えいにつながる様々なリスクがあることに留意しましょう。また、悪意のあるの行為は、外部からの攻撃のみでなく、内部犯行犯による可能性もあることに留意しましょう。

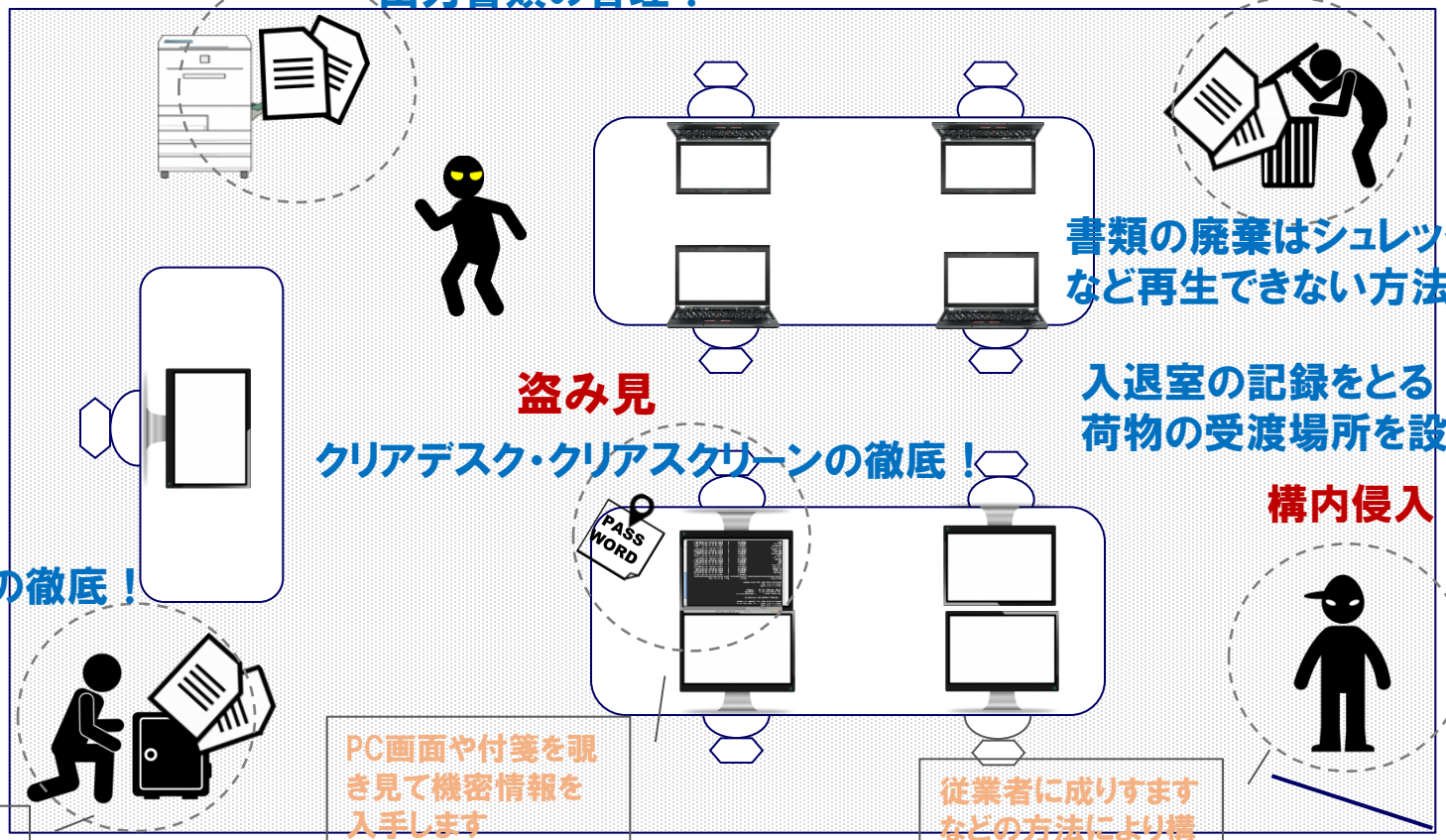
OAのトレイやデスクの上に放置した書類を持ち去ります

持ち去り

出力書類の管理！

ゴミ箱の書類をあさり、機密情報を入手します

トラッシング




書類の廃棄はシュレッダーなど再生できない方法で！

盗み見

クリアデスク・クリアスクリーンの徹底！

入退室の記録をとる！
荷物の受渡場所を設ける！

構内侵入

施錠管理の徹底！

PC画面や付箋を覗き見て機密情報を入手します

従業者に成りすますなどの方法により構内に侵入します

機密情報を権限のない者が盗み出します

盗難

# パスワードへの攻撃

パスワード管理は情報セキュリティ対策の基本です。パスワードが奪われると不正アクセスなどあらゆる攻撃に使用される危険性があります。

## 攻撃手法

### 従来からの攻撃手法

**ブルートフォースアタック**
あらゆる単語を力技で入力し続ける手法です。一般的にはツールを使用して高速で入力します。

**辞書攻撃**
admin　password・・・などパスワードに使われやすい単語を総当たりで入力する手法です。

### 最近増加した攻撃手法

**パスワードリスト攻撃**
何らかの方法で入手したID・パスワードのリストを用いて、本人に成りすまして正規ルートからアクセスを試みる手法です。攻撃者は実行のために必要なパスワードリストを、ターゲットとする情報システムよりもセキュリティの脆弱なサイトなどから入手してきます。
ユーザーの多くが複数のサイトで共通のID・パスワードを用いる傾向を悪用した攻撃手法です。

## 主な対策

他人にわかるパスワード( 名前、誕生日等 )は設定してはいけません。
パスワードは複雑で十分な長さをもったものを設定しましょう。
当社のルールでは英数大文字小文字混在の8桁以上がルールです。
社内においても誰にも教えてはいけません。

# マルウェアとは

マルウェアとは、不正な動作を行うことを目的に作成された悪意のあるソフトウェアやプログラムの総称です。

## 代表的なマルウェア

■ウイルス
他のプログラムに寄生して、動作を妨げたり、有害な作用を及ぼすプログラム

■ワーム：
自己増殖型（他のプログラムに寄生せず単独で存在するタイプ）のウィルス。
ネットワークを徘徊し、脆弱性のあるコンピュータに進入する。

■トロイの木馬：
便利なアプリケーション等に見せかけて、実際は悪事を働くプログラム

■スパイウェア：
感染したパソコンの内部情報をユーザの意思とは関係なく自動的に外部に送信する

## マルウェアの主な感染経路

■メール経由：
メール本文や添付ファイルに仕組まれたウィルスに感染

**近年特定の組織を標的にした攻撃が増加中！**

■USBメモリ経由：
ウィルスに感染したUSBを接続することでウィルスに感染

■Web経由：
悪意のあるWebページを閲覧することで感染

■ファイル交換ソフト（P2P）経由：
Winny、Shareのようなファイル交換ソフトを経由してウィルスに感染

# マルウェア対策の基本

マルウェアについて理解したところで、マルウェア対策の基本について確認しましょう。結局は当たり前の事のことを確実に実施する事が大切なのです。「少しだけなら大丈夫」、「今回は大丈夫」といった例外を自分の中で作らないようにすることが事故の防止につながります。

## ウィルス対策ソフト

- ✓ ウィルス定義ファイルの更新を確実にする
- ✓ 常時スキャンだけでなく定期的にファイル全体へのスキャンを実施する

※ウィルス定義ファイル：既知のウイルスに固有の振舞いを登録したウィルスソフト内のファイル（パターンファイル）

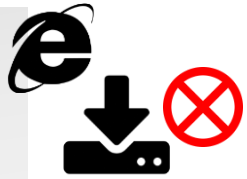
## 更新プログラムの適用

ソフトウェアを提供する業者から公開された更新プログラム（セキュリティパッチ）を即座に適用する


**注意** 脆弱性が発見されてから攻撃を受けるまでの期間はどんどん短くなってきています（ゼロディ攻撃といいます）。アップデートのメッセージが出たら“後で実行する”を選択せず、即時に実行することが必要です。

## Webブラウザのセキュリティ

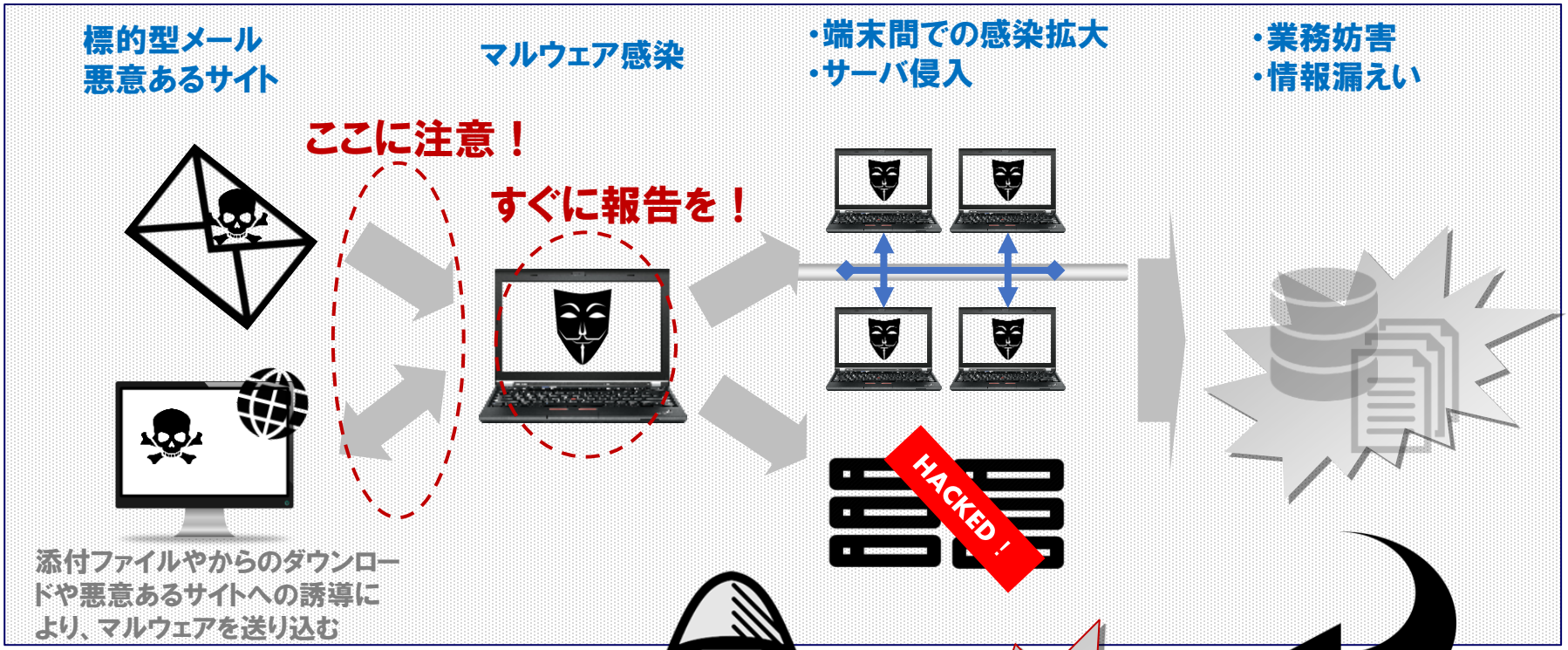
- ✓ 業務に関係のないWebサイトにアクセスしない
- ✓ ソフトウェアのダウンロードは管理者の許可を得る
- ✓ クラウドサービスの利用は管理者の許可を得る



# 標的型攻撃

標的型攻撃は、特定の組織内の情報を狙って行われるサイバー攻撃の一種です。ターゲットとなる組織の従業者宛てにマルウェアが仕込まれた電子メールを送ることなどによって開始されます。

準備段階 → 侵入（初期 → 拡大期） → 目的遂行




**知らない人からのメールは十分に注意し、不用意にURLにアクセスしたり、添付ファイルを開けたりしないよう注意してください！**

# 標的型攻撃メールの見抜き方

**実在する取引先を騙ったり、自分が送ったメールへの返信を装ったりと手口がますます巧妙化している。**

## 標的型攻撃メールの文面（例）

××××の取り組み検討状況について（情報提供） - メッセージ

ファイル(F)　編集(E)　表示(V)　挿入(I)　書式(O)　ツール(T)　アクション(A)　ヘルプ(H)

返信(R)　全員へ返信(L)　転送(W)

① 差出人: 田中 太郎 [taro.tanaka@gmail.com]
宛先: 鈴木 次郎 [jiro.suzuki@houterasu.or.jp]
CC:
② 件名: ××××の取り組み検討状況について（情報提供）
③ 添付ファイル: ××××見積書.exe (295 KB)

関係各位

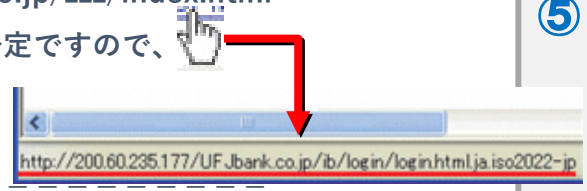
お疲れさまです。
○○部△△△△課の田中です。

④ △△△△課では××××の取り組みについて検討を行いました。

検討結果の資料を以下のURLに公表しています。
⑤ URL: http://xxx.yyy.tokyo.jp/zzz/index.html

来週にも公式発表される予定ですので、至急ご確認ください。

よろしくお願いします。




－－－－－－－－－－－－－－－－－－－－－－－－

⑥ □□□事務所○○部△△△△課
田中　太郎　E-mail:taro.tanaka@houterasu.or.jp
TEL:0 3 -3111-2222　FAX:03-3111-2223
－－－－－－－－－－－－－－－－－－－－－－－－

## 見抜くポイント！

### ① 差出人（送信者）

送信者の名前やアドレスが見慣れない。
組織内の話題が外部アドレスで届いている。
フリーメールアドレスから送信。
関係者のメールアドレスに偽装
（後ろに異なるアドレスが表示されている）。

### ② 件名

興味を持たせて開封したくなる内容。
【緊急】と急がせて吟味させまいとしている。

### ③ 添付ファイル

本文と関係のないファイル名である。
実行形式ファイル（exe / scr / cplなど）、ショートカットファイル（lnk など）が添付されている。
上記ファイルとわからないようアイコン偽装。

### ④ 本文

記載URLをクリックさせるよう不自然に誘導。
信頼しそうな組織になりすましている。

### ⑤ URL

本文表示とカーソル時のURLが異なる（HTMLメールの場合）。

### ⑥ 署名

送信者の署名が存在しないか、曖昧である。
架空の組織名、氏名を使っている。
差出人のメールアドレスと署名が異なる。
本人は実在するが電話番号が実在しない。

# 情報セキュリティ事故事例①

## 委託先が「Emotet」感染、個人情報が流出の可能性 - 相模原市

神奈川県相模原市は、業務委託先がマルウェア「Emotet」に感染し、同市の委託業務に関連する個人情報などが流出した可能性があることを明らかにした。
同市によれば、委託先事業者のパソコンがマルウェア「Emotet」に感染。削除していなかった委託業務に関連するメールが外部に流出したもの。3月17日にメールを受信した事業者や個人から同市に連絡があり問題が判明した。
在宅医療、介護連携事例発表会の参加者に関する情報169件をはじめ、アウトリーチ事例検討会の参加者関連情報125件、テイクアウトメニュー販売会の参加店舗に関する情報4件などが外部へ流出した可能性がある。

（Security NEXT - 2022/03/28 ）

https://www.security-next.com/135184

**POINT**

委託先で発生した事故であっても、委託元の管理責任が問われます。

# 情報セキュリティ事故事例②

## SQLi攻撃でメールアドレスが流出か - アウトドア用品企画会社

アウトドア用品やゲーミング家具などの企画、開発を行っているビーズは、ウェブサイトが不正アクセスを受け、顧客や取引先のメールアドレスが流出した可能性があることを明らかにした。
同社によれば、SQLインジェクションの脆弱性を突く外部からの不正アクセスを受けたことを2月21日に認知し、調査を行ったところ、保有するメールアドレスの一部が流出している可能性が判明したという。
流出の可能性があるのは、アンケートに回答した一部顧客や同社の部品販売システムで2013年6月から2016年4月にかけて利用された顧客のメールアドレス1万772件。取引先のメールアドレス1万2663件も含まれる。

（Security NEXT - 2022/03/03 ）
https://www.security-next.com/134486

**POINT**

SQLi攻撃とは、HPの脆弱性を狙った不正アクセス手法です。

# 情報セキュリティ事故事例③

## メール誤送信で学外の研究参加者のメアド流出 - 長崎県立大

長崎県立大学は、同大が実施する横断研究の参加者へ送信した事務連絡メールで誤送信が発生し、メールアドレスが流出したことを明らかにした。
同大によれば、2月24日14時前、同大が実施する五島市における横断研究の一部参加者57人へ送信した事務連絡メールで誤送信が発生したもの。
送信先を誤って宛先に入力したため、受信者間でメールアドレスが閲覧できる状態となった。

（Security NEXT - 2022/03/03 ）

https://www.security-next.com/134566

**POINT**

誤送付、誤送信は最も多いセキュリティ事故の一つです。
送信前の宛先のチェックを改めて行いましょう。

# テレワークにおけるセキュリティ

感染症対策により一気に広まったテレワークですが、今後も導入が進展していきます。しかし、家庭における情報セキュリティ対策のレベルは、オフィスとの比較において著しく低下することに留意したうえで、オフィスとは違ったセキュリティ対策について検討しなければなりません。

オフィス

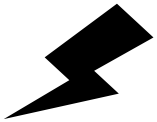
情報へのアクセス

不正持出・利用

情報や端末の持ち出しは許可を得たうえで行う！


使用する端末は会社が貸与したもの、又は許可したものに限定！

通信



盗聴
フィッシング・・

通信は暗号化すること！
疑問点は管理者に確認する！

利用端末

マルウェア感染

作業環境

盗聴・盗難

家庭での作業場所、保管場所、廃棄方法に注意！

Cloud

利用サービス

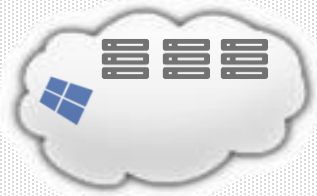
盗聴
割り込み・・

Web会議などのコミュニケーションツールは脆弱性も確認する！
会社が指定するサービスを利用すること！（次のスライド参照）

# オンラインミーティングにおけるセキュリティ

新しい情報技術の採用や業務プロセスの改革には情報セキュリティの脆弱性が伴います。 Web会議の業務利用が始まりましたが、情報セキュリティリスクが伴う事を意識しながら利用することが大切です。以下に想定されるリスクと対策を示します。

## 準備段階



**セキュリティが脆弱なシステムの利用**

Web会議ツールは情報システム管理者から指定されたものを使用する！
※指定以外のツールを使用する必要がある場合は情報システム管理課に相談する。

PC端末及びWeb会議ツールのアップデートが必要な場合は指示に従い確実に余裕を持って行う！

## 実施段階

**意図しない参加者の紛れ込み**

外部関係者が参加するWeb会議では、参加者の事前登録機能、待機室(ロビー)での参加者確認機能を活用する！

**盗み見・盗み聞き**
**意図しない映り込みによる情報漏えい**
**(背景に掲示された書類など)**

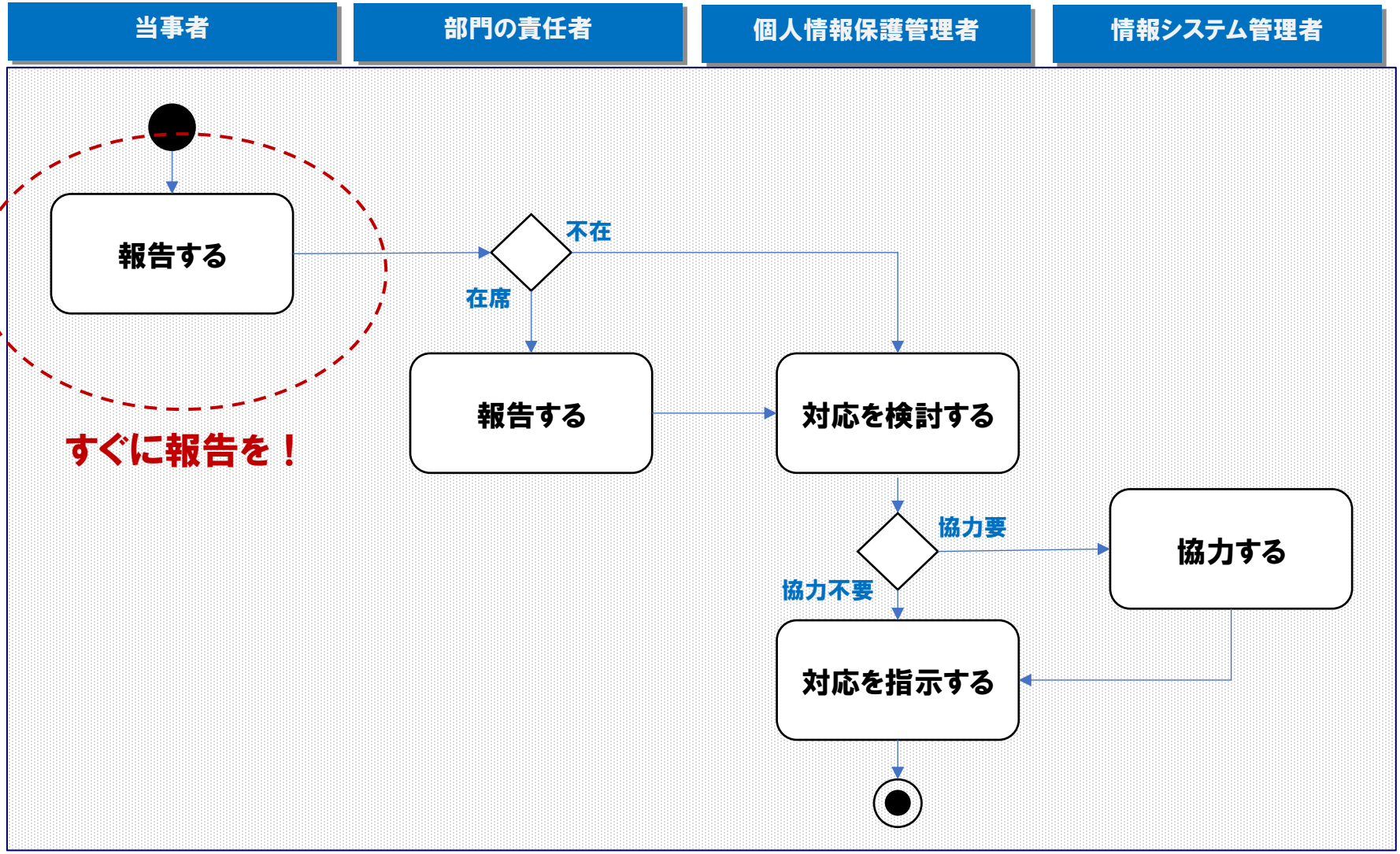
実施する場所に注意！
背景にも注意！

**誤った資料の共有**

会議に使用しないファイルは閉じて置くこと！

# 報告

セキュリティの事故が生じた際は、迅速な報告が大切です。些細な事でもすぐに報告しましょう。
報告が遅れると事態がどんどん悪化する危険性があります。くれぐれも自分一人で解決しようなどとは思わないでください！



# 心掛け

その他、以下の点につていても注意を払いましょう。

**むやみに個人の住所、電話番号を教えないこと**

社外からの問合せに、本人の承諾なしに従業員等の自宅住所や電話番号等は教えてはいけません。本人から折り返し連絡を入れる旨を、問合せ先に伝えましょう。

**予期しない個人情報の提供が発生していないか気をつけること**

個人情報の提供には、原則として本人の同意が必要です。資料・データを社外へ提供するときは、個人情報や秘密情報を含んでいないか、含む場合は提供が社内で承認されているかを必ず確認してください。

最後に・・

**個人情報保護は組織の誰かがやるものではなく、全員で取り組むべき組織としての仕組みなのです。決して他人事と思ってはいけません。**
**疑問に感じた点を曖昧にせずどんどん管理者に確認しましょう。**