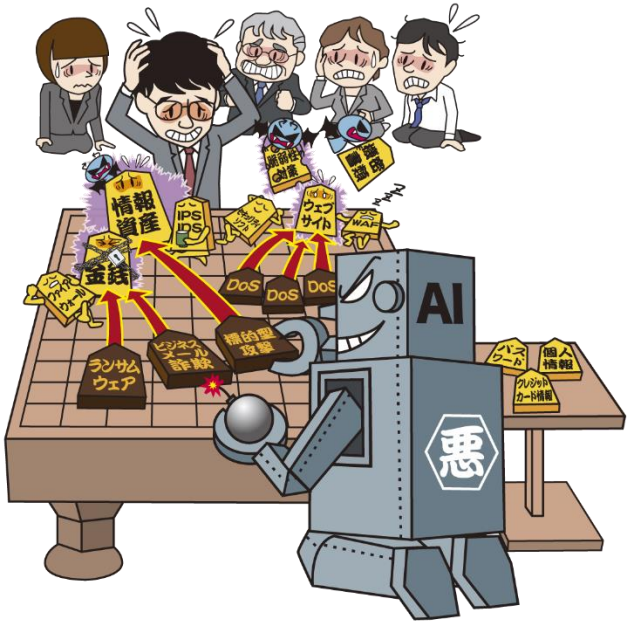
IPA Better Life with IT

# 情報セキュリティ10大脅威 2019

## ～情報セキュリティ10大脅威 組織編～

### ～局面ごとにセキュリティ対策の最善手を～




独立行政法人情報処理推進機構（IPA）
セキュリティセンター
2019年6月

# 情報セキュリティ10大脅威 2019

- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」の投票により、
    情報システムを取巻く脅威を順位付けして解説


情報セキュリティ
10 大脅威 2019
～局面ごとにセキュリティ対策の最善手を～
IPA 独立行政法人 情報処理推進機構 セキュリティセンター
2019 年 3 月


1 章 情報セキュリティ 10 大脅威 2019 概要

■「情報セキュリティ 10 大脅威 2019」
2018 年において社会的に影響が大きかったセキュリティ上の脅威について「10 大脅威選考会」の投票結果に基づき、「情報セキュリティ 10 大脅威 2019」では、「個人」と「組織」向け脅威として、それぞれ表 1.1 の通り順位付けした。

表 1.1 情報セキュリティ 10 大脅威 2019「個人」および「組織」向けの脅威の順位

| 「個人」向け脅威 | 順位 | 「組織」向け脅威 |
|---|---|---|
| クレジットカード情報の不正利用 | 1 | 標的型攻撃による被害 |
| フィッシングによる個人情報等の詐取 | 2 | ビジネスメール詐欺による被害 |
| 不正アプリによるスマートフォン利用者への被害 | 3 | ランサムウェアによる被害 |
| メール等を使った脅迫・詐欺の手口による金銭要求 | 4 | サプライチェーンの弱点を悪用した攻撃の高まり |
| ネット上の誹謗・中傷・デマ | 5 | 内部不正による情報漏えい |
| 偽警告によるインターネット詐欺 | 6 | サービス妨害攻撃によるサービスの停止 |
| インターネットバンキングの不正利用 | 7 | インターネットサービスからの個人情報の窃取 |
| インターネットサービスへの不正ログイン | 8 | IoT 機器の脆弱性の顕在化 |
| ランサムウェアによる被害 | 9 | 脆弱性対策情報の公開に伴う悪用増加 |
| IoT 機器の不適切な管理 | 10 | 不注意による情報漏えい |

IPA から「10 大脅威選考会」に 2019 年版の投票を依頼するにあたり、2018 年版の脅威候補に対して見直しを行った。

本章では、「情報セキュリティ 10 大脅威 2019」の脅威候補の変更点と「情報セキュリティ 10 大脅威 2019」にランクインした脅威の特徴を記載する。なお、各脅威の詳細については 2 章にて解説する。

6

# 情報セキュリティ10大脅威 2019

IPA

## 章構成

### 1章.情報セキュリティ10大脅威 2019 概要

- 10大脅威の概要およびセキュリティ対策の基本を解説

### 2章.情報セキュリティ10大脅威 2019

- 脅威の概要と対策について解説
- 個人と組織における各脅威の解説

### 3章.注目すべき脅威や懸念

- 知っておくべき脅威や懸念を解説

# 情報セキュリティ10大脅威 2019 脅威ランキング

IPA

| 「個人」向け脅威 | 順位 | 「組織」向け脅威 |
|---|---|---|
| クレジットカード情報の不正利用 | 1 | 標的型攻撃による被害 |
| フィッシングによる個人情報等の詐取 | 2 | ビジネスメール詐欺による被害 |
| 不正アプリによる<br>スマートフォン利用者への被害 | 3 | ランサムウェアによる被害 |
| メール等を使った<br>脅迫・詐欺の手口による金銭要求 | 4 | サプライチェーンの弱点を悪用した<br>攻撃の高まり |
| ネット上の誹謗・中傷・デマ | 5 | 内部不正による情報漏えい |
| 偽警告によるインターネット詐欺 | 6 | サービス妨害攻撃によるサービスの停止 |
| インターネットバンキングの不正利用 | 7 | インターネットサービスからの<br>個人情報の窃取 |
| インターネットサービスへの不正ログイン | 8 | IoT機器の脆弱性の顕在化 |
| ランサムウェアによる被害 | 9 | 脆弱性対策情報の公開に伴う悪用増加 |
| IoT機器の不適切な管理 | 10 | 不注意による情報漏えい |

# 情報セキュリティ対策の基本

| 攻撃の糸口 | 情報セキュリティ対策の基本 | 目的 |
|---|---|---|
| ソフトウェアの脆弱性 | ソフトウェアの更新 | 脆弱性を解消し攻撃によるリスクを低減する |
| ウイルス感染 | セキュリティソフトの利用 | 攻撃をブロックする |
| パスワード窃取 | パスワードの管理・認証の強化 | パスワード窃取によるリスクを低減する |
| 設定不備 | 設定の見直し | 誤った設定を攻撃に利用されないようにする |
| 誘導（罠にはめる） | 脅威・手口を知る | 手口から重要視するべき対策を理解する |

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 後述する各脅威における対策のほか、上記対策は常に意識

# 情報セキュリティ10大脅威 2019
# 組織編　各脅威の解説

※以降の各脅威の対策では、前項の「情報セキュリティ対策の基本」は実施されている前提とし、記載には含めていません。

# 【1位】標的型攻撃による被害

## ～標的型攻撃メールの多くはOffice文書ファイルを悪用～


- メール等によりPCをウイルスに感染させ組織内部へ潜入
- 長期にわたって侵害範囲を徐々に広げる
- 組織の機密情報を窃取

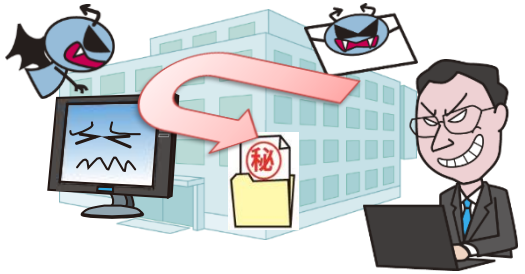
# 【1位】標的型攻撃による被害
## ～標的型攻撃メールの多くはOffice文書ファイルを悪用～

IPA

- 攻撃手口

**・ウイルスに感染させて機密情報を窃取**

- メールを利用した手口（標的型攻撃メール）
  - 不正な添付ファイルを開かせる
  - 不正なウェブサイトへのリンクをクリックさせる
- ウェブサイトを利用した手口
  - 標的組織が頻繁に利用するウェブサイトを調査し、当該サイトを閲覧するとウイルスに感染するように改ざん（水飲み場型攻撃）



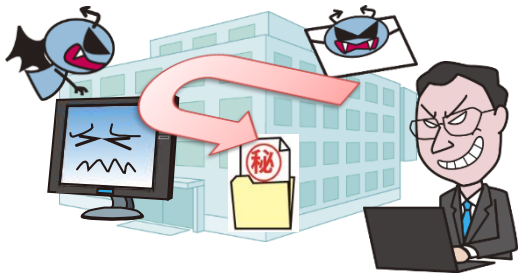
# 【1位】標的型攻撃による被害
## ～標的型攻撃メールの多くはOffice文書ファイルを悪用～

IPA

- 攻撃手口

**・不正アクセスによって機密情報を窃取**

- 不正アクセスによる手口
  - 組織が利用するクラウドサービスへ不正にログイン
  - 社内システムへ正規の経路を悪用し不正にアクセス
  - 社内システムへウイルスを感染させる



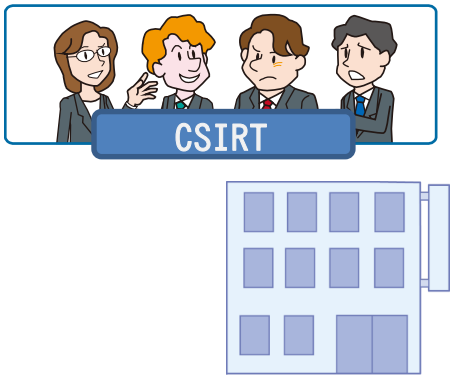
# 【1位】標的型攻撃による被害
## ～標的型攻撃メールの多くはOffice文書ファイルを悪用～

- 2018年の事例/傾向
  - サイバー情報共有イニシアティブ(J-CSIP)による報告
    - 悪意のあるCSVファイルが添付されたメールを観測 (※1)
      (Excelの起動時にプログラムを実行する機能を悪用)
    - MS Office製品の文書ファイルを悪用した手口も観測 (※2)
      ファイルの拡張子は「.wiz」、「.iqy」、「.slk」等
      (WordやExcelの起動時にプログラムを実行する機能を悪用)

【出典】
※1 サイバー情報共有イニシアティブ(J-CSIP)運用状況 [2018年1月～3月]
https://www.ipa.go.jp/files/000066063.pdf
※2 WIZファイルを悪用する攻撃手口に関する注意喚起
https://www.ipa.go.jp/files/000069663.pdf

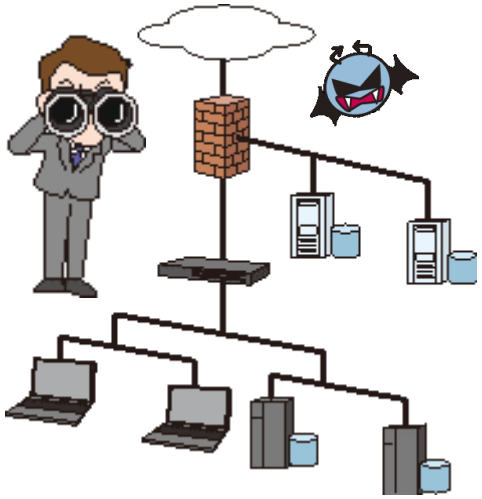
# 【1位】標的型攻撃による被害
## ～標的型攻撃メールの多くはOffice文書ファイルを悪用～

- 対策
  - 経営者層
    - ・組織としての体制の確立
      - –迅速かつ継続的に対応できる組織内体制（CSIRT）の構築
      - –対策予算の確保と継続的な対策実施
      - –セキュリティポリシーの策定
  - セキュリティ担当者
    - ・被害の予防/対応力の向上
      - –情報の管理とルール策定
      - –セキュリティ教育・インシデント訓練
      - –サイバー攻撃に関する情報収集
    - ・被害を受けた後の対応
      - –CSIRTの運用
      - –影響調査および原因の追究、対策の強化



# 【1位】標的型攻撃による被害
## ～標的型攻撃メールの多くはOffice文書ファイルを悪用～

- 対策
  - システム管理者
    - ・被害の予防
      - –セキュアなシステム設計
      - –アクセス制御・データの暗号化
      - –ネットワーク分離
    - ・被害の早期検知
      - –ネットワーク監視・防御
      - –エンドポイントの監視・防御
  - 従業員、職員
    - ・情報リテラシーの向上
      - –セキュリティ教育の受講
    - ・被害を受けた後の対応
      - –CSIRTへ連絡



# 【2位】ビジネスメール詐欺による被害

## ～日本語のメールが使用されたビジネスメール詐欺の事例も～


- 取引先や経営者とやりとりするようなビジネスメールを装う
- メールを巧妙に細工し、企業の金銭を取り扱う担当者を騙す
- 攻撃者の用意した口座へ送金させる

# 【2位】ビジネスメール詐欺による被害

～日本語のメールが使用されたビジネスメール詐欺の事例も～

## ● 攻撃手口

・何らかの手段を用いて標的組織の業務情報等を窃取
・窃取した情報を利用したメールで送金依頼（金銭詐取）

- 取引先との請求書を偽装
- 経営者へのなりすまし
- 窃取した標的組織のメールアカウントの悪用
- 社外の権威ある第三者へのなりすまし

# 【2位】ビジネスメール詐欺による被害

## ～日本語のメールが使用されたビジネスメール詐欺の事例も～

- 2018年の事例/傾向
  - ビジネスメール詐欺で日本人の逮捕者 (※1)
    - ・2018年7月、米国の農業関連会社が約7,800万円の被害に
    - ・日本国内の会社役員ら男女4名が逮捕
  - 日本語が使用されたビジネスメール詐欺 (※2)
    - ・2018年、日本語が使用されたビジネスメール詐欺のメールに関してIPAで情報提供を受ける
    - ・2018年8月、当該事例や手口に関する注意喚起を実施
      （海外との取引や英語メールのやりとりがない国内組織も注意）

【出典】
※1 7千万円送金させた疑い ビジネスメール詐欺で逮捕
https://www.nikkei.com/article/DGXMZO32602020U8A700C1CC1000/
※2 【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口（続報）
https://www.ipa.go.jp/security/announce/201808-bec.html

# 【2位】ビジネスメール詐欺による被害

～日本語のメールが使用されたビジネスメール詐欺の事例も～

## ● 対策

### ■ 組織（金銭の決裁権限を持つ責任者、金銭を取り扱う担当者）

・被害の予防

<メールの真正性の確認>

－普段とは異なるメールに注意

－メール以外の方法で事実確認

－送信元のメールドメインに注意

－過剰に判断を急がせるメールに注意

－電子署名の付与

<メールアカウントの適切な管理>

－パスワードの適切な管理

－ログイン通知機能等で不正ログイン対策

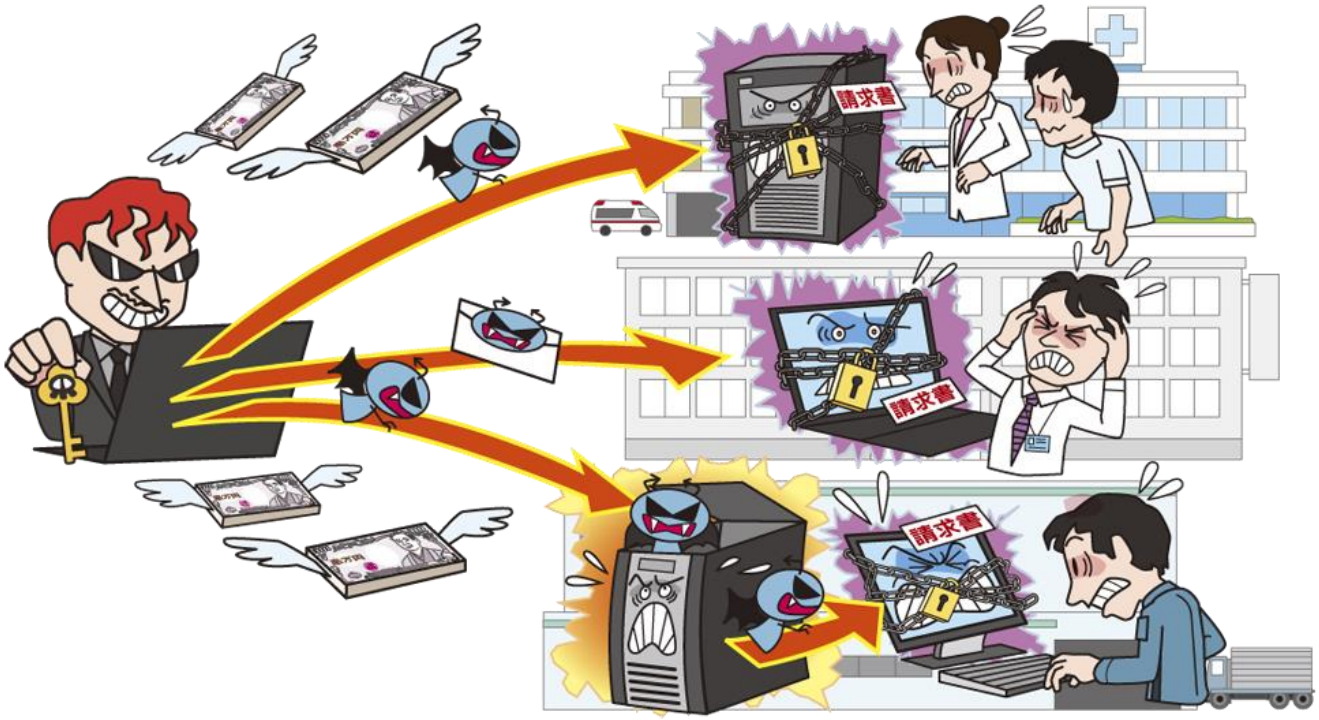
# 【2位】ビジネスメール詐欺による被害

## ～日本語のメールが使用されたビジネスメール詐欺の事例も～

- 対策
  - 組織（金銭の決裁権限を持つ責任者、金銭を取り扱う担当者）
    - ・被害を受けた後の対応
      - –CSIRTへの連絡
      - –警察に相談
      - –踏み台や詐称されている組織への連絡
      - –影響調査および原因追及、対策の強化

# 【3位】ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～




- PCやスマートフォンのファイル暗号化や画面ロックを行い制限をかけ、解除と引き換えに金銭要求
- 業務に必要なファイルを暗号化された場合、事業継続にも支障がでるおそれがある

# 【3位】ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～

## 攻撃手口

**・ウイルス（ランサムウェア）に感染させて金銭を要求**

### メールを利用した手口

・不正な添付ファイルを開かせる

### 不正アクセスによる手口

・管理用のRDP（リモートデスクトップ）等でサーバーに不正アクセス

・サーバー上で攻撃者がウイルスを実行（感染させる）

# 【3位】ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～

## 攻撃手口

**・ウイルス（ランサムウェア）に感染させて金銭を要求**

### 脆弱性を悪用した手口

- ・OSの脆弱性を悪用しウイルスを実行（感染させる）
- ・攻撃ツール等を利用してネットワーク越しに次々と感染させる

### ウェブサイトを利用した手口

- ・ランサムウェアをダウンロードさせるようにウェブサイトを改ざん
- ・当該サイトを閲覧するようにメールなどで誘導

# 【3位】ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～

- 2018年の事例/傾向
  - 病院の電子カルテシステムがランサムウェアに感染 (※1)
    - ・電子カルテシステムが約二日間停止
    - ・要求された金銭は支払わなかった
    - ・バックアップシステムの不備によりデータが一部復元不可
  - 「SamSam」の被害総額約6億7,000万円に (※2)
    - ・2015年頃から確認されているランサムウェア
    - ・サーバーの管理等に用いるRDPにてサーバーにアクセスし、ランサムウェアを実行(感染させる)

【出典】
※1 電子カルテシステムの障害発生について
https://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/press-release.pdf
※2 SamSam: 600 万ドル (約6億7000万円) 近くの身代金を手にしたランサムウェア
https://www.sophos.com/ja-jp/press-office/press-releases/2018/08/samsam-the-almost-6-million-ransomware.aspx

# 【3位】ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～

## 対策

### 経営者層

・組織としての対応体制の確立

- 迅速かつ継続的に対応できる体制（CSIRT等）構築
- 対策の予算の確保と継続的な対策の実施

### システム管理者、従業員

・被害の予防

- 受信メール、ウェブサイトの十分な確認
- サポートの切れたOSの利用停止、移行
- フィルタリングツールの活用
- ネットワーク分離
- 共有サーバのアクセス権最小化
- バックアップの取得

# 【3位】ランサムウェアによる被害

～ランサムウェアに感染し、不当に金銭を要求されたり、業務を妨害される～

- 対策
  - システム管理者、従業員

・被害を受けた後の対応

－CSIRTへ連絡

－バックアップからの復旧

－復号ツールの活用

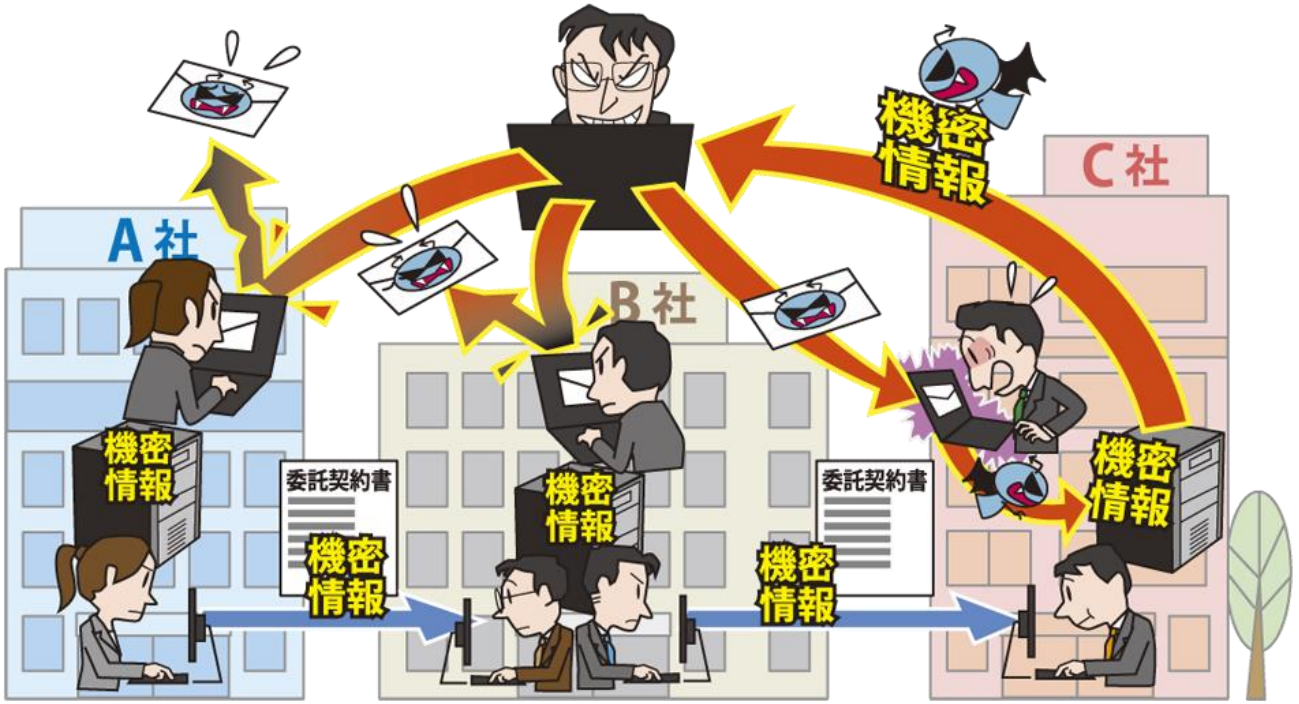
－影響調査および原因の追究、対策の強化

＜例外措置＞

推奨はされないが、暗号化されたファイルが人命に関わると、
金銭を支払ったケースも。

# 【4位】サプライチェーンの弱点を悪用した攻撃の高まり

## ～業務委託先にも適切なセキュリティ管理を要求～




- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先などの一連の商流（サプライチェーン）において、セキュリティ対策が甘い組織が攻撃の足がかりとして狙われる
- 一部業務を委託している外部委託先組織から情報が漏えい

# 【4位】サプライチェーンの弱点を悪用した攻撃の高まり

～業務委託先にも適切なセキュリティ管理を要求～

## ● 要因

**・自組織のみがセキュリティ対策を講じても穴ができる**

- サプライチェーンのセキュリティ対策不足
- サプライチェーンを適切に選定、管理していない
- 再委託先や再々委託先の管理は困難
  - ・委託先組織の先に再委託先組織や再々委託先組織がある場合、その管理は委託先組織が行うため、委託元からのセキュリティ対策管理はさらに難しくなる

# 【4位】サプライチェーンの弱点を悪用した攻撃の高まり

## ～業務委託先にも適切なセキュリティ管理を要求～

- 2018年の事例/傾向
  - 委託先への不正アクセスによる情報漏えい（※1）
    - ・業務委託を行っていた委託先の企業に対し不正アクセスが行われ、電子メールアドレスが漏えいした
  - 実施すべき情報セキュリティ対策を仕様書等で明示していない組織が多い（※2）
    - ・IPAが公開した調査結果によると、情報通信業以外の委託元企業の過半数が明示していない（特に、製造業では71%、卸売業・小売業では74%）

【出典】
※1 不正アクセスによるお客様情報の流出に関するお詫び
https://www.porsche.co.jp/news/201802-001.php
※2 「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」報告書について
https://www.ipa.go.jp/security/fy29/reports/scrm/index.html

# 【4位】サプライチェーンの弱点を悪用した攻撃の高まり

## ～業務委託先にも適切なセキュリティ管理を要求～

- **対策**
  - **委託元組織**
    - ・被害の予防
      - –業務委託や情報管理における規則の徹底
      - –信頼できる委託先組織の選定
      - –委託先からの納品物の検証
      - –契約内容の確認
      - –委託先組織の管理
    - ・被害を受けた後の対応
      - –影響調査および原因の追究、対策の強化
      - –被害への補償

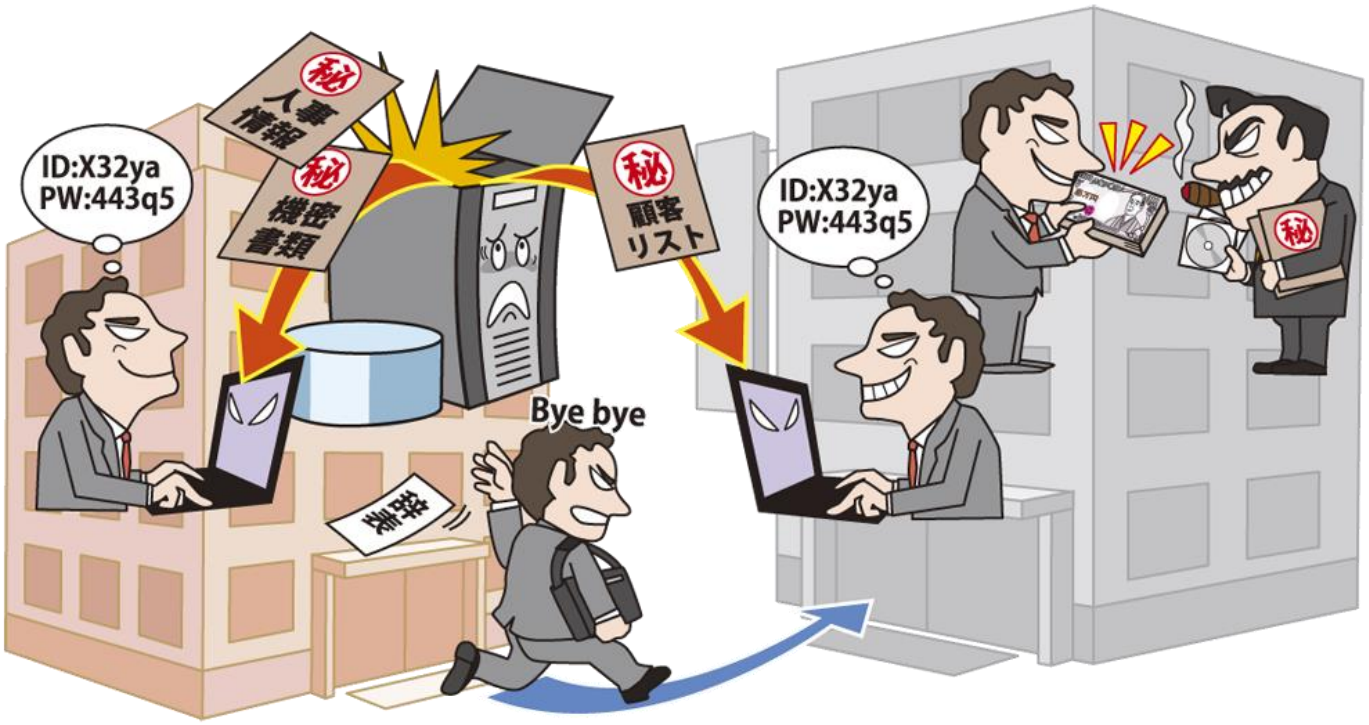
# 【4位】サプライチェーンの弱点を悪用した攻撃の高まり

## ～業務委託先にも適切なセキュリティ管理を要求～

- **対策**
  - **委託先組織**
    - ・被害の予防
      - －攻撃者の目的や攻撃手段は多岐にわたるため、他の脅威の対策も参考に業務に応じた広範な対策が必要
    - ・被害を受けた後の対応
      - －委託元への連絡

# 【5位】内部不正による情報漏えい

## ～不正を許さない管理・監視体制を～




- 組織の従業員や元従業員等による機密情報の漏えい
- 組織関係者による不正行為により、組織の社会的信用の失墜、損害賠償による経済的損失

# 【5位】内部不正による情報漏えい

～不正を許さない管理・監視体制を～

## ● 攻撃手口

**・内部の従業員は重要情報にアクセスしやすい**
**・悪意をもって情報を外部に提供してしまう**

### ■ アクセス権限の悪用

・付与されたパスワードを悪用し、組織の重要情報を取得
・必要以上のアクセス権限を付与していると被害が大きくなる

### ■ 離職前のアカウントの悪用

・離職前に使用していたアカウントを使って不正に情報を取得

### ■ USBメモリーやメール等による持ち出し

# 【5位】内部不正による情報漏えい

## ～不正を許さない管理・監視体制を～

- 2018年の事例/傾向
  - 従業員が社員情報を私物パソコンに転送（※1）
    - ・自組織の業務用パソコンを分解してハードディスクを抜き取り、賃金データ等を私用パソコンに転送し他団体に送付
  - 従業員が顧客のクレジットカード情報を窃取（※2）
    - ・元アルバイト従業員が勤務時に顧客のクレジットカード情報を窃取しインターネット通販で不正利用

【出典】
※1 日経が元社員を告訴 社員3千人分の賃金データ漏洩容疑
https://www.asahi.com/articles/ASL735TGPL73UTIL047.html
※2 従業員がカード情報を盗み取りネット通販で不正利用（セキ薬品）
https://scan.netsecurity.ne.jp/article/2018/08/27/41320.html

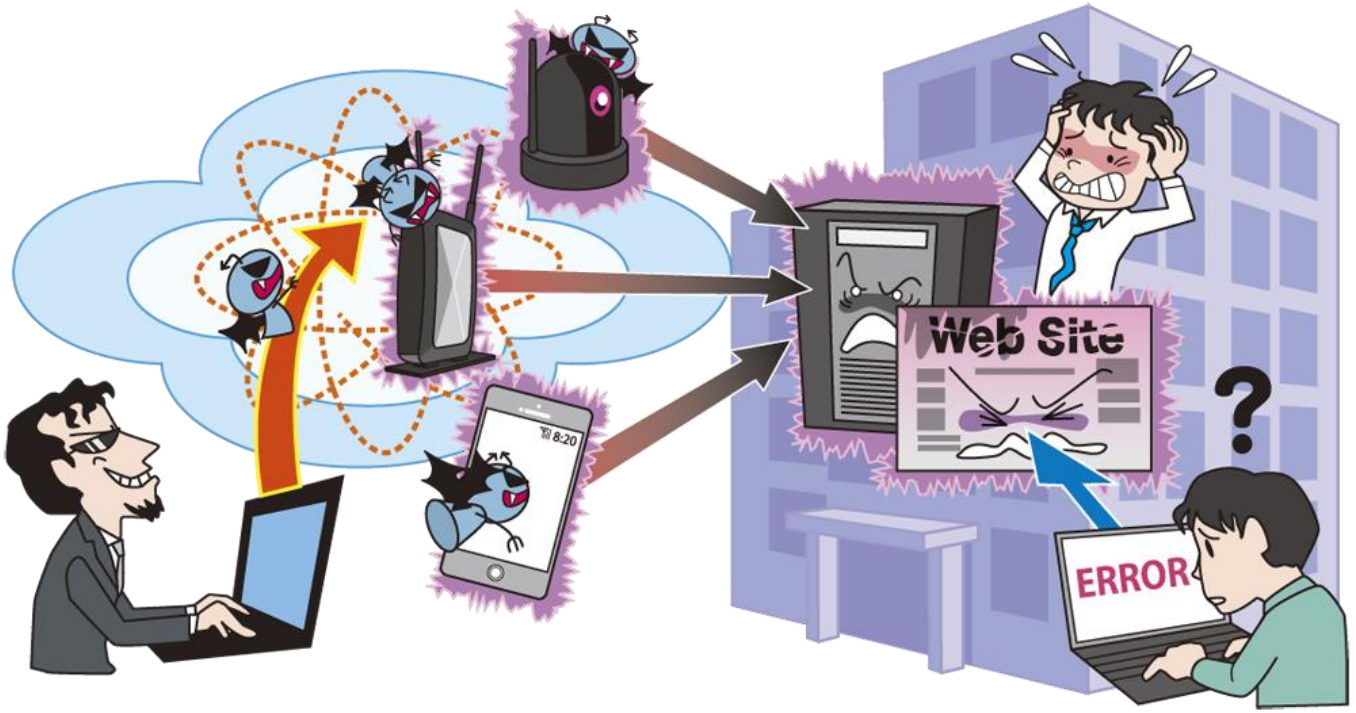
# 【5位】内部不正による情報漏えい

## ～不正を許さない管理・監視体制を～

- **対策**
  - **経営者、管理者**
    - ・被害の予防
      - －基本方針の策定
      - －情報資産の把握、体制の整備
      - －重要情報の管理、保護
    - ・情報モラルの向上
      - －人的管理、コンプライアンス教育徹底
    - ・被害の早期検知
      - －システム操作履歴の監視
    - ・被害を受けた後の対応
      - －CSIRT、警察等への連絡
      - －影響調査および原因の追究、対策の強化
      - －内部不正者に対する適切な処罰実施

# 【6位】サービス妨害攻撃によるサービスの停止

## ～国内外問わず大規模なDDoS攻撃が発生～




- 標的組織のサーバー等に大量の通信による高負荷をかける
- 高負荷をかけられたサーバーは処理遅延やサービス停止
- サービス停止による機会損失、信用失墜等の被害

# 【6位】サービス妨害攻撃によるサービスの停止
～国内外問わず大規模なDDoS攻撃が発生～

## ● 攻撃手口

**・サーバーに大量の処理要求を送信し高負荷状態に**

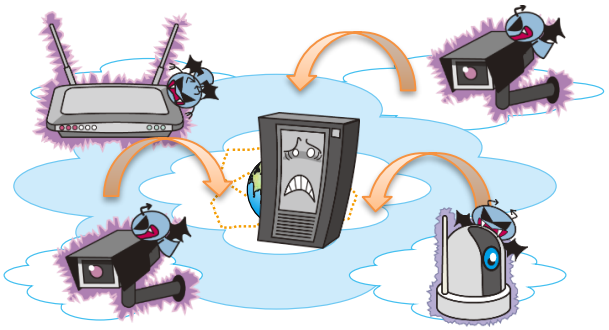
### ■ ボットネットを利用したDDoS攻撃
・ウイルス感染させた端末等からボットネットを形成し、DDoS攻撃に利用する

### ■ リフレクター攻撃
・送信元のIPアドレスを標的組織のサーバーに偽装したパケットを多数のDNSサーバーやSNMPサーバー等に送信する

### ■ DDoS代行サービスの利用
・ダークウェブ等にあるDDoS代行サービスを利用
・専門的な技術が無くても比較的容易に攻撃を行える

# 【6位】サービス妨害攻撃によるサービスの停止
## ～国内外問わず大規模なDDoS攻撃が発生～

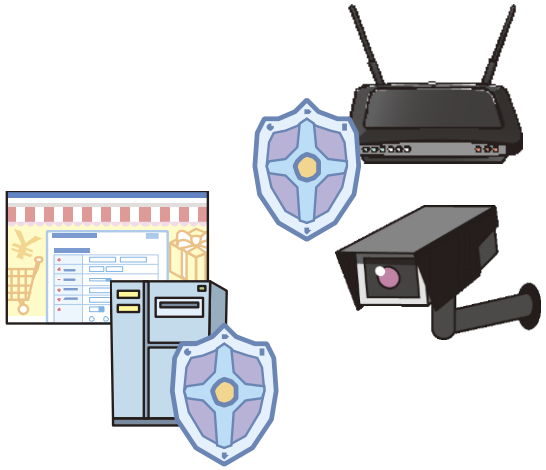
- 2018年の事例/傾向
  - memcachedによる大規模なDDoS攻撃（※1）
    - オープンソースのメモリキャッシュシステムを踏み台に利用
    - 最大335万ppsのパケットによる33.08Gbpsもの通信量
  - DDoS攻撃によるサービス利用制限（※2）
    - 動画サイトへのDDoS攻撃で処理遅延やサービス停止
    - 通信を遮断しても手段を変えて執拗なDDoS攻撃



【出典】
※1 memcached のアクセス制御に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180009.html
※2 【解除済み】一部地域からの利用制限について
https://blog.nicovideo.jp/niconews/92066.html

# 【6位】サービス妨害攻撃によるサービスの停止
## ～国内外問わず大規模なDDoS攻撃が発生～

- 対策
  - ウェブサイトの運営者
    - ・被害の予防
      - -DDoS攻撃の影響を緩和するISPやCDN等の利用
      - -サーバーへの外部からの適切な通信制御
      - -システムの冗長化等の軽減策
      - -ウェブサイト停止時の代替サーバーの用意や告知手段の整備
    - ・被害を受けた後の対応
      - -CSIRTへの連絡
      - -通信制御
        （攻撃元IPアドレスからの通信遮断等）
      - -サービス利用者への状況の告知
      - -影響調査および原因の追究、対策の強化



# 【7位】インターネットサービスからの個人情報の窃取

## ～インターネットサービスのセキュリティ対策の最確認を～


- インターネットサービス内に保管された個人情報等を窃取される
- 窃取された情報を不正利用される

# 【7位】インターネットサービスからの個人情報の窃取

～インターネットサービスのセキュリティ対策の最確認を～

## ● 攻撃手口

**・不正アクセスでインターネットサービスから情報窃取**

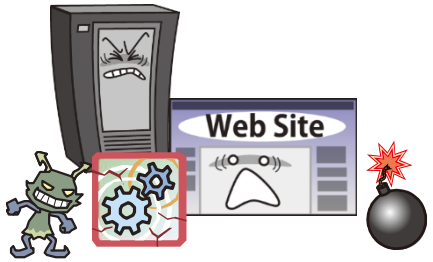
### ■ サーバーのソフトウェアの脆弱性を悪用

・サーバーで稼働するOS、ミドルウェア、CMS等の複数のソフトウェアの脆弱性を悪用

### ■ Webアプリケーションの脆弱性を悪用

・インターネットサービスで稼働しているWebアプリケーションの脆弱性を悪用

（SQLインジェクション攻撃、フォームジャッキングなど）



# 【7位】インターネットサービスからの個人情報の窃取

～インターネットサービスのセキュリティ対策の最確認を～

- 2018年の事例/傾向
  - コンタクトレンズ販売大手のウェブサイトへの攻撃（※1）
    - ・サーバーソフトウェアであるOpenSSLの既知の脆弱性「Heartbleed」を悪用された攻撃
    - ・最大3,412件のクレジットカード情報が漏えい
  - 医療関連組織のウェブサイトへの攻撃（※2）
    - ・システムの脆弱性を突いたSQLインジェクション攻撃
    - ・システムに登録されたメールアドレスやパスワード等、最大で2万名以上の情報が漏えい

【出典】
※1 Webサイトの脆弱性を4年前から放置か、メニコン情報漏洩の原因
https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00561/
※2 不正アクセスで認定医情報が流出か - 日本がん治療認定医機構
http://www.security-next.com/091799

# 【7位】インターネットサービスからの個人情報の窃取

～インターネットサービスのセキュリティ対策の最確認を～

## ● 対策

### ■ インターネットサービス運営者等

・被害の予防

－セキュアなインターネットサービスの構築

－セキュリティ診断の実施

（Webアプリケーション診断やプラットフォーム診断等）

－WAF、IPSの導入

・被害の早期検知

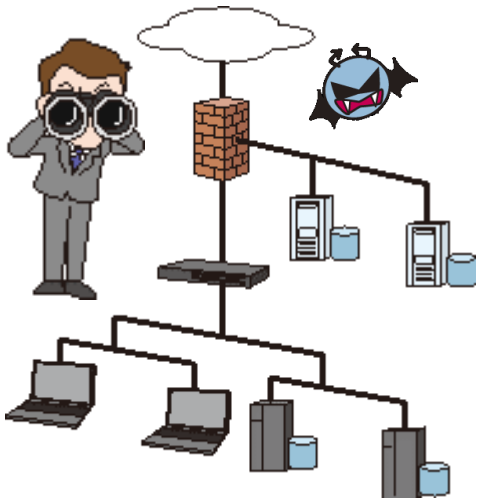
－適切なログと継続的な監視

・被害を受けた後の対応

－CSIRTへの連絡

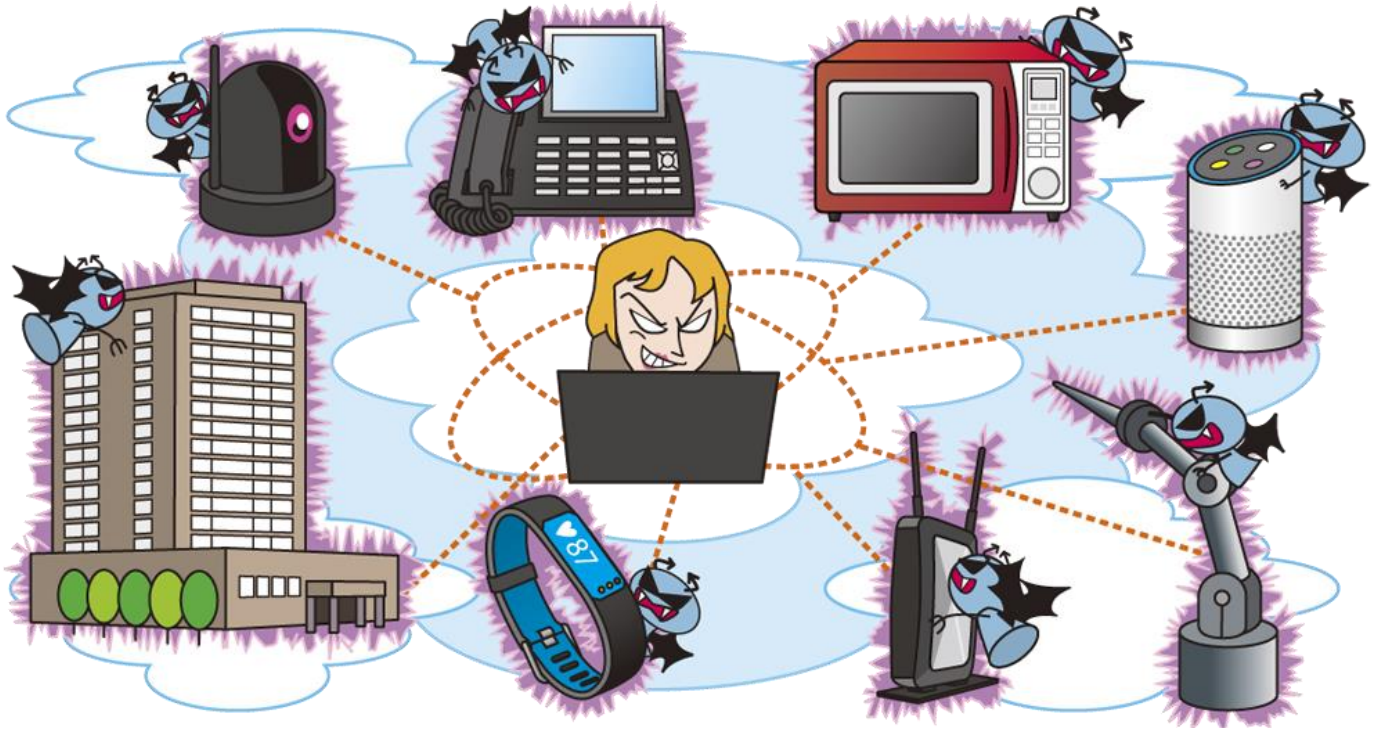
－影響調査および原因の追究、対策の強化

－漏えいした情報に対する利用者への補償



# 【8位】IoT機器の脆弱性の顕在化

## ～IoT機器の脆弱性を突く攻撃が増加、開発ベンダーは対策が急務～



- IoT機器の脆弱性が悪用され、乗っ取られる
- 機能を不正に利用される等、業務に支障がでるおそれ
- DDoS攻撃の踏み台等に利用される

# 【8位】IoT機器の脆弱性の顕在化

～IoT機器の脆弱性を突く攻撃が増加、開発ベンダーは対策が急務～

## ● 攻撃手口

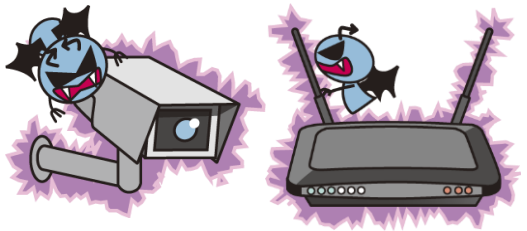
**・IoT機器は当然ながらインターネットに接続している**
**・脆弱性があると不正アクセスやウイルスの被害に**

### ■ 脆弱性を悪用した攻撃

・IoT機器が持つ脆弱性を悪用し、不正アクセスしたりウイルスに感染させたりする

### ■ インターネット上でウイルスが感染活動を行う

・同じ脆弱性を持つIoT機器がインターネット上にないか探索し、脆弱性があればそのIoT機器もウイルスに感染させる



# 【8位】IoT機器の脆弱性の顕在化

～IoT機器の脆弱性を突く攻撃が増加、開発ベンダーは対策が急務～

## 2018年の事例/傾向

### 河川監視カメラへ不正アクセス（※1）

・カメラに不正アクセスし、「I'm hacked bye2」等の文字を表示するように不正に操作された

### ルーターに侵入し、DNS設定を不正に書き換え（※2）

・DNS設定を書き換えられたルーター経由でウェブサイトを閲覧すると不正なサイトへ誘導される

・誘導されたサイトではFacebookの機能向上をうたったメッセージが表示され、従うと不正なスマホアプリがダウンロードされる

【出典】
※1 河川監視カメラへ不正アクセス、「I'm hacked.bye2」のメッセージ残す
https://scan.netsecurity.ne.jp/article/2018/05/01/40886.html
※2 ルーターの設定書き換え、不正アプリに感染させる攻撃 被害相次ぐ
http://www.itmedia.co.jp/news/articles/1803/30/news106.html

# 【8位】IoT機器の脆弱性の顕在化

～IoT機器の脆弱性を突く攻撃が増加、開発ベンダーは対策が急務～

## 対策

### IoT機器の開発者

・被害の予防

- 初期パスワード変更の強制化
- 脆弱性の解消
  （セキュアプログラミング、脆弱性検査、ファジング等）
- ソフトウェア更新の自動化
- わかりやすい取扱説明書の提供
- 不要な機能の無効化
- 安全なデフォルト設定
- 利用者への適切な管理の呼びかけ
- ソフトウェアサポート期間の明確化

# 【8位】IoT機器の脆弱性の顕在化

## ～IoT機器の脆弱性を突く攻撃が増加、開発ベンダーは対策が急務～

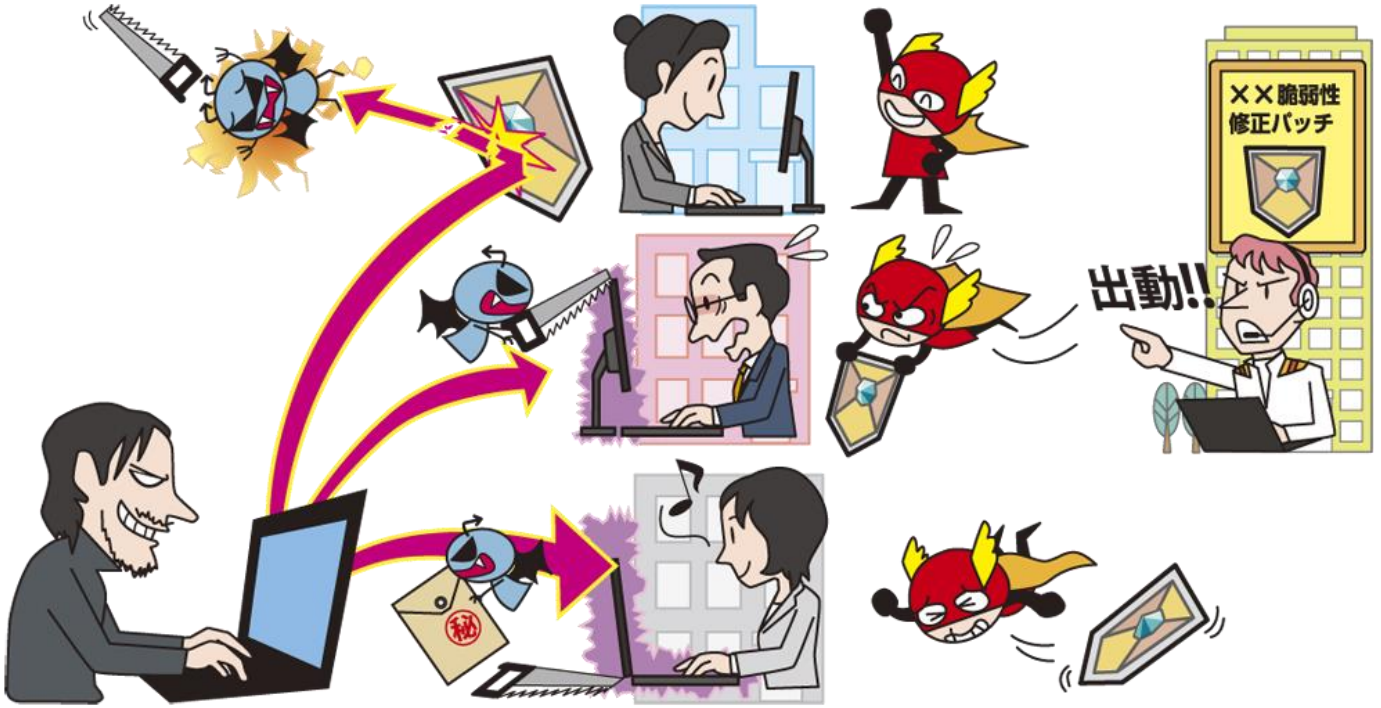
- 対策
  - 組織のシステム管理者、利用者

・被害の予防
  - –パッチが公開されたら迅速に更新
    （自動更新機能の有効化等）
  - –機器の管理画面や管理ポートに対する適切なアクセス制限

・被害を受けた後の対応
  - –CSIRTへの連絡
  - –IoT機器の電源オフ
  - –IoT機器の初期化後、「被害の予防」実施
  - –影響調査および原因の追究、対策の強化

# 【9位】脆弱性対策情報の公開に伴う悪用増加

## ～脆弱性対策はスピード勝負、迅速かつ適切な対応を～




- 脆弱性対策のために公開された脆弱性情報を攻撃に悪用
- 対策未実施の利用者に対して攻撃を行う
- 情報漏えいや改ざん、ウイルス感染等の被害に

# 【9位】脆弱性対策情報の公開に伴う悪用増加

～脆弱性対策はスピード勝負、迅速かつ適切な対応を～

## ● 攻撃手口

・脆弱性が発見されると対策のため情報が公開される
・その情報は攻撃にも悪用できる

### ■ 対策未実施の脆弱性を悪用

・公開された脆弱性を悪用し、当該脆弱性の対策が未実施である利用者に対して攻撃を行う
・利用者が多い製品の場合、攻撃手口を使いまわせるため被害が拡大するおそれがある

# 【9位】脆弱性対策情報の公開に伴う悪用増加

～脆弱性対策はスピード勝負、迅速かつ適切な対応を～

- 2018年の事例/傾向
  - Apache Struts2 の脆弱性を悪用した攻撃 (※1)
    - ・2018年8月に Apache Struts2 の脆弱性が公開
    - ・その数日後には脆弱性を悪用する攻撃コードが公開
    - ・約2週間後には攻撃コードを使ってコインマイナーを仕掛ける活動を観測
  - Drupalの脆弱性情報公開に伴う攻撃の増加 (※2)
    - ・2018年3月にDrupalの脆弱性公開
    - ・その後4月に脆弱性を悪用する攻撃コード公開
    - ・本脆弱性を狙ったと見られる攻撃が国内でも活発化

【出典】
※1 「Apache Struts 2」の脆弱性、仮想通貨採掘攻撃に悪用される
http://www.itmedia.co.jp/enterprise/articles/1809/06/news066.html
※2 「Drupal」脆弱性、国内で1日あたり数万件規模のアクセス - 70カ国以上から
http://www.security-next.com/092540

# 【9位】脆弱性対策情報の公開に伴う悪用増加

～脆弱性対策はスピード勝負、迅速かつ適切な対応を～

## 対策

### システム管理者、ソフトウェア利用者


・被害の予防
  - 資産の把握、体制の整備
  - 脆弱性関連情報の収集
  - WAF、IPSの導入
  - ネットワーク監視および攻撃通信の遮断
  - セキュリティのサポートが充実している ソフトウェアやバージョンを利用
  - すぐに対策パッチが適用できない場合には一時的なサーバー停止等

・被害を受けた場合の対応
  - CSIRTへの連絡
  - 影響調査および原因の追究、対策の強化

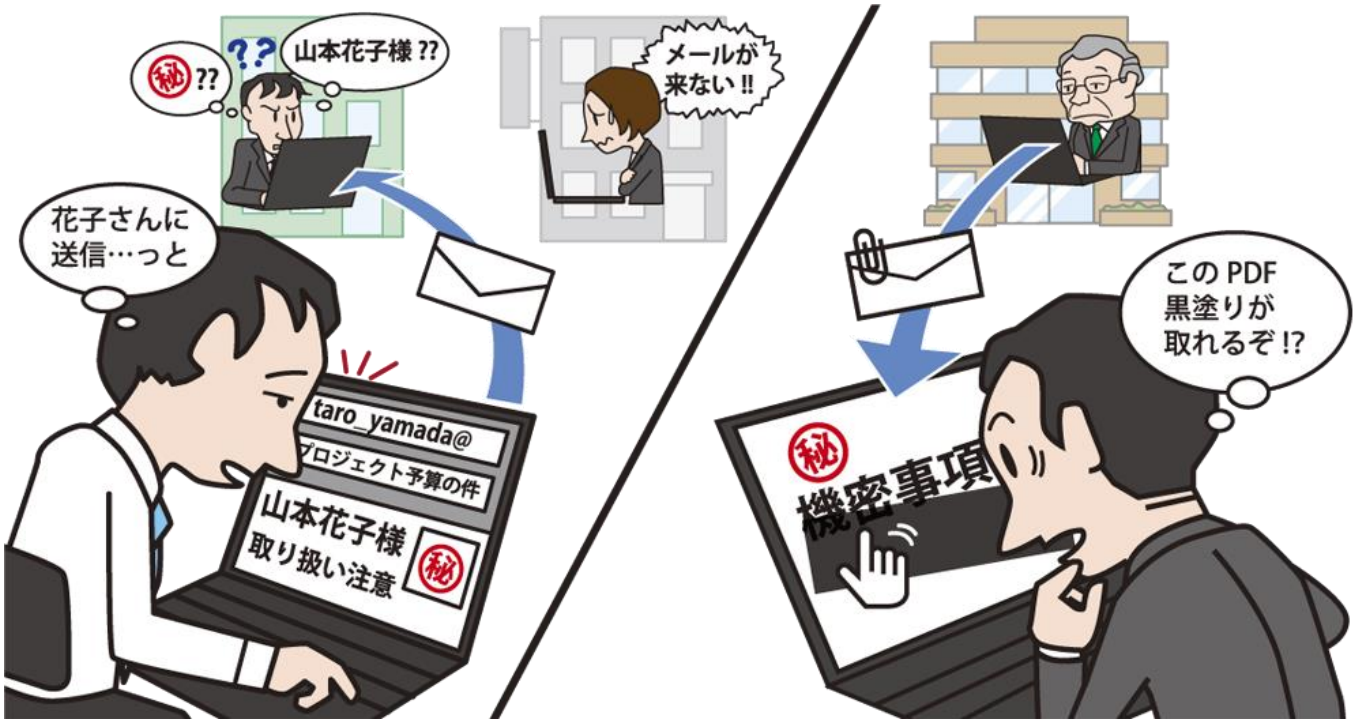
# 【9位】脆弱性対策情報の公開に伴う悪用増加

## ～脆弱性対策はスピード勝負、迅速かつ適切な対応を～

- **対策**
  - **開発ベンダー**
    - ・被害の予防
      - –製品に組み込まれているソフトウェアの把握、管理の徹底
      - –脆弱性関連情報の収集
      - –脆弱性発見時の対応手順の作成
      - –情報を迅速に発信できる仕組みの整備

# 【10位】不注意による情報漏えい

## ～一度の過失が組織の信用を大きく脅かす～




- 従業員の不注意等によって意図せず機密情報を漏えい
- 情報漏えいすることによる社会的信用の失墜、漏えいした情報の悪用による二次被害

# 【10位】不注意による情報漏えい

～一度の過失が組織の信用を大きく脅かす～

## ● 要因

**・個人のリテラシーやモラル不足からの不注意**

**・組織の管理体制の不備**

### ■ 取扱情報の重要性に対する認識不足からの不注意

・重要情報をカバンで持ち出し、カバンを紛失して漏えい

・宛先等の確認不十分なままメールを送信し誤送信

### ■ 情報を取り扱う際の本人の状況

・体調不良や急ぎの用件があることによる注意力散漫

### ■ 組織規程および確認プロセスの不備

・重要情報の定義、取扱規程、持ち出し許可手順等の不備

# 【10位】不注意による情報漏えい

## ～一度の過失が組織の信用を大きく脅かす～

- 2018年の事例/傾向
  - 取材音声データ等の情報をメールで誤送信 (※1)
    - ・宗教団体に関する住民インタビューの音声ファイルのダウンロード先情報等を含むメールを誤って宗教団体側に送付
  - 業務用端末等の紛失 (※2)
    - ・ガス会社作業員が421世帯分の顧客情報を記録した端末と制服を紛失。端末は後日発見された
    - ・セキュリティ対策を施しており、情報の流出はなかったとの報告

【出典】
※1 取材データの誤送信で職員8人を懲戒処分 - NHK
http://www.security-next.com/100289
※2 紛失したお客さま情報が入った業務用携帯端末および制服の発見について
https://www.tokyo-gas.co.jp/important/20181225-01.pdf

# 【10位】不注意による情報漏えい

## ～一度の過失が組織の信用を大きく脅かす～

- 対策
  - 経営者、管理者、当事者
    - ・情報リテラシーや情報モラルの向上
      - －従業員のセキュリティ意識教育
      - －組織規程および確認プロセスの確立
    - ・被害の予防
      - －確認プロセスに基づく運用
      - －情報の保護（暗号化、アクセス制限）
      - －外部に持ち出す情報や端末の制限
      - －業務用携帯端末の紛失対策機能の有効化
    - ・被害の早期検知
      - －問題発生時の内部報告体制の整備
      - －外部からの連絡窓口の設置

# 【10位】不注意による情報漏えい

## ～一度の過失が組織の信用を大きく脅かす～

- **対策**
  - ・被害を受けた後の対応
    - –CSIRTへの連絡
    - –影響調査および原因の追究、対策の強化
    - –被害拡大や二次被害要因の排除
    - –漏えいした内容や発生原因の公表
- **被害者（情報漏えいされた人）**
  - ・被害を受けた後の対応
    - –漏えいが発生した組織からの情報に従う
      - ※パスワードの変更、クレジットカード情報の変更等

# まとめ

## 情報セキュリティ対策の基本を実践

- 「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は長年変わらない

## 各脅威の手口の把握および対策を実践

- 脅威に備えるためには攻撃手口や動向、および自組織が抱える要因等を把握することが重要
- 「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしないので、各組織ごとにリスク分析を実施のうえ、対策の優先度を決定する

# 詳細な資料のダウンロード

## ■情報セキュリティ10大脅威　2019

本資料に関する詳細な内容は以下のウェブサイトをご覧ください

※以下のURLへアクセス、またはQRコードをスマートフォンの
　QRコードリーダーアプリで読み込み、ウェブサイトをご覧ください


https://www.ipa.go.jp/security/vuln/10threats2019.html

## ■アンケートご協力のお願いについて

IPAが公開しているツールや資料の品質向上のため、アンケートへのご協力をお願い致します

https://touroku.ipa.go.jp/?url=http%3A%2F%2Fspd-evsan-ap01.ipa.go.jp%2Fentry%2FMemberLogin%3Fevent_id%3DEA0000000074