# 「情報セキュリティ10大脅威」から見るサイバー攻撃の動向

2017年8月24日
独立行政法人 情報処理推進機構（IPA）
技術本部 セキュリティセンター





## IPAの「情報セキュリティ10大脅威」とは？

- IPAが2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等からIPAが脅威候補を選出
- セキュリティ専門家や企業のシステム担当等、から構成される「10大脅威選考会」が投票

**脅威の概要** **被害事例** **対策方法**

# 情報セキュリティ10大脅威 2017

- 章構成
  - 1章.情報セキュリティ対策の基本 スマートフォン編
    - スマートフォンで実施すべき対策を解説
  - 2章.情報セキュリティ10大脅威 2017
    - 脅威の概要と対策について解説
  - 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





# 10大脅威の特徴

**同じ脅威でも、影響を受ける立場によって影響度は変化**


- 家庭等でパソコンやスマホを利用する人「個人」

- 企業や政府機関などの組織
- 組織のシステム管理者や社員・職員

「組織」

**「個人」と「組織」の10大脅威を選出**

| 「個人」の10大脅威 | 順位 | 「組織」の10大脅威 |
|---|---|---|
| インターネットバンキングや<br>クレジットカード情報の不正利用 | 1位 | 標的型攻撃による情報流出 |
| ランサムウェアによる被害 | 2位 | ランサムウェアによる被害 |
| スマートフォンやスマートフォン<br>アプリを狙った攻撃 | 3位 | ウェブサービスからの個人情報の窃取 |
| ウェブサービスへの不正ログイン | 4位 | サービス妨害攻撃による<br>サービスの停止 |
| ワンクリック請求などの不当請求 | 5位 | 内部不正による情報漏えいと<br>それに伴う業務停止 |
| ウェブサービスからの個人情報の窃取 | 6位 | ウェブサイトの改ざん |
| 匿名によるネット上の誹謗・中傷 | 7位 | ウェブサービスへの不正ログイン |
| 情報モラル不足に伴う犯罪の低年齢化 | 8位 | IoT機器の脆弱性の顕在化 |
| インターネット上のサービスを<br>悪用した攻撃 | 9位 | 攻撃のビジネス化<br>（アンダーグラウンドサービス） |
| IoT機器の不適切管理 | 10位 | インターネットバンキングや<br>クレジットカード情報の不正利用 |

**10大脅威2017からの新しい脅威も**





| 2016年版の「組織の10大脅威」 | 順位 | 2017年版の「組織の10大脅威」 |
|---|---|---|
| 標的型攻撃による情報流出 | 1位 | 標的型攻撃による情報流出 |
| 内部不正による情報漏えいと<br>それに伴う業務停止 | 2位 | ランサムウェアによる被害 |
| ウェブサービスからの個人情報の窃取 | 3位 | ウェブサービスからの個人情報の窃取 |
| サービス妨害攻撃による<br>サービスの停止 | 4位 | サービス妨害攻撃による<br>サービスの停止 |
| ウェブサイトの改ざん | 5位 | 内部不正による情報漏えいと<br>それに伴う業務停止 |
| 脆弱性対策情報の公開に伴い<br>公知となる脆弱性の悪用増加 | 6位 | ウェブサイトの改ざん |
| ランサムウェアを使った詐欺・恐喝 | 7位 | ウェブサービスへの不正ログイン |
| インターネットバンキングや<br>クレジットカード情報の不正利用 | 8位 | IoT機器の脆弱性の顕在化 |
| ウェブサービスへの不正ログイン | 9位 | 攻撃のビジネス化<br>（アンダーグラウンドサービス） |

**前年に引き続き警戒が必要な脅威**

| 2016年版の「組織の10大脅威」 | 順位 | 2017年版の「組織の10大脅威」 |
|---|---|---|
| 標的型攻撃による情報流出 | 1位 | 標的型攻撃による情報流出 |
| 内部不正による情報漏えいと<br>それに伴う業務停止 | 2位 | ランサムウェアによる被害 |
| ウェブサービスからの個人情報の窃取 | 3位 | ウェブサービスからの個人情報の窃取 |
| サービス妨害攻撃による<br>サービスの停止 | 4位 | サービス妨害攻撃による<br>サービスの停止 |
| ウェブサイトの改ざん | 5位 | 内部不正による情報漏えいと<br>それに伴う業務停止 |
| 脆弱性対策情報の公開に伴い<br>公知となる脆弱性の悪用増加 | 6位 | ウェブサイトの改ざん |
| ランサムウェアを使った詐欺・恐喝 | 7位 | ウェブサービスへの不正ログイン |
| インターネットバンキングや<br>クレジットカード情報の不正利用 | 8位 | IoT機器の脆弱性の顕在化 |
| ウェブサービスへの不正ログイン | 9位 | 攻撃のビジネス化<br>（アンダーグラウンドサービス） |

**脅威自体が無くなったわけではない**



| 2016年版の「組織の10大脅威」 | 順位 | 2017年版の「組織の10大脅威」 |
|---|---|---|
| 標的型攻撃による情報流出 | 1位 | 標的型攻撃による情報流出 |
| 内部不正による情報漏えいと<br>それに伴う業務停止 | 2位 | ランサムウェアによる被害 |
| ウェブサービスからの個人情報の窃取 | 3位 | ウェブサービスからの個人情報の窃取 |
| サービス妨害攻撃による<br>サービスの停止 | 4位 | サービス妨害攻撃による<br>サービスの停止 |
| ウェブサイトの改ざん | 5位 | 内部不正による情報漏えいと<br>それに伴う業務停止 |
| 脆弱性対策情報の公開に伴い<br>公知となる脆弱性の悪用増加 | 6位 | ウェブサイトの改ざん |
| ランサムウェアを使った詐欺・恐喝 | 7位 | ウェブサービスへの不正ログイン |
| インターネットバンキングや<br>クレジットカード情報の不正利用 | 8位 | IoT機器の脆弱性の顕在化 |
| ウェブサービスへの不正ログイン | 9位 | 攻撃のビジネス化<br>（アンダーグラウンドサービス） |

**より警戒していかなければならない脅威**

| 2016年版の「組織の10大脅威」 | 順位 | 2017年版の「組織の10大脅威」 |
|---|---|---|
| 標的型攻撃による情報流出 | 1位 | 標的型攻撃による情報流出 |
| 内部不正による情報漏えいと<br>それに伴う業務停止 | 2位 | ランサムウェアによる被害 |
| ウェブサービスからの個人情報の窃取 | 3位 | ウェブサービスからの個人情報の窃取 |
| サービス妨害攻撃による<br>サービスの停止 | 4位 | サービス妨害攻撃による<br>サービスの停止 |
| ウェブサイトの改ざん | 5位 | 内部不正による情報漏えいと<br>それに伴う業務停止 |
| 脆弱性対策情報[illegible]に伴い<br>公知となる脆[illegible]増加 | 6位 | ウェブサイトの改ざん |
| ランサムウ[illegible]詐欺・恐喝 | 7位 | ウェブサービスへの不正ログイン |
| インターネッ[illegible]や<br>クレジットカ[illegible]正利 | 8位 | IoT機器の脆弱性の顕在化 |
| ウェブ[illegible] | 9位 | 攻撃のビジネス化<br>（アンダーグラウンドサービス） |
| 過失[illegible] | 10位 | インターネットバンキングや<br>クレジットカード情報の不正利用 |





# 「組織」にとっての脅威は？

IPA

# 組織の10大脅威 2017

IPA

【組織の脅威：第１位】
標的型攻撃による情報流出





# 【1位】標的型攻撃による情報流出

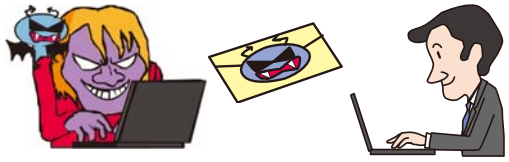
## ～引き続き警戒、標的型攻撃による被害が増加～

IPA

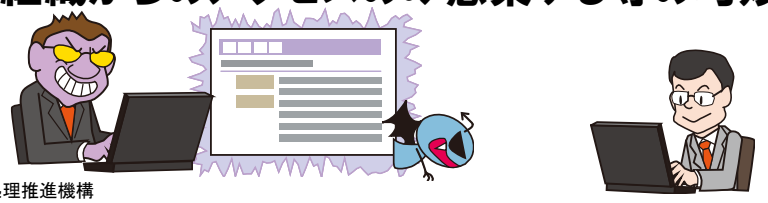
- 特定の企業・組織を狙い撃ちするサイバー攻撃
- メールによるウイルス感染等により組織内部に侵入
- 組織の機密情報が流出
- 取引先や関連会社を踏み台にして本丸を狙うこと

# 手口

- メールによる感染
  - 攻撃対象の組織にメールを送信
  - ウイルス含む添付ファイル付きメールを開き、ウイルスに感染
  - メールに記載された不審なリンクをクリックし、ウイルスに感染



- ウェブ閲覧による感染（水飲み場型攻撃）
  - 攻撃対象の組織が利用しているウェブサイトを改ざん
  - 従業員等がウェブサイトにアクセスしウイルスに感染
  - 攻撃対象の組織からのアクセスのみ感染する等の巧妙化も

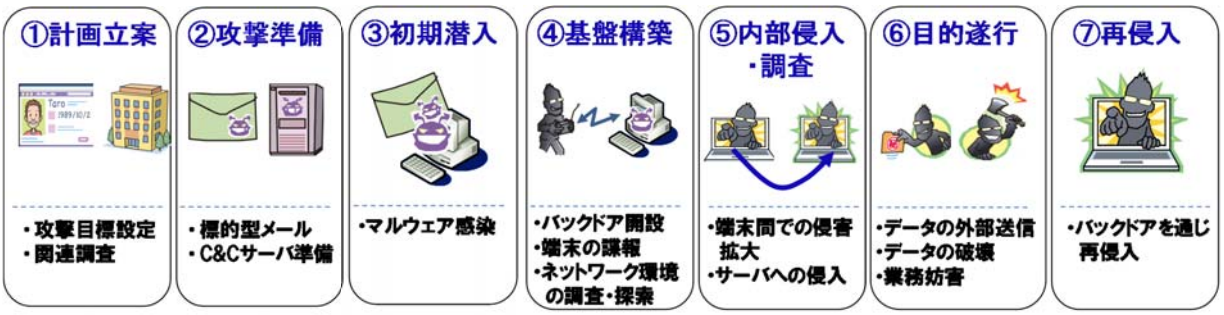






# 標的型攻撃の攻撃シナリオ

- 特定の企業・組織を狙い撃ちするサイバー攻撃
  - 標的の身辺を**事前に調査**し攻撃を仕掛ける
  - 政府機関、業務関連会社等を**装ったメール**を送り付ける
  - **ウイルス感染したPCを踏み台**にして組織内部に侵入
  - 機密情報の外部送信や破壊、業務妨害等を行う

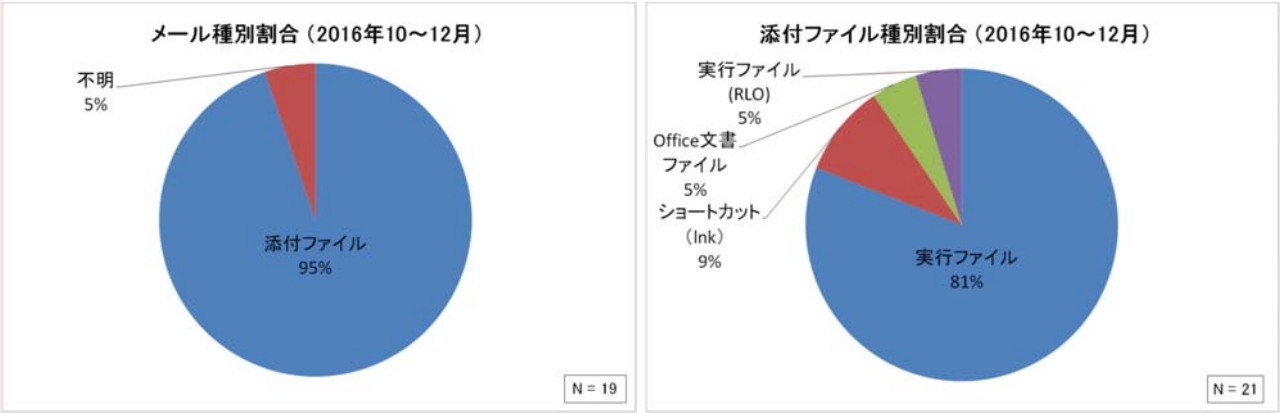


# 被害事例

- 2016年の事例/傾向
  - 旅行会社JTBから678万件の個人情報流出の可能性
    - 取引先になりすましたメールの添付ファイルを開き、ウイルスに感染
    - 遠隔操作により個人情報を保管しているサーバへと侵害が拡大
  - 経団連のPCが外部と不審な通信
    - 23台の事務局PCが10台の外部サーバとの間で不審な通信
    - 標的型攻撃に悪用される「PlugX」、「Elirks」の検体を発見
  - 富山大学、標的型攻撃により研究成果等が外部流出の可能性
    - 非常勤の研究者のPCが添付ファイルを開きウイルスに感染
    - 感染PC内には個人情報や原発の汚染水処理に関する研究成果等を保有していた可能性



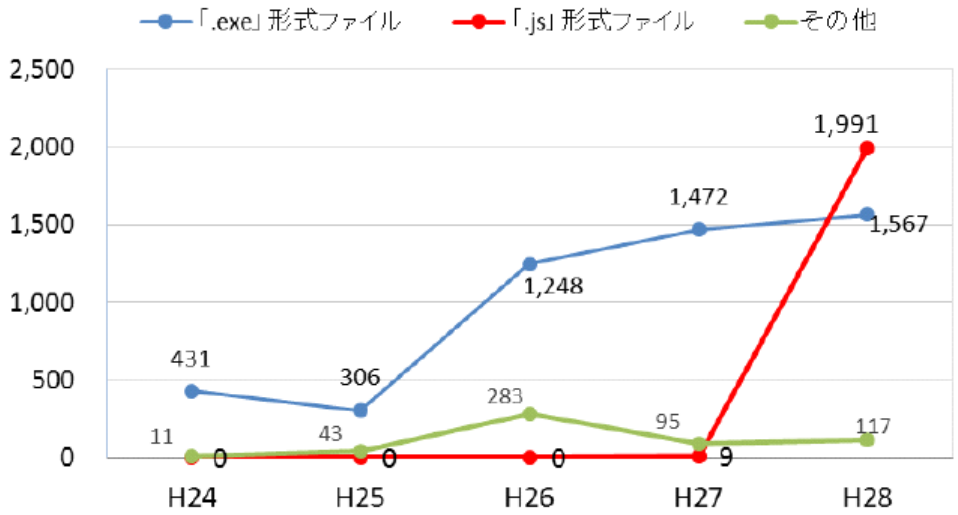

# 標的型攻撃メールの傾向1
## （J-CSIP運用状況 2016年10月～12月）




（出典）IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2016年10月～12月］

- メール種別は「添付ファイル」がほとんど（９５％）
  →１通に２つの添付ファイル（ExcelとPDF）のケースも
- 添付ファイル種別は「実行ファイル」が８割超
  →ZIPファイルを解凍すると実行ファイルが現れる

# 標的型攻撃メールの傾向2




【出典】平成28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（警察庁）

- 警察庁の情報によると、
  2016年は、圧縮ファイルに含まれるファイルとして、
  「JSファイル」の件数が急増





# 標的型攻撃メールの着眼点

## テーマ（件名）

- 開封せざるを得ない内容（取材依頼／就職活動／クレーム）
- 興味をそそられる内容（議事録）
- 来たことのない公的機関からのお知らせ（注意喚起）

## 送信者

- フリーメールアドレス
- 署名詐称

## メール本文

- 不自然な日本語
- 記載されたURL
  （表示と異なるリンク先）

## 添付ファイル

- 実行ファイル／Officeファイル

**怪しい点がないかを総合的に判断**

# 【紹介】標的型攻撃対策の参考資料

## ●IPAテクニカルウォッチ
## 「標的型攻撃メールの例と見分け方」

- **メールの見分け方**
  - 注意するときの着眼点
  - 標的型攻撃メールの例
  - 添付ファイルの種類と解説

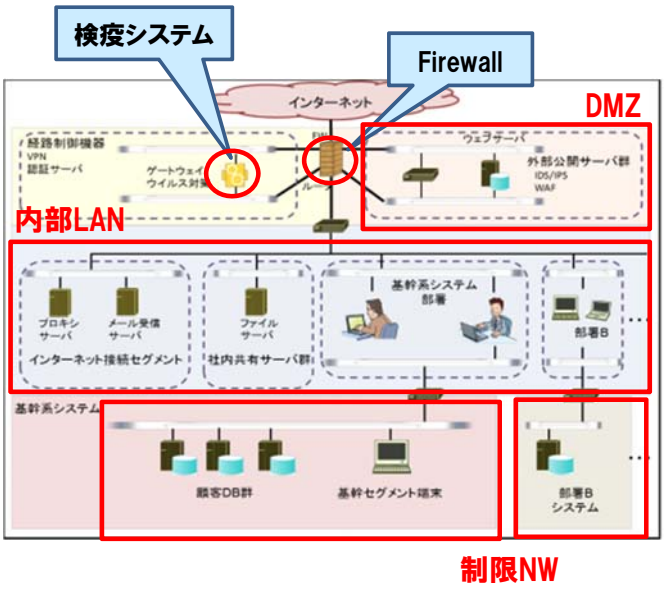




# 組織の対策

# 入口対策の特徴と弱点

- **不正侵入を阻止**
  - **FireWall**
    - 許可された通信のみ通過
    - 通信内容は関知しない
  - **IDS／IPS**
    - 攻撃を行う通信を検知
    - 未知の攻撃の阻止は難しい
  - **ウイルス対策ソフト**
    - ウイルスの侵入を阻止
    - 未知のウイルスの対処難

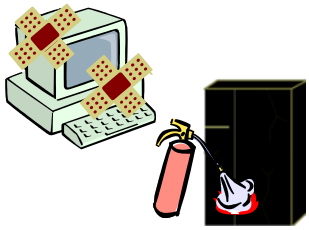


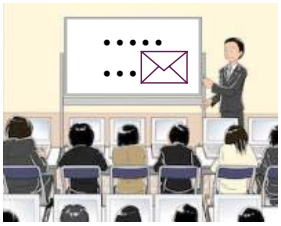

**外から内への侵入に備える境界防御の概念であるが**
**侵入を完全に防ぐのは困難**




# 入口対策の特徴と弱点

- **脆弱性対策（セキュリティパッチ適用）**
  - **エンドポイント（PC）へのパッチ適用**
    - セキュリティ対策の基本であり、効果大
    - 全端末に適用することが侵入を防ぐ前提
    - 利用者主導による対策の為、漏れの可能性
  - **サーバ機器等へのパッチ適用**
    - 互換性の問題で適用できないケースの問題
    - システム停止が許容できない運用上の事情
- **啓発活動による対策**
  - **不審メールを開かない個人や組織への啓発**
    - 組織内での注意力・対策熱が上がる
    - **1人でも感染すれば組織内に侵入**
    - **マルウェア開封率0%が必須条件**

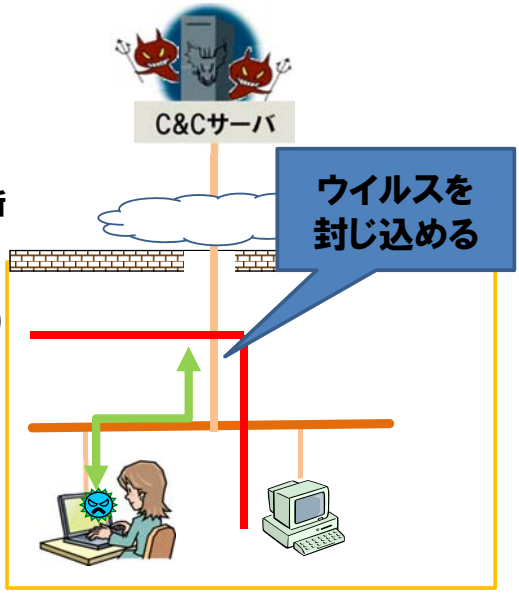




**セキュリティ対策には**
**一長一短があり、**
**完全な対策は難しい**

# 内部対策(出口対策)の考え方

- **バックドア通信の検知と抑止**
  - **プロキシサーバとFWの設定**
    - 正常な通信の流れを作る
    - ルール外の通信を試みるウイルスの検知と遮断
- **感染予防策**
  - **アクセス区画の整理(ネットワークの分離)**
    - VLANを構築
    - VLAN間の通信を制限
    - ウイルスの偵察行為を阻止
  - **侵食予防(ログ・通信の監視)**
    - VLAN毎に通信の監視
    - 感染発覚時は、VLANを切り離す




**多 層 防 御**




# 【紹介】標的型攻撃対策の参考資料

- **「高度標的型攻撃」対策に向けたシステム設計ガイド**
  - 攻撃者が歩きづらいシステム設計
  - 6つの「対策セット」を紹介


- **IPAテクニカルウォッチ「攻撃者に狙われる設計・運用上の弱点についてのレポート」**
  - システム設計・運用上の弱点
  - 弱点を生む10の落とし穴

# 組織の10大脅威 2017

IPA

【組織の脅威：第２位】
ランサムウェアによる被害

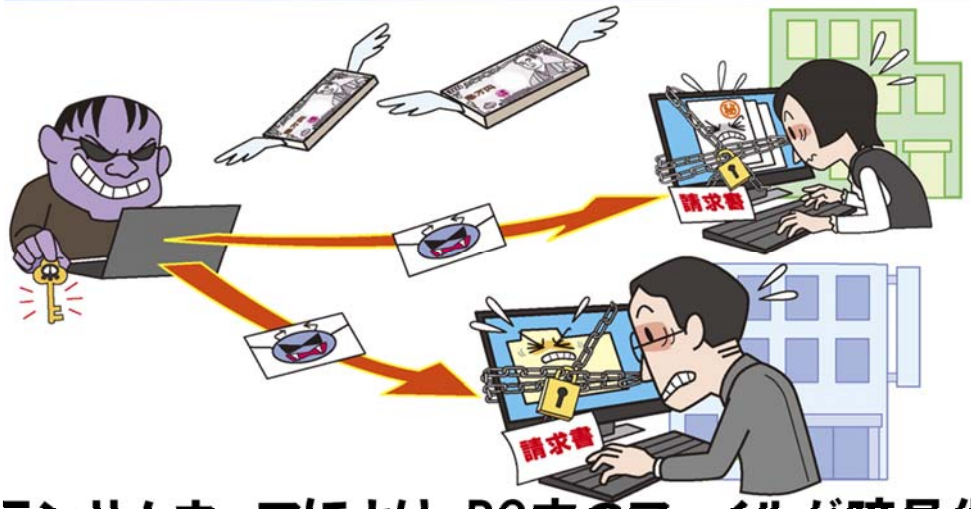




# 【２位】ランサムウェアによる被害

## ～ランサムウェアによる被害が急増～

IPA




- ランサムウェアにより、PC内のファイルが暗号化され、ファイル復元に身代金を要求される
- 日本語対応やスマートフォンを標的とする等、巧妙化
- 共有サーバのファイルまで暗号化されることも

# ランサムウェアの脅威

**ランサムウェアに感染すると・・・**

## パソコンの利用に制限をかけられる

- ファイルを暗号化され、開けなくなる　**ファイル暗号化型**
- 端末をロックされ、操作できなくなる　**端末ロック型**

## 制限解除のためのメッセージが表示される

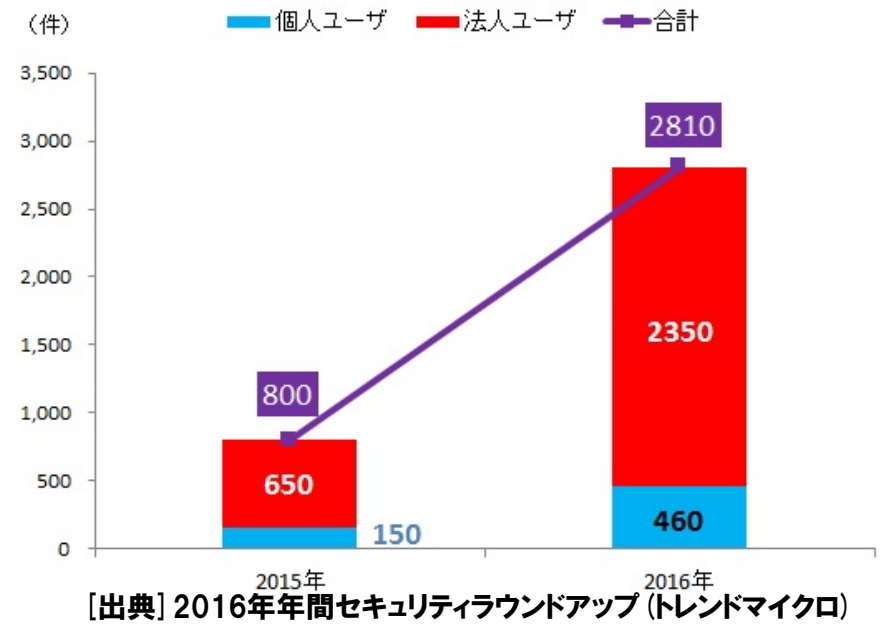
- 発生した事象や復旧方法（金銭の支払いの要求）などが記載されている





# ランサムウェアの被害が急増

**ランサムウェア被害報告件数推移**




［出典］2016年年間セキュリティラウンドアップ（トレンドマイクロ）

- 2015年と比較して、3.5倍の被害件数

# ランサムウェアの脅威

## ランサムウェアの感染経路

### ウェブサイトからの感染

- 改ざんされた正規のウェブサイトを閲覧することで感染
- 不正広告を閲覧することで感染
- ダウンロードしたファイルを開くことで感染

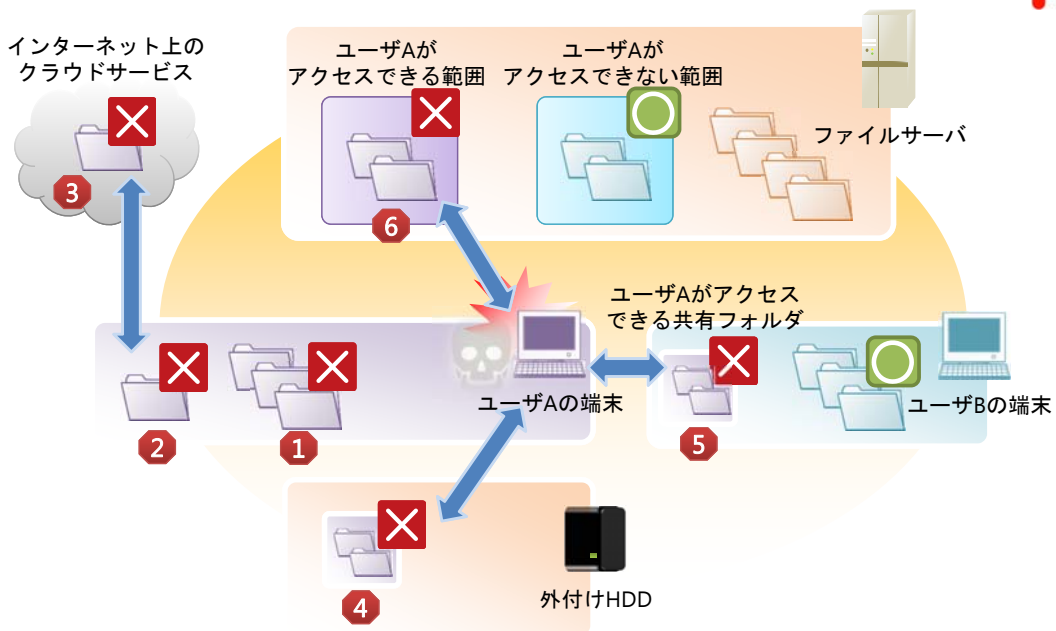
### メールからの感染

- メール本文に記載されたURLからアクセスすることで感染
- メールの添付ファイルを開くことで感染





# ランサムウェアの影響範囲




1. 感染端末内に保存されているファイル
2. 感染端末内のクラウドと同期するフォルダ内のファイル
3. ファイル暗号化後の同期によるクラウド内のファイル(上書き)
4. 感染端末に接続されている外付けHDD内のファイル
5. 感染端末と共有しているフォルダ内のファイル
6. 感染端末がアクセス可能な場所に保存されているファイル

# Wanna Cryptor (WannaCry)

- 2017年5月に日本で広く被害が確認されたMicrosoft SMBサーバの脆弱性を悪用するランサムウェア
- 日立、JR東、イオン、ホンダ、マクドナルド等で被害
- ランサムウェアに感染後、ネットワーク上に同じ脆弱性が残る端末がないか探索し、感染拡大を図る自己増殖型





# ランサムウェアの対策

## ランサムウェア感染による被害を防ぐため

### 感染しないために・・・

1. OSおよび利用ソフトウェアを最新の状態にする
2. ウイルス対策ソフトを導入する
3. メールの添付ファイルに注意する

### 感染してしまったときのために・・・

4. 重要なファイルを定期的にバックアップする

# ランサムウェアの対策

## バックアップにおける留意事項

1. バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続する。

通常時はランサムウェアの暗号化対象にならないように、パソコンと接続しないでおく。

2. バックアップに使用する装置・媒体は複数用意し、バックアップする。

バックアップファイルが暗号化されてしまったり、失敗することも考慮し、複数バックアップを取得。

3. バックアップから正常に復元できることを定期的に確認する

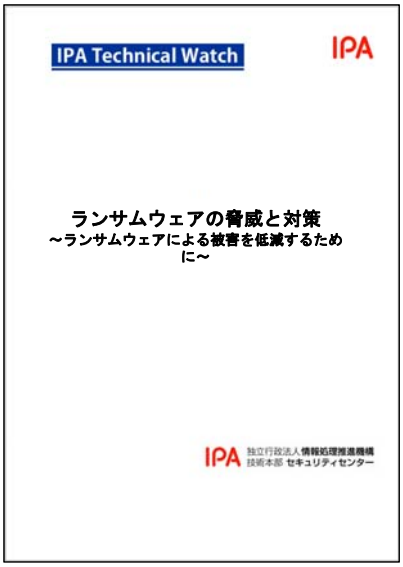
バックアップから復元できなければ意味がない。





# 【紹介】ランサムウェア対策の参考資料

- IPAテクニカルウォッチ
  「ランサムウェアの脅威と対策」
  - ランサムウェアの脅威
  - ランサムウェアの感染事例
  - ランサムウェアへの対策



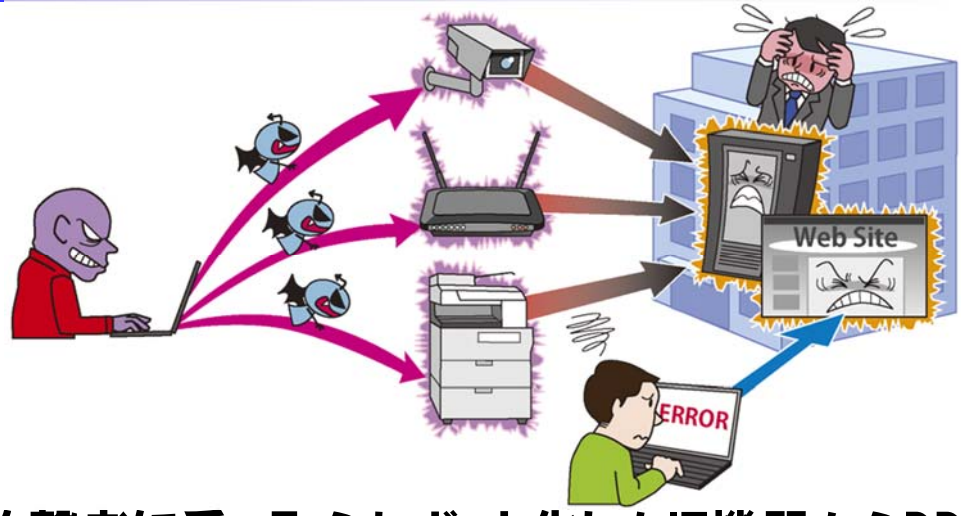
# 組織の10大脅威 2017

【組織の脅威：第４位】
サービス妨害攻撃による
サービス停止




# 【４位】サービス妨害攻撃によるサービスの停止

～ボットネットウイルスの普及に伴う攻撃の大幅増加～




- 攻撃者に乗っ取られボット化したIT機器からDDoS攻撃
- 組織のウェブサイトや組織の利用しているDNSサーバに大量のアクセス
- ウェブサイトの利用者がアクセスできない状態に

# 攻撃方法

## ボットネットの悪用

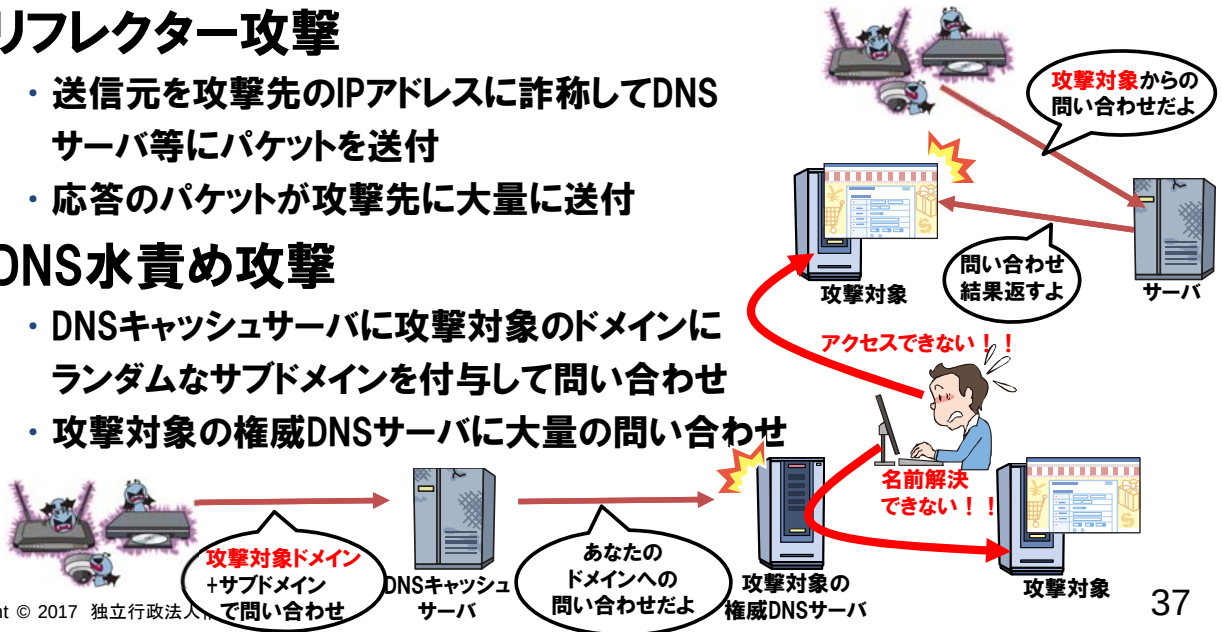
- 脆弱性等を悪用し、ウイルスに感染したネットワーク機器群（数百～数万）
- C&Cサーバからの指示により、攻撃対象のウェブサイトに攻撃

## リフレクター攻撃

- 送信元を攻撃先のIPアドレスに詐称してDNSサーバ等にパケットを送付
- 応答のパケットが攻撃先に大量に送付

## DNS水責め攻撃

- DNSキャッシュサーバに攻撃対象のドメインにランダムなサブドメインを付与して問い合わせ
- 攻撃対象の権威DNSサーバに大量の問い合わせ







# 被害事例

## 2016年の事例/傾向

### 主義主張のためのDDoS攻撃

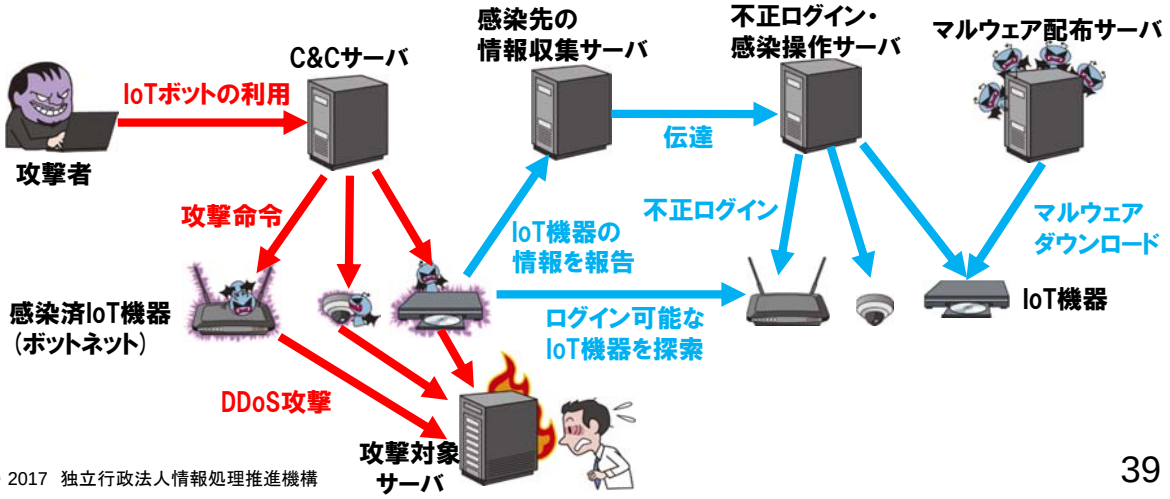
- 犯罪グループ（ハクティビスト）による主義主張（反捕鯨等）のための日本を対象とした攻撃
- ICA（国際協力機構）やJCR（日本格付研究所）等のサイトにDDoS攻撃
- 利用者がウェブサイトを閲覧できない状態に

### ボットネットウイルスの拡散

- 毎秒1テラビットという大規模なDDoS攻撃を確認
- 原因は、ウイルス「Mirai」に感染したIoT機器で構成されたボットネット
- ボットネットによる攻撃件数は2015年の6.4倍の1億2,600万件まで急増

# Miraiとは

- Miraiとは
  - Linuxで動作するIoT機器に感染するウイルス
  - ハードコーディングされた「ユーザ名とパスワード」を用いて、telnet（ポート番号23および2323）でログイン可能なIoT機器を狙う
  - 「DDoS攻撃を仕掛ける機能」と「感染を拡大する機能」を持つ








# Miraiとは

- 悪用されたtelnetのIDとパスワード例

| ユーザ名 | パスワード | 該当するIoT機器の例 |
|---|---|---|
| root | xc3511 | Shenzhen Ele Technology, DVR |
| root | vizxv | Zhejiang Dahua Technology, Camera |
| root | admin | IPX International, DDK Network Camera |
| admin | admin | |
| root | 888888 | Zhejiang Dahua Technology, DVR |
| root | xmhdipc | Shenzhen Anran Security Technology, Camera |
| root | default | |
| root | juantech | Guangzhou Juan Optical & Electronical Tech |
| root | 123456 | |
| root | 54321 | 8x8, Packet8 VoIP Phone 等 |

| ユーザ名 | パスワード | 該当するIoT機器の例 |
|---|---|---|
| support | support | |
| root | （未設定） | Vivotek, IP Camera |
| admin | password | |
| root | root | |
| user | user | |
| root | pass | Axis Communications, IP Camera 等 |
| admin | smcadmin | SMC Networks, Routers |
| admin | 1111 | Xerox, Printers 等 |
| root | 666666 | Zhejiang Dahua Technology, Camera |
| root | klv123 | HiSilicon Technologies, IP Camera |

# なぜ感染してしまったのか？

- 感染理由
  - ポート番号23または2323でtelnetが動作していた
    - 利用者でサービスを無効化していなかった
    - 無効化する管理インタフェースが存在しない場合も
    - telnetのサービスが存在することが利用者に通知されていない場合も
  - ユーザ名、パスワードが初期値のまま動作していた
    - 利用者がユーザ名パスワードを変更していなかった
    - パスワードがハードコーディングされており、利用者が変更出来ない場合も
    - ユーザ名やパスワードの存在が利用者に通知されていない場合も

**開発者側において、IoT機器に対して**
**セキュリティの配慮が必要であった**




# 対策

- 対策一覧
  - ウェブサービス提供事業者
    - 被害の予防
      - DDoS攻撃の影響を緩和するISPによるサービスの利用
      - システムの冗長化等の軽減策
    - 被害を受けた後の対策
      - 通信制御（DDoS攻撃元をブロック等）
      - ウェブサイト停止時の代替サーバーの用意と告知手段の整備
  - IoT機器ベンダー
    - 被害の予防
      - 脆弱性対策
      - 不要な機能の無効化（telnet等）
      - 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

**DDoS被害に遭わないためにウェブサービス提供事業者**
**だけではなく、IoT開発ベンダーも対策を**

# Miraiの他にも

- IoT機器を守ろうとする(？)ウイルス「Hajime」
  - 初期ユーザ名＆パスワードでtelnetで不正ログインして感染
  - 23, 5538, 5555, 7546ポートの通信を遮断し、不正利用を阻止する挙動
  - DDoS攻撃は行わず、作成者の善意(？)の警告メッセージを表示
  - ブラジル・イラン・タイ・ロシア等を中心に数万台のIoT機器が感染？
- IoT機器を使用不能にするウイルス「BrickerBot」
  - 初期ユーザ名＆パスワードでtelnetで不正ログインして感染
  - 設定変更、インターネット接続妨害、動作速度低下、機器上のファイル消去等の致命的な改変を行い、最終的に使用不能に
  - Miraiに悪用されるくらいなら、IoT機器を壊してしまえという考え方か？
  - 作成者は、「Mirai」を壊滅するため、200万台以上のIoT機器を使用不能状態にしたと主張
- 複数のウイルスによるIoT機器の陣取り合戦状態に




# 来年の10大脅威は・・・・

| 順位 | 2017年版の「組織の10大脅威」 |
|---|---|
| 1位 | 標的型攻撃による情報流出 |
| 2位 | ランサムウェアによる被害 |
| 3位 | ウェブサービスからの個人情報の窃取 |
| 4位 | サービス妨害攻撃による<br>サービスの停止 |
| 5位 | 内部不正による情報漏えいと<br>それに伴う業務停止 |
| 6位 | ウェブサイトの改ざん |
| 7位 | ウェブサービスへの不正ログイン |
| 8位 | IoT機器の脆弱性の顕在化 |
| 9位 | 攻撃のビジネス化<br>（アンダーグラウンドサービス） |
| 10位 | インターネットバンキングや<br>クレジットカード情報の不正利用 |

2018年版の
10大脅威は・・・？