

# 情報セキュリティ10大脅威2018

～2章 情報セキュリティ10大脅威 組織編～

～引き続き行われるサイバー攻撃、  
あなたは守りきれますか？～



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  
2018年4月

# 情報セキュリティ10大脅威 2018

## ● 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



## ● 章構成

### ■ 1章.情報セキュリティ対策の基本 IoT機器(情報家電)編

- ・ IoT機器(情報家電)における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 2018

- ・ 脅威の概要と対策について解説
- ・ 個人と組織の2つの立場で解説

### ■ 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 2018



## ● 順位

「個人」向け脅威	順位	「組織」向け脅威
インターネットバンキングや クレジットカード情報等の不正利用	1	標的型攻撃による被害
ランサムウェアによる被害	2	ランサムウェアによる被害
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを 狙った攻撃	4	脆弱性対策情報の公開に伴う 悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するための セキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告による インターネット詐欺	10	犯罪のビジネス化 (アンダーグラウンドサービス)

# 情報セキュリティ10大脅威 2018

## ● 組織における立場毎の注意すべき脅威

順位	脅威名(組織)	組織の立場	組織内の立場				
			経営層	セキュリティ管理者	システム管理者	製品開発者	一般従業員
1	標的型攻撃による被害	被害者	○	○	○	○	○
2	ランサムウェアによる被害	被害者	○	○	○	○	○
3	ビジネスメール詐欺による被害	被害者	○	○			○
4	脆弱性対策情報の公開に伴う悪用増加	ソフトウェアの開発者	○			○	
		ソフトウェアの利用者	○	○	○		○
5	脅威に対応するためのセキュリティ人材の不足	被害者	○	○	○	○	
6	ウェブサービスからの個人情報の窃取	ウェブサービスの開発者	○			○	
		ウェブサービスの提供者	○	○	○		
7	IoT機器の脆弱性の顕在化	IoT機器の開発者	○			○	
		IoT機器の利用者	○	○	○		
8	内部不正による情報漏えい	被害者	○	○	○	○	○
9	サービス妨害攻撃によるサービスの停止	被害者	○	○	○		
10	犯罪のビジネス化(アンダーグラウンドサービス)	被害者	○	○	○	○	○

経営層: 代表取締役社長や理事等の組織のトップ層

セキュリティ管理者: 組織におけるセキュリティの管理者

システム管理者: 組織で運用しているシステムの管理者

製品開発者: 製品の開発者

一般従業員: 営業や総務、財務等の組織におけるIT利用者

## 2章. 情報セキュリティ10大脅威2018 組織編



# 【1位】標的型攻撃による被害

～組織全体でセキュリティ意識の向上を～



- 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
- 組織の機密情報を窃取
- 踏み台とするために業種や会社規模に関係なく狙われる

# 【1位】標的型攻撃による被害

～組織全体でセキュリティ意識の向上を～

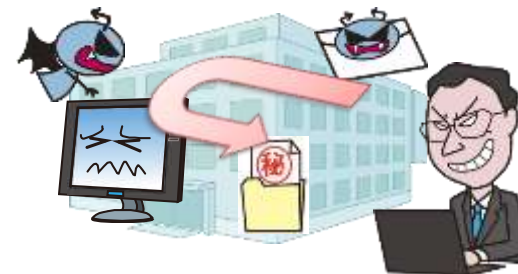
## ● 攻撃手口

### ■ メールを使った手口

- ・ ウイルスを含んだ添付ファイルを開かせる
- ・ ウイルスを含んだウェブサイトへのリンクをクリックさせる

### ■ ウェブを使った手口

- ・ ウイルスをダウンロードするよう標的組織が利用するウェブサイトを改ざん
- ・ DMZ上に存在するサーバーの脆弱性を悪用し、内部に侵入する





# 【1位】標的型攻撃による被害

～組織全体でセキュリティ意識の向上を～

## ● 2017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

- ・ J-CSIP参加組織(11業界227組織)において標的型攻撃メールの受信件数173件
- ・ MS Office製品の脆弱性を悪用する添付ファイル付き標的型攻撃を確認
- ・ 海外の関連企業のアカウントを乗っ取った上で、国内企業に対して標的型攻撃を仕掛けるケースも



# 【1位】標的型攻撃による被害

～組織全体でセキュリティ意識の向上を～

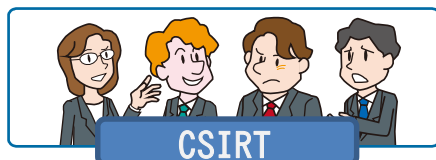
## ● 対策一覧

### ■ 経営者層

- － 問題に対応する体制 (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
  - － セキュリティ対策の状況把握
- ・ 被害を受けた後の対応
  - － 組織内体制 (CSIRT) の運用
  - － 影響調査および原因の追究



### ■ システム管理者

#### ・ 被害の予防

- － 被害を抑止するためのシステム設計
- － アクセス制御・データの暗号化
- － OS・ソフトウェア更新
- － ネットワーク分離・バックアップ取得

#### ・ 被害の早期検知

- － ネットワーク、エンドポイントの監視・防御

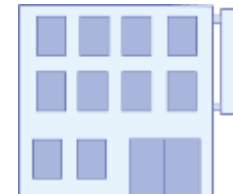
### ■ 従業員・職員

#### ・ 被害の予防

- － セキュリティ教育の受講
- － OS・ソフトウェアの更新
- － セキュリティソフトの導入・更新
- － 取引先セキュリティ対策の確認

#### ・ 被害を受けた後の対応

- － CSIRTへ連絡



# 【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～



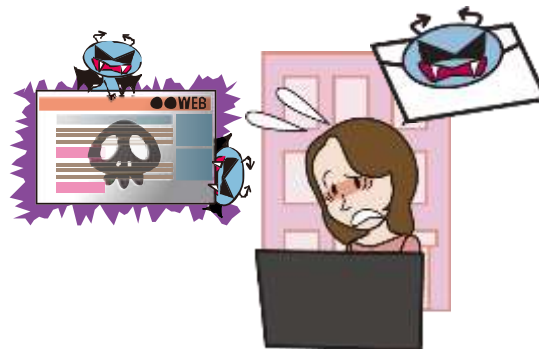
- PCやスマートフォンのファイル暗号化や画面ロック等の制限をかけ、解除に金銭を要求
- 組織のファイルサーバーも暗号化されるおそれ
- ネットワークを介してOSの脆弱性を悪用し、感染拡大するランサムウェアが登場

# 【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

## ● 攻撃手口

- メールの添付ファイルを開かせる
- 悪意のあるウェブサイトへのリンクをクリックさせる
- 製品の脆弱性を悪用しランサムウェアに感染させる  
(Internet Explorer, Adobe Flash Player, Java 等の脆弱性)
- ネットワークを介してOSの脆弱性を悪用し感染させる
- 不正なスマートフォンのアプリをインストールさせる



# 【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

## ● 2017年の事例／傾向

### ■ 自己増殖型ランサムウェア（WannaCry）の登場（5月）

- ・ OSの脆弱性「MS17-010」を悪用し、ネットワーク間で感染
- ・ 世界的に感染を拡大
- ・ 国内の大手企業や地方公共団体等に被害

### ■ 対策されてない機器が継続してWannaCryに感染（11月）

### ■ セキュリティ対策が日々進化する一方、攻撃手法も進化

- ・ セキュリティ対策ソフトからの検出を回避



# 【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

## ● 対策一覧

### ■ 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/PC・スマートフォン利用者

- ・ 被害の予防
  - － 受信メール、ウェブサイトの十分な確認
  - － OS・ソフトウェアの更新
  - － セキュリティソフトの導入
  - － フィルタリングツールの活用
  - － 共有サーバのアクセス権最小化
  - － バックアップの取得
- ・ 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



～偽の振込・送金依頼に注意～

- 15

# 【3位】ビジネスメール詐欺による被害

～偽の振込・送金依頼に注意～

## ● 攻撃手口

- 取引先になりすまし、偽装した請求書を送りつける
- 経営者等になりすまし、指定の口座へ振り込ませる
- メールアカウントを乗っ取り、従業員になりすまし、偽の請求書を送りつける
- 弁護士など社外の権威ある第三者になりすまし、指定の口座へ振り込ませる
- 詐欺を行う前に経営者等になりすまし、企業内の従業員の情報を盗み取る



# 【3位】ビジネスメール詐欺による被害

～偽の振込・送金依頼に注意～

## ● 2017年の事例 / 傾向



### ■ 日本航空にてビジネスメール詐欺被害

- ・ 偽の請求書メールで約3億8,000万円の被害
- ・ 取引先のメールアドレスに模したメールが送付された

### ■ トrendマイクロ社による調査報告

- ・ メールドメインを選択できる無料のウェブメールサービスを悪用
- ・ メールの返信先(Reply-To)を偽装
- ・ 標的組織のメールアドレスに模したドメインを利用

# 【3位】ビジネスメール詐欺による被害

～偽の振込・送金依頼に注意～

## ● 対策一覧

### ■ 組織

#### ・被害の予防

- －メールの真正性を確認
- －振込先の口座変更ある場合は取引先に連絡
- －普段と異なる言い回しや表現の誤りに注意
- －送信元アドレスや送信元ドメインを確認
- －電子署名の付与(なりすまし防止)
- －メールを利用しない取引方法を検討

#### ・基本的な対策

- －OS・ソフトウェアの更新
- －セキュリティソフトの導入
- －メールアカウントの適切な管理

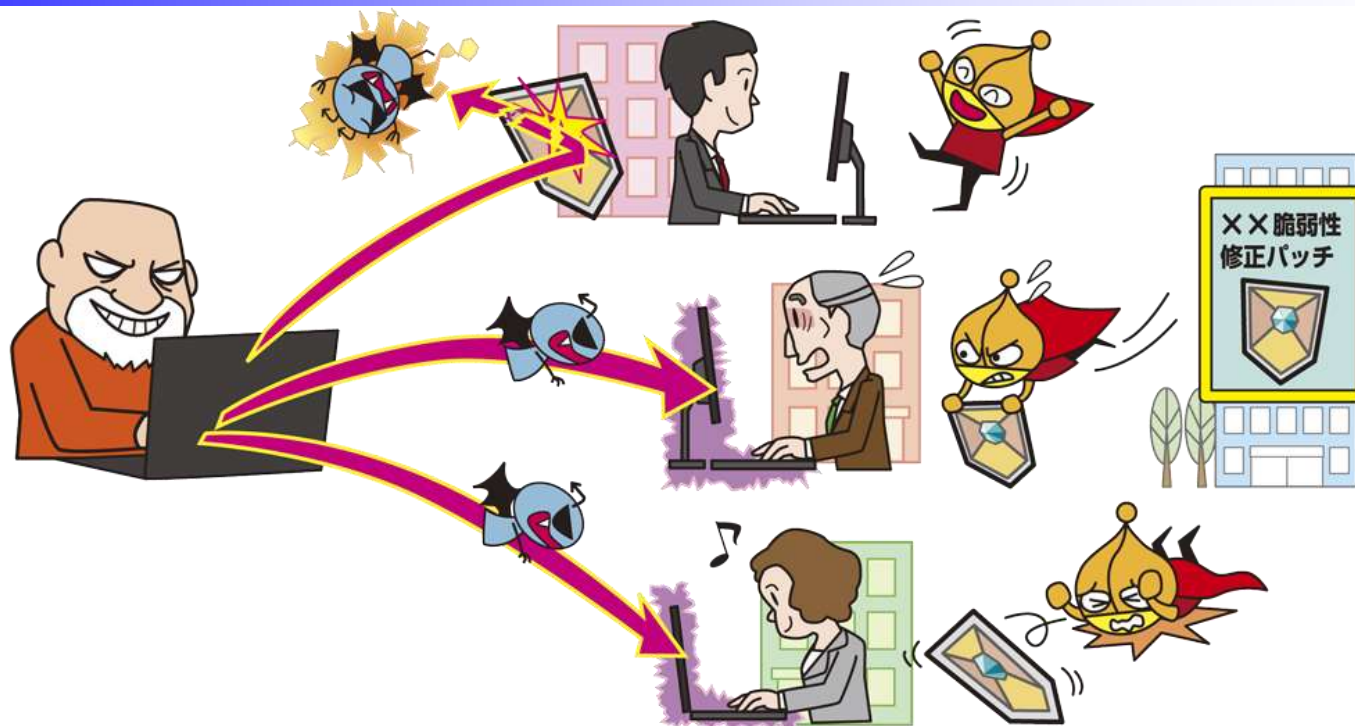
#### ・被害を受けた後の対応

- －CSIRTへ連絡
- －警察に相談
- －詐称されている組織への連絡
- －影響調査および原因の追究



# 【4位】脆弱性対策情報の公開に伴う悪用増加

～未対策の脆弱性が狙われる！迅速な対応を～



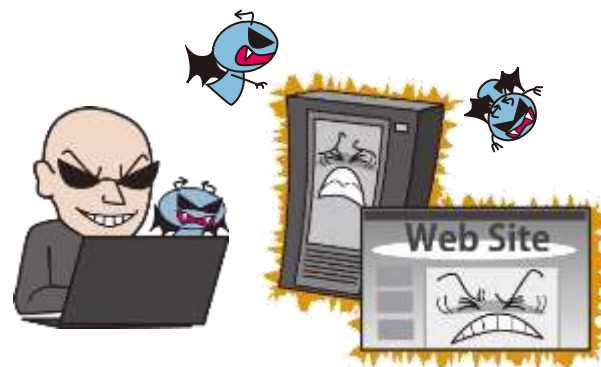
- 公開された脆弱性対策情報を悪用
- パッチを適用していないソフトウェア製品の利用者を標的に
- 広く利用されているソフトウェア製品は被害拡大のおそれ

# 【4位】脆弱性対策情報の公開に伴う悪用増加

～未対策の脆弱性が狙われる！迅速な対応を～

## ● 攻撃手口

- 脆弱性対策情報を基に攻撃コードを作成
- パッチ適用する前のソフトウェア製品の利用者を攻撃
- 未知もしくは未公開の脆弱性を悪用（ゼロデイ攻撃）
- Apache StrutsやWordPressなど広く利用されているソフトウェア製品を狙う





# 【4位】脆弱性対策情報の公開に伴う悪用増加

～未対策の脆弱性が狙われる！迅速な対応を～

## ● 2017年の事例／傾向

### ■ WordPress利用のウェブサイトを改ざん

- ・ パッチ未適用の多数のウェブサイトに被害

### ■ Apache Strutsの脆弱性を悪用

- ・ 米国Equifax社 約1億4,500万人の個人情報流出

### ■ 攻撃コードの公開による攻撃の増加

- ・ 11月中旬にMicrosoft Officeの脆弱性対策情報が公開
- ・ 11月下旬に攻撃コードが公開され、脆弱性を悪用する攻撃が多発



# 【4位】脆弱性対策情報の公開に伴う悪用増加

～未対策の脆弱性が狙われる！迅速な対応を～

## ● 対策一覧

### ■ 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
  - － OS・ソフトウェアの更新
  - － WAF・IPSなどのセキュリティ機器の導入
  - － ネットワークの監視
  - － セキュリティサポートが充実している製品の利用
- ・ 被害を受けた後の対応
  - － CSIRTへ連絡
  - － 影響調査および原因の追究

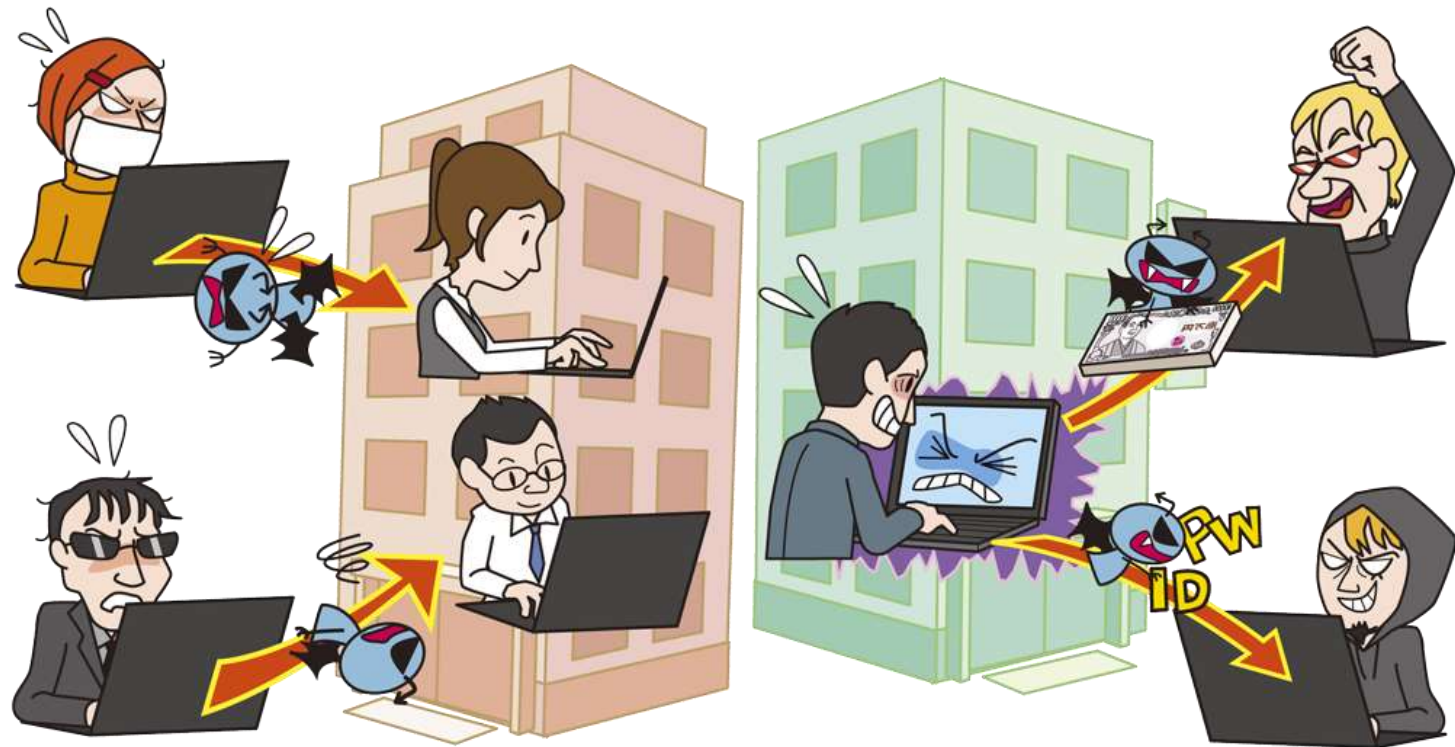
### ■ 開発ベンダー

- ・ 製品セキュリティの管理
  - － 組込みソフトウェアの管理
  - － 脆弱性関連情報の収集
- ・ 対応体制の整備
  - － 脆弱性発見時の対応
  - － 情報発信の環境を整備
- ・ パッチの迅速な提供



# 【5位】脅威に対応するためのセキュリティ人材の不足 IPA

～組織や国は積極的なセキュリティ人材の育成を～



- 組織内におけるセキュリティ人材が不足
- セキュリティ上の脅威に対応できる体制が整えられず、被害拡大のおそれ

# 【5位】脅威に対応するためのセキュリティ人材の不足 IPA

～組織や国は積極的なセキュリティ人材の育成を～

## ● 2017年の事例

### ■ 経済産業省におけるセキュリティ人材調査

- ・ 2016年時点で約13万人が不足、2020年には推計約19.3万人の不足

### ■ 内閣サイバーセキュリティセンター(NISC)による取組

- ・ 「サイバーセキュリティ人材育成プログラム」を作成
- ・ 産官学の人材育成戦略の方向性を示す

### ■ セキュリティ・キャンプによる人材の発掘と育成

- ・ 若年層に対し高度な情報セキュリティ技術の習得機会を提供
- ・ 若年層に対し次代を担う情報セキュリティ人材を発掘・育成
- ・ 主催：独立行政法人情報処理推進機構

一般社団法人セキュリティ・キャンプ協議会



# 【5位】脅威に対応するためのセキュリティ人材の不足 IPA

～組織や国は積極的なセキュリティ人材の育成を～

## ● 対策一覧

### ■ 組織

- ・ 組織としての対応体制の確立
  - － 人材における予算の確保や中長期的な戦略
  - － 人材育成を視野にした採用
  - － ジョブローテーションによる技術・知識共有
  - － 資格習得などキャリアパスによる人材育成
- ・ 情報リテラシーの向上
  - － セキュリティ教育
  - － 外部の教育サービスを活用
  - － 外部開催のCTFや勉強会等への取り組みを促進



# 【5位】脅威に対応するためのセキュリティ人材の不足 IPA

～組織や国は積極的なセキュリティ人材の育成を～

## ■ 独立行政法人情報処理推進機構

### ・ 情報処理試験制度

- ITエンジニアの不足等を背景として発足した国家資格
- ITの知識・技能に関する共通の評価指標としての活用
- 技術の多様化・需要変化に対応できるITエンジニアを育成





# 【6位】ウェブサービスからの個人情報の窃取

～ウェブサービスの脆弱性対策は迅速に～



- 個人情報やクレジットカード情報を窃取される被害が続いている
- 窃取した情報を悪用し、不審メールの送りつけやクレジットカードの不正利用も

# 【6位】ウェブサービスからの個人情報の窃取

～ウェブサービスの脆弱性対策は迅速に～

## ● 攻撃手口

- 企業が開発したウェブアプリケーションの脆弱性を悪用
- OS・ミドルウェア・CMS等の脆弱性を悪用
- 共通的に使われるソフトウェア( OpenSSL、Apache Struts、WordPress等 )の脆弱性を悪用



# 【6位】ウェブサービスからの個人情報の窃取

～ウェブサービスの脆弱性対策は迅速に～

## ● 2017年の事例／傾向

### ■ チケット販売のウェブサイト不正アクセス

- ・ 最大約15万5,000件の個人情報漏えいした可能性
- ・ Apache Struts2の脆弱性を悪用

### ■ 登山情報サイトに不正アクセス

- ・ 氏名やメールアドレス等、約1,160件の情報漏えい
- ・ 開発プログラムにSQLインジェクションの脆弱性



# 【6位】ウェブサービスからの個人情報の窃取

～ウェブサービスの脆弱性対策は迅速に～

## ● 対策一覧

### ■ ウェブサービス運営者

#### ・ 被害の予防

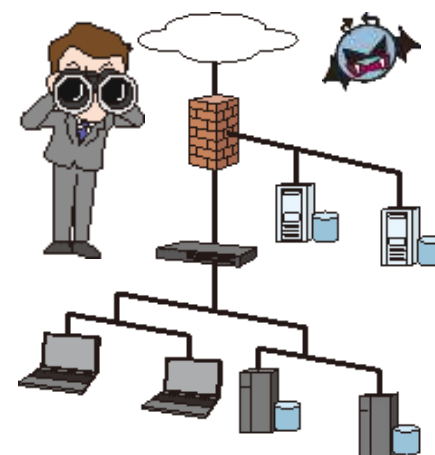
- － セキュリティ対策の予算・体制の確保
- － セキュアなウェブサービスの構築
- － セキュリティ診断によるチェック
- － OS・ソフトウェアの更新
- － WAF・IPSの導入

#### ・ 被害の早期検知

- － 適切なログの取得と継続的な監視

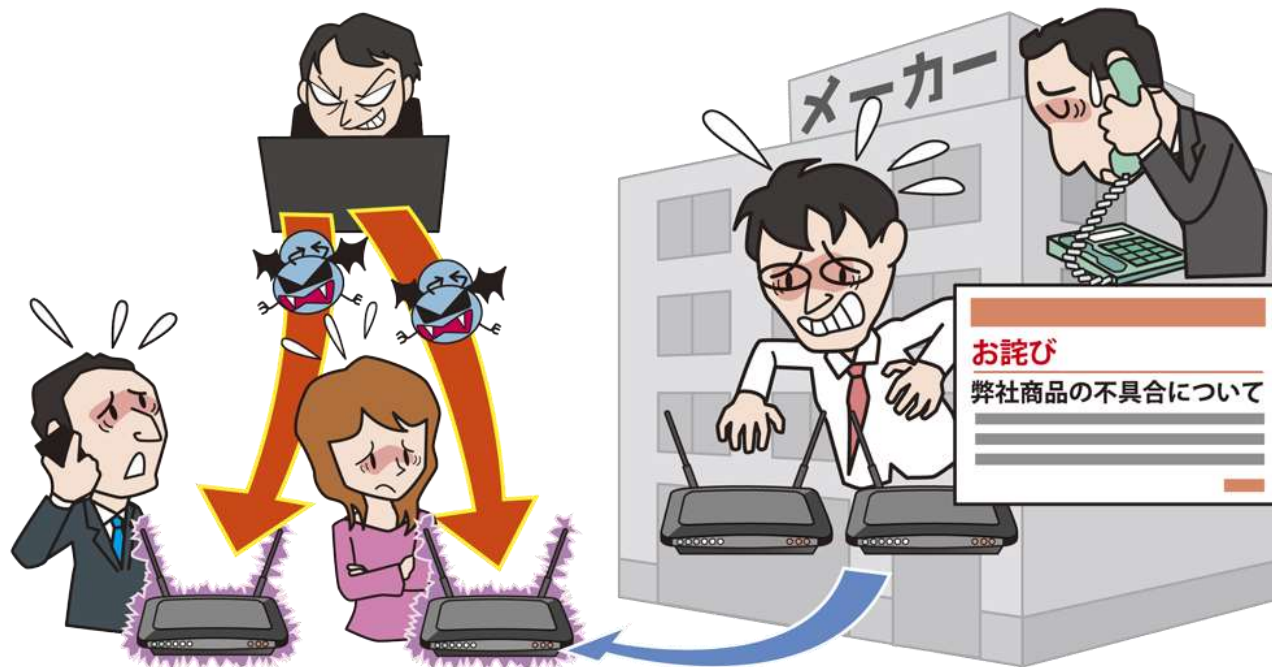
#### ・ 被害を受けた後の対応

- － CSIRTへ連絡
- － 影響調査および原因の追究
- － 漏えい情報における補償



# 【7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頻発、開発ベンダーは脆弱性に対する適切な対処を～



- IoT機器の脆弱性を悪用し、ウイルスを感染させる被害が続いている
- 感染したIoT機器はボット化し、DDoS攻撃等に悪用

# 【7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頻発、開発ベンダーは脆弱性に対する適切な対応を～

## ● 攻撃手口

- IoT機器の脆弱性を悪用し、ウイルスを感染
- 感染したIoT機器の機能を不正利用
- 同じ脆弱性を持つIoT機器を探索し、感染を拡大
- DDoS攻撃を行いインターネットサービスを妨害





# 【7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頻発、開発ベンダーは脆弱性に対する適切な対応を～

## ● 2017年の事例 / 傾向

### ■ ウイルス「Mirai」亜種によるDDoS攻撃

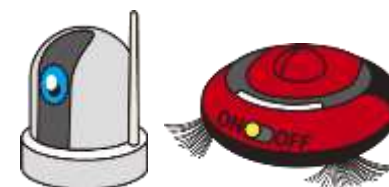
- ・ 7月～9月にボットネットを形成
- ・ 11月に100Gbpsを超えるDDoS攻撃が発生

### ■ 脆弱性を悪用し数百万台規模のウイルス感染

- ・ インターネットに接続された監視カメラなどを標的
- ・ 国内設置の監視カメラにも感染を確認

### ■ ロボット掃除機に第三者から不正に操作される脆弱性

- ・ 無線LANのセキュリティ設定が不十分な場合は危険



# 【7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頻発、開発ベンダーは脆弱性に対する適切な対処を～

## ● 対策一覧

### ■ IoT機器の利用者

- ・ 情報リテラシーの向上
  - － 使用前に説明書を確認
- ・ 被害の予防
  - － ソフトウェア更新(自動設定含む)
  - － 外部からの不要なアクセスを制限
  - － 不要な機能やポートを無効化
  - － 廃棄時は初期化
- ・ 被害を受けた後の対応
  - － CSIRTへ連絡
  - － 機器の電源オフまたは初期化
  - － 影響調査および原因の追究

### ■ IoT機器の開発者

- ・ 被害の予防
  - － 分りやすい取扱説明書の作成
  - － 安全なデフォルト設定や脆弱性の解消
  - － 初期パスワードの変更を強制化
  - － ソフトウェア更新の自動化
  - － 不要な機能の無効化
  - － アクセス可能な範囲を制限
  - － 安全なデフォルト設定や脆弱性の解消
  - － 迅速なセキュリティパッチを提供
  - － 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】内部不正による情報漏えい

～内部不正を許さない管理・監視体制を～



- 従業員・元従業員が内部情報を持ち出し私的に利用
- 社内規則を守らず、社外で業務を行うために持ち出し、その情報を紛失
- 組織の社会的信用が失墜し、経営にも影響を及ぼす

# 【8位】内部不正による情報漏えい

～内部不正を許さない管理・監視体制を～

## ● 攻撃手口

- 自分が持つアクセス権限の範囲で情報を取得
- 過去に使用していたアカウントを不正使用
  - ・ 在任していた時の認証情報を使い情報を取得
- 外部記憶媒体や電子メール等で持ち出し
  - ・ USBメモリー、CD/DVD、ノートPC、紙媒体など



# 【8位】内部不正による情報漏えい

～内部不正を許さない管理・監視体制を～

## ● 2017年の事例／傾向

- 元従業員が業務情報を持ち出し、異なる組織へ持込み
  - ・ 顧客情報や営業情報など約3万2,800件を持ち出し
- 日本年金機構職員が個人情報を買収
  - ・ 金銭目的で年金加入者の個人情報を持ち出し
- 教職員が個人情報を持ち出し、帰宅途中に紛失
  - ・ 小学校4校の児童の個人情報を外部記憶媒体で持ち出し
  - ・ 外部記憶媒体が入った鞆ごと紛失する



# 【8位】内部不正による情報漏えい

～内部不正を許さない管理・監視体制を～

## ● 対策一覧

### ■ 組織

#### ・ 被害の予防

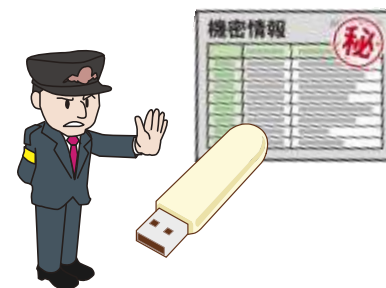
- － 資産の把握・管理体制の整備
- － 重要情報の保護（アクセス制御、暗号化）
- － アカウント、権限の管理・定期監査
- － 外部記憶媒体の利用制限
- － 未許可の機器の接続禁止
- － 情報取扱ポリシーの作成と周知徹底
- － 機密保護に関する誓約
- － 罰則の周知と相互監視の強化

#### ・ 被害の早期検知

- － システム操作の記録・監視

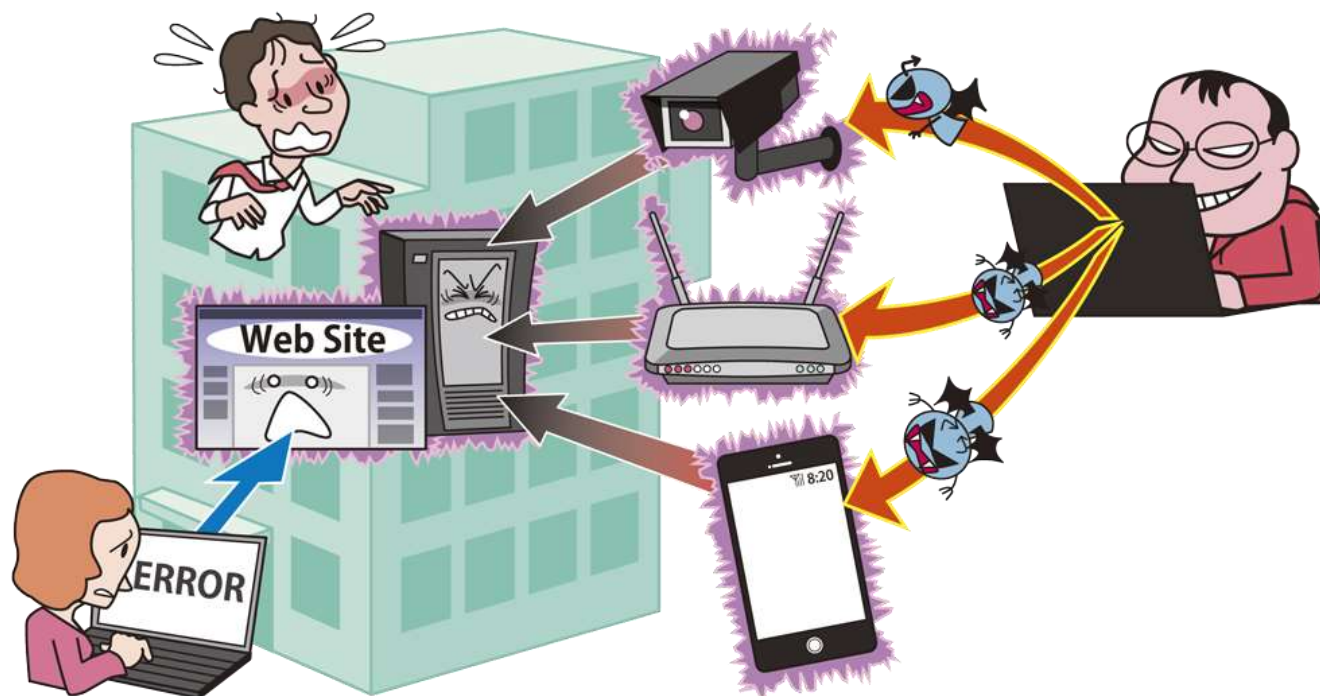
#### ・ 被害を受けた後の対応

- － CSIRTへ連絡
- － 影響調査および原因の追究
- － 警察への相談



# 【9位】サービス妨害攻撃によるサービスの停止

～ボットウイルスの感染拡大に伴う攻撃の大幅増～



- 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サーバーに大量のアクセス
- ウェブサイトの利用者がアクセスできない状態に

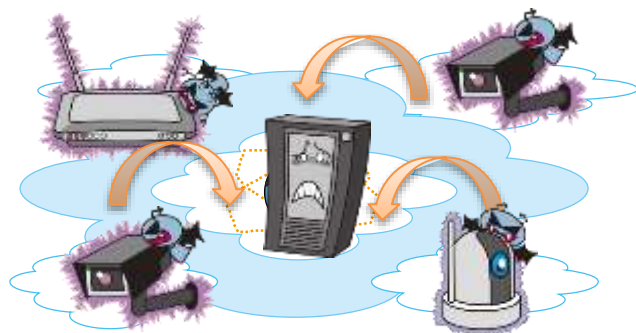


# 【9位】サービス妨害攻撃によるサービスの停止

～ボットウイルスの感染拡大に伴う攻撃の大幅増～

## ● 攻撃手口

- あらかじめ構築されたボットネットを利用
- DNSリフレクター攻撃（送信元を偽りDNSサーバーに問い合わせる）
- DNS水責め攻撃（権威DNSサーバーを高負荷にする）
- DDoS代行サービス（攻撃を代行する不法なサービス）



# 【9位】サービス妨害攻撃によるサービスの停止

～ボットウイルスの感染拡大に伴う攻撃の大幅増～

## ● 2017年の事例／傾向

### ■ スマートフォンからDDoS攻撃

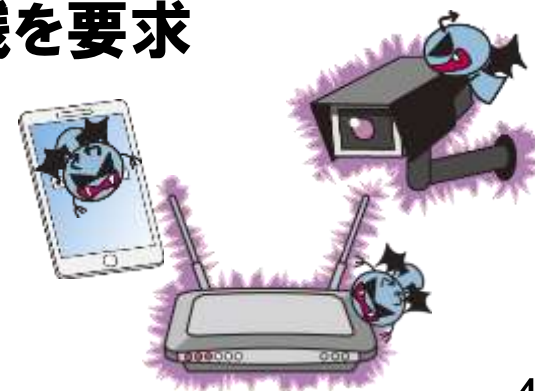
- ・ Android用アプリにウイルスが仕込まれ、スマートフォンをボット化

### ■ IoT機器のボット化

- ・ IoT機器を踏み台に「Mirai」亜種が活発化

### ■ DDoS攻撃を脅迫に利用

- ・ DDoSの攻撃の停止と引き換えに金銭を要求



# 【9位】サービス妨害攻撃によるサービスの停止

～ボットウイルスの感染拡大に伴う攻撃の大幅増～

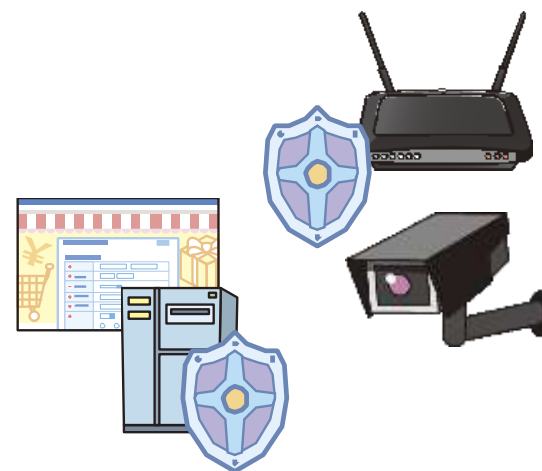
## ● 対策一覧

### ■ ウェブサイトの運営者

- ・ 被害の予防
  - システムの冗長化等の軽減策
  - ネットワークの冗長化
  - DDoS攻撃の影響を緩和するISPやCDNサービスの利用
  - ウェブサイト停止時の代替サーバの用意と告知手段の整備
- ・ 被害を受けた後の対応
  - CSIRTへ連絡
  - 通信制御(攻撃元のブロック等)
  - 利用者へ状況の告知
  - 影響調査および原因の追究

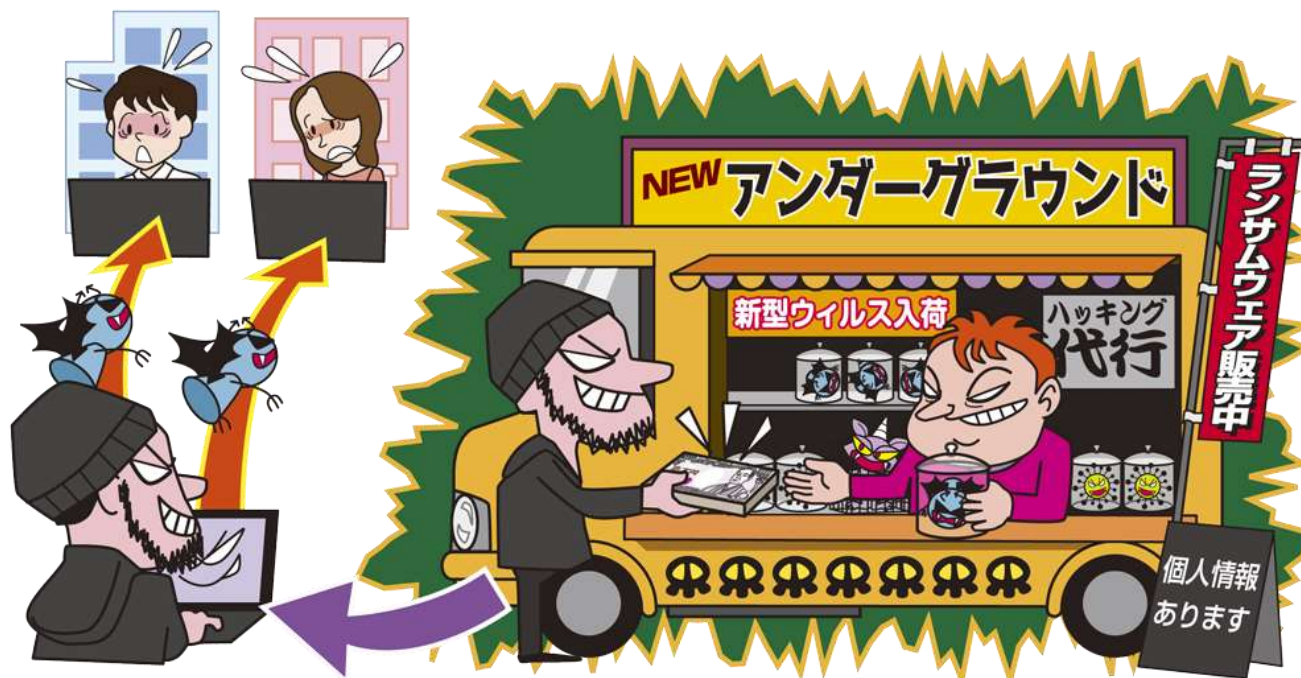
### ■ IoT機器ベンダー

- ・ 被害の予防
  - 脆弱性対策や脆弱性の解消



# 【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～様々な攻撃ツールがアンダーグラウンドで販売されている～



- サイバー犯罪に使用するサービスやツール等の取引市場
- 通常のブラウザでは検索できないウェブサイト上に存在
- 専門知識は不要で容易にサイバー攻撃が可能

# 【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～様々な攻撃ツールがアンダーグラウンドで販売されている～

## ● 攻撃手口

- 購入したサービスやツールを利用して攻撃
- 購入した認証情報を利用してウェブへ不正ログイン

## ● 2017年の事例/傾向

- ランサムウェアを容易に作成するAndroidアプリの公開
- 悪意のハッカーを育成するトレーニングサービスの売買
- Macユーザを標的にしたウイルスの存在
  - ・ 約45万種存在し、無料のランサムウェアも



# 【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～様々な攻撃ツールがアンダーグラウンドで販売されている～

## ● 対策一覧(一例)

### ■ 経営者

- ・ 組織としての対応体制の確立
  - － 問題に対応できる体制(CSIRT等)構築
  - － 予算の確保と継続的な対策の実施

### ■ システム管理者

- ・ 被害の予防
  - － DDoSの攻撃の影響を緩和するISPやCDN等のサービス利用
  - － システムの冗長化など軽減策
- ・ 被害を受けた時の対応
  - － CSIRTへ連絡
  - － 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の用意と告知手段の整備
  - － 影響調査および原因の追究

### ■ PC利用者

- ・ 被害の予防
  - － セキュリティ教育
  - － 受信メール、ウェブサイトの十分な確認
  - － OS・ソフトウェアの更新
  - － セキュリティソフトの導入
  - － 多要素認証方式などの認証方式の利用
- ・ 被害の早期検知
  - － 不審なログイン履歴の確認
- ・ 被害を受けた後の対策
  - － バックアップからの普及



- 以下のページのPDF資料をご覧ください。

## 情報セキュリティ10大脅威 2018

<https://www.ipa.go.jp/security/vuln/10threats2018.html>

