【公表予定】
資　料　6

サイバーセキュリティ対策について

2020年6月12日

独立行政法人情報処理推進機構
セキュリティセンター長　瓜生　和久

サイバーセキュリティ脅威の動向
ー情報セキュリティ10大脅威 2020ー

- 2019年に発生した社会的に影響が大きかったと考えられる情報セキュリティ事案を基に、有識者により構成される「10大脅威選考会」で審議・決定（2020年1月公開）

https://www.ipa.go.jp/security/vuln/10threats2020.html

10大脅威2020
ー個人向け、組織向けー

IPA

・企業に対する組織的かつ執拗な標的型攻撃の脅威継続
・内部不正／不注意による情報漏えいの脅威の増加

昨年順位	「個人」向け脅威	順位	「組織」向け脅威	昨年順位
New!	スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取 Keep!	1
2	フィッシングによる個人情報の詐取	2	内部不正による情報漏えい ↑	5
1	クレジットカード情報の不正利用	3	ビジネスメール詐欺による金銭被害	2
7	インターネットバンキングの不正利用	4	サプライチェーンの弱点を悪用した攻撃	4
4	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害	3
3	不正アプリによるスマートフォン利用者への被害	6	予期せぬIT基盤の障害に伴う業務停止	16
5	ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい ↑	10
8	インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取	7
6	偽警告によるインターネット詐欺	9	IoT機器の不正利用	8
12	インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止	6

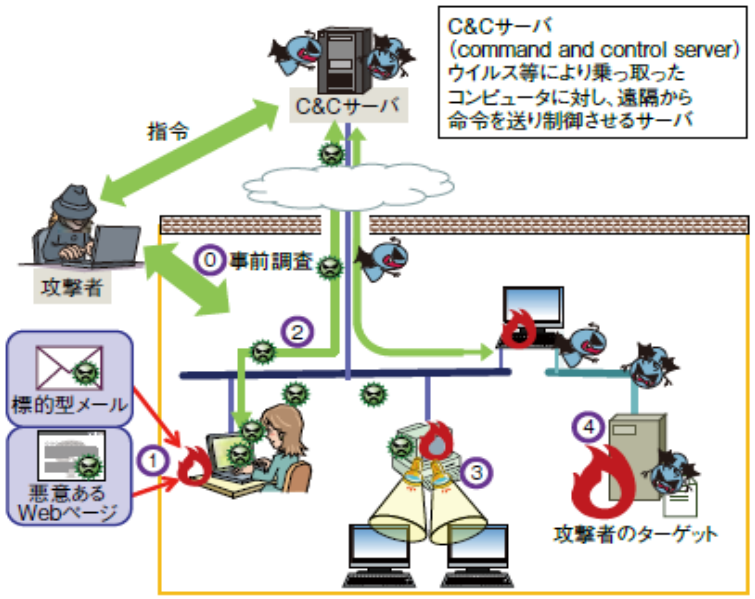
10大脅威に共通する基本的対策

IPA

基本セキュリティ対策
★ソフトウェアの最新版への更新
★ウイルス対策ソフトのインストール
★強いパスワードの使用
★脅威と攻撃手法を知ること（敵を知り…）
★セキュリティ設定見直し（己を知る） (OS、ネットワーク、クラウド)

- **10大脅威の順位は毎年変わる**
  しかし、基本的なセキュリティ対策に変化はない。
- **ITユーザが「常に狙われている」ことは変わらない**
  そして、自助のため<u>セキュリティ対策の意識を常に高く</u>保つこと

【組織１位】:標的型攻撃による機密情報の窃取



0 [事前調査段階]
ターゲットとなる組織を攻撃するための情報を収集する。

1 [初期潜入段階]
標的型攻撃メールや、Webサイト閲覧を通してウイルスに感染させる。

2 [攻撃基盤構築段階]
侵入したPC内でバックドアを作成し、外部のC&Cサーバと通信を行い、新たなウイルスをダウンロードする。

3 [システム調査段階]
情報の存在箇所特定や情報の取得を行う。
攻撃者は取得情報を基に新たな攻撃を仕掛ける。

4 [攻撃最終目的の遂行段階]
攻撃専用のウイルスをダウンロードして、攻撃を遂行する。

【日本国内企業事例】

- 2019年6月
  日本企業の国内研究所のサーバに不審ファイル
  ⇒外部からの不正アクセス発覚
- 不正アクセスは日本企業の中国の子会社から
  ⇒子会社と日本国内の本社や拠点とを結ぶネットを経由して侵入
  ⇒社内セキュリティ製品の脆弱性を悪用
  ⇒管理サーバの制御を奪取
  ⇒各パソコンにウイルス配信・感染拡大
  攻撃者は機密情報を窃取するため、広い権限を持つ管理職層のパソコンを狙い不正アクセス
- 未公開の脆弱性を悪用するゼロデイ攻撃だった
  ユーザ企業側で根本的な対策を行うことは困難
  多層的なセキュリティ対策を実施しておくこと
  ⇒被害の低減に有効

標的型攻撃手口

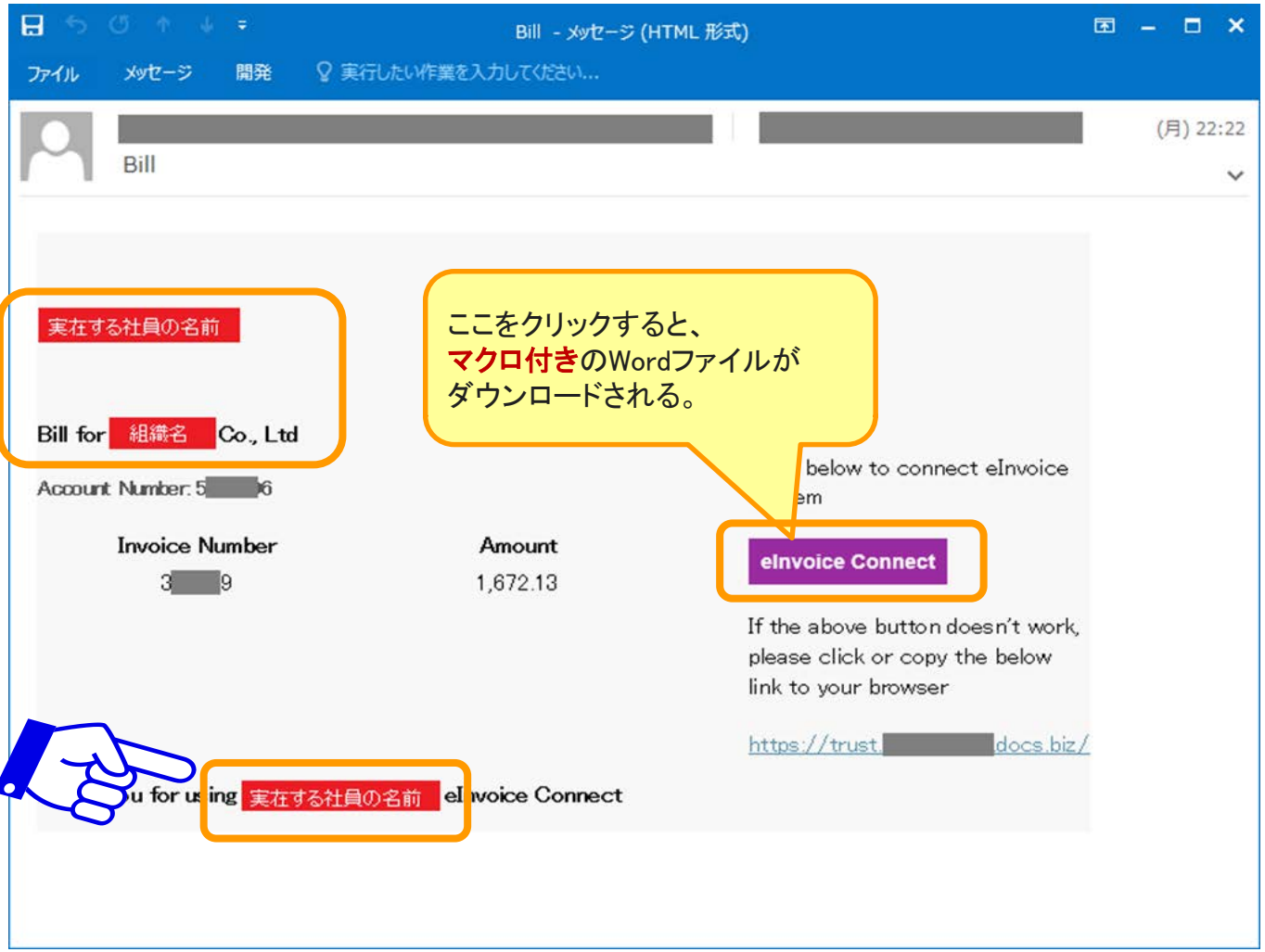
ウイルスに感染させて機密情報を窃取

- 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**）

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

標的型攻撃メールの例



【出典】サイバー情報共有イニシアティブ運用状況［2019年1月～3月］（IPA）

【組織2位】内部不正による情報漏えい

- 2019年のインシデント事例 (※1,※2)
  - ICT関連事業者の従業員が、廃棄を受託していたHDDを窃取し、売却。
    HDDは神奈川県庁で使用されていたもの。
    神奈川県民の個人情報等の機密情報が完全消去されず残存し漏えい。
  - データ漏えいが発覚後、従業員は逮捕。
  - 政府は、公的機関等に対し、**ICTデバイス廃却の際の手順がしっかり遵守されているか**の確認を要請。

※1　https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html
※2　https://www.broadlink.co.jp/info/pdf/20191209-02-press-release.pdf

内部犯行の攻撃手口

内部の従業員は重要情報にアクセスしやすい

- 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

悪意をもって情報を外部に提供してしまう

- USBメモリーやメール等による持ち出し

内部不正を防止するには

情報セキュリティ対策の継続した見直しと改善

①適切なアクセス権限管理

やりにくくする

最小権限の原則・重要情報へのアクセス制限

②持ち出し困難化

（労力の）割りに合わない

コピー制限、社外へのメールやWebの制限

③視認性の確保

やると見つかる

カメラ等の監視機構整備・ログの記録・定期的な確認

④ルール化と周知徹底

いいわけさせない

秘密情報に対する認識向上・外部記録媒体の持ち出しルール

⑤働きやすい環境の整備

その気にさせない

信頼関係の維持・向上、罰則規程の整備

IPA

独立行政法人**情報処理推進機構**

Information-technology Promotion Agency, Japan