IPA Better Life with IT

白書2021に見る情報セキュリティの動向

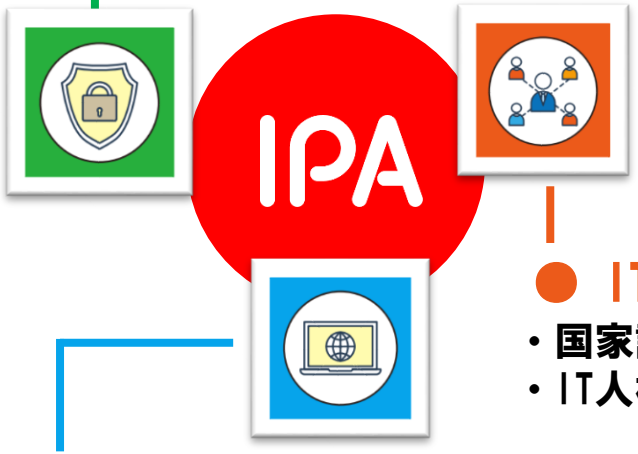
2021年10月

独立行政法人情報処理推進機構
セキュリティセンター　セキュリティ対策推進部
セキュリティ分析グループ

ＩＰＡ（情報処理推進機構）のご紹介

Information-technology Promotion Agency, Japan

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人
- 誰もが安心してITのメリットを実感できる「 頼れるIT社会 」を目指しています



● 情報セキュリティ

・ウイルス、不正アクセス等の届出機関
・情報セキュリティの調査研究、普及啓発活動
・標的型サイバー攻撃への情報共有・初動対応の実施

● IT人材育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成・発掘・スキル明確のとりくみ。若手人材育成。

● IT社会の動向調査・分析・基盤構築

・新たなIT社会の動向調査、新しい技術の安全性・信頼性の確保に向けた指針策定など

情報セキュリティ白書2021

サブタイトル

進むデジタル、広がるリスク：

守りの基本を見直そう

2021年7月30日発行

- IT活用による新しい価値創造を目指すDXの推進やパンデミック対策としての新しい生活・働き方（ニューノーマル）の定着
- 脆弱な組織からの侵入を狙ったサプライチェーン攻撃、特定のターゲットからの高額な身代金を狙って手口が巧妙化したランサムウェア攻撃等の深刻な被害
- 何を守る，誰が守る，どうやって守るを見直し，共通認識を持つことが重要

https://www.ipa.go.jp/security/publications/hakusyo/2021.html

情報セキュリティ白書2021の目次

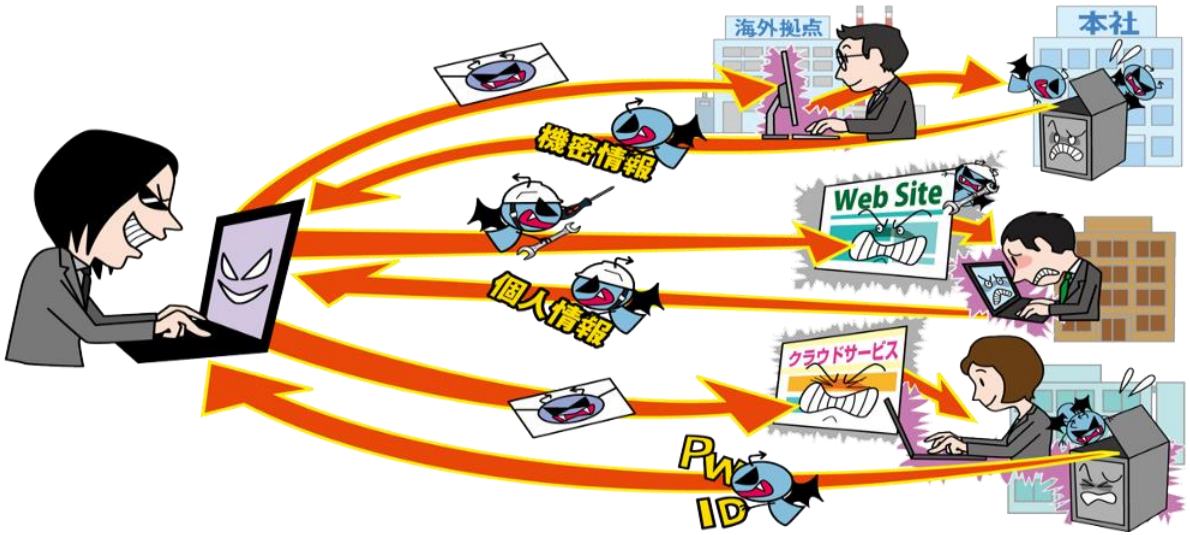
情報セキュリティ白書2021見出し

第1章 情報セキュリティインシデント・脆弱性の現状と対策

標的型攻撃

情報セキュリティ白書2021　1.2.1　標的型攻撃　P17

- メール等を利用し特定組織のPCをウイルスに感染させる
- 組織内部に潜入し長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報窃取やシステムの破壊を行う



標的型攻撃による機密情報の窃取
10大脅威2021　組織編　2位

標的型攻撃の流れ

情報セキュリティ白書2021　1.2.1　標的型攻撃　P17

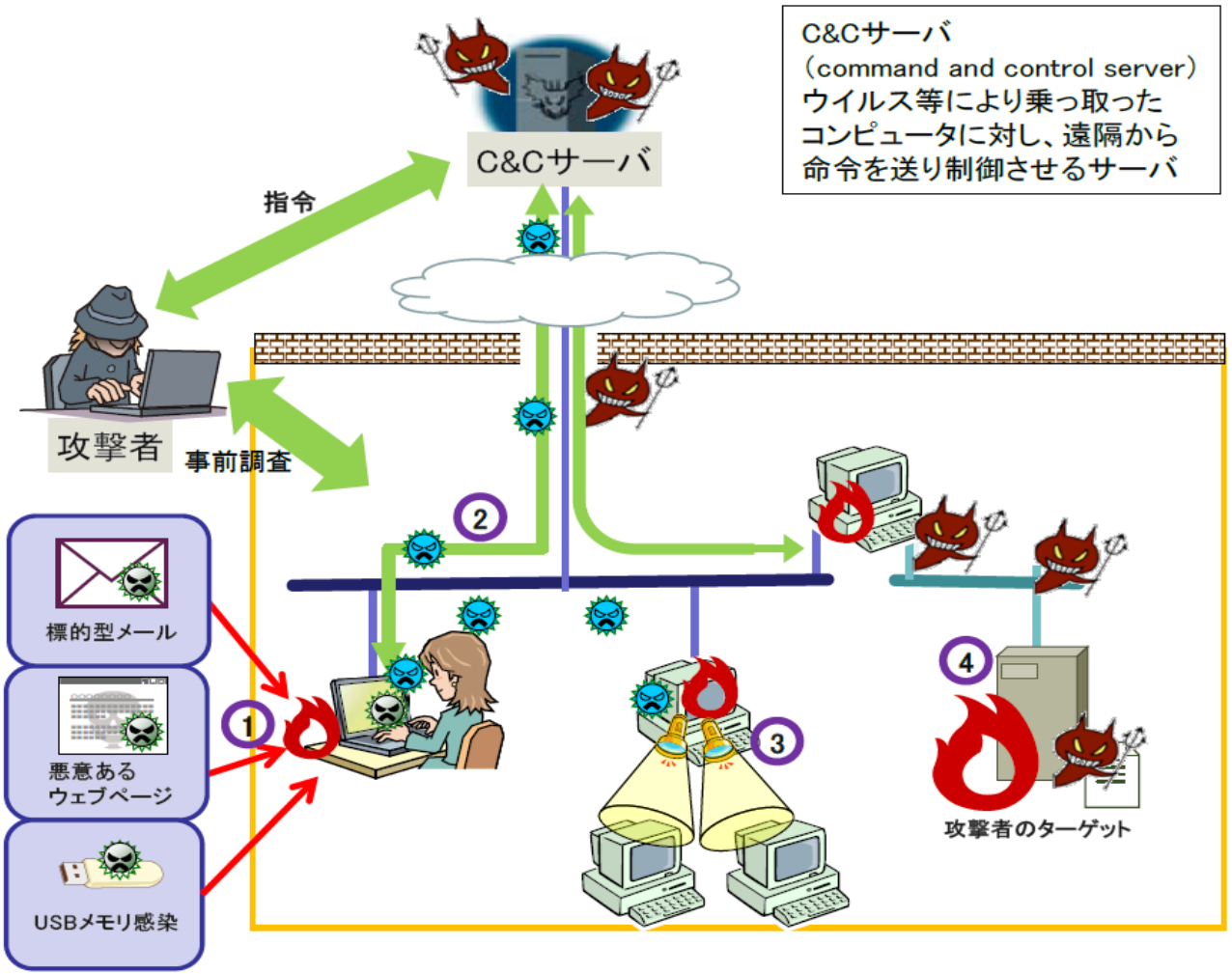
0[事前調査]
ターゲットとなる組織を攻撃する為の情報を収集

1[初期潜入段階]
標的型メールやUSBメモリ、ウェブサイト閲覧を通してウイルスに感染する。

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

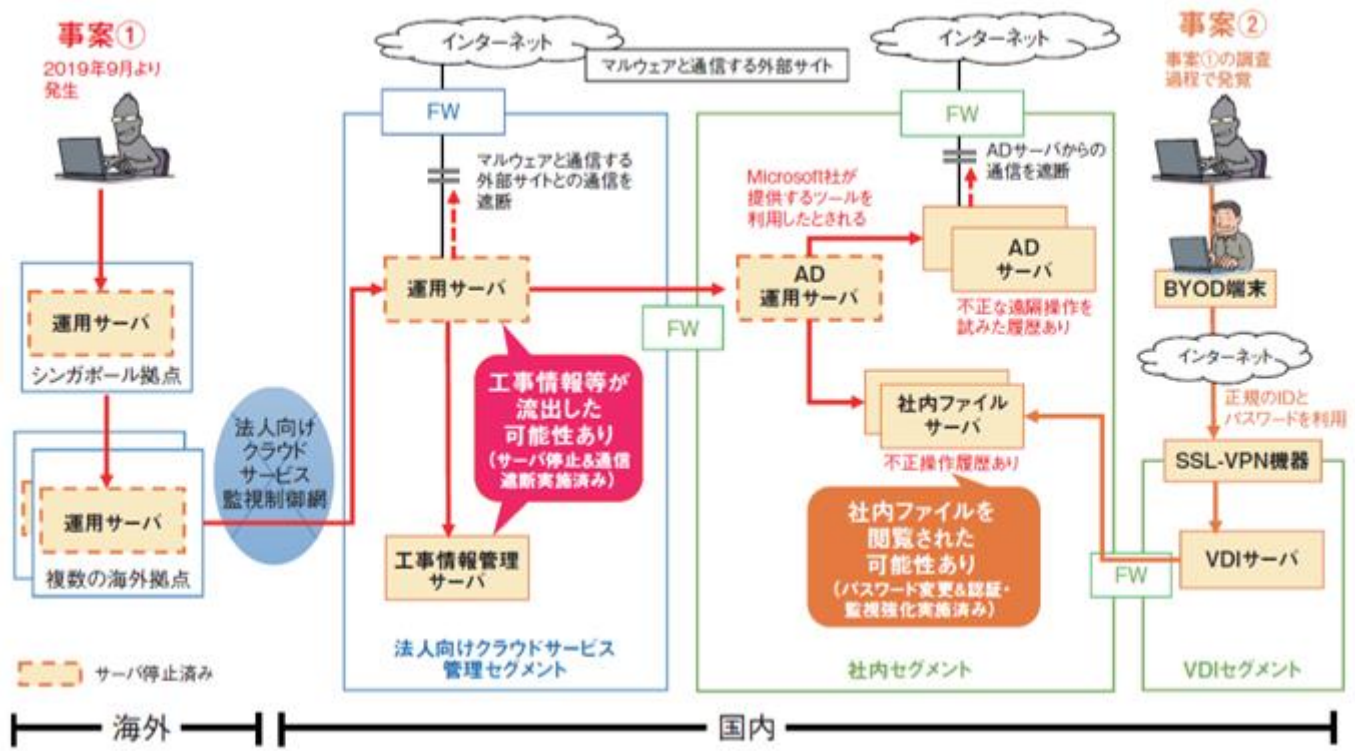
4[攻撃最終目的の遂行段階]
攻撃専用のウイルスをダウンロードして、攻撃を遂行する



C&Cサーバ
（command and control server）
ウイルス等により乗っ取ったコンピュータに対し、遠隔から命令を送り制御させるサーバ

標的型攻撃の事例

情報セキュリティ白書2021　1.2.1　標的型攻撃　P17

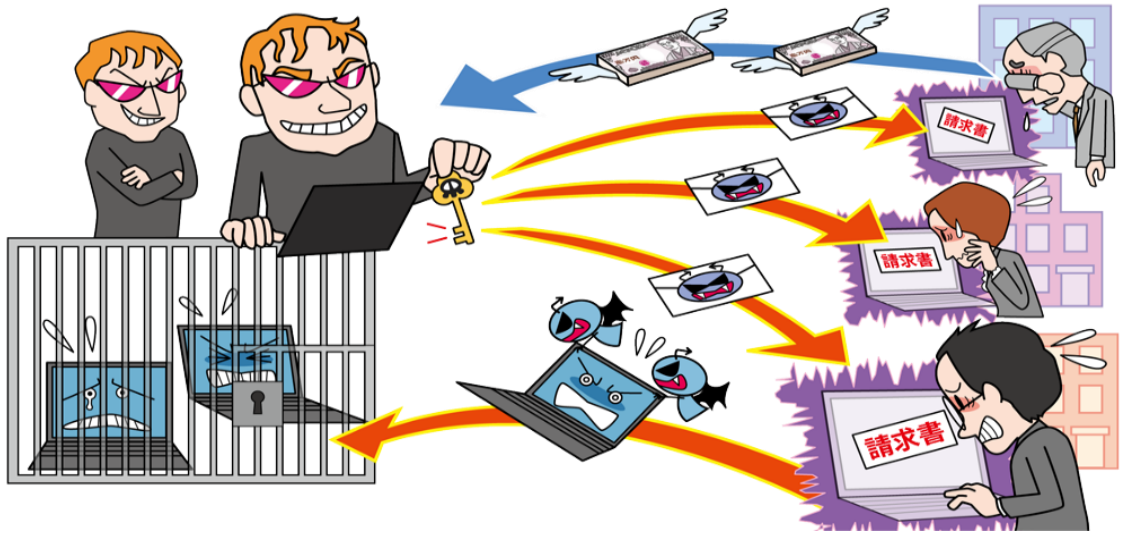


【出典】 NTT コム社「当社への不正アクセスによる情報流出の可能性について（第2 報）」を基にIPA が編集
https://www.ntt.com/about-us/press-releases/news/article/2020/0702.htm

新たなランサムウェア

情報セキュリティ白書2021　1.2.2 新たなランサムウェア攻撃　P23

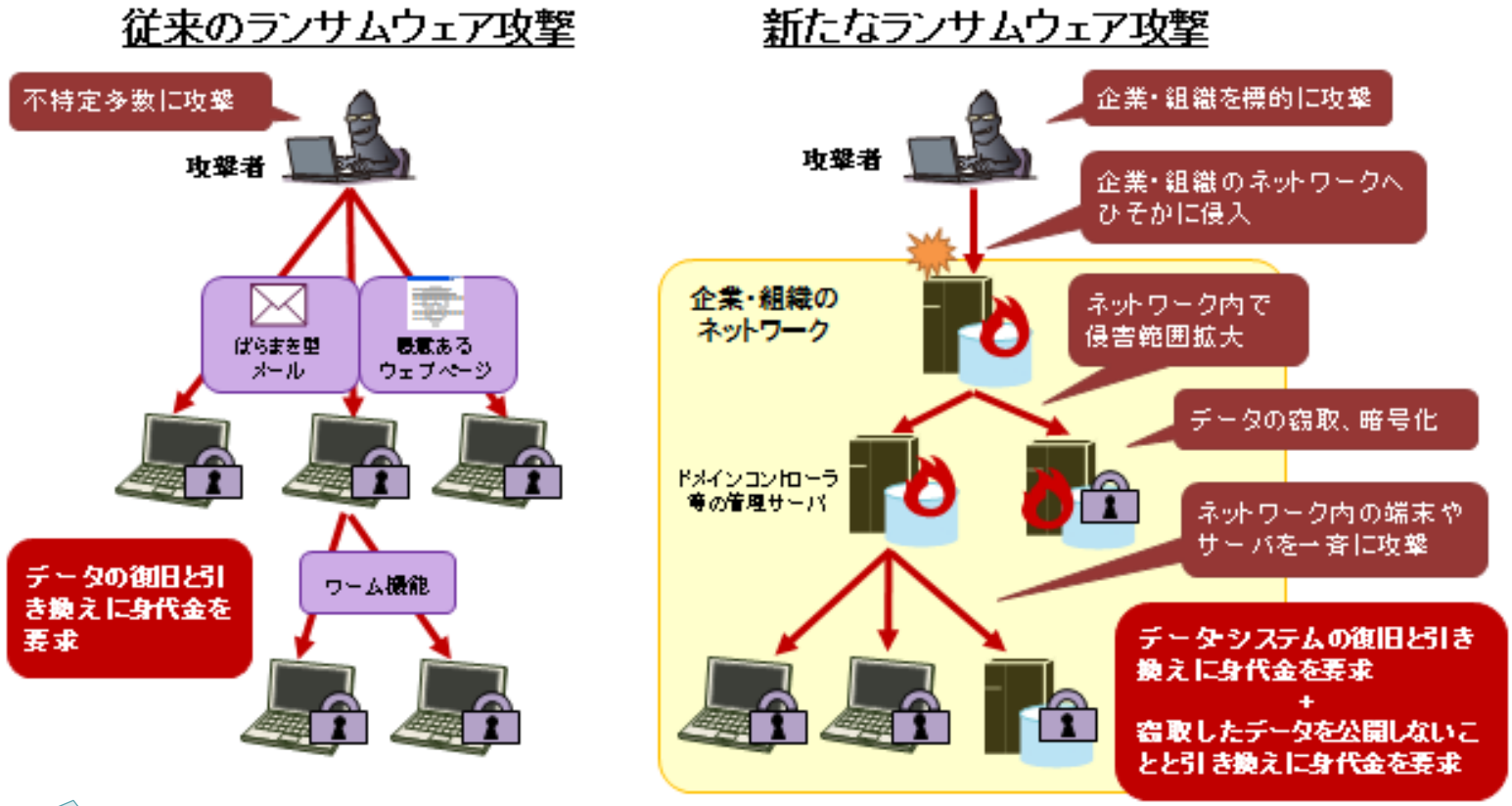
- PC等に保存されているファイルを暗号化され使用不可に
- 復旧と引き換えに金銭を要求される
- 情報を窃取しそれを公開すると脅迫するケースも



ランサムウェアによる被害
10大脅威2021　組織編　1位

従来のランサムウェアとの違い

情報セキュリティ白書2021　P24



2017年5月
WannaCry
が有名

- ✓ <https://www.ipa.go.jp/security/announce/2020-ransom.html>
- ✓ 2020年8月に国内事例が広がってきたため発表
- ✓ Human Operated ransomwareと2重脅迫型ランサムウェアの2種類をとりあげた注意喚起

ランサムウェア攻撃の国内事例

情報セキュリティ白書2021　P24,229

- ゲームメーカーのサーバーがランサムウェアに感染　(※1)
  - ゲームメーカーの社内システムにおいてデータが暗号化され、メールやファイルが使えなくなる等の業務一時停止
  - 顧客や株主情報等を暴露すると脅迫
  - 暗号化解除と暴露の取り止めを条件に身代金を要求
- 特定の組織に特化したランサムウェア　(※2)
  - 自動車メーカーがサイバー攻撃から大規模システム障害
  - 国内外の工場で出荷が一時停止、オフィス系ネットワークシステムにも影響

【出典】
※1　暗号化と暴露で11億円を要求、カプコン襲った「二重脅迫型」ランサムウェアの脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/112400040/
※2　ホンダを標的に開発か、ランサムウェア「EKANS」解析で見えた新たな脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/

ランサムウェア攻撃の海外事例

情報セキュリティ白書2021　P105

- 2021年5月7日、米国石油パイプライン事業最大手の Colonial社はサイバー攻撃を受け、**パイプライン操業を停止**した。8日にはネットワークへのランサムウェア攻撃を認めた。
- FBIは **RaaS（Ransomware as a Service）をビジネスとする東欧系ハッカー集団**による攻撃であるとした。当該集団は目的は金銭であり、政治的混乱を起こす意図はないと発表した 。
- 身代金約について、Colonial社CEOは「早期復旧のために**支払った**」ことを認めた（約4.4億ドル）。
- 2021年7月28日、Biden大統領は重要インフラのサイバーセキュリティ強化プロジェクトの実施を宣言した。

https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

A Colonial Pipeline facility in Pelham, Ala. The company said it had learned on Friday that it was the victim of a cyberattack. Jay Reeves/Associated Press

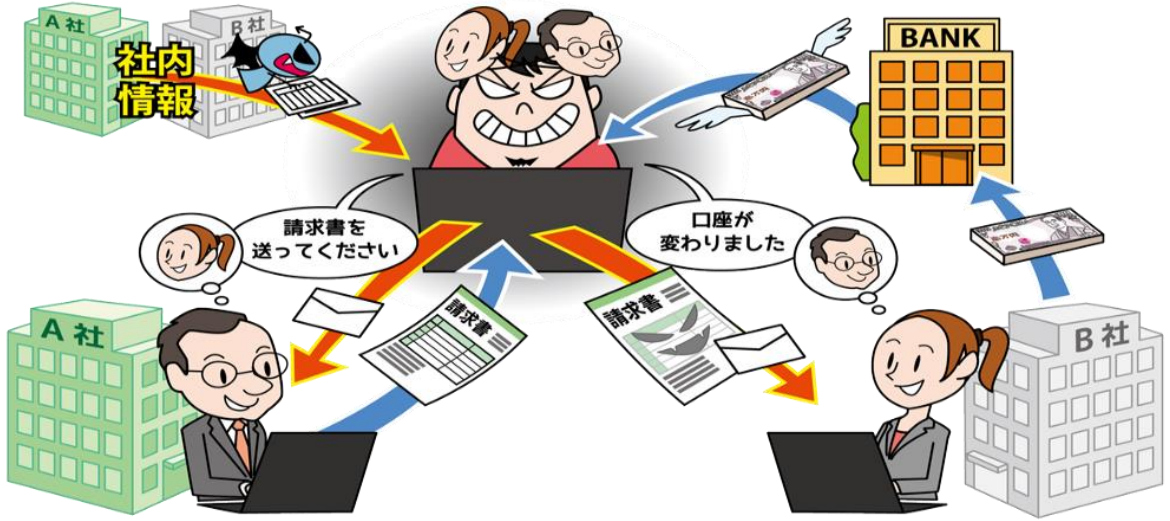
By David E. Sanger, Clifford Krauss and Nicole Perlroth

Published May 8, 2021　Updated May 13, 2021

ビジネスメール詐欺による金銭被害

情報セキュリティ白書2021
1.2.3 ビジネスメール詐欺(BEC)P28

- 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
- 攻撃者が用意した口座へ送金させる

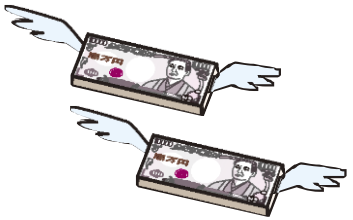


ビジネスメール詐欺による金銭被害
10大脅威2021　組織編　5位

ビジネスメール詐欺による金銭被害事例

情報セキュリティ白書2021
1.2.3 ビジネスメール詐欺（BEC）P30

– 巧妙化する日本語の偽メール （※1）
  - サイバー情報共有イニシアティブ（J-CSIP）が注意喚起
  - 新型コロナウイルスを話題とする偽メールの事例を確認
  - 日本語に不自然な点が少なく日本語を使える攻撃者がいる
    ⇒国内組織が本格的に標的になってきている
– ビジネスメール詐欺の多くは「取引先との請求書偽装」（※2）
  - JPCERT/CCがビジネスメール詐欺の実態調査について公表
  - 攻撃手口では「取引先との請求書の偽装」が多数
  - 以下のポイントからやり取りの過程で気づくこともできる
    - 支払い済みの請求・請求書の体裁が不自然
    - 見慣れない地域への送金
    - 送金先口座の凍結
    - 不自然なローカル言語　等



【出典】
※1 ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）
https://www.ipa.go.jp/files/000081866.pdf
※2 ビジネスメール詐欺の実態調査報告書
https://www.jpcert.or.jp/research/20200325_BEC-survey.pdf

情報セキュリティ対策の基本

- 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
- 下記の「情報セキュリティ対策の基本」は常に意識

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

「情報セキュリティ10大脅威 2021」より

情報セキュリティ白書2021見出し

第2章 情報セキュリティを支える基盤の動向（1／2）

2.1 国内の情報セキュリティ政策の状況
- 2.1.1 政府全体の政策動向
- 2.1.2 経済産業省の政策
- 2.1.3 総務省の政策
- 2.1.4 警察によるサイバー犯罪対策
- 2.1.5 CRYPTRECの動向

2.2 国外の情報セキュリティ政策の状況
- 2.2.1 国際社会と連携した取り組み
- 2.2.2 米国の政策
- 2.2.3 欧州の政策
- 2.2.4 アジア太平洋地域でのCSIRTの動向

2.3 情報セキュリティ人材の現状と育成
- 2.3.1 情報セキュリティ人材の状況
- 2.3.2 産業サイバーセキュリティセンター
- 2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度
- 2.3.4 情報セキュリティ人材育成のための活動

2.4 組織・個人における情報セキュリティの取り組み
- 2.4.1 企業における対策状況
- 2.4.2 中小企業に向けた情報セキュリティ支援策
- 2.4.3 教育機関・政府および地方公共団体等法人における対策状況
- 2.4.4 一般利用者における対策状況

情報セキュリティ白書2021見出し

第2章 情報セキュリティを支える基盤の動向（2／2）

政府のセキュリティ政策動向概観
白書2021に掲載したもの

情報セキュリティ白書2021
2.1.1, 2.1.2, 2.1.3. 2.3.1. 2.4.2, 2.6.3

- NISC（内閣サイバーセキュリティセンター）
  - サイバーセキュリティ2020
    政府のサイバーセキュリティ戦略に基づく2020年度の行動計画
- 経済産業省
  - 産業サイバーセキュリティ研究会
    企業のサイバーセキュリティ強化に関する課題検討と政策推進
    WG1　サイバーフィジカルセキュリティフレーワークの策定、国際標準化提案
    WG2　サイバーセキュリティ経営ガイドラインの普及推進
    サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）設置
    セキュリティ人材育成モデル検討・育成手引書作成，資格制度改訂
    WG3　サイバーセキュリティ製品有効性検証基盤の整備
- 総務省
  - IoT・5Gセキュリティ総合対策2020の推進
    政府調達クラウドのセキュリティ評価制度（ISMAP）推進　（内閣府・経済産業省と共同）
    IoTセキュリティ対策の推進：脆弱なIoT機器の検出・注意喚起
    テレワークセキュリティの推進：ガイドライン改訂
    自治体情報セキュリティの見直し・ガイドライン改訂

サプライチェーンセキュリティ関連政策

情報セキュリティ白書2021
2.1.2, 2.1.3, 2.4.2. 2.6.3

- 政府調達対応情報セキュリティ基準（防衛装備庁）
  - 米国NISTのSP800-171相当の規定（2019年）
- 技術情報の適切な管理に係る認証制度（経済産業省）
  - 産業競争力強化法に基づき、中小企業における技術情報管理を強化するための認証制度（2018年5月）
- サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）（経済産業省）
  - 中小企業を含む官民連携によるサプライチェーンセキュリティ推進コンソーシアム（2020年11月）
- 情報システム・モデル取引・契約書、セキュリティ関連文書公開（経済産業省）
  - IT開発・運用委託契約において、セキュリティ要件を明確化するための契約モデルと手引き書（2020年12月）
- クラウドセキュリティ管理基準及び監査規定（ISMAP）（内閣府、総務省、経済産業省）
  - 政府調達クラウドのセキュリティ認定事業者登録制度（2020年7月）

米国のセキュリティ状況と政策概観

- パンデミック・大統領選挙をめぐるフェイク情報による混乱（インフォデミック）が深刻化
  - 2020年前半はコロナ関連の国家間の中傷・詐欺情報、後半は大統領選挙をめぐる偽情報が世論の対立を増幅。米国議会占拠事件に発展
- 国防重視のサプライチェーンセキュリティ政策は推進継続
  - 中国との覇権争いとパンデミックがからみ、Huawei等の中国ベンダー排除を中心とするサプライチェーンセキュリティの見直しが継続
  - DoDは新たにサイバーセキュリティ成熟度モデル（CCMC）に基づくIT調達を開始。NISTのSP800-171に基づく調達が不評のため、方針転換
- 大規模インシデントが連続、政府のセキュリティ対策見直しが必須
  - 2020年12月にSolarWinds, 2021年3月にMicrosoft Exchange, 5月にColonial事案が発生。Biden政権は対策強化を関係省庁に指示

欧州のセキュリティ状況と政策概観

- インフォデミック対策では、EUはプラットフォーマーを規制
  - プラットフォーム事業者への政治広告の規制など、強い対策をとると明言。中国・ロシアへのけん制もあると思われる
- ポストコロナのデジタルサービス強化のためセキュリティ投資を増強
  - デジタル時代の基盤サービスにおいてセキュリティを技術革新の重要パートと位置づけ、投資を強化
- サプライチェーンセキュリティでは米国追従と独自路線に分かれる
  - 5Gインフラに関し、英国・スウェーデン・フランスが中国ベンダーに対して厳しい姿勢を維持する一方、ドイツは柔軟に対応すると明言
- 個人情報保護の新たな運用
  - 人権・プライバシー保護のためのワクチンパスポート関連法制を整備
  - GDPR運用は厳格化したが、違約金減額は臨機応変に実施

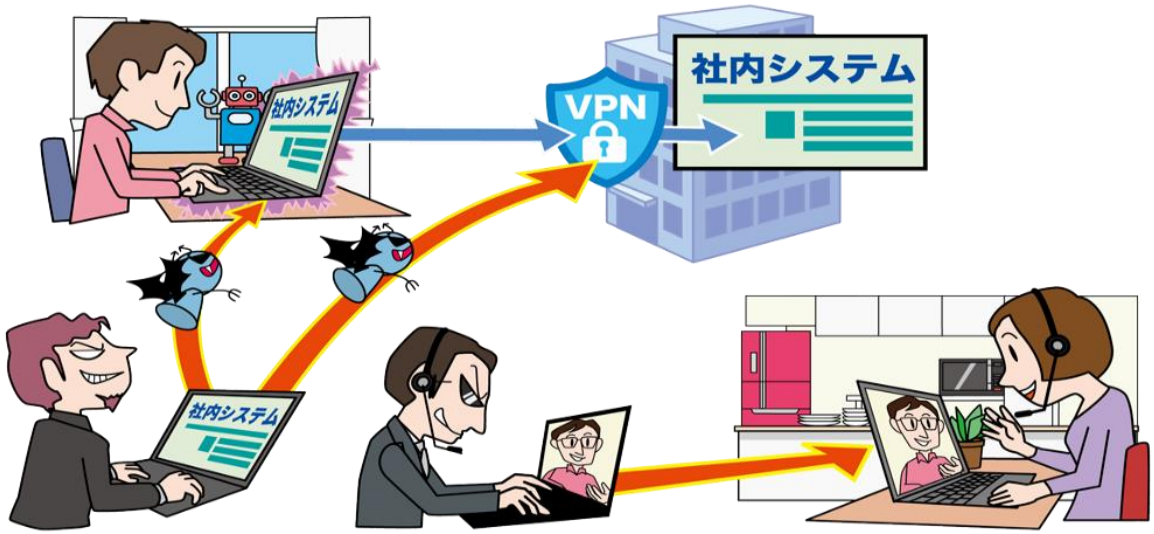
情報セキュリティ白書2021見出し

第3章 個別テーマ

テレワークの情報セキュリティ

情報セキュリティ白書2021　3.3テレワークの情報セキュリティ　P211

- 2020年はコロナ禍の影響によりテレワークへの移行が増加
- ウェブ会議サービスやVPNの本格的な活用の始まりに伴い、それらを狙った攻撃が発生
- ウェブ会議ののぞき見やテレワーク用PCのウイルス感染のおそれ



テレワーク等のニューノーマルな働き方を狙った攻撃
10大脅威2021　組織編　3位

NIST*のセキュリティ関連活動

- 2020年度注目の規格
  - SP800-53 Rev.5
    - 連邦政府のセキュリティ管理策標準第5版。ISO27000シリーズに匹敵
    - 日本語版あり（2021年7月）
  - NISTIR 8259B, 8259C,8259D
    - IoTセキュリティのプラクティス集ドラフト
  - SP800-181 Rev.1
    - 人材育成フレームワーク（NICE Framework）改訂版
    - セキュリティに関するタスク・スキルのリファレンス
  - SP800-207
    - ゼロトラストアーキテクチャガイドライン。日本語版あり（2020年12月）
  - Critical software 調達ガイドライン（策定中）
    - SolarWinds事案を受け、2021年5月の大統領令により策定する新たなソフトウェア調達ガイドライン。今秋ドラフト公開予定。

*NIST: 国立標準技術研究所　National Institute of Standards and Technology
日本語版規格のリスト：
https://www.ipa.go.jp/security/publications/nist/index.html

参考：2020年度のセキュリティイベント（１）

	○主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2020年　4月	● テレワーク環境やオンライン会議サービスの脆弱性、及びビジネスメール詐欺について、国内外で注意喚起（1.2.3、1.3.1、2.2.2） ● イスラエル水道システムにサイバー攻撃（3.1.1）	交通 ISAC が創設（3.1.4） 米国でテレワークのセキュリティガイダンス、コロナ禍における重要インフラ基盤の運用と従業員の安全に関するガイダンスを公開（2.2.2）
5月	● 情報通信事業者が海外拠点からの不正アクセスを公表（1.2.1） ● ノルウェーの投資ファンドが海外送金で 1,000 万ドルのビジネスメール詐欺被害（1.2.3）	欧州で位置情報及び接触追跡ツールに関するガイドライン、研究目的の健康情報処理に関するガイドラインを公開（2.2.3） 米国でサプライチェーンリスク管理指針を公開（2.2.2）
6月	● 国内大手自動車メーカやアルゼンチン電力会社がランサムウェア攻撃被害を公表（3.1.1） ● Ripple20 のゼロデイ脆弱性を公表（1.2.5、3.1.2、3.2.2）	「政府情報システムのためのセキュリティ評価制度（ISMAP）」運用開始（2.6.3）
7月	● 情報通信事業者が BYOD 端末経由の不正アクセスを公表（1.2.1）	「サイバーセキュリティ 2020」公開（2.1.1） 「IoT・5G セキュリティ総合対策 2020」公開（2.1.3）
8月	● IPA が新たなランサムウェア攻撃について注意喚起（1.2.2） ● 米国金融機関が海外送金 1,080 万ドルのビジネスメール詐欺被害（1.2.3）	IPA が「脆弱性対処に向けた製品開発者向けガイド」公開（3.2.4） 米国 NIST が SP 800-207（ゼロトラストアーキテクチャ）公開（3.4.2）
9月	● 携帯通信会社が提供するマネーサービスを介した銀行の預金の不正引き出しが発覚（1.1.2）	経済産業省が「サイバーセキュリティ体制構築・人材確保の手引き第１版」公開（2.1.2、2.3.1）

参考：2020年度のセキュリティイベント（２）

10月	● JPCERT/CC がランサム DDoS 攻撃の注意喚起（1.2.4）	■ 総務省が「スマートシティセキュリティガイドライン（第1.0 版）」公開（2.1.3）
11月	● ゲーム会社が「新たなランサムウェア攻撃」被害を公表（1.2.2） ● NISC が「新たなランサムウェア攻撃」について注意喚起（1.2.2）	■ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）設立（2.1.2、2.4.2） ■ 「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」策定（2.1.2、3.1.4）
12月	● NISC、JPCERT/CC が VPN 製品の脆弱性に対する注意喚起（1.2.5、1.3.1、3.1.2） ● 米国でネットワーク管理用プラットフォームのウイルス感染で大規模被害公表（3.1.1）	■ 「情報システム・モデル取引・契約書」第二版公開（2.1.2） ■ 米国 NIST が SP 800-53 Rev.5（組織のセキュリティ・プライバシー管理策）更新（3.4.2）
2021 年　1月	● NISC がクラウドサービス製品の設定不備について注意喚起（1.2.8） ● Europol による Emotet テイクダウン（1.2.6）	■ 産業サイバーセキュリティ研究会 WG1 に宇宙産業 SWG を設置（2.1.2）
2月	● 米国で浄水場への攻撃で薬品投入量を操作される被害（3.1.1）	■ 警察庁、総務省、ICT-ISAC、及び ISP 各社が連携して、Emotet 感染の恐れのある利用者に注意喚起を行う取り組みを開始（1.2.6）
3月	● 海外航空会社の顧客管理システムが不正アクセスを受け、加盟していた日本の航空会社にも被害（1.2.8）	■ サイバーセキュリティに関する国連オープン・エンド作業部会最終会合開催（2.2.1）

※ 2020 年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項番である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

ご清聴ありがとうございました

情報セキュリティ白書，情報セキュリティ10大脅威はIPAのサイトからダウンロードいただけます

情報セキュリティ白書2021

https://www.ipa.go.jp/security/publications/hakusyo/2021.html

情報セキュリティ10大脅威2021

https://www.ipa.go.jp/security/vuln/10threats2021.html