サイバーセキュリティ対策セミナー

令和４年度　第１期

本テキスト（付録等も含む）は、各社において「自組織のセキュリティ啓発」のために、自由にご活用いただけます。

はじめに

対象者 中小企業者のサイバーセキュリティ担当者等

目的 サイバー攻撃・犯罪の被害からの防御・認知方法・対処要領を習得し、サイバー犯罪による被害や被害拡大を防止する

主なテーマ

1. サイバー攻撃・犯罪の情勢
2. 標的型メール攻撃 実習あり
3. ランサムウェアによる攻撃 実習あり
4. その他の主な攻撃

※必要に応じて、巻末の「**用語集・索引**」、別添の「**付録**」をご活用ください。

1

本セミナーは、「**中小企業者のサイバーセキュリティ担当者等**」を対象に、「サイバー攻撃・犯罪の被害からの**防御・認知方法・対処要領**を習得し、サイバー犯罪による**被害や被害拡大を防止**する」ために開催するものです。

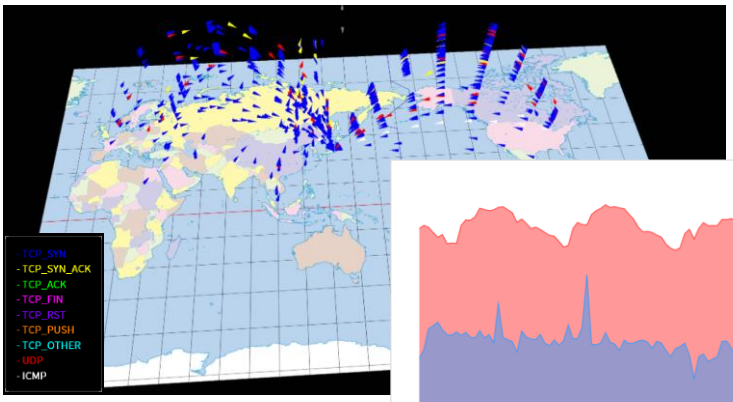
本テキストの巻末には、「**用語集・索引**」が掲載されています。分からない用語がある場合等にご活用ください。
また、本テキストには、**実際のセキュリティ対策やインシデント対処に役立つ付録**が用意されています。自組織のセキュリティ対策、インシデント対処の準備にご活用ください。

付録	説明
A.セキュリティ対策チェックリスト	自組織のセキュリティ対策を点検する際に活用できるチェックリストです。
B.インシデント対処フロー	標準的なインシデント対処の流れをまとめた資料です。 自組織の環境に合わせてカスタマイズしてご活用ください。
C.よくあるQ&A事例集	セキュリティ対策やインシデント対処等に関連するQ&Aをまとめた資料です。

1. サイバー攻撃・犯罪の情勢

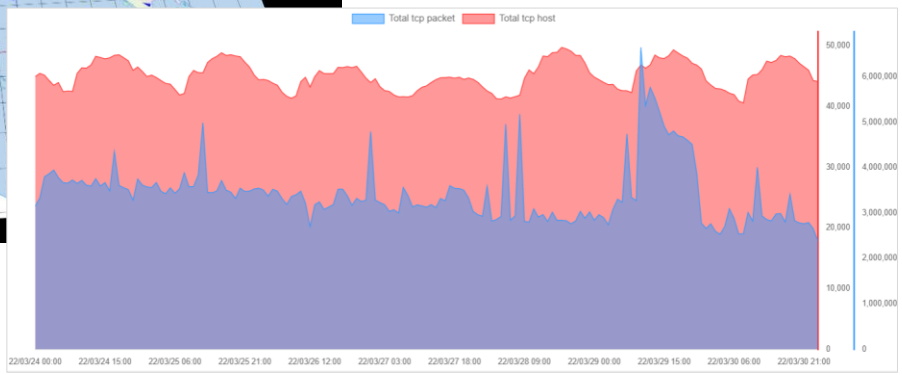
1.1 数字で見るサイバー攻撃・犯罪

今この瞬間にも、サイバー攻撃に起因すると思われる膨大なパケットが、日本に向けて送信され続けている



▲ダークネットに到達したパケット

▼ダークネット観測の統計値



【出典】国立研究開発法人 情報通信研究機構（NICT）「NICTERWEB」（https://www.nicter.jp/）

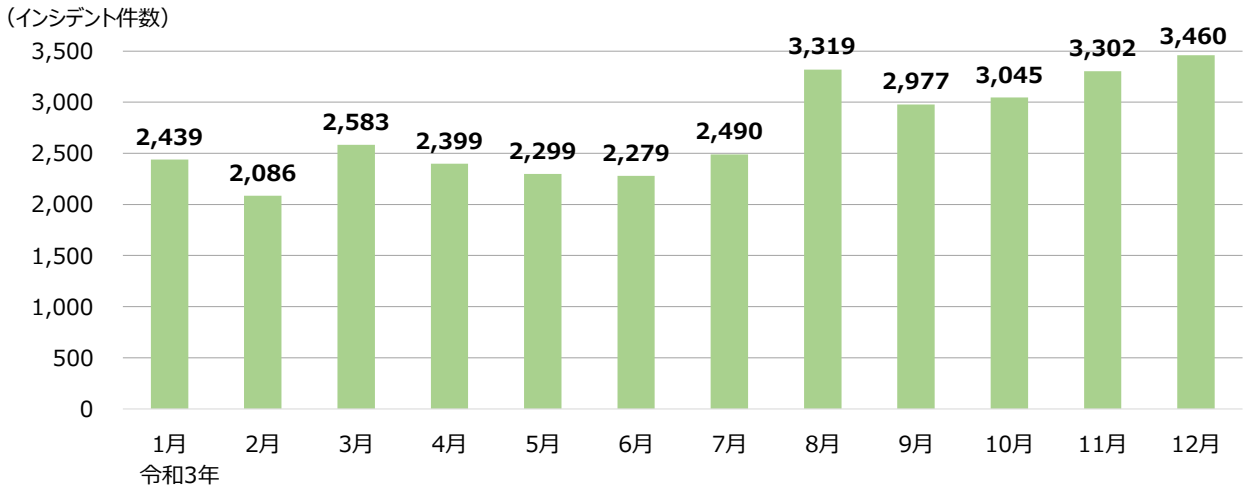
3

今この瞬間にも、**サイバー攻撃に起因**すると思われる**膨大なパケット**が、日本に向けて送信され続けており、サイバー攻撃・犯罪は決して対岸の火事ではありません。

「国立研究開発法人 情報通信研究機構（NICT）」では、**無差別型サイバー攻撃の動向把握**のために、**ダークネットの通信**を観測しています。
ダークネットは、どの機器にも割り当てられていない**未使用のIPアドレス群**であり、本来ダークネットを宛先・送信元とする通信は発生しないはずです。しかし、観測結果によると膨大な通信が確認されており、そのほとんどがサイバー攻撃に起因するものであると推測されています。

1.1 数字で見るサイバー攻撃・犯罪

日本国内で毎月2千件を超えるインシデントが発生しており、どの組織でもインシデント発生の可能性がある



【出典】JPCERT/CC「インシデント報告対応レポート」（https://www.jpcert.or.jp/ir/report.html）

4

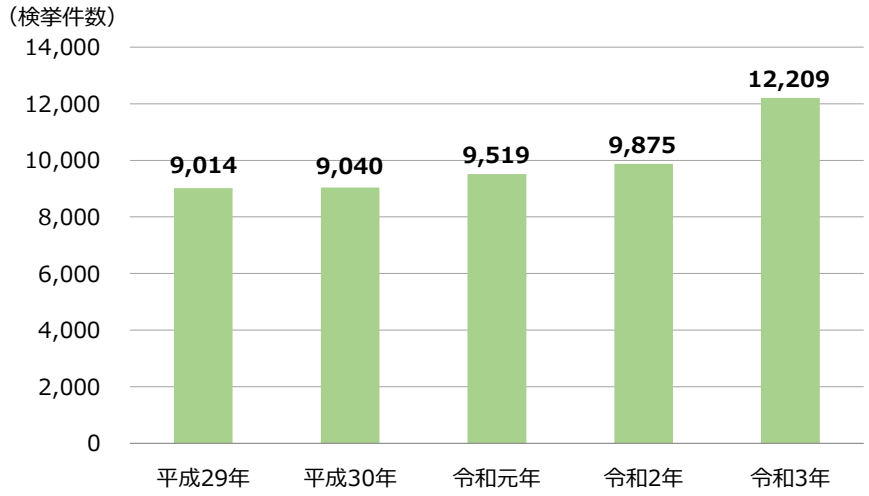
日本国内で**毎月2千件を超えるインシデント**が発生しており、**どの組織でもインシデントが発生する可能性**があります。

本グラフは、あくまでもJPCERT/CC（※）に報告されたインシデント件数であり、実際には、もっと多くのインシデントが発生していると推察されます。
インシデントの内訳は、アカウント情報の窃取を狙ったと思われる「**フィッシングサイト**」が最多であり、サイバー攻撃・犯罪のターゲット調査と思われる「**スキャン**」が続きます。

※JPCERT/CCは、日本国内のインシデント報告の受付、対応支援、発生状況の把握、手口の分析、再発防止策の検討・助言等を、技術的な立場から行う組織。

1.1 数字で見るサイバー攻撃・犯罪

サイバー犯罪の検挙件数は年々増加している



【出典】警察庁「令和３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」
（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf）

5

警察庁によると、「不正アクセス禁止法（※1）違反」や「コンピュータ・電磁的記録対象犯罪（※2）」といったサイバー犯罪の**検挙数は年々増加**しており、令和3年は「**12,209件**」に達する見込みであると発表されています。
また、「ランサムウェアによる被害が拡大し、市民生活に大きな影響を及ぼす事案も確認されているほか、不正アクセスによる情報流出や、サイバー攻撃事案への国家レベルの関与も明らかとなるなど、サイバー空間における脅威は極めて深刻な情勢が続いている」と情勢が分析されています。

※1 不正アクセス禁止法で禁止されている行為は、次のとおりです。
- なりすまし（他人のID・パスワード等を不正に利用する）行為
- セキュリティ・ホール（プログラムの不備等）を攻撃して侵入する行為
- 他人のID・パスワードを不正に取得する行為及び不正に保管する行為
- 他人のID・パスワードを第三者に提供する行為（業務その他正当な理由による場合を除く）
- 他人のID・パスワードの入力を不正に要求する行為（いわゆるフィッシング行為）

【出典】警視庁「不正アクセス」（https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/law/fusei_access.html）

※2 本調査におけるコンピュータ・電磁的記録対象犯罪の詳細は、次のとおりです。
- 電子計算機使用詐欺
- 電磁的記録不正作出・毀棄等
- 電子計算機損壊等業務妨害
- 不正指令電磁的記録に関する罪

1.2 サイバー攻撃の事例

No.	時期	被害組織	被害概要	攻撃手口等
1	R3.8	食品会社	•財務管理（26社利用）、販売管理（11社利用）を行う主要な基幹システムサーバ、ファイルサーバ、バックアップサーバがマルウェアの感染し、システム停止 **•BCP（事業継続計画）を上回る被害が発生**	ランサムウェアと思われる（公表なし）
2	R3.10	地方病院	**•地方の町立病院がランラムウェアに感染**し、電子カルテシステムが停止 **•システム再構築に2億円**の費用見込み（**R3年12月末に復旧**）	システムの脆弱性、ランサムウェア
3	R3.11	ECサイト利用企業	•ECサイトシステムの脆弱性が悪用され、情報漏えいやXSSの被害が発生 **•複数の企業が本システムを利用していたため、複数のECサイトで被害**	システムの脆弱性、サプライチェーン
4	R3.12	不特定	•Log4jの深刻な脆弱性CVE-202144228が公表 •HeartBleed、Shellshock、Wannacryレベルなみの深刻度と評価	ライブラリの脆弱性
5	R4.2	不特定	•マルウェア**Emotet**が再流行 **•様々な企業/組織になりすましたメール**が出回っている •感染被害のあった企業/組織が**外部に対して注意喚起等の対応**を実施	Emotet なりすましメール
6	R4.2	自動車	**•サプライヤー**のシステム障害（**ランサムウェア**）により**全工場の操業が停止**	ランサムウェア サプライチェーン
7	R4.3	ECサイト利用企業	•クレジットカード決済代行会社の**決済データセンターサーバに対して不正アクセス** サービスを利用していた企業、自治体など数十件以上で被害が発生	サプライチェーン SQLインジェクション

（上記以外にも、サービス妨害被害、改ざん被害、フィッシング被害等が発生しています）

※各組織の公表資料、ニュースサイト等から独自に収集した情報であり、最新状況と異なる場合があります。

6

様々な業種で、非常に多くのサイバー攻撃が確認されています。

Emotetの急激な感染再拡大

Emotet（エモテット）は、メールに添付された悪質な「パスワード付きZIPファイル」、「マクロが埋め込まれたExcelやWordファイル」、メール文中の「不正なリンク」等から感染するマルウェアです。Emotetに感染すると、メールアドレスやパスワード、電話帳等の情報を窃取されたり、さらに他の悪質なマルウェアに感染させられたりします。

令和2年頃に猛威を振るいましたが、国際的な作戦が実行され、令和3年1月に欧州刑事警察機構が「テイクダウン（攻撃者サーバーの停止）に成功した」と発表していました。
しかし、令和3年末頃から、急激な感染再拡大が確認されており、注意が必要です。
（Emotetの詳細は、「2. 標的型メール攻撃」で解説します。）

ランサムウェア被害の増加

ランサムウェアとは、感染端末をロックしたり、ファイルを暗号化したりすることによって使用不能にした後、元に戻すことと引き換えに「身代金」を要求するマルウェアのことです。

以前は「ばらまき型」が主流でしたが、近年は標的の組織に侵入し、機密情報を窃取した上で重要サーバー等を暗号化し、「情報暴露」と「データ復元」の二重で脅迫されるケースが増えています。
（ランサムウェアの詳細は、「3. ランサムウェアによる攻撃」で解説します。）

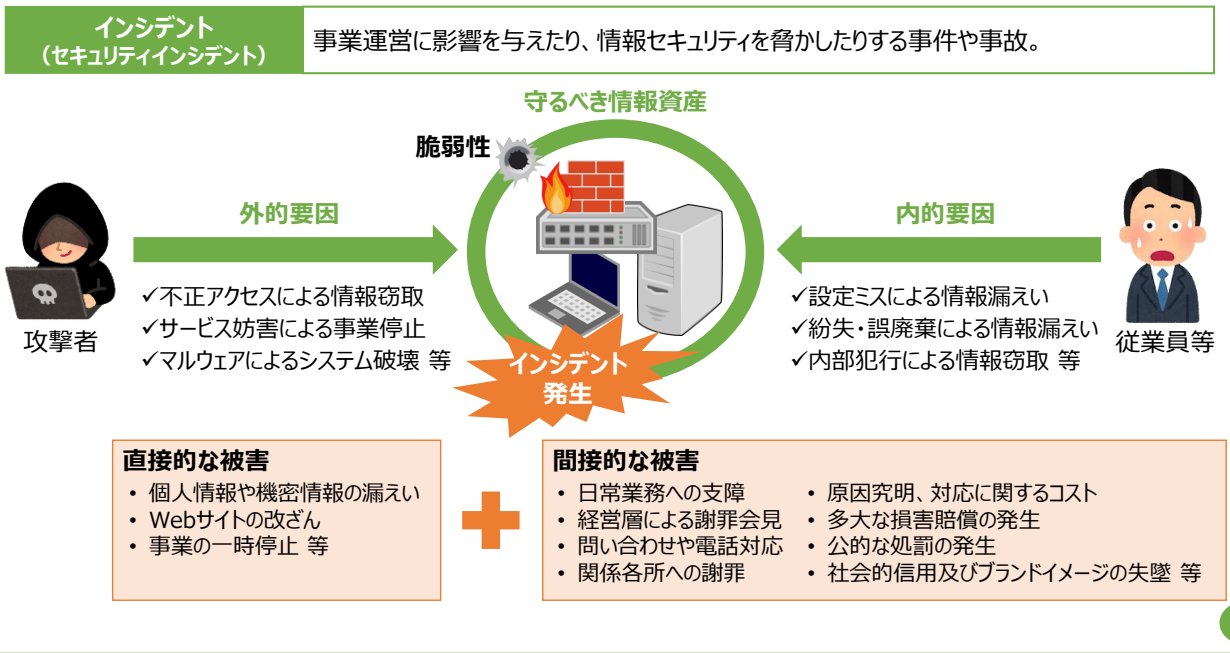
サプライチェーンを狙った攻撃

サプライチェーンとは、サービス提供を行うための一連のビジネス活動を意味し、取引先や関連企業などを含めたビジネス活動の流れを指します。

セキュリティ対策が不十分な取引先や関連会社を攻撃し、これらの組織を足掛かりに、標的の組織に侵入するケースが多く確認されています。

また、標的組織で利用されている「ソフトウェア製品」や「製品の更新プログラム」等に不正なプログラムを混入させたり、「ソフトウェア製品」の脆弱性を悪用して攻撃を行います。

1.3 インシデントの影響



「**インシデント**」（セキュリティインシデント）とは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のことです。

インシデントを発生させる脅威には、「**外的要因**」と「**内的要因**」があります。
「**守るべき情報資産**」に、ソフトウェアが最新バージョンに更新されていない、組織内PCがきちんと管理されていないといった「**脆弱性**」が存在すると、これらの脅威が現実のものとなり、インシデントが発生する可能性が高まります。

インシデントが発生すると、個人情報や機密情報の漏えい、Webサイトの改ざんといった「**直接的な被害**」だけではなく、「**間接的な被害**」も発生し、事業継続に甚大な影響を及ぼします。

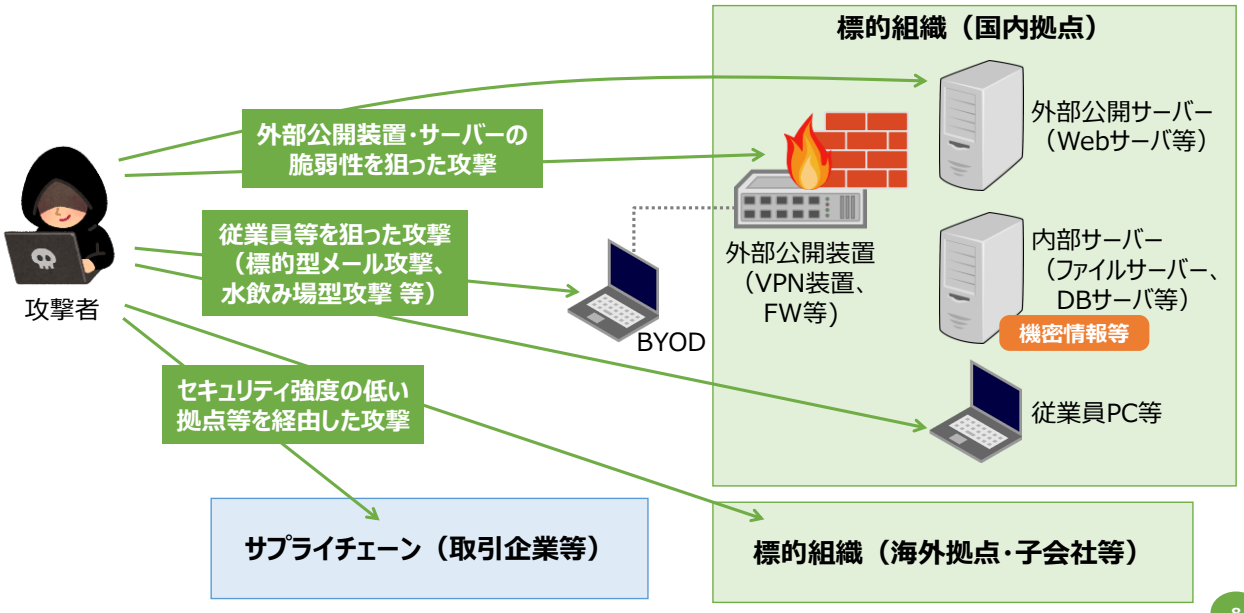
次ページでは、特に甚大な被害となりやすい「**外的要因**」について、攻撃者がどのように標的組織に侵入するのか、主な侵入経路を解説します。

Let's try

インシデントを防ぐためのセキュリティ対策の点検
インシデントを防ぐためのセキュリティ対策ができているか、「**付録A. セキュリティ対策チェックリスト**」を参考に、自組織の対策状況を点検してみてください。

インシデント発生時のための備え
万が一インシデントが発生した場合に、影響を最小化し、業務継続するためには事前の備えが必要です。
自組織で必要な備えができているか、「**付録B. インシデント対処フロー**」を参考に点検してみてください。

1.4 攻撃者の主な侵入経路



攻撃者は、様々な手法で標的組織への侵入を試みます。
近年では、テレワーク等のニューノーマルな働き方の急速な拡大に伴い、VPN装置やBYODから組織内に侵入される事例が増えています。

また、セキュリティ強度の低い「**サプライチェーン（取引先企業等）**」や、「**標的組織の海外拠点・子会社等**」が狙われ、標的組織の情報が盗まれたり、標的組織に侵入するための踏み台にされたり、といった事例が多数報告されています。

本セミナーでは、従業員等を狙った「**標的型メール攻撃**」について、「2. 標的型メール攻撃」で詳しく解説します。

用語解説

BYOD（ビーワイオーディー）
Bring Your Own Deviceの略。個人所有の機器を業務利用すること。

FW（ファイアーウォール）
IPアドレス、ポート番号・プロトコル等をもとに通信の許可（通過）、拒否（遮断）を行うセキュリティ対策製品。専用のハードウェアだけでなく、OSの機能、またソフトウェアとして実装する場合もある。

VPN（ブイピーエヌ）
Virtual Private Networkの略。認証や暗号化により、公衆ネットワーク上で仮想的な専用ネットワークを実現する技術。

2. 標的型メール攻撃

2.1 標的型メール攻撃とは

標的型メール攻撃	ソーシャルエンジニアリング等で調べた情報を基に、関係者や公的機関等を装い、標的組織にマルウェアを添付したメールを送信、または攻撃者サーバーに誘導してマルウェア感染させる攻撃。

手口例	特徴
文書ファイルの添付	• WordやExcelといった文書ファイルを添付 • 文書ファイルのマクロを悪用して攻撃者サーバーに誘導
圧縮ファイルの添付	• メールサーバー等での検知を逃れるために、マルウェアをパスワード付きZipに圧縮 • パスワード付きZipはビジネスメールで多用されており、騙されやすい • 文書ファイルをパスワード付きZipにして添付される例もあり
URLからの誘導	• メール本文のURLから攻撃者サーバーに誘導 • HTML表示で、実際のリンク先と異なるURLが表示される場合もあり

10

「**標的型メール攻撃**」とは、ソーシャルエンジニアリング等で調べた情報を基に、関係者や公的機関等を装い、標的組織にマルウェアを添付したメールを送信、または攻撃者サーバーに誘導してマルウェア感染させる攻撃です。

近年、標的型メール攻撃でよく利用される手口は、「**文書ファイルの添付**」、「**圧縮ファイルの添付**」、「**URLからの誘導**」等です。

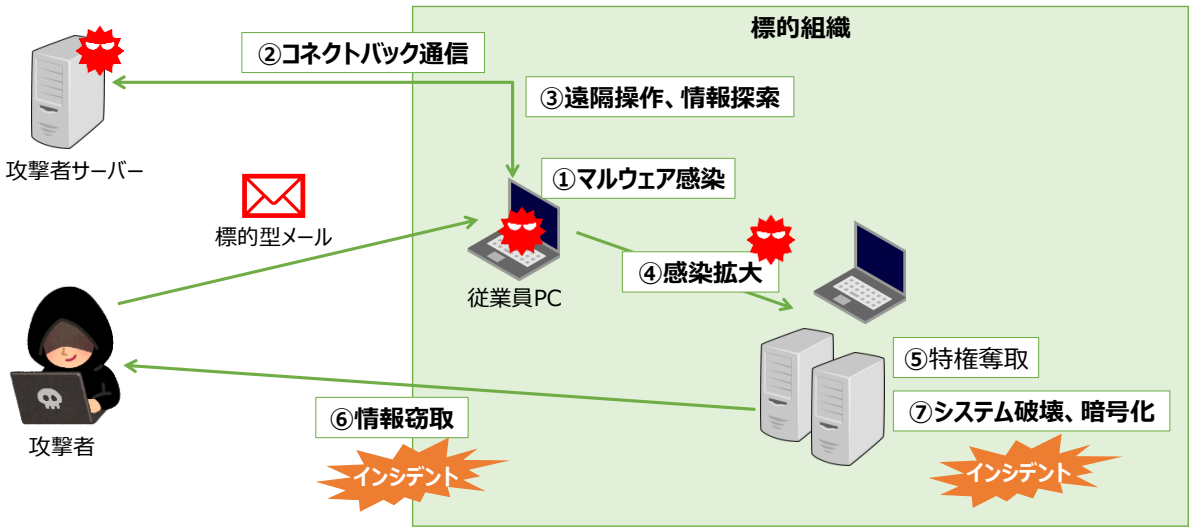
攻撃者は、メール受信者に疑われないように、巧妙な仕掛けを行います。特に、問い合わせ等を装い、複数回メールをやり取りして信用させた後にマルウェアを送り込む「やりとり型」は、さらに判別が難しくなっています。

用語解説

ソーシャルエンジニアリング
人間の心理や行動、組織的な体制等の隙、ミス、漏れ等を突いた攻撃。
代表的な手口に、「ショルダーハッキング」（肩口からアカウントやパスワード等の入力を覗き見る手口）、トラッシング（廃棄業者を装ってゴミ箱をあさったり、廃棄物から情報を盗んだりする手口）等がある。

マルウェア
不正かつ有害な動作を行うことを目的として、悪意を持って作成されたソフトウェアやコードのこと。
特徴によって、「ウイルス」「ワーム」「トロイの木馬」「ボット」等に分類される場合もある。

2.2 マルウェア感染による被害例



11

標的型メール攻撃により従業員PC等が**マルウェアに感染**すると、従業員PCを足掛かりに**攻撃者に組織内へ侵入**されてしまいます。マルウェア感染により攻撃者に侵入される例を紹介します。

① 標的型メール攻撃をきっかけに、従業員PCが**マルウェアに感染**。

② マルウェア（RAT等）によって、従業員PCから攻撃者サーバーへ**コネクトバック通信**が行われる。

③ 攻撃者サーバーから従業員PCが**遠隔操作**され、**情報探索**等が行われる。

④ 従業員PCから組織内のPCやサーバーに、**感染が拡大**する。

⑤ 攻撃者が、機密情報等にアクセスするために、**管理者アカウント**等の**特権を奪取**する。

⑥ **機密情報を窃取**する。

⑦ システムが**破壊**されたり、**身代金要求のために暗号化**されたりする。
（システム暗号化については、「3. ランサムウェアによる攻撃」で詳しく解説します。）

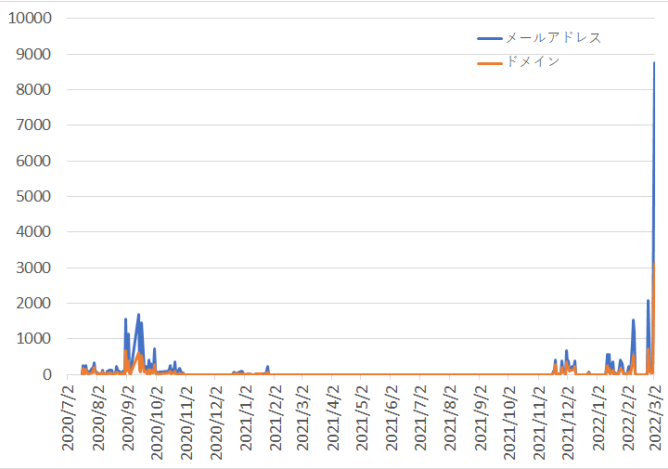
用語解説

RAT（ラット）
Remote Access Toolの略。インターネット上の攻撃者サーバとコネクトバック通信を行い、遠隔操作を可能とするプログラム。

コネクトバック通信
マルウェアに感染したPCが、攻撃者サーバに接続する通信。組織内のPC側から通信することで、FWをすり抜ける。

2.3 Emotetへの感染を狙う標的型メール攻撃

Emotetに感染し、メール送信に悪用される可能性のある「.jpメールアドレス数」の新規観測の推移



【出典】JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」
（https://www.jpcert.or.jp/at/2022/at220006.html）

Emotetの主な感染経路

メールに添付された悪質な「**パスワード付きZIPファイル**」「**マクロが埋め込まれたExcelやWordファイル**」、メール文中の「**不正なリンク**」等。

Emotetに感染すると

メールアドレスやパスワード、電話帳等の情報を窃取されたり、**さらに他の悪質なマルウェアに感染**させられたりする。

感染の拡大

攻撃者は、窃取した**メール情報を悪用**してなりすましメールを送る等、さらにEmotetの感染を拡大させる。

12

Emotetへの感染を狙う標的型メール攻撃は、2020年頃（令和2年頃）に猛威を振るいましたが、国際的な作戦が実行され、2021年1月（令和3年1月）に欧州刑事警察機構が「テイクダウン（攻撃者サーバーの停止）に成功した」と発表していました。
しかし、**2021年末頃**（令和3年末頃）から、**急激な感染再拡大**が確認されており、注意が必要です。

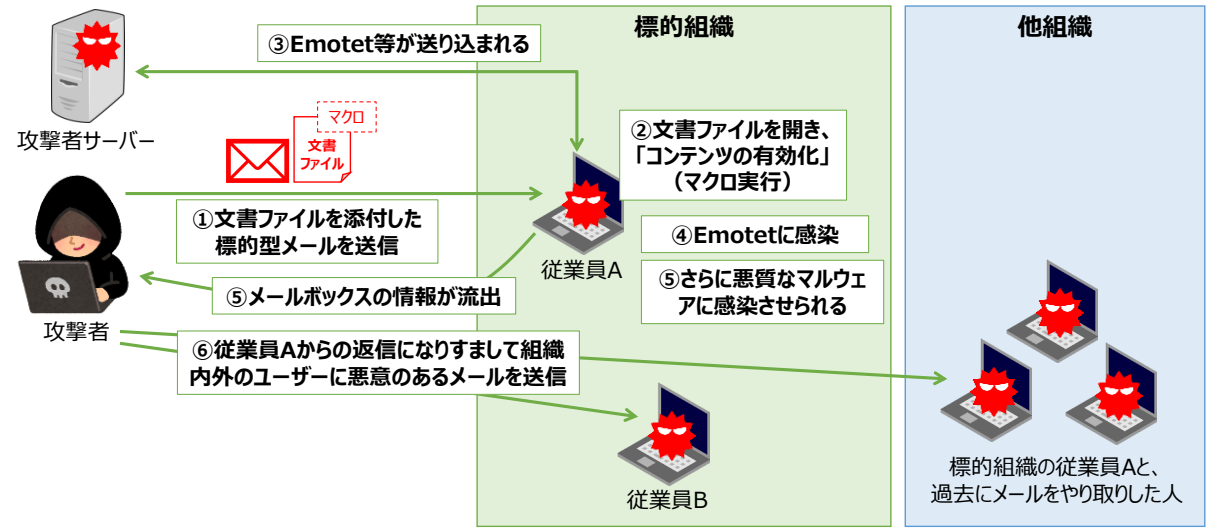
Emotetは、メールに添付された悪質な「**パスワード付きZIPファイル**」、「**マクロが埋め込まれたExcelやWordファイル**」、メール文中の「**不正なリンク**」等から感染するマルウェアです。

Emotetに感染すると、**メールアドレスやパスワード**、**電話帳等の情報を窃取**されたり、**さらに他の悪質なマルウェアに感染**させられたりします。
感染有無の確認には、JPCERT/CCが提供するツール「**EmoCheck**」が有効です。

攻撃者は、Emotetに感染したPC等から窃取したメール情報を悪用して、過去にメール送受信履歴のある人になりすましメールを送る等、さらにEmotetの感染を拡大させます。Emotetに感染してしまうと、自組織だけでなく、取引先等の関係者にも影響を及ぼす可能性があります。

2.3 Emotetへの感染を狙う標的型メール攻撃

正規メールへの返信を装う攻撃



多くの組織で被害が報告されている「**正規メールへの返信を装う攻撃**」について、事例を紹介します。

① 攻撃者は、関係者になりすまして、標的組織の従業員Aに「**文書ファイルを添付した標的型メール**」を送信。
この文書ファイルには、Emotetへの感染を誘導するための**マクロ**が仕込まれている。

② 標的組織の従業員Aは、受信した文書ファイルを開き、特に疑いを持つことなく「コンテンツの有効化」をクリック。
これによりマクロが実行され、攻撃者サーバーと通信を開始。
※マクロ事態は無害なものであり、ウイルススキャン等で文書ファイルに異常は見つからない。

③ 攻撃者サーバーからEmotet等が送り込まれる。

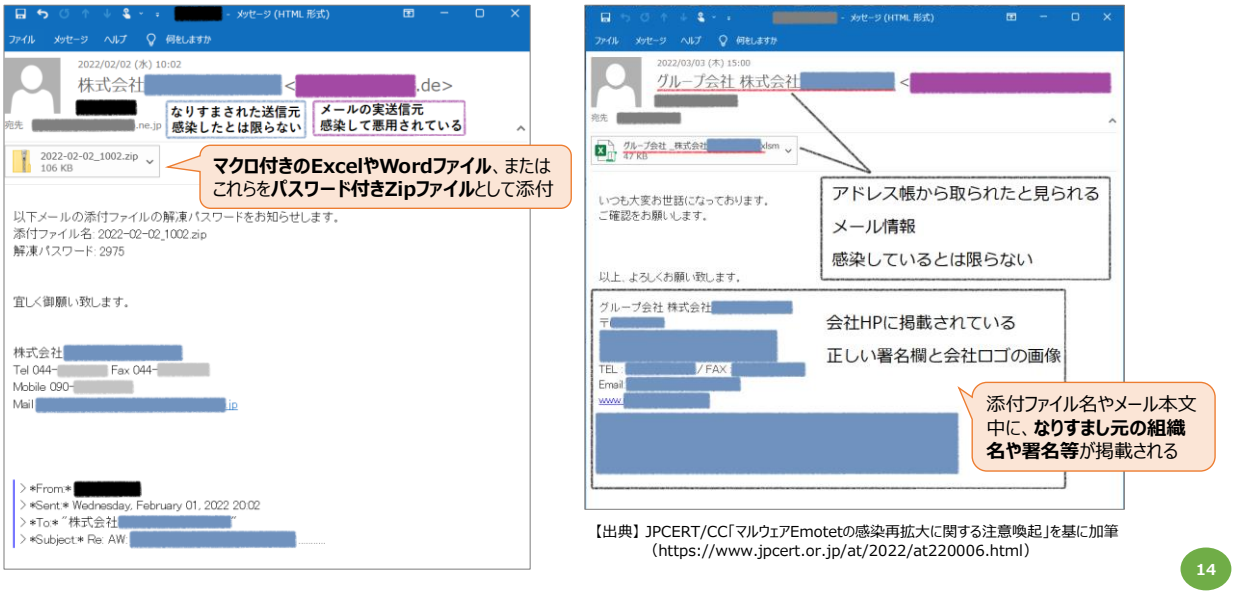
④ 従業員AのPCがEmotetに感染。

⑤ Emotetにより、メールボックスの情報（連絡先、過去のメール等）が攻撃者に流出。
また、Emotetによって「さらに悪質なマルウェア」に感染させられる。

⑥ 攻撃者は、従業員Aからの返信になりすまし、組織内外のユーザーに悪意のあるメールを送信し、感染を拡大。

2.3 Emotetへの感染を狙う標的型メール攻撃

Emotetの特徴/動向（JPCERT/CC公開）



【出典】JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」を基に加筆
（https://www.jpcert.or.jp/at/2022/at220006.html）

14

JPCERT/CCの観測によると、令和3年11月後半より増加しているEmotetには、次のような特徴があります。

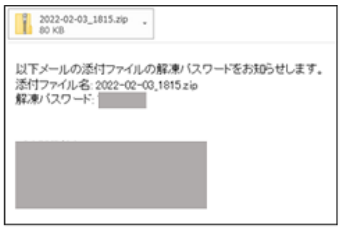
- 主に**マクロ付きのExcelやWordファイル**、またはこれらを**パスワード付きZipファイル**としてメールに添付
- メール本文に添付ファイルの開封を促す記載、ExcelやWordファイルにはマクロ実行を促す記載あり
- メールの添付ファイル名やメール本文中に、**なりすまし元の組織名や署名等**が掲載
- ファイル開封後に**マクロを有効化**することで、**Emotetの感染**に繋がる
- その他にも、メール本文中のリンクをクリックすることで悪性なExcelやWordファイルがダウンロードされたり、アプリケーションのインストールを装ってEmotet感染を狙うケースもあり

また、JPCERT/CCの観測によると、Emotetの感染によってメールが送信されるケースは、感染者とその関係者を巻き込む形で複数のパターンに分かれます。

- **自組織がEmotetに感染し、なりすましメールが配信される**
  Emotet感染により窃取された情報（メール情報やアドレス帳等）が、なりすましメールに悪用される。
- **取引先がEmotetに感染し、なりすましメールが配信される**
  従業員が過去にメールをやり取りした取引先のPCがEmotetに感染、そのPCから窃取された情報に含まれていた当該従業員の情報が、なりすましメールに悪用される。
  （なりすまされている従業員等のPCがEmotetに感染しているとは限らない。）

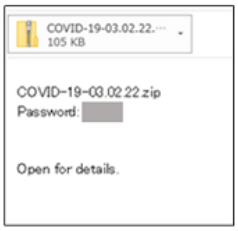
2.3 Emotetへの感染を狙う標的型メール攻撃

Emotetへの感染を狙うメール内容例（IPA公開）

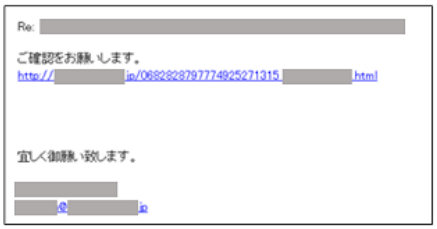


本文が日本語で書かれ、
パスワード付きZIPファイルが添付された攻撃メール

Excel文書ファイルが添付された攻撃メール



本文が英語で書かれ、パスワード付き
ZIPファイルが添付された攻撃メール



不正なURLリンクを含む攻撃メール

【出典】IPA「「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて」
（https://www.ipa.go.jp/security/announce/20191202.html）

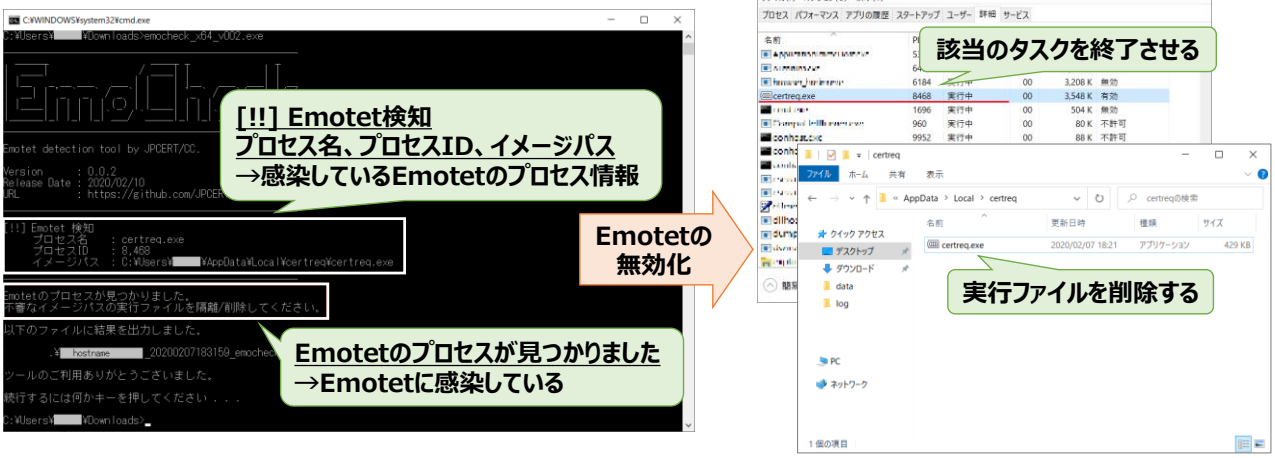
15

令和3年11月～令和4年2月にIPAで確認された、Emotetへの感染を狙うメール内容の一例です。
IPAの調査によると、これら以外にも様々なパターンのメールが存在し、いずれも「**添付ファイルの開封**」や「**URLリンクのクリック**」を誘導する内容となっています。

2.3 Emotetへの感染を狙う標的型メール攻撃

Emotetの感染有無確認・無効化（JPCERT/CC公開）

EmoCheckの実行



【出典】JPCERT/CC「マルウエアEmotetへの対応FAQ」を基に加筆・修正
（https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）

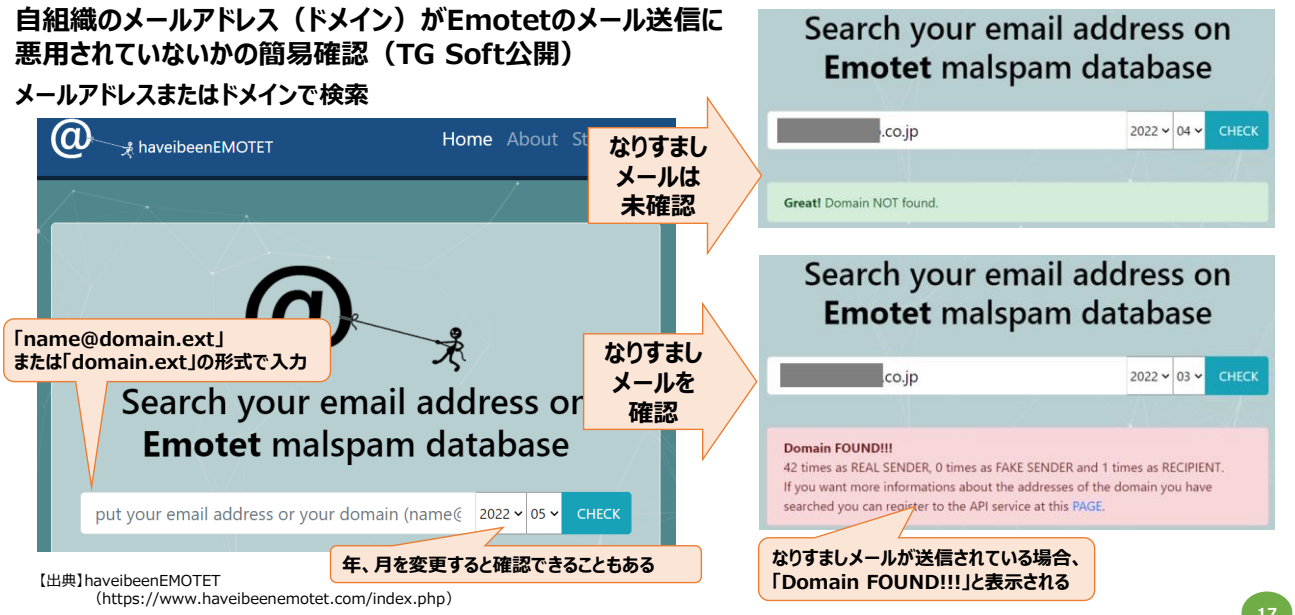
16

Emotetの感染が疑われる場合、EmoCheckを実行することで感染有無を確認できます。
EmoCheckを実行して、「Emotetのプロセスが見つかりました」と表示された場合、Emotetに感染しています。

Emotetを無効化するためには、「タスクマネージャーから**該当タスクを終了させる**」とともに、「エクスプローラーから**実行ファイルを削除**」します。
無効化後、再度EmoCheckを実行し、Emotetが検知されないことを確認します。

＜EmoCheckのダウンロード＞
https://github.com/JPCERTCC/EmoCheck/releases

2.3 Emotetへの感染を狙う標的型メール攻撃



【出典】haveibeenEMOTET
（https://www.haveibeenemotet.com/index.php）

自組織のメールアドレス（ドメイン）がEmotetのメール送信に悪用されていないか「haveibeenEMOTET」というWebサイトで簡易的に確認できます。本Webサイトは、イタリアのセキュリティ企業「TG Soft」社が公開しており、無償で利用できます。自組織になりすましたメールが送信されている場合、「Domain Found!!!」というメッセージが表示されます。メッセージの詳細から、次の内容を確認できます。

【REAL SENDER】（Emotetが感染して自組織の実際のメールアドレスが悪用されている可能性がある）
端末がEmotetに感染し、メールアドレスやパスワードが盗まれ、自組織のメールアドレス（ドメイン）がEmotetのメール送信に悪用されている可能性があります。メールのパスワード変更、EmoCheckなどを用いたマルウェアのスキャンの実施を推奨します。また、組織から社外に対して注意喚起を行うなどの検討を推奨します。

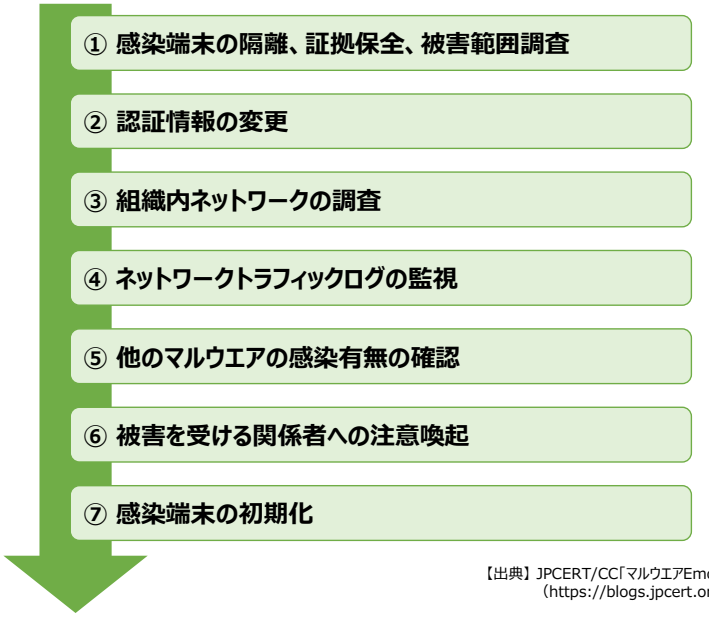
【FAKE SENDER】（自組織になりすましたメールが送信されている可能性がある）
自組織とは異なるメールアドレス（ドメイン）から自組織になりすましたEmotetのメールが送信されている可能性があります。自組織の端末がEmotetに感染、または自組織とメールのやりとりがある組織はEmotetに感染して、受信/送信メールの内容や連絡が盗まれた可能性があります。自組織の端末がEmotetに感染している可能性があるため、メールのパスワード変更、EmoCheckなどを用いたマルウェアのスキャンの実施を推奨します。
また、組織から社外に対して注意喚起を行うなどの検討を推奨します。

【RECIPIENT】（なりすましたメールの受信有無）
メールアドレス/ドメインがEmotetの不審なメールを受信している可能性がある。
既知の連絡先から受信したメールにも最大限の注意を払う必要がある。

なお、本サイトは簡易的な確認のため、自組織になりすましたメールが送信されていることを「**必ず確認できるものではない**」ことにご注意ください。

＜haveibeenEMOTET＞
https://www.haveibeenemotet.com/index.php

2.4 マルウェア感染時の対応



【出典】JPCERT/CC「マルウエアEmotetへの対応FAQ」を基に加筆・修正
（https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）

18

Emotet等のマルウェアに感染した場合、被害拡大を防ぎ、影響を最小限に留めるために、次のような対応を行うことが求められます。どのようなツールを使い、どのような手順で対応するか、あらかじめ想定しておくことが重要です。

① **感染端末の隔離、証拠保全、被害範囲調査**
有線・無線ネットワークを切断して感染端末を隔離し、感染端末のメモリ・ハードディスク情報等を保全します。（隔離前に保全した方が良い情報もあります。）
保全した情報等から、感染端末にどのような情報が保存されていたのか確認し、漏えいした可能性のある情報を特定します。

② **認証情報の変更**
メールアカウント、Webブラウザに保存していた認証情報等を変更し、悪用されることを防ぎます。

③ **組織内ネットワークの調査**
組織内の他の端末等に感染が広がっていないか確認します。

④ **ネットワークトラフィックログの監視**
通信状況を監視し、感染端末を隔離できているか、他に感染している端末がないか確認します。

⑤ **他のマルウエアの感染有無の確認**
特にEmotetは、他のマルウェアに感染させる機能があるため、他のマルウェアに感染していないかも併せて確認します。

⑥ **被害を受ける関係者への注意喚起**
漏えいした情報を悪用され、被害を受ける可能性のある関係者へ注意喚起します。

⑦ **感染端末の初期化**
可能な限り、感染端末を初期化して、マルウェアを完全に除去します。

2.5 標的型メールからのマルウェア感染を防ぐ対策

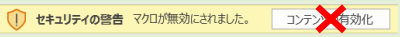
従業員等が実施できる対策の例

日頃から実施しておく対策

- ☐ OSやアプリケーション、セキュリティソフトを常に最新の状態に保つ
- ☐ Officeのマクロ自動実行を無効化する

メール閲覧時等に実施する対策

- ☐ 身に覚えのないメールの添付ファイルは開かない
- ☐ メール本文中のURLリンクはクリックしない
- ☐ 返信メールに見えても、不自然な点があれば添付ファイルは開かない
- ☐ 信頼できないメールの添付ファイルで、マクロやセキュリティに関する警告が表示されたら、「コンテンツの有効化」「マクロを有効にする」ボタンはクリックしない



- ☐ メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する
- ☐ 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する

システム管理部門等が実施する対策の例

- ☐ 従業員等に注意喚起する
- ☐ 従業員等の意識向上のために、標的型メール訓練の実施を検討する
- ☐ メールセキュリティ製品を導入し、マルウエア付きメールを検知できるようにする
- ☐ メールの監査ログを有効化する
- ☐ マルウェア感染時の対応手順を検証しておく

【出典】JPCERT/CC「マルウエア Emotet の感染に関する注意喚起」
「マルウェアEmotetの感染再拡大に関する注意喚起」を基に加筆・修正
（https://www.jpcert.or.jp/at/2019/at190044.html、
https://www.jpcert.or.jp/at/2022/at220006.html）

19

標的型メールからのマルウェア感染を防ぐための対策を紹介します。

従業員等が実施できる対策の例

日頃からOSやアプリケーション、セキュリティソフト、さらに悪用されることの多いOffice製品等をセキュアな状態に保つことが重要です。
また、メール閲覧時等にも、マルウェア感染しないための心掛けが重要です。
具体的な対策例は、上図のとおりです。

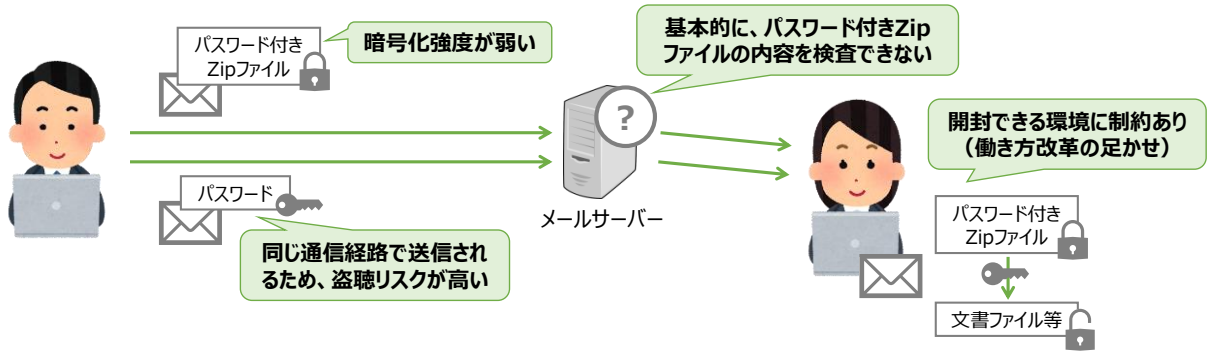
システム管理部門等が実施する対策の例

「従業員等が実施できる対策」等を分かりやすく整理し、日頃から従業員等に注意喚起することが重要です。
また、各種セキュリティ製品・サービス等の導入も有効です。
さらに、万が一マルウェアに感染してしまった時を想定し、対応手順をまとめて検証しておくことも有効です。
具体的な対策例は、上図のとおりです。

2.5 標的型メールからのマルウェア感染を防ぐ対策

＜参考＞ 脱PPAPの拡がり

Pパスワード付きZipファイルを送ります **P**パスワードを送ります **A**暗号化 **P**プロトコル（手順）



様々な弱点があり、Emotetで悪用される場合も多いため、受信をブロックする企業が増えている

20

標的型メールからのマルウェア感染を防ぐために、「**脱PPAP**」が拡がっています。

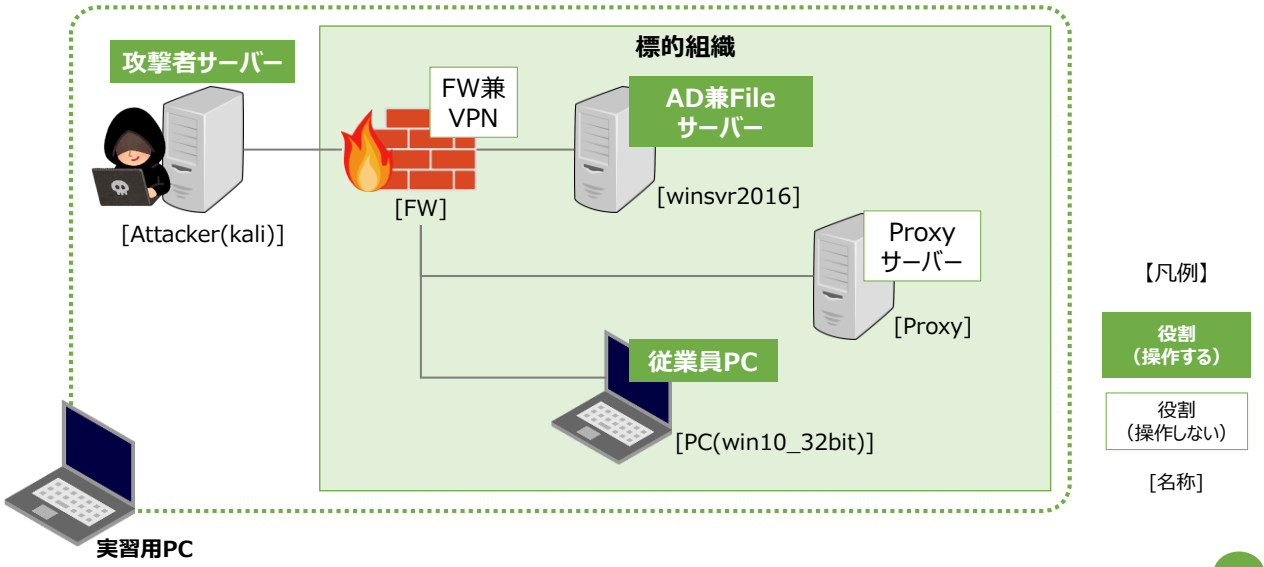
PPAPとは、P（パスワード付きZipファイルを送ります）、P（パスワードを送ります）、A（暗号化）、P（プロトコル）を表す俗語であり、ビジネスメールでファイルを送受信する際に、頻繁に利用される形式です。

PPAPには様々な弱点があり、令和2年11月に内閣府・内閣官房が「脱PPAP」を宣言したことをきっかけに、多くの企業で「パスワード付きZipファイル」の受信をブロックする動きが拡がっています。

特に、ビジネスメールで頻繁に利用されており、受信者が不審感を持ちづらいことに付け込み、Emotetを送り付ける際に悪用されるケースも多いため、近年急速に脱PPAPが拡がっています。

[実習]Emotet感染・対応の体験

実習環境の構成



21

実習用PC上（仮想環境）で、5台のサーバーやPCが、それぞれ独立して動作しています。

「**Emotet感染・対応の体験**」では、「**攻撃者サーバー**」と「**従業員PC**」、
「**ランサムウェア感染・対応の体験**」では、「**攻撃者サーバー**」と「**AD兼Fileサーバー**」
をそれぞれ操作しながら、実習を進めます。

用語解説

FW（ファイアーウォール）
IPアドレス、ポート番号・プロトコル等をもとに通信の許可（通過）、拒否（遮断）を行うセキュリティ対策製品。専用のハードウェアだけでなく、OSの機能、またソフトウェアとして実装する場合もある。

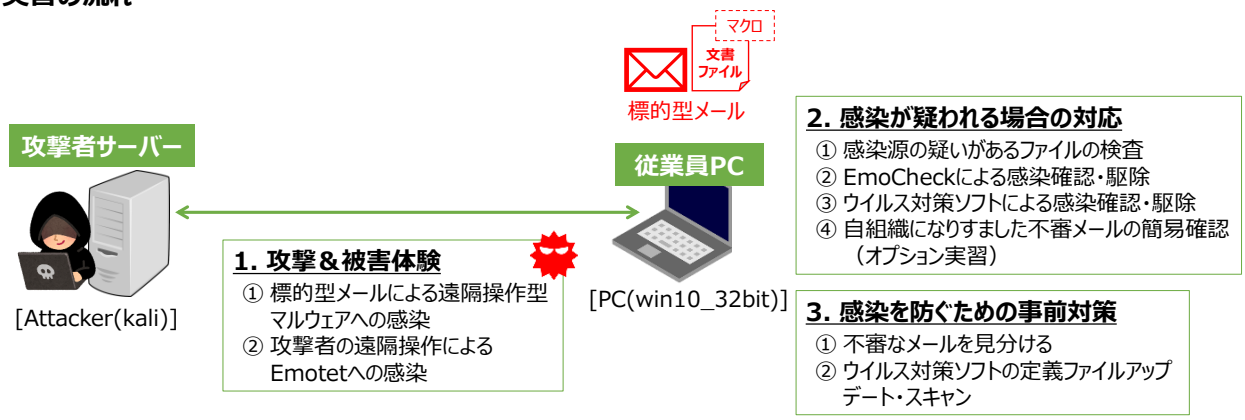
VPN（ブイピーエヌ）
Virtual Private Networkの略。認証や暗号化により、公衆ネットワーク上で仮想的な専用ネットワークを実現する技術。

AD（エーディー）
Active Directoryの略。ユーザーやコンピューター等のリソースを一元管理するシステム。

Proxy（プロキシ）
組織内利用者のインターネットアクセスを代理で処理するサーバ。外部ネットワークからはProxyサーバと通信しているようにしか見えない。

[実習]Emotet感染・対応の体験

実習の流れ



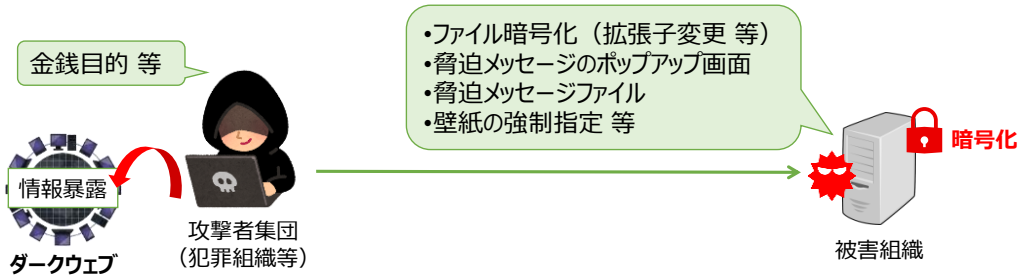
22

実習は、上記の流れで実施します。
「**実習手順書**」を参照しながら、講師の指示に従って実習を進めます。

3. ランサムウェアによる攻撃

3.1 ランサムウェアとは

ランサムウェア	感染端末をロックしたり、ファイルを暗号化したりすることによって使用不能にした後、元に戻すことと引き換えに「身代金」を要求するマルウェアのこと。



「RaaS」の広がり による攻撃増加

RaaS（Ransomware as a Service）とは、
ランサムウェアをサービスとして取引するビジネス

「二重の脅迫」を 受けるケースも増加

暗号化による脅迫に加え、組織内に**侵入**して
窃取した情報の暴露をネタに脅迫される

24

ランサムウェアとは、感染端末をロックしたり、ファイルを暗号化したりすることによって使用不能にした後、元に戻すことと引き換えに「身代金」を要求するマルウェアのことです。
ランサムウェアの「ランサム（ransom）」は「身代金」を意味し、ドルでの支払いを要求するものや、ビットコインでの支払いを要求するもの等、多くの種類があります。

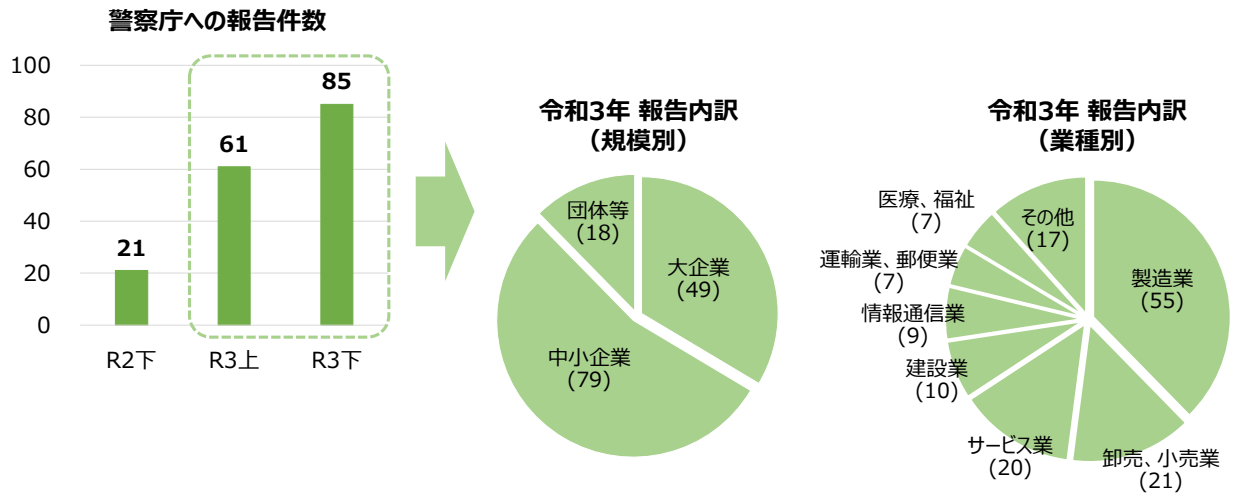
ランサムウェアの被害が拡大している要因の一つに、「**RaaS**」の広がりがあります。
RaaS（Ransomware as a Service）は、ランサムウェアをサービスとして取引するビジネスであり、料金を支払えば誰でもランサムウェアによる攻撃を実現できてしまいます。
RaaSで提供される機能として、ランサムウェアの作成、攻撃インフラ基盤等があります。ランサムウェアの攻撃によって得た身代金を、成果報酬として攻撃に協力した者に支払うような動きも確認されています。

また、近年では、暗号化による脅迫に加え、組織内に侵入して窃取した情報の暴露をネタに脅迫される「**二重の脅迫**」（二重恐喝）も増えています。
攻撃者は、**ダークウェブ**上のリークサイト（暴露サイト）に被害組織の名前を掲載したり、被害組織から窃取した機密情報の一部を暴露したりして、攻撃が事実であるとアピールし、身代金支払いの交渉を成功させようとする場合があります。実際に、窃取された情報の一部が暴露され、その後、次々と情報を暴露された事例もあります。

用語解説

ダークウェブ
アクセスするために、特定の認証方式や、アプリケーションが必要なWebサイト。身元の特定が困難であり、違法薬物や、個人情報等の闇取引に利用されることが多い。

3.2 ランサムウェアの被害状況



【出典】警察庁「令和３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」
（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf）

25

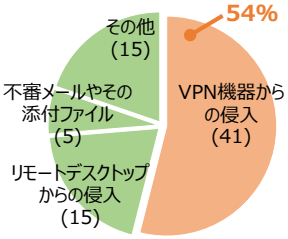
警察庁によると、ランサムウェアの報告件数は右肩上がりで増加しており、令和3年には合計146件の被害が報告されています。
令和3年の被害報告内訳を見ると、企業規模を問わず被害が発生しており、対象業種も製造業を筆頭に様々な業種に及んでいます。

次ページで、令和３年の被害報告の特徴を解説します。

3.2 ランサムウェアの被害状況

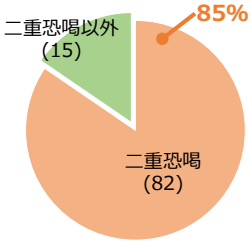
令和3年被害報告の特徴（警察庁発表より）

感染経路



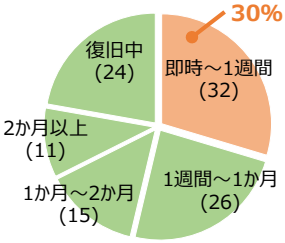
<有効回答 76件>

被害手口



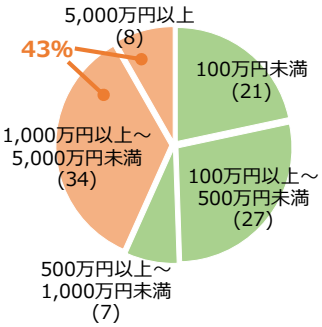
<手口を確認できた
被害 97件>

復旧に要した時間



<有効回答 108件>

調査・復旧費用の総額



<有効回答 97件>

【出典】警察庁「令和３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」
（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf）

26

警察庁に報告された令和3年のランサムウェア被害の特徴は、次のとおりです。

- **感染経路**
  「**VPN機器からの侵入**」が**54%**と最も多く、次いで「**リモートデスクトップからの侵入**」が多かった。
  テレワークに利用される機器等の脆弱性や、強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めている。

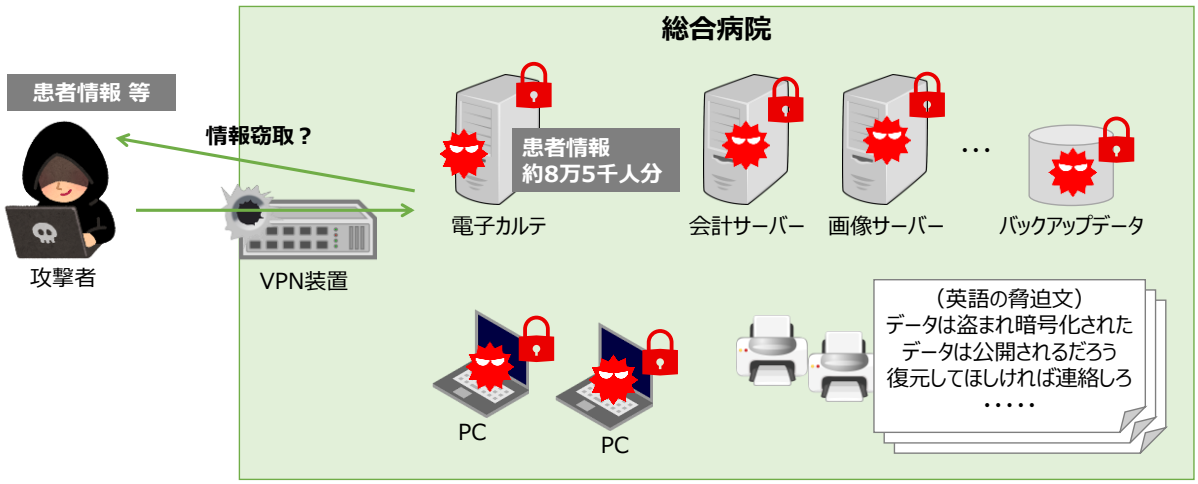
- **被害手口**
  手口を確認できた被害（97件）のうち、**85%**が「**二重恐喝**」を受けた。

- **復旧に要した時間**
  「**即時～1週間**」が**30%**と最も多かった。しかし、「**2か月以上**」要したケースもあった。

- **調査・復旧費用の総額**
  「**1,000万円以上**」が**合計43%**を占める。

3.2 ランサムウェアの被害状況

＜被害事例①＞総合病院



※本事例紹介は、ニュースサイト等で公開されている情報を独自に分析して作成したものです。

27

令和3年10月に総合病院で発生した、ランサムウェアの被害事例を紹介します。

【攻撃者の侵入経路等】
「脆弱性のある旧型のVPN装置」（リモート接続機器）から侵入されたと考えられています。
なお、攻撃は「LockBit 2.0」と呼ばれる攻撃者集団によるものであったと推測されています。

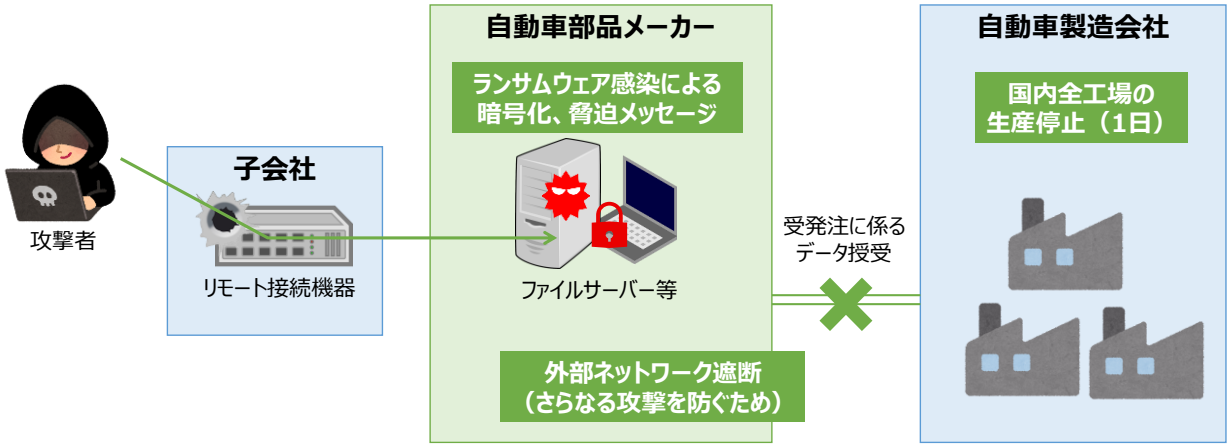
【検知状況】
10月31日深夜、数十台のプリンターが勝手に印刷を始め、用紙切れになるまで脅迫文が印刷され続けました。
さらに感染が拡大し、電子カルテをはじめとした医療システム、PC等がランサムウェアにより暗号化され、使用不能状態となりました。

【総合病院の対応等】
受付システムが使えないため人力で対応し、電子カルテも参照できないため、患者本人に確認しながら治療に当たったとされています。大きな混乱となり、外来患者の新規受け付けも一時的に停止されました。

バックアップシステムも暗号化され復旧目途が立たないとして、当初はシステムを新規構築しなおす予定であると公表されていました。しかし、専門業者の協力のもと、年末にはシステムの復旧に成功したと公表されています。

3.2 ランサムウェアの被害状況

＜被害事例②＞自動車部品メーカー



※本事例紹介は、被害組織の公式発表資料等を独自に分析して作成したものです。

28

令和4年3月に自動車部品メーカーで発生した、ランサムウェアの被害事例を紹介します。

【攻撃者の侵入経路等】
自動車部品メーカーの子会社が利用していた「リモート接続機器」に脆弱性があり、子会社を経由して不正アクセスを受け、サーバーやPCの一部データがランサムウェアにより暗号化されたと公表されています。

【検知状況】
自動車部品メーカーは、2月26日夜間に「ファイルサーバーの障害を検知」し、再起動後に「マルウェアへの感染」と「脅迫メッセージの存在」を確認したと公表しています。

【自動車部品メーカーの対応等】
2月27日未明には、さらなる攻撃を防ぐために、外部ネットワークを遮断しました。
取引先の自動車製造会社との「受発注に係るデータ授受」等について、部分的な復旧や代替手段を検討したものの困難であり、自動車製造会社が国内全工場の生産を停止する事態に陥りました。

ホームページやメール送受信など、順次安全を確認しながら復旧を進めているものの、令和4年4月時点で、まだすべての復旧に至っていないと発表されています。
また、令和4年4月時点で情報窃取の痕跡は確認されていないとするものの、「なりすましメールの注意喚起」等、さらなる被害拡大防止のための対応にも追われています。

3.3 ランサムウェアの対策例

目的	対策例	対策ポイント
感染を防ぐため	標的型メール攻撃を警戒する	詳細は、「2. 標的型メール攻撃」参照。
	脆弱性に対応する	外部から接続可能な装置（VPN装置等）、サーバ・端末のOSやソフトウェア等にはセキュリティパッチを適用し、脆弱性を放置しない。
	ウイルス対策ソフトを導入する	定義ファイルを最新に保つ。
	認証情報を適切に管理する	推測されにくいパスワードの設定を求める。また、可能であれば多要素認証を導入する。
感染時の被害を軽減するため	データのバックアップを取得しておく	バックアップも一緒に暗号化されないように、バックアップは業務ネットワークから切り離して保管する。 また、バックアップから復旧できるか確認しておく。
	アクセス権限を必要最小限とする	侵入されてもアクセスできる範囲が最小限となるように、アクセス権限は必要最小限とする。
	ネットワークを監視する	外部との不審な通信を検知した場合は、迅速に対応する。

【出典】警察庁サイバー犯罪対策プロジェクト「ランサムウェア被害防止対策」を基に加筆・修正
（https://www.npa.go.jp/cyber/ransom/index.html）

29

ランサムウェアの対策例を紹介します。

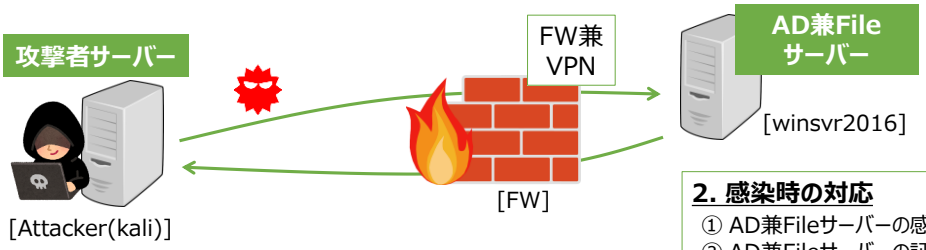
そもそも「**ランサムウェアの感染を防ぐため**」に、攻撃者の侵入を防ぐことが重要です。
攻撃者の侵入経路となりやすい「標的型メール攻撃を警戒する」「脆弱性に対応する」といった対策が有効です。
また、「ウイルス対策ソフトを導入」して感染を防ぐ、「認証情報を適切に管理」して攻撃者に突破されにくくするといった対策も有効です。

しかし、攻撃は巧妙化・増加しており、すべての攻撃を完全に防ぐことは困難です。
万が一、「**ランサムウェアに感染してしまった場合に被害を軽減するため**」に、「データのバックアップを取得しておく」、「アクセス権限を必要最小限とする」、「ネットワークを監視する」といった対策をとっておくことが有効です。

これらの対策は、ランサムウェアに限らず、マルウェア感染への対策となります。

[実習]ランサムウェア感染・対応の体験

実習の流れ



1. 攻撃＆被害体験
① VPNの脆弱性を突いたアカウント窃取
② 窃取したVPNアカウントを悪用したVPN接続
③ AD兼Fileサーバーからの機密情報窃取＆ランサムウェア感染

2. 感染時の対応
① AD兼Fileサーバーの感染確認＆ネットワーク切断
② AD兼Fileサーバーの証拠保全
③ 漏えいした可能性のあるファイルの調査
④ 感染したランサムウェアの特定＆ファイル復号
⑤ AD兼Fileサーバーの復旧（オプション実習）

3. 感染に備える事前対策
① バックアップ（オプション実習）

30

実習は、上記の流れで実施します。
「**実習手順書**」を参照しながら、講師の指示に従って実習を進めます。

[参考]ランサムウェアに関する情報

機関	サイト	内容例	URL
JPCERT/CC	ランサムウェア対策特設サイト	種類、対策、感染時の対処法等	https://www.jpcert.or.jp/magazine/security/nomore-ransom.html
	侵入型ランサムウェア攻撃を受けたら読むFAQ	対応ポイント、留意点	https://www.jpcert.or.jp/magazine/security/ransom-faq.html
IPA	ランサムウェア対策特設ページ	注意喚起、脅威と対策等	https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
警察庁	ランサムウェア被害防止対策	手口、防止策、軽減策、感染時の対応、再発防止策等	https://www.npa.go.jp/cyber/ransom/index.html
法執行機関、民間組織等	No More Ransom ポータルサイト	復号ツールの提供等	https://www.nomoreransom.org/ja/index.html
JC3	脅威情報（ランサムウェア対策について）	状況、予防策、感染時の対応等	https://www.jc3.or.jp/threats/topics/article-375.html

31

近年、ランサムウェアの被害が急増しており、様々な組織がランサムウェアに関する脅威や対策方法を発信しています。
平時から情報を収集し、自社でできる対策を確実に実施することが重要です。

4. その他の主な攻撃

4.1 情報セキュリティ10大脅威（IPA）

順位	組織における脅威	説明
1	ランサムウェアによる被害	• データを暗号化され、復旧と引き換えに金銭を要求される。 • 情報を窃取され、それを公開すると二重脅迫される場合も多い。
2	標的型攻撃による機密情報の窃取	• 標的型メール攻撃等によりマルウェアに感染させられ、組織内部に侵入される。 • 攻撃者は長期的に侵害範囲を広げ、組織の機密情報窃取やシステム破壊を行う。
3	サプライチェーンの弱点を悪用した攻撃	• セキュリティ対策が不十分なサプライチェーン組織が攻撃の足掛かりとして狙われる。 • 取引先や業務を委託している外部組織から情報が漏えいする。 • 標的組織の従業員等がよく閲覧する「サプライチェーン組織の**Webサイトが改ざん**」される場合もある。（水飲み場型攻撃）
4	テレワーク等のニューノーマルな働き方を狙った攻撃	• Web会議サービスやVPN装置を急ピッチで導入した企業も多く、これらの隙を突いた攻撃。 • Web会議の覗き見による情報漏えいや、テレワーク用PCのマルウェア感染等も多い。 • 不適切なアカウント管理により、**アカウント情報が漏えい**する場合も多い。
5	内部不正による情報漏えい	• 組織の従業員や元従業員等が、機密情報を漏えいさせる。 • 組織関係者による不正行為により、社会的信用の失墜、損害賠償による経済的損失等の影響が大きい。

【出典】IPA「情報セキュリティ10大脅威 2022」を基に加筆・修正
（https://www.ipa.go.jp/security/vuln/10threats2022.html）

33

IPA（独立行政法人情報処理推進機構）は、前年に発生したセキュリティインシデントや攻撃状況等から脅威を分析し、「情報セキュリティ10大脅威」として毎年公表しています。
令和4年に公表された「組織における脅威」（企業や政府機関等における脅威）は、上記のとおりです。

「ランサムウェアによる被害」と「標的型攻撃による機密情報の窃取」は、昨年同様に「1位」「2位」にランクインしており、引き続き警戒が必要です。
「ランサムウェア」の詳細は、「3. ランサムウェア攻撃」をご参照ください。
また、標的型攻撃のきっかけとなることが多い「標的型メール攻撃」の詳細は、「2. 標的型メール攻撃」をご参照ください。

4.1 情報セキュリティ10大脅威（IPA）

順位	組織における脅威	説明
6	脆弱性対策情報の公開に伴う悪用増加	• 脆弱性対策のために公開された情報が悪用される。 • 脆弱性情報の公開後、攻撃コードが流通して攻撃が本格化するまでの時間が短くなっている。 • 広く利用されている製品の脆弱性では、被害が大きくなる。 • 脆弱性を悪用し、次のような目的で**Webサイトが改ざん**される場合も多い。 「主義主張」、「Webサイトに接続したユーザーをマルウェアに感染させる」、「Webサイト上でユーザーが入力した情報を窃取する」
7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	• 脆弱性の修正プログラムや回避策が公開される前に、脆弱性を悪用して攻撃される。
8	**ビジネスメール詐欺**による金銭被害	• 取引先や経営者とのやり取りを装った巧妙なメール。 • 金銭を扱う担当者等がターゲットとなり、攻撃者が用意した口座に送金させられる。
9	予期せぬIT基盤の障害に伴う業務停止	• 利用中のデータセンターやクラウドのIT基盤等が停止し、事業継続に甚大な影響を与える。
10	不注意による情報漏えい等の被害	• 従業員等の不注意（メール誤送信、クラウド保存データの公開範囲設定ミス等）により、意図せず機密情報が漏えいする。

【出典】IPA「情報セキュリティ10大脅威 2022」を基に加筆・修正
（https://www.ipa.go.jp/security/vuln/10threats2022.html）

34

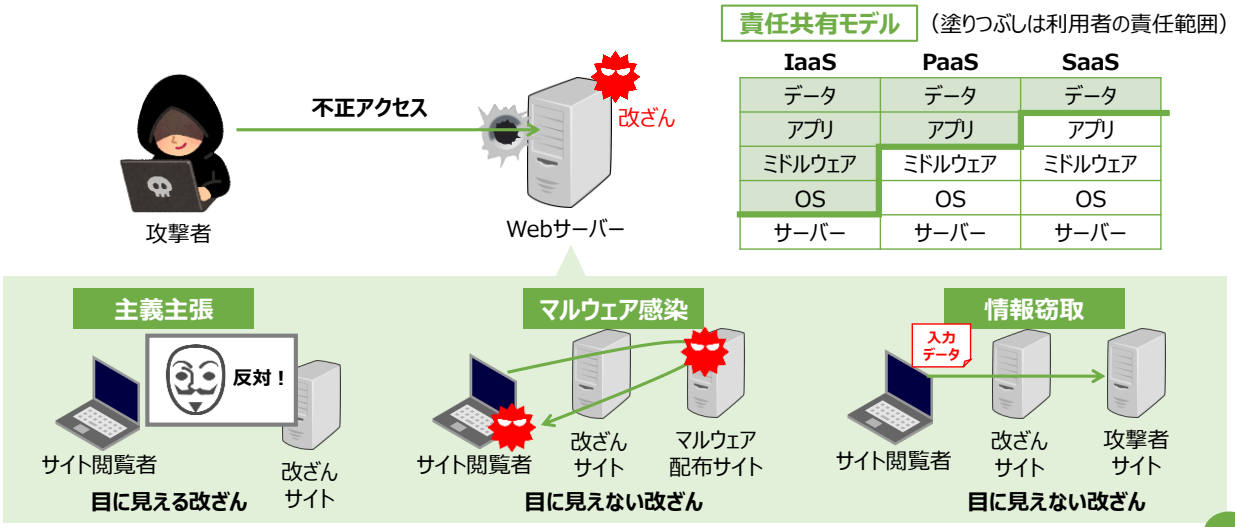
「6位 脆弱性対策情報の公開に伴う悪用増加」は、前年の10位からランクアップしています。
令和3年12月に発生した「Apache Log4j」（Javaのログ出力ライブラリ）の脆弱性は、世界中で多くの組織が対応を迫られました。

「7位 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」は、令和4年に新しくラインクインしました。
VPN装置の脆弱性や、WindowsOSの印刷スプーラーの脆弱性等が悪用され、ゼロデイ攻撃が行われました。

次ページ以降で、「Webサイトの改ざん」、「アカウント情報の漏えい」、「ビジネスメール詐欺」についてポイントを解説します。

4.2 Webサイトの改ざん

Webサイト改ざん　悪意のある第三者によって、Webサイト内のシステムやコンテンツが意図しない状態に変更されてしまうこと。



Webサイトを管理するサーバーのOSやアプリ等に脆弱性があると、攻撃者から脆弱性を悪用した不正アクセスを受け、Webサイトが改ざんされる恐れがあります。Webサイトの改ざんには、目的によって主に次の3つがあります。

- **主義主張**
  個人的な主義主張を訴えるために、Webサイトの見た目や内容を書き換える。
- **マルウェア感染**
  WebサイトにアクセスしたPCをマルウェア感染させるために、Webサイトにプログラム等を埋め込む。
  （改ざんに気付かせないために、Webサイトの見た目や内容は変えないことが多い。）
- **情報窃取**
  Webサイトに入力したID/パスワード等の情報を窃取するために、プログラム等を埋め込む。
  （改ざんに気付かせないために、Webサイトの見た目や内容は変えないことが多い。）

Webサイトが改ざんされると、多くのサイト閲覧者に影響を及ぼすこととなります。
Webサイトの改ざんを防ぐための定期的な点検を推奨します。

特に近年、Webサイトを「**オンプレミス環境**」だけでなく、「**クラウド環境**」に構築するケースが増えています。
クラウド環境は、サービス形態によって利用者の責任範囲が異なるため、自組織の責任範囲を意識して対策を実施することが重要です。（上記「責任共有モデル」を参照）
主なクラウドサービスの形態には、「**IaaS**」（サーバーやネットワークの基盤のみが提供される）、「**PaaS**」（基盤に加えてアプリケーションを実行する環境も提供される）、「**SaaS**」（メール等、特定の利用用途に応じたサービスが提供される）があります。

用語解説

オンプレミス環境
組織の施設内に設置したサーバー等の環境。サーバーやネットワークの基盤から、格納するデータまで、すべてが自組織の責任範囲となる。

4.2 Webサイトの改ざん

改ざんを防ぐ、早期発見するための対策例

目的	対策例	対策ポイント
製品の脆弱性を狙ったサイバー攻撃の回避・低減	定期的に、利用製品 (プラグインも含む) のバージョンが最新であることを確認する	Webサイトで利用している製品を整理し、「**数週間～1ヶ月**」に**1回**程度、製品に脆弱性がないか確認する。（脆弱性対策情報データベース：https://jvndb.jvn.jp/）
Webアプリケーションに脆弱性や設定不備が存在しないか確認	定期的に、Webアプリケーションのセキュリティ診断を実施する	「**1年**」に**1回**程度、さらに「**機能追加等の変更が行われた時**」に、Webアプリケーションに脆弱性がないか確認する。※「OWASP ZAP」等を活用して自組織で診断することも可能。（OWASP ZAP：https://www.zaproxy.org/）
ファイルが改ざんされていないか、不正に作成されていないか等を確認	定期的に、Webサーバー上のファイルを確認する	「**1週間**」に**1回**程度、ファイルのリスト（ファイル名、サイズ、更新日時、ハッシュ値）やバックアップの取得と比較する。
Webサイト運用に関する契約内容を確認し、必要な運用保守・対策実施に抜け漏れがないことを確認	定期的に、委託内容や委託作業を確認する	「**1年**」に**1回**程度（契約更新時等）、さらに「**機能追加等の変更が行われた時**」に、委託内容、委託作業について確認する。

【出典】JPCERT/CC「Webサイトへのサイバー攻撃に備えて」を基に加筆・修正
（https://www.jpcert.or.jp/newsflash/2018071801.html）

36

Webサイトの改ざんの対策例は、上記の通りです。
製品やWebアプリケーションの脆弱性をなくし、攻撃者に不正アクセスする隙を与えないことが重要です。

＜弱性対策情報データベースによる脆弱性確認の例＞

利用している製品を入力して検索します。

深刻度(CVSSv3)
緊急(9.0～10.0)
重要(7.0～8.9)
警告(4.0～6.9)
注意(0.1～3.9)

深刻度(CVSSv2)
危険(7.0～10.0)
警告(4.0～6.9)
注意(0.0～3.9)

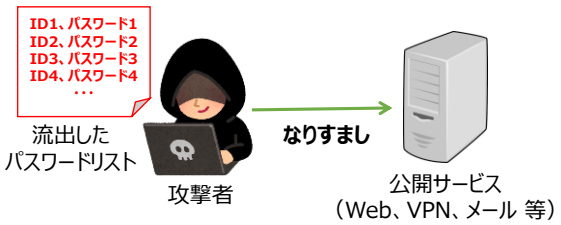
入力した製品に関連する脆弱性情報が表示されます。

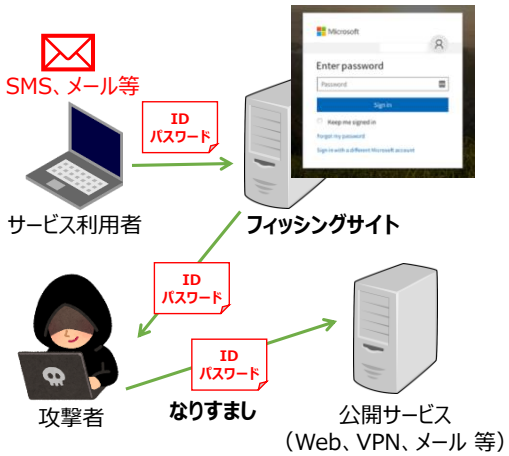
ID	タイトル	CVSSv3	CVSSv2	公表日	最終更新日
JVNDB-2022-000026 (JVN#31606885)	WordPress 用プラグイン「MicroPayments - Paid Author Subscriptions, Content, Downloads, Membership」におけるクロスサイトリクエストフォージェリの脆弱性	4.3	2.6	2022/04/15	2022/04/15
JVNDB-2022-000023 (JVN#42543427)	WordPress 用プラグイン Advanced Custom Fields における認証欠如の脆弱性	6.5	4.0	2022/03/30	2022/03/30
JVNDB-2022-000002 (JVN#72788165)	WordPress 用プラグイン Quiz And Survey Master における複数の脆弱性	5.4	4.0	2022/01/12	2022/01/12
JVNDB-2021-009477	WordPress 用 Youtube Feeder プラグインにおけるクロスサイトリクエストフォージェリの脆弱性	8.8	6.8	2021/07/30	2022/04/28
	WordPress 用 Download Manager プラグインにおける危険なタイプのファイル				

【出典】弱性対策情報データベース(https://jvndb.jvn.jp/)

4.3 アカウント情報の漏えい

パスワードリスト攻撃	不正に入手したIDとパスワードのリストを用いて、正規の認証方法によって不正アクセスを試みること。
フィッシング	正規サイトに似せた偽サイトに誘導した上で、ID・パスワード等を入力させて窃取し、正規の認証方法によって不正アクセスを試みること。





37

インターネットバンキング、インターネットショッピング、Webメール、テレワーク時のVPN等 、様々なサービスでアカウント情報が管理されています。
アカウント情報が漏えいすると、意図せず銀行口座から送金されたり、勝手に買い物をされたり、重要なメールを盗み取られたりと、甚大な被害が生じます。

攻撃者はアカウント情報を入手し、公開サービスに不正ログインしようと試みます。
代表的な攻撃手法として、「パスワードリスト攻撃」や「フィッシング」があります。

- **パスワードリスト攻撃**
  攻撃者は、流出したアカウントのIDとパスワードの一覧（パスワードリスト）を、何らかの手段（ダークウェブ上に公開されている場合もある）で入手する。
  IDとパスワードは、複数サービスで使い回されていることが多いため、入手したパスワードリストでログインできるサービスがないか試行する。
  （IDとパスワードを使い回していると、簡単に不正にログインされてしまう。）
- **フィッシング**
  SMS（ショートメッセージ）やメールで、フィッシングサイト（偽サイト）に誘導する。
  サービス利用者が入力したアカウント情報を窃取し、本人になりすまして公開サービスに不正ログインする。

4.3 アカウント情報の漏えい

被害を受けないための対策例

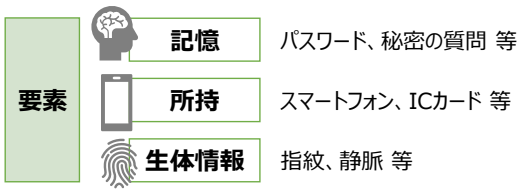
目的	対策例	対策ポイント
パスワードの強化	パスワードをできるだけ長くする	• 文字列の長さは、12文字以上が推奨
	パスワードを複雑にする	• 様々な文字種（大小英字、数字、記号）を組み合わせる • 推測されやすい単語、生年月日等は避ける • 単純な文字の並び（数字、キーボードの配列順等）、ログインIDは避ける
	パスワードを使いまわさない	• 他のサービスで使用しているパスワードは使用しない
認証方式の強化	多要素認証を利用する	• ワンタイムパスワードや生体認証が提供されている場合は利用する
不審なログインの早期発見	ログイン履歴を確認する	• 通常とは異なるログインを通知する機能（ログイン履歴やログインアラート等）が提供されている場合は利用する

【出典】JPCERT/CC「STOP!パスワード使い回し」を基に加筆・修正
（https://www.jpcert.or.jp/pr/stop-password.html）

多要素認証とは

複数の要素を**組み合わせて認証**する方式。

＜例＞
「ID・パスワード入力」（記憶）と「指紋認証」（生体情報）



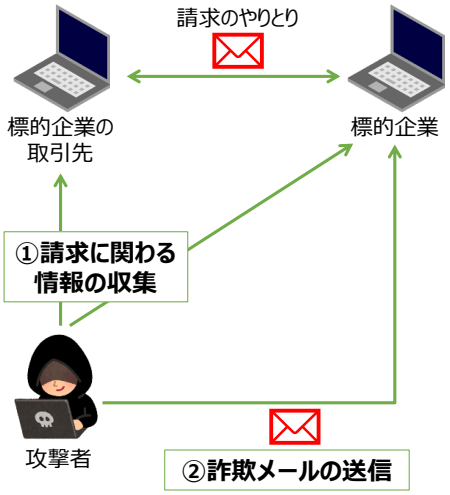
38

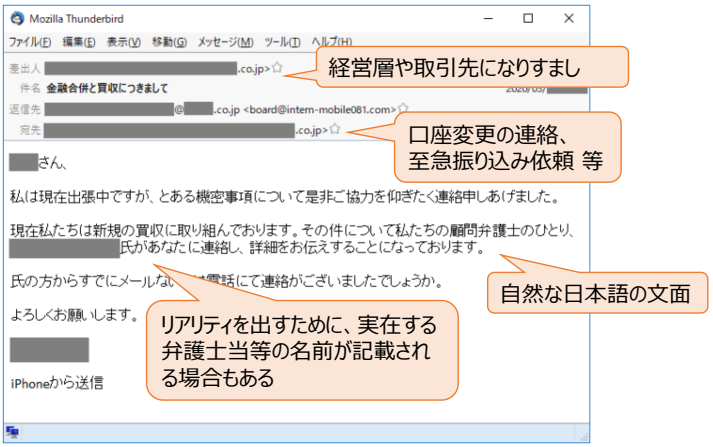
アカウント情報の漏えいにより、被害を受けないための対策例は上記の通りです。

「**パスワードの強化**」により、パスワードリスト攻撃等によって不正アクセスされるリスクを軽減できます。
また、「**認証方式の強化**」により、万が一パスワードが漏えいしても、不正アクセスを防ぐことができます。
さらに、定期的に「**不審なログインの確認**」を行うことで、不正アクセスに早期に気付くことができます。

4.4 ビジネスメール詐欺

ビジネスメール詐欺　取引先や経営者等になりすましたメールにより、攻撃者の口座に入金させる詐欺。





【出典】IPA「【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」を基に加筆・修正
(https://www.ipa.go.jp/security/announce/2020-bec.html)

39

金銭を目的とした「**ビジネスメール詐欺**」（Business E-mail Compromise）にも注意が必要です。
BEC（ビーイーシー）と省略して表現される場合もあります。

攻撃者は、あらかじめ請求に関わる情報を収集した上で、経理担当者等に詐欺メールを送信します。
詐欺メールの特徴は、上記の通りです。
日本国内でも、数億円の被害が発生した事例もあり、注意が必要です。

4.4 ビジネスメール詐欺

被害を受けないための対策例

目的	対策例	対策ポイント
詐欺メールを見分ける	普段と異なるメールに注意する	「内密にお願いしますという要求」や、「即時対応を求める要求」は、詐欺メールではないか疑う。
	送信元メールアドレスを確認する	フリーメールからのメールではないか、よく似た偽装メールアドレスでないか確認する。
	事実確認する	メールの署名に記載されている電話番号ではなく、元々把握している電話番号等を使って事実かどうか確認する。
	情報共有する	不審なメールは社内で相談・連絡し、情報共有する
体制の強化	電信送金に関する社内規定を整備する	急な振込先や決済手段の変更等が発生した場合、取引先へメール以外の方法で確認する。
		複数の担当者によるチェックを徹底する。
マルウェア・不正アクセス対策	基本的なマルウェア感染対策を実施する	「不審なメールの添付ファイルは開かない」、「セキュリティソフトを導入し、最新の状態を維持する」、「OSやアプリケーションの修正プログラムを適用し、最新の状態を維持する」等の基本的な対策を実施する。
	パスワードをセキュアに運用する	「4.3 アカウント情報の漏えい」を参照。

【出典】IPA「【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」を基に加筆・修正
（https://www.ipa.go.jp/security/announce/2020-bec.html）

40

ビジネスメール詐欺の対策例は、上記の通りです。

まずは、不審なメールを疑うことが重要です。
特に、普段と異なる対応を依頼された場合は、送信元のメールアドレスが正しい確認したり、元々把握している電話番号を使って事実確認することが有効です。

また、個人の感覚に頼るだけではなく、組織として電信送金に関する社内規定を整備し、体制を強化することが重要です。
さらに、攻撃者に情報を収集させないために、基本的なマルウェア・不正アクセスへの対策を実施することが重要です。

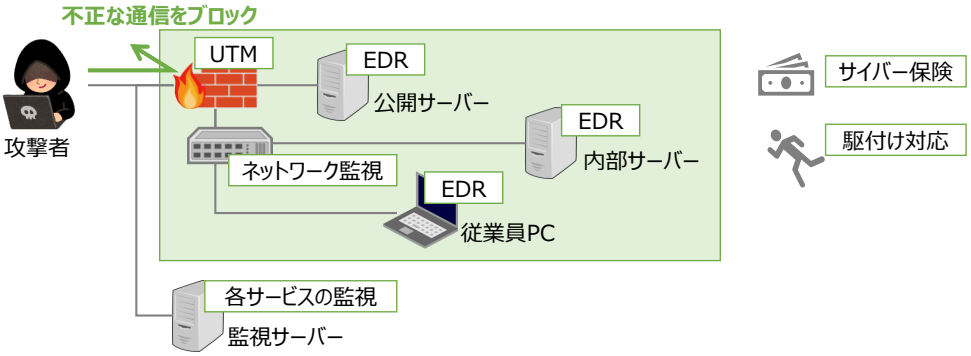
[参考]サイバーセキュリティお助け隊サービス

サイバーセキュリティお助け隊サービス

(https://www.ipa.go.jp/security/otasuketai-pr/)

- ✓ サイバーセキュリティ対策の導入・運用を支援するサービス
- ✓ 中小企業向けに、安価かつ効果的なワンパッケージで、様々なサービスが提供されている

提供サービスイメージ



41

「**サイバーセキュリティお助け隊サービス**」は、サイバーセキュリティ対策の導入・運用を支援するサービスです。
中小企業向けに、安価かつ効果的なワンパッケージで、様々なサービスが提供されています。

＜提供サービスの例＞

サービス	内容	初期費用	月額費用
UTM （サイバー保険、駆付け対応も含む）	組織ネットワークの出入口等に機器を設置して、不正な通信をブロックするサービス	16,500円/台	月6,600～9,800円/台
EDR （サイバー保険、駆付け対応も含む）	PCやサーバ等にソフトをインストールして、不正なふるまいを検知/対処するサービス	0～150,000円 ※セルフ、オンサイト対応によって変わる	月550～2,200円/台
ネットワーク監視 （サイバー保険、駆付け対応も含む）	組織の出入口、内部のネットワーク等に機器を設置して、不正な通信を監視するサービス	51,000～/台	月9,800円～/台

用語解説

UTM（ユーティーエム）
Unified Threat Managementの略。ファイアーウォール、IDS/IPS等の機能を1つのハードウェアに統合し、集中的に管理するセキュリティ対策製品。

EDR（イーディーアール）
Endpoint Detection and Responseの略。サーバーやPCの不審な挙動を検知するセキュリティ対策製品。

用語集・索引

英字

AD（エーディー） [p21]
Active Directoryの略。ユーザーやコンピューター等のリソースを一元管理するシステム。

BEC（ビーイーシー） [p39]
Business E-mail Compromiseの略。ビジネスメール詐欺のこと。

BYOD（ビーワイオーディー） [p8]
Bring Your Own Deviceの略。個人所有の機器を業務利用すること。

EDR（イーディーアール） [p41]
Endpoint Detection and Responseの略。
サーバーやPCの不審な挙動を検知するセキュリティ対策製品。

Emotet（エモテット） [p12]
マルウェアの一種で、メールに添付された悪質な「パスワード付きZIPファイル」、「マクロが埋め込まれたExcelやWordファイル」、メール文中の「不正なリンク」等から感染する。感染すると、メールアドレスやパスワード、電話帳等の情報を窃取されたり、さらに他の悪質なマルウェアに感染させられたりする。

FW（ファイアーウォール） [p8、21]
Firewallの略。ファイアーウォールのこと。

IaaS（イアース/アイアース） [p35]
クラウドサービス形態の一つで、サーバーやネットワークの基盤のみが提供される形態。

IDS（アイディーエス） [p41]
Intrusion Detection Systemの略。ファイアーウォールを通過した通信の中で、OSやミドルウェア等への攻撃を検知するセキュリティ対策製品。

IPS（アイピーエス） [p41]
Intrusion Prevention Systemの略。IDSの機能に加えて不正な通信を遮断する機能を持つセキュリティ対策製品。

PaaS（パース） [p35]
クラウドサービス形態の一つで、サーバーやネットワークの基盤に加えて、アプリケーションを実行する環境も提供される形態。

Proxy（プロキシ） [p21]
組織内利用者のインターネットアクセスを代理で処理するサーバ。外部ネットワークからはProxyサーバと通信しているようにしか見えない。

英字

RAT（ラット） [p11]
Remote Access Toolの略。インターネット上の攻撃者サーバとコネクトバック通信を行い、遠隔操作を可能とするプログラム。

RaaS（ラース） [p24]
Ransomware as a Serviceの略。ランサムウェアをサービスとして取引するビジネスのこと。

SaaS（サース） [p35]
クラウドサービス形態の一つで、メール等、特定の利用用途に応じたサービスが提供される形態。

UTM（ユーティーエム） [p41]
Unified Threat Managementの略。ファイアウォール、IDS/IPS等の機能を1つのハードウェアに統合し、集中的に管理するセキュリティ対策製品。

VPN（ブイピーエヌ） [p8、21]
Virtual Private Networkの略。認証や暗号化により、公衆ネットワーク上で仮想的な専用ネットワークを実現する技術。

Webサイト改ざん [p35]
悪意のある第三者によって、Webサイト内のシステムやコンテンツが意図しない状態に変更されてしまうこと。

ア

インシデント [p7]
事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のこと。

ウイルス [p13]
マルウェアの一種。
自己伝染機能(他のPC等にウイルス自身のコピーを作成する)、潜伏機能(発病まで一定期間沈黙する)、発病機能(システム破壊・情報窃取等を実行する)のうち、1つ以上の機能を持つプログラムのこと。

オンプレミス環境 [p35]
組織の施設内に設置したサーバー等の環境。サーバーやネットワークの基盤から、格納するデータまで、すべてが自組織の責任範囲となる。

カ

コネクトバック通信 [p11]
マルウェアに感染したPCが、攻撃者サーバに接続する通信。組織内のPC側から通信することで、FWをすり抜ける。

サ

サプライチェーン [p6]
サービス提供を行うための一連のビジネス活動を意味し、取引先や関連企業などを含めたビジネス活動の流れを指す。

ソーシャルエンジニアリング [p10]
人間の心理や行動、組織的な体制等の隙、ミス、漏れ等を突いた攻撃。
代表的な手口に、「ショルダーハッキング」（肩口からアカウントやパスワード等の入力を覗き見る手口）、トラッシング（廃棄業者を装ってゴミ箱をあさったり、廃棄物から情報を盗んだりする手口）等がある。

タ

ダークウェブ [p24]
アクセスするために、特定の認証方式や、アプリケーションが必要なWebサイト。身元の特定が困難であり、違法薬物や、個人情報等の闇取引に利用されることが多い。

ダークネット [p3]
どの機器にも割り当てられていない未使用のIPアドレス群のこと。本来ダークネットを宛先・送信元とする通信は発生しないはずだが、実際は膨大な通信が観測されており、そのほとんどがサイバー攻撃に起因するものであると推測されている。

多要素認証 [p38]
複数の要素（記憶、所持、生体情報）を組み合わせて認証する方式。

ハ

パスワードリスト攻撃 [p37]
不正に入手したIDとパスワードのリストを用いて、正規の認証方法によって不正アクセスを試みること。

ビジネスメール詐欺 [p39]
取引先や経営者等になりすましたメールにより、攻撃者の口座に入金させる詐欺。

標的型メール攻撃 [p10]
ソーシャルエンジニアリング等で調べた情報を基に、関係者や公的機関等を装い、標的組織にマルウェアを添付したメールを送信、または攻撃者サーバーに誘導してマルウェア感染させる攻撃。

ハ

ファイアーウォール [p8、21]
IPアドレス、ポート番号・プロトコル等をもとに通信の許可（通過）、拒否（遮断）を行うセキュリティ対策製品。専用のハードウェアだけでなく、OSの機能、またソフトウェアとして実装する場合もある。

フィッシング [p37]
正規サイトに似せた偽サイトに誘導した上で、ID・パスワード等を入力させて窃取し、正規の認証方法によって不正アクセスを試みること。

マ

マルウェア [p10]
不正かつ有害な動作を行うことを目的として、悪意を持って作成されたソフトウェアやコードのこと。
特徴によって、「ウイルス」「ワーム」「トロイの木馬」「ボット」等に分類される場合もある。

ラ

ランサムウェア [p24]
感染端末をロックしたり、ファイルを暗号化したりすることによって使用不能にした後、元に戻すことと引き換えに「身代金」を要求するマルウェアのこと。