CPMS Cyber Protection Managed Service

「情報セキュリティ10大脅威 2022」を更に深堀り！

ランサムウェア流行の背景やEmotet活動再開の詳細に迫る！

IPA「情報セキュリティ10大脅威 」とは

社会的影響が大きい事案を元にIPAが選出した選考員150名による審議・投票によって決定

情報セキュリティ分野の研究者や企業の実務担当者などが選出されており、エムオーテックス社員も選考員として参加

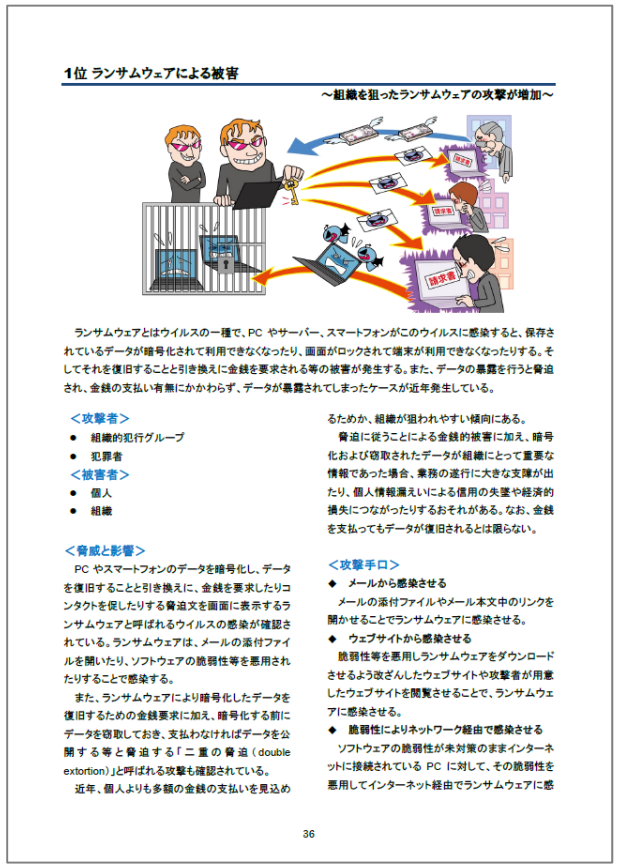

情報セキュリティ

10 大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～

IPA 独立行政法人情報処理推進機構 セキュリティセンター

2021 年 2 月


1位 ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

ランサムウェアとはウイルスの一種で、PC やサーバー、スマートフォンがこのウイルスに感染すると、保存されているデータが暗号化されて利用できなくなったり、画面がロックされて端末が利用できなくなったりする。そしてそれを復旧することと引き換えに金銭を要求される等の被害が発生する。また、データの暴露を行うと脅迫され、金銭の支払い有無にかかわらず、データが暴露されてしまったケースが近年発生している。

＜攻撃者＞
- 組織的犯行グループ
- 犯罪者

＜被害者＞
- 個人
- 組織

＜脅威と影響＞

PC やスマートフォンのデータを暗号化し、データを復旧することと引き換えに、金銭を要求したりコンタクトを促したりする脅迫文を画面に表示するランサムウェアと呼ばれるウイルスの感染が確認されている。ランサムウェアは、メールの添付ファイルを開いたり、ソフトウェアの脆弱性等を悪用されたりすることで感染する。

また、ランサムウェアにより暗号化したデータを復旧するための金銭要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と脅迫する「二重の脅迫（double extortion）」と呼ばれる攻撃も確認されている。

近年、個人よりも多額の金銭の支払いを見込めるためか、組織が狙われやすい傾向にある。

脅迫に従うことによる金銭的被害に加え、暗号化および窃取されたデータが組織にとって重要な情報であった場合、業務の遂行に大きな支障が出たり、個人情報漏えいによる信用の失墜や経済的損失につながったりするおそれがある。なお、金銭を支払ってもデータが復旧されるとは限らない。

＜攻撃手口＞

◆ メールから感染させる

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる。

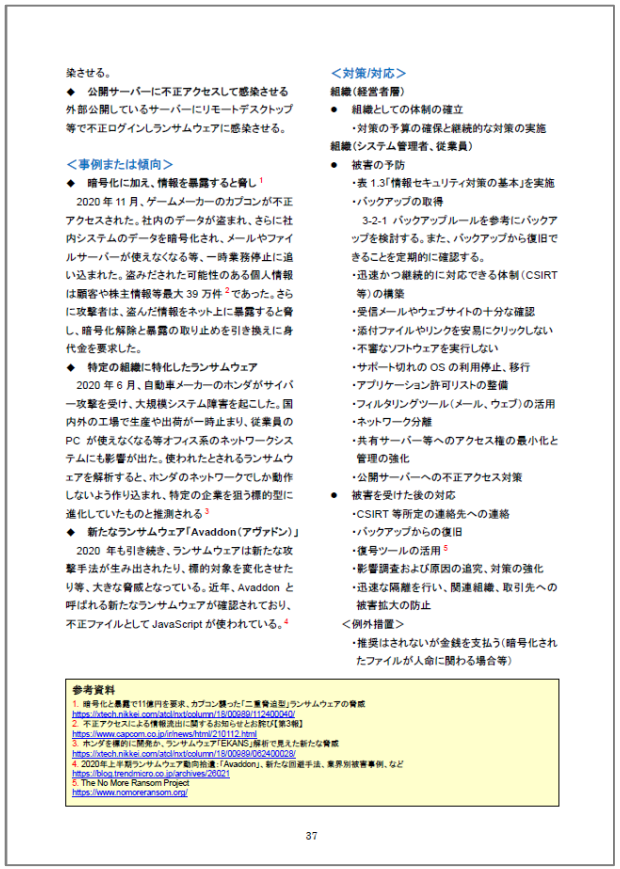
◆ ウェブサイトから感染させる

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんしたウェブサイトや攻撃者が用意したウェブサイトを閲覧させることで、ランサムウェアに感染させる。

◆ 脆弱性によりネットワーク経由で感染させる

ソフトウェアの脆弱性が未対策のままインターネットに接続されている PC に対して、その脆弱性を悪用してインターネット経由でランサムウェアに感染させる。

36


◆ 公開サーバーに不正アクセスして感染させる

外部公開しているサーバーにリモートデスクトップ等で不正ログインしランサムウェアに感染させる。

＜事例または傾向＞

◆ 暗号化に加え、情報を暴露すると脅し[1]

2020 年 11 月、ゲームメーカーのカプコンが不正アクセスされた。社内のデータが盗まれ、さらに社内システムのデータを暗号化され、メールやファイルサーバーが使えなくなる等、一時業務停止に追い込まれた。盗みだされた可能性のある個人情報は顧客や株主情報等最大 39 万件[2]であった。さらに攻撃者は、盗んだ情報をネット上に暴露すると脅し、暗号化解除と暴露の取り止めを引き換えに身代金を要求した。

◆ 特定の組織に特化したランサムウェア

2020 年 6 月、自動車メーカーのホンダがサイバー攻撃を受け、大規模システム障害を起こした。国内外の工場で生産や出荷が一時止まり、従業員の PC が使えなくなる等オフィス系のネットワークシステムにも影響が出た。使われたとされるランサムウェアを解析すると、ホンダのネットワークでしか動作しないよう作り込まれ、特定の企業を狙う標的型に進化していたものと推測される[3]

◆ 新たなランサムウェア「Avaddon（アヴァドン）」

2020 年も引き続き、ランサムウェアは新たな攻撃手法が生み出されたり、標的対象を変化させたり等、大きな脅威となっている。近年、Avaddon と呼ばれる新たなランサムウェアが確認されており、不正ファイルとして JavaScript が使われている。[4]

＜対策/対応＞

組織（経営者層）
- 組織としての体制の確立
  - ・対策の予算の確保と継続的な対策の実施

組織（システム管理者、従業員）
- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・バックアップの取得

3-2-1 バックアップルールを参考にバックアップを検討する。また、バックアップから復旧できることを定期的に確認する。
  - ・迅速かつ継続的に対応できる体制（CSIRT 等）の構築
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・不審なソフトウェアを実行しない
  - ・サポート切れの OS の利用停止、移行
  - ・アプリケーション許可リストの整備
  - ・フィルタリングツール（メール、ウェブ）の活用
  - ・ネットワーク分離
  - ・共有サーバー等へのアクセス権の最小化と管理の強化
  - ・公開サーバーへの不正アクセス対策
- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡
  - ・バックアップからの復旧
  - ・復号ツールの活用[5]
  - ・影響調査および原因の追究、対策の強化
  - ・迅速な隔離を行い、関連組織、取引先への被害拡大の防止

＜例外措置＞
- ・推奨はされないが金銭を支払う（暗号化されたファイルが人命に関わる場合等）

参考資料
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. 不正アクセスによる情報流出に関するお知らせとお詫び【第3報】 https://www.capcom.co.jp/ir/news/html/210112.html
3. 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/
4. 2020年上半期ランサムウェア最新動向（「Avaddon」、新たな回避手法、業界別被害事例、など https://blog.trendmicro.co.jp/archives/26021
5. The No More Ransom Project https://www.nomoreransom.org/

37

出典：2021年2月26日 IPA 「情報セキュリティ10大脅威 2021」解説書

2年連続「ランサムウェア」と「標的型攻撃」被害が1位・2位にランクイン

「3位 サプライチェーン」や「4位 テレワーク」についても、ほぼ順位に変動なく、サイバー攻撃に関する脅威が上位を占めている

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位 →
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位 →
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位 ↑
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位 ↓
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位 ↑
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位 ↑
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位 ↓
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位 ↓
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位 ↓

※引用：IPA「情報セキュリティ10大脅威2022」

CPMS とは

AI を活用した高精度のウイルス対策ソフトを2種類ご用意しています

CPMS Cyber Protection Managed Service

— Product 1 —

BlackBerry Protect

BlackBerry Optics

— Product 2 —

deep instinct™

AI による予測検知

オフラインでも変わらない高い検知率

過検知が少ない

CPMS は2種類のウイルス対策ソフトのうち、用途に応じて選択頂けます

多くの導入実績と LANSCOPE との連携も可能

BlackBerry Protect　BlackBerry Optics

- **国内の導入実績を重視**されるお客様
- **LANSCOPE 連携**をご利用したいお客様
- **インターネット非接続環境**での運用をお考えのお客様
- **EDR 要件**への対応をお求めのお客様

幅広い OS やファイルタイプに対応

deep instinct™

- **EXE ファイルだけでなく Word や Excel など多くのファイルタイプ**への対応をご要望のお客様
- **スマートフォン対応**をご要望のお客様
- **複数エンジンでの防御**をお求めのお客様

CPMS 比較表

BlackBerry Protect は導入社数が多くオプションも豊富
Deep Instinct は検知対象のファイルタイプが多く、マルチ OS に対応しているのが特長です

	BlackBerry Protect	Deep Instinct
対応OS	Windows、Mac、Linux	Windows、Mac、iOS、Android
対応するファイルタイプ	PE（exeやdll）	PE,PDF,Office,Macro,RTF,SWF,JAR,TIFF,Fonts,JTD …
EDR	BlackBerry Optics をオプション提供	無し
MOTEXの販売実績	約1,200社	約40社
コンソール	日本語対応済み	日本語対応済み
LANSCOPEオンプレミス版・クラウド版連携	連携可能	将来的に連携予定
価格（年額）	**5,400円**	**3,600円**
追加機能	・運用／代行（￥170／月額　￥2,040／年額） ・レポートサービス（￥80／月額　￥960／年額） ・Optics（￥150／月額　￥1,800／年額）	ー
3分で分かる！各製品の説明資料はコチラ	https://go.motex.co.jp/l/320351/2021-12-07/69qvbx	https://go.motex.co.jp/l/320351/2021-12-07/69qvc2

情報セキュリティ10大脅威 2022

・ランサムウェアによる被害（第1位）
・標的型攻撃による機密情報の窃取（第2位）
・修正プログラムの公開前を狙う攻撃（**初登場**：第7位）

ランサムウェアによる被害（第1位）

某食品加工業

身代金支払額：約12億円

ランサムウェア攻撃を受け一部工場の操業を停止せざるを得なくなった。

大半のシステムは復旧していたが、さらなる攻撃で顧客や従業員のデータが危険にさらされるリスクを考慮して社内のIT専門家および第三者のサイバーセキュリティ専門家と協議の上、身代金を支払った

某インフラ業

身代金支払額：約4億8000万円

システムにマルウェアが侵入して**短時間で 100GB 以上のデータが盗まれた**。情報の一部をインターネットに公開すると脅迫があり身代金要求を受けていた。**第三者がパイプラインへの攻撃を可能とする情報を入手した恐れがあるため**燃料パイプラインの操業を停止。一部地域で燃料が不足して住民はパニックに陥った。

某医療機関

身代金支払額：0円（支払いに応じず）

電子カルテがランサムウェアに感染。**バックアップデータも暗号化された**ため復旧に時間を要した。

結果、過去処方した薬剤や診療履歴が分からず、一時診療が出来なくなった。

約2ヶ月診療人数を制限しつつ対応。身代金要求を受けていたが応じなかった。

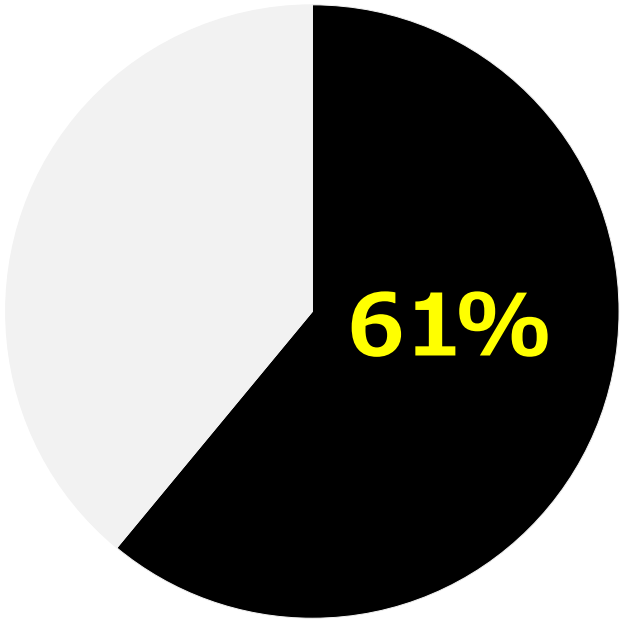
👉 Point

2021年はサイバー攻撃が世界的にも多く、有名企業だけでなく中小企業にも被害が拡大しました。攻撃者側も身代金の窃取を工夫しており、脅迫方法も様々なバリエーションが確認されています。某医療機関では、院内のコピー機から脅迫文が印刷され、コピー機にストックされた紙が尽きるまで印刷されていました。このような脅迫に屈しないことも大事ですが、そもそもランサムウェアに感染しないように事前対策することも重要です。

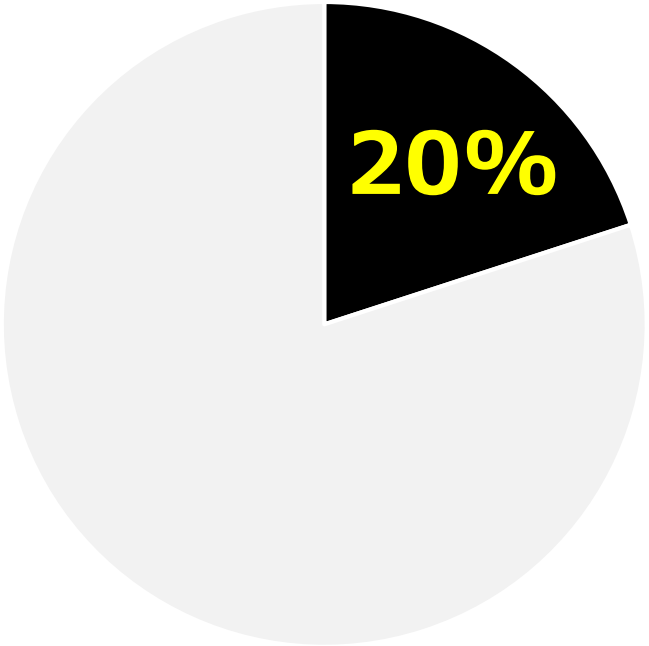
多くの組織では支払いを拒否しているものの、一部では2億円の身代金を支払っている

一度支払うと再度脅迫され、追加の身代金を支払うケースも確認されている

日本の調査対象者のうち
過去1年以内にランサムウェア被害に遭った割合



被害組織のうち、実際に身代金を払った割合



支払った身代金の平均額

225万ドル
（約2億2500万円）

身代金の支払い後、さらなる脅迫を受けた割合

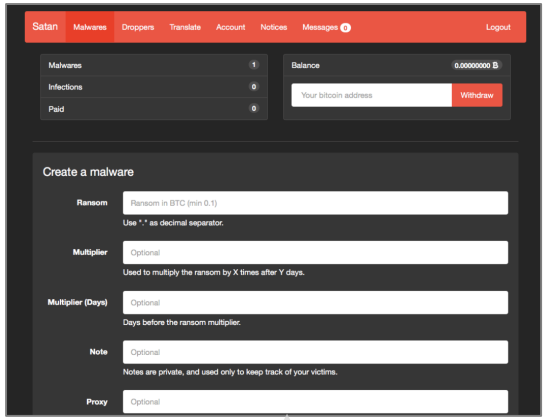
100%
(平均95万ドルを追加で支払い)

出典：一般社団法人日本プライバシー認証機構「拡大するランサムウェアビジネス」より引用
2021年9月～11月、日本や諸外国の主要業界に従事するITセキュリティ担当者2,200人を対象に調査

なぜ、ランサムウェア攻撃が増えているのか？

Ransomware as a Service（通称：RaaS）というビジネスモデルが構築
企業をランサムウェアに感染させることで報酬を得られる仕組みです

ランサムウェア作成 → **攻撃** → **報酬を山分け**



必要事項を入力するだけで作成可能！

データを暗号化し、身代金を請求

【RaaS 提供者】　【攻撃者】

振り込まれた身代金を山分け

Point

今やランサムウェアの作成は誰でも出来てしまいます。なんと闇サイトにあるランサムウェアの作成画面で必要事項を入力するだけなんです。また、攻撃者もランサムウェアを送り込むだで専門知識は必要ありません。日本プライバシー認証機構によれば、ランサムウェア提供者、攻撃者の他に身代金の交渉役も存在しているようです。脅迫が成功して身代金を獲得すると、提供者に約3割、攻撃者に約7割の配分で報酬が山分けされるそうです。

未来に発生するマルウェアを予測して検知！あらゆる未知・亜種のマルウェアから保護

BlackBerry Protect の AI は、**2年以上前**のバージョンでも、最新のマルウェアを検知した実績があります

一時期流行した凶悪マルウェア「Emotet」。2021年11月に活動再開が確認されています

IPA にも Emotet 感染のお問い合わせが増えていると発表があり、多くの被害が発生しているようです

＜2021年11月16日＞
活動再開の報告あり

＜2021年1月頃＞
テイクダウンが確認される

＜2014年頃の初期Emotet＞
オンラインバンク狙いのトロイの木馬
オンラインバンキングの情報を窃取する

＜Emotet の基本機能＞

①電子メールを軸に大規模な攻撃を展開

実際のメールへの返信を装ったばらまきメールなど、
巧妙にEmotet本体のダウンロードを誘導

②自己増殖能力を持つ

ネットワーク内の他のデバイスへ自ら感染を拡大し、
大規模な組織の内部での大きな被害を引き起こす

③他のマルウェアに感染させる機能がメイン

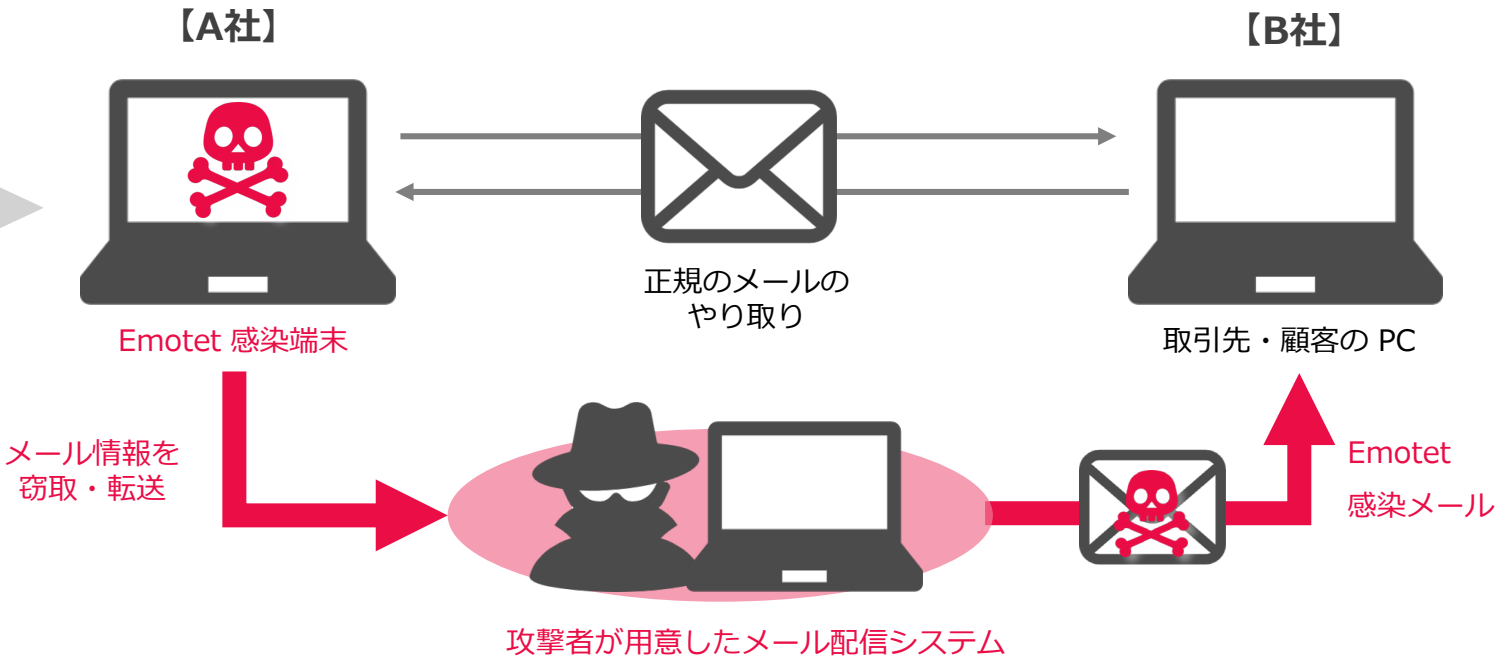
ランサムウェアなどのさらに強力なマルウェアを
呼び寄せるプラットフォームとして動作し、被害を拡大
最終的にはランサムウェアなどを用いて自らの活動の
痕跡を消し去る

Emotet に感染すると…

窃取したメール情報を悪用し、取引先や顧客に対して Emotet のばらまきメールを送信

【窃取される恐れのある情報】

- 端末やブラウザに保存されたパスワード等の認証情報
- メールアカウントとパスワード
- メール本文とアドレス帳の情報

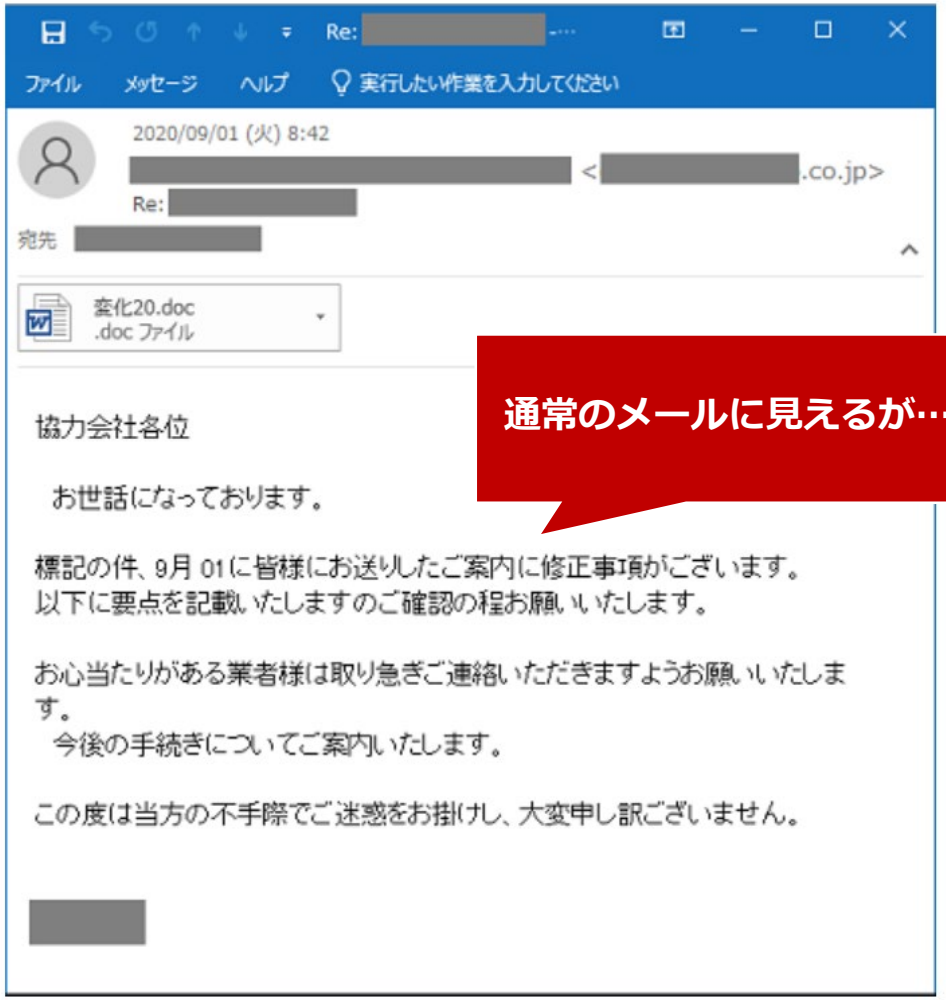


Point

Emotet に感染するとメールアカウントやアドレス帳の情報が抜き取られてしまいます。結果、攻撃者が自分になりすまして取引先にメールを送り、感染が拡大してしまいます。感染した会社は企業ブランドの低下や最悪の場合、取引先から損害賠償を請求される可能性もあります。次ページでご紹介しますが、なりすましメールも巧妙に作成されており見抜くのが難しいです。なお、Emotet は従来型のウイルス対策ソフトで防御できないことが多いです。

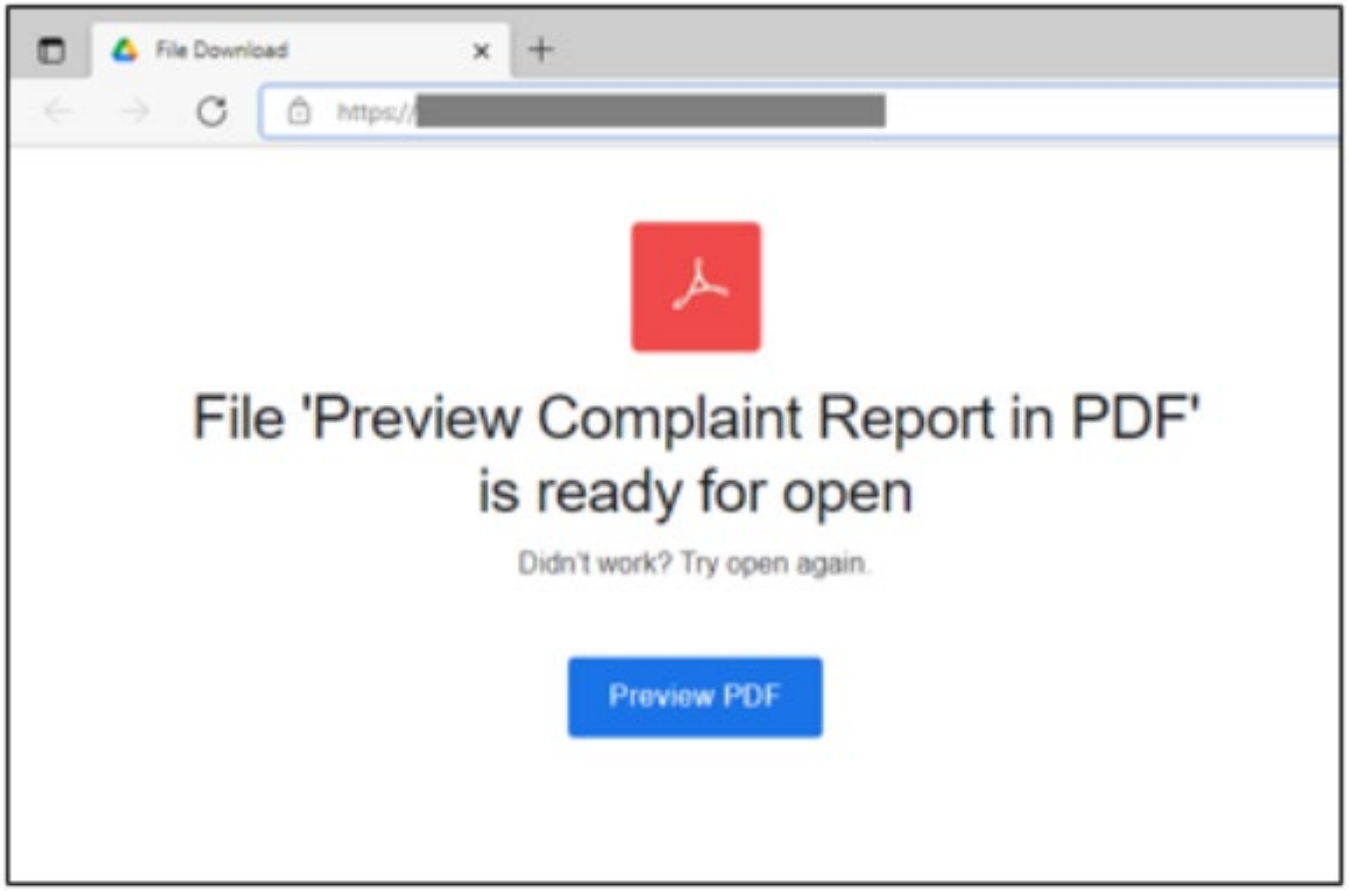
Emotet の攻撃手法

日本語の攻撃メールの例（従来の攻撃手法）※



通常のメールに見えるが…

メールから誘導される偽ウェブサイトの例（新しい攻撃手法）※

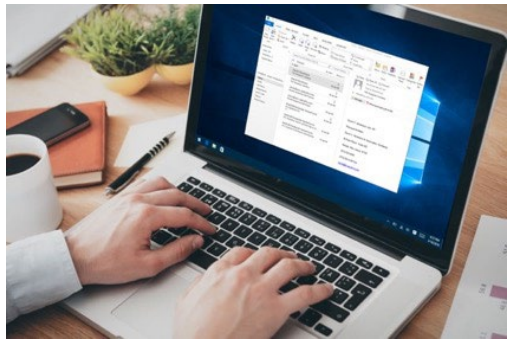
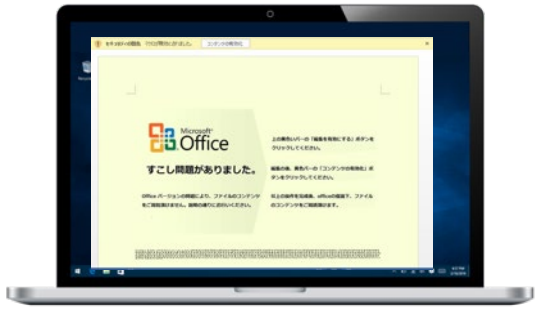


※出典：「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

Deep Instinct であれば Emotet も防御できる

Deep Instinct は Emotet の防御も可能！
Emotet が動き出す前に AI が検知して、攻撃を未然に防ぐ

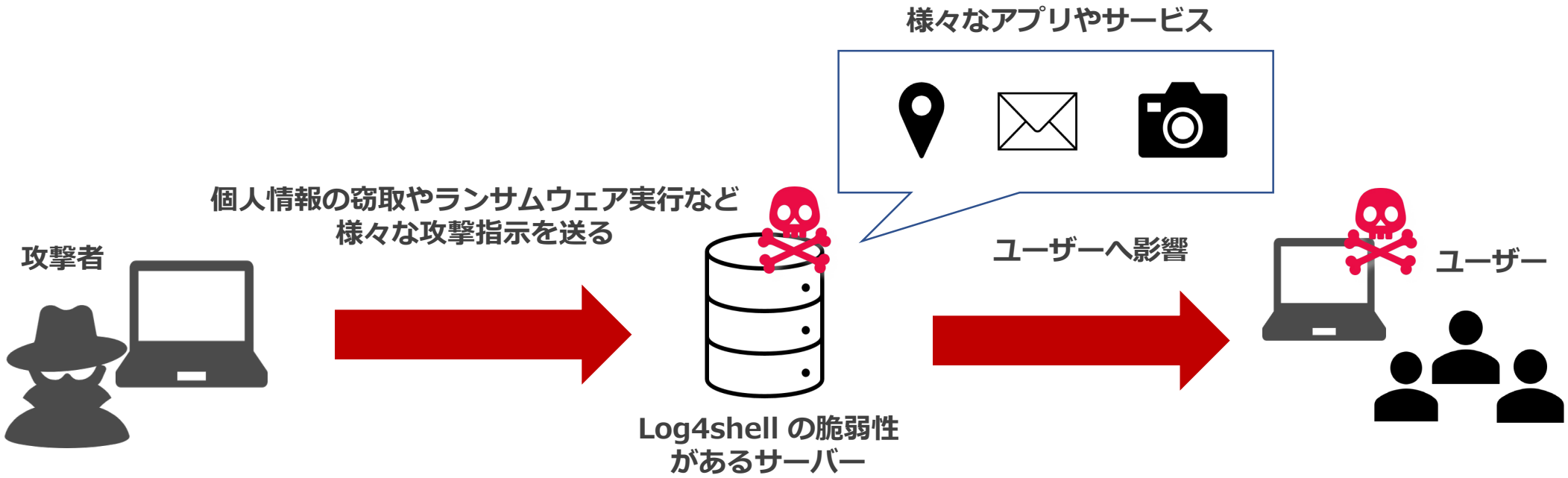
Emotet の攻撃プロセス

STEP1	STEP 2	STEP3
		
取引先を装ったメールに Word・Excel・Zip 等が添付されて届く	マルウェア本体をダウンロード するスクリプトが実行	マルウェア本体が ダウンロードされ実行
悪性マクロが仕組まれた Word や Excel を検知し開封させない	悪性 VBA マクロや Powershell を検知	ダウンロードされたマルウェアを隔離

修正プログラムの公開前を狙う攻撃（初登場：7位）

2021年12月、WannaCry と同様の警告が出される脆弱性「Log4Shell」が発見される

Java のログ出力ライブラリとして様々なアプリで利用され影響を受けるアプリケーションは多数。至急対策が求められている。

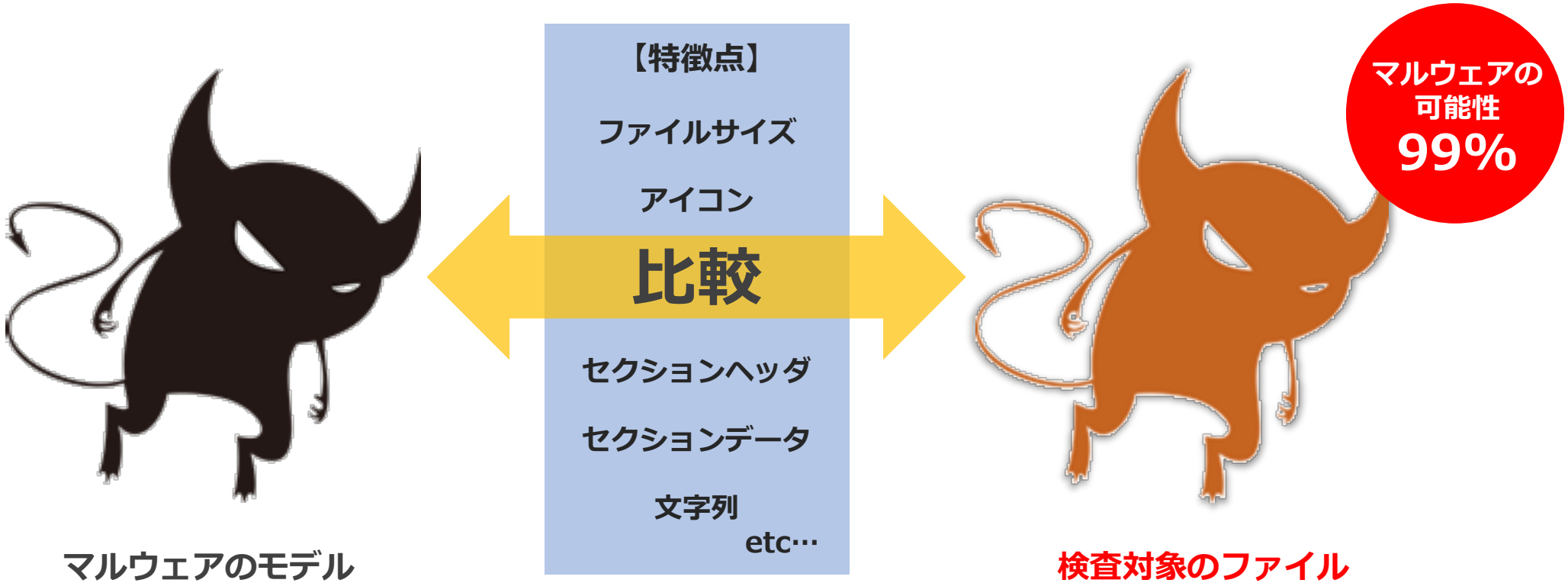


👉 Point

Log4j2 は、身近なアプリケーションに採用されている仕組みのため、アプリ提供元からの情報を必ずご確認頂きアップデートをお願いします。
既に脆弱性を悪用してサイバー攻撃被害も発生しており注意が必要です。CPMS では、脆弱性自体を解消することは出来ませんが、脆弱性を悪用してマルウェアが送り込まれた場合、CPMS がマルウェアを隔離することは可能です。

脆弱性自体は Deep Instinct で対策できないが、マルウェアは止められる

AI が膨大な情報からマルウェアの特徴を学習
脆弱性を悪用して、未知のマルウェアを送り込まれても 99% 防御します



マルウェアのモデル
過去に発見されたマルウェアなど
ありとあらゆる危険なファイルの
特長を分析・数理モデル化

検査対象のファイル
マルウェアのモデルと比較することで
過去に発見されたマルウェアと全く同じでなくとも
その特徴からマルウェアであると特定できる

体験版のご案内

両製品とも無料体験版もご用意しています！
無償で操作方法のレクチャーや質疑応答いたしますので、是非お試しください

BlackBerry Protect

▼体験版のお申込みはこちら

概　　要	BlackBerry Protect がキャンペーン期間中にライセンス数無制限で使えます。また、検知したファイルについてサマリーレポートを作成させて頂きます。さらに専任スタッフによる導入時の支援付きで、負担なく使い始められます。
対　　象	BlackBerry Protect を初めて導入するユーザー様
ご利用期間	1ヶ月間
申 し 込 み	上記キャンペーンサイトからエントリー
申 込 期 間	2022年3月31日

deep instinct™

▼体験版のお申込みはこちら

概　　要	Deep Instinct が 100L まで、1ヶ月間無料でお試し頂けます。 さらに専任スタッフによる導入時の支援付きで、負担なく使い始められます。体験中の不明点にも対応しますので、じっくりしっかり体験が可能です。
対　　象	Deep Instinct を初めて導入するユーザー様
ご利用期間	1ヶ月間
申 し 込 み	上記キャンペーンサイトからエントリー
申 込 期 間	常時受付

お役立ち資料のダウンロード

サイバーセキュリティの最新情報やご検討に役立つ資料を無料でダウンロード頂けます

▼お申し込みはこちら

2021年のサイバー攻撃「10の事例」を振り返る
2021年の国内外のサイバー攻撃事例を振り返り
どんな特徴や傾向が見られたか、新たなリスク
として認識される脅威も紹介します。

▼お申し込みはこちら

巧妙化するサイバー攻撃から、あらゆる環境を守る！
Deep Instinct 7つの導入事例
Deep Instinct をご導入いただいているユーザー様
より伺った運用事例をご紹介します。

その他の資料も下記からダウンロード出来ます
https://www.lanscope.jp/cpms/download/

お問い合わせ先

■製品に関するお問い合わせ

エムオーテックス株式会社 営業部

大　阪本社： 06-6308-8989

東　京本部： 03-5460-0775

名古屋支店： 052-253-7346

E-Mail：sales@motex.co.jp

■ご導入後の運用に関するお問い合わせ

エムオーテックスサポートセンター

0120-968-995

※携帯からは06-6308-8981

※受付 9:30～12:00/13:00～17:30（月～金、MOTEXの営業日）

メールでのお問い合わせ

support@motex.co.jp（※24時間受付）

関連サイト

エムオーテックス株式会社 コーポレートサイト	http://www.motex.co.jp/
CPMS（Cyber Protection Managed Service） 製品サイト	https://www.lanscope.jp/cpms/
BlackBerry Protect 製品紹介	https://www.lanscope.jp/cpms/blackberryprotect/
Deep Instinct 製品紹介	https://www.lanscope.jp/cpms/deepinstinct/