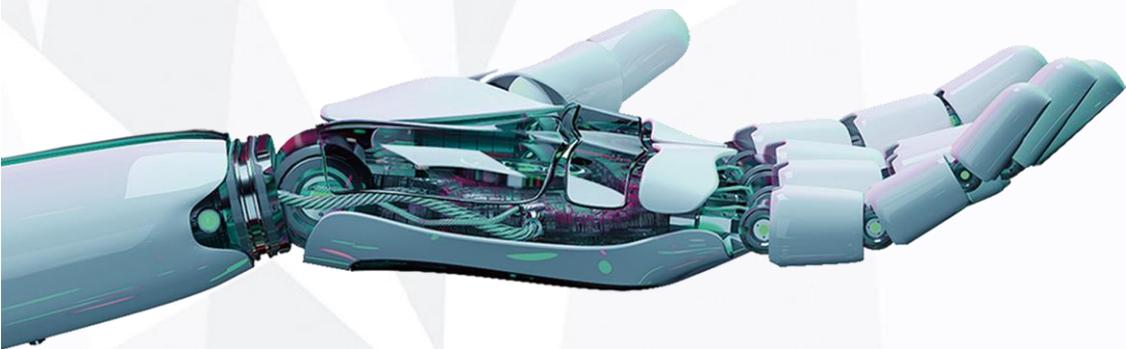




CPMS

Cyber Protection
Managed Service



実施すべき ランサムウェア対策の ポイントが分かる！

CPMSユーザー様の運用実例もご紹介

2022年1月27日 IPA 発表の「情報セキュリティ10大脅威 2022」から見る傾向

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位 
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 
5位	内部不正による情報漏えい	6位 
6位	脆弱性対策情報の公開に伴う悪用増加	10位 
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
8位	ビジネスメール詐欺による金銭被害	5位 
9位	予期せぬIT基盤の障害に伴う業務停止	7位 
10位	不注意による情報漏えい等の被害	9位 

今期のポイント

1位：「ランサムウェアによる被害」

2021年は、日本だけでなく世界的にもランサムウェアの被害が多く確認されました。従業員規模や業界関係なく、幅広く攻撃が実施されており注意が必要です。

2位：「標的型攻撃による機密情報の窃取」

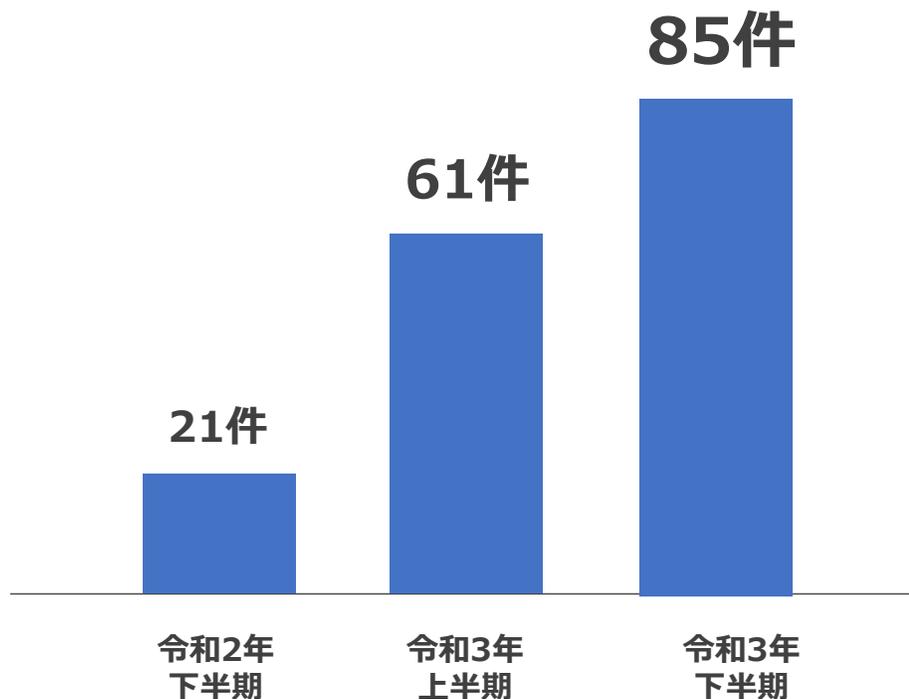
一時期大流行した凶悪マルウェア「Emotet」が、2021年11月に活動再開しています。巧妙に取引先を装ったメールにマルウェアを添付して配信することで被害が拡大しました。

7位：「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」

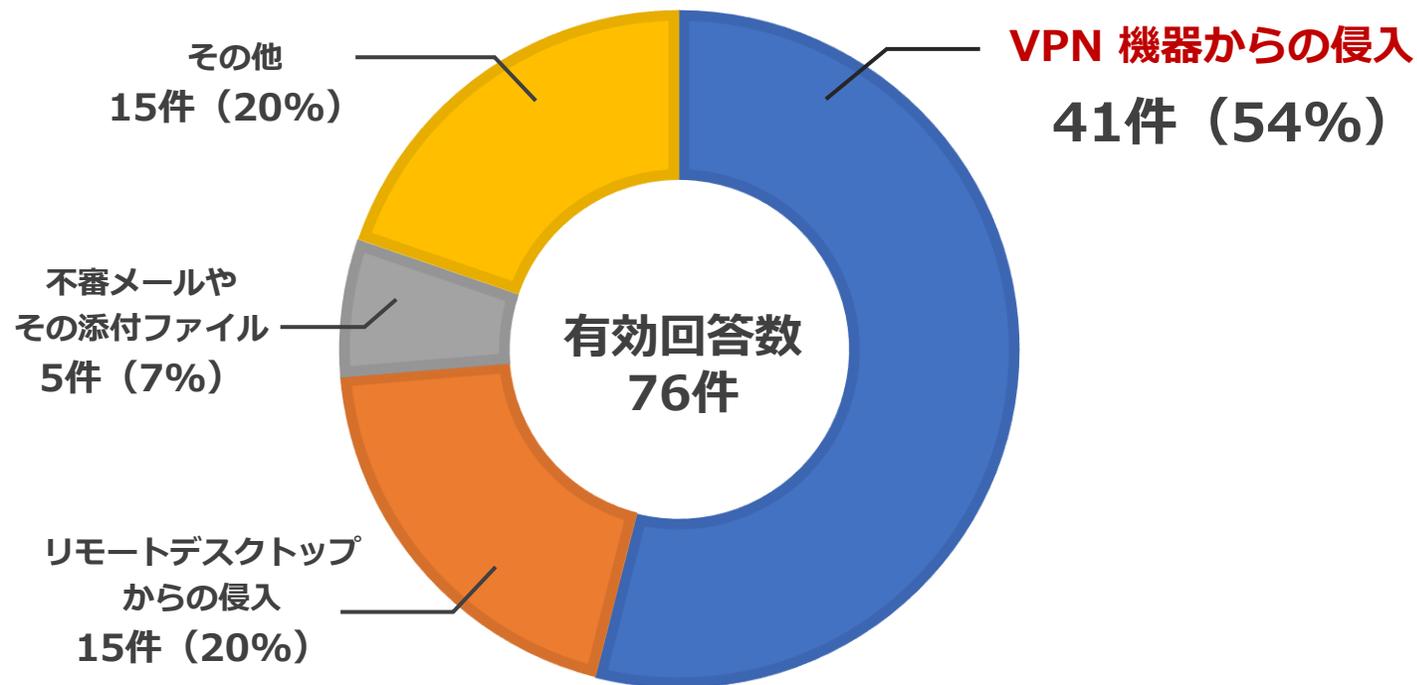
2021年12月、Apacheのログ収集ツールである「Log4j2」に脆弱性が発見されました。「Log4j2」は身近なアプリにも組み込まれているため影響範囲が大きい事件となりました。

※引用：IPA「情報セキュリティ10大脅威2022」

ランサムウェア被害の報告件数の推移※



ランサムウェアの感染経路※

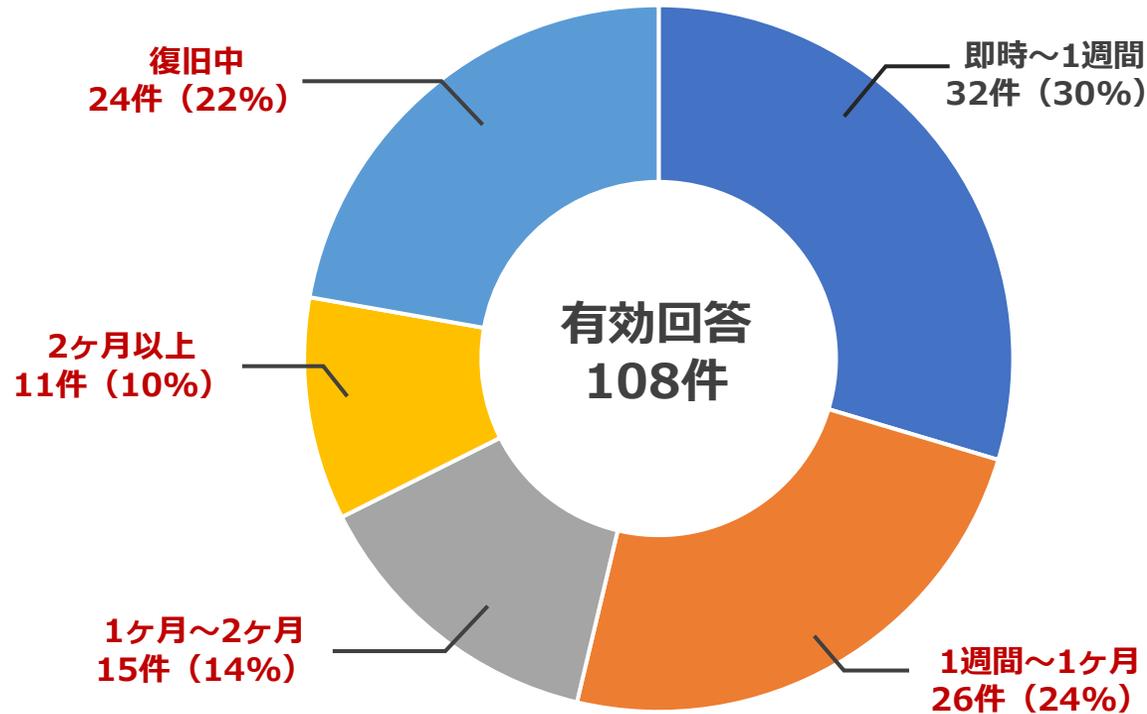


👉 ポイント

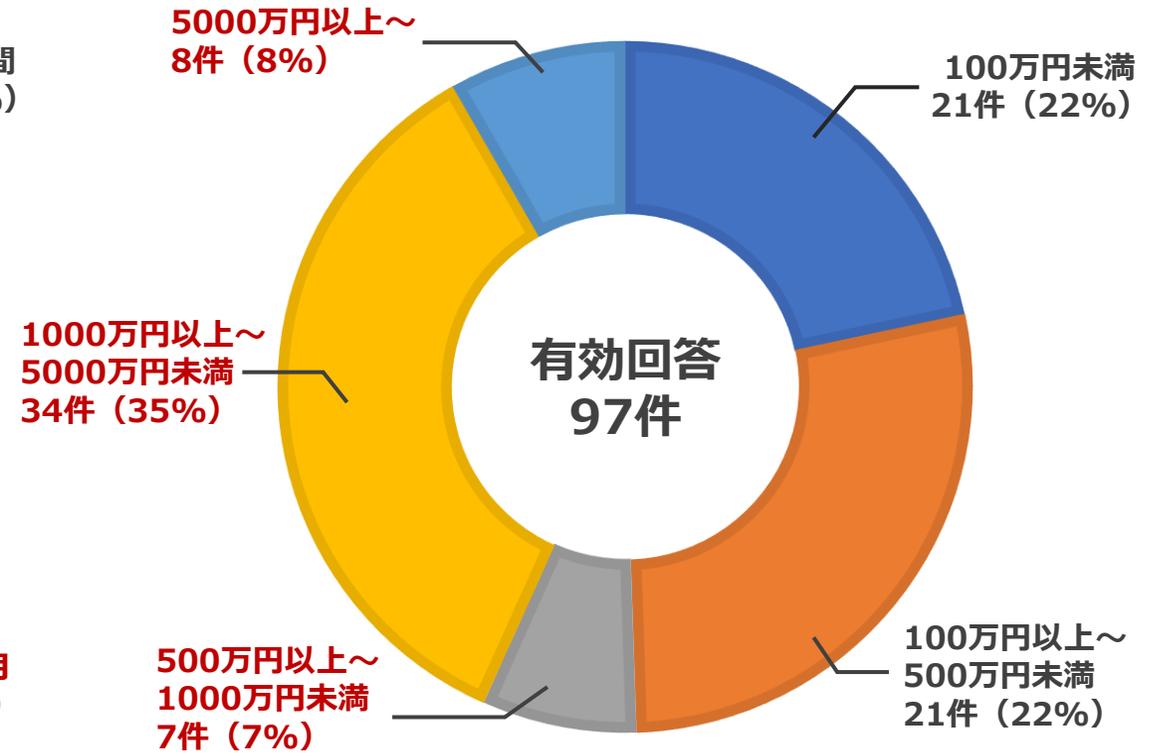
ランサムウェアの被害件数は年々右肩上がりの状況です。主な感染経路は、「VPN 機器の脆弱性を悪用した侵入」が多くなっています。新型コロナウイルスの影響で急遽テレワークを始めたことにより、VPN 機器の利用が増えました。対応に追われた企業のシステム部門は予備の VPN 機器を使わざるを得ない状況となり、**最新バージョンにアップデートをしていなかったため**、感染被害が増加しました。

※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」

復旧に要した期間※



調査・復旧費用の総額※



👉 ポイント

ランサムウェアに感染すると復旧までに1週間以上かかるケースが大半です。2021年11月頃に発生した某医療機関でのランサムウェア感染事件でも電子カルテが暗号化されてしまい、一時期に診療体制が制限されました。その後、**通常の体制に戻るまで2ヶ月ほど時間を要しています**。また、感染したシステムによっては調査・復旧費用が莫大なものになってしまう可能性があり、割合としては**500万円以上が半分を占めています**。

※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」

ウイルス対策ソフトで検知されないように、大量の未知・亜種のマルウェアを作成

1度使ったマルウェアを再度攻撃に使用することは、ほとんど無い



1日に作られるマルウェアの数

最近では誰でもマルウェアを作成出来ます。企業のシステム環境は常に悪意のあるユーザーによって、**膨大なセキュリティリスク**にさらされていると言えます。



マルウェアの平均寿命

マルウェアは生まれてから、**58秒で消滅します**。常に未知の新しいセキュリティリスクが生まれては消えています。



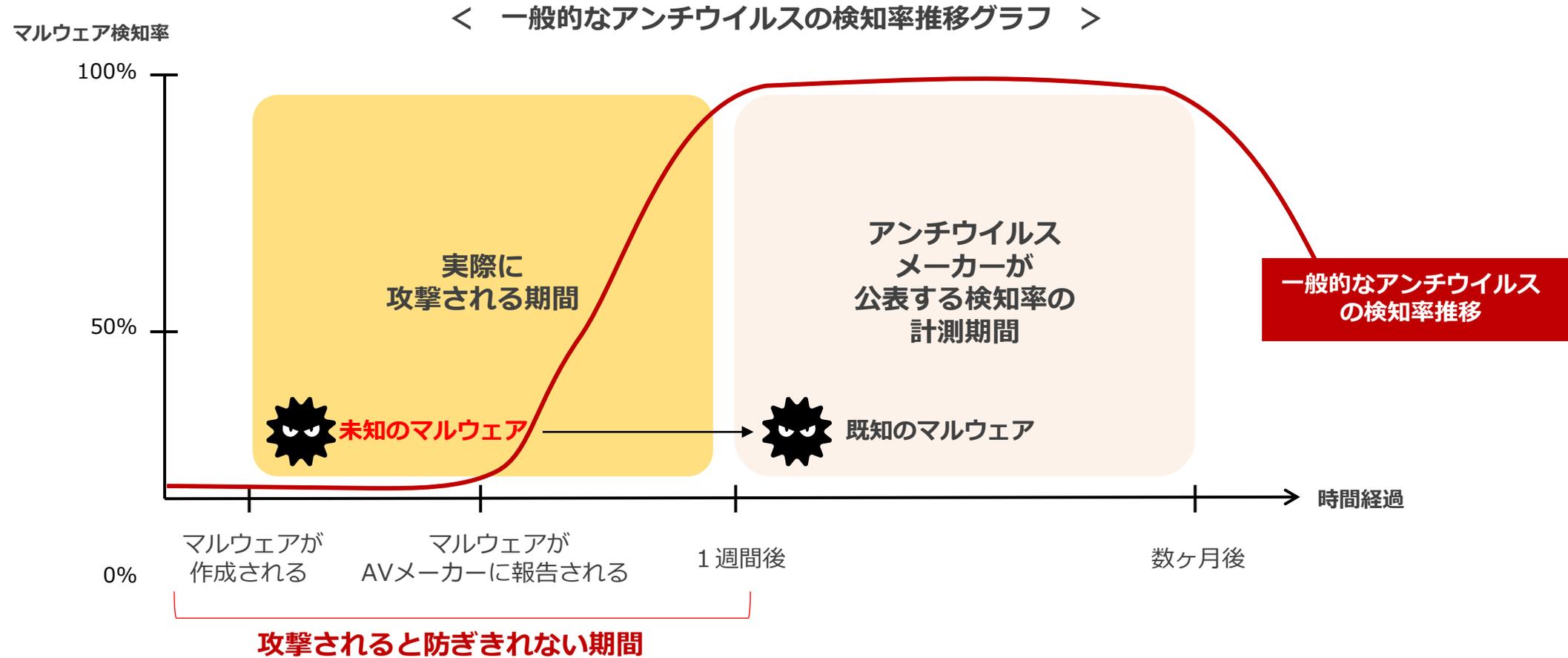
同じマルウェアが使われる割合

別の組織で再発見されるマルウェアは**たったの0.5%**。つまり、同じマルウェアが2度以上使われることはほとんどありません。攻撃に使われる**マルウェアは、ほぼ“未知”である**と言えます。

VERIZON DBIR（データ漏洩/侵害調査報告書）2016の調査より

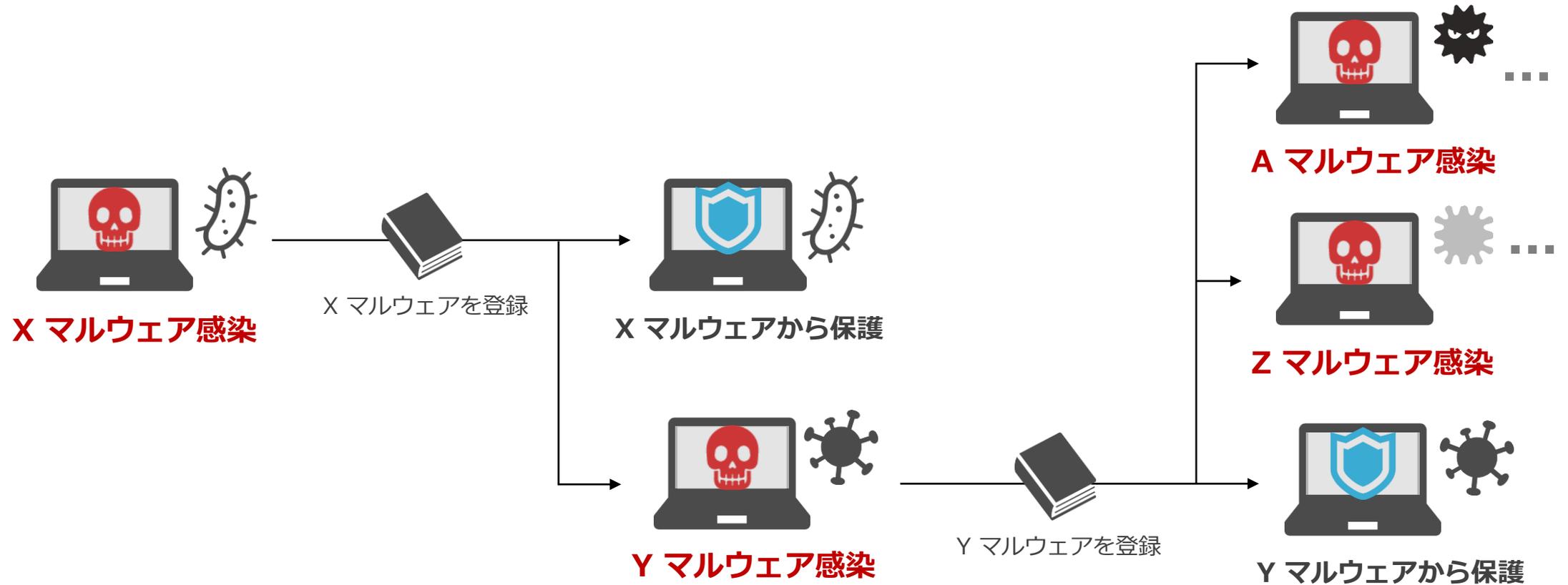
未知のマルウェアは既存アンチウイルスの検知方式では攻撃を受けてしまう期間が発生

現在主流となっているやシグネチャ型は、攻撃を受けてからパッチを作成します。その間は攻撃を防ぐ手立てはありません



攻撃は使い捨て未知のマルウェアばかり…シグネチャベースのパターンマッチングでは限界

パターンマッチング方式は、感染報告後シグネチャに登録されれば、検知・保護が可能だが初見では検知が難しい仕組みです



未知・亜種のマルウェアを 99% 防御

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



— Product 1 —



BlackBerry® Protect



BlackBerry® Optics

— Product 2 —



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

AI が未知・既知問わずマルウェアを隔離します
定義ファイルを使わないため、シグネチャ更新管理からも解放されます



CPMS

Cyber Protection Managed Service

マルウェア検知率 99%



高性能な AI により
未知・既知問わず検知可能

毎日のアップデート不要



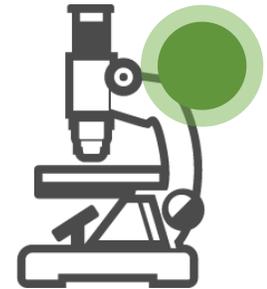
定義ファイルを使用しないため
毎日のアップデート不要

PC 負荷が少ない



サイズは 150MB 以下、
CPU 負荷 1% 以下

誤検知が少ない



従来製品と比較しても
誤検知は数十～数百分の1

事前に膨大な情報を AI に与えマルウェアの特徴を徹底学習
AI がファイルの特徴から「未知のマルウェア」を判定する



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

ランサムウェアの
可能性
99%

CPMS は既知・未知問わずマルウェア対策が可能
また、エージェント更新やフルスキャン頻度も少なく運用も簡単！

	CPMS	シグネチャ型ウイルス対策ソフト
既知のマルウェア検知（振る舞い検知など）	○	○
未知のマルウェア検知（AI検知）	○	×
ファイルレスマルウェア防御	○	×
ソフトウェアの脆弱性を利用した攻撃防御	○	×
エージェントの更新頻度	年に数回	毎月1～2回ほどシグネチャ更新が必要
フルスキャンの頻度	初回インストール時	シグネチャ更新時

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



- ・ コストを重視されるお客様
- ・ PC とスマホにウイルス対策ソフトを導入したいお客様
- ・ 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

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、macOS、Linux	Windows、macOS、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1,400社 (2016年7月から販売開始)	約150社 (2021年2月から販売開始)
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	連携予定 (LANSCOPE クラウド版)
価格 (年額)	5,400円	3,600円
追加機能	<ul style="list-style-type: none"> ・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) 	—

■ 製造業 A社様 : Deep Instinct ご利用

ランサムウェアの隔離に成功！運用を見直すキッカケになりました！

デバイス 500 台

管理 OS Windows

導入前 : 効果の少ないシグネチャ更新、鳴り響く EDR のアラートに消耗

- ・毎日シグネチャをアップデートしてフルスキャンを実施。更新時、PC に高い負荷をかけていた
- ・EDR からほぼ毎日アラートが鳴っていたが、誤検知が多く次第にログを見なくなった

導入後 : 対応時間が 3 割削減！ Deep Instinct の検知力の高さを実感

- ・Deep Instinct はシグネチャレスで誤検知も少なく、対応工数が大幅削減
- ・既存のウイルス対策ソフトで検知できなかったランサムウェアも隔離したので効果を実感

A 社様の誤検知率



スキャンファイル数 337,992,649

脅威検出 (ファイル) 126

誤検知 3

誤検知率 (%) 0.000001%

■ 不動産業 B社様 : BlackBerry Protect をご利用

テレワークでも安心な環境を構築！人材不足の中小企業こそ最適な製品です！

デバイス 450 台

管理 OS Windows

導入前 : テレワークで、社内 NW 外のため多層防御が機能しない

- ・ファイヤーウォールなどの他セキュリティツールによる多層防御が機能していない状態
- ・エンドポイントのウイルス対策ソフトがセキュリティの最終防衛線。強力な製品が必要

導入後 : 防御力が高く、メーカーサポートも手厚いので安心できる

- ・BlackBerry Protect が強力なため安心。MOTEX のサポートが手厚く中小企業でも使える製品



【サポート体制】

MOTEX サポートセンターが操作方法や運用方法、QA など手厚くサポートさせていただきます。操作手順書などのマニュアルもご用意しています。

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



▼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いただきます。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9月30日

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

付録：セキュリティチェックシート

✓	チェック項目	詳細
	バックアップ	機微な情報、リスクの高いデータについては、単にバックアップを取得するだけでなく、オフラインで保管しておく。これに加えて、クラウドストレージを用いる場合でも、予めデータをもとに戻す手順の確立とテストは重要である。
	ユーザー権限の厳密化	先に述べたように、ランサムウェア攻撃では、単にデータの暗号化による盗難だけでなく、被害者ネットワークを水平に動き回り（ラテラルムーブメント）、被害者にとって重要なデータを窃取しようとする。このため、Active Directory で管理しているユーザーアカウントを再確認し、特権ユーザーの絞り込みやルールの見直しを行い侵害を抑えることが重要
	パッチ	OS などの脆弱性パッチはテストの上、更新適用しておく。最近では、Microsoft Exchange の脆弱性（ProxyShell）を悪用して水平展開を行うランサムウェアも観測されている。最新のパッチを適用することで、このような侵害の広がりを防ぐことができる。
	ウイルス対策ソフト	最新の状態で、組織に合う最良の設定で利用する。また次世代型のように未知・既知の脅威どちらでも高精度で検知・駆除できるものを検討する。
	VPN機器	VPN機器が最新バージョンになっているかを確認する
	ファイアウォール	ファイアウォールを用いて不正 IPアドレスへの通信を適切にブロックする。
	ホワイトリスト運用	アプリケーションのホワイトリスト運用などで、許可されたアプリケーション以外の実行を防止するような運用管理を行う。
	メールスキャン	メールの送受信スキャンを実施し、スパムや不正なもの、実行ファイルが添付されているものなどを検知・駆除する。
	リモート接続サービス	リモート接続サービスを棚卸し、使用していないものは無効にしたり、接続時の認証に多要素認証を取り入れたり、リスク管理方針に基づいて継続的な認証（c.f. ゼロトラストアーキテクチャー）を実装する。
	従業員教育の実施	<p>ユーザー認知トレーニングの実施：ユーザーは、コンピューターに一番近い存在。彼らに対して、認知を高め、トレーニングを実施する。</p> <ul style="list-style-type: none"> ・信頼できないウェブサイト、メールの添付ファイルやリンククリックなどをしない。メールゲートウェイなどでフィルタ設定も検討する。 ・信頼できない Webサイトからファイルをダウンロードしない。 ・不明な USBメモリを使わない

■ 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

CPMS (Cyber Protection Managed Service) 製品サイト

BlackBerry Protect 製品紹介

Deep Instinct 製品紹介

<http://www.motex.co.jp/>

<https://www.lanscope.jp/cpms/>

<https://www.lanscope.jp/cpms/blackberryprotect/>

<https://www.lanscope.jp/cpms/deepinstinct/>

MOTEX