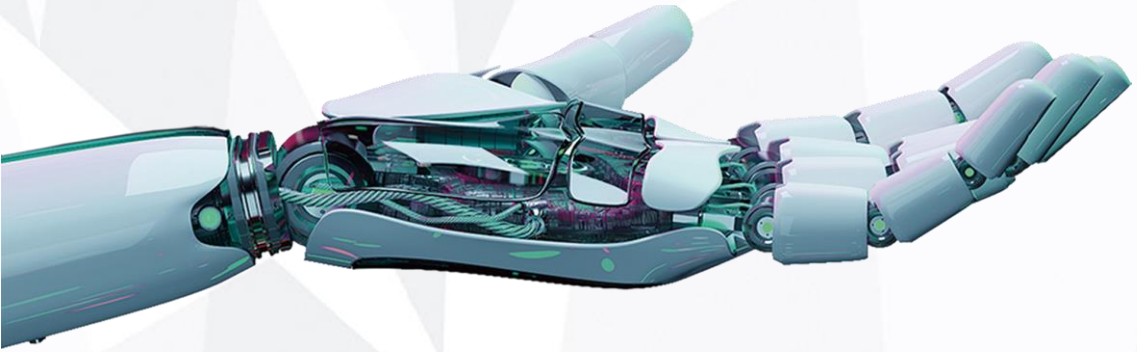
CPMS
Cyber Protection
Managed Service

ランサムウェア対策で知っておきたい

暗号化阻止のタイムリミット



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

※引用：IPA「情報セキュリティ10大脅威2022」

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。

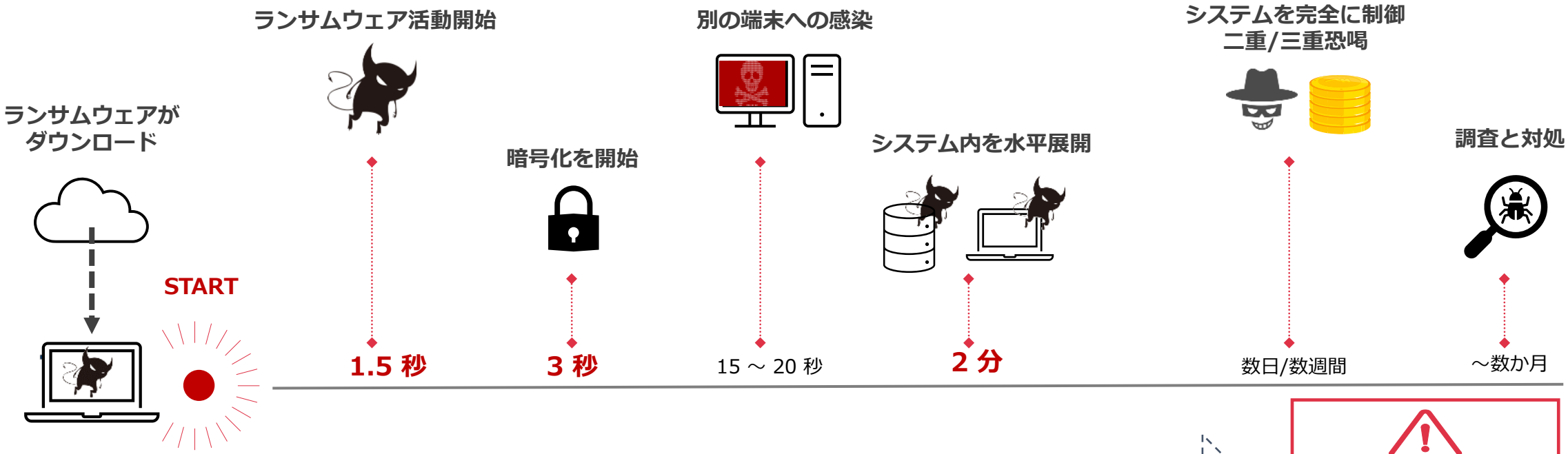
7位：「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」

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。

ランサムウェアの活動開始～被害発生までの流れ

感染スピードが早いランサムウェアが増えている

端末に侵入してから 3 秒後に暗号化を開始、2 分後には全社に広がってしまう場合がある※



シグネチャ型ウイルス対策

シグネチャがないため検知できず…

EDR

このタイミングでは未検知

アラートは出すが、僅かな時間で人が対処することは困難

事後対応

バックアップから復元
以下の損失から回復

- 顧客の信頼失墜
- 金銭的損失
- 企業ブランドの低下

※Deep Instinct 社調べ

各ランサムウェアが 10 万ファイルを暗号化するのにかかる時間

ランサムウェアファミリー	暗号化にかかった時間（中央値）
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:02
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza(PYSA)	01:54:54
中央値の平均	**00:42:52**

出典：Splunk：Ransomware Encrypts Nearly 100,000 Files in Under 45 Minutes を基に MOTEX で作成

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

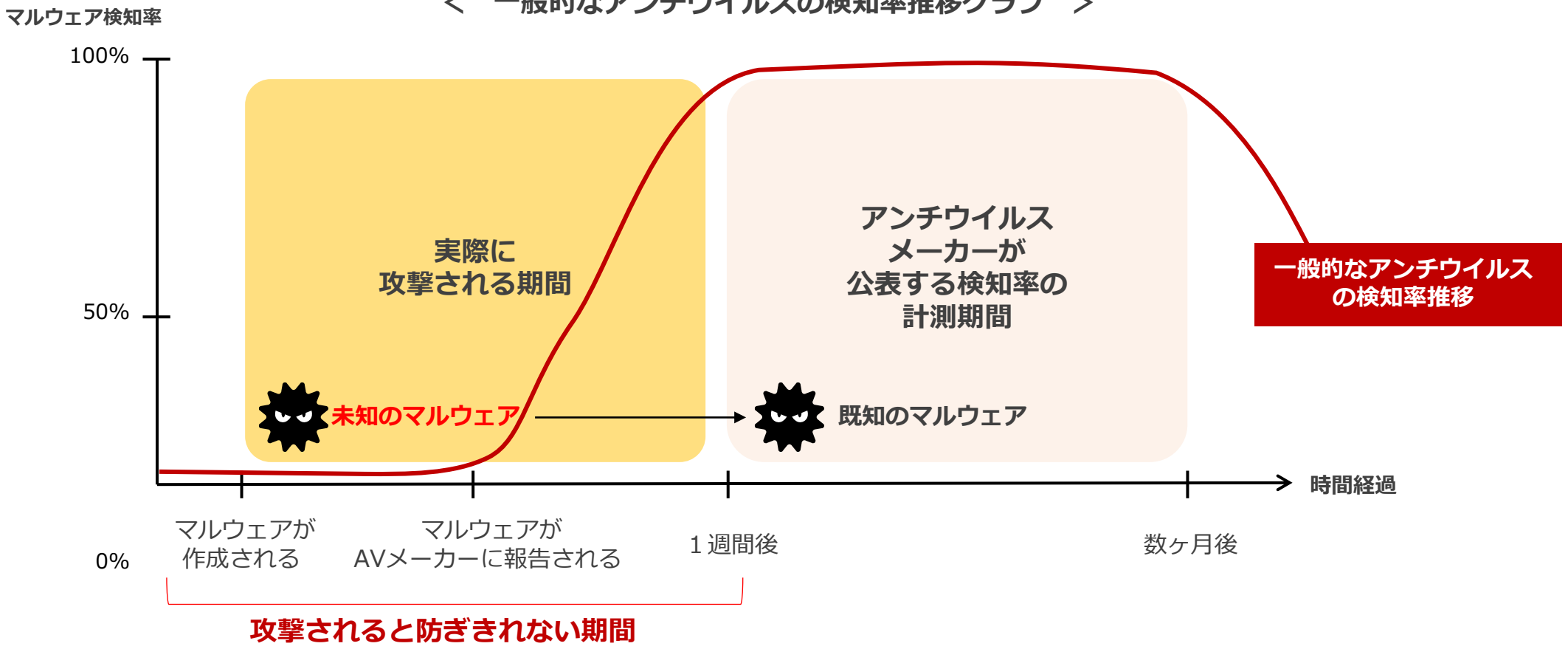
別の組織で再発見されるマルウェアは
たったの0.5%。つまり、同じマルウェアが
2度以上使われることはほとんどありません。
攻撃に使われる**マルウェアは、ほぼ”未知“であるといえます。**

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

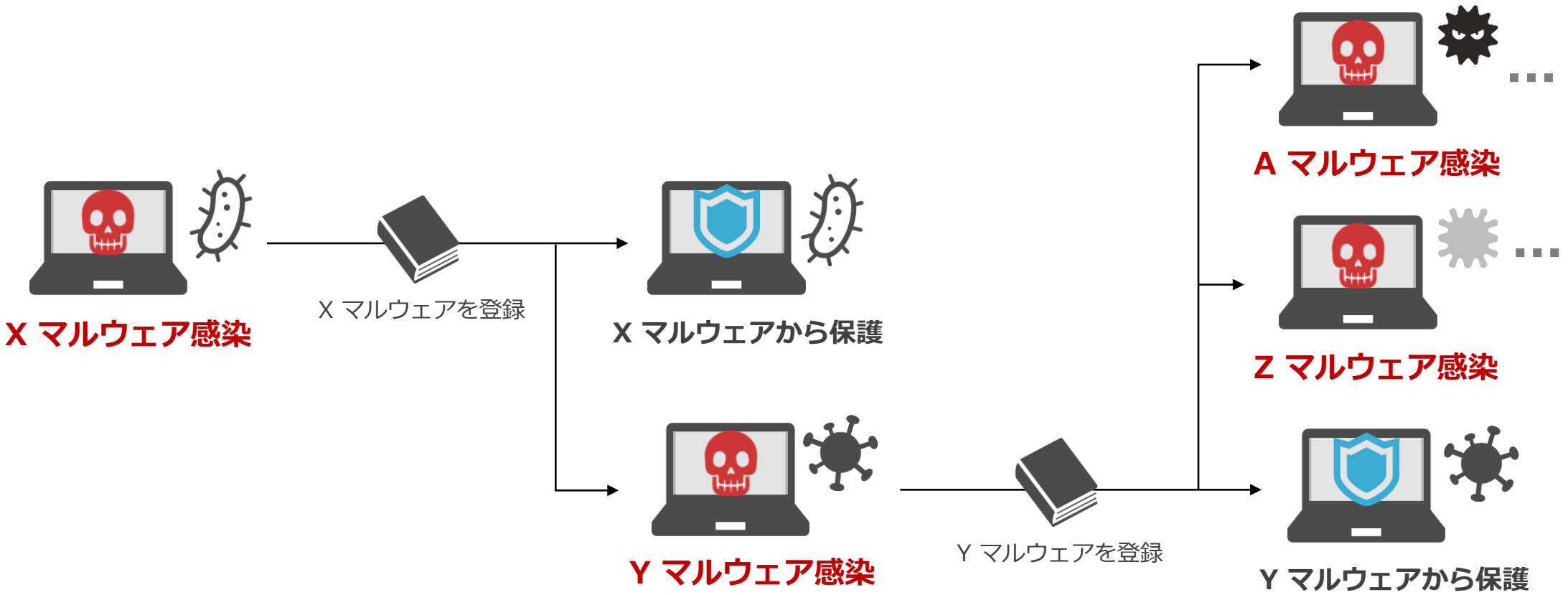
現在主流となっているやシグネチャ型は、攻撃を受けてからパッチを作成します。その間は攻撃を防ぐ手出てはありません

＜　一般的なアンチウイルスの検知率推移グラフ　＞



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



マルウェアに対抗するには高精度のアンチウイルスが必要

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

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

AI 型ウイルス対策ソフト「CPMS」とは

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

AI 型ウイルス対策ソフトは、なぜ検知精度が高いのか？

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「未知のマルウェア」を判定し、マルウェアが動く前に隔離を実施

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

【特徴点】

ファイルサイズ

アイコン

比較

セクションヘッダ

セクションデータ

文字列

etc…

膨大な特徴点から総合的に判断

ランサムウェアの可能性 99%

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

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™

- **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	・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

■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頂きます。
操作手順書などのマニュアルも
ご用意しています。

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	EDR
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	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	シグネチャ更新時

①運用がしやすい製品を選ぶ

ひと言で EDR といっても、製品によって機能・価格・契約形態・導入形態などはさまざまです。
例えば機能でいうと、**解析や調査に重点が置かれた EDR** もあれば、**アンチウイルスなどの機能と一体化させた防御に重点を置く EDR** もあります。
また、EDR からのアラートやインシデントレポートに基づいて、**実際に判断や対応をするのは社内の人間です。滞りなく運用できるようなサポート**はあるのか**サポートは無償なのか有償なのか**といったことも踏まえて、自社にとって運用のしやすい EDR を選ぶ必要があります。

②アンチウイルス製品と連携していること

すでに導入しているアンチウイルス製品のベンダーが提供する EDR 製品や EDR サービスを選ぶと、**アンチウイルス製品との連携も良く導入の負担を少なくすることが可能です。**また、EDR を含めたセキュリティ・プラットフォームを新たに導入するという方法もあります

③EDR 導入が向いている組織と向いていない組織

EDR の運用は一般的に難易度が高い傾向にあります。インシデントレポートを理解することができ、それをもとに適切な対策を練ることができる人材がいなければ、EDR を存分に使いこなすことはできません。 インシデント対応などの専門知識をもった人材を確保できる組織においては、EDR は極めて有用です。
逆にいうと、こうした人材の登用や育成を導入前に行なうことが困難だという組織は、EDR 導入には向いていないといえるでしょう。
もちろん万が一のときのために EDR は有効ですが、組織の体制やリソースが追いつかない状態で導入をしても思ったような効果は得られません。
まずはアンチウイルスで事前防御を万全に整えることが大切です。

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9月30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/