LANSCOPE
Cyber Protection

あなたのEDRの選び方、間違っています！

メーカーでは教えてくれないEDRの選び方

はじめに

近年、EDR（Endpoint Detection and Response）をご検討される企業様がさらに増えてきたと感じています。総務省から発行されているテレワークセキュリティガイドラインや2022年12月に公開された日本自動車工業会/日本自動車部品工業会の『自工会／部工会・サイバーセキュリティガイドラインV2.0解説書（初版）』などの各種ガイドラインでサイバー攻撃対策の一部として EDR が紹介されています。また、富士キメラ総研の「2022 ネットワークセキュリティビジネス調査総覧」によれば、EDR 市場に関して、2027年度には 510 億円の規模にまで成長すると予測し、2021 年度の実績と比較すると約 3.4 倍にまで達するとしています。また、既に大企業では EDR の導入が進んでいるため、今後は中堅企業への導入が進むと予想されています。

しかし、年々被害が増加するサイバー攻撃の対策として確かに EDR は効果的ではありますが、一方で EDR を導入したものの運用方法が分からず使いこなせていない、費用対効果を感じられていないという声も聞くようになりました。当然ではありますが、EDR を導入しただけでマルウェア対策ができるわけではありません。企業によっては、EDR と併せて EDR の運用を代行する Managed Detection and Response（以下、MDR）を検討する必要もあれば、そもそも EDR までは不要で次世代型アンチウイルス（Next Generation Anti-Virus、以下、NGAV）で事足りると判断されるケースもあります。自社にとって、どのようなマルウェア対策製品が必要なのかを見極める必要があります。

本ホワイトペーパーでは、「そもそも EDR とはどういう製品なのか？」から「EDR 製品の比較検討のポイント」、「EDR 利用実態調査」まで幅広く情報をまとめています。さらに、「自社に EDR が本当に必要なのか？」を確認できるフローチャートもご用意しています。

皆様が自社に最適なサイバー攻撃対策を検討するうえで、お役に立てば幸いです。

EDR とは？

- ウイルス対策ソフト（EPP）と EDR との違い
- EDR の導入効果
- EDR 製品を比較する時のポイント

ウイルス対策ソフト（EPP）と EDR の違い

EPP（Endpoint Protection Platform）

一般的に「ウイルス対策ソフト」と表現されることが多いです。

マルウェア感染防止に焦点を合わせた製品で、組織や企業のネットワークに入り込んだマルウェアを EPP が検知して、感染する前に隔離したり、不正なプログラムが実行されることを防ぐ機能が備わっています。従来型のウイルス対策ソフトは、あらかじめマルウェアのパターンをソフトウェアに登録しておき、侵入してきたマルウェアと照合して検知する方式が一般的でした。しかし近年では、**次世代型アンチウイルスソフト（NGAV）の登場により、未知のマルウェアも高い精度で検知ができるようになってきています。**

EDR（Endpoint Detection and Response）

マルウェア感染時の対処をサポートするための製品です。

どれほど検知率が高い EPP を導入していたとしても、マルウェアに感染するリスクを 0 にすることはできません。そこで、EDR ではログを取得することでマルウェアがどのように侵入してきたのか、原因特定をサポートします。ただし、EDR はマルウェアを検知したときに自動的に侵入経路の特定を行うわけではないため、マルウェアに感染してしまった端末が複数ある場合は全ての端末に対して手動で対応しなければなりません。感染が広範囲に及ぶとみられる場合は、EDR を利用した対応に多大な工数がかかる点には注意が必要です。

EPP は、侵入してきたマルウェアを阻止する
EDR は、マルウェア感染の原因を調査して復旧させる

EPP(ウイルス対策ソフト)＝マルウェアを阻止

ファイル防御 → 振る舞い防御

対象となる脅威や作業

ファイルスキャン
- ドキュメント
- マクロ
- スクリプト
- 実行ファイル

振る舞い防御
- インジェクション
- PowerShell 実行
- 権限昇格
- シェルコード実行
- ランサム動作

高精度にマルウェアの侵入を阻止することが重要

感染

EDR＝マルウェア感染の原因を調査・復旧

異常検知 → 封じ込め → 調査 → 復旧

イベント検知
- プロセス遷移
- 水平展開
- C2通信

感染端末の隔離
- ネットワーク隔離

イベント調査
- 侵入経路分析
- データ取得

デバイス復旧
- デバイス修復
- データ修復

その他の付帯サービス
- マネージドサービス（MDR）
- 脅威ハンティング
- 脅威インテリジェンス

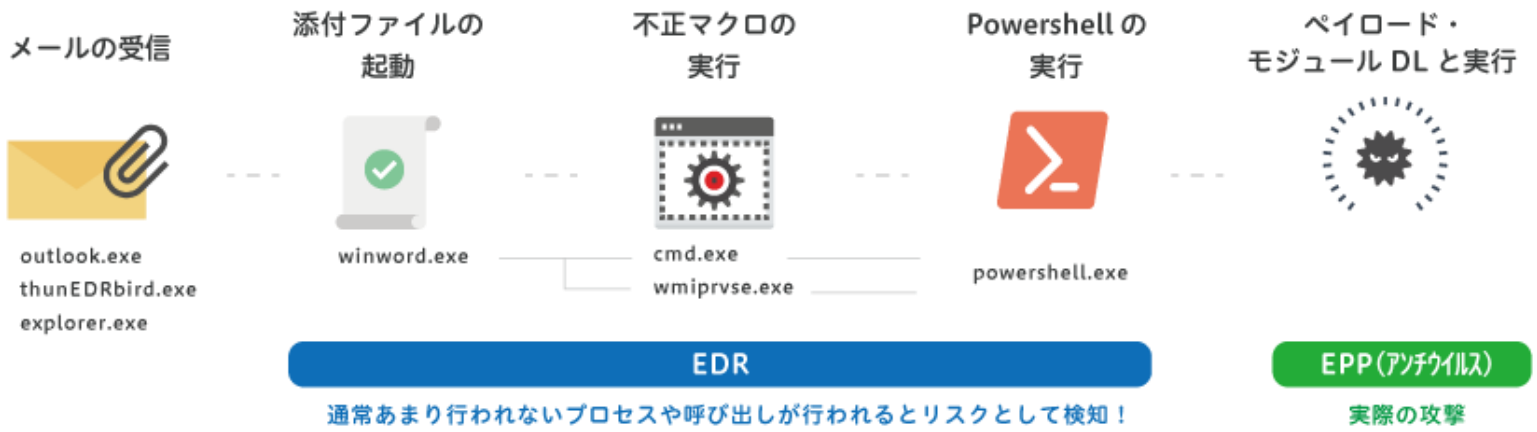
EPP ですり抜けたマルウェアに対して迅速に調査・解析し対処することが重要

EDR の導入効果

従来型のウイルス対策ソフトは、マルウェアなどのファイルそのものに対しての検知や、それらのファイルが実際に動き出す時にメモリにどのような形で命令を送っているのかをモニターして不正な動きを検知します。一方、EDR では、“攻撃そのもの“を検知することができます。例えば、ある巧妙な標的型攻撃を行う攻撃グループが、特に金融機関をターゲットにしているとします。金融機関でセキュリティを担当する部門側では、標的型攻撃の傾向を脅威情報として把握しておき、それを EDR で検知するポリシーをセットしておきます。このようにすると、**ウイルス対策ソフトでファイルを検知・駆除するよりも前の段階で、攻撃に気付くことができる可能性が高まります。**近年は、ウイルス対策ソフトで検知できない「未知のマルウェア」を使った攻撃が主流になっており、より EDR の重要性が高まっています。

標的型攻撃として猛威を振るったマルウェア「Emotet」も、巧妙な感染手法を実行し被害が拡大しました。具体的には、「取引先企業などを装ったメールを受信したユーザーが、添付ファイル（Office の Word など）を開き、開いたファイルで誘導されるボタンを押下するとマクロが有効化。その後、コマンドと PowerShell にてプログラムが実行され、攻撃本体のファイルをダウンロードして実行、マルウェアに感染」という流れが多いと言われています。**市場にある多くの EDR では、検知ポリシーが具体的になっており、上記の例では添付の Office ファイルからマクロが実行されたタイミングや、PowerShell の実行の内容から検知することが可能になります。**ちなみに従来型のウイルス対策ソフトでは、先に述べた通りファイルを検知対象の中心にしていることから、ファイルがダウンロードされる前の段階の攻撃などは、検知することができません。

■EDR の優位性（Emotet の攻撃の場合）



EDR 製品を比較する時のポイント

市場にリリースされている EDR 製品のどれもが、皆さまの組織に当てはまるとは限りません。他のソフトウェア製品やサービスと同様、いくつかの角度から比較検討が必要となります。特に EDR で何を中心にモニタリングしたいかを検討する必要がありますが、おおよそ検討のポイントは以下に含まれます。

● 導入関係

・EDR 導入に際し必要となるインフラはあるか（オンプレ型、アプライアンス型、クラウド型など）
・自組織で必要な OS に対するサポートがあるか
・エージェント展開の容易さ（Windows なら GPO、macOS なら Jamf、Linux なら Chef などが使えるか）、再起動の有無など
・エージェントの稼働負荷、容量、などが許容範囲か

●検知機能・精度

・EDR 製品にセットで提供されている EPP のマルウェア検知手法は、パターンファイルによる検知か、AI（人工知能）による静的検知か
・必要な情報が可視化されるか（プロセス、ネットワーク接続、ファイル変更、レジストリ変更、バイナリ、ユーザ情報、メモリ構造など）
・エンドポイントログはローカルのどこに（暗号化されて）保存されるか
・どのような種類の脅威が検知されるか（マルウェア、ファイル、PUP、不正利用など）
・脅威検索手法が豊富か（バイナリ検索、YARA などもあるか）
・検知精度や誤検知・過検知などの第三者評価などがあるか

●対策機能

・対策として隔離、ファイル削除、レジストリ削除、正常状態への復旧機能があるか
・上層部や報告先に求められるレポートが出力できるか
・自組織で使っている他製品と連携ができるか（トラッキング、SIEM、メールなど）
・ベンダーから提供されるサポート内容

EDR を導入すれば、ホントにランサムウェア対策できるのか？

- 近年のランサムウェア被害を振り返る
- EDR 利用実態調査

「ランサムウェアによる被害」が3年連続1位の結果に
大企業から中小企業に至るまで、規模に関係なく被害が発生している

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	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5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	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化（アンダーグラウンドビジネス）	NEW

※引用：IPA「情報セキュリティ10大脅威2023」

👉 今期のポイント

1位：「ランサムウェアによる被害」

2022年も、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：「サプライチェーンの弱点を悪用した攻撃」

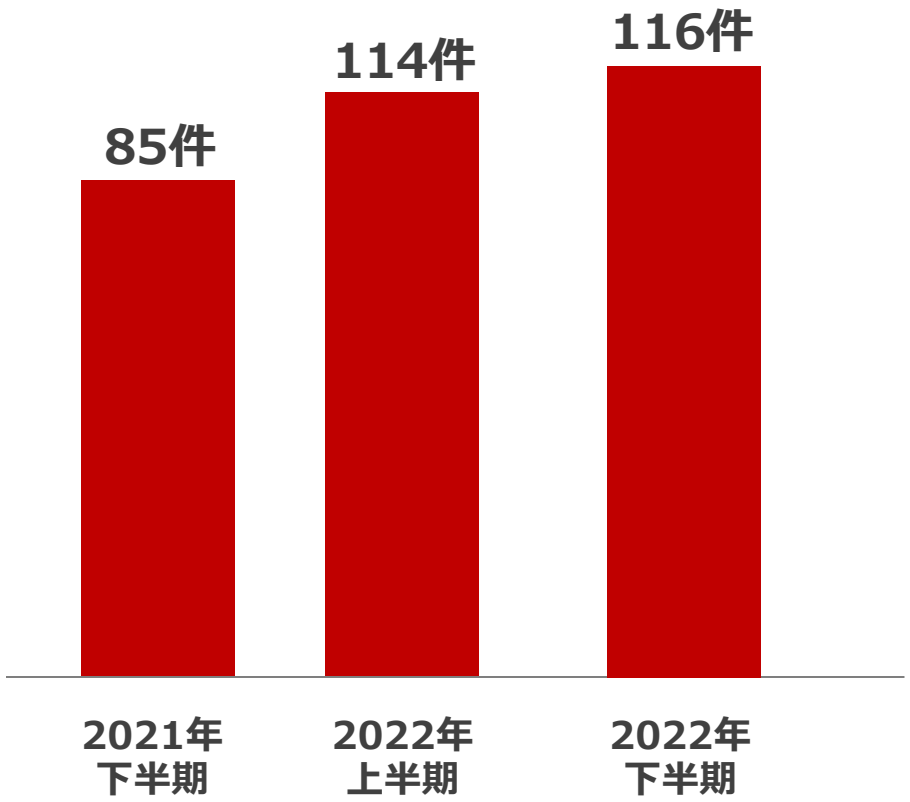
某大手製造業の取引先企業がマルウェア感染したことにより、工場の稼働が停止しました。取引先企業のネットワークを経由して被害に遭うケースが複数確認されています。

3位：「標的型攻撃による機密情報の窃取」

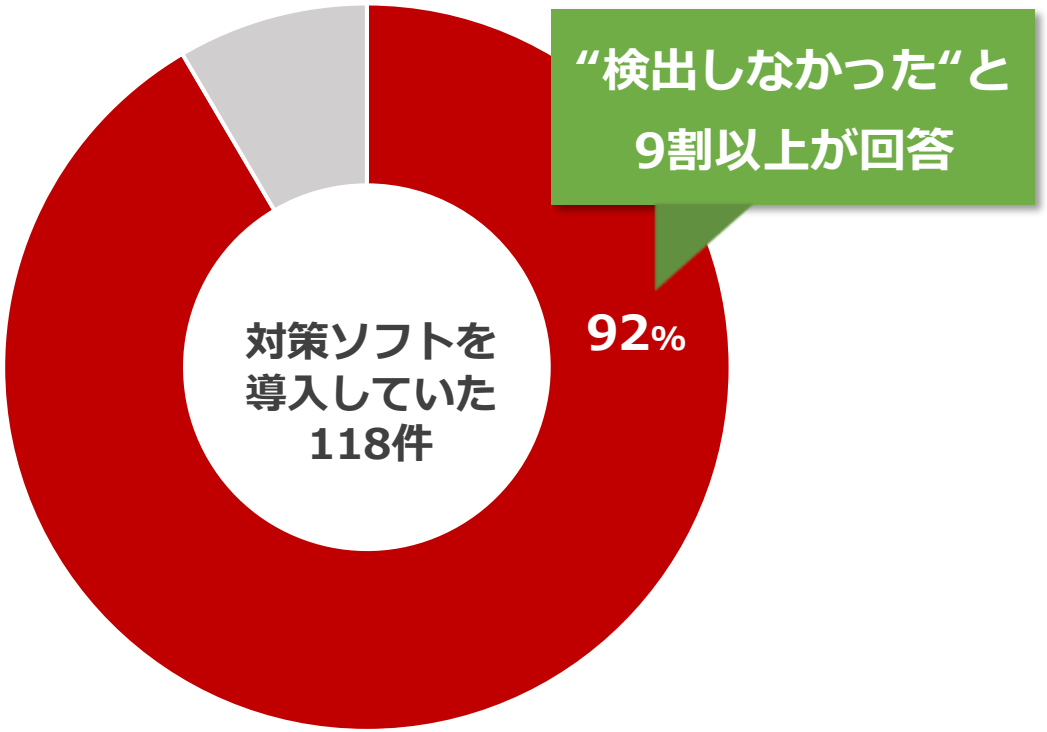
2022年3月、凶悪マルウェア「Emotet」が猛威を振るいました。JPCERT/CCによれば、攻撃が流行した2020年に比べ、2022年は5倍の被害を確認。また3月以降、定期的にアップデートも観測されています。

ランサムウェア被害件数は増加傾向
ウイルス対策ソフトを導入していたが、被害者の多くが“検出しなかった”と回答

■ランサムウェア被害の報告件数の推移※

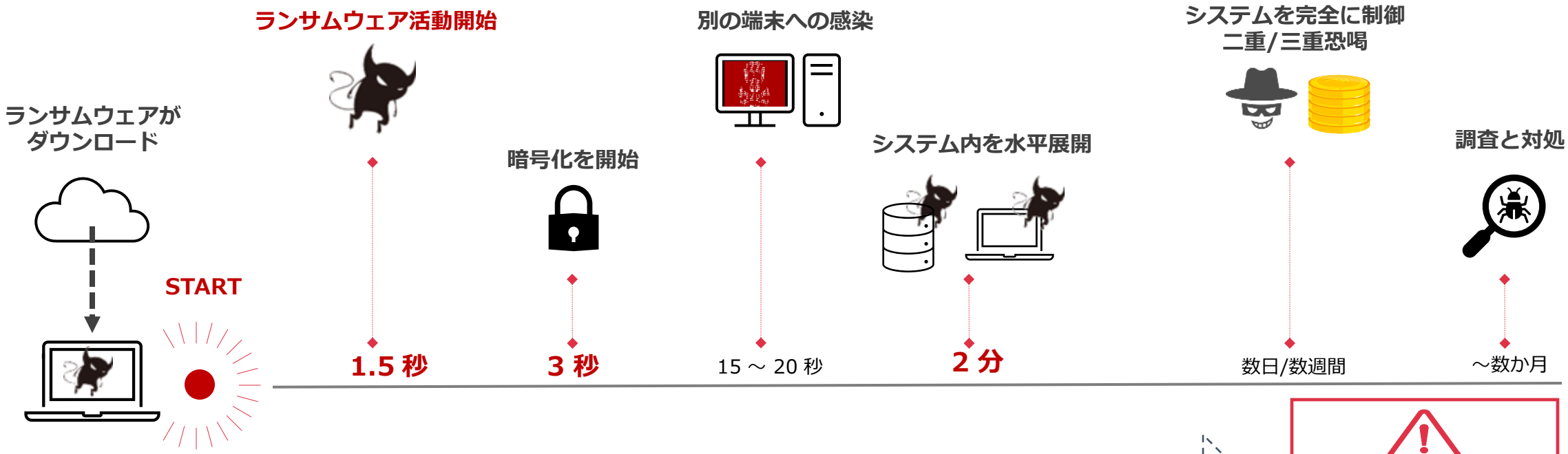


■ウイルス対策ソフトがランサムウェアを検出したか？※



※ 出典：警察庁 令和4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/R04_cyber_jousei.pdf

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、2 分後には全社に広がってしまう場合もある



【事件から見る】ランサムウェア感染は深夜・早朝に行われる

■某大阪府の病院

・給食の業務委託先を経由されて感染した可能性

・フォレンジック調査から、2022年10月31日**午前3時32分**に、何者かが、リモートメンテナンス用 VPN の脆弱性を突いて侵入

■某徳島県の病院

・2021年10月31日**未明**：院内の複数のコピー機からデータ窃取、暗号化した内容の文書が大量に印刷される
・0時30分：電子カルテの不具合を確認。システム担当者に連絡
・3時00分：システム担当者が到着後、電子カルテのネットワークを遮断。
・8時00分：ランサムウェアの感染を確認

■某運送業

・7月9日 **23時頃**：職員がファイルサーバー上のファイルに異常を確認
・7月10日未明：ファイルサーバー、及びバックアップサーバーに格納された全てのファイルにアクセス不能

深夜・早朝に EDR からアラートが検出されても
即座に被害拡大を阻止することは困難

Splunk が 10 万ファイル（約54GB）の暗号化速度を検証

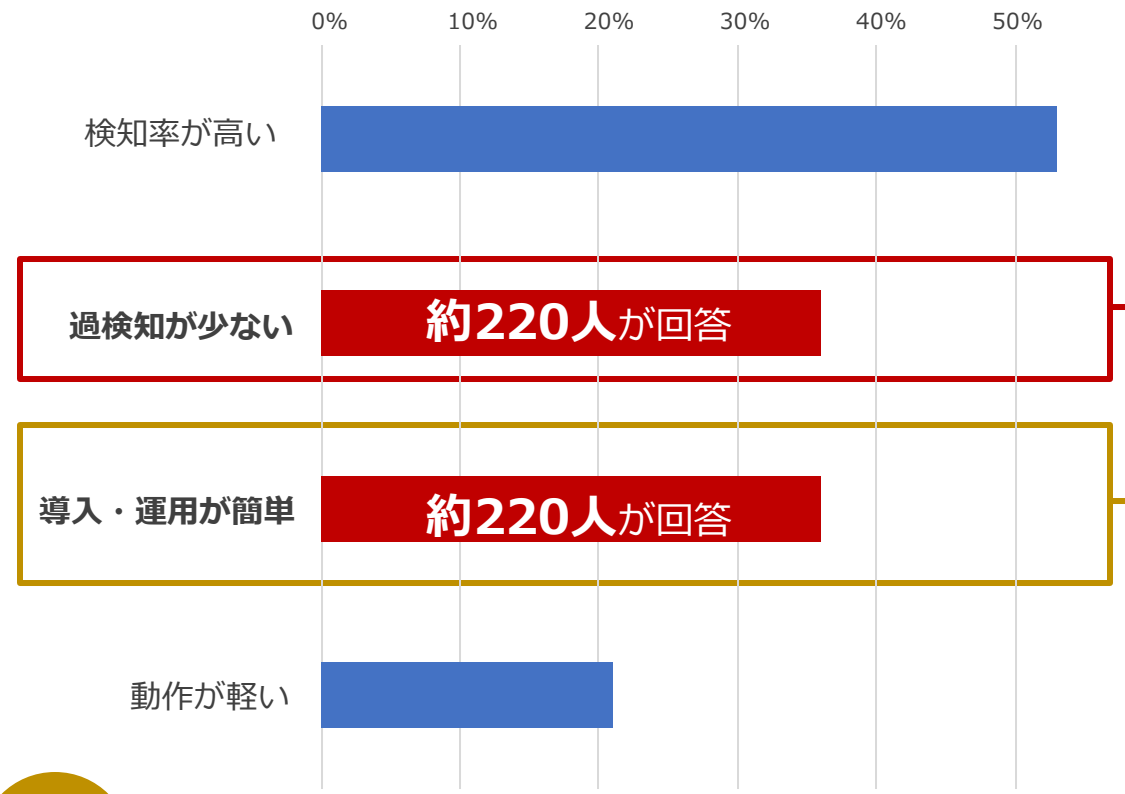
短時間でファイルが暗号化されるため、ランサムウェアが動く前に止めることが重要

ランサムウェアファミリー	暗号化にかかった時間
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	**00:42:52**

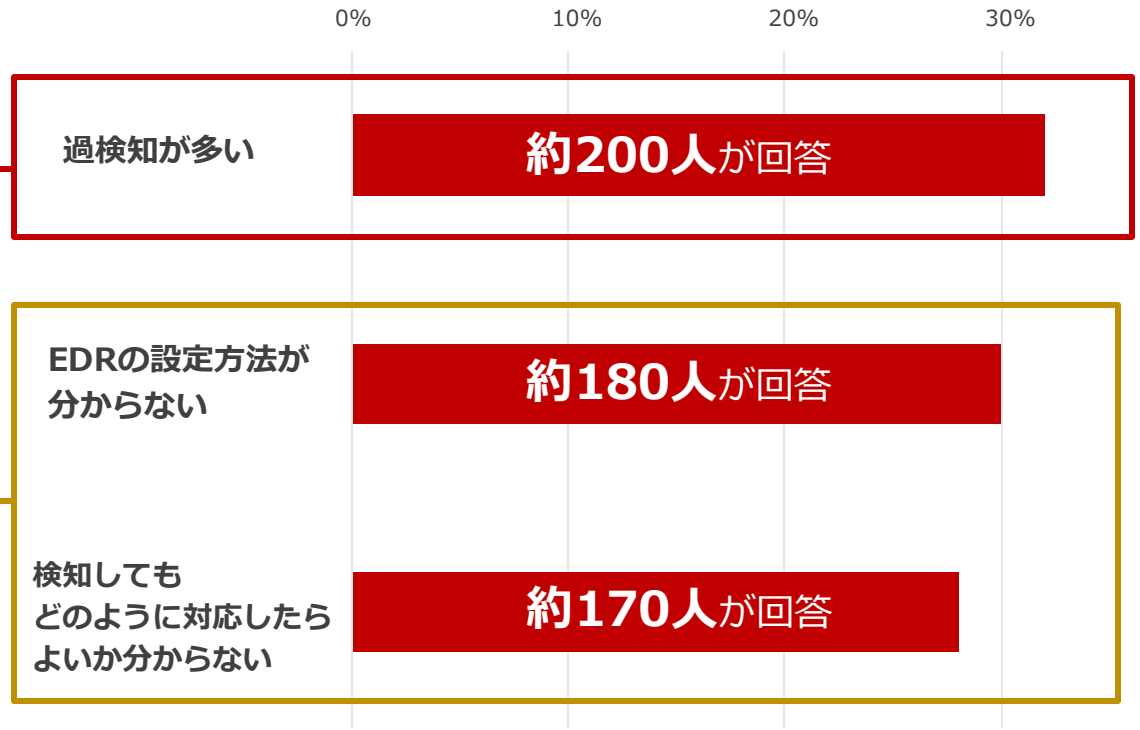
出典：Splunk：Ransomware Encrypts Nearly 100,000 Files in Under 45 Minutes を基に MOTEX で作成

【EDR 利用実態調査】EDR 導入前と導入後のギャップ

EDR を導入した理由を教えてください ※複数回答可
（有効回答数：618）



EDR 運用で困ったことを教えてください ※複数回答可
（有効回答数：618）



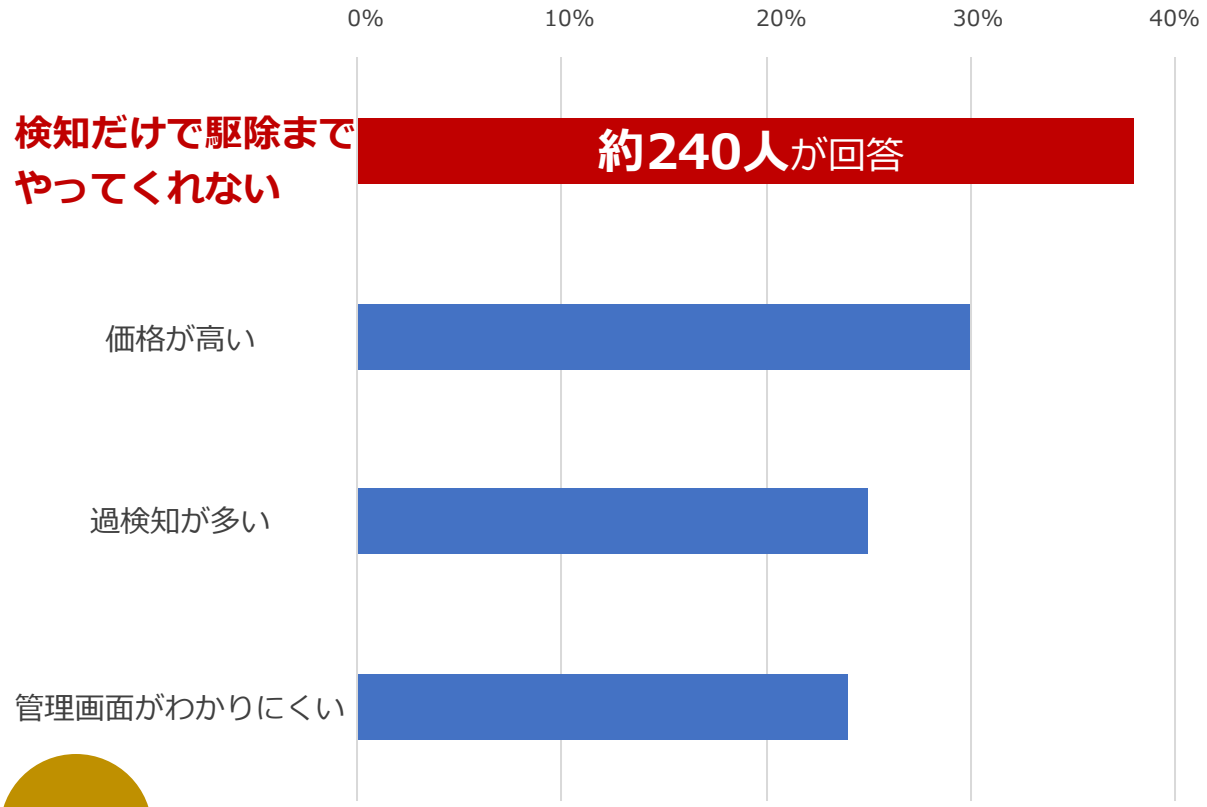
※ EDR 利用実態調査（調査期間：2022年11月15日～16日・2022年12月2日）
ゼネラルリサーチ株式会社が従業員数 300～5,000 名規模の企業に所属している情シス担当者に調査

Point!

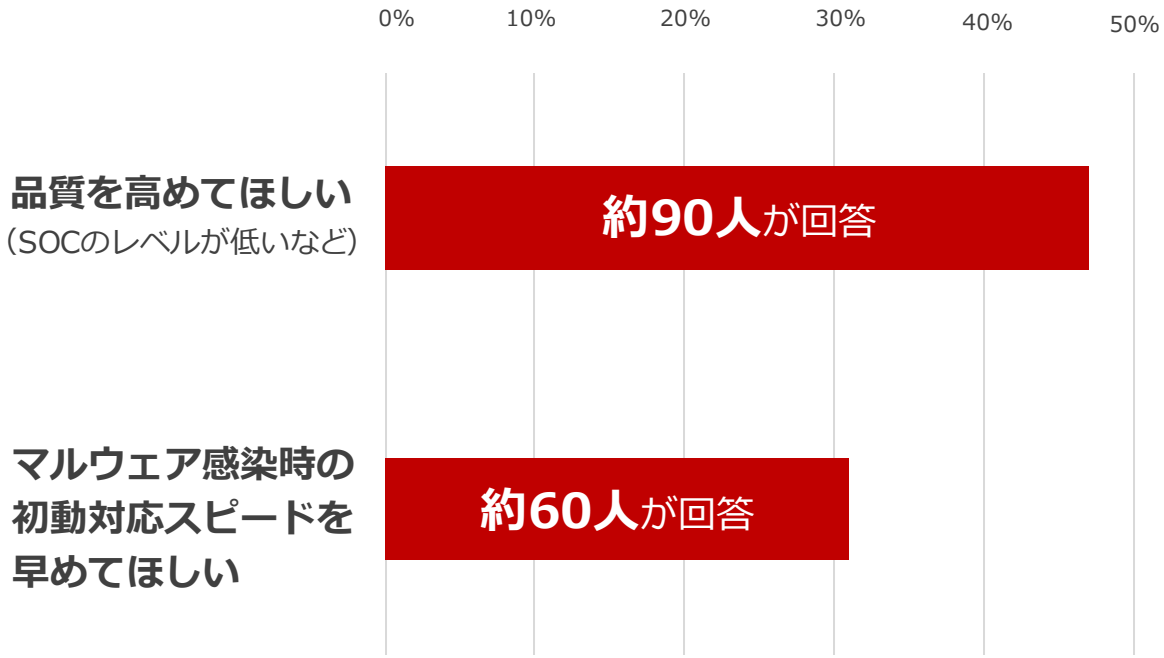
情シス 1,000 人に EDR 利用実態調査を行い、「導入理由」と「運用で困ったこと」を調査しました。結果、当初は「誤検知が少ない」、「導入・運用が簡単」と思い導入したものの、実際に運用してみると過検知が多かったり、運用方法が分からないといった声が多く集まりました。**EDR の運用は難易度が高く、効果的に運用するにはサイバーセキュリティに詳しい人材を確保する必要があります。**

EDR は「マルウェアを駆除するツール」ではない

EDR の改善してほしいところを教えてください ※複数回答可
（有効回答数：618）



SOC サービスについて改善してほしいところを教えてください
※複数回答可（有効回答数：197）



※ EDR 利用実態調査（調査期間：2022年11月15日～16日・2022年12月2日）
ゼネラルリサーチ株式会社が従業員数 300～5,000 名規模の企業に所属している情シス担当者に調査

Point!

EDR の改善点についても調査したところ、「過検知が多い」、「管理画面が分かりにくい」などの意見が寄せられました。特に目立ったのが**“検知だけで駆除までやってくれない”という回答です。**そもそも EDR は「マルウェアを駆除するツール」ではないため、誤って認識されているように見受けられます。また、EDR のオプションとして提供されている **SOC（MDR）の品質についても不満の声が見られました**。

EDR 導入を検討する際に押さえておきたいポイント

- EDR の運用には、セキュリティに詳しい人材が必要
- EDR だけでなく、高い検知率を誇る NGAV を導入し感染を未然に防ぐことも重要
- MDR を検討する際は、必ず運用担当者のスキルを確認
- EDR は「全ての企業に最適なマルウェア対策」ではない各企業で「適したマルウェア対策」の形は異なる

【フローチャートで見る】自社にあったマルウェア対策とは？

EDR を運用できる人材が自社にいるか

Yes → **EDR を導入**

EDR から通知されるアラートや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 を運用することは困難です。 一方で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であれば、EDR は極めて有用です。

MOTEX では EDR 製品として、CylanceOPTICS※ をご提供しております。

※ CylanceOPTICS を購入するには、CylancePROTECT の導入が必要です

No ↓

MDR を検討できるか

Yes → **MDR を導入**

EDR の運用代行として MDR を提供しているベンダーもあります。24時間365日、自社が攻撃されていないかの監視を代行し、ポリシー設定のチューニングなども行います。

MOTEX では MDR サービスとして、CylanceGUARD をご提供しております。

No ↓

検知力の高い NGAV を導入

EDR を運用できる人材がいない、予算的にも MDR の導入が難しい場合には、高精度にマルウェアを検知する次世代型 AI アンチウイルスソフト（NGAV）をご検討ください。

MOTEX では 次世代型 AI アンチウイルスソフト（NGAV）として、CylancePROTECT deep instinct をご提供しております。

未知・亜種のマルウェア感染から 99%※ 防御
AI を活用した高精度のマルウェア対策製品を 2種類ご用意しています

LANSCOPE Cyber Protection

— *Product 1* —

CylancePROTECT® CylanceOPTICS® CylanceGUARD®

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

— *Product 2* —

deep instinct™

誤検知が少ない

※CylancePROTECT：2023年3月　Tolly 社 のテスト結果より

※Deep Instinct：Unit221B　社調べ

LANSCOPE サイバープロテクションは 2 種類のマルウェア対策製品から、用途に応じて選択いただけます

多くの導入実績と EDR・MDR が利用可能

CylancePROTECT
CylanceOPTICS
CylanceGUARD

- **EDR 要件**への対応をお求めのお客様
- **EDR の運用を外部に任せたい**とお考えのお客様
- **インターネット非接続環境**※での運用をお考えのお客様

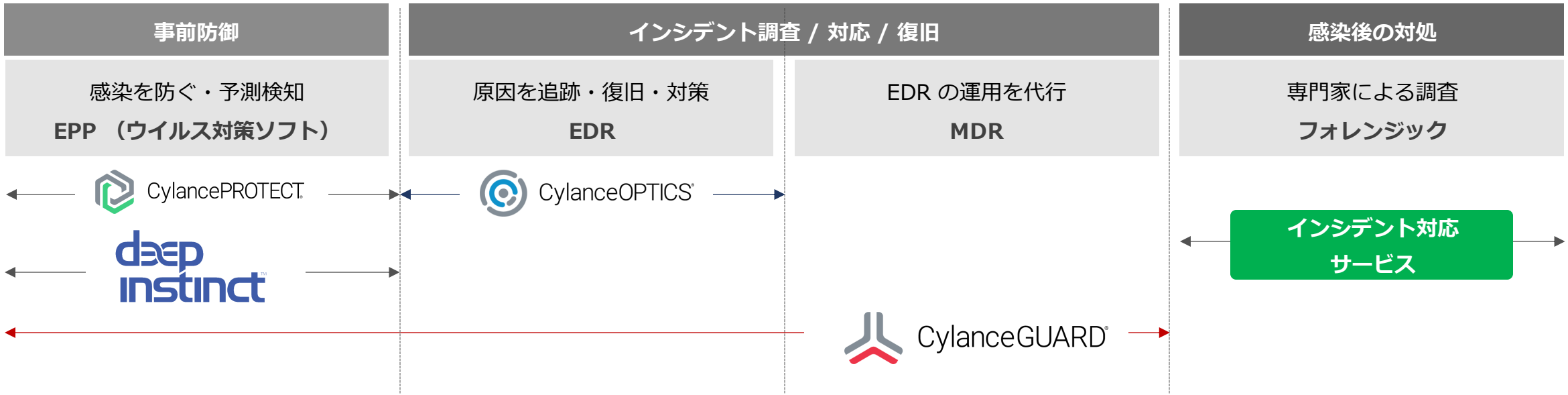
※インターネット非接続環境での利用は CylancePROTECT のみ可能

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

マルウェア感染対策～被害発生時の調査・分析まで
MOTEX が、まとめてご支援できる体制をご用意しています



▼こんなお客様にオススメ

限られた予算で高精度に防御したい	EDR を導入して感染原因を調査したい	EPP・EDR・MDR をまとめて導入したい
CylancePROTECT / deep instinct	CylanceOPTICS ※	CylanceGUARD

※ CylanceOPTICS を購入するには、CylancePROTECT の導入が必要です。

次世代型 AI アンチウイルス「CylancePROTECT」

- CylancePROTECT
- CylanceOPTICS（EDR）
- CylanceGUARD（MDR）

CylancePROTECT

未知・亜種のマルウェアもマシンラーニングで 99%※ 検知！次世代のアンチウイルス

次世代型AIアンチウイルス

CylancePROTECT

AI を活用したマシンラーニングによる予測検知が可能で、未知・亜種のマルウェアも 99%※ の高検知が実現。別途オプションの OPTICS（EDR）で感染原因の調査も可能

- AI による高精度な予測検知
- パターンファイルを使っていないので日々のアップデート不要
- 過検知が少なく低負荷

※2023年3月 Tolly社のテスト結果より

CylancePROTECT

数理モデルに基づくアプローチ！人工知能が未知のマルウェアを動作前に防御

検知の高さはもちろん、パターンファイルを使っていないのでアップデートの手間・クライアント負荷がありません

DNA レベルの
マルウェア解析

AI（人工知能）
による自動判断

パターンファイルを使っていないため
毎日のアップデートが不要

CylancePROTECT

未来に発生するマルウェアを予測して 99% 検知！あらゆる未知・亜種のマルウェアから保護

CylancePROTECT の検知方式は、**2年ほど前の過去の検知エンジン**でも、未知のマルウェアを予測検知しています

CylancePROTECT

LANSCOPE
Cyber Protection

powered by CylancePROTECT

次世代型 AI アンチウイルス

CylancePROTECT が

- 5L から購入可能
- 月額￥450～/年額¥5400~
- 選べる「運用代行オプション」
- 選べる「レポートオプション」

CylancePROTECT

企業のニーズに併せて必要なプランを選択可能

基本ライセンス　年額 5,400 円 or 月額 450 円※

●CylancePROTECT

AI を活用した高精度のマルウェア検知・隔離機能をご提供

●初期運用サポート

CylancePROTECTの製品概要や導入手順などを説明
（画面共有で約1時間）

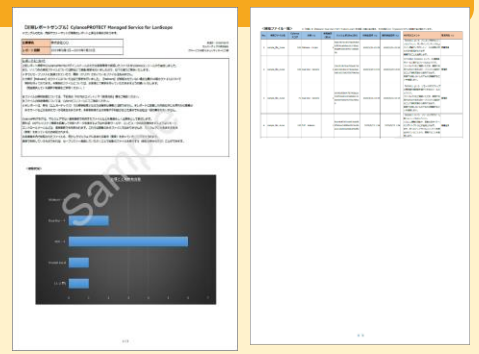
●保守サービス

製品に対する保守サービス対応
受付時間：月~ 金 9:30 ～ 12:00 ／ 13:00 ～ 17:30
（土日祝日年末年始および当社規定の休日を除く）
・専用Webサイトのご利用　　・最新バージョンアップ
・専用ヘルプデスクサービス　・その他サポート

※最小購入ライセンスは5ライセンス～になります。

定期レポート（オプション） 年額 960 円 or 月額 80 円

年に4回（利用期間開始（更新）後、3・6・9・12ヶ月目）、マルウェア検知結果のサマリーレポートを提供



運用代行（オプション） 年額 2,040 円 or 月額 170 円

お客様に代わって、エムオーテックスの技術者が CylancePROTECT の運用作業を代行します。

CylanceOPTICS

AI アンチウイルスに統合された「防御にフォーカスした」負荷の少ない EDR※

AI による未知のマルウェア 99% の高検知のため、後工程が最小限で済むため管理者の手間が少ない事が特徴です

攻撃防御 → 継続監視 → 自動対処 → 脅威ハンティング（ InstaQuery ） → 関連情報の入手（ FocusData ）

CylancePROTECT ← CylanceOPTICS →

CylancePROTECT と統合　AI を活用　予防にフォーカス

●分散型モデルによるイベント情報収集　●根本原因分析による侵入経路特定　●隠れた脅威の発見

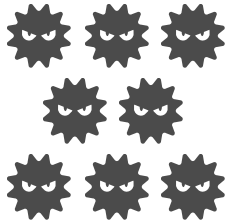
●脅威の封じ込めによる被害の最小化　●端末挙動からの動的な脅威検知と対処

※CylancePROTECT の有償オプション
※価格：年間 ¥1,800/台

CylanceOPTICS

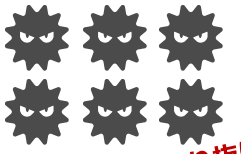
CylancePROTECT によりマルウェア感染を 99% 防御することで 管理者の運用工数を大幅に軽減することが可能

一般的なEPP＋EDR（従来の EDR 製品）



一般的な EPP

パターンファイル型や
サンドボックス等の動的検知

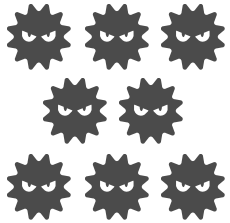


パターンファイルでは
防ぎきれない

一般的な EDR

検知イベントすべてに対処
管理者の運用負担増

CylancePROTECT + CylanceOPTICS



CylancePROTECT

AI を活用した機械学習が
導き出したアルゴリズム

検知率 99% で
予測防御

CylanceOPTICS

すり抜けは 99% 無し
管理者の運用負担が少ない

CylanceGUARD®

世界トップレベルのセキュリティ専門家による MDR サービス
AI アンチウイルス・EDR・導入支援・MDR をオールインワンでご提供

CylanceGUARD®

CylancePROTECT	CylanceOPTICS	ThreatZERO	MDR
			
高性能 AI により 99% マルウェアを防御	マルウェアの侵入経路を特定 再発防止策の検討に	PROTECT・OPTICS の 有効な使い方をレクチャー	セキュリティ専門家が 24時間365日監視

※ CylanceGUARD の価格は営業までお問い合わせください

CylanceGUARD®

世界トップレベルのセキュリティ専門家が 24時間365日サポート
スキルが高いため応答時間も迅速、お客様へのサポートも手厚いのが特長です

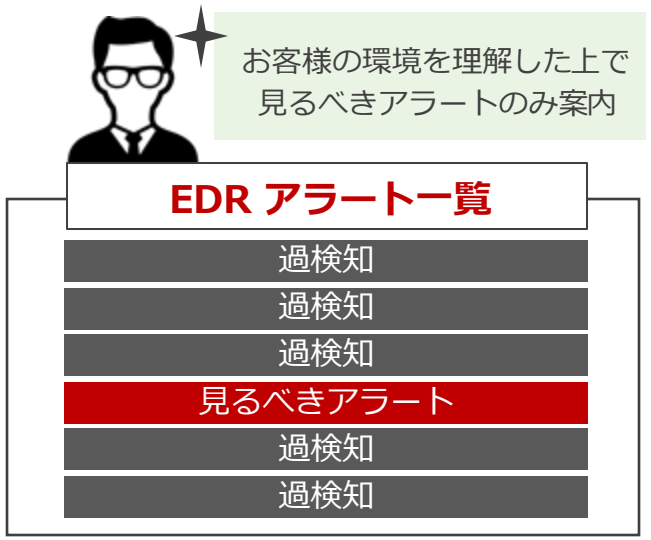
高いスキルを持ったメンバーが対応

サイバーセキュリティの修士号を
対応メンバー全員が取得

DEFCON29 OpenSOC※①
優勝メンバーが対応

お問い合わせに迅速に応答

見るべきアラートのみ案内

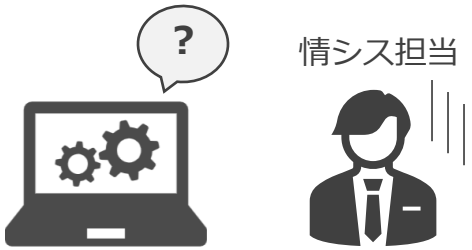
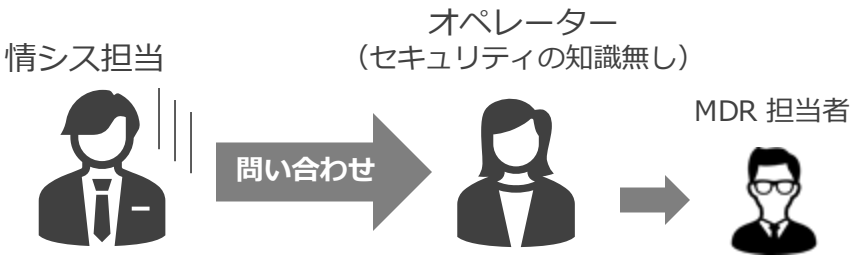
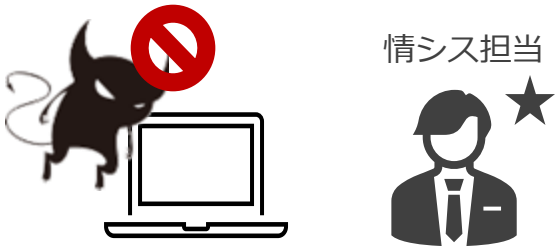
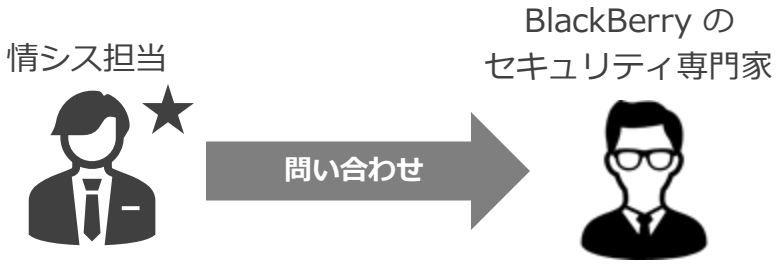


※① DEFCON29 (2021) OpenSOC とは、世界的に有名なハッキングに対する SOC コンテスト
※② 2023年6月時点。 SLO は60分

【機能別に見る】CylanceGUARD と一般的な MDR との比較

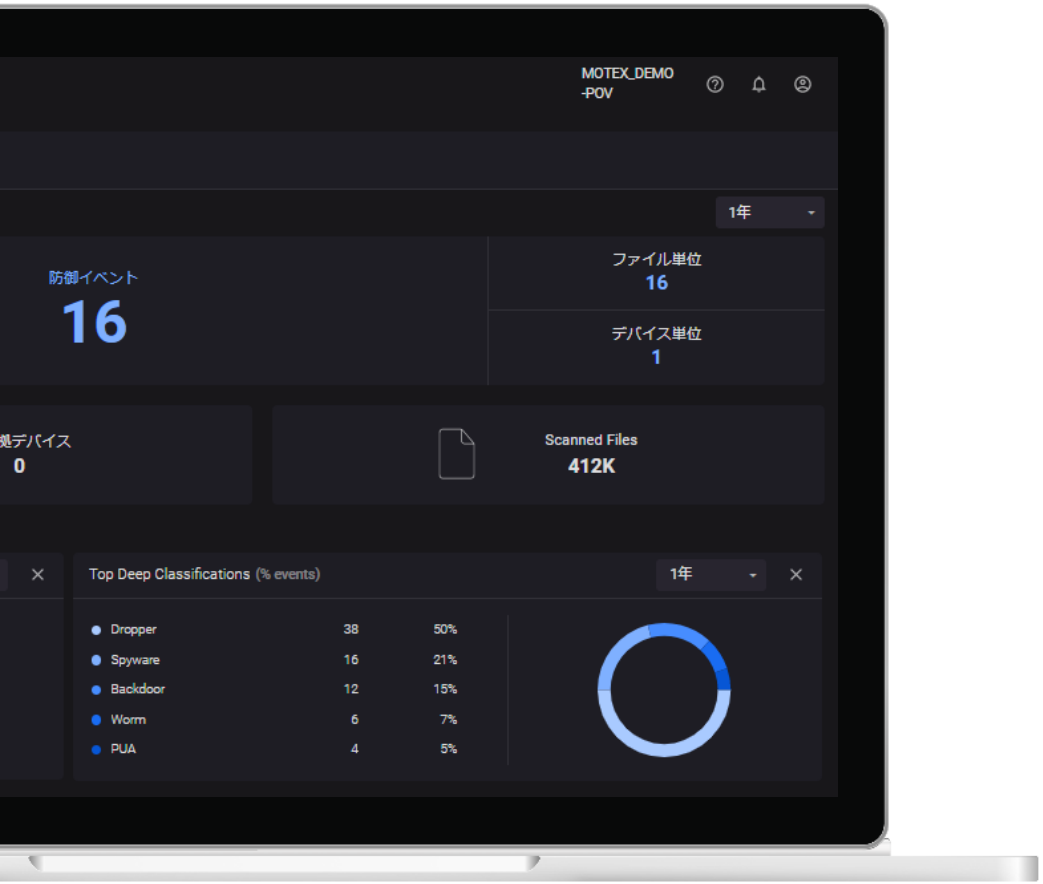
CylanceGUARD®

■一般的な MDR の場合（アンチウイルスソフト・EDR・MDR をセットで提供）

アンチウイルスソフト	EDR	MDR
		
検知方法がパターンファイルのため 未知・亜種のマルウェアに対抗できない	過検知が大量に通知。MDR を契約していても アラートを知らせるだけで対処方法が不明	オペレーター経由で MDR 担当と連絡を取る必要があり、 緊急時において迅速な対応ができないケースも
CylanceGUARD® の場合 		
この時点で 99% 防御を実現 未知・亜種のマルウェアから高精度に防御	**セキュリティ専門家がお客様環境を 理解した上で、見るべきアラートのみを通知**	**専用のポータルサイトから問い合わせをすることで直接 セキュリティ専門家に連絡が可能。平均応答時間は9分**

次世代型 AI アンチウイルス「Deep Instinct」

ディープラーニングをサイバー攻撃対策に活用した第3世代型ウイルス対策ソフト



次世代型 AI アンチウイルス

deep instinct™

- 未知の脅威を予防
- AI による自律性で人手やスキルに頼らない
- OS に依存しないマルチデバイス対応

元イスラエル国防軍サイバーセキュリティ出身者が設立したアンチウイルスベンダー

世界でいち早くディープラーニングに注目しサイバー攻撃対策に活用

社名	ディープインスティンクト株式会社
代表者（CEO）	Lane Bess
設立年	2015年
本社所在地	ニューヨーク
日本法人所在地	東京
従業員数	300名

https://www.deepinstinct.com/ja

👉 Point

▼デロイトトーマツ社「Technology Fast 500 2021 NORTH AMERICA」にて28位と急成長中の企業
▼海外でも多くの企業が Deep Instinct を導入している

ディープラーニングをサイバー攻撃対策に活用した OS を問わないサイバーセキュリティ

1．マルチ OS 対応

Windows, iOS, Android, macOSに対応

2．ゼロディ脅威の防御（ディープラーニング）

未知の脅威を予防できる

PE 以外の様々な脅威にも対応

3．運用コストが低い

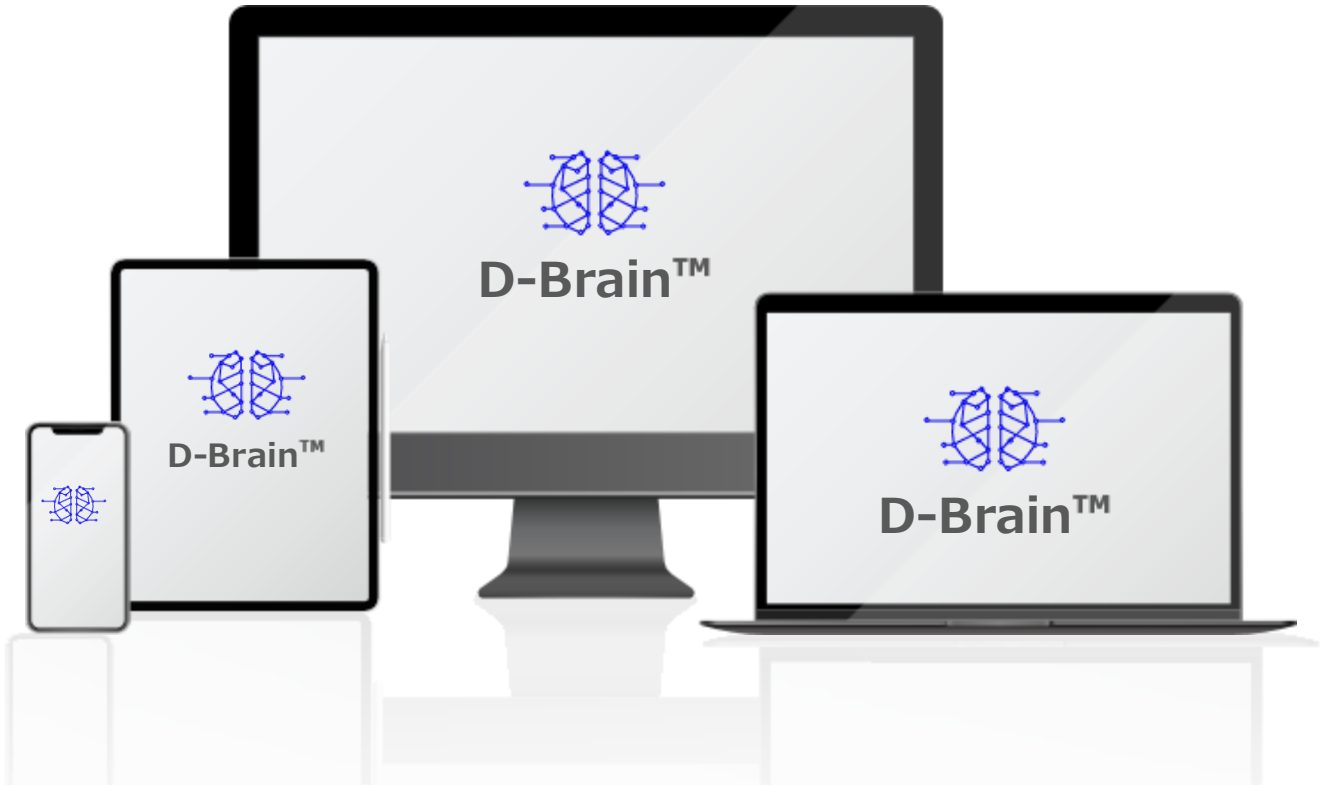
誤検知が少ない

リソース消費が少なく軽い

毎日のアップデートやフルスキャン不要

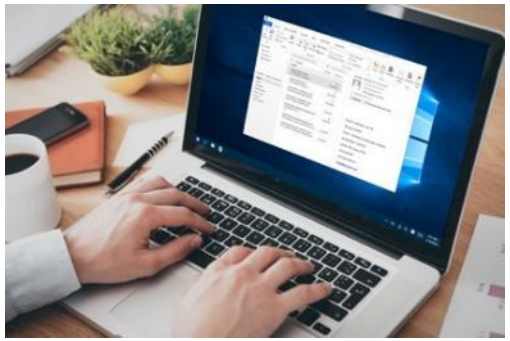
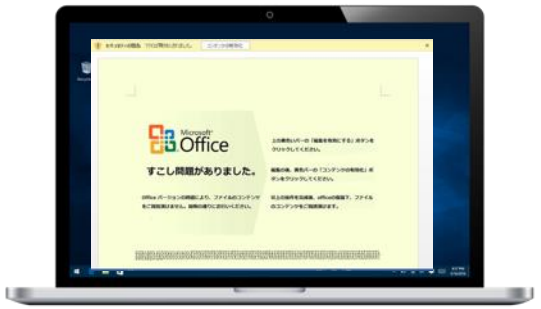
オフラインでも動作*

※インストール時にはインターネット接続が必要です
※バージョンアップ時もインターネット接続は必須です
※インターネット非接続時の設定変更とログ確認は不可



Emotet などのファイルレスマルウェアにも Deep Instinct は有効
4つの AI が各 STEP で防御！1つ抜けられたとしても次の AI が止める！

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**	**悪性 VBA マクロや PowerShell を検知** ＋振る舞い検知も可能	**ダウンロードされたマルウェアを隔離**

従来型のウイルス対策ソフトや EDR とは一線を画する性能
Deep Instinct が、あらゆる凶悪マルウェアから企業を守ります

未知の脅威を 99%※予防

こんな企業様にオススメ！

- □ シグネチャ型では**限界**を感じている
- □ **セキュリティに詳しくないけど**
  最新のマルウェアは防ぎたい！
- □ **安価**で強力な製品を導入したい！

※Unit 221B 社調べ

AI のアップデートは年1回ほど

こんな企業様にオススメ！

- □ 導入中のウイルス対策ソフトの
  シグネチャ更新管理に疲弊している
- □ **フルスキャンが PC やアプリの**
  動作を妨げている

少ない誤検知

こんな企業様にオススメ！

- □ **EDR やウイルス対策ソフトの**
  誤検知の多さに消耗している
- □ 誤検知したファイルのセーフリスト
  登録に工数を掛けたくない！

PC・スマホを一元管理

こんな企業様にオススメ！

- □ **管理 OS が多岐に渡るため**
  アンチウイルスも一元管理したい
- □ **最近、スマホのマルウェア感染も**
  気になってきた

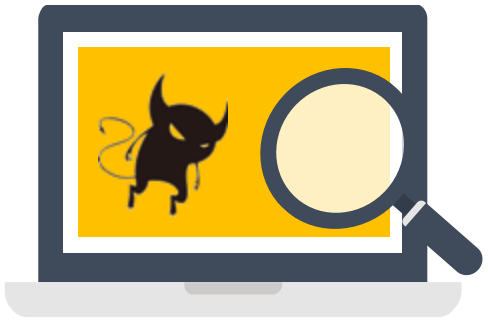
インシデント対応サービス

インシデント対応サービスは、CylancePROTECT や Deep Instinct 未導入のお客様でも購入いただけます。

『感染端末』や『感染のおそれがある端末』に対してフォレンジック調査が可能
また、被害の調査方針や対策方法などのアドバイスを実施します

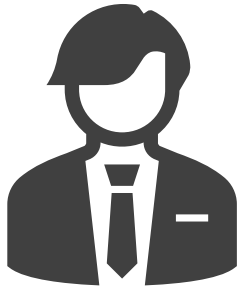
フォレンジック調査

端末調査
（Windows・macOS・Linux に対応）



通信ログ調査
（オプション）

インシデント対応アドバイザリ
（オプション）



※ 本サービスでは、マルウェアの動的・静的解析は行いません。
※ macOS の調査は環境により対応しかねる場合がございます。
※ 通信ログ調査は、ネットワーク機器側で過去 30 日程度の通信ログを保管している場合のみ実施できます。
※ 価格については営業までお問い合わせください。

収集データから攻撃の痕跡を調査し、インシデントの原因究明をご支援
特定した痕跡情報から対策などを含めた報告書も作成します

項目	内容
対象端末	Windows / macOS / Linux 端末
調査対象	ヒアリング結果に応じて、以下等のデータを調査対象とします。また、状況に合わせて、別の調査手法をご提示します。 **■端末調査（標準）** （1）端末：ディスク、メモリ、ツール実行結果 （2）各種機器：資産管理ツールの操作ログ、セキュリティ機器のアラート(EPP / EDR / IDS / IPS) **■通信ログ調査（オプション）** （3）通信機器(FW / Proxy / VPN 機器等)：通信ログ、アクセスログ、認証ログ
調査内容	保全作業後、収集データに対し【侵害の痕跡 / 侵入原因 / 感染拡大 / 情報漏えいを示唆する痕跡】を調査・分析します。 調査対象 (1) (2) が全て揃わない場合や情報欠落している場合など、情報漏えいや感染拡大等の影響特定に至らない場合があります。
調査手法	ファイルシステム調査、タイムライン調査、カービング調査、メモリ解析、各種ログ調査、マルウェア簡易調査（ IoC 調査）
調査期間	保全作業後、最短 15 営業日～/台 で報告書提出 ※ 弊社にて調査対象データ受領後に必要な期間です。調査量等に応じて変更する場合があります。
報告・提供物	調査中に情報漏えい等の重大な事実の痕跡が確認された場合、暫定対策に活用できる痕跡が確認された場合（不審な通信先、ハッシュ値等）は随時ご報告差し上げます。また、最終報告として調査結果報告書の提出及び報告会を実施いたします。

国家資格を保有する経験豊富なセキュリティエンジニアが
インシデントの調査方針や対策方法などをアドバイスいたします

項目	内容
概要	定期的なインシデント調査のお打ち合わせに参加し、対応方針などをアドバイスさせていただきます。
期間	別途お見積り ※ 弊社営業日の日中の対応となります
要員	情報処理安全確保支援士（国家資格）保有メンバー
内容	・ 原因究明に向けた技術アドバイス ・ インシデント終結に向けたロードマップ提案および推進のアドバイス ・ 暫定対策、対処へのアドバイス ・ インシデント対応後の恒久対策のアドバイス
備考	・初動/封じ込め等の対応は、適宜リモート会議を開催 ・状況確認等の定期的な会議体は、1時間程度/回のリモート会議を想定

※ 本サービスには、フォレンジック調査は含みません。

各種ご案内

両製品とも無料体験版をご用意しています！
無償で操作方法のレクチャーや疑問点にお答えしますので、ぜひお試しください

CylancePROTECT

CylanceOPTICS

▼体験版のお申し込みはこちら

概　　要	キャンペーン期間中、CylancePROTECT・OPTICSがライセンス数無制限でお試しいただけます。また、検知したファイルについて希望者の方に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	CylancePROTECT・OPTICS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

deep instinct™

▼体験版のお申し込みはこちら

概　　要	Deep Instinctが 100ライセンスまで、1ヶ月間無料でお試しいただけます。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。体験中のお問い合わせ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

製品について詳細な説明を聞きたい場合は、オンライン相談へお申し込みください！

こんな方におすすめ！

- **詳細な製品説明**をしてほしい
- 競合製品との**比較情報**を知りたい
- CylancePROTECT や Deep Instinct の**管理画面**を見たい
- **他社の運用事例**を聞いて利用イメージを持ちたい

「オンライン相談」のお申し込みはコチラ

https://www.lanscope.jp/cyber-protection/businesstalk/

製品に関するお問い合わせ

■ 営業本部

大阪本社　06-6308-8980
東京本部　03-3455-1811
名古屋支店　052-253-7346
九州営業所　092-419-2390
E-mail　sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター　0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間　9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ　support@motex.co.jp