LANSCOPE Cyber Protection

CylancePROTECT

最新の脅威トレンドをもとに、
運用提案してくれるのは、どっち？

SOCサービス vs MDR

意外と知らない監視手法の違い

はじめに

ランサムウェア対策の一環で、日々の脅威監視を行う SOC （Security Operation Center）サービスや MDR （Managed Detection and Response）をご検討されている企業様もいらっしゃることかと思います。確かに、ランサムウェアに感染した際、迅速に事態を把握し対処を行えるかが重要です。しかし、SOC サービスや MDR と一口に言っても、対応範囲に明確な違いがあります。万が一感染した際に「対応してもらえると思っていたのに、想定と違った！」と気づいては目も当てられません。
そこで本資料では、SOC サービスと MDR の違いや、これらのサービスがどういった企業に適しているのかをまとめていますので、比較検討する際にお役に立てば幸いです。

なお、SOC サービスや MDR は提供しているベンダー様によって、サービス内容はさまざまです。
本資料では、一般的な内容をもとに作成しておりますので、ご了承ください。

SOC サービス と MDR の違い

●SOC サービスとは

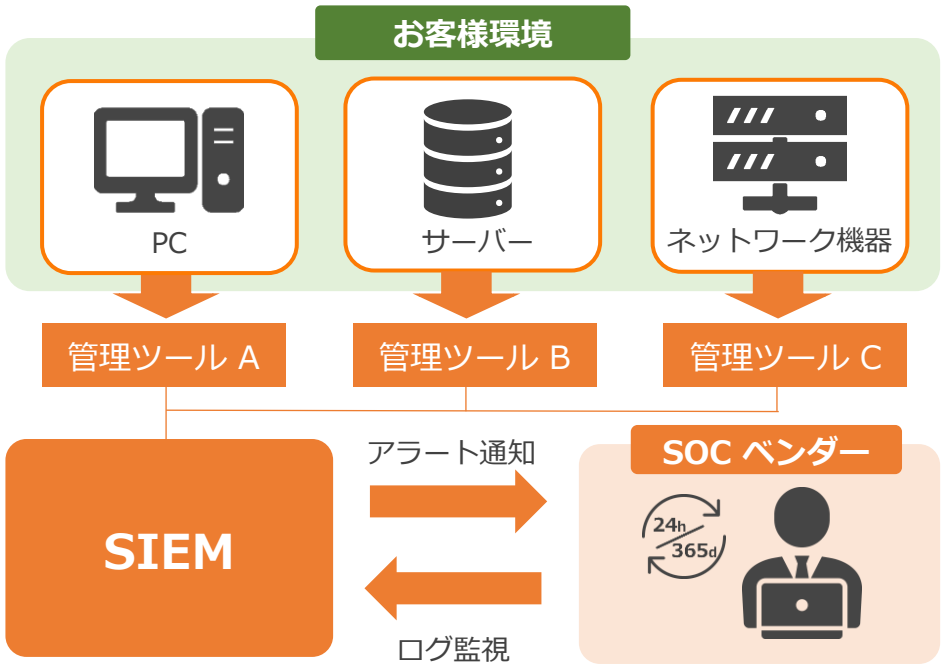
SOC（Security Operation Center）とは、セキュリティの強化といち早いインシデント対応を目的として、24時間365日体制で脅威を監視し、インシデントの検知・分析を担う組織を指します。SOC の監視範囲は、PC やサーバー、ネットワーク機器と幅広く、これらの機器のログなどを SIEM（Security Information and Event Management）というツールに集約して、脅威監視やインシデントの検知を行います。
本来であれば、情報システム部門とは別に、セキュリティの専門組織として社内に SOC を立ち上げるのが理想的です。しかし、現実的には人員不足の観点から、SOC として独立した組織を構築するのは困難です。そのため、**日々の脅威監視を代行する「SOC サービス」を提供するベンダーが増えています。**

●MDR とは

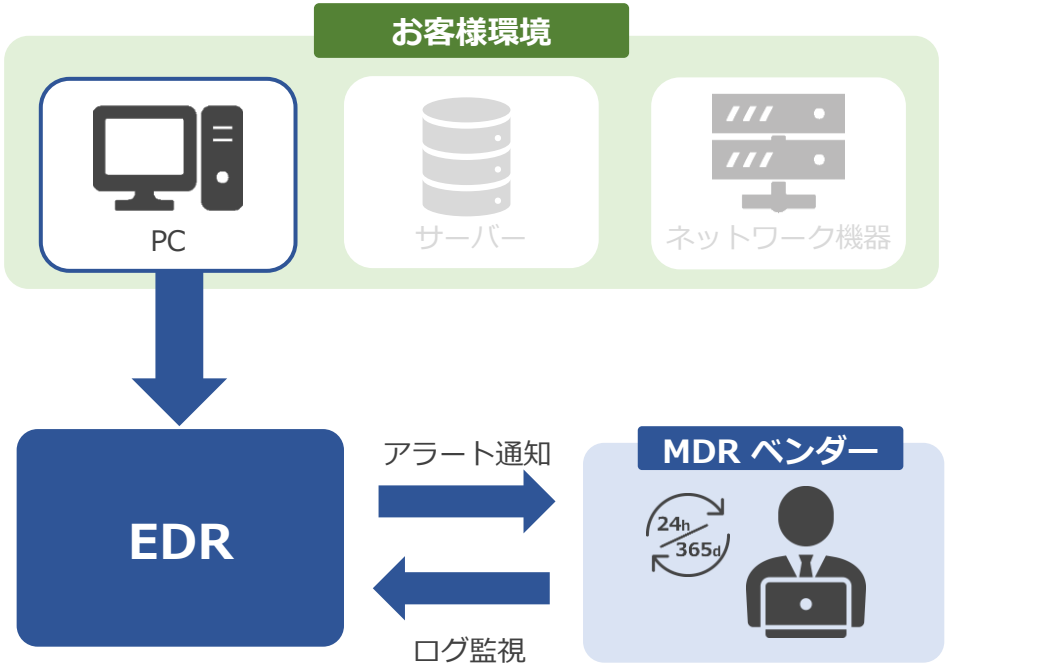
MDR（Managed Detection and Response）とは、24時間365日体制で脅威監視を行う、運用サービスのことです。セキュリティベンダーやサービスプロバイダーが、企業の「エンドポイント」などの環境を監視し、不審な挙動や脅威を発見します。基本的には、MDR は単体で販売しておらず、「EDR（Endpoint Detection and Response）」などのオプションとして提供していたり、ウイルス対策ソフトと EDR、MDR をワンパッケージで提供するなど、さまざまな提供形態があります。**サービス内容も24時間365日監視するだけでなく、最新の脅威トレンドに合わせた運用をするなど、SOC サービスに比べ、より高度なサービスを提供している傾向にあります。**

SOC サービス と MDR の違い

SOC サービス



MDR



■ SOC サービスの特徴

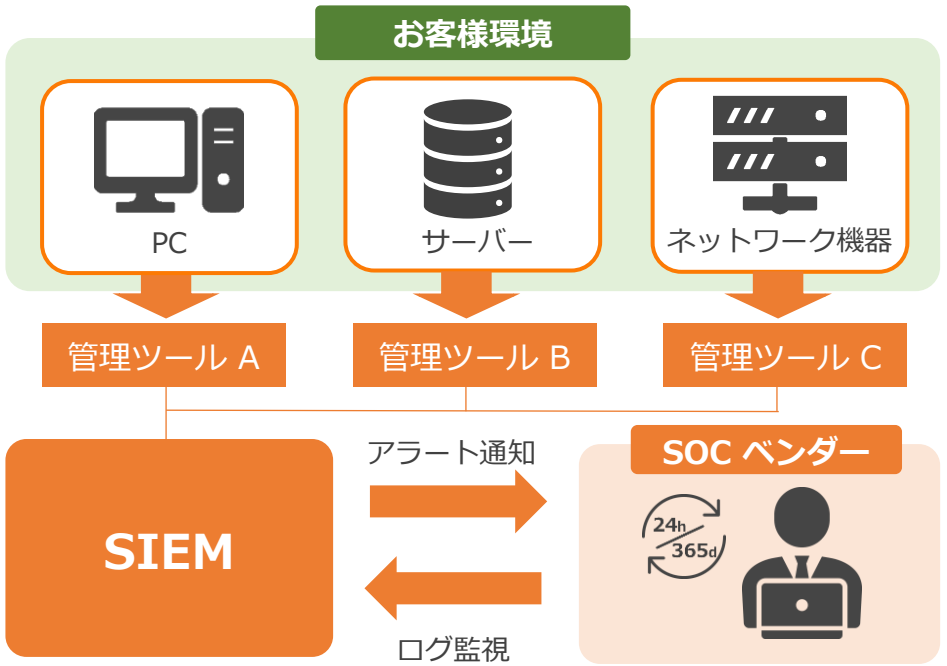
- 24時間365日、脅威を監視
- PC やサーバーなどの情報を SIEM に集約し、一元管理
- SOC サービスが指定したセキュリティポリシーで運用

■ MDR の特徴

- 24時間365日、脅威を監視
- EDR が対応している機器のみを監視
- 運用方法を熟知したメーカーにより、高度な運用が可能

各サービスのメリット・デメリット

SOC サービス



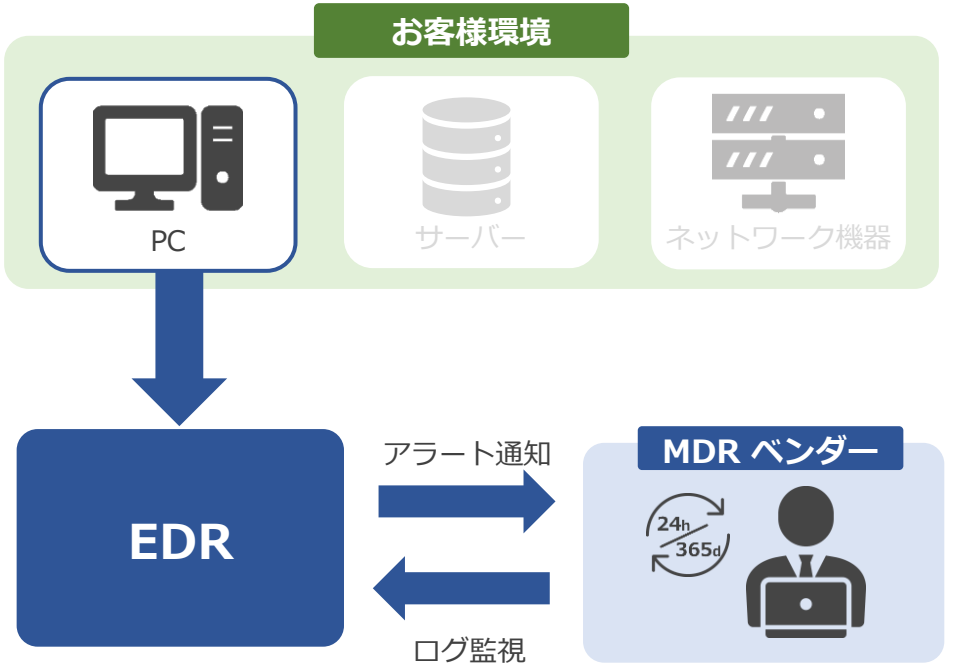
メリット

- さまざまなエンドポイントやネットワークなど、幅広く監視
- システムの脆弱性を確認し、セキュリティパッチの適用も実施

デメリット

- **SOC サービスが指定した検知ルールで運用されることが多いため、最新の脅威トレンドへの対応や自社環境に合わせた監視は行われない**

MDR



メリット

- EDR に特化した高度な脅威監視を実施
- 最新の脅威トレンドや自社の環境に合わせた設定で運用

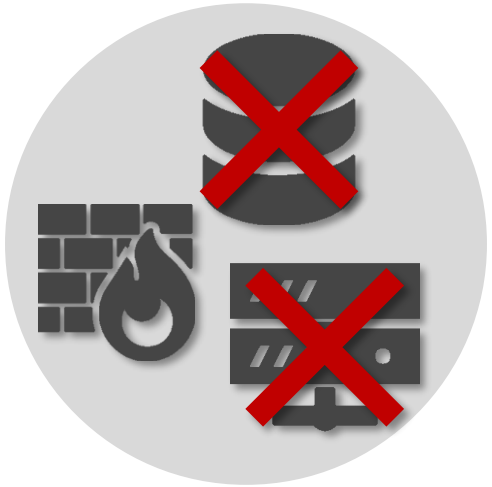
デメリット

- **監視範囲が限定されるため、網羅的な脅威監視はできない**

感染原因の詳細調査や復旧対応は行わない

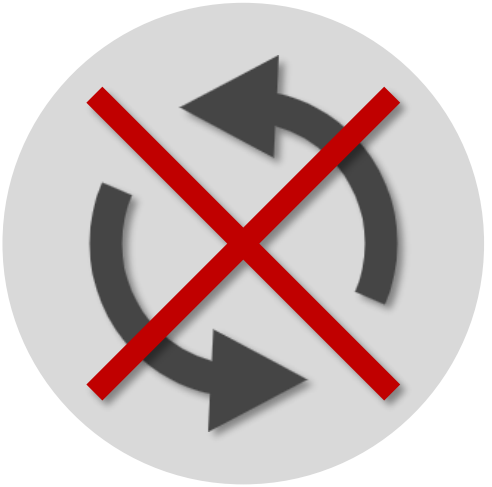
マルウェア感染直後の初動対処はサービスに含まれる場合もありますが感染原因などの詳細な調査や端末の復旧作業は、自社での対応となります。

サービスによって運用できない製品がある



例えば、同じサーバー管理ツールでもA 社の製品は使用不可、B 社の製品は使用可能などのケースがあるため、事前に確認が必要です。

アップデートなどの作業は実施してくれない



管理ツールのバージョンアップやエージェントのインストール・アンインストールなどの作業は自社で行う必要があります。

SOC サービス と MDR どちらを選んだら良いのか？

SOC サービス・MDR のどちらのサービスも24時間365日脅威を監視して、企業のセキュリティ人材の不足も解消できるというメリットがあります。しかし、実際には運用できる製品が限定され、また対応範囲なども異なります。自社が求めるセキュリティレベルや環境に応じて、どちらのサービスが適切かを検討することが重要です。

SOC サービスが向いている企業

- ✓ **基礎的なセキュリティポリシーが確立されておらず、網羅的な支援を必要としている**
- ✓ **PC やネットワーク機器など、幅広く監視してほしい**

MDR が向いている企業

- ✓ **自社で EDR の運用が困難なため、専門家に監視を代行してほしい**
- ✓ **最新の脅威トレンドや自社の環境に最適な設定で運用してほしい**

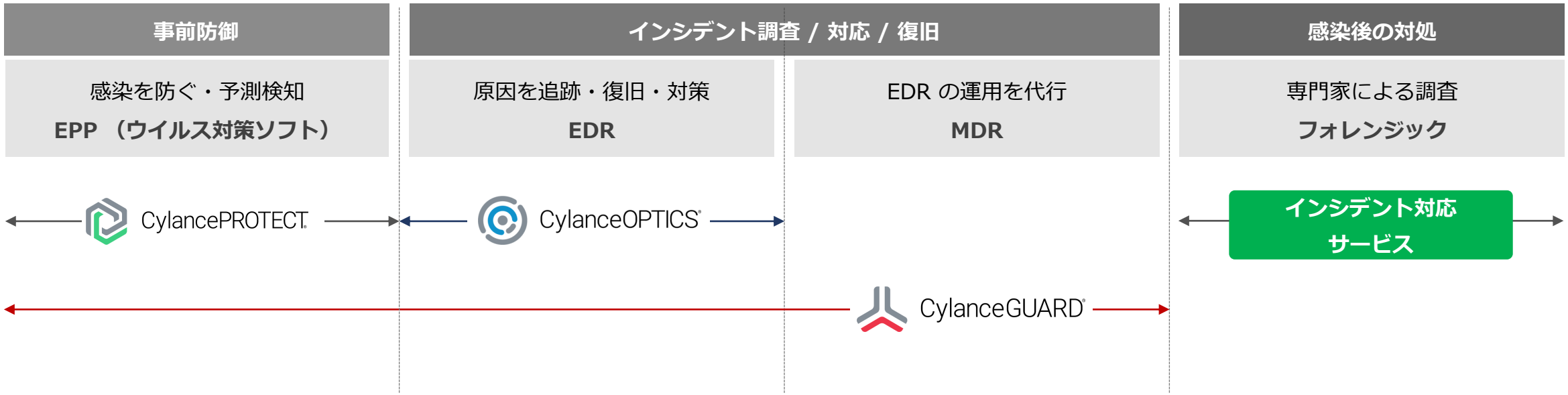
MOTEX では、世界トップレベルのセキュリティ専門家による MDR サービス「CylanceGUARD」をご提供しています！

MDR サービス「CylanceGUARD」

LANSCOPE Cyber Protection

LANSCOPE サイバープロテクション powered by CylanceGUARD

マルウェア感染時の調査・解析～その後の防御まで
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　CylanceOPTICS ※　CylanceGUARD

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

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

高性能 AI により
99%※マルウェアを防御

CylanceOPTICS

マルウェアの侵入経路を特定
再発防止策の検討に

ThreatZERO

PROTECT・OPTICS の
有効な使い方をレクチャー

MDR

セキュリティ専門家が
24時間365日監視

※2023年3月 Tolly 社のテスト結果より

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

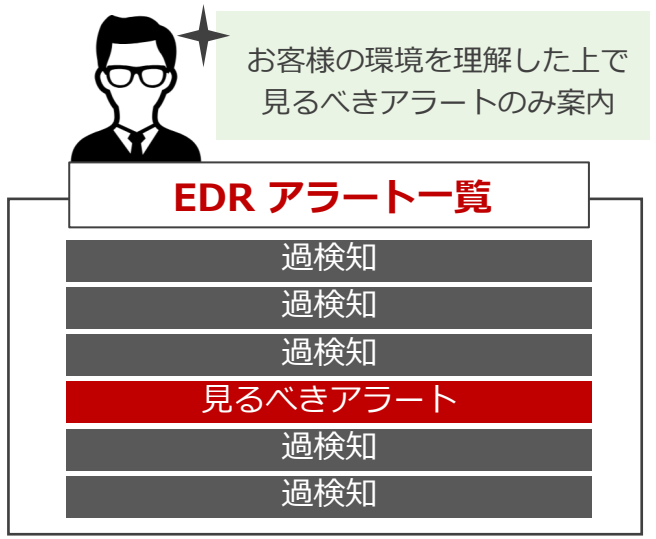
高いスキルを持ったメンバーが対応

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

CylanceGUARD と一般的な MDR との比較

■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
 情シス担当	 情シス担当	情シス担当 問い合わせ オペレーター（セキュリティの知識無し） MDR 担当者
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  情シス担当	セキュリティ専門家 ・24/365 で監視 ・最適な設定  情シス担当	情シス担当 問い合わせ BlackBerry の セキュリティ専門家
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**

CylancePROTECT・CylanceOPTICS のご紹介

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

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

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

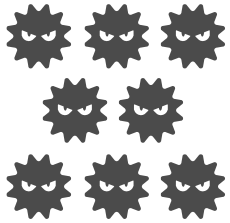
●脅威の封じ込めによる被害の最小化　●端末挙動からの動的な脅威検知と対処

※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

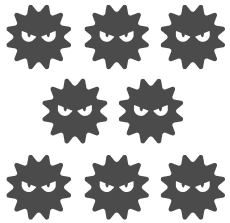
パターンファイル型や
サンドボックス等の動的検知

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

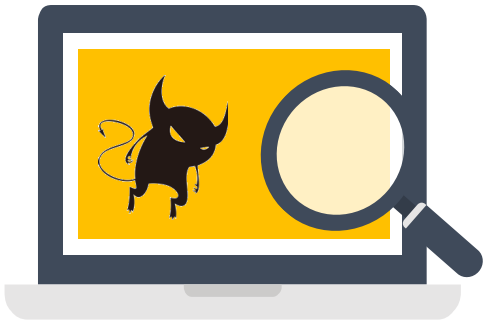
インシデント対応サービス

本サービスは、CylancePROTECT、CylanceOPTICS、CylanceGUARD 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・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。
※ 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 / 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）**※ 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にのみ対応可能です。 （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

台数無制限　　レポート解説付

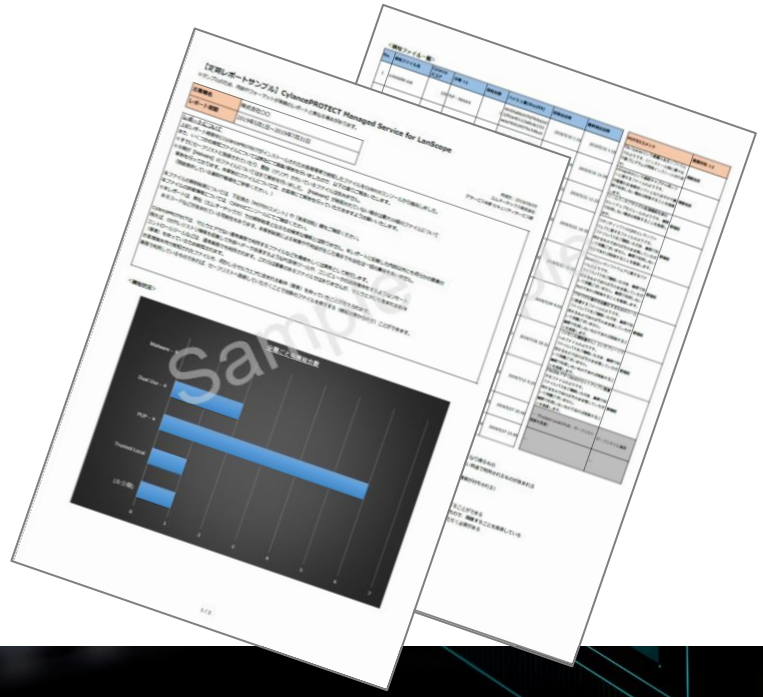
CylancePROTECT 1ヶ月無料体験版

～端末に潜む マルウェア を見つけ出せ！～

CylancePROTECT・OPTICS を 1 ヶ月無料で何台でもインストール可能！

自社ネットワーク内に危険なマルウェアが潜んでいないかを無料で調査できます。

体験後、ご希望の方にはマルウェア検知結果のサマリーレポートをプレゼントします！



【お申し込みはこちら】

https://www.lanscope.jp/lp/cpms/

（CylanceOPTICS の体験を希望される際には、お申込みフォームの備考欄にご記載ください。）

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 CylanceOPTICS 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/cylance/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