報道関係者各位
（参考資料）

2019 年 12 月 9 日
株式会社インターネットイニシアティブ

IIJ、「IIJセキュアエンドポイントサービス」において EDR機能「CylanceOPTICSオプション」を提供開始

--マルウェア感染後の不正挙動検知により迅速なインシデント対応を支援し、被害拡大のリスクを軽減--

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎）は、クラウド型総合エンドポイントセキュリティサービス「IIJ セキュアエンドポイントサービス」において、マルウェア感染を前提とした不正挙動の検知とその対応支援を行う EDR（Endpoint Detection and Response）機能として「CylanceOPTICS（サイランスオプティクス）オプション」を追加し、本日より提供を開始いたします。

「IIJ セキュアエンドポイントサービス」では基本機能として、PC などの端末（エンドポイント）がマルウェアなどの脅威に感染することを事前検知し、防御する AI 活用型アンチウイルス「CylancePROTECT（サイランスプロテクト）」を提供していますが、本オプションは、感染後の迅速な対応につなげることを目的としたもので、インシデント対応時間を大幅に短縮し、対応負荷および被害拡大のリスクを軽減します。

EDR が注目される背景と課題

昨今、サイバー攻撃の高度化・巧妙化により、マルウェア感染を完全に防ぐことは困難と考えられています。そのため、マルウェアに感染する前提に立ち、エンドポイントでの検知と対応の迅速化を目的とする EDR が注目されています。

一般的に EDR はアンチウイルスと併せて利用され、アンチウイルスで検知できなかったマルウェアや不正挙動の検知と停止をおこなうとともに、収集した情報を可視化することで、エンドポイントで発生している事象の把握とインシデント対応を支援します。

しかし、従来のアンチウイルスと EDR の組合せでは、未知のマルウェアなど多くの脅威のすり抜けによって大量の検知アラートが発生し、アラートを精査する管理者に高い負荷がかかることや、重要度の高いイベント情報が膨大なアラートに埋もれてしまうことなどが課題となっています。

「CylanceOPTICS オプション」の特長

「IIJ セキュアエンドポイントサービス」の基本機能の一つである「CylancePROTECT」は、AI アルゴリズムを活用し、特徴点のディープラーニングによって脅威を検出することで、従来型のシグネチャによるパターンマッチングを用いたアンチウイルス製品と比べて、未知のマルウェアに対しても高い検知率を誇ることが特長です。

今回、この「CylancePROTECT」と EDR 機能「CylanceOPTICS オプション」を連携させることで、EDR で検知するアラートの件数を大幅に削減することができます。管理者は重要度の高い検知イベントに集中して対応できるため、インシデント対応の負荷を軽減し、被害拡大のリスクを最小化します。

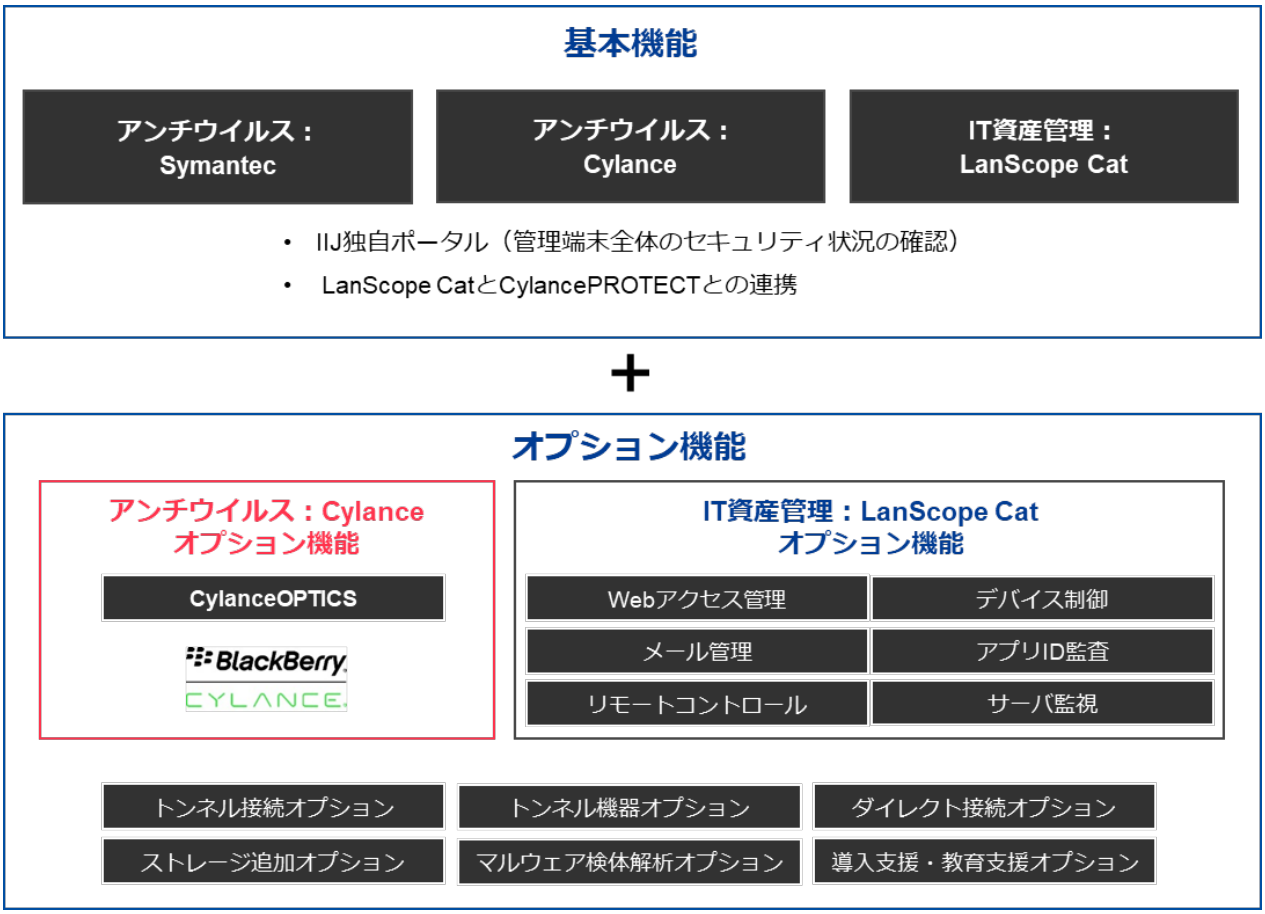
「CylanceOPTICS オプション」の主な機能

1. 異常動作検知・自動対処（Detections）
   Cylance 社の検知ルールで不正な動作を検知します。過去 7 日間のイベント数やイベント詳細も確認できます。
2. 感染端末隔離（Device Lockdown）
   特定の端末で疑わしい挙動を検知した場合などに、リモート操作で該当端末をネットワークから隔離することができます。
3. 根本原因分析（Focus Data）
   発見したファイルがどのように操作されていたのかを時系列で表示し、インシデントの原因を明白にできます。
4. スレットハンティング（InstaQuery）
   入手した脅威情報等に基づき社内 PC の状況を確認できます。今まで見過ごしていた脅威の有無を調査することが可能です。

「IIJ C-SOC サービス」との連携（2020 年 2 月提供予定）

「IIJ C-SOC サービス」※との連携により、「CylanceOPTICS オプション」のログと IIJ の各種セキュリティサービスやお客様運用機器のセキュリティログとの相関分析を行うことが可能です。IIJ の専門エンジニアによる 24 時間 365 日体制でのインシデント対応支援および対応策の提示など、セキュリティ運用における支援範囲が広がります。

IIJ セキュアエンドポイントサービスのサービスメニュー



サービス費用
導入する機能、端末台数に応じた個別見積もりです。

お見積り例:
端末数 1,000 台、利用機能が CylancePROTECT＋CylanceOPTICS の場合
月額 595 円（税抜）/端末～

サービス詳細は https:/www.iij.ad.jp/biz/endpoint/cylance.html をご覧ください。

※「IIJ C-SOC サービス」
ファイアウォールなどのセキュリティ機器やお客様運用機器からセキュリティログの収集と分析をおこない、24 時間 365 日体制でセキュリティインシデントへの対応をワンストップでサポートするサービスです。詳細は https://www.iij.ad.jp/biz/c-soc/をご覧ください。

IIJ は今後も、「安全をあたりまえに」をコンセプトとするセキュリティ事業ブランド「wizSafe（ウィズセーフ）」のもと、お客様がインターネットを安全に利用できる社会の実現を目指してまいります。

報道関係お問い合わせ先
株式会社インターネットイニシアティブ 広報部 加藤、増田
TEL：03-5205-6310 FAX：03-5205-6377
E-mail：press@iij.ad.jp
URL: https://www.iij.ad.jp/