

## MDRサービス for Palo Alto Networks Cortex XDR

セキュリティエキスパートがCortex XDRの運用から対策までをサポート

Cortex XDRが検知したアラートを監視し、インシデント発生時にはエンドポイントの隔離や脅威除去支援、再発防止策の提案まで、一貫して対応。管理者の負担軽減と、より強固なセキュリティ対策を実現します。

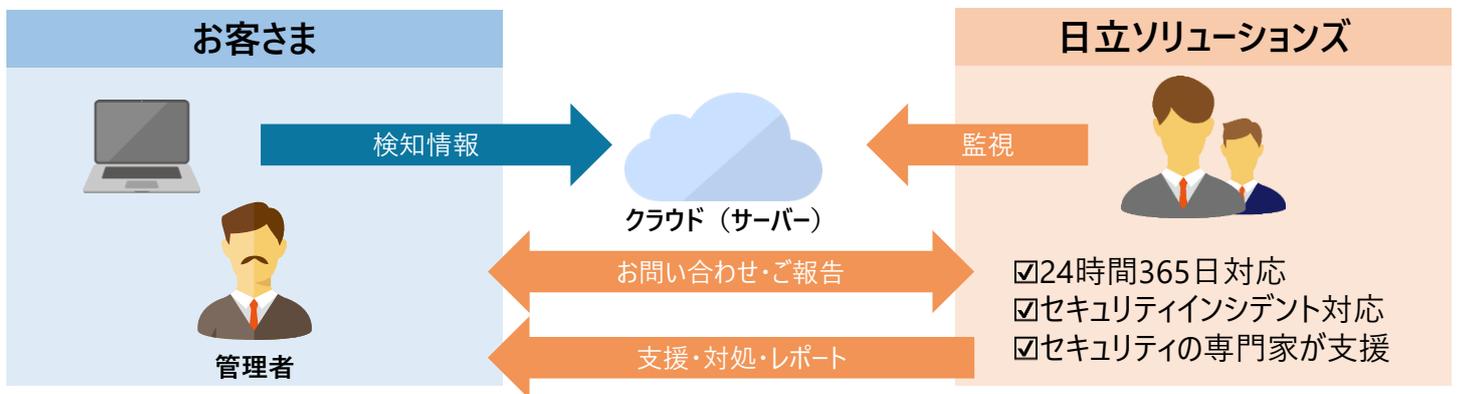
※MDR:Managed Detection and Response



### 管理者が抱える課題

- 外部脅威対策の運用は、負担が大きい
- マルウェア被害が発生したが、どのように対処すればよいかわからない
- マルウェア本体だけではなく、マルウェアから派生した脅威にも対応したい

## セキュリティエキスパートが運用から対策まで支援



### インシデントの監視から報告までワンストップで提供

インシデントの監視からインシデント発生時の対応、報告までの一連の流れを、セキュリティエキスパートがワンストップで支援します。

### 24時間365日体制のサポート

24時間365日体制でイベントを監視。インシデント発生時は、Cortex XDRのアラート解析により危険度を判定。対応が必要な脅威の場合は封じ込めなどの対処まで実施します。

### アラートの原因となった脅威を除去し、復旧を支援

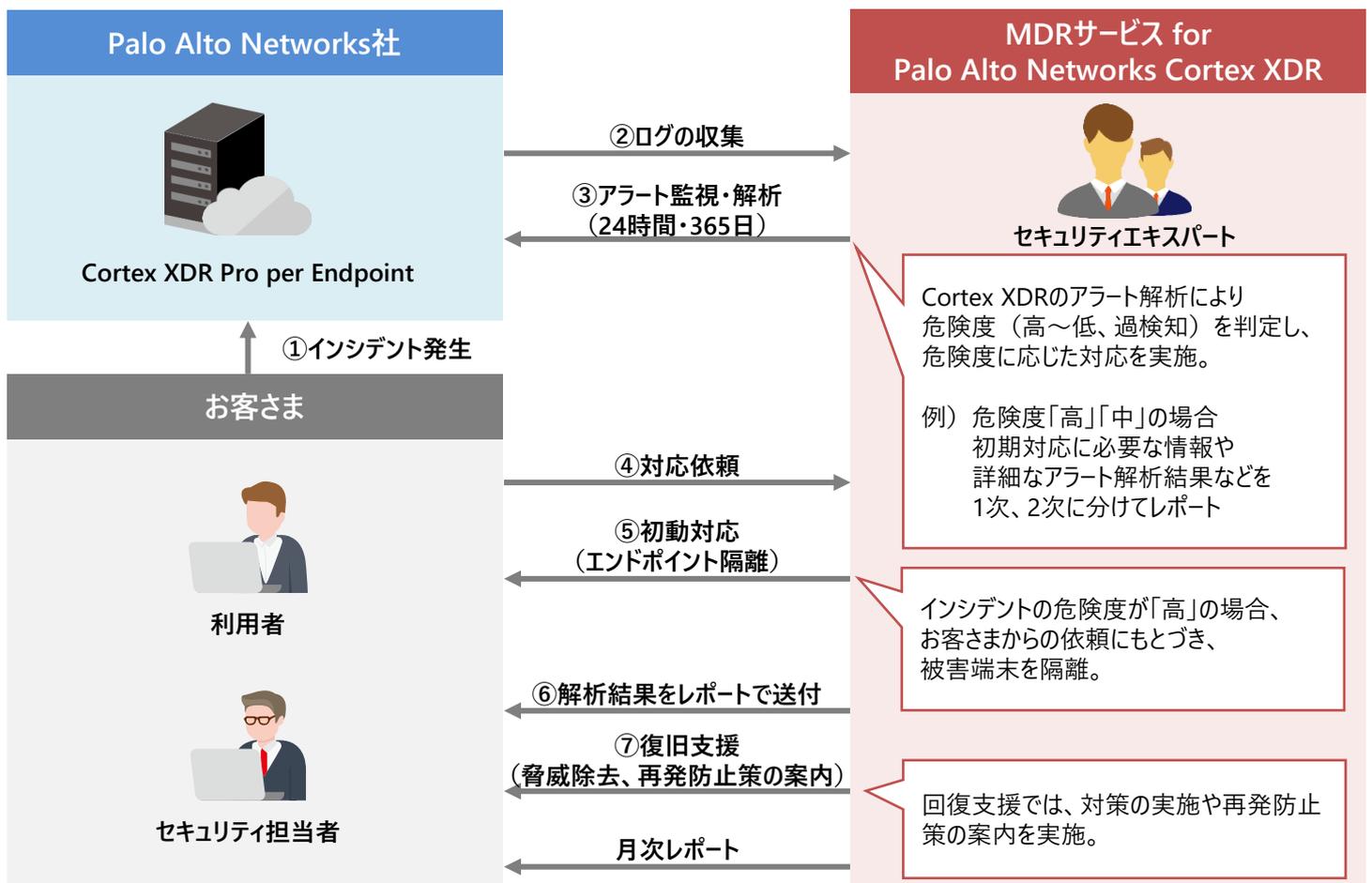
マルウェア関連のファイルやレジストリを徹底除去し、全端末を調査・対応。再感染防止のためハッシュ登録や危険情報提供で同様の攻撃を抑止します。

# サービスメニュー概要

下記4つの運用フェーズごとにサービスを提供。必要なサービスを選択可能です。

製品導入	①監視	②初動対応	③復旧支援	④調査
運用フェーズ	サービス内容			
① 監視	24時間365日イベントを監視し、アラートを解析することにより危険度を判定し、具体的な侵害状況や早期対応に必要な情報を通知します。			
② 初動対応	アラート発生時にエンドポイントの隔離を実施します。			
③ 復旧支援	マルウェアの駆除など、エンドポイントに残存する脅威の除去作業を支援します。また、再発防止策の案内なども行います。			
④ 関連調査	組織内に侵入・潜伏している未検知の脅威や、脆弱性などの情報を調査して報告します。			

## サービス利用イメージ



※本リーフレット中の会社名、商品名は各社の商標、または登録商標です。 ※本文中および図中では、TMマーク、®マークは表記しておりません。 ※本リーフレットの一部分は、生成AIにより生成されたコンテンツを使用しています。 ※製品の仕様は、改良のため、予告なく変更する場合があります。 ※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取りください。 なお、ご不明な場合は、当社担当営業にお問い合わせください。 ※本リーフレット中の情報は、作成時点のものであります。

株式会社 日立ソリューションズ

[www.hitachi-solutions.co.jp](http://www.hitachi-solutions.co.jp)

本リーフレット掲載商品・サービスの詳細情報

<https://www.hitachi-solutions.co.jp/paloalto/products/s-operation/mdr.html>

