

マネージドセキュリティサービス for Palo Alto Networks Prisma Access

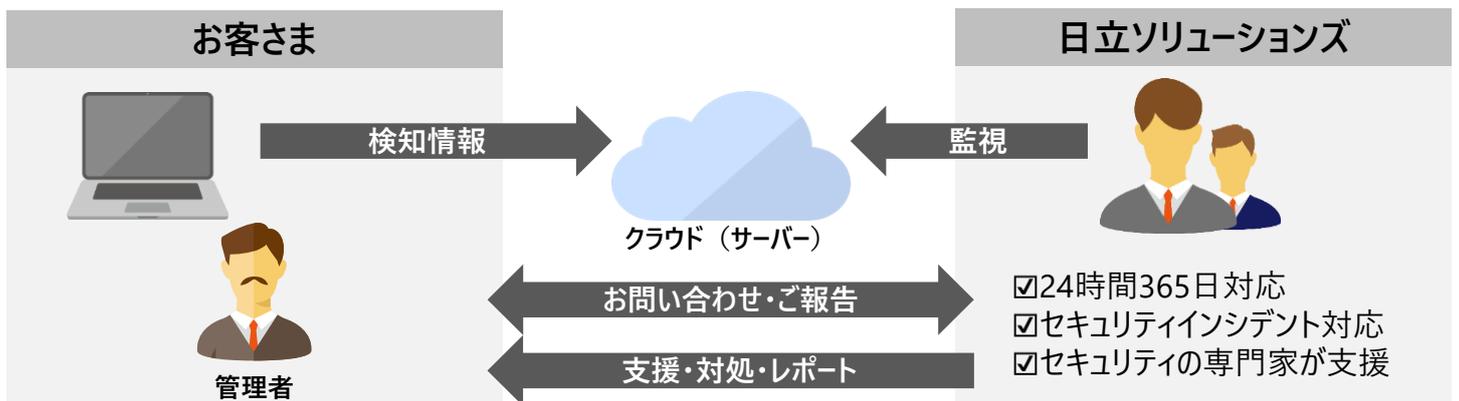
セキュリティエキスパートがお客さまに代わり、Prisma Accessからのアラートを監視し、分析、対策まで実施



管理者が抱える課題

- インシデント発生時に対応できる体制を整えることが難しい
- セキュリティの専門知識を持った人財が不足している
- インシデントによる被害拡大を防ぎたい

／ 管理者の負担軽減とセキュリティ対策の強化を実現 ／



監視からインシデント対応までワンストップで提供

アラートやログの監視からインシデント対応まで、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

検出したアラートとログを24時間監視し、あらかじめ設定したルールに一致した場合は調査・分析を行い、必要に応じて通知と初動対応まで実施します。

プロアクティブな対応によりインシデントの拡大を防止

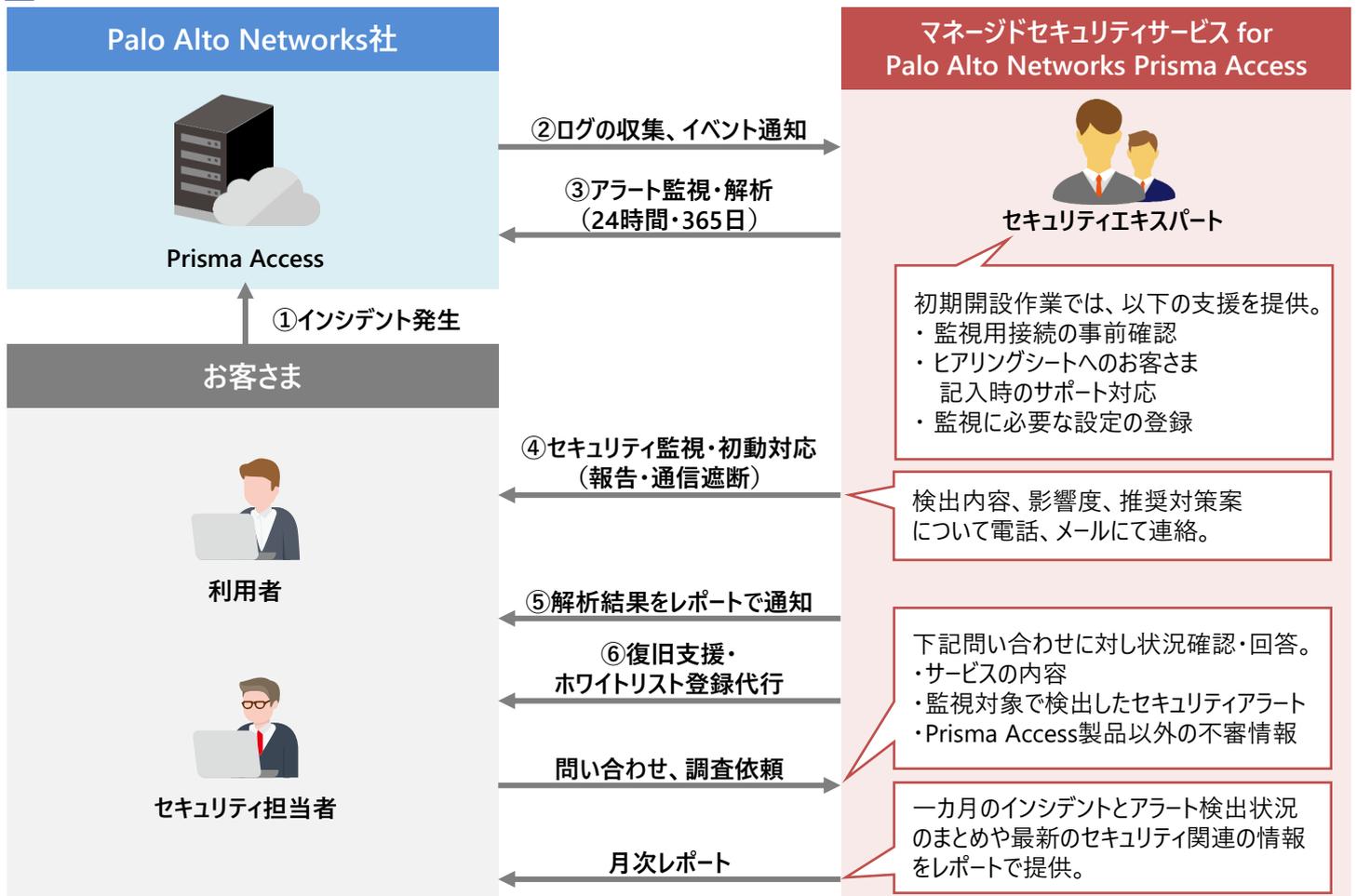
Prisma Accessによる解析・遮断に加え、他製品を活用して追加調査と対策を行います※。また、必要に応じて不正活動を抑制し、被害拡大を防止します。

※MDRサービス for Cortex XDR、MDRサービス for CrowdStrikeをご購入いただいている場合

サービスメニュー概要

| 提供項目 | サービス内容 |
|-------------|--|
| サービス監視 | 稼働状態に異常が認められた場合、異常を確認した時点でお客さまへご連絡。 |
| セキュリティ監視 | <p>検出したセキュリティアラート、および収集したログ*1を24時間365日監視。 分析ルール、および相関分析ルールにマッチしたアラートやログが検出された場合は調査を行い、インシデントの有無を判定。</p> <p>インシデントと判定された場合、以下を実施。 不正通信の遮断/URLフィルタリング機能によるブラックリスト設定/他監視対象のMDR契約に対する抑制作業*2</p> <p>*1 Prisma Accessのシステム上高リスクとして検出したものおよび確認が必要と判断したものが対象。 *2 別途他監視対象のMDR契約が必要。</p> |
| システムオペレーション | Prisma AccessのURLフィルタリング機能に関してホワイトリストの設定作業を実施。 |
| 問い合わせ対応 | サービス仕様の問い合わせやご要望に応じてPrisma Access のログに対する調査を実施。 |
| レポート | 月次レポートにて監視結果を報告。 |

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

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/cloud/mss.html>

