社内に侵入したマルウェアの感染拡大を防止

パロアルトネットワークス 次世代ファイアウォール＋秘文 Device Control 連携ソリューション

サイバー攻撃は、日々高度化・巧妙化しています。
特定の企業を狙って作られたマルウェアを使った標的型攻撃は、
巧妙な仕掛けにより、感染に気づかないうちに被害が拡大してしまいます。
そのため、マルウェアに感染することを考慮した対策が必要です。

パロアルトネットワークス 次世代ファイアウォール
多彩な機能による多層防御により、
標的型攻撃対策に優れた次世代ファイアウォール

＋

秘文 Device Control
端末側でデバイスの利用や接続先
ネットワークを制御するエンドポイント製品

POINT 1 マルウェア感染から遮断にかかる時間を短縮し、情報漏洩リスクを軽減

マルウェア検知後の利用者への警告、ネットワーク遮断を自動化することで、管理者の運用負荷を軽減できます。また、感染から遮断にかかる時間を短縮することで内部感染拡大や情報漏洩リスクを軽減できます。

POINT 2 マルウェア感染の可能性を利用者に自動通知するため、即座に対策を指示可能

自動通知による利用者への早急な注意喚起が可能です。警告画面のメッセージは管理者が編集できるため、管理者への連絡を促すなど具体的な対策を指示することができます。

POINT 3 遠隔操作で感染端末の復旧作業が可能

通信を遮断した後も、管理者は遠隔操作で感染端末の状況確認や遮断解除を行うことができるので、感染後の運用負荷を軽減できます。

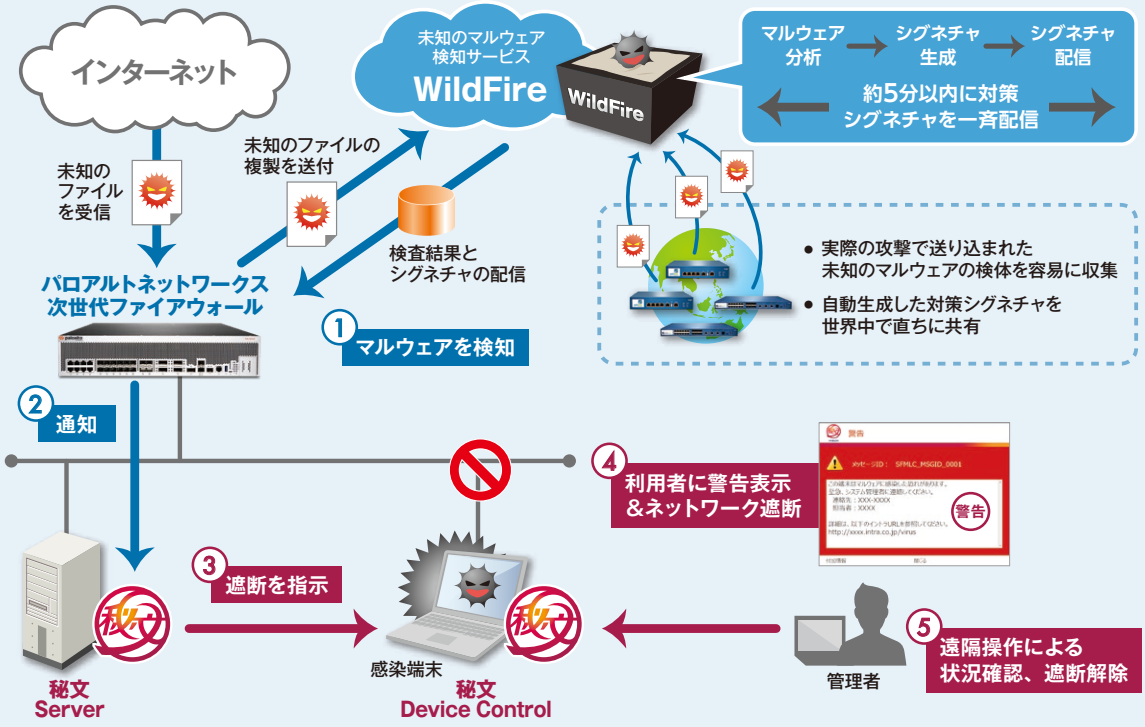
株式会社 日立ソリューションズ

■ システム構成例

パロアルトネットワークス 次世代ファイアウォール　WildFireを利用※1※2 ＋ 秘文 Device Control

WildFireが未知のマルウェアを検知

WildFireはクラウドベースのサンドボックス環境です。受信した未知のファイルのマルウェア分析を自動で行います。
また世界中のパロアルトネットワークス 次世代ファイアウォールからマルウェアの情報を収集し随時対応するため、一般的なウイルス対策製品が未対応のマルウェアでもすぐに対策が可能です。



マルウェアに感染した端末をネットワークから自動遮断し、感染拡大を防止

パロアルトネットワークス 次世代ファイアウォールがマルウェアを検知すると、秘文 Device Controlが感染端末の利用者に警告表示することで、感染の可能性があることを注意喚起できます。
また感染端末のネットワーク自動遮断や、遠隔操作による感染端末の状況確認、遮断解除も可能です。

パロアルトネットワークス 次世代ファイアウォール　TPを利用※2 ＋ 秘文 Device Control

Threat Prevention（TP：脅威防御）が怪しい通信を検知

TPのアンチスパイウェア機能を利用して、C&C通信※3やキーロガーなどの外部への怪しい通信を検知し、感染端末の利用者への警告表示や、感染端末のネットワーク遮断を自動で行います。
遠隔操作による感染端末の状況確認、遮断解除も可能です。

※1 WildFireの利用は、Threat Prevention（TP：脅威防御）ライセンスの利用が前提です。　※2 秘文 Device Control との連携は、TPまたはWildFireの選択制となります。両方と連携することはできません。
※3 マルウェア感染端末がインターネットにアクセスし、攻撃者が感染端末に指令を出して遠隔で制御をする通信です。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/paloalto/

S16K-25-04　2024.09