ゲートウェイやエンドポイントでは対応できない IoT 製品の脅威対策
Juniper Connected Security

JUNIPER NETWORKS | Engineering Simplicity

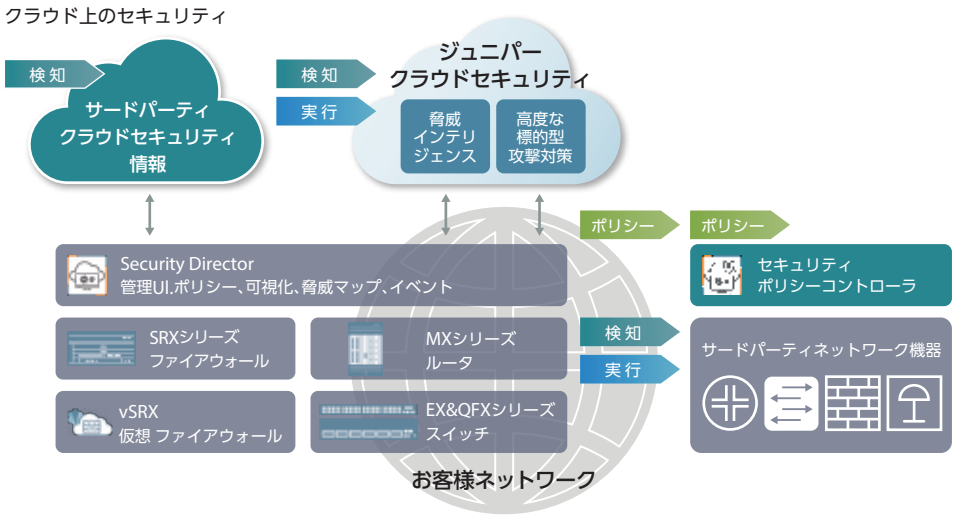
ゲートウェイやエンドポイントでは対応できないIoT製品の脅威対策

Juniper Connected Security
ジュニパー コネクテッド セキュリティ

ジュニパーネットワークスのJuniper Connected Securityは、ネットワークをセキュリティドメインとして機能させ、侵入した脅威をリアルタイムで検知します。
対策が必要な脅威や感染ホストを検知した場合、自動的にポリシーを実行して迅速に脅威を排除・隔離します。

Juniper Connected Security差別化のポイント

ネットワーク全体で脅威を排除	・MACアドレスベースで、動的にセキュリティ脅威を排除 ・外部攻撃および内部からのセキュリティ問題に対応
モビリティへの対処	・感染した機器が移動しても追跡して隔離 ・エージェントレスで、BYODが持ち込むセキュリティの脅威にも対応
クラウドとの連携	・クラウド連携した“集合知”の最新情報による解決 ・リアルタイムでセキュリティ脅威の検知および対処
検知および施行の自動化	・ネットワーク内部に侵入した脅威を自動的に検知 ・事前に定義したポリシーに基き、自動的に脅威を排除

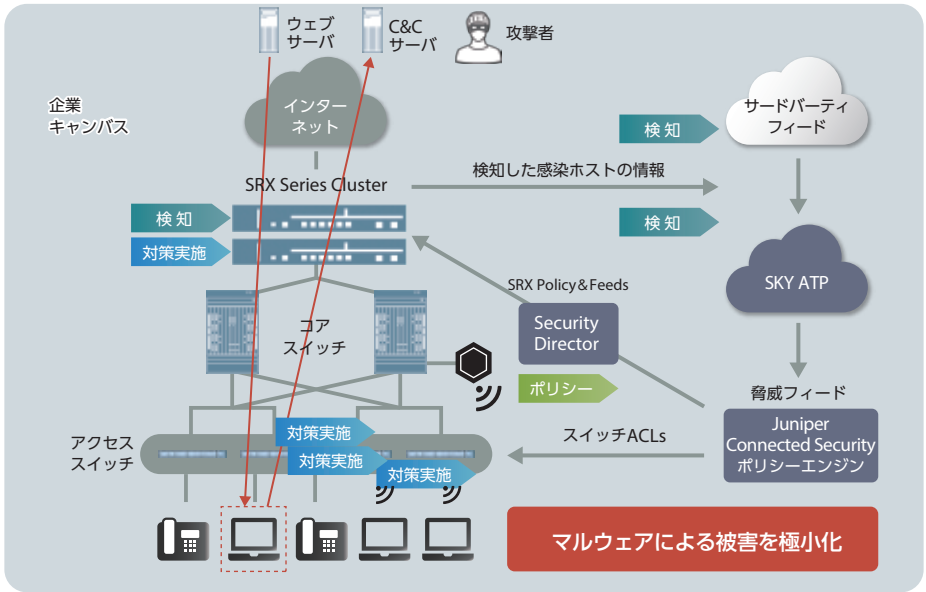


ポリシー
社内ルールに基づいた
セキュリティポリシーを適用

検知
クラウド上の最新脅威情報を活用して、
侵入した脅威をリアルタイムに検知

実行
事前に適用したポリシーに基づき、
侵入した脅威をピンポイントでブロック

キャンパスネットワークにおけるJuniper Connected Security動作例



ポリシーの設定
ポリシーエンジンの設定
(例) 脅威レベル8以上の
感染ホストは、通信を遮断

脅威の検知
クラウドで脅威情報を検出
Sky ATPまたはサードパーティからの
脅威情報フィードにより、
感染端末とC&Cサーバ通信を検知

ポリシーの実行
感染端末を隔離
感染端末のMACアドレスの
通信を遮断するポリシーを適用

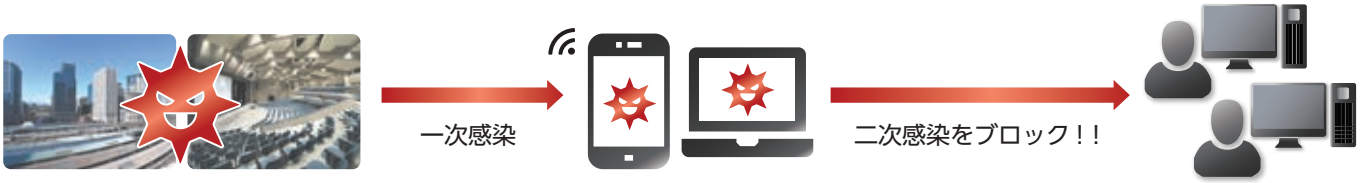
従来の脅威対策では対処困難な領域でJuniper Connected Securityを活用

ユースケース 1

○ ポイント
IP/MACレベルで
感染デバイスを追跡・隔離

公衆Wi-Fiなどから感染するウィルス被害が増加中！ あなたのPCも感染しているかも！？

公衆Wi-fiは便利ですが、マルウェアに感染する温床・エクスプロイト攻撃の実験場所となっています。
知らずのうちにPCが感染し、ネットワークに接続後には感染拡大が始まります。
感染端末の検知・追跡・隔離を自動で行うJuniper Connected Securityでは、このようなケースでも安心です。

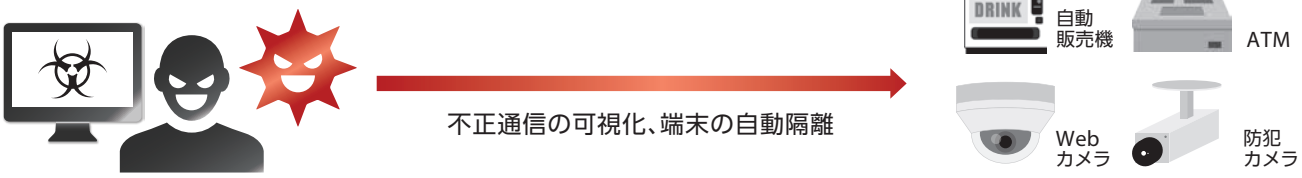


ユースケース 2

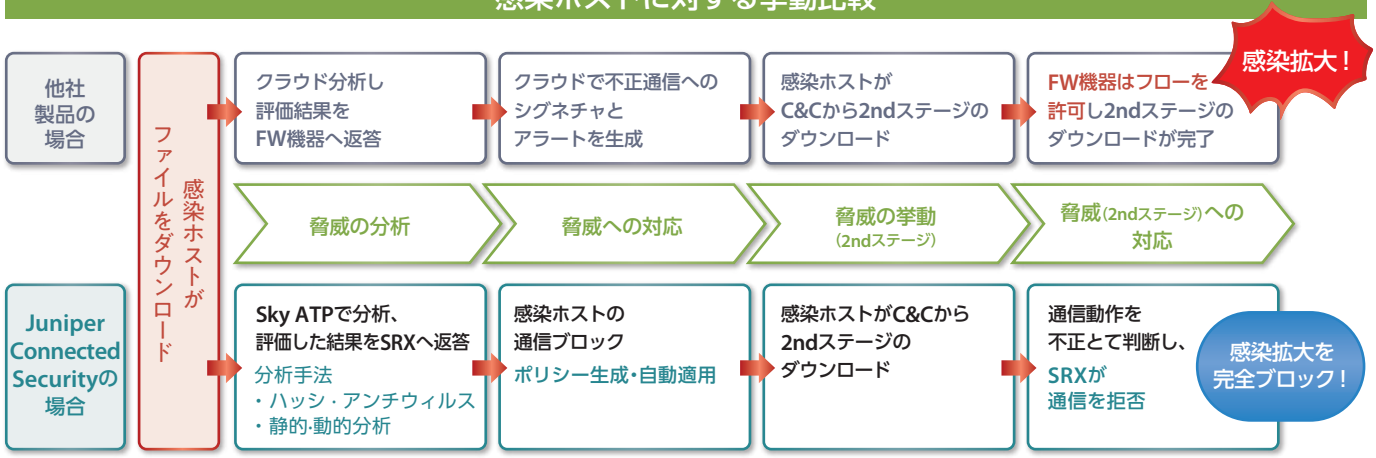
○ ポイント
セキュリティ管理が難しい
IoT機器や遠隔端末を自動監視

増え続ける遠隔管理端末。IT化された機器が狙われています！

セキュリティ対策が難しいWebカメラやATMなどが攻撃対象として狙われていることがニュースでも話題になっています。ネットワーク全体を守るJuniper Connected Securityでは、このような端末と攻撃者との通信（C&C）を監視し不正な通信内容を識別・可視化し、端末の隔離を自動で実施します。



感染ホストに対する挙動比較



ぜひご覧ください!
ジュニパーのセキュリティソリューションまとめサイト
https://www.juniper.net/jp/jp/dm/security/

製品や購入に関して
お気軽にお問合せください

ジュニパーネットワークス株式会社
E-Mail : otoiawase@juniper.net Tel : 03-5333-7410
受付時間: 午前10:00 ～ 午後5:00（土日・祝日、年末年始除く）

June 2018