スレットハンティングの世界

ログからは分からない脅威の最前線

Canon

キヤノンマーケティングジャパン株式会社

自己紹介

氏名：山田 和政

所属：キヤノンＩＴソリューションズ

資格：GCIH, CISSP, RISS

スレットハンティングチームリーダー

専門分野はパケット分析によるスレットハンティング

お客様向け新サービスの開発や既存サービスの品質管理を担当

インシデントレスポンス支援やセキュリティ対策のアドバイスも行う

セッションの目的

お客様のセキュリティを強化するアイデアを提供する

Chapter1：身近にある実際の脅威
セキュリティを回避して侵入する攻撃を認識する
脅威を認識することで初めて対策を検討できるようになる

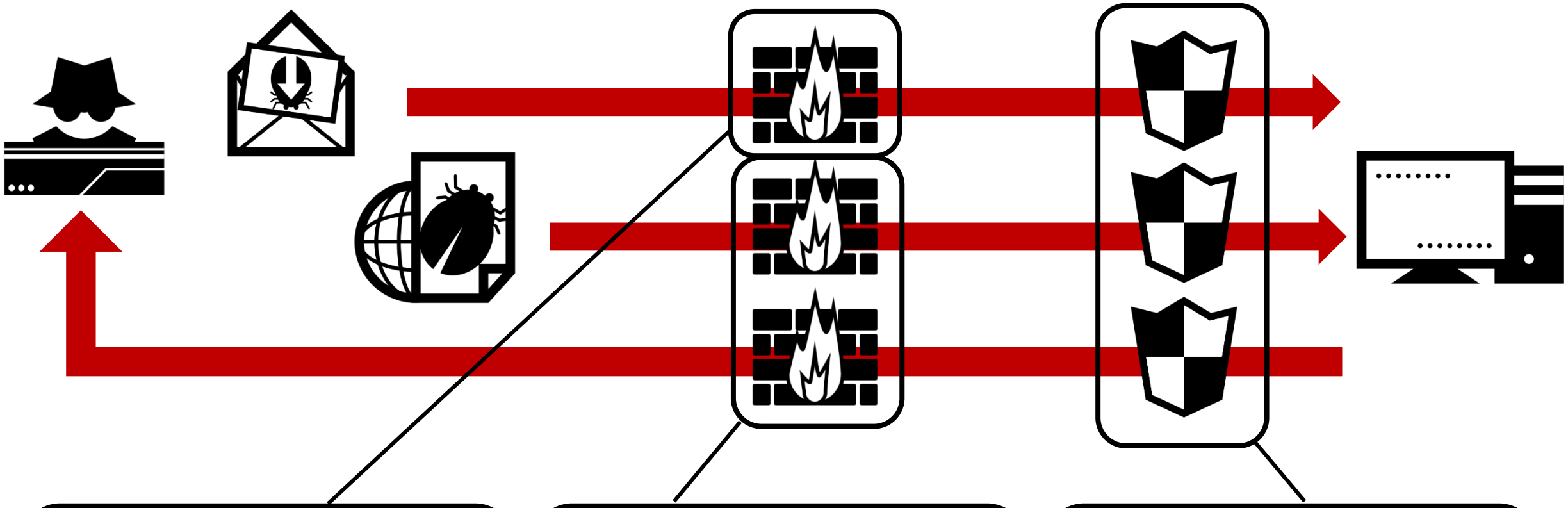
Chapter2：スレットハンティング
スレットハンティングの実践例を理解する
お客様のセキュリティ対策にもこの考え方を取り入れる事ができる

Chapter3：セキュリティの強化
ここまでの話をセキュリティ対策改善に繋げる方法を理解する

身近にある実際の脅威

Chapter 1

ある組織を襲ったサイバー攻撃



メールセキュリティ

添付ファイルが付いたスパムメールを検知しなかった

ウェブセキュリティ

マルウェアのダウンロードを防げなかった

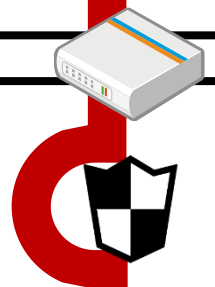
アンチウイルス

感染したマルウェアを駆除できなかった

スレットハンティングの必要性

攻撃者はセキュリティの回避を前提として
侵入プランを立ててくる

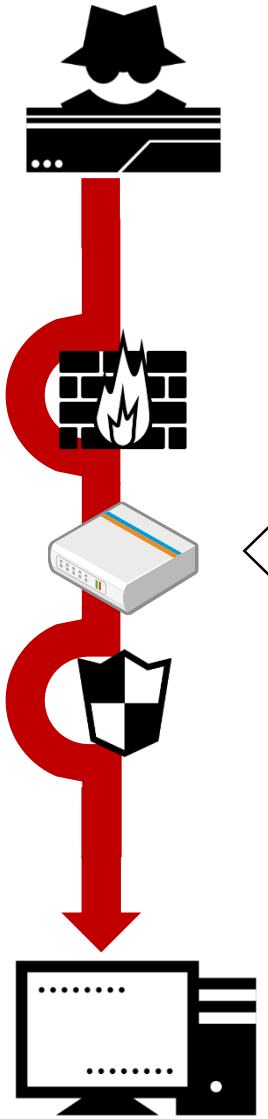
ネットワークセキュリティを通過した脅威は
アラートで認識できず多くの場合はログにも残らない



エンドポイントセキュリティを回避した脅威も同様
さらにネットワーク探索はエンドポイントでは検知できない

どこにも記録が残らず攻撃が成立した事に気付けない

私たちの提案



RSA NETWITNESS® PLATFORM

直感的な操作が可能な
フルパケット分析ツール

数TBのパケットに対して
数秒でデータ抽出が可能

攻撃者が遠隔に居る以上
必ず痕跡が含まれる

＋

Canon
キヤノン IT ソリューションズ株式会社

スレットハンティングを
専門とするチーム

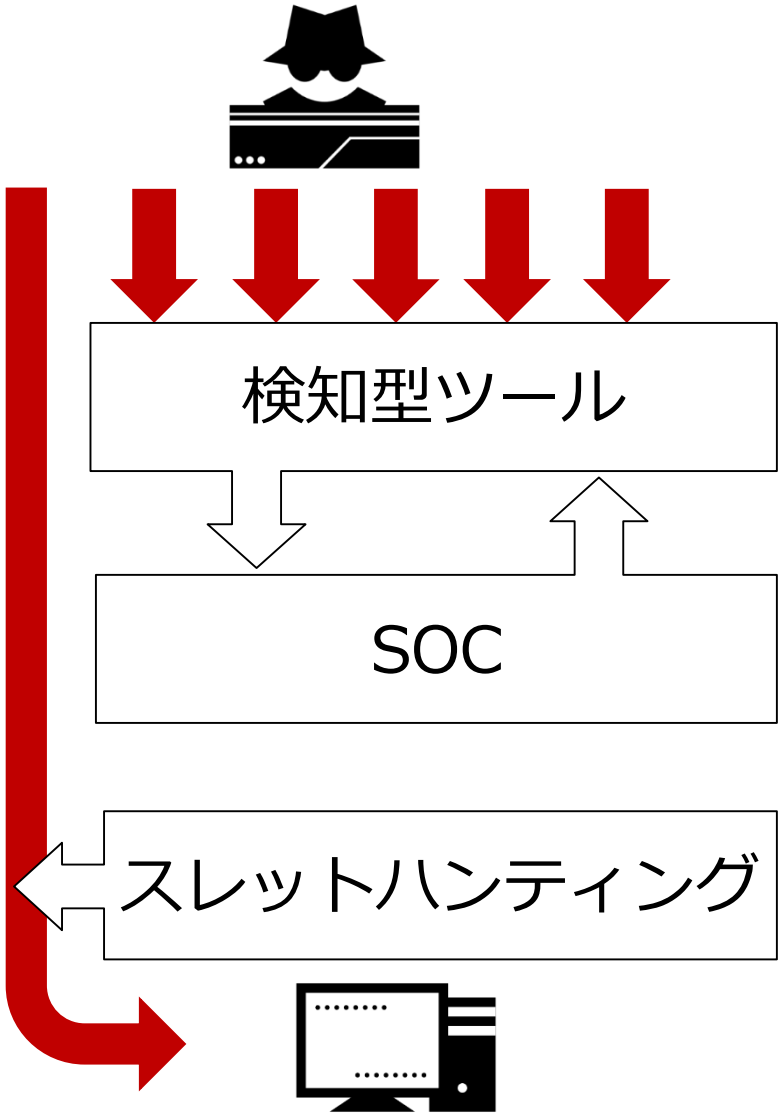
実際のパケットから
脅威インテリジェンスを生成

反復的な分析と改善により
お客様の戦略を支援

スレットハンティング

Chapter 2

既存セキュリティとの違い



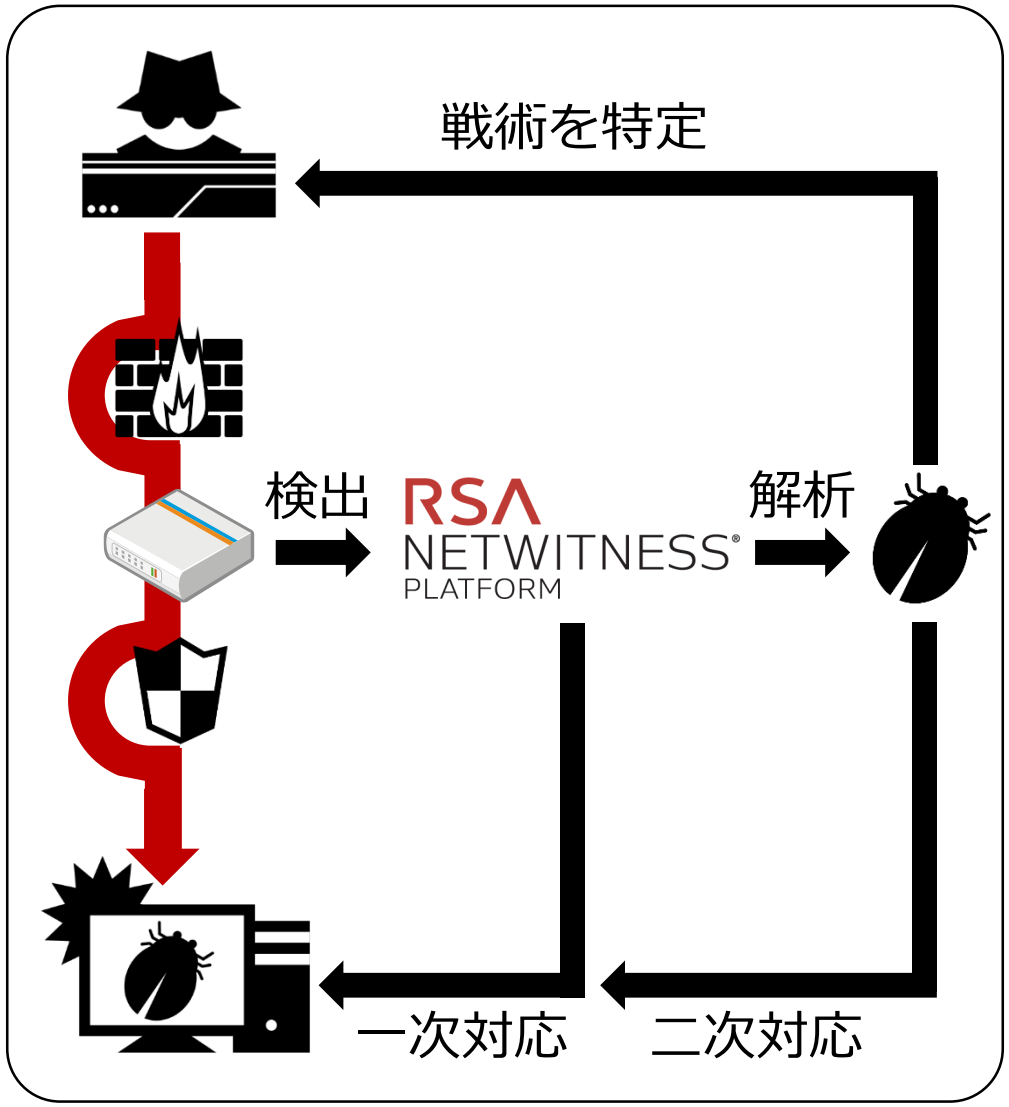
IPSやUTMのようなツールの目的は
自動的に脅威を検知・駆除・遮断すること

SOCの目的はセキュリティツールが出す
大量のアラートから真の脅威を識別し対応すること

スレットハンティングの目的は
アラートが上がらない隠れた脅威を発見すること

インテリジェンスの生成

お客様対応の経験



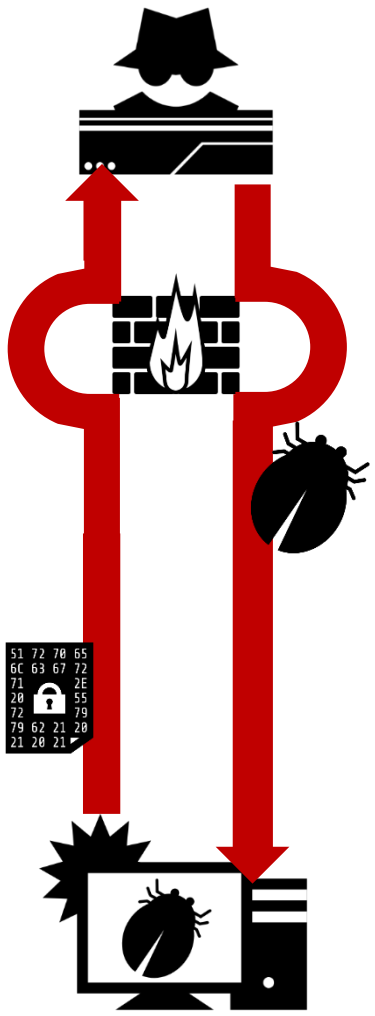
＋

外部情報

- セキュリティベンダ
- セキュリティ研究者
- CERT/CSIRT
- 企業
- 学術機関

＝ 実戦に耐えうるインテリジェンス

仮説の検証



仮説

攻撃者はマルウェアを暗号化して更に拡張子を偽装することで
ネットワークセキュリティにおけるマルウェア検出を回避する

検証方法

仮説条件に合うパケットを抽出するクエリを実行する

```
extension = "png" &&                    # 拡張子がpngである
filetype != "png" &&                    # バイナリの構造がpngではない
agent.ext !exists &&                    # ユーザーエージェントが存在しない
ir.general = "four_or_less_headers"     # HTTPヘッダが4個以下しか存在しない
```

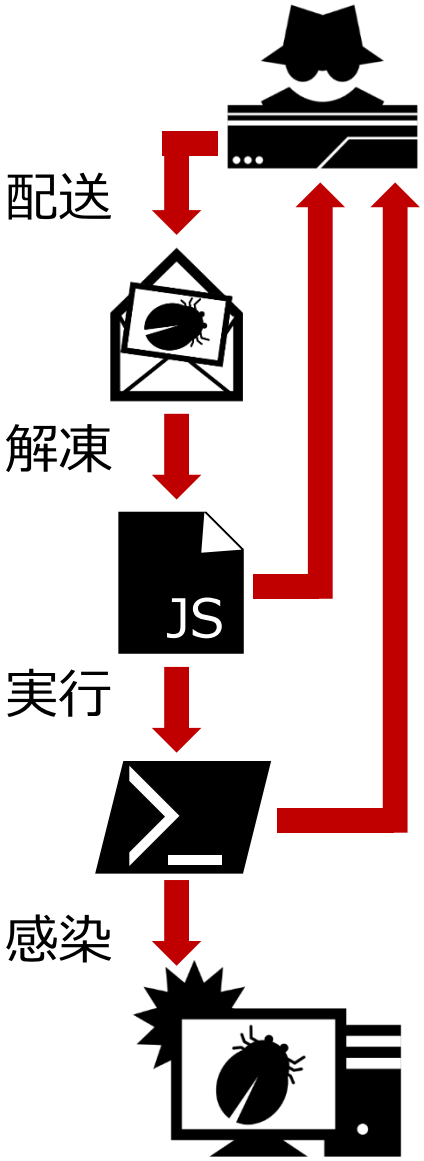
結果

ハッシュや通信先が違うが同じ戦術を採用したマルウェアが検出された
さらに画像ファイルに偽装されて外部に流出したデータを確保できた

セキュリティの強化

Chapter 3

分析結果のフィードバック



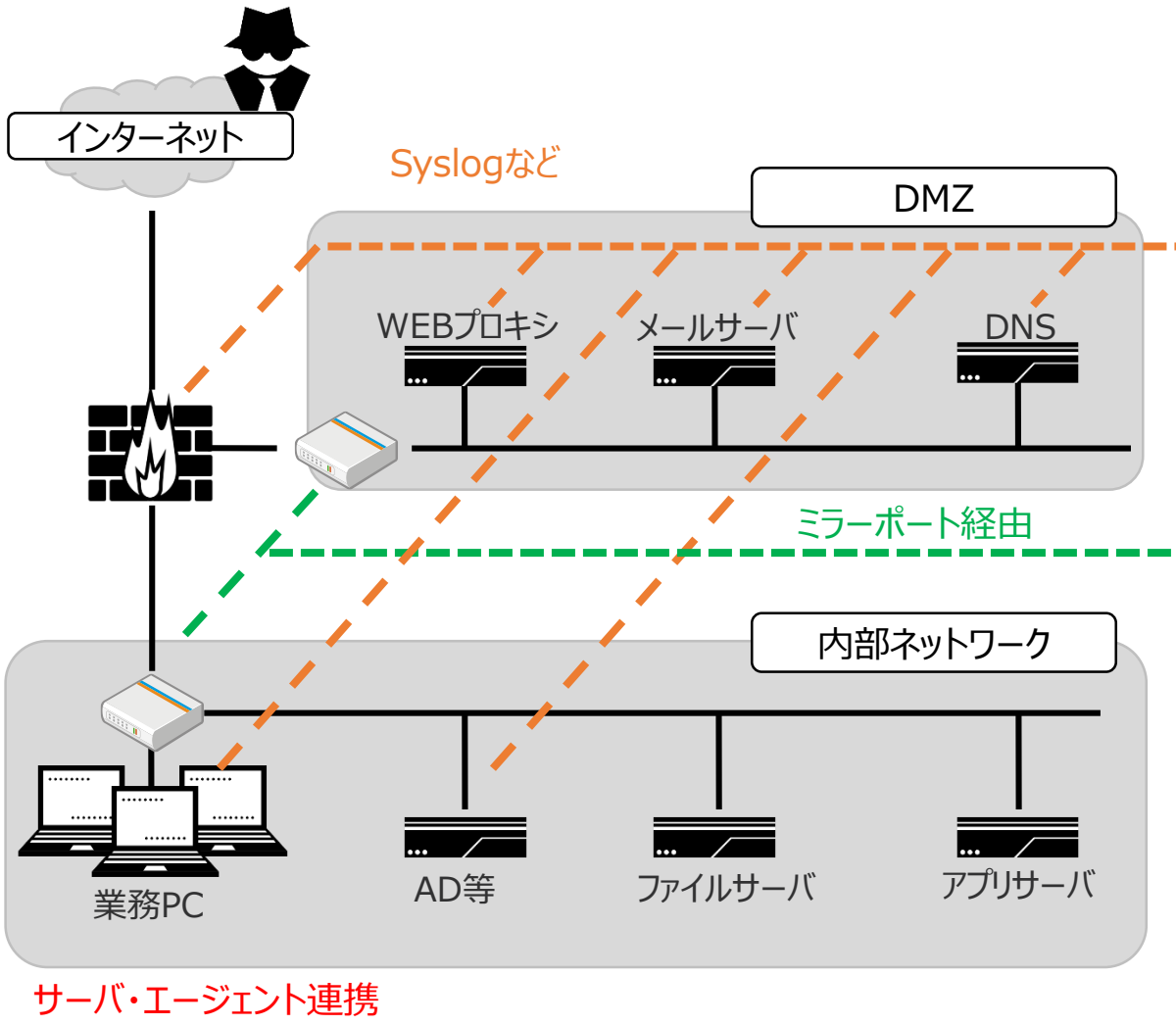
配送
パスワード圧縮されたドロッパーがスパムの添付ファイルとして配送される

実行
解凍されたjavascriptファイルが実行されるとPowershellスクリプトを取得する
Powershellスクリプトはメモリ上にロードされて実行される

感染
Powershellスクリプトはマルウェア本体を取得する
マルウェアは自動的にインストールされ感染活動を開始する

推奨策
添付ファイル付きメールのブロック
javascriptファイルの実行アプリケーション関連付け変更
Powershellプロセスによる外部通信のブロック

スレットハンティングサービス



RSA NETWITNESS® PLATFORM

Netwitness Logs

デバイスやサーバのログを集約

Netwitness Network

トラフィックの収取と蓄積

Canon

キヤノン ITソリューションズ株式会社

スレットハンティング

防御を回避した脅威の可視化

継続的チューニング

最新の脅威を捉える仮説検証

月次レポート

セキュリティの改善策を提案