WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

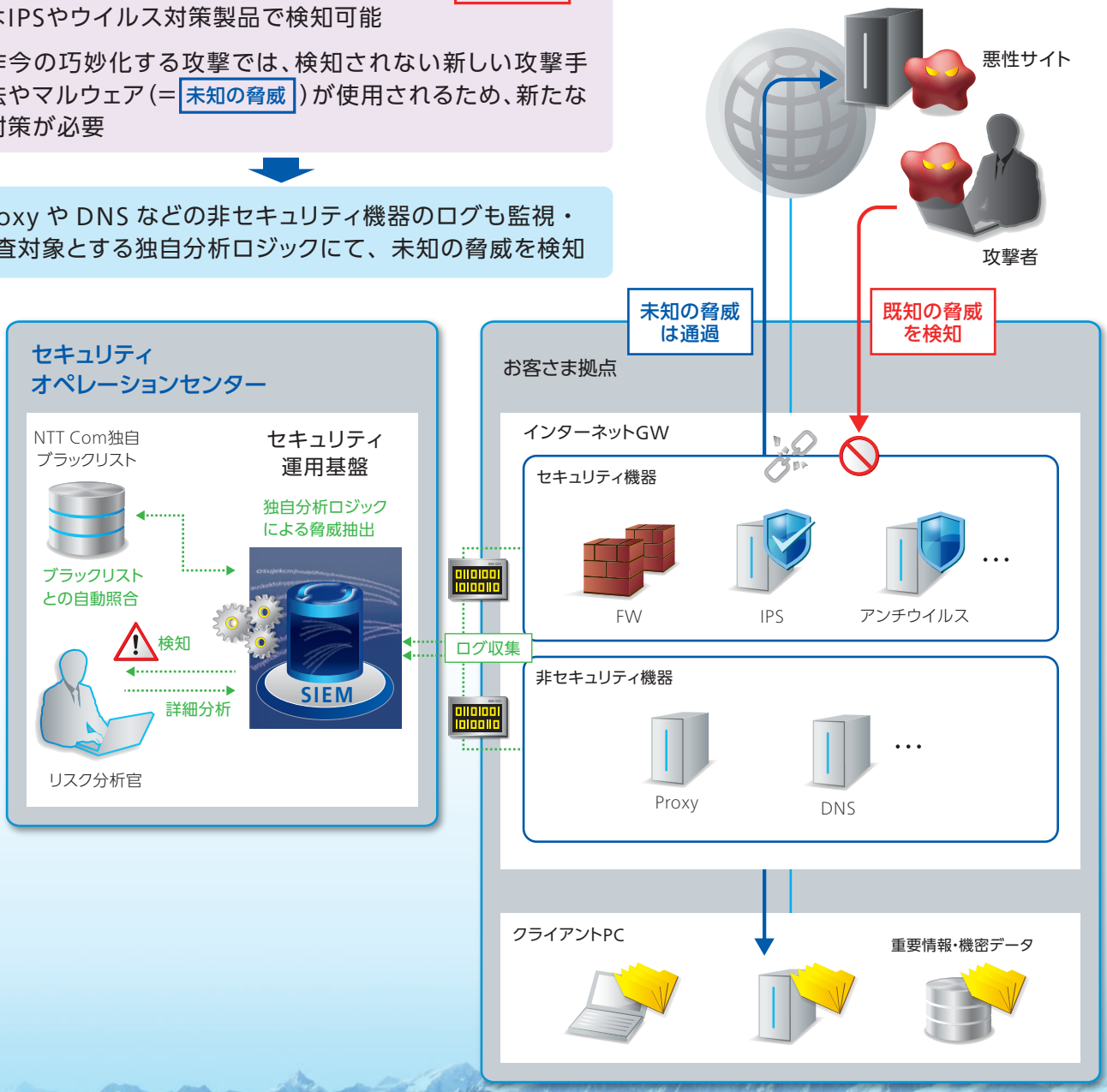
NTT Communications
Transform. Transcend.

Correlation Log Analysis (CLA)

企業のICT環境への巧妙な手法を用いた不正アクセスなど
未知のセキュリティ脅威をリアルタイムに検知する

- 過去に特定されている攻撃やマルウェア（＝既知の脅威）はIPSやウイルス対策製品で検知可能
- 昨今の巧妙化する攻撃では、検知されない新しい攻撃手法やマルウェア（＝未知の脅威）が使用されるため、新たな対策が必要

Proxy や DNS などの非セキュリティ機器のログも監視・調査対象とする独自分析ロジックにて、未知の脅威を検知

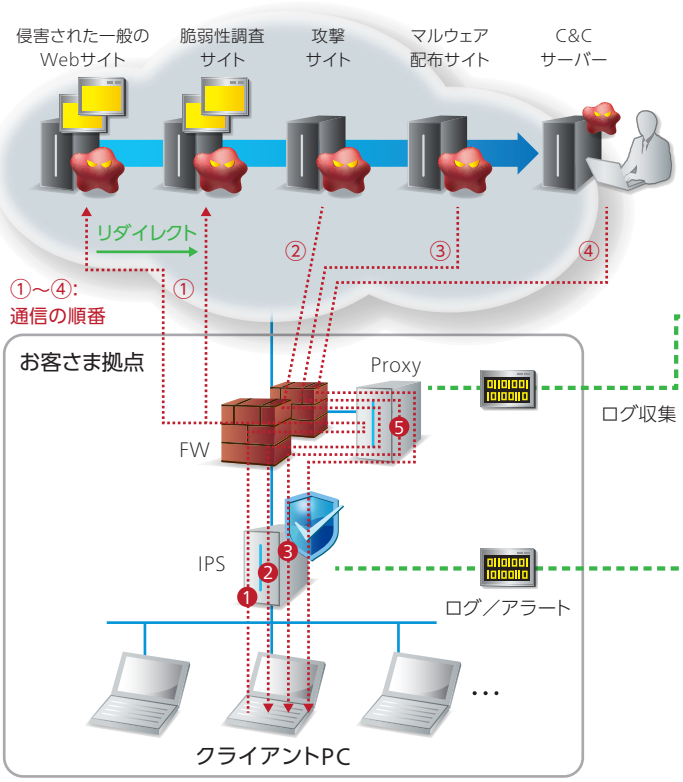


NTT Comはここが違う！

- 段階を踏み時間をかけて行われる攻撃を攻撃パターン抽出や長時間監視で見逃しません。(800以上の分析ロジック(2016年9月末時点))
- NTT研究所のハニーポットを活用した独自ブラックリストにより、悪性サイトとの通信有無を検知します。
- リスク分析官の最新の知見を定期的に分析ロジックに反映させることで、日々巧妙化する攻撃手法を効率的に自動検出でき、リスク分析官個々人のノウハウをGROC全体で共有、安定した分析レベルを実現します。
- セキュリティ運用基盤の自動検出とリスク分析官オリエンティッドの詳細分析機能(PCAPデータの呼び出しなど)で迅速な詳細分析報告を実施します。(リスク分析官がインシデントと判断してから目標15分)
- グローバル規模の、他の国や地域での流行や新手法の知見を分析に活用し、脅威の見逃しを低減します。
- セキュリティ運用基盤および分析ロジックは独自開発であり、市販されていないため、分析ロジックの解析や検出回避行動を防止できます。

《未知の脅威の検知事例》

ドライブ・バイ・ダウンロード攻撃を「セキュリティ機器:IPS」および「非セキュリティ機器:Proxy」のログを相関分析(CLA:Correlation Log Analysis)することで検出した事例



(1) IPSのシグネチャにて、通信 ① ② ③ を検知
(それぞれ単独では、誤検知と看過されるアラート ❶ ❷ ❸)

(2) SIEMの分析ロジックにより、❶ ❷ ❸ の組み合わせを「攻撃(キルチェーン)」であると判定(❹)

(3) (2)をトリガーにリスク分析官が分析を開始。Proxyログから生成されたアラート(❺)をチェックし、PCAPデータを解析、ファイルダウンロード ③ を確認し、攻撃を確信

(4) (3)を実施中にProxyログ内のアクセス先URLとNTT Com独自ブラックリストとの照合をSIEMが行い、C&Cサーバーとの接続 ③ を検出(❻)

(5) (3)および(4)の結果を踏まえて、リスク分析官が攻撃の全貌を把握し、対処方法をお客さまに提案

お問い合わせ先
NTTコミュニケーションズ株式会社
ホームページ www.ntt.com/business/services/security/security-management/wideangle.html

2016.09