FireEyeサンドボックスからSonicWallへマイグレーション
トラフィックに潜む脅威をCaptureATPで保護！

大手人材派遣業 B様

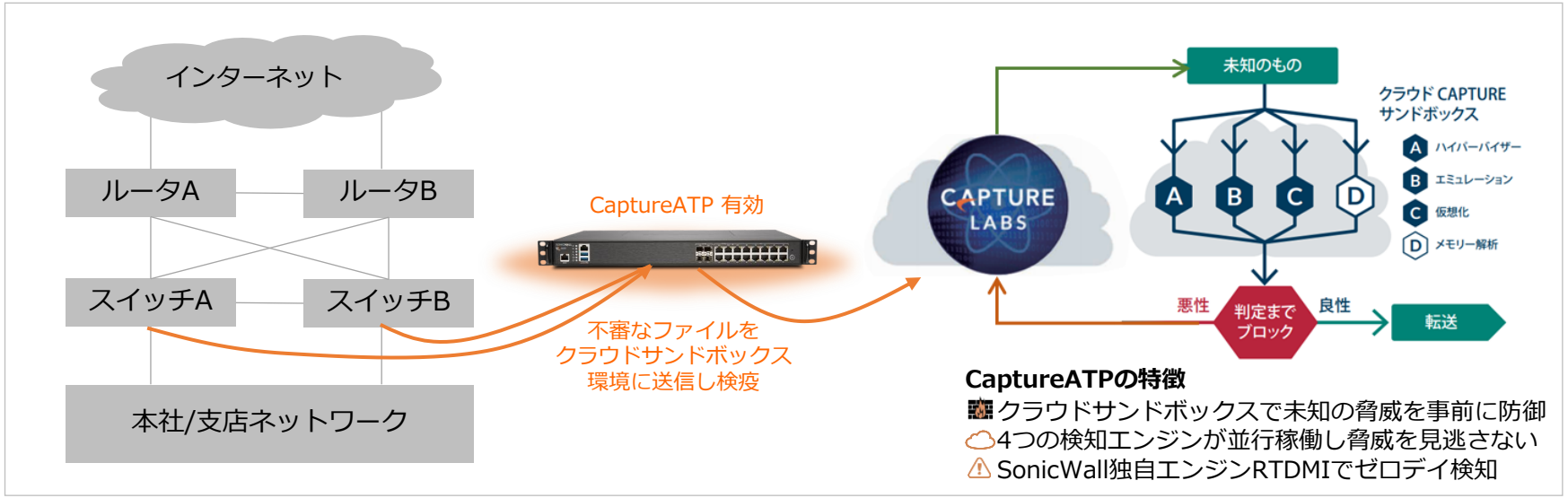
企業概要
社　　員：3000名
既存製品：FireEye NXシリーズ

課　題
FireEyeがEOLのため、後継機器を選定する必要があった。近年では会社のトラフィック量が増大したため、FireEyeでパケットロスが発生していた。また、近年の脅威をFireEyeをすり抜け、実被害が発生していたため、検知能力の向上も必至となっていた。

導入モデル
・NSa6700
タップモードでFWを配備。冗長化されたメインスイッチのトラフィックをSonicWall NSa6700にミラーリングさせ、全てのトラフィックをCaptureATP(クラウド型マルチエンジンサンドボックス)で検疫。

導入効果
導入した直後にこれまでFireEyeで検知できていなかった脅威をCaptureATPで検知することができた。無償で出力できるFW検知レポートによって経営層に対して稼働実績を報告することができるようになった。

1. FireEye NXモデルからSonicWallに完全移行
2. マルチエンジン搭載のCaptureATPにより検知能力向上
3. リモートアクセスVPNのトラフィックも検疫対象



CaptureATPの特徴
クラウドサンドボックスで未知の脅威を事前に防御
4つの検知エンジンが並行稼働し脅威を見逃さない
SonicWall独自エンジンRTDMIでゼロデイ検知