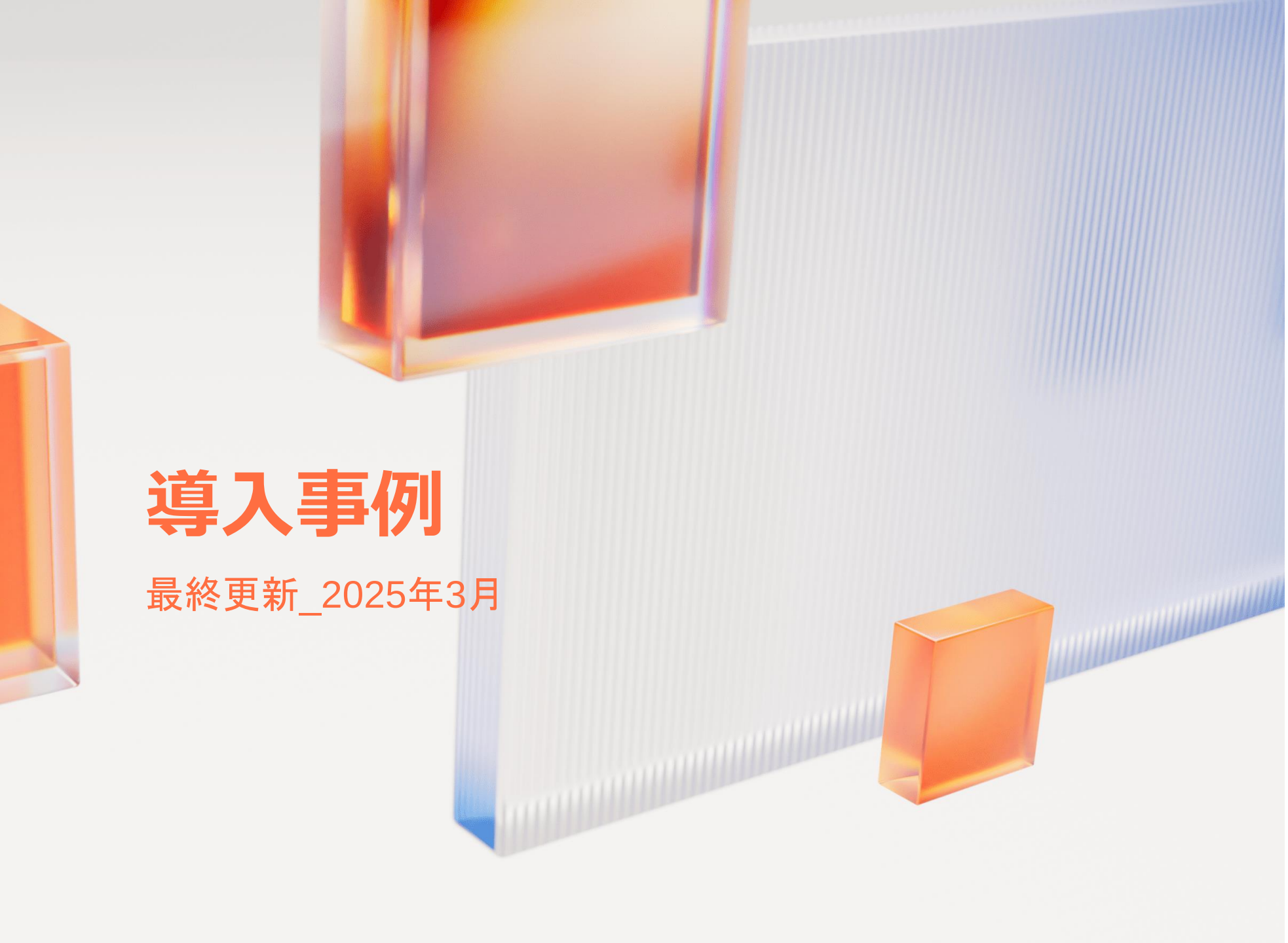


導入事例

最終更新_2025年3月

SONICWALL

導入事例_業種別

- 【NEW】Cloud SECURE EDGE
- 自治体／学校関連
- 医療／病院／士業
- 企業
- IT

Cloud SECURE EDGE

医療関係 K様

Cloud Secure Edge × HENNGEとのSAML連携！ HENNGE Oneを活用しアカウントライフサイクルを改善

企業概要
社　　員：45名
既存製品：HENNGE One

課　題
ルータのリモートアクセスアクセス機能を使っていたが、アカウント情報が整理されておらず、退職者のアカウントから社内にアクセスされるインシデントが発生していた。

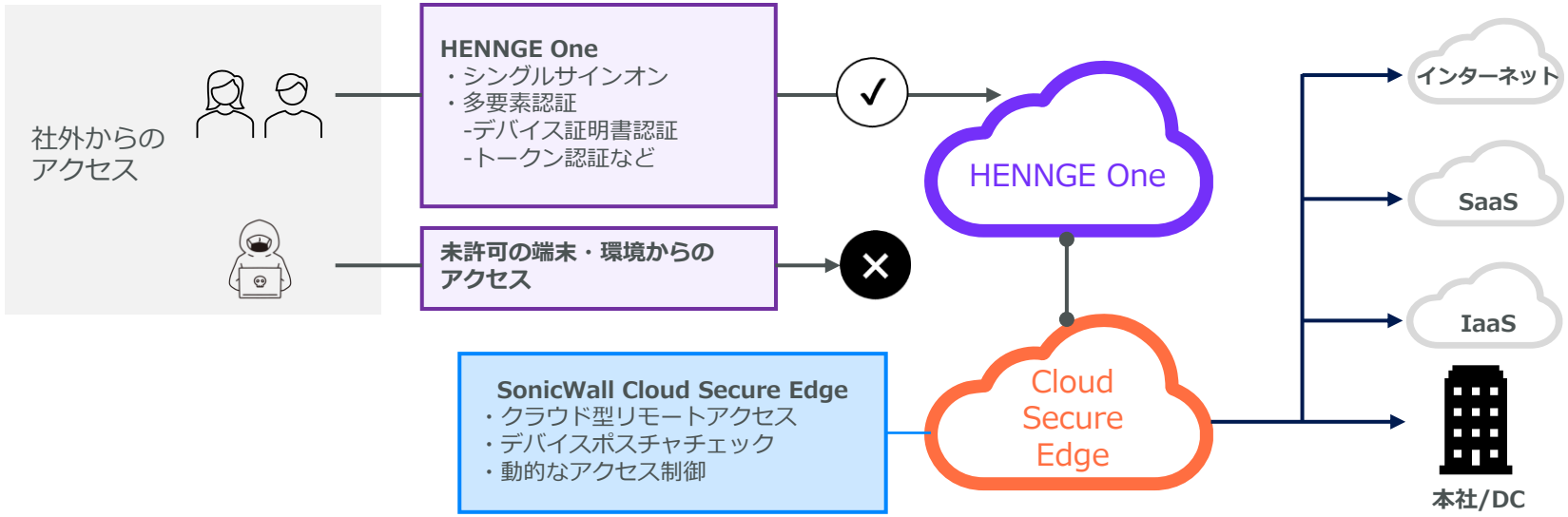
導入ソリューション
・HENNGE One
・Cloud Secure Edge
　・SPA Basic 45
　・SPA Advanced 2ライセンス

導入効果
HENNGE OneとCloud Secure Edgを連携させることで、アカウント運用を一本化することができた。また、これまで認証はID/のみだったが、HENNGE Oneのデバイス証明書を使用した多要素認証により、リモートアクセスアクセス接続時のなりすまし対策を強化することができた。

1 アカウント運用をHENNGE Oneで一本化

2 HENNGE、SonicWallともに内製による手厚いサポート体制

3 リモートアクセス接続時にHENNGE Oneの多要素認証を適用



Cloud Secure Edgeでオンプレミス VPN環境の脱却 脆弱性対応のない安心安全なリモートアクセス環境を実現

SIer C様

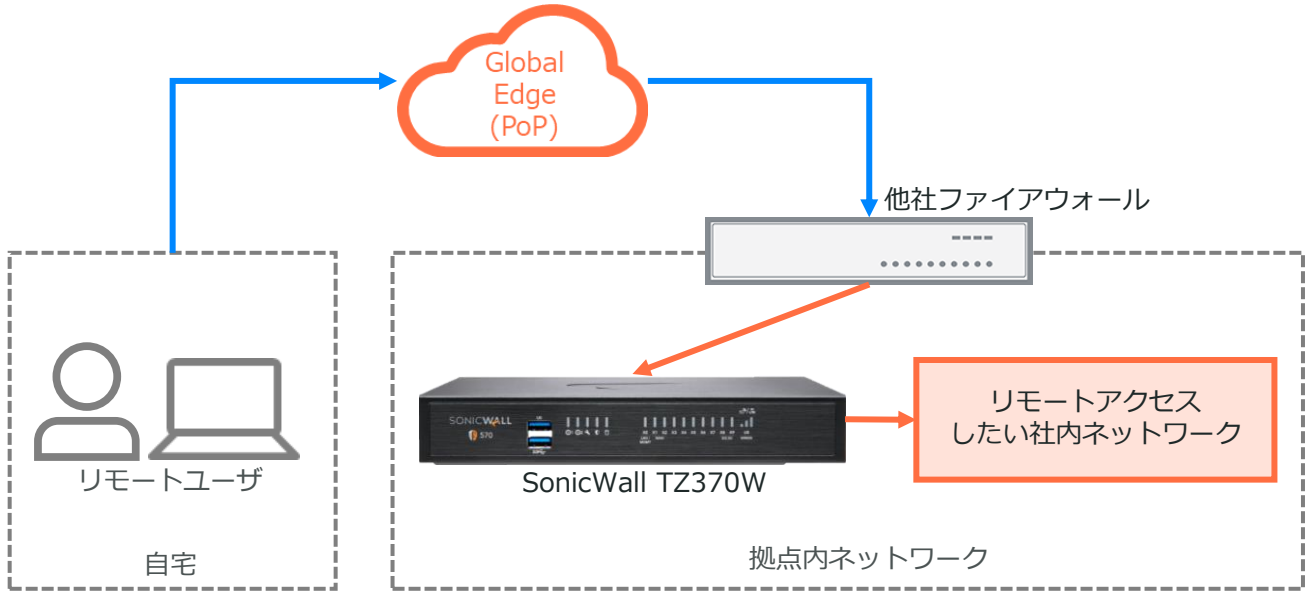
企業概要
社　　員：110名
既存製品：他社ファイアウォール

課　題
他社ファイアウォールのSSL-VPNを利用していたが度々発見される脆弱性の対応に苦慮。脆弱性対応を必要としないリモートアクセスを検討していた。

導入ソリューション
・TZ370W
・Cloud Secure Edge
　・SPA Basic 60ライセンス
　・SPA Advances 20ライセンス

導入効果
既存の他社ファイアウォールはそのままで使用し続けるがSSL-VPN機能を無効にし、リモートアクセスはCloud Secure Edgeで行うようポリシーを変更。脆弱性対応の必要がなくなった。これにより脆弱性を起因とした不正アクセスのリスクもなくなった。リモートアクセスの使い勝手はこれまでと変わらず、スムーズな移行ができた。

1. 脆弱性対応含むVPN機器の管理不要
2. 脆弱性を悪用した不正アクセスリスクの低減
3. アクセス先がIaaSでもオンプレでも一貫した認証ポリシーを適用



情報通信業 T様

Cloud Secure Edgeでリモートアクセス環境を再整備！
デバイスポスチャ機能で会社PCからの利用に限定！

企業概要
社　　員：50名
既存製品：SonicWall TZ570W

課　題
社員向けにリモートアクセス環境を整備している。多要素認証を有効にしているが、私用デバイスによる接続が確認されている。会社貸与デバイスに限定したリモートアクセスを実現したい。

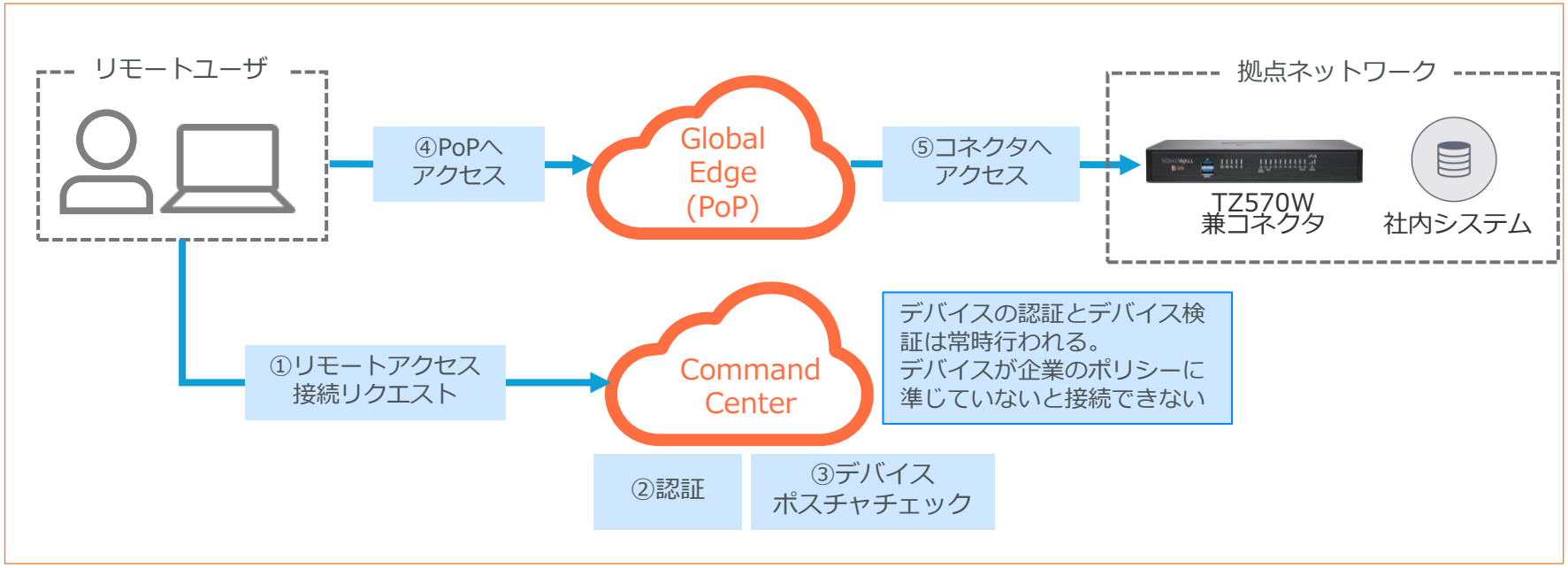
導入ソリューション
・既存のTZ570W
・Cloud Secure Edge
　・SPA Basic 20ライセンス
　・SPA Advanced 5ライセンス

導入効果
Cloud Secure Edgeのデバイスポスチャチェック機能により、会社貸与デバイスに限定したリモートアクセス環境を再整備することができた。具体的には特定のレジストリ値の有無をチェックすることで判断している。既存でIDaaSを利用していたため、CSEの導入はスムーズに行うことができた。

1 デバイスポスチャチェックにより不正アクセスのリスクを低減

2 既存TZ570WをCSEのコネクタとして利用

3 FWの負荷をCSEにオフロードすることでパフォーマンス向上



地方インフラ T様

企業概要
社　　員：130名
既存製品：他社ファイアウォール

課　題
社内では5つの部署がリモートアクセスを利用しているが、部署ごとおよび役職ごとにアクセス先の権限が整理されていなかった。特に情報システムがアクセスする高セキュリティエリアに対して厳格なアクセス制御が必要だった。

導入ソリューション
・TZ670W
・Cloud Secure Edge
　・SPA Basic 100ライセンス
　・SPA Advanced 15ライセンス
　・SIA Advanced 100ライセンス

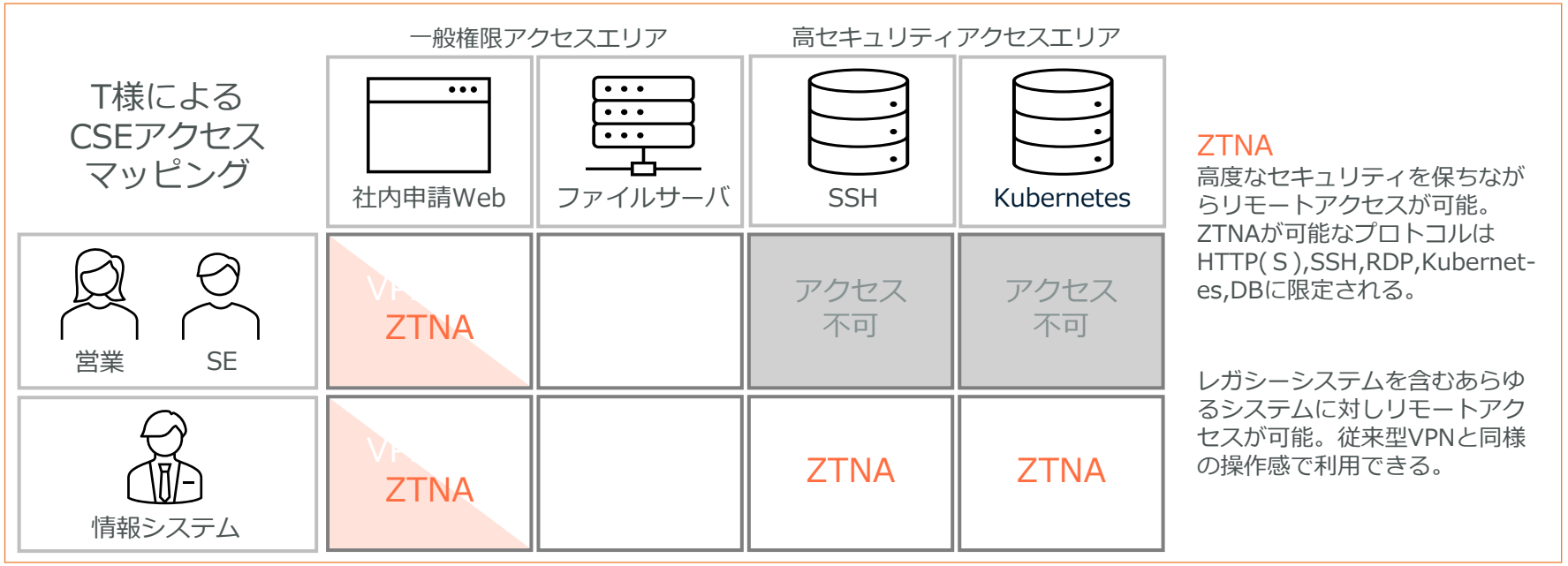
導入効果
リモートアクセスで接続する社内システムを部門および役職ごとに整理し、誰がどのシステムにZTNAとVPNaaSを使用して接続するかのアクセスルールを策定。ZTNA/VPNaaSにより不正アクセスリスクを低減しつつ、脆弱性対応の必要もなくなったため運用工数が削減された。

Cloud Secure EdgeのVPNaaSとZTNAにより利用者ごとに適切なアクセス手法を提供

1 VPNaaSとZTNAを接続先リソースごとに細かくアクセス制御

2 高セキュリティエリアにはZTNA、一般接続エリアにはVPNaaS

3 従来型VPNに比べて不正アクセスリスクを大幅に低減



自治体／学校関連

K市教育委員会様

GIGAスクール構想により市内29校にNSa2650を導入！ ICT教育を支える安全なネット接続を実現

分野
教育機関

課　題
各学校のインターネットトラフィックは教育委員会ネットワークのセンタールータに集約されインターネットに接続する形態であった。GIGAスクール導入に伴い各学校のトラフィックが大幅に増加することを危惧。各学校から直接インターネットに接続できる構成に変更することが要件であった。各学校からインターネットアクセスが可能になることによりセキュリティ対策の強化が急務であった。

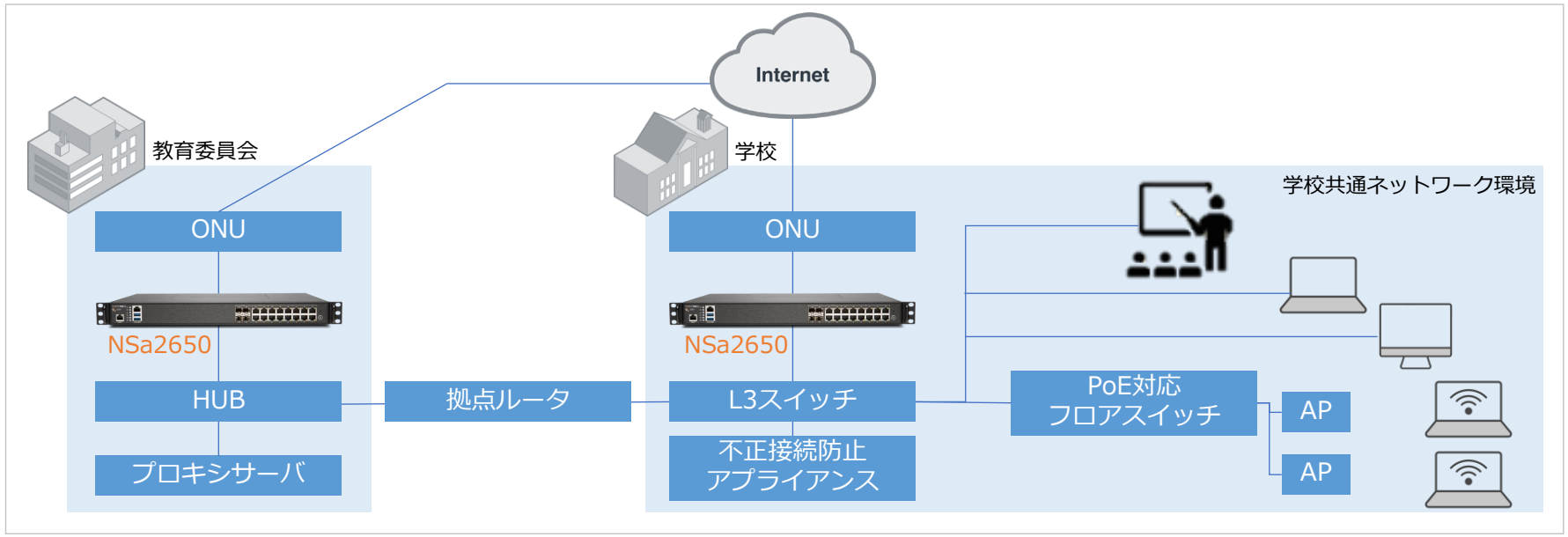
導入モデル
・NSa2650 30台
教育委員会に1台、市内29校に1台ずつ配備。

導入効果
インターネットブレークアウト機能によりトラフィックに応じて学校から教育委員会ネットワークへのアクセスと直接インターネット接続を分散することができた。
1クラス30人の児童たちが一斉にタブレットを利用しても快適にアクセスができ、200人以上の教職員が同時に参加する研修でも全く問題がなかった。トラフィックの比較でも、コストパフォーマンスが最も優れていた。

1 インターネットブレークアウトによりトラフィックを分散

2 CaputureATPにより各学校のセキュリティレベルが向上

3 200人以上が参加するWeb研修でもパフォーマンスに問題なし



H市役所様

分　野
地方自治体

企業概要
職　　員：3700名
既存製品：ファイアウォール、IPS

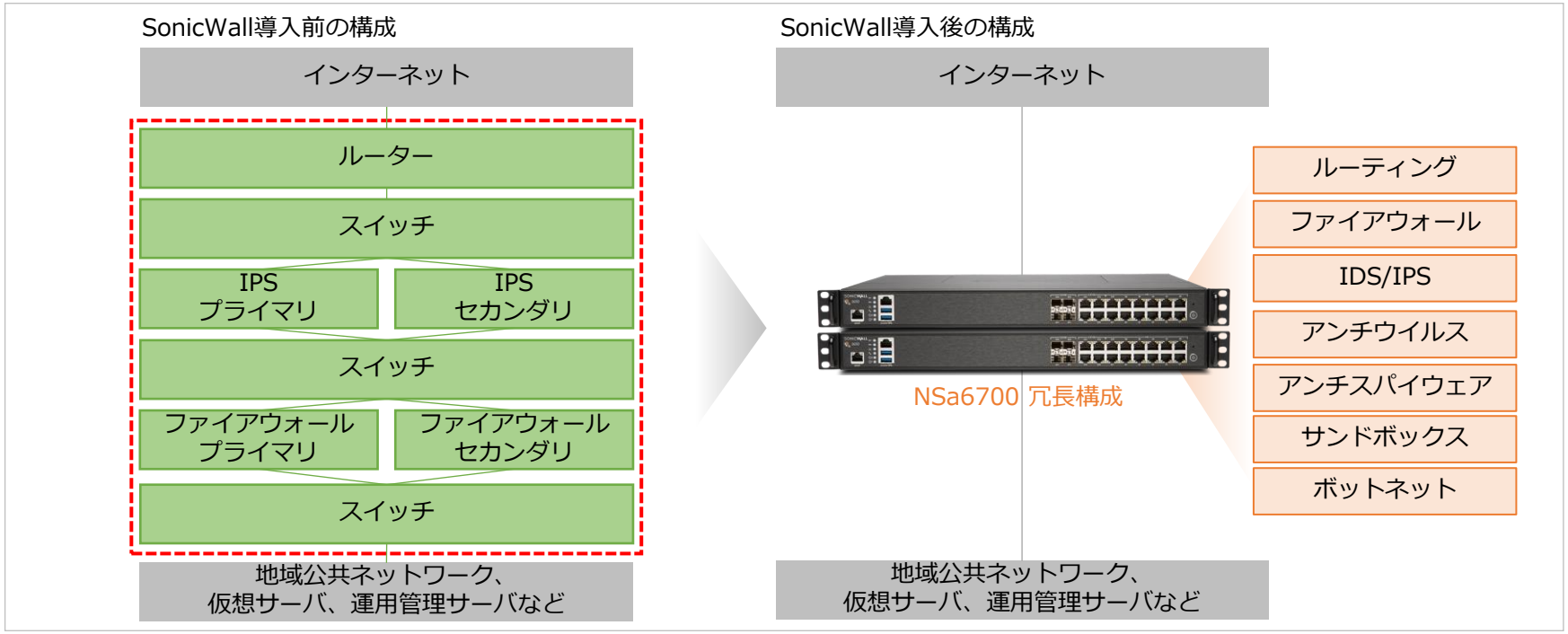
課　題
H市ゲートウェイにはルータ、スイッチ、IPS、FWのアプライアンスが配備されており、複数機器の運用管理の問題や、多段構成によるパフォーマンス低下の問題を抱えていた。また、高度な脅威に対してシグネチャ以外の対策を進める必要があった。

導入モデル
・NSa6700 冗長構成

導入効果
管理するアプライアンスが8つからNSa6700の2台に集約することができ、コスト削減・パフォーマンスが向上した。UTMのセキュリティ機能を全て活用することでセキュリティ対策のレベルを強化することができた。

UTM機能全体の性能とコストパフォーマンスが決め手
8つのゲートウェイアプライアンスを2つに集約！

1. 複数セキュリティ機能をSonicWallに全て集約
2. 費用対効果の高いモデルで満足いくパフォーマンス
3. サンドボックスによりシグネチャに依存しない対策を実現



関西圏教育機関（某大学）様

NextGenFWの導入でセキュリティ対策を強化し キャンパスにおける統合的なWiFi環境も実現！

1 マルチクラウドサンドボックスエンジンで最新の脅威

2 自動プロファイル配信によりアクセスポイント簡易デプロイ

3 単一のコンソールでUTMとアクセスポイントを一括管理

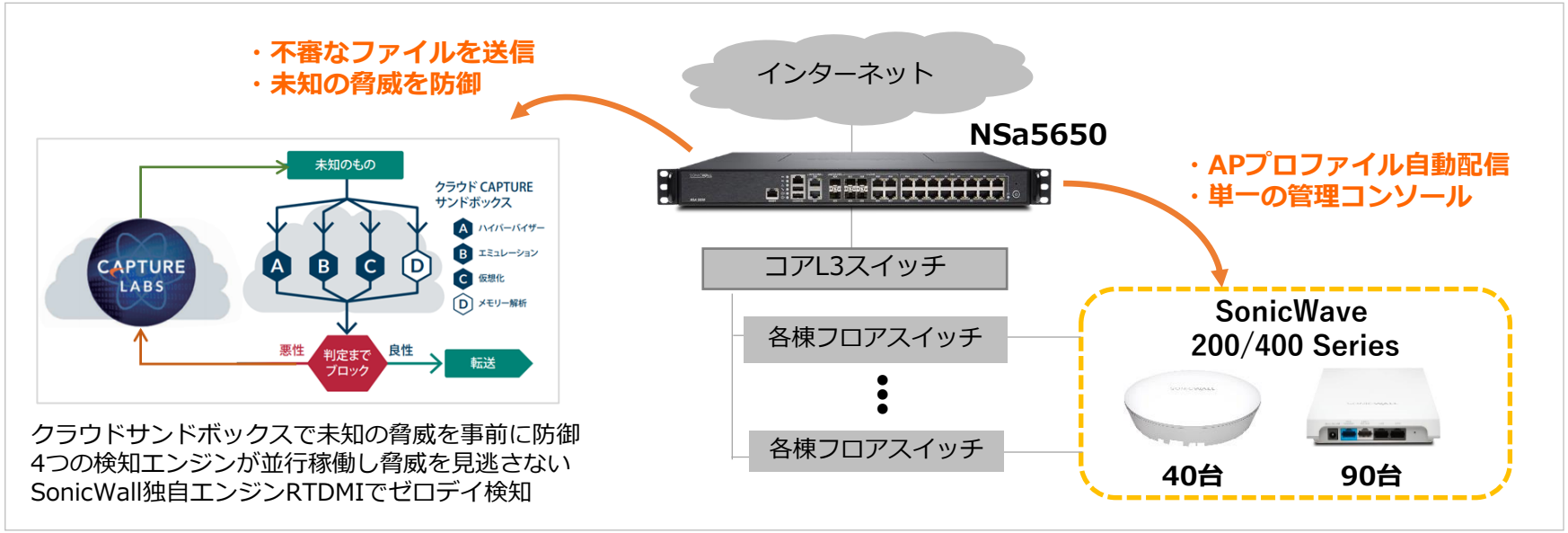
分　野
教育機関

企業概要
学生/教員：1500名
既存対策：従来型ファイアウォール

課題
・最新の脅威に対応するために既存のFWでは不十分であり、次世代FWの導入を検討。また、新型コロナウィルスの影響により授業をオンライン化するため、簡単導入かつ簡易管理可能なアクセスポイントの採用も差し迫った課題であった。

導入モデル
・NSa5650×2台
・SonicWave×130台
NSa5650＋Capture ATPを出入口対策として導入。また、WiFiコントローラ機能も提供しており合計130台のAPを統合管理。

導入効果
Capture ATP（マルチサンドボックスエンジン）により最新の脅威に対応。さらにNSa5650管理コンソールから全てのAPが統合管理可能で情報システム担当者（1名）の運用負担/コストを大幅削減。



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

医療／病院／士業

千葉県内 市立A病院様

分　野
地域中核病院

企業概要
病床数　：約600
既存対策：SYSLOGベースの解析ツール

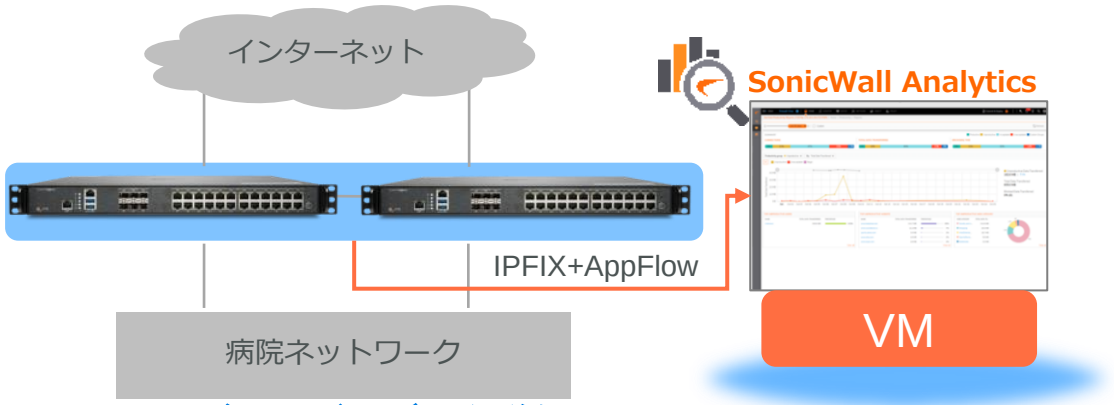
課　題
他病院で不正アクセスや攻撃による甚大な被害が報告されており、同院でも兆候の発見、検知やブロックの状況を早期に把握することが急務だったが、既存ツールでは十分でなく、迅速な初動の為にNWセキュリティを可視化できるツールが必要であった。

導入モデル
・Analytics IPFIX オンプレミス/VM版
・NSa 4700 6台
UTMが発信するデータをAnalyticsが分析表示することにより、攻撃・トラフィック・アプリケーションを詳細に可視化。

導入効果
問題を未然に把握し、迅速な初動対応が可能となった。レポート生成機能により、具体的で詳細なIT運用報告を院内に対して行うことができた。

他病院での被害教訓から、不正アクセスや攻撃を早期に分析・可視化し、問題の早期発見と迅速な対応を実現

1. 異常兆候の把握、インシデント発生時の迅速な初動対応
2. 院内の月次IT運用報告資料としてAnalytics生成レポートを利用
3. ネットワーク輻輳時の状況や原因の確認



UTMがサーバへデータ送信

UTMから収集したデータをモニタ・蓄積・分析して可視化

可視化されたデータを元に迅速な初動対応、月次報告会にレポート利用

SMA6210 × HENNGEとのSAML2.0連携！
顧客ID認証基盤との連携で認証ポリシーの一元化を実現

医療福祉 T様

企業概要
社　　員：7500名

課　題
3つの社内アプリケーションをオンプレミスで開発予定。外勤の従業員がPCおよびスマホでアプリにリモート接続。以下の要件を満たす必要があった。
1.HENNGEとのSAML2.0連携
2.クライアント証明書認証
3.接続元IPアドレスの制限
4.接続グループごとのポータルサイト構築
5.リスクベースアクセス制御
　5.1.アンチウイルスソフトの更新状況
　5.2.Windowsバージョン
　5.3.Active Directoryドメイン参加

導入モデル
・SMA6210
・同時接続800ユーザライセンス

導入効果
SonicWall SEが顧客の検証環境で顧客と一緒に検証を行うことで、顧客が求める全ての要件を満たすことができた。
スループットパフォーマンスも問題なく全て想定通り稼働できている。

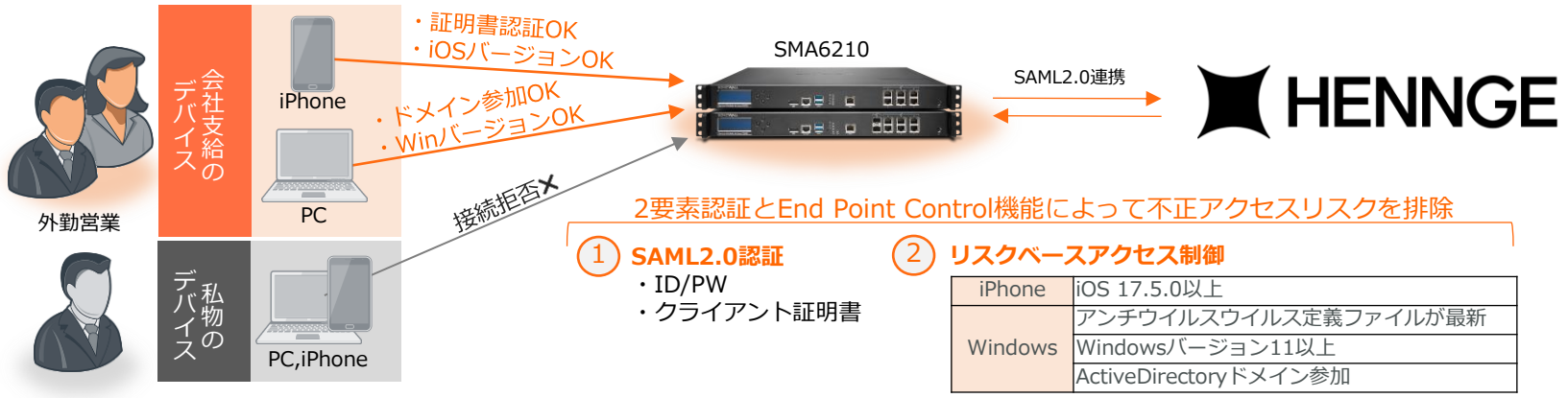
1 HENNGE OneとのSAML2.0連携

2 SMA End Point Controlによるリスクベースアクセス制御

3 柔軟なアクセス認可設定により“最小特権の原則”を実現

顧客要件
・ユーザ認証
・デバイス認証
・デバイスの信頼性を確保

対応策
・HENNGE Oneとの連携
・クライアント証明書認証
・End Point Control



都内法律事務所 G様

UTMとEDRによる多層防御で“弁護士情報セキュリティ規定”に準拠した対策を実現！MSSPで無駄のないライセンス購入

分　野
士業

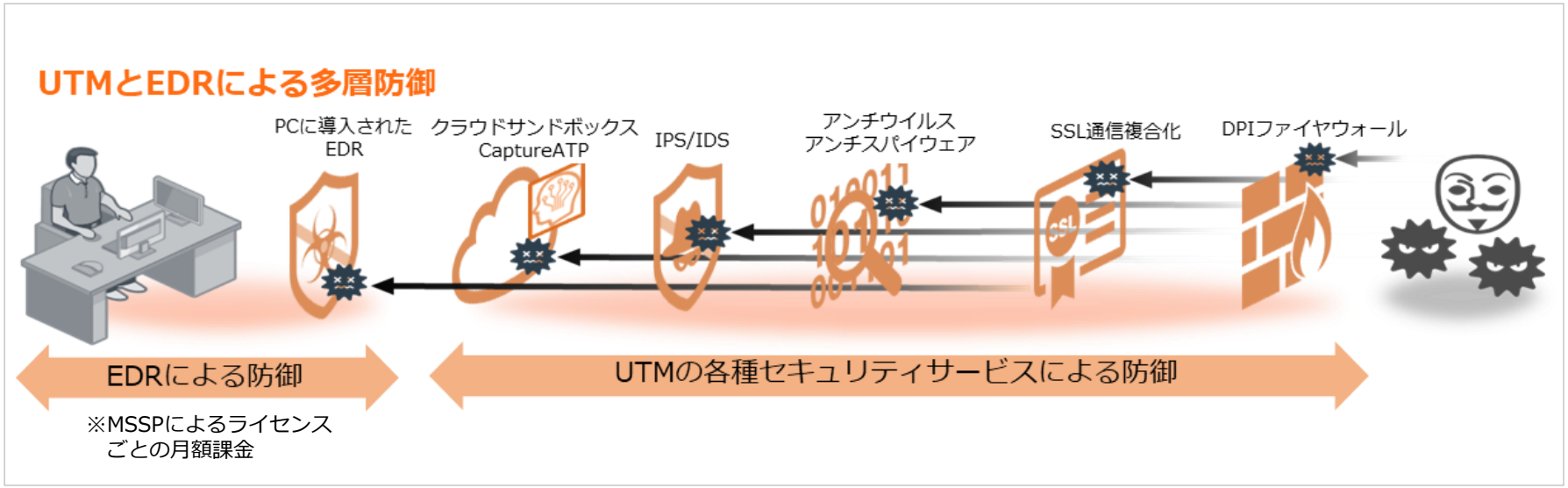
企業概要
弁護士およびスタッフ：100名/5拠点
既存製品：PC標準のアンチウイルス

課　題
・同業他事務所でサイバー攻撃によってシステム破壊事案が発生したことにより、サイバーセキュリティへの危機感が増した。
・明確なIT管理者がおらず、セキュリティ対策をどこから着手してよいか分からない状況であった。
・2024年6月に施行される「弁護士情報セキュリティ規程」の水準をクリアする必要があった。

導入モデル
・TZ570W × 5台
・Capture Client(EDR) × 100ライセンス

導入効果
今回の導入策をセキュリティ対策の屋台骨として、自所の情報セキュリティ規定を定義し、実践することができた。

1. 日弁連が定める弁護士情報セキュリティ規定への対応
2. エンドポイントとネットワークの多層防御を実現
3. MSSPによる柔軟で無駄のないユーザライセンス購入形態を採用



企業

SonicWall NSa2700 冗長構成で安心・安全な社内重要システムの外部アクセスゲートウェイを構築

平井精密工業株式会社様

分　野
精密機械部品を製造する総合加工メーカー

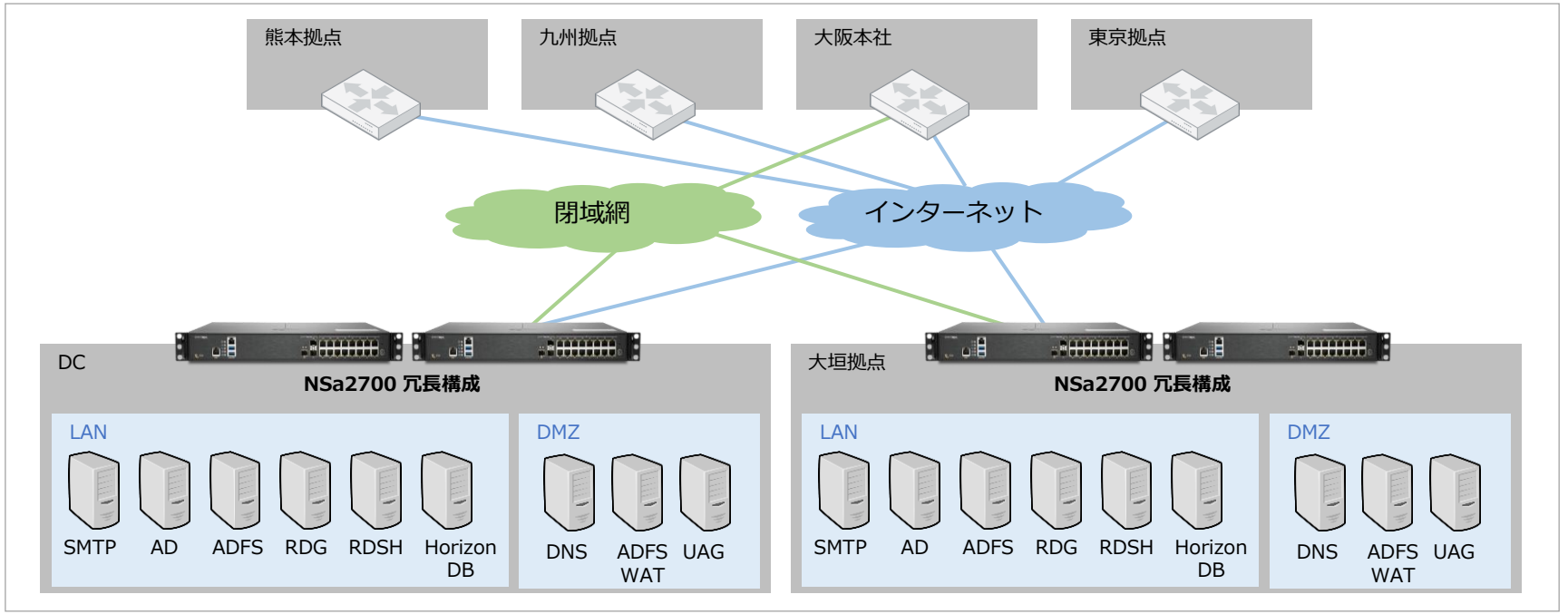
企業概要
社員：436名
営業拠点：大阪本社、東京、大垣、九州
生産拠点：大阪本社、大垣、熊本
データセンター：1拠点

導入モデル
・NSa2700×4台 (冗長構成 2式)
データセンター、大垣拠点にNSa2700を配備。外部からLAN内の重要システムへのアクセスを受け付けるゲートウェイとして稼働。またコンテンツフィルタリングで有害サイトへのアクセスを制御。

導入効果
費用対効果の高いスペックと冗長構成により可用性を維持することで、安定した業務を行えている。また、社内システムに対する各種偵察攻撃に対し遮断とログ出力によって効果を可視化できている。

今後の展望
SonicWallの無線アクセスポイント(SonicWave)やスイッチ(SW series)をNSa2700で統合管理を検討中。

1. ADFS、RDP、VDIの外部アクセスをSonicWallに集約
2. 公開サーバに対する外部からの攻撃を遮断
3. BCP対策としてミラーサイトにもSonicWall冗長構成



専門商社 D様

SonicWallをSOCの監視によりNIST SP800 CSFに準拠！「検知できる仕組み」と「対応できる体制」を実現

分　野
卸売・小売業

企業概要
社　　員：1100名
拠　　点：国内3拠点

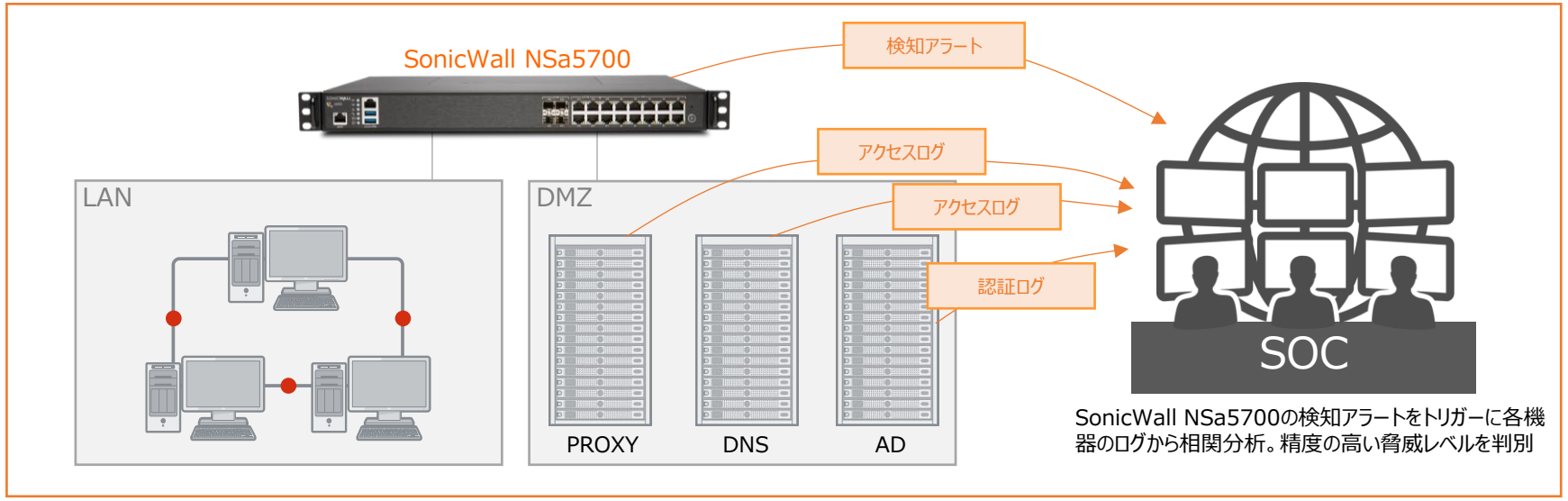
導入背景
・海外でマルウェア感染したPCが社内で感染拡大。情報システム部門が事態収束までおよそ3か月間対応。
・検知の仕組み、検知後の体制強化が急務

導入モデル
・SonicWall NSa5700
・クラウド型サンドボックスオプション
・他社 SOCサービス

導入効果
外部の脅威に対しSonicWall次世代ファイヤウォールで検知し、MSSによって適切な対処・復旧対応を可能とするセキュリティ運用体制を実現。システム担当者はアラートの都度調査・分析する手間を省き、重要業務に集中して取り組むことができた。

NIST サイバーセキュリティフレームワークを活用したD社のインシデント恒久対策マッピング

サイバーフレームワークのコア機能	特定	防御	検知	対応	復旧
	情報資産・脅威の洗い出し・ポリシー策定	サイバー攻撃を防ぐための防御策を実施	サイバー攻撃の発生を検知する	検知されたサイバー攻撃に対処する	サイバー攻撃による被害から復旧する
D社の実施内容	恒久対策方針策定	次世代ファイヤウォール SonicWall NSa5700 GWアンチウイルス・侵入防止 ボットネットフィルタ・サンドボックス		マネージド・セキュリティ・サービス 相関分析・アラートレベル判別 推奨対策案提示・定期レポート	
	セキュリティポリシーの制定				
	システム監査	PCアンチウイルス		情報システム部による社内連携	情報システム部による復旧作業・改善



SonicWall NSa5700の検知アラートをトリガーに各機器のログから相関分析。精度の高い脅威レベルを判別

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

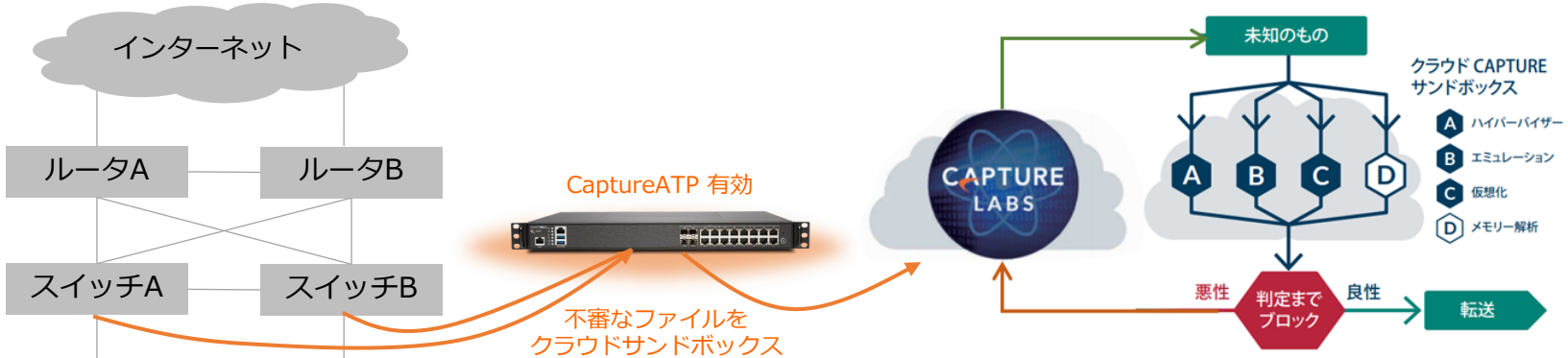
企業概要
社　　員：3000名
既存製品：FireEye NXシリーズ

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

化粧品メーカー E様

SonicWall × SecureSoft e-Gate SOCで 外部/内部で発生する脅威をプロアクティブに検知かつ対処！

分　野
製造業

企業概要
社　　員：300名

課　題
従業員による不正なアプリケーションを利用したことによるマルウェア感染インシデントが発生。標的型攻撃および内部不正利用を検知・対処できる仕組み作りが急務だった。

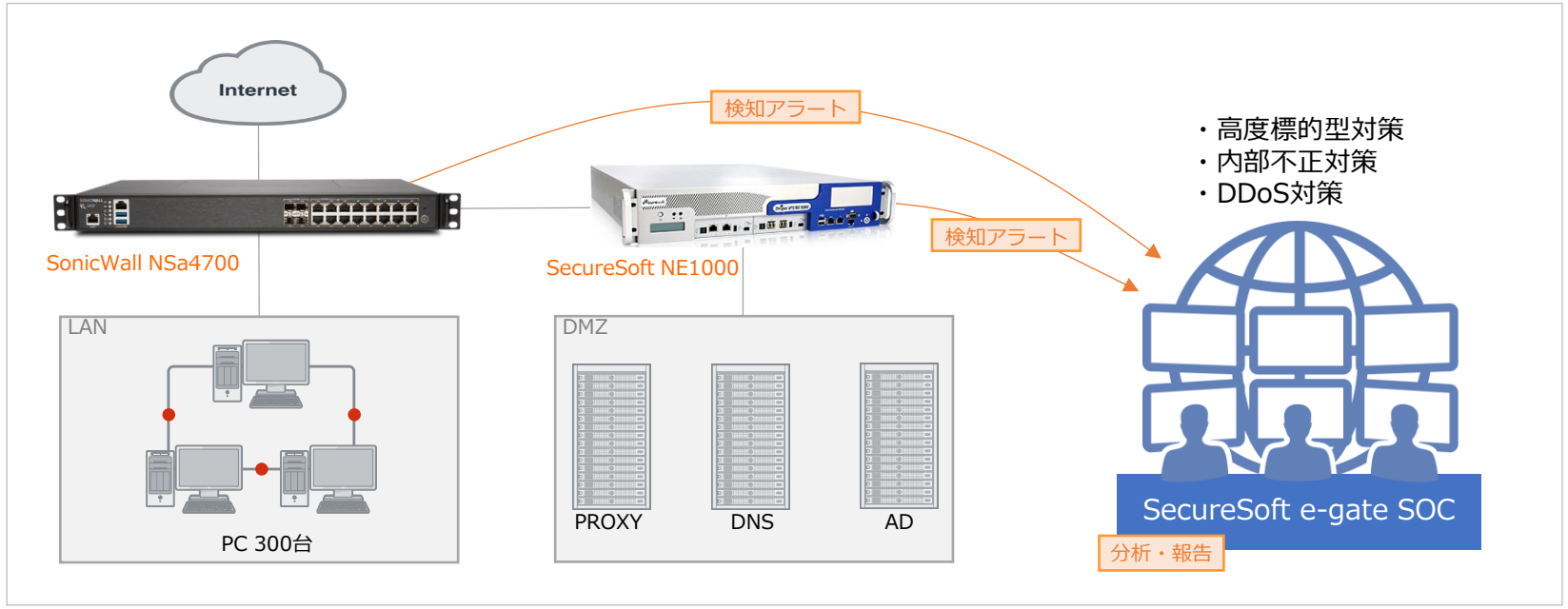
導入モデル
・SonicWall社 NSa4700
・SecureSoft社 Sniper NE1000
・SecureSoft社 e-Gate(SOC)

導入効果
外部・内部で発生するサイバー脅威に対しNSA4600及びSniperNE1000で検知し、e-Gate SOCによって適切な対処を可能とするセキュリティ運用体制を実現。標的型攻撃や内部不正だけでなくDDoSの検知も可能となった。

1 ActiveDirectory,PROXY,DNSのログと相関分析

2 独自脅威インテリジェンスによって標的型攻撃・DDoS攻撃に対応

3 相関分析により内部不正アクティビティの兆候を検知



高級アパレル H様

企業概要
店舗数：国内11拠点
既存対策：NEC、アライドテレシス

課　題
全国にある店舗では、百貨店のネットワークに相乗りする形で運用されており、路面店では即興的に機器が調達されるなど、システム構成が統一されていなかった。
特にネットワークセキュリティ対策は全く施されていなかった。既存のルーター契約や百貨店のネットワーク構成を変更せずにセキュリティ強化を図ることが求められていた。

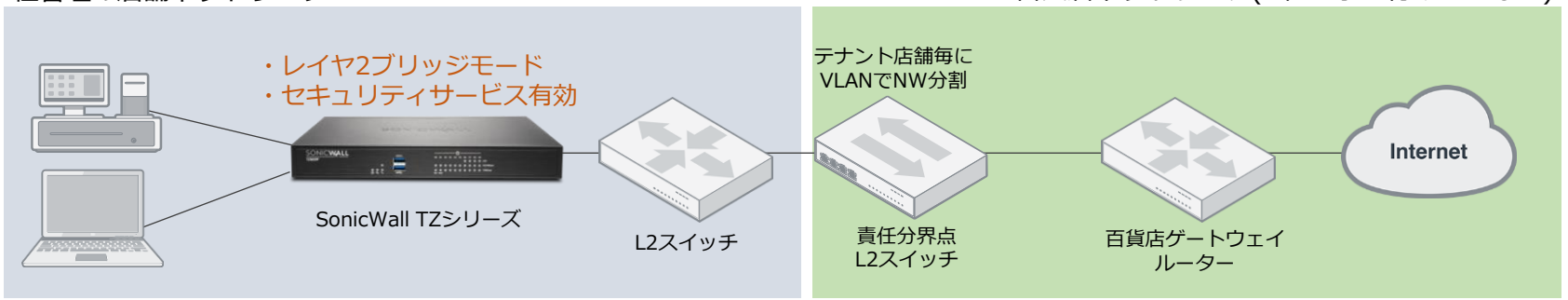
導入モデル
・TZ370W 4台
・TZ470W 6台
・TZ670 1台
レイヤ2ブリッジモード(インラインモード)による配置方法で既存のネットワーク構成を変えることなく導入。

導入効果
店舗に設置されたPCには、H社が重要視する販売情報、在庫情報、マーケティング情報が保管されています。SonicWallの導入により、データの機密性が向上し、従業員は安心して日々の業務に集中できるようになった。

百貨店/路面店の既存ネットワーク環境をそのままに全国11店舗のセキュリティレベルを向上！

1. レイヤ2ブリッジモードにより既存環境はそのまま
2. 店舗PCの重要情報をUTMセキュリティサービスで保護
3. 導入リスクが少なく1店舗あたりわずか2分で導入完了

レイヤ2ブリッジモードとは？
SonicWall UTMがブリッジのように機能し、トラフィックに対しセキュリティ機能で検疫は行うが、IPアドレスを変更したり、ルーティングを行ったりすることはしない。これにより、既存のネットワーク構成を変更せずにセキュリティ機能を追加することが可能。



ネットワークセキュリティは百貨店に依存。しかしほとんどの百貨店で特にネットワークセキュリティ対策は行っていなかった。

首都圏製造業 T様

次世代ファイヤウォールでサプライチェーン攻撃を防御し低コストでのセキュリティ強化を実現！

1. 次世代ファイアウォールでセキュリティ強化
2. 低価格ライセンスコストと豊富な機能が決め手
3. YAMAHA等の国内メーカールータとのマルチベンダーVPNを低コストで導入

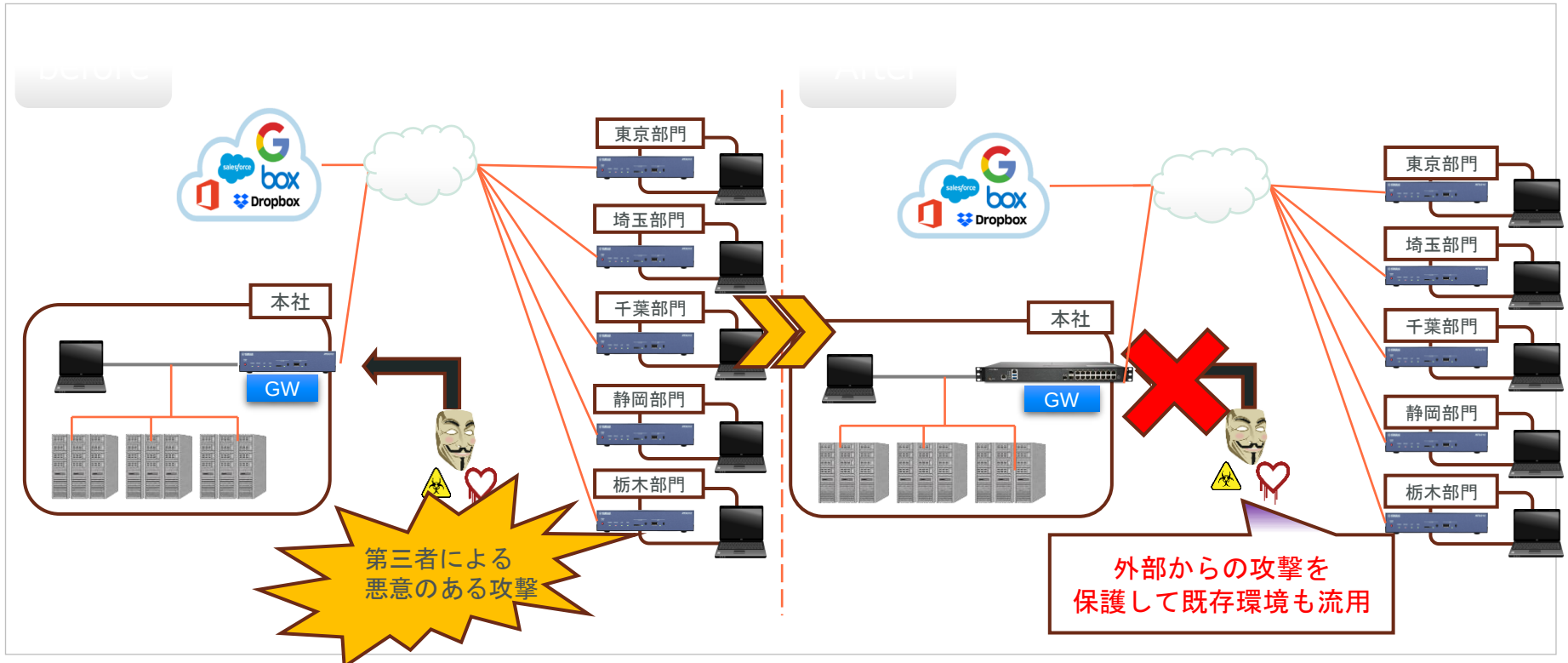
分　野
製造販売業

企業概要
社　　員：250名
既存対策：従来型ファイアウォール

課　題
サプライチェーン攻撃が発生した際に取引先でのフォレンジック調査にて踏み台とした攻撃だったと認識された場合、対応に苦慮することが想定されていたため、セキュリティを強化しつつ、現行の構成も活用できるNW構成を考えていた。

導入モデル
・NSA2700
将来的には複数の次世代ファイヤウォール同士での拠点間VPNを構築し、本社集約されるトラフィックの軽減についても検討。

導入効果
最小限の費用でGWセキュリティを導入し、構築コストも抑えられた



運輸関連業 C様

企業概要

社　　員：1700名
拠　　点：国内5拠点および自宅
既存製品：Fortigate

課　題

・既存のSSL-VPN機器で運用していたID/PWのみの認証にセキュリティリスクを抱えていた。
・会社支給の業務用PC/スマホからのSSL-VPN接続以外に、セキュリティポリシーを無視した自宅PC及びiPhoneからの接続を多数確認していた。

導入モデル

・セキュアモバイルアクセスシリーズ SMA6210
・同時接続500ユーザライセンス
・CaptureATP(クラウド型サンドボックス)

導入効果

SMA6210の標準機能のみで2要素認証を実現。EPCによる接続元デバイスのセキュリティ状況チェック&CaptureATPによりマルウェア感染リスクを大幅に低減。

SMA6210でSSL-VPN接続時の多要素認証を実現 CaptureATPとの統合でトラフィック内の未知の脅威も防御

1　ユーザのなりすまし防止と危険なデバイスのアクセスを制限

ユーザのなりすまし防止の対策
-Eメールによるワンタイムパスワード
-スマホアプリによるワンタイムパスワード

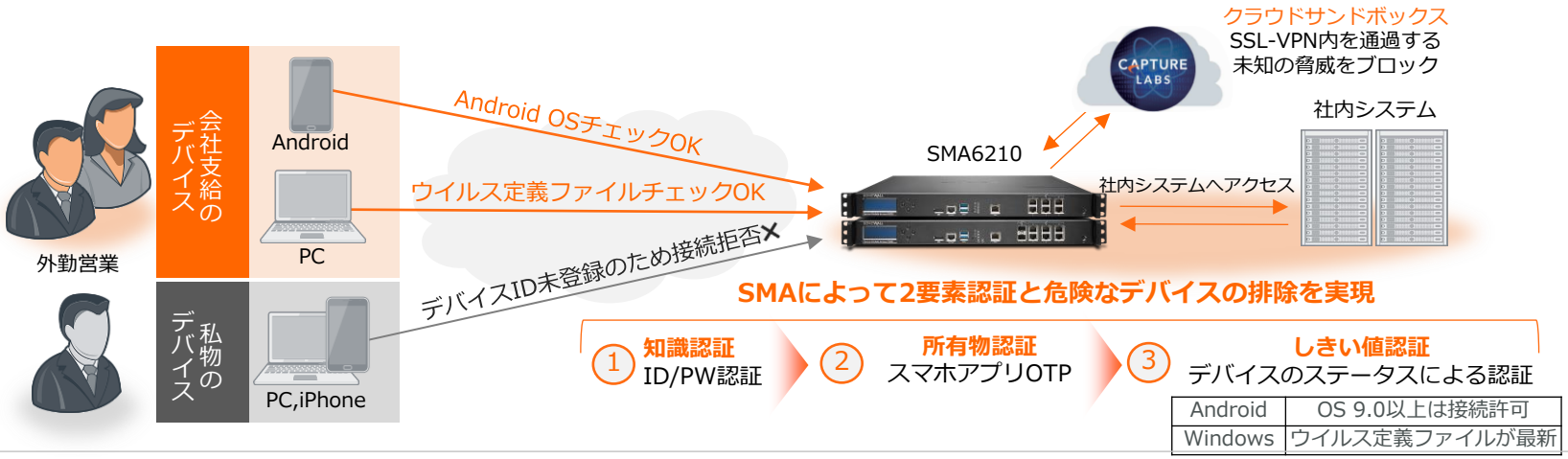
危険なデバイスのアクセス制限機能
-エンドポイントコントロールによってデバイスのステータスをリアルタイムで識別し、動的にアクセスを制限

2　盲目的に信頼されていたSSL-VPNのトラフィックを検疫

SSL-VPNトラフィックはこれまで盲目的に信頼された通信としてみなされていたが、SSL-VPNを通じて脅威の横展開がリスクとして考えられるため、 クラウド型のマルチエンジンサンドボックス(CaptureATP)によってそのリスクを軽減する。

3　Active Directory連携で管理者運用の負担を軽減

SMA6210ではActiveDirectoryの他に、RADIUS、LDAP、SAML2.0といった外部認証基盤との連携が可能。
既存でご利用の認証基盤を利用することで、ユーザアカウントのライフサイクル運用の負担を軽減する。



生保・損保 N様

国内17拠点の分散環境に対し一貫したセキュリティ対策 全機器をSonicWallに統一することでコスト40%削減

分　野
生命保険 損害保険

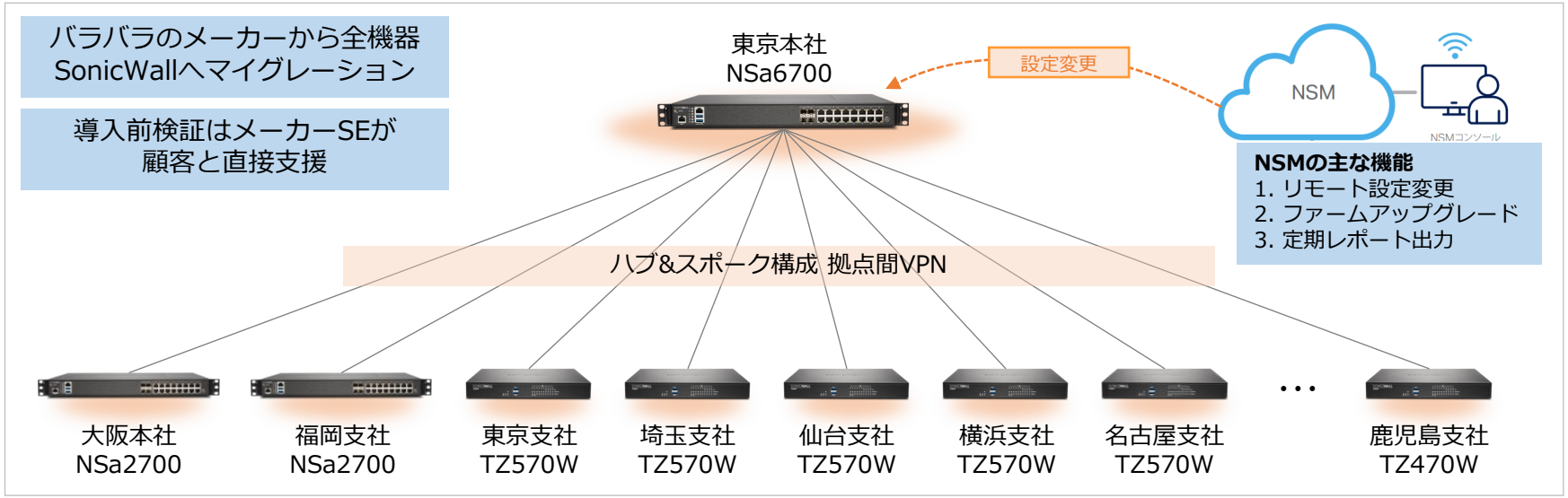
企業概要
社　　員：900名
既存製品：Paloalto, Sophos, YAMAHA

課　題
事業拡大に伴い急速な事業所展開を行っている。情報システム担当は3名のみで、特にメーカーに縛りを設けず各々が各拠点に対しネットワーク機器を導入してきた。
トータルで一貫性のあるセキュリティ対策の必要性とボリュームによるコスト削減を検討していた。

導入モデル
・NSa6700×1
・NSa2700×2
・TZ470W×7
・TZ570W×7
・Network Security Manager(NSM)

導入効果
新たに策定したセキュリティポリシーに沿った機器設定を全てのFWに実施した。
また、全拠点一括導入により40%のコストダウンに成功した。

1. 17拠点全てのFWに対しゴールデンイメージを適用
2. SonicWall FW17台一括購入で40%コスト削減
3. 分散環境でもクラウドで一元的に管理を実現



エンドポイントの追加対策としてCapture Client EDRを導入 ランサムウェア攻撃への対応を強化

青果卸売 N様

分　野
卸売り

企業概要
社　　員：300名
既存製品：Symantec アンチウイルス

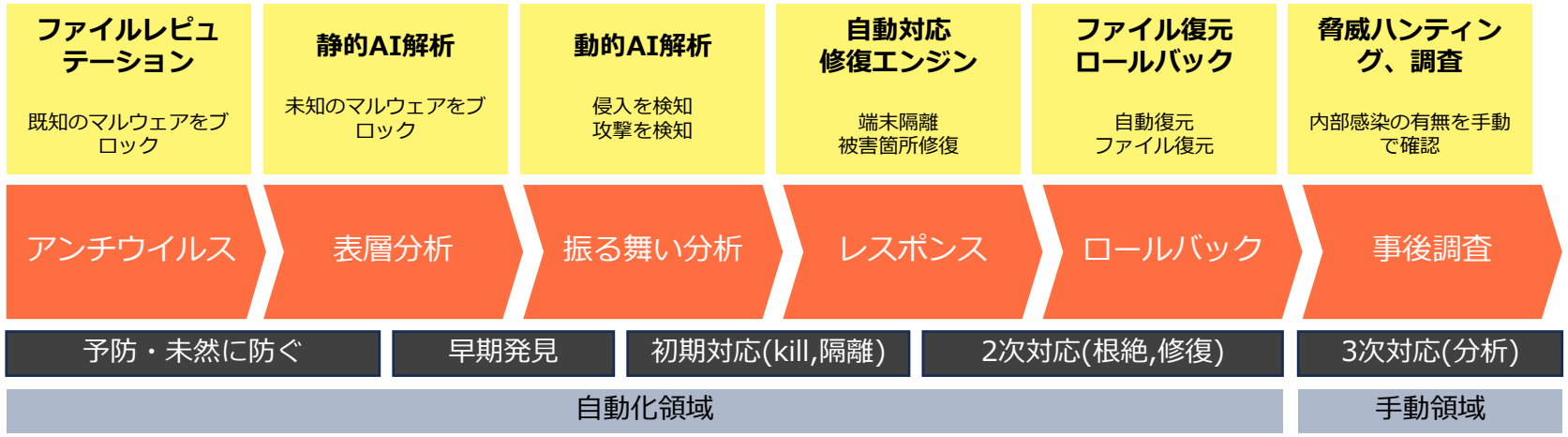
課　題
2022年10月にランサムウェア被害を受け、ランサムウェア対策製品を検討。既存は従来のアンチウイルスソフトを導入。Active Directoryも侵入された形跡もあったため、サーバを含めた被害を前提とした事後対策が求められていた。

導入モデル
・Capture Client 300ライセンス

導入効果
第1段展開にOA端末、第2弾ではサーバに対してCapture Clientのエージェントを適用し、問題なく稼働。運用開始以降、大きなインシデントは発生していないものの、インシデントの兆候がある端末を回収し、再セットアップを行うといった予防対応を取ることができている。

1. OA端末、Active Directoryの全台に対しEDR導入
2. ロールバック機能により暗号化ファイルの即時復号化
3. インシデントの兆候を見極めプロアクティブな対応を実現

Capture Client EDRの概要



大手買取業 E様

高いパフォーマンス誇るSonicWall NSsp10700で従前よりもかなり安定した通信環境を実現！

分　野
買取業

企業概要
社　　員：1000名
既存対策：ルータのみ

課　題
従来から利用していたルータが、Web会議等によるトラフィック増加に耐えることができず、通信品質の低下を招いてしまっていたため、高トラフィックに対応でる製品の導入が必須となり、高機能でありながらコストを抑えて冗長構成できる製品を求めていた。

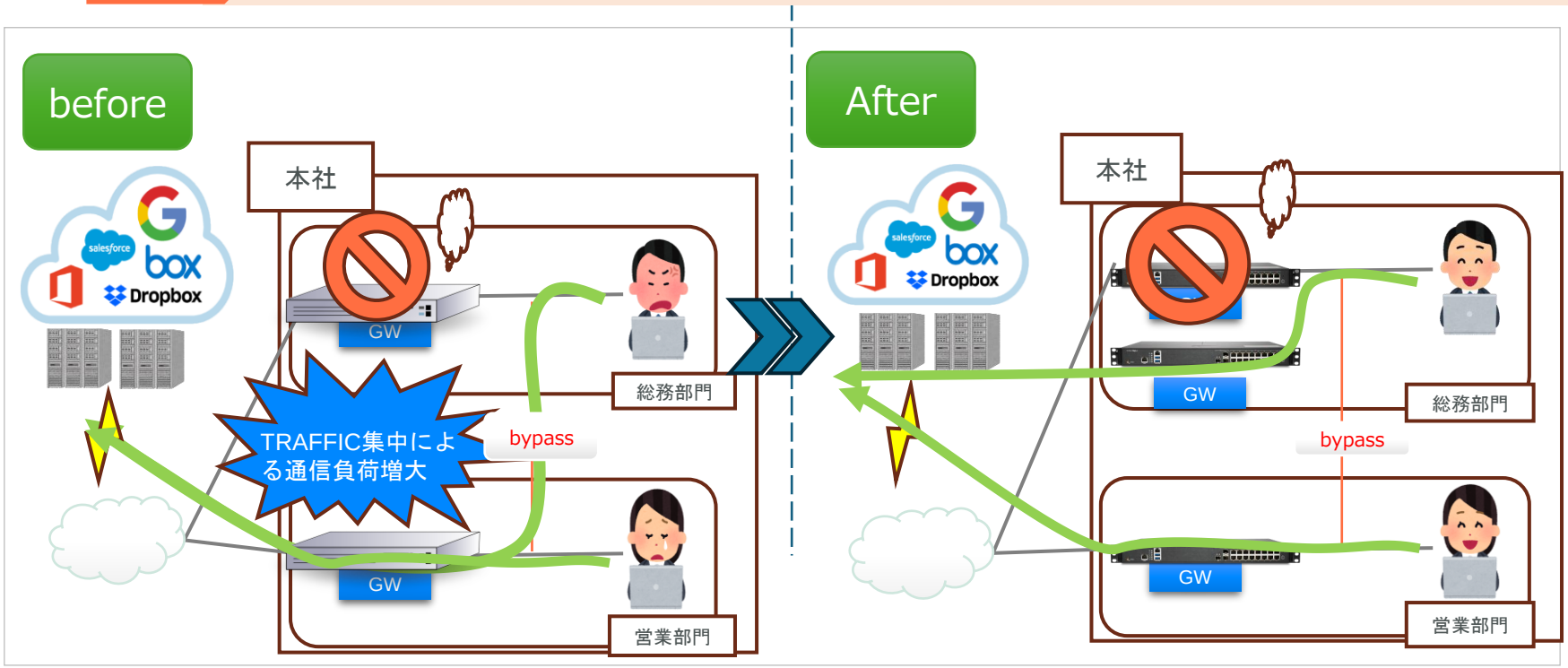
導入モデル
・NSsp10700
・NSM Essential
オプションとしてNSMを選択し、情報システム管理者が遠隔にいながらも機器が管理できる状態を実現（多店舗展開ビジネスのため本社不在のことが多い）

導入効果
各部門から通信をブレイクアウトする方式を実践でき、より安定したネットワーク環境に

1 SD-WAN機能で通信品質の向上

2 導入費用が前回の50%削減することに成功

3 クラウド管理により情報システム管理者の負荷軽減



製造業 B様

企業概要
社　　員：300名
既存製品：SONICWALL/某UTMメーカー

課　題
既存製品がEOLのため、後継機器を選定する必要があった。また、ファイアウォールのみの利用であったため、高度な攻撃に対して防御できているか不安を感じていた。

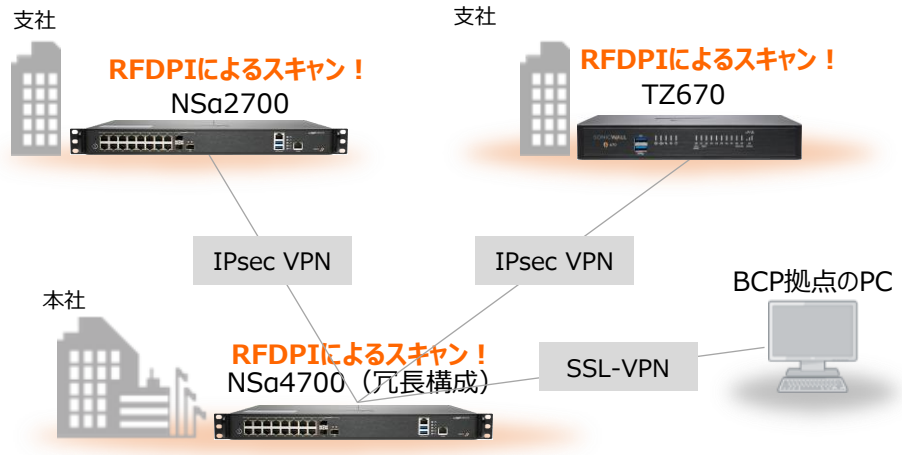
導入モデル
・NSa4700／NSa2700／TZ670
本社は冗長構成。支社は従業員に応じて機器を選定。

導入効果
セキュリティを高めたいと考えていた際、SONICWALL社のキャンペーンを提案され、コストを抑えつつ、セキュリティレベルを上げることに成功。
導入後にこれまで既存の導入機器で検知されていなかった脅威をRFDPIで検知。
週次レポートで経営層に対して稼働状況を報告できている。情シスがカスタマーサポートへ直接連絡できることで、サポートの待ち時間が大幅に短縮。

Bigger&Betterキャンペーンを活用し、EPSSライセンスを導入。無制限のRFDPI©でセキュリティレベルを向上

※Bigger＆Betterキャンペーン：SONICWALL旧製品／他社製品からお得な乗換キャンペーン

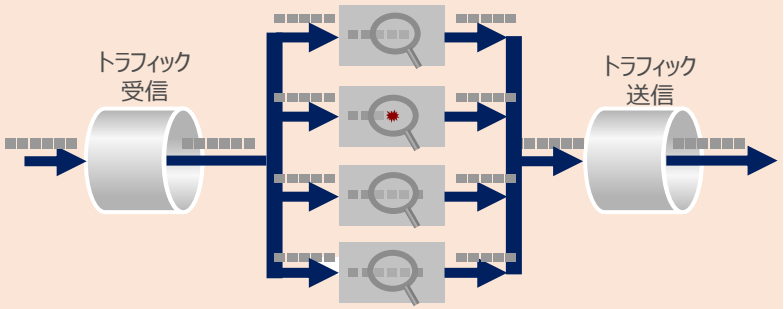
1. キャンペーンを活用しセキュリティライセンスをアップグレード
2. 検査対象のファイルサイズが無制限のTZ/NSaを導入
3. 情シス直サポート対応により対応時間が大幅に短縮



本社・支社に流れるデータもRFDPIで高速スキャン
クラウドサンドボックスで未知の脅威を事前に防御
災害時のBCP対策としてSSL-VPNによるリモート接続

SonicWallが実現するパケット検査方法　RFDPI©

パケットを再構築せずパケットのままスキャン



・パケットを蓄積せずスキャンすることで遅延を抑える
・スキャンするファイルサイズに制限なし

IT

大手SIer J様

インターネット回線10Gbps増速化に合わせて ゲートウェイセキュリティを新たに強化

分　野
IT

企業概要
社　　員：1100名
既存製品：Fortigate

課　題
2020年の新型コロナウイルスによる緊急事態宣言の発出に伴い、テレワークを促進した。しかし、通信料の増大によるパフォーマンスの低下が発生し、Web会議の映像劣化や音声が途切れるといった問題が頻発していた。

導入モデル
・NSa6700 冗長構成
インタネット回線の10Gbpsへの増速、および社内ネットワークでも10Gbpsを実現すべく本モデルを配備。

導入効果
パフォーマンスの改善により、Web会議でのストレスはほぼ感じることはなくなった。今回からセキュリティサービスを全て有効にして稼働しており、これまで発見できていなかった脅威を検知した。

1 Web会議同時アクセス600人でもパフォーマンス問題なし

2 冗長構成時のスタンバイ機は全てのライセンスが無償

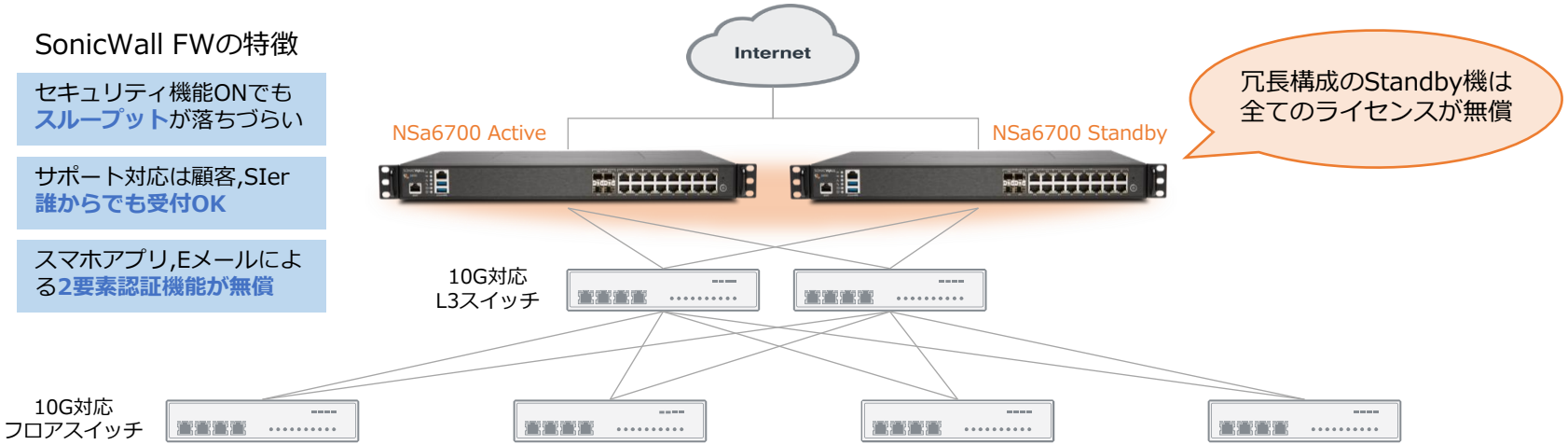
3 リモートアクセスVPN認証時の2要素認証機能も無償提供

SonicWall FWの特徴

セキュリティ機能ONでも **スループット**が落ちづらい

サポート対応は顧客,SIer **誰からでも受付OK**

スマホアプリ,Eメールによる**2要素認証機能が無償**



EC事業者 J様

企業概要

社　　員：500名
拠　　数：国内3拠点

課　題

販売パートナーは本顧客の機器運用も請け負っている。LAN内に配備していたFWは、月に数回のファイアウォール設定変更作業と数か月に一度のファームウェアアップグレード作業を現地に出向き対応していた。作業は深夜帯に行われていたため、販売パートナーは工数の削減を希望しており、顧客としても夜間帯のオンサイト作業費用を削減したいと考えていた。

導入モデル

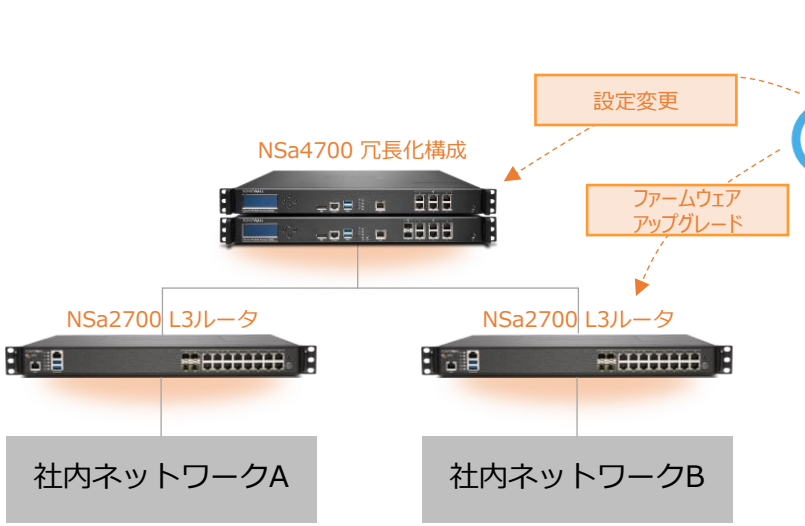
・NSa4700
・NSa2700 ×2台
・Network Security Manager(NSM)

導入効果

設定変更作業およびファームウェアアップグレード作業はほぼ全てNSMを通じてリモートで実施することができるようになった。また、NSMのトラフィックの可視化/分析機能を活用し、定期レポートを出力することで、トラフィックのボトルネックを突き止めることができた。

Network Security Manager(NSM)で複数拠点に対しファームウェアアップグレード作業をリモートで完結！

1. 複数拠点の設定変更作業をリモートでスケジューリング
2. LAN内のファイアウォールでもリモート作業が可能
3. トラフィック可視化/分析機能により通信ボトルネックの解明



NSMの主な機能

1. ファイアウォール操作の一元化
2. ファームウェアアップグレード
3. トラフィックの可視化/分析
4. 定期レポート出力

関西地方通信事業者A様

ネットワークトラフィックの詳細分析による セキュリティ向上と管理効率化！

分　野
通信業

企業概要
社　　員：200名
既存対策：従来型ファイアウォール

課　題
従来から利用してきたファイヤウォールのネットワークトラフィックの監視と分析が不十分であり、脅威の早期発見や迅速な対応が困難でした。リアルタイムでの異常検知ができず、潜在的なセキュリティリスクを見逃す可能性が高かったです。また、手動によるレポート作成や分析は時間と労力を要し、管理業務の効率が低下していました。

導入モデル
・NSa2700
・Analtics
・NSM Onprem

導入効果
従来行っていたレポートの収集のほかに支店間の設定管理や運用を本社担当者が一括して作業を行うことを想定。

1 リアルタイムでの脅威検知と対応

2 包括的なレポート機能による規制遵守

3 管理業務の効率化とコスト削減

某通機系販売店　様

分　野
情報通信機器・OA機器の販売、施工、
メンテナンス・通信事業サービスの取次業務

企業概要
社　　員：約400名
既存対策：通信機器メーカー製簡易UTMのリセール

課　題
価格重視で、専任メーカーではないベンダーが提供する”安かろう悪かろう”のUTMを主に取り扱っていた。
また、機器調達後の構築・設置手配や運用時の問い合わせ等、リセラーにとって手離れが悪い商材であった。

導入モデル
・TZ270W
・Network Security Manager

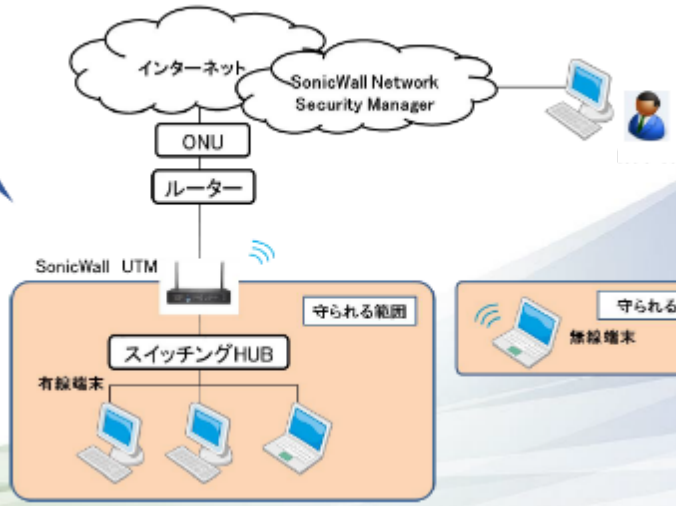
導入効果
数あるUTMメーカーの中の先駆者であり、信頼・実績・コストパフォーマンスに優れたSonicWallを採用する事でセキュリティ対策を強化。また、初期設定や構築に加え、運用(設定変更、FWアップグレード等)をSonicWallパートナーに任せることで、専任の技術者がいない小規模企業でも手軽に導入が可能となった。

高機能・コストパフォーマンスの高い次世代ファイアウォールを専任の技術者がいない小規模企業でも手軽に導入・運用が可能！

1. 次世代ファイアウォールでセキュリティ強化
2. 既存環境の設定・構成を変更せずに導入が可能
3. 初期設定・導入後の運用もすべておまかせ

インラインモード(スイッチングHUBのようなモード)に
事前設定したものをご提供する事により、
既存環境の設定・構成を変更せずに導入が可能です。

各種セキュリティ設定や
無線、FWも設定されているので、
IPアドレス以外は、
変える必要がありません。




SONICWALL®
Never alone.
Relentless security.