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

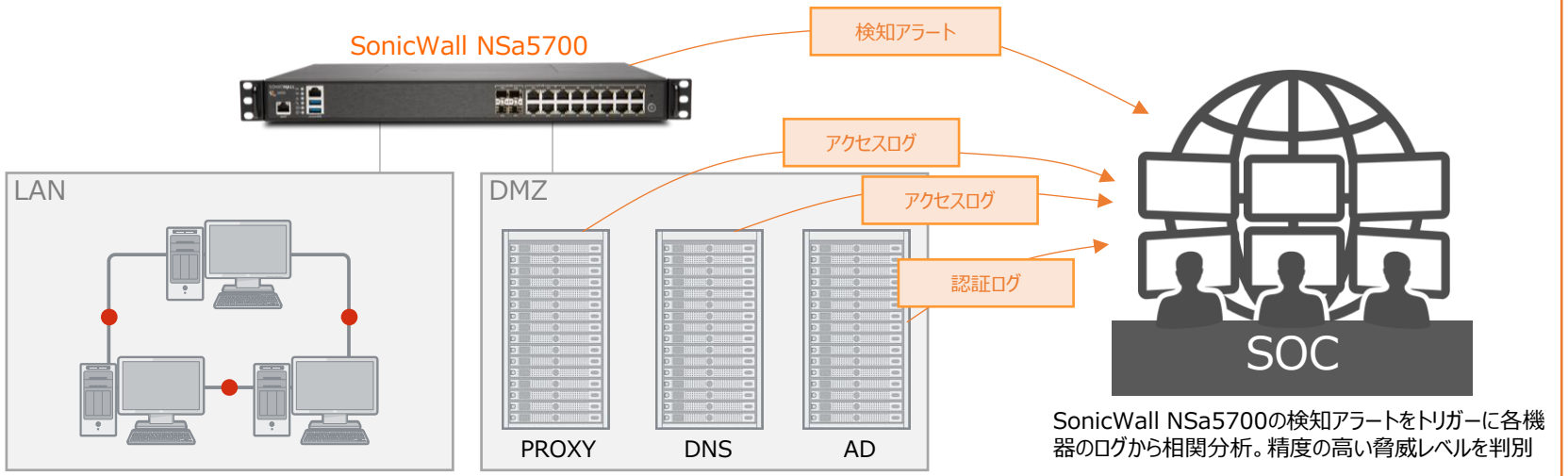
導入背景
・海外でマルウェア感染したPCが社内で感染拡大。情報システム部門が事態収束までおよそ3か月間対応。
・検知の仕組み、検知後の体制強化が急務

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