2 ②自治体向けビジネス ◆セキュリティソリューション

セキュリティ専門家不在の自治体・企業を中心にセキュリティトータルソリューションを提供

高度な専門技術を核にした“セキュリティトータルソリューション”に注力するNTTアドバンステクノロジ（以下、NTT-AT）。専門家不在の自治体・企業を中心にしたコンサルからインシデント対応支援までのネットワークセキュリティサービス＆ソリューションの取組み状況を紹介する。

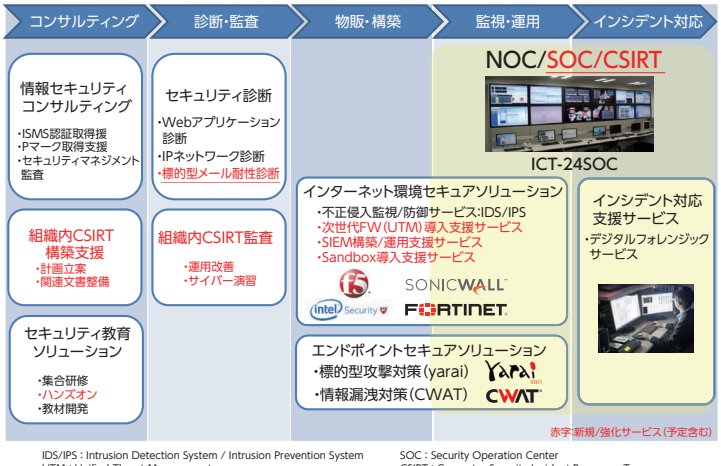
「NWセキュリティサービス＆ソリューション」をワンストップ提供

情報セキュリティコンサルティングからセキュリティ診断、関連製品の販売・構築、NOC（ネットワークオペレーションセンタ）／SOC（セキュリティオペレーションセンタ）を活用した監視・運用、インシデント対応支援までのセキュリティトータルソリューション「ネットワーク(NW) セキュリティサービス＆ソリューション」に注力するNTT-AT。

セキュリティ営業SE部門の福井将樹部門長は、「標的型攻撃等によりセキュリティの脅威が高まるなか、情報セキュリティ市場において、急速に運用サポートのアウトソースニーズが高まっています。特にこの傾向は、自社対応できる人材の確保や育成が困難な地方自治体や中堅・中小企業において顕著で、今後この領域の市場規模拡大が見込まれます。情報セキュリティは、関連製品を導入しただけでは対策になりません。運用が極めて重要です。弊社では、主に専門家不在の自治体や企業を中心に、図1に示す“NWセキュリティ＆ソリューション”をワンストップで提供しています」と強調する。

NTT-ATは、NTTグループ企業や官公庁等のセキュリティ運用の豊富な受託実績に加え、ICT24オペレーションセンタのSOCを活用した専門エンジニア集団による“セキュリティオペレーションサービス”の提供も開始している。最近の代表的な受注例として福井部門長は、「“自治体セキュリティクラウド”の補助金対象の設備運用に関して、NTT東日本様・西日本様と連携して提案活動を展開し、すでに例えば京都府様や秋田県様など複数の大規模自治体へのサービス提供が決定しています」と述べている。

NTTアドバンステクノロジ株式会社
トータルソリューション事業本部
セキュリティ営業SE部門
部門長　**福井 将樹**氏



IDS/IPS：Intrusion Detection System / Intrusion Prevention System
UTM：Unified Threat Management
FW：Firewall
SOC：Security Operation Center
CSIRT：Computer Security Incident Response Team
SIEM：Security Information and Event Management

図1　NTT-ATの「NWセキュリティサービス＆ソリューション」

目利き力、提案・構築力、運用力が大きな強み

「NWセキュリティサービス＆ソリューション」の基本コンセプトは、①インシデントの検知だけでなく、顧客ニーズに合わせたその後の対応支援（インシデントレスポンス、フォレンジックサ

ービス）を含めたトータルサービスの提供、② SOC/CSIRT（コンピュータセキュリティインシデントレスポンスチーム）によるセキュリティ運用だけでなく、NOC によるネットワーク運用監視、SI/NI を含めたワンストップ対応の 2 点だ。また NTT-AT ならではの大きな特長であり強みとして、以下の 4 点があげられる。

・セキュリティ監視装置、ログ分析エンジン (SIEM) などを活用した情報分析、システム管理、技術開発の豊富なノウハウ。特に SOC/CSIRT を支える専門部門＝セキュリティラボを有し、最新動向の解析と蓄積を日々実施している。
・NTT-CERT（コンピュータエマージェンシーレスポンスチーム）の支援業務等を通して蓄積したインシデントレスポンスやデジタルフォレンジックスのノウハウ。
・セキュリティ製品販売代理店として培った製品に関する専門技術、ノウハウ。例えば、UTM(統合脅威管理) 製品の“SonicWALL”や“FortiGate”、WAF(Web アプリケーションファイアウォール) 製品の“BIG-IP”等々の豊富な販売実績を有している。
・セキュリティ関連システム（試用、商用）開発を通して培った技術、ノウハウ。

“抜き打ち訓練”による標的型メール耐性診断サービスも提供

NTT-AT の NW セキュリティサービス＆ソリューションのなかで、最近特に引き合いが多くなっているサービスが、「標的型メール耐性診断サービス」だ。本サービスは、巧妙に偽装した標的型メールに騙されないために、社員への“抜き打ち訓練”を行い、企業の情報セキュリティインシデント耐性を強化するものだ。標的型メールは、巧妙な偽装が進化し続けているため、対策の講習やマニュアルだけでは防げないのが実状である。

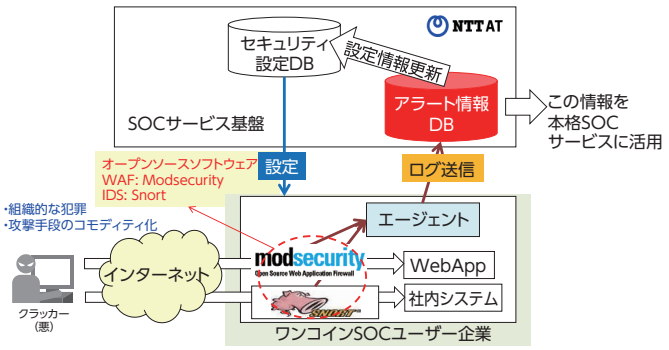


図 2「ワンコイン SOC サービス（仮）」の提供イメージ

この点を踏まえ NTT-AT では、情報セキュリティ分野において数多くのインシデント事例を扱ってきた経験をベースに、実際の攻撃事例に基づくリアリティの高い標的型メールを再現し、“本物と見紛う”疑似標的型メールを送信し、インシデント耐性を診断するサービスの提供を開始した。提供価格は、本サービスを契機に具体的な対策支援等を視野に入れた戦略的なサービスであることから、診断対象のメールアドレス数が 100 までで、メール文面数 1 種の場合で 20 万円、同 2 種の場合で 30 万円と安価に設定されている。

近々、2 つの新サービスをリリース

NTT-AT では近々、SOC サービス基盤を活用した 2 つの革新的なサービスを提供する予定だ。1 つは、Fortinet 社とのタイアップによる「FortiSandbox サポートサービス」で、標的型攻撃対策手段として評価の高い「FortiSandbox」の運用を支援するサービスだ。同製品は、独自の二重構造のサンドボックスでプロアクティブな脅威検知と緩和対策の提供に加え、脅威の本質を把握することで実効性の高い対策を可能にするソリューションとして高く評価されている。NTT-AT では、Fortinet 社のセキュリティ研究部門「FortiGuard Labs」との連携により、脅威の最新動向を盛り込んだ、初の日本語版レポートも提供する。

もう一つは、NTT グループの地域事業会社との連携を基軸にした新サービスで、専門家不在で予算も限られている基礎自治体やセキュリティ対策に費用がかけられない中小企業、個人事業主向けのクラウド型セキュリティ運用サービス「ワンコイン SOC サービス（仮）」だ（図 2）。福井部門長は、「年内には試験サービスを開始する予定です。本サービスで得られたセキュリティログ情報を元に、中堅企業以上を対象にした、SOC サービスも展開していきたいと考えています」と抱負を述べている。