NTTコミュニケーションズ／トレンドマイクロ

トレンドマイクロと連携したNTTコミュニケーションズのSOC（Security Operation Center）－スピアー攻撃など脅威の傾向変化にも対応

セキュリティはアウトソーシングの方向へ－注目を集めるSOC－

コンプライアンス（法令遵守）やセキュリティに対する社会的要請が高まる中、安心・安全なICT環境の実現が不可欠となっている。そのような中、ファイアウォール・不正侵入検知/防御装置（IDS/IPS）の監視やウイルス監視を行い、ログを収集して脅威を分析し、いち早く適切な対策を促すSOC（Security Operation Center）の重要性が急速に高まっている。しかし、SOCの重要性が増大する一方で、常時監視、膨大なログ情報の収集・分析を行い、多様化するセキュリティ上の脅威に対して迅速な対応を促すSOCのような専門組織を自社で抱えることはなかなか難しい。特に、高度なバックドアツールを使用した不正侵入やゼロデイアタック、BOTやスパムの蔓延、さらには特定の企業や組織を狙ったスピアー攻撃（標的型攻撃）などに迅速・的確に対応するためには、外部の専門企業にアウトソーシングするのが最適解といえる。

ネットワークセキュリティを網羅的に管理するサービスを展開

脅威の多様化・巧妙化に対応したセキュリティ運用の強化という企業が抱える課題を解決するサービスとして注目を集めているのがNTTコミュニケーションズのSOCを核にしたセキュリティ運用アウトソーシングサービスだ。

NTTコミュニケーションズのSOCは2003年8月、ネットワークセキュリティの脅威に対応する専門技術組織として設立された。「現在、OCN、Verio等のIPネットワーク管理技術、大手企業のITシステム障害対応力、セキュリティ専門研究機関（NTT-CERT、トレンドマイクロのトレンドラボ、ISS X-Force）との連携を強みに、世界トップレベルの情報コントロール体制のもと、侵入防止から、リスク監視や検疫などのイントラネットセキュリティ、ウイルスやマルウェアの感染防止と駆除等のエンドポイントセキュリティまで、ネットワークセキュリティを網羅的に管理するマネージドサービスを提供しています。」（NTTコミュニケーションズ㈱ITマネジメントサービス事業部　セキュリティオペレーション部門　竹内 文孝担当課長）

NTTコミュニケーションズならではの情報コントロール体制（図1）、特にトレンドラボやX-Forceと個別にホットラインを設け、中立的な立場で情報をコントロールし、常に最新のセキュリティリスクとその対策情報を得ることができるというのは、NTTコ

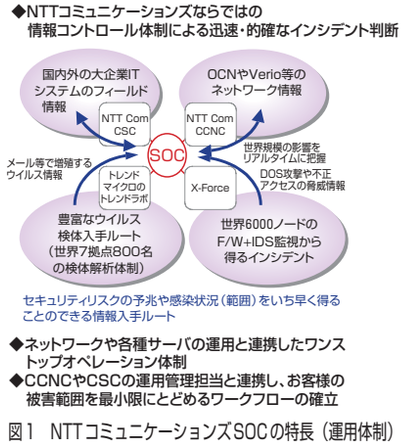

図1　NTTコミュニケーションズSOCの特長（運用体制）

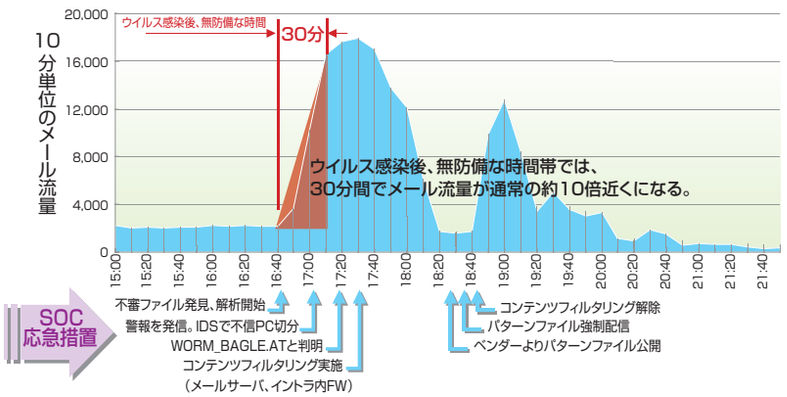

図2　NTTコミュニケーションズSOCの運用事例

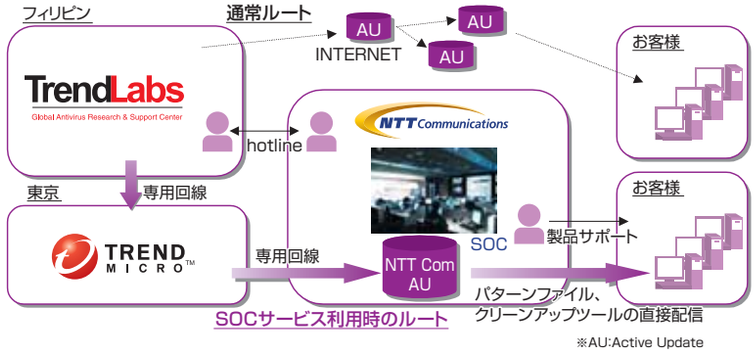

図３　トレンドマイクロと連携した世界最速級※のパターン配信

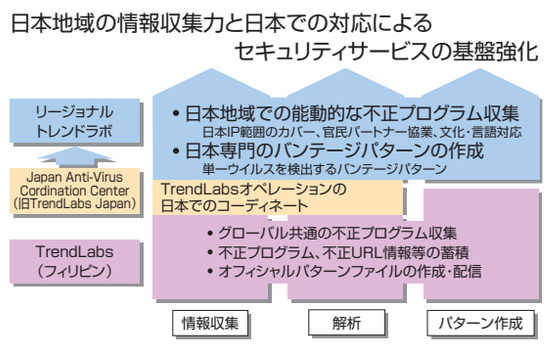

図４　「リージョナルトレンドラボ（RTL）」設立の目的

ミュニケーションズのSOCの他社にはない大きな強みといえる。

トレンドマイクロとの連携で世界最速級※のパターン配信を実現

セキュリティ対策は時間との戦いだ。対応が遅れると大きな被害を招く。図２にNTTコミュニケーションズSOCの運用事例を示すが、これは総合的なウイルス対策により、メールシステムダウンを阻止した事例である。ウイルス感染とメール流用が指数関数的に増大し、約30分間で通常メール流量の10倍近くになったが、NTTコミュニケーションズのSOCの応急措置により、システムダウンに至ることなく通常のメール流量に改善された例である。セキュリティ対策における30分という時間の重要さが、この実測データから見てとれる。早期に警報配信・不審PC切分け、コンテンツフィルタリング等の応急措置を実施してセキュリティリスクの影響範囲を最小化した後、パターンファイル適用などの恒久措置を施すことがきわめて重要といえる。

NTTコミュニケーションズのSOCは、トレンドマイクロとの連携により、パターンファイル、クリーンアップツールをNTTコミュニケーションズのAU（Active Update）から顧客に直接配信するという世界最速級※のパターン配信サービスを実現している。

※トレンドマイクロのシステムを採用しているサービスプロバイダ各社の中で最速

脅威の傾向変化への対応を目指しトレンドマイクロはRTLを設立

セキュリティ脅威の最近の特徴として、スピアー攻撃が増加していることがあげられる。検体情報（不正プログラム）を入手しやすい不特定多数への攻撃と異なり、スピアー攻撃は実態を把握し難いという課題がある。このようなスピアー型など対象が限定された攻撃や、頻発する亜種への対応を目指し、トレンドマイクロは、各地域に特化した専門のウイルス解析＆サポートセンター「リージョナルトレンドラボ(RTL)」を設立している。

日本地域でも、本年５月にRTLを設立し、日本地域での能動的な不正プログラムの収集、日本専門のバンデージパターン（単一の不正プログラムに対応する一時的なパターンファイル）を作成している（図４）。具体的には、①マルウェアの傾向把握、②マルウェアサンプルの収集、③攻撃状況の監視、④マルウェアの解析、⑤バンデージパターンファイルの作成、⑥顧客への配布を行う。

このようにトレンドマイクロでは、世界中の脅威情報の収集、ソリューションを提供するトレンドラボ（フィリピン）と日本地域に特化したRTLの双方を運用し、セキュリティサービスの基盤強化を図っている。

「NTTコミュニケーションズのSOCに専任のTAM（Technical Account Manager）チームによる支援など、緊密な関係を実現しています。RTLの設立を契機に、NTTコミュニケーションズとの協力関係を一段と強化し、日本固有の脅威への対応を図っていきたいと考えています。」（トレンドマイクロ㈱　NTT法人営業課　廣石 雅義課長代理）

お問い合わせ先

NTTコミュニケーションズ㈱
ITマネジメントサービス事業部
SOC担当
TEL：03-6800-8340

トレンドマイクロ㈱
法人向け営業代表
TEL：03-5334-3601