2 セキュリティ

コンサルからオペレーションまで、セキュリティのトータルサービスプロバイダーを目指す

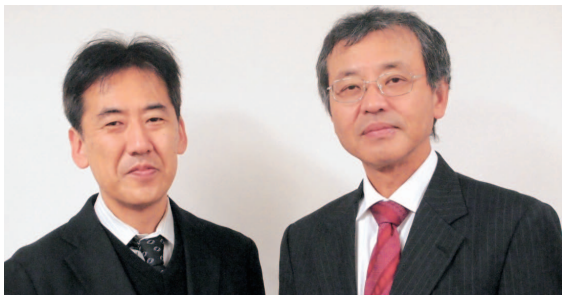
新中期経営戦略構想の4本柱の重点事業領域の1つである“セキュリティ”の展開に注力するNTTアドバンステクノロジ（以下、NTT-AT）。本稿では、自社データセンタによるセキュリティオペレーションの強化と、NTT研究所のR&D支援などで培った高度なセキュリティ技術やセキュアネットワーク構築技術などを核にしたセキュリティサービスの取組みを紹介する。

サイバー攻撃対策のベストプラクティスを提供するNTT-AT

増加する一方のサイバー攻撃。攻撃の手法・手口も極めて高度化かつ複雑化している。特に、昨年6月発覚した日本年金機構の大規模な情報漏えいがきっかけとなり、改めてネットワークの「入口対策」、「出口対策」、「内部対策」からなるセキュリティ対策の重要性が注目を集めた。

誰もがサイバー攻撃の標的となり得る現在、セキュリティ対策の定期的な見直しは不可欠だ。また、高度な専門技術を持つセキュリティ人材の雇用が困難な自治体や中堅・中小企業にとっては、セキュリティノウハウや人的リソースを補完するという観点で、セキュリティ専門企業が提供するセキュリティサービスの活用も選択肢の1つだ。必要なセキュリティ対策として、ファイアウォール（FW）やセキュリティ監視システム（IPS/IDS）、未知のマルウェア検知など、多種多様なセキュリティ対策を検討・導入する企業・団体が増えている。しかし、それらのセキュリティ機器を適切に運用し、高度なサイバー攻撃に対処できるセキュリティエンジニアを抱えられる企業・団体はごくわずかだ。

NTT-ATネットワークソリューション事業本部セキュリティソリューションビジネスユニットの福井将樹BU長は、「NTT-ATは、セキュリティ診断やコンサルティングなどのサービスを17年前（1999年）から提供しており、高度な専門技術を保有しています。また、24時間365日の“ICT-24オペレーションセンタ”を8年前（2008年）に開設し、NOC（ネットワークオペレーションセンタ）及びサーバハウジングセンタとしてネットワークの遠隔監視やサーバ&クラウドオペレーション業務を提供中であり、NTTグループ企業や官公庁などのセキュリティ運用の受託実績も多数あります。さらに、セキュリティ製品販売代理店として蓄積した製品専門技術、ノウハウも有しています。NTT-ATではサイバー攻撃対策のベストプラクティスとして、こういった高度なセキュリティ技術を備えた専門エンジニア集団が、お客様のシステムがセキュリティの脅威にさらされていないか常に



NTTアドバンステクノロジ㈱
ネットワークソリューション事業本部
［左］セキュリティソリューションビジネスユニット
ビジネスユニット（BU）長　**福井 将樹**氏
［右］ICT-24オペレーションセンタ
センタ長　**大村 弘之**氏

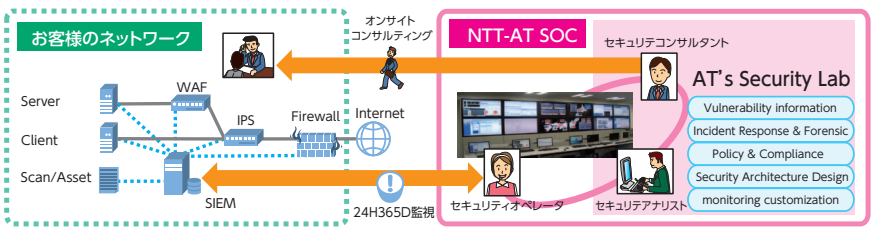


図1　セキュリティオペレーションサービスの提供イメージ

遠隔から監視・分析してお知らせする“セキュリティオペレーションサービス”を2016年度第1四半期には提供開始する予定です」と語る。

本サービスは、「ICT-24オペレーションセンタ」を、NOCやサーバ&クラウドオペレーション機能に加え、SOC（セキュリティオペレーションセンタ）として進化させた「NTT-AT SOC」を基盤にサービス提供するものだ（図1）。サービスの詳細は現在検討中だが、監視方針の策定コンサルティングから各種セキュリティデバイス／ログ分析製品の構築・設定、イベント収集・分析と分析結果に基づく相関分析ルール作成・提供、運用支援、インシデント対応までのトータルサービスを提供する。

福井BU長は、「主要ターゲットは、県・市町村などの自治体や、導入済みの様々なセキュリティ対策製品が出すログやアラートが大量で適切な確認などの対応がとれずに困っている中堅企業、セキュリティ専任技術者が不在のためセキュリティ製品の個別運用にお困りの中堅・中小企業を想定しています。すでに自治体に対しては、NTT東日本様、NTT西日本様の法人部隊とともに、提案対応中です」と述べている。

なお、NTT-ATでは後述するように、NTT-AT SOCを活用した「セキュリティオペレーションサービス」の提供に先駆け、情報セキュリティ事故発生時における対応と事故原因の究明を手厚く支援するサービスとして、「サイバーセキュリティインシデント対応支援サービス」と「デジタルフォレンジックサービス」の2つのサービスを2015年12月に提供開始している。

1.5次保守を強みとする「ICT-24オペレーションセンタ」のSOC化

NTT-AT SOCのベースとなったのは2008年に運用開始した「ICT-24オペレーションセンタ」だ。BCP(事業継続計画）実現に優れたMM21（みなとみらい21）地区に開設された同センタでは、システムやネットワークの24時間リモート監視運用サービスに加え、24時間テクニカルヘルプデスクサービス、さらにはネットワークシステムの構築から大規模な通信処理サービス、アプリケーションの開発までワンストップでのトータルサポートサービスを実現。まさに木村丈治社長の持論である「お客様との関係強化を図るための“手離れの悪い仕事”」を基軸としたトータルソリューションの基盤サービスとして、従来のデータセンタとは異なるユーザビリティとシステムのノンストップ運用を実現し、高品質・高信頼な管理・運用業務を提供している。

NTT-ATが提供するトータルソリューションの基盤として耐震性に優れた堅牢な建物、情報共有に有効なディスプレイウォールなどの充実したオペレーション設備と全ラックに温度センサと電流センサを設置したハウジング設備に加え、電源設備は無瞬断切替（商用電力＋UPS＋非常用発電設備）と最大電源利用時24時間分の燃料（2000L）を別倉庫に備蓄している。またバックヤードのスタッフルームやミーティングルーム以外の高セキュリティエリアは、ISMS（ISO27001）に基づいた入退室時ICカード･生体認証（認証装置＋監視カメラ）、入退室記録取得による厳重管理と、ビル入退室用ICカードとRFIDタグ付き鍵によるRFID鍵管理システムにより、鍵の貸し出し・返却を厳正に管理して重要情報の流出を未然に防止する対策を講じている。

ICT-24オペレーションセンタの大村弘之センタ長は、「私どもが提供する保守運用サービスの最大の特長であり強みは、通常のオペレーション担当とは別に高いスキルと豊富な経験を持つスペシャリストが24時間常駐し、イレギュラーな事象にも適切に対応するテクニカルヘルプデスクサービスの提供です。これにより1.5次保守運用を実現しています。1次保守運用は運用業務のグローバルスタンダードであるITIL（IT Infrastructure Library）をベースにしたオペレーションマニュアルに基づいて実施していますが、1.5次保守運用の実現によって、障害発生時におけるベンダーへのエスカレーション率を下げ、コスト削減やお客様へのサービス向上が図れます。この1.5次保守運用が評価され、自社開発のネットワークシステムやサーバシステム以外にも、NTT事業会社様が開発した全国規模のネットワークサービスや情報ポータルサイトシステムなどをはじめ多数の自治体・

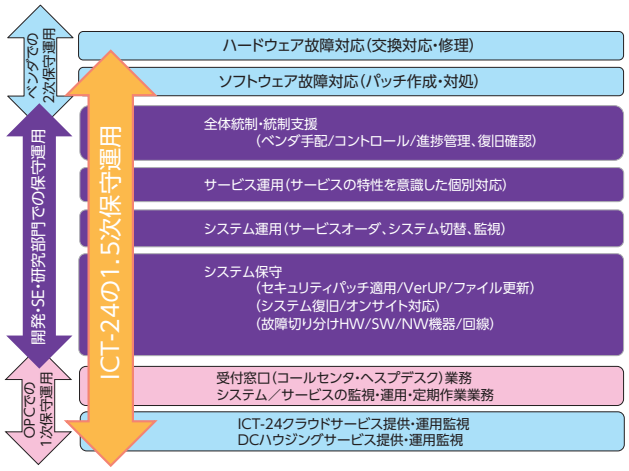


図2　「ICT-24」の1.5次保守運用メニュー体系図

一般企業様の保守運用業務を受託しています」と語る。

図2に1.5次保守運用メニューの体系を示すが、本サービスは主にプラットフォーム（物理サーバ、ネットワーク機器、OS、DB　等）に対して提供する。

NTT-ATでは、この「ICT-24オペレーションセンタ」にセキュリティオペレータを24時間365日常駐させるとともに、新たに社内のセキュリティコンサルタントやセキュリティアナリストなどの高度なセキュリティエンジニアを集約させたセキュリティラボ「AT's Security Lab」を整備する。「NTT-AT SOC」として進化させた「ICT-24オペレーションセンタ」と、「AT's Security Lab」を連携させて、ここを基盤にした新たなセキュリティトータルソリューションを提供するというのがNTT-ATのセキュリティ事業戦略だ。

NTT-ATでは、NTT研究所の最先端セキュリティ技術のR&D活動の支援や、国内外の最先端のセキュリティ製品の展開で培った高度なセキュリティ技術と、セキュアなネットワーク構築の豊富な実績・ノウハウをベースに、1999年からセキュリティ診断サービスや情報セキュリティのコンサルティングサービスを提供してきた。これらの技術やノウハウを生かして、2016年度第1四半期に提供開始するのがサイバー攻撃の脅威を24時間365日遠隔から監視・分析する「セキュリティオペレーションサービス」であり、すでに2015年12月に先行的に提供開始したのが以下で紹介する2つの支援サービスだ。

サイバーセキュリティインシデント対応支援サービス

本サービスは、サイバー攻撃によるインシデントが発生した際に必要となる、初動対応から、影響分析、原因分析、社内外への報告書作成支援など一連の対応をサポートするサービスだ。

サイバーセキュリティインシデントは、発生そのものを抑止することに加え、被害を拡大させないための原因究明と対応を迅速に行えるかどうかが、その後の企業の命運を分けるといっても過言ではない。NTT-ATでは、事故発生直後の初動対応から事態収束、さらに改善・再発防止まで、NTT-AT SOCのセキュリティ対策専門スタッフで構成されるセキュリティインシデント専門チームを中心に、初動対応から事態収束後の対応まで、あらゆる段階で万全にサポートする。本サービスの主な特長を以下に示す。

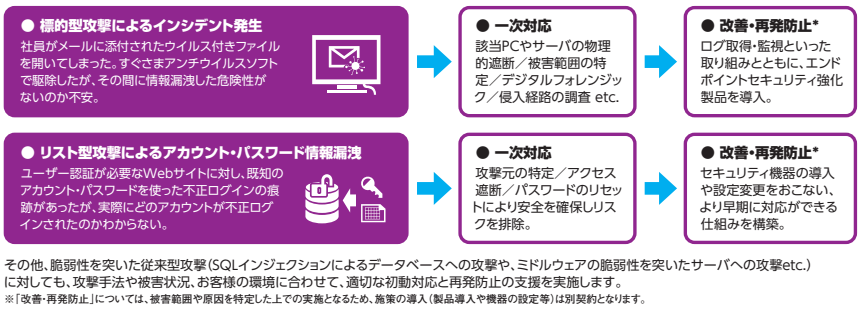
①初動～事後対応まで手厚く支援

事故発生直後の初動対応から事態収束、さらに改善・再発防止まで、あらゆる段階で支援する。

②社内外の対応支援と報告書作成

お客様やステークホルダーの信頼回復には、セキュリティインシデント発生の原因や対応策を明確にすることが重要である。NTT-ATでは調査結果をわかりやすい報告書にまとめ、社内幹部への説明や、社外へのプレスリリース資料作成も支援する。

③経験豊富な専門技術者による迅速



その他、脆弱性を突いた従来型攻撃（SQLインジェクションによるデータベースへの攻撃や、ミドルウェアの脆弱性を突いたサーバへの攻撃etc.）に対しても、攻撃手法や被害状況、お客様の環境に合わせて、適切な初動対応と再発防止の支援を実施します。
※「改善・再発防止」については、被害範囲や原因を特定した上での実施となるため、施策の導入（製品導入や機器の設定等）は別契約となります。

図3　主なインシデント発生事例と対応及び再発防止策の例

写真1　「AT's Security Lab」での
解析作業風景

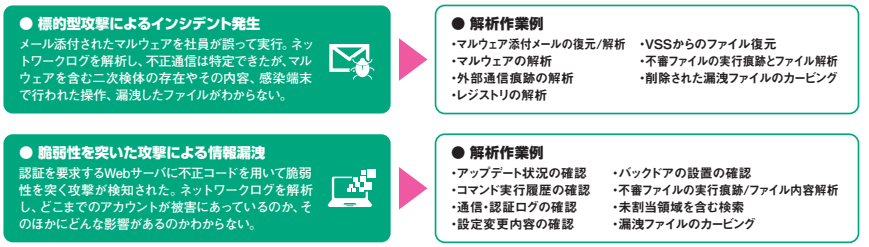


図4　主なインシデント発生事例とデジタルフォレンジック解析作業の一例

な解析

サイバーセキュリティインシデント発生時の証拠保全や原因の究明、被害範囲の特定といった高度な情報解析作業を、長年 NTT グループでセキュリティ対策を担ってきた専門スタッフが、迅速かつ正確に行う。

主なインシデント発生事例と対応及び再発防止策の例を図3に示した。

最新のデジタル鑑識技術を活用したデジタルフォレンジックサービス

本サービスは、インシデント発生後の分析作業において、残されたデータから原因の特定や流出情報の調査などの解析を行う高度なエンジニアリングサービスであり、極めて高度なスキルのセキュリティエンジニアリング集団を擁する NTT-AT だからこそ実現できたサービスだ。

“デジタルフォレンジック”とは、不正アクセスや機密情報漏えいなどのサイバーセキュリティインシデントにおける原因究明手段として、PC やサーバなどの記録媒体やネットワーク機器のログファイルなどを分析し、その証拠を見つけ出す技術的作業の一般的な総称で、本来は警察捜査の「法医学」や「科学捜査」、「鑑識」といった意味である“Forensics”から引用され、使われるようになった用語である。NTT-AT の「デジタルフォレンジックサービス」は、不正アクセスに使われた遠隔操作マルウェアの発見・解析・除去や、脆弱性を狙った情報流出に関するネットワークのログ情報解析などで、その原因 や流出した情報の詳細を特定するデジタル鑑識技術だ。経験豊富な専門技術者が高度な解析機器を駆使し、“隠された真実”を明らかにする。本サービスの主な特長を以下に示す。

①NTTグループで培った豊富な経験と実績

NTT グループ内においてセキュリティ関連業務に携わってきた経験豊富、かつ高度な知識を持った専門技術者が、お客様の課題に応える。

②専用機器による高度な解析

専用機器（デュプリケータやフォレンジックソフトウェア）を用いた、正確な保全と入念な解析を行い、記録媒体やログに隠された真実を明らかにする。

③高い機密性を備えた解析専用ラボ「AT's Security Lab」を完備

極めて機密レベルが高い情報を取扱うため、解析専用ラボへの入室は生体認証により認可された解析担当者のみに制限している。

主なインシデント発生事例とデジタルフォレンジック解析作業の一例を図4に示した。

以上、NTT-AT における ICT-24 オペレーションセンタの SOC 化と、そこを基盤にしたトータルセキュリソリューションの提供に向けた取り組みを紹介した。

大村センタ長は、「NTT-AT　SOC を基盤に、中堅・中小のお客様のセキュリティ向上や、海外現地法人を含めた NTT グループ会社を対象にしたセキュリティ施策の展開に貢献したいと思っています」と今後の抱負を述べている。また福井 BU 長は、「NTT-AT SOC と AT's Security Lab を活用したトータルセキュリティソリューションのラインナップ化とサービス展開に注力し、セキュリティのトータルサービスプロバイダーを目指します」とセキュリティビジネスのビジョンを語った。