

3 セキュリティビジネス

「CSIRT as a Service」の展開に注力

— 会員制コミュニティサービス「CS@T倶楽部」も提供 —

NTT アドバンステクノロジー(以下、NTT-AT)の中期事業計画の5本柱の1つとして、事前対策(特定・防御)から事後対策(検知・対応・復旧)までの包括的なセキュリティ事業を推進するセキュリティ事業本部。「CSIRT as a Service」をコンセプトに、幅広いセキュリティソリューションの提供に加え、CSIRT 運営を支援するコミュニティ型サービスも提供している。

コンサル・教育～インシデント 対応まで、トータルなセキュリ ティサービスを展開

世界でも稀な約80名という多数のCISSP有資格者を擁するNTT-ATのセキュリティ事業本部では、情報セキュリティに関する高度なスキル・ノウハウをベースに、事前対策(特定・防御)から事後対策(検知・対応・復旧)まで、包括的なセキュリティ事業を推進している。

福井氏は、「私どもは、“CSIRT as a Service”を重点テーマにNTT研究所の先端技術や国内外のパートナー企業のセキュリティ商材・技術協力をベースに、セキュリティインシデントの特定・防御、検知・対応・復旧までの対策をトータルに支援するセキュリティサービスを展開しています。これによりNTTグループの事業を支えお客様のセキュリティ強化を包括的に支援したいと思っています」と述べている。

CSIRT(Computer Security Incident Response Team)は、セキュリティインシデントに対する事前対策に加え、発生した際には迅速に対応し、被害を極小化することなどを目的としたチームだ。特にインシデント発生時、組織がより迅速に適切な対応をとれるようにするCSIRTの役割は極めて重要である。組織内にCSIRT

チームを設立する動きが加速しているが、その構築・運営には高いスキルと経験・ノウハウが求められる。このため、“CSIRTを設立したが、上手く機能していない”といったことにもなりかねない。そこでNTT-ATでは、顧客のCSIRTチームの代替およびCSIRTの運営を支援することを目的にした包括的なセキュリティサービスを提供している。その主なサービスは、診断・コンサル・訓練・監査、CSIRT/SOC支援に加え、端末・ネットワーク・クラウドを含むITシステム全体の状態をモニタリング・分析し、原因を特定して対処するマネージドサービス、フォレンジクス・再発防止を含む復旧支援からなっている(図1)。

同社は、NTT研究所が運営するグループ向けCSIRT組織であるNTT-CERTの支援業務も受託して



NTT アドバンステクノロジー株式会社
セキュリティ事業本部
マネージドサービス BU
[左] BU長 福井 将樹氏
[右] 副主任技師 徳武 美奈子氏

おり、CSIRTの構築・運営・インシデント対応に関する豊富な経験やスキル・ノウハウを有している。

徳武氏は、「私どもでは、情報セキュリティに関する高いスキル・経験をベースにしたコンサルティングや教育に加え、NTT-CERTの支援業務で培った豊富な経験・ノウハウを活かした組織内CSIRT支援のほか、セキュリティ診断や監査、販売・構築、監

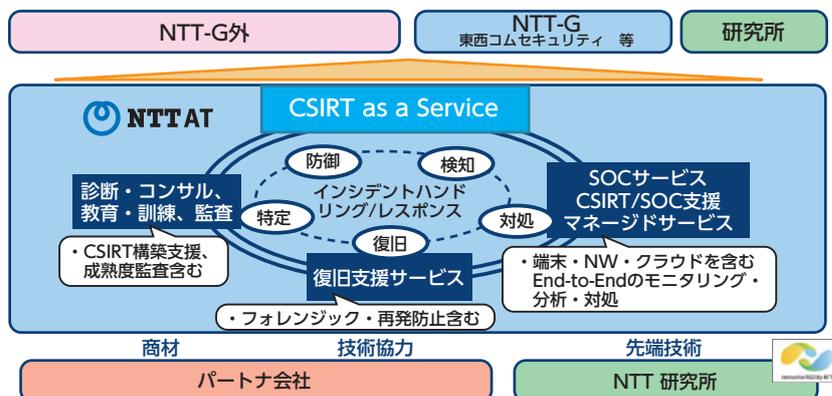


図1 NTT-ATの「CSIRT as a Service」の概要

視運用、インシデント対応までの各領域で有効な国内外の先進的なセキュリティ商材を目利き・組み合わせて最適化した、幅広いセキュリティソリューションを提供しています(図2)。抜け・漏れ・落ちのないトータルな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る点が大きな強みであり特長です」と強調する。

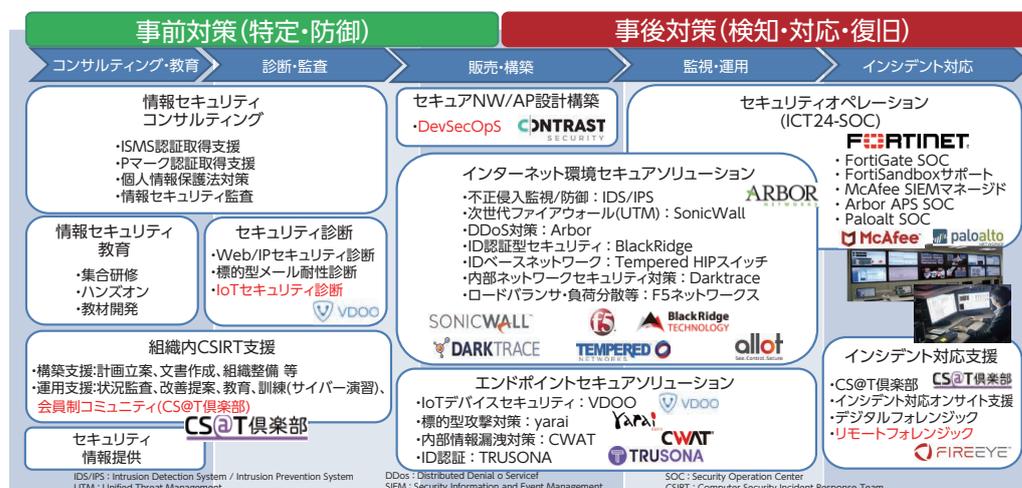


図2 NTT-ATのセキュリティソリューションマップ

年間36万円でサイバー保険付きの会員制コミュニティ型サービス「CS@T倶楽部」を提供

NTT-ATならではの「CSIRT as a Service」の特徴的なサービスとして、企業・団体などの組織内CSIRTを支援する会員制のコミュニティ型サービス「CS@T倶楽部」(<https://www.ntt-at.co.jp/product/csirt-club/>)がある。年々高度化・巧妙化するサイバー攻撃に対して、CSIRTの運用者だけではとても対応しきれないのが実状だ。実際、①セキュリティインシデントが発生しても、どうしていいかわからない、②気軽に相談できる専門家や仲間が周りにいない、③セキュリティ対策に多額の投資はできないといった声を耳にする。

そこでNTT-ATでは、中堅・中小企業をメインターゲットに、図3に示すようなCSIRT運営を手厚くサポートする幅広いメニューからなるコミュニティ型サービス「CS@T倶楽部」の本格提供を本年7月より開始した。本サービスの主な特徴として以下の3点が挙げられる。

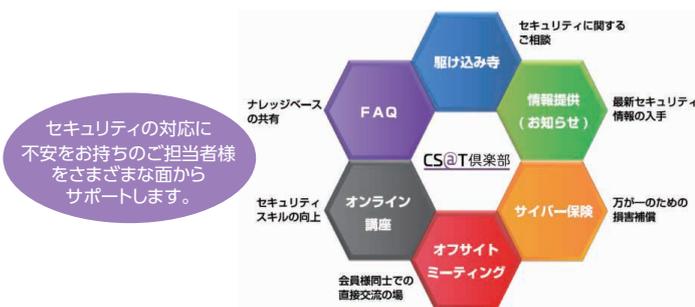


図3 「CS@T倶楽部」のサービス構成

1. インシデント発生時の“駆け込み寺”

突然の事件・事故の際は、被害の拡大防止と原因究明のため、メール&会員専用ポータルサイトに24時間365日体制で相談を受け付けている。

2. 有事に備えた体制構築を全面サポート

平常時も会員専用ポータルサイトを通じてさまざまな情報を発信。コミュニティページでは会員同士が匿名で情報交換することも可能。

3. 漏えい事故の際の賠償責任保険をセット

すべての会員には、サイバー攻撃や情報漏えい事故などによる賠償損害や費用損害を補償する三井住友海上の賠償責任保険「サイバープロテ

クター」付帯。情報流出などで損害賠償が発生した際にも安心。

基本サービスの提供料金は年額36万円と低価格ながら気軽に相談でき、しかもサイバー保険が付帯しているのは、CSIRTの運用者にとっては魅力的なサービスといえる。

「1年間で200社の会員獲得を目標にしています。また“CS@T倶楽部”の仕組みのOEM提供も行っており、NTTコミュニケーションズが提供している“セキュリティサポートデスク”のオンラインコミュニティサービスに採用されています。なお、今後の“CSIRT as a Service”のラインナップについては、IoTセキュリティやEDR(Endpoint Detection and Response)サービスの展開を予定しています」(福井氏)。