

インタビュー

セキュリティ R&D の専門技術者 集団として、NTT 事業及び社会へ の貢献を目指す

本年4月のNTTのR&D体制再編に伴い、NTT研究所のセキュリティ技術のR&Dやセキュリティ運用支援の機能を切り出して新設された「NTTセキュアプラットフォーム研究所」。設立の背景・狙いから、主要ミッション、セキュリティR&Dの推進状況について、桑名栄二所長にうかがった。

NTT 研究所のセキュリティ R&D の専門技術者集団

——本年4月、NTTのR&D体制の再編に伴い、「NTTセキュアプラットフォーム研究所」（以下、SC研）が新設されました。はじめに、設立の背景・狙い、主要ミッションからお聞かせください。

桑名 サイバー攻撃の増加やスマートフォンを狙った情報窃取の増加に代表されるように、全世界のサイバーセキュリティを取り巻く環境は、今、まさに大きく変わろうとしています。このような時代の変化にいち早く対応するため、高度な技術と専門知識を有したセキュリティ技術者集団を組織し、NTT事業会社や外部研究機関、セキュリティベンダ等との強固な連携により、お客様に安心安全を提供することがNTT R&Dの使命と考えました。このような背景のもと、従来、情報処理研究を担っていた研究所組織から、セキュリティ技術のR&Dとセキュリティ運用支援の機能を切り出し、NTTグループ内外との連携・協力

体制の核として設立したのがSC研です。今春の紫綬褒章を受章した、SC研に所属する岡本龍明R&Dフェロー他3名のグループが30年近くに研究所の一角で暗号の研究を始めたのがセキュリティR&Dの先駆けですが、今や約180名の専門技術者を擁する一つの組織体として、活動を開始しています。

SC研の主要ミッションは、NTTグループが提供するコミュニケーションサービスを安心して安全なものにすることです。分野としては、法人系分野、社内情報システム、更にはNTTが所有するインフラがありま



日本電信電話株式会社
NTTセキュアプラットフォーム研究所
所長 桑名 栄二氏

す。これをよりセキュアなものにしていくことです。図1に示すように、①クラウドやスマートフォンなどの新システム・サービスの利用拡大、②攻撃の仕組みの複雑化と目的も金銭や組織活動の妨害へと深刻化、③取り扱うデータ量も爆発的に増加し、守るべき情報資産の割合も増加、といった3つの変化に迅速に対応するセキュリティR&Dを推進するというのが基本的な考え方です。

——SC研様の組織の概要をお聞かせください。

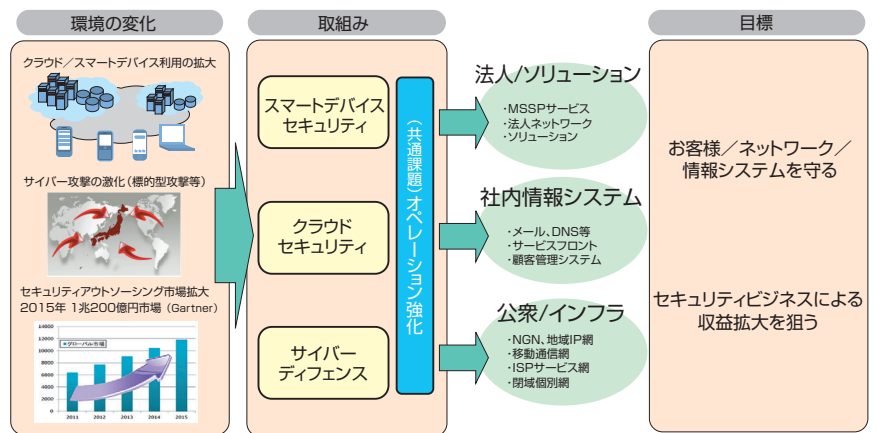


図1 SC研におけるセキュリティR&Dの基本方針

桑名 次世代暗号等、暗号に関する先端研究を行う「岡本特別研究室」、セキュリティ対策の維持強化に向けた研究開発を行う「セキュリティマネジメント推進プロジェクト」、安心・安全なネットワーク基盤に関する研究開発を行う「ネットワークセキュリティプロジェクト」、安心・安全な情報基盤に関する研究開発を行う「情報セキュリティプロジェクト」、公共サービスのICT化を支える技術の研究開発を行う「パブリックICTソリューションプロジェクト」の構成で、セキュリティR&D活動を展開しています。

「セキュリティR&D宣言2012」を掲げ、3つの重点R&D施策を展開

——設立初年度の重点R&D施策をお聞かせください。

桑名 SC研では、世の中に蔓延する新たなセキュリティ脅威からお客様やICTインフラといった資産を守るべく、技術と運用の両面から以下の3つのR&Dに取り組み、安心・安全に貢献しますという「セキュリティR&D宣言2012」を掲げました。

- ・ICT環境の脅威と脆弱性を徹底的に把握する技術と運用スキームの研究開発を行います
 - ・安全性が保障できる先進的システムの研究開発と標準化を進めます
 - ・セキュリティイベント情報を継続的にウォッチ&分析し、インテリジェンスに変えての速やかな対応を行う運用スキームを構築します
- 設立初年度の今年、この3つのR&Dに重点的に取り組みます。

——その中で、最も重要と考えている領域は……。

桑名 やはり一番は、クラウドサービスを支えるセキュリティ技術です。お客様の情報資産をクラウド上で安心して蓄積・処理できる（見逃さず、損失せず、漏洩せず）ようにするには、システムの状況やセキュア度を徹底的に可視化／モニタリングするセキュリティ技術と、複数の攻撃手法を組み合わせた攻撃に対応するための様々なセキュリティ技術を活用した多面的・多層的セキュア化が重点R&D領域だと考えています。

——ファイアウォールやIDS/IPS（不正侵入検知／防御装置）だけでは守り切れない……。

桑名 点で防御する方法では、限界があります。様々なセキュリティ技術を活用して多面的・多層的にセキュリティ化を図る必要があると思っています。例えば、お客様の端末、NTTのホームゲートウェイ、ネットワーク、データセンタ、クラウド上の仮想基盤など、多面的・多層的に防御する必要があります。

——各論の頁で、各プロジェクトの最近の取組みをいくつかご紹介しますが、先ほどのお客様の情報資産をクラウド上に安心して預けられるようにするために、どのようなセキュリティ技術に取り組んでいますか……。

桑名 データを単独では意味のない複数の断片に分割して分散保管し、分割データを復元せずに秘匿したまま統計分析処理を行う秘密分散／秘密計算技術、クラウド上のログを連結・可視

化するクラウドフォレンジックス技術、クラウドに復号処理をアウトソースし、復号鍵を管理することなくデータを保管することが可能なクラウド鍵管理型暗号などがあげられます。

セキュリティCOEとして世界最先端を走り続ける

——最後に、今後の抱負と研究者へのメッセージをお願いします。

桑名 セキュリティCOEとして、研究開発の世界最先端を走り続けるとともに、暗号研究、マルウェア対策、セキュリティ評価、ログ分析の4つの柱に対して技術的優位性を与えることで、NTTグループ各社の競争優位を下支えしたいと思っています。現在、次世代アルゴリズム考案に向けた革新的暗号研究では、世界の最先端を走っています。また、ハニーポットを用意し、高度なマルウェア対策仮想化技術に取り組んでおり、世界最高精度の攻撃検知・解析手法の構築・提供を行っています。

私自身は、世の中の役に立ちたいと頑張っている若手研究者が元気に、活躍できるような組織にすることを常に心掛けています。若手研究者には、「セキュリティ技術を極めると同時に、人と人、組織と組織が連携し、もっともっと化学反応を起こすような人間たれ！」と言いたいですね。またセキュリティ脅威はグローバルですから、セキュリティR&Dのグローバル化についても今後、力を入れていきたいと思っています。

——本日は有り難うございました。

（聞き手・構成：編集長 河西義人）