FFR yarai analyzer 導入事例

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ

革新的で信頼性が高く、国内、海外を問わない シームレスなICTサービスを提供する“Global ICT Partner”

NTTコミュニケーションズ（略称：NTT Com）では、2015年に向けて、国内・海外を問わず、シームレスにクラウドサービスを提供するという「グローバルクラウドビジョン」を掲げています。

NTT Comのグローバルクラウドサービスでは、法人や個人のお客様を対象とし、ネットワークやホスティングをはじめとしたインフラから、SaaSによる様々なアプリケーションまで幅広いサービスを提供しています。

お客様がこれらのサービスを安心・安全にお使いいただけるよう、セキュリティにも力を入れています。

先端IPアーキテクチャセンタでは、これらのサービスを支える基盤となる技術のR&Dに携わっており、現在は、クラウド、スマートフォン、セキュリティの3つの分野に注力しています。

先端IPアーキテクチャセンタ
セキュリティ テクニカルユニット　主査
畑田　充弘 氏

「セキュリティ テクニカルユニットでは、セキュリティにフォーカスし、サイバーセキュリティと情報アシュアランスの2つの観点からR&Dを進めています。
サイバーセキュリティでは、インシデントが発生した際に如何に早く検知・防御できるか、あるいは復旧できるかといったインシデントレスポンスの一連の工程を調査・研究しています。
情報アシュアランスでは、例えばアプリケーション開発において、そもそも脆弱な部分を作り込まないために、要件定義、設計、コーディング、テストといった各工程での技術サポートを行っています。」（畑田氏）

導入の背景 サイバーセキュリティ上の実態を把握する必要性

「サイバーセキュリティにおいては、実際にどのようなことが起きているのかを把握する必要があります。攻撃の手法や攻撃の規模といったインシデントの実態を知らずに、適切な製品を選択して自社のサービスに取り込み、お客様に提供することはできません。」（畑田氏）

NTT Comでは、実態把握の一環として、ハニーポットを運用しており、そこで収集したマルウェアを解析するためにFFR yarai analyzer（略称：yarai analyzer）を利用しています。

「yarai analyzerを導入した目的としては、ハニーポットで収集したマルウェアやインシデントで捕獲したマルウェアを自分たちの意思の中ですぐに解析したいといったことが最も大きな要因でした。

また、昨今の未知マルウェアへの対策トレンドとして、Sandboxを搭載したセキュリティ対策製品が幾つか登場しましたが、それらの製品の解析結果の妥当性は、一つの製品の解析結果だけを見ても判断できないため、各製品の解析結果を比較することが必要でした。また、従来の検体解析の課題として、環境依存の問題によって解析できないケースもあり、複数の製品を横並びで利用することが必要でした。」（日吉氏）

先端IPアーキテクチャセンタ
セキュリティ テクニカルユニット
日吉　龍 氏

導入の経緯
FFRIの技術力に注目

「我々のミッションの一つとして、製品やその技術の目利きといったものもあり、良い製品があれば検証して、自社のインフラを強化したり、お客様に提供するサービスにも取り込むことを提案することが求められていますが、FFRIの技術力やセキュリティリサーチ能力には、会社設立当時から注目しており、FFRIの動向は常にウォッチしていました。

そんな中で、サイバーセキュリティの実態把握のために、手軽に検体解析を実施できるyarai analyzerは、我々がまさに必要とする製品でした。」（畑田氏）

導入の効果
マルウェア判定の明確さとわかり易い判定理由、解析環境の自由度の高さ

先端IPアーキテクチャセンタ
セキュリティ テクニカルユニット　主査
田中　恭之 氏

「yarai analyzerを導入するにあたって、評価したポイントとしては、マルウェア判定の明確さと、その判定の理由を具体的にレポートに表示してくれることでした。

純国産製品であることから、検体の挙動などの解析結果が日本語でわかり易く表現されており、外資系ベンダーの製品と比較して、言葉の解釈上の誤解が発生するリスクも少ない点が最も大きなポイントでした。

また、解析環境を自由にカスタマイズできることもポイントの一つです。マニュアルに従って環境を構築することで、自分の好きなように解析環境をセットアップできるため、環境依存の問題からも解放されました。マニュアルもわかり易く、解析環境の構築にあたってサポートに問い合わせる必要もありませんでした。」（田中氏）

今後の展望
システム間連携による自社サービスへの展開を検討

「現時点では、サイバーセキュリティにおけるマルウェアの動向把握の一環として、yarai analyzerを利用していますが、最終的にはサイバー攻撃を防御・回避するために自社サービスに取り込むといったことを検討していきたいと考えています。そのためにも、システム間連携のし易いインタフェースを我々からも要望することで、より良いパートナーとなれればと思っています。」（田中氏）

製品・サービスについてのお問い合わせは
株式会社FFRI
〒150-0013
東京都渋谷区恵比寿1-18-18　東急不動産恵比寿ビル4階
TEL：03-6277-1811　E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。
http://www.ffri.jp/

2013年6月現在
Ver.2.00.02