株式会社エヌ・ティ・ティ・データ

新しい領域のセキュリティに対応する体制作り

KASPERSKY lab

高度化と多様化が進むサイバー攻撃に より早く、より正確に対応できる セキュリティ人材の育成へ

株式会社エヌ·ティ·ティ·データ(以下、NTTデータ)は、Global IT Innovatorをグループビジョンとして掲げ、システムインテグレーション事業とネットワークシステムサービス事業およびこれらに関する一切の事業をグローバルに展開しています。お客様のビジネスを支えるシステムとネットワークを提供する同社にとって、サイバーセキュリティは重要な取り組みの1つであり、以前から技術やインテリジェンスを収集するだけでなく、社内のセキュリティ人材育成に力を入れています。

しかし、サイバーセキュリティの「防御」に関しては攻撃者の攻撃技術が、防御技術を上回る場合もあり、「絶対」という言葉はありません。どれだけ守りを固めても「攻撃者が有利」であるという事実に変わりはなく、攻撃者の侵入をいかに早く検知し、正しく、迅速に対処するかが、重要になります。中でも近年注目が高まっているキーワードが、サイバー攻撃や情報流出などの被害を最小化するために必要な“インシデント対応”と、その問題の解決や法的な対応に向けて、分析に必要な証拠の保全および調査·分析などを行う“デジタルフォレンジック”です。

NTTデータでは、これまで様々なインシデントのデジタルフォレンジックを行い、社内にその技術とノウハウを継承してきましたが、絶えず進化した攻撃によるインシデントの解析や新しい脆弱性による被害の調査が必要になっています。そうした中、NTTデータが求める高度な技術力と知見力を持つセキュリティ人材の育成に有効な外部トレーニングとして、今回選ばれたのがカスペルスキーの提供する「サイバーセキュリティ　トレーニングサービス」でした。このサービスは「カスペルスキー　インテリジェンスサービス」がカバーする5つの領域のうち、「教育·育成」分野に該当するサービスで、インシデントレスポンス、デジタルフォレンジック、マルウェア解析·リバースエンジニアリングトレーニングなどがあります。

通信 / IT

- 設立:1988 年
- 「Global IT Innovator」というグループビジョンを掲げ、ITを事業のコアとして、世界的な舞台への進出を本格化。ITを活用した新たなビジネスやサービスを構想し実現することで、社会やビジネスの発展に貢献しています。

リスクを**予見**する
攻撃を**防御**する
インデントに**対処**する
攻撃を**発見**する
セキュリティの**啓発・教育** / スキル**育成**

「カスペルスキー インテリジェンスサービスがカバーする5つの領域」

「いくら防御を固めても、攻撃者の有利に変わりはなく、侵入を完全に防ぐことはできません。企業側の対応において、デジタルフォレンジックは非常に重要です。そのため当社では専門部署以外の人材にも教育を行うことで、システム構築前から、フォレンジックを意識した適切なシステム構成、ログ取得方法、運用法などをご提案できるように準備しています」

株式会社エヌ・ティ・ティ・データ
セキュリティ技術部 サイバーセキュリティ統括部
部長 鴨田 浩明 氏

課題

あらゆるビジネスや社会インフラにICTが浸透している現在、サイバーセキュリティ対策においては、デジタルフォレンジックを始めとする「“侵入を検知した後の対応”が大切」と、NTTデータ セキュリティ技術部 サイバーセキュリティ統括部 部長 鴨田 浩明 氏は言います。

「防御に100%の力を注ぐのではなく、防御・対応・復旧にバランスよくセキュリティにかけるリソースを配分することが大切です。特に、侵入などの被害をいかに早く検知し、対処するか。そして、被害に遭った企業や組織には、その原因や被害の全容等をいかに早く把握・特定してお客様に報告するという責任があります。

そのためには、初動対応として証拠を保全し、分析するデジタルフォレンジックを行うことが必要不可欠になります」

NTTデータには、デジタルフォレンジックに関する確たる技術とノウハウが蓄積されていますが、サイバー攻撃の手口や手順はさまざまに変化します。最新の手口に、素早く、的確に対応するためには「幅広いフォレンジックツールを使えるように、多彩なナレッジを吸収し、異なるスキルを持った人材を育てることも大切」と鴨田氏は言います。

カスペルスキーのソリューション

NTTデータが、カスペルスキーのトレーニングに注目した背景には、カスペルスキー製品の「業界屈指の検知力」と業界をリードするインテリジェンスへの評価があったと、鴨田氏は説明します。

「カスペルスキーのセキュリティ製品は、マルウェアなどの検知率が非常に高いと、業界内でも定評があります。それだけ高い技術を持つカスペルスキーのフォレンジック研修ならば、きっと得るものも大きいだろうと期待したのです」

今回NTTデータが受講した「デジタルフォレンジック トレーニング（基礎編）」では、セキュリティに関して体系的に整理したテキストを基に、グローバルの第一線でインシデント対応サービスを提供するKaspersky LabのGlobal Emergency Response Team (GERT) に所属するのセキュリティ エンジニアが

株式会社エヌ・ティ・ティ・データ
コンサルティング担当
課長代理 井上 哲也 氏

「非常に体系的に整理されたテキストが分かりやすかったです。また、インシデントを再現した実機を使って、非常にリアルに対応を学ぶことができたのは貴重な経験でした。また、ツールに頼らず、必要な情報が、どこにある・どのファイルに・どのように格納されているかなど、他のトレーニングでもなかなか得られないような情報まで得ることができました。何よりも、今後自分がどのような技術を身につけていくべきか、はっきりと見えたことがありがたかったです」

株式会社エヌ・ティ・ティ・データ
コンサルティング担当
主任 松尾 将大 氏

「実機を触りながらトレーニングできたこと、そして講師の方が、豊富な経験談を交えて、“どういう観点で、どこを見て、痕跡を探すか”という勘所を解説してくれたことが、非常に分かりやすかったです」

講師として担当しました。テキストには収録しきれない最新の事例を含めてフォレンジック解析のノウハウを解説しました。さらに、実際のインシデントを再現した実機やデータを使った研修では、座学では得られない“追体験”が可能になっていました。
今回、NTTデータが受講者として選んだのは、社内のセキュティ専門チームであるCSIRT（Computer Security Incident Response Team：シーサート）とは別部署に所属する2名です。その目的は「お客様への提案時に、インシデント発生を見込んだ効果的なログの管理方法や、インシデント対応方法や体制なども含めて提案できるようにすること」にあると鴨田氏は言います。
「例えば、PCなどのマルウェア感染が検知された際に、すぐにネットワークから切り離したり、アンチウィルスソフトでスキャンしたり、電源を落としたりといった様々な行動が推奨されていますが、その結果、証拠となる端末内の痕跡が消えてしまう場合もあります。だからこそ、日頃からログを取得・管理し、万一の事態に備える必要があります。普段お客様と接する機会の多いコンサルティング部門などにも、こうした知識を持った人材を増やすことで提案の質が向上していくと期待しています」

展望

鴨田氏は次のように続けます。
「当社は、システムインテグレーターとして、お客様のセキュリティ対策まで期待に応えていく必要があります。数年前までは、防御が中心でしたが、最近ではフォレンジックを含め、インシデントの初動対応からシステムの復旧まで総合して請け負う機会が増えてきています。
そのためには、社内のCSIRTを増強するだけではなく、お客様への提案を行う各部署にセキュリティの高い知識を備えた人員を配置し、全社的な体制強化を図っています。
さらに今後は、IoT（Internet of Things）や自家用車の自動走行など、新しい領域のセキュリティ対策が求められます。
社内に、より広く、より多様な技術と、知識と、ノウハウを蓄積させていくためにも、ぜひ今後とも、カスペルスキーと連携していきたいと考えています」

**カスペルスキーの製品とサービスについて、詳しくは担当の営業に
お問い合わせいただくか、www.kaspersky.co.jp をご覧ください。**

株式会社カスペルスキー
〒101-0021
東京都千代田区外神田3-12-8
住友不動産秋葉原ビル 7F
jp-sis@kaspersky.com
www.kaspersky.co.jp/industrial-security-cip

BD-KSIS-SS-201705-001