# IBM セキュリティー・オペレーション・センターのご紹介

## ― 国境なきサイバー攻撃に立ち向かうインターネット・セキュリティーの最前線 ―

近年、インターネットにおけるサイバー攻撃が、Webサイトを無差別に改ざんするなどの愉快犯的な攻撃から、標的型攻撃に代表される特定の企業や団体、個人を狙って機密情報や個人情報を盗み取るような攻撃へと変化する傾向にあります。また、2011年9月以降、日本国内の企業・政府関係機関を対象にしたサイバー攻撃がさまざまなメディアで報道されるようになり、ますます情報セキュリティー対策に注目が集まり、外部のセキュリティー専門家が提供する運用サービスを検討する傾向が高まっています。

今回、このような情報セキュリティーへの脅威を監視・分析しているIBMのSecurity Operation Center（以下、SOC）と、SOCで観測している脅威の動向を年2回公開している「Tokyo SOC 情報分析レポート」を紹介いたします。

### 1. 世界規模の情報収集力を持つ9拠点のSOC

IBMのSOCの特長として第一に、世界規模でリアルタイムに発生している脅威動向の情報収集が挙げられます。SOCでは、133カ国の約4,000社のお客様に不正アクセスの監視サービスを提供しています。世界9拠点のSOC（図1）では、お客様環境に設置したファイアウオールやIPSなどのセキュリティー機器約2万台を監視・管理しており、1日当たり約130億件のイベントが送られてきます。SOCのセキュリティー・エンジニアは、送られてくるイベントを分析することで、お客様のシステムを守るために必要な脅威情報を全世界レベルで収集しています。

この全世界レベルで収集した脅威情報を基に、お客様環境に設置しているセキュリティー機器の変更を行うとともに、セキュリティー・インシデント発生時にはセキュリティー情報をお客様への対応アドバイスやセキュリティー・アドバイザリーといった形で提供しています。

### 2. セキュリティー研究機関「X-Force」との連携

IBMでは、「X-Force」に代表されるセキュリティー研究センターを世界9拠点に設置しています。SOCでは、リアルタイムで発生している脅威情報をX-Forceへ提供し、その調査、研究結果のフィードバックを受けるというサイクルを回していることが、IBMのSOCが持つ第二の特長です。

X-Forceでは、SOCで収集された脅威情報をさまざまな角度から分析し、新たな攻撃手法や脆弱性（ぜいじゃく）をいち早く発見する調査、研究を行っています。また、お客様のシステムを新たに発生する脅威から守るために、SOCはX-Forceからフィードバックされた調査結果をSOCの監視システムに反映しています。

### 3. 国内の脅威動向を解説した「Tokyo SOC 情報分析レポート」

前述した世界9拠点のSOCで観測した脅威情報およびセキュリティー研究機関の研究結果に基づき、主に日本国内に影響を与える脅威の動向を日本の東京セキュリティー・オペレーション・センターに所属するセキュリティー・エンジニアが年2回、2月と8月に「Tokyo SOC 情報分析レポート※1」として発信しています。このレポートでは、実際に行われている攻撃の説明や攻撃数の推移、対策などを解説しています。

また、「Tokyo SOC 情報分析レポート」のほかにも、タイムリーな最新の脅威動向をブログ形式の「Tokyo SOC Report※2」で解説しています。

これらの情報を、セキュリティー・ポリシーの策定や、情報セキュリティー対策を設計する際の参考として、また、情報セキュリティーに関する知識向上の一助として、ぜひご活用ください。

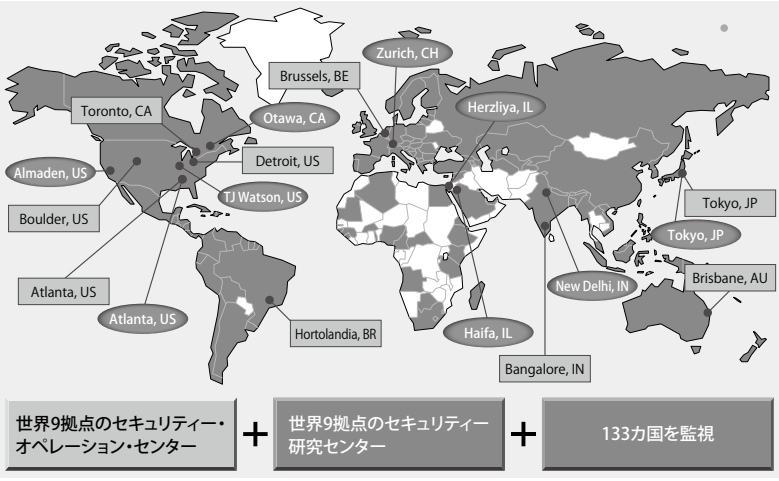


図1. IBM セキュリティー・オペレーション・センター

※1 Tokyo SOC 情報分析レポート
http://www.ibm.com/services/jp/ja/it-services/soc-report-201202.html
※2 Tokyo SOC Report
https://www.ibm.com/connections/blogs/tokyo-soc/?lang=ja