マネージドセキュリティサービス 最前線
第4回 ー 実例ベースで考える ー

～グローバルにおけるセキュリティ対策のポイント～

インシデント対応から分かるグローバル運用の難しさ

NTTコミュニケーションズ㈱　経営企画部
マネージドセキュリティサービス推進室長
与沢 和紀

NTTコムセキュリティ㈱
オペレーション＆コンサルティング部
羽田 大樹

グローバルに市場を求めて日系企業が海外に支社や拠点を置くことは近年では当然のように行われているが、その規模が大きくなるほど企業の戦略を支えるICTシステムも現地のベンダーが構築し、現地で運用することになる。連載第4回となる今回は、我々がアジアにおいて現地で行ったインシデント対応の事例をもとに、グローバルにおけるセキュリティ対策の難しさと対策を行う際のポイントについて考察する。

インシデント対応の経緯

今回インシデント対応したお客さまは日本だけでなく世界でもブランド力を持つ製造業であり、世界中にも数多くの拠点を持っている。インシデントが発生したのは、このお客さまのアジア地域を管轄するハブ拠点となるデータセンターにおいてである。ある日の深夜に、インターネット境界に設置したファイアウォールの負荷が突然高まり、業務通信が止まってしまったのだ。お客さまの現地ベンダーがこの事象を調査したところ、DMZに設置したいくつかのサーバーが大量に不審なトラフィックを送信していたことが分かった。原因が不明であったが、該当サーバーを一時的に切り離して様子を見たところ問題がおさまったため、再びシステムを稼動させたという。システムは無事に復旧されて暫定対策が行われたように見えるが、なぜこのような事象が発生したのか原因が分からず、より大きな問題を抱えたままであることも考えられるため、お客さまから弊社に緊急調査を依頼されたのだった。

まずは情報を整理する必要があるが、システムはアジアのハブ拠点となるデータセンターに存在しており、担当者も現地にいる。電話会議とメールでのヒアリングは困難を極めた。ネットワーク構成図を見てシステムの全体像は分かったものの、システムの規模が大きいため、各サーバーの働きや通信経路までは聞き出せず、さらに事象の原因についてあたりがついていないために調査すべき対象サーバーの数も多くなり、調査するログファイルの容量が共有できないほど大きくなってしまった。現地ベンダーと直接対話することもできず伝言ゲームになってしまい、こちらが指定した情報や実行して欲しいコマンドがなかなか伝わらなかった。要するに拠点が海外であるために、コミュニケーションが格段に難しくなったのだ。

最終的にお客さまから現地に来てほしいという依頼を受け、関係者が集結して現地でアクション会議を開いた。１日かけてシステム構成を詳細に把握し、インシデントが発生した時の対応を時系列で整理した結果、ようやく今回のインシデントの全貌が見えてきた。特にこの中で現地ベンダーにて不審と判断した事象が10点近く存在することが分かり、ここで議論のポイントが整理できたのである。

不審と思われるポイントを整理して関連するログファイルを特定できたため、現地ベンダーにヒアリングしながらログの解析や設定の確認を行い、事象を１つずつ明らかにしていくこととし、例えば、大量に送信されたトラフィックの一部は、定期的に実行される巨大なファイルをバックアップする正規の業務通信あるため除外するなどの分析を順次実施した。結果としては、不審な事象の大半は正常な動作であることが分かり、最終的に問題は２点に絞ることができた。

１点目は設定の不備を悪用してDMZ上のサーバーをDoS攻撃の踏み台として利用し、外部に攻撃を仕掛けていたことである。今回はシステムが停止したため幸いにも外部への攻撃は発生しなかったが、問題は解決しておらず再びシステムが停止する可能性があったと

いうことになる。もう1点は同じウイルスに感染した複数のサーバーが存在していたということである。事象が明確になったためその場で問題点を修正し、ようやくインシデントをクローズすることができた。

グローバルにおけるセキュリティのポイント

最も重要なのは、セキュリティに限らずシステムの運用や統制を現地だけに任せず、支社や各拠点のガバナンスを確立することである。今回のインシデント調査は実は現地ベンダーではなく、本社から依頼を受けていた。現地では事象が落ち着いており原因を調査する前にクローズしようとしていたため、本社が「待った」をかけたのである。また、ウイルス感染していたホストも現地の担当者が独自の判断で調達したものであったため、セキュリティ更新が適切に管理されていなかった。必ずしも日本が要求する水準でセキュリティの運用や対応がなされている訳ではないことに留意したい。

次に、有事に備えた体制を構築し、コミュニケーションの手段を確立しておく。インシデントの解決には、セキュリティの知識だけではなく、システム構成や業務を細かく把握する必要がある。システム管理者だけでも、セキュリティベンダーだけでも解決できるものではないため、伝言ゲームの距離を極力短くして円滑なコミュニケーションを図る。コミュニケーションの中には、ログや設定などの受け渡し方法、言語や時差も考慮しておく必要がある。さらに、この中に強固なパートナーシップを提携しているセキュリティベンダーがいれば、緊急時であっても情報を一から共有せずに本質的な議論に進めるであろう。

最後に、インシデントの現場では何が正常で何が異常かシステム管理者でも分からなくなるため、混乱した現場での報告は事実と推測が入り混じってしまう。これらは明確に区別して整理を行い、推測については1つずつログやシステム情報と突合して事実として確定

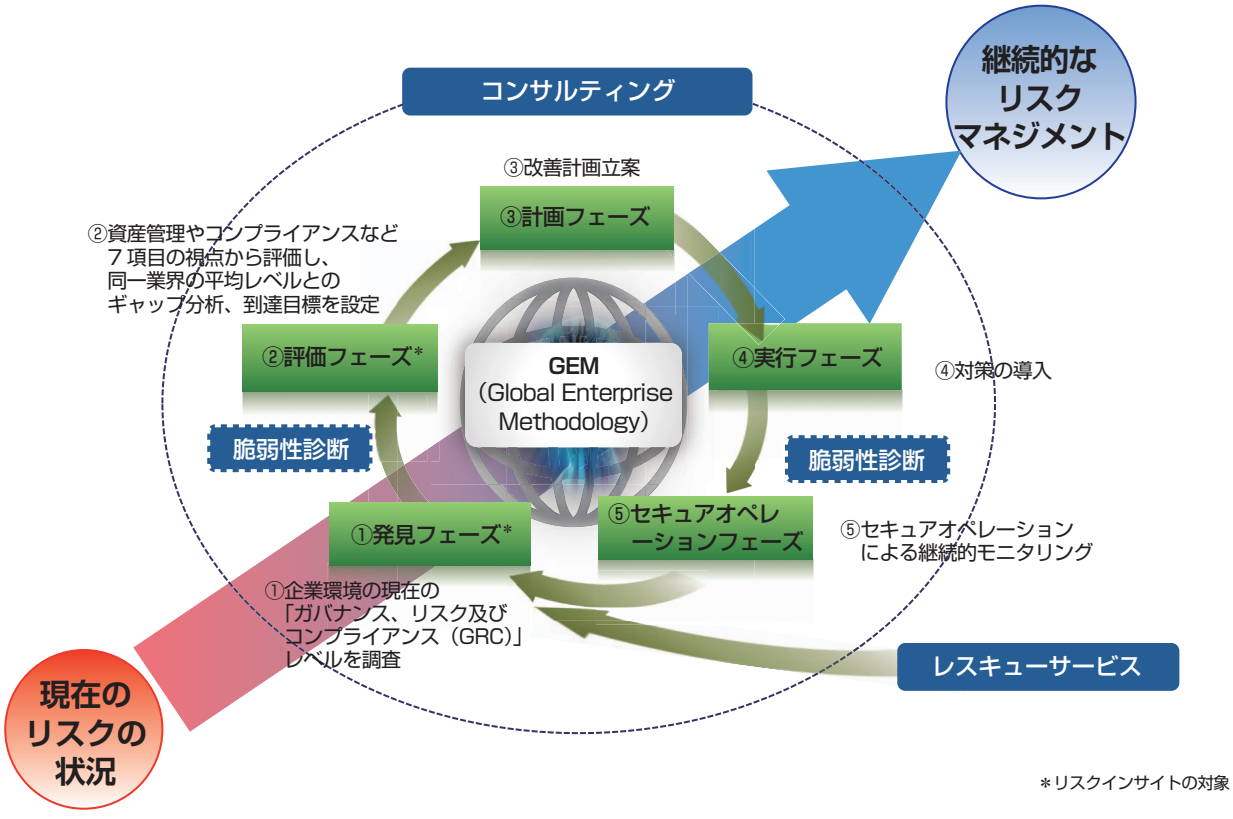

図1　プロフェッショナルサービスの概要

マネージドセキュリティサービス 最前線

第4回 ー 実例ベースで考える ー

プロフェッショナルサービス

	メニュー		概要	初期費用 *1（税別）
コンサルティング	総合コンサルティング		GEM及びその他要望に基づくコンサルを提供	個別見積
	エントリーモデル *2	バーチャルCSO	時間契約（80時間相当）で、戦略的アドバイスや資格に基づいたアドバイスを実施	2,300,000円
		非常勤エキスパート	時間契約（9日間相当）で、月毎のセキュリティのテーマでアドバイスを実施	1,500,000円
		ワークショップ	個別テーマに基づく説明会（1回半日）	200,000円
		リスクインサイトエクスプレス	リスクの簡易診断・評価	160,000円
レスキューサービス	総合インシデントレスポンス		緊急事態にプロフェッショナルエンジニアが調査・分析を実施初動対応、調査分析、改善提案まで提供	個別見積
	インシデント初動対応パック *2		情報の整理、事象の把握と調査、被害の拡大防止までを実施	1,000,000円
脆弱性診断	Webアプリケーション/ネットワーク脆弱性診断		Webサイトの改ざんやネットワーク経由でのICT環境への不正アクセスなど、システムの弱点である脆弱性を診断、可視化	個別見積

*1：提供条件等の詳細は別途お問い合わせください
*2：日本独自メニュー

表1　プロフェッショナルサービスのメニュー及び料金

していく。この際にログを解析できる技術者と、コーディネートできる進行役が必要である。

対策について

セキュリティ対策やリスクマネジメントを考える際に重要なポイントの1つとして、予めセキュリティマネジメント体制を確立しておき、有事の際への対応も出来るようにしておく必要がある。

NTTコミュニケーションズでは、経験豊富なセキュリティエキスパートにより、グローバルに展開するお客さまのICT環境のセキュリティレベルを把握し改善する「WideAngleプロフェッショナルサービス」を昨年11月、日本でも提供し始めた（図1、表1）。その中で、Global Enterprise Methodology（GEM）というグローバルで統一したリスク定量化・管理手法により、お客さまのICT環境の調査・改善・モニタリングを含め総合的にコンサルティングするサービスを展開している。これにより、全世界の拠点や組織のセキュリティ対策の成熟度を共通の尺度で俯瞰することができ、計画的なセキュリティ対策への投資が可能となる。本事例ではアジア内であったため、日本から応援体制を構築したが、グローバルに展開するNTT Com Security（NCS）であるが故に迅速かつ均一な対応が可能である。本サービスは、NCSにおいて、約25年の海外提供実績があるが、日本独自メニューとして、広範囲にわたるコンサルティングサービスの中からご要望の多い業務を個別メニュー化した「エントリーモデル」を用意し、よりコンサルティングサービスを受けやすいようにした。セキュリティコンサルタントの知見やノウハウが必要な業務をピンポイントで手軽に利用できる。

更に、不正アクセスやマルウェア感染、情報漏洩などのお客さまのセキュリティインシデント発生時に、プロフェッショナルエンジニアが初動対応から調査・分析、改善提案を行うレスキューサービスも提供している。本サービスも日本独自メニューとして、予め設定した料金で、事象の把握から被害の拡大防止を行う応急処置の検討、報告までを実施する「インシデント初動対応パック」の提供を開始した。緊急対応が必要かつ費用の見通しを立てることが困難な状況において、専門的スキルを有するプロフェッショナルエンジニアによる初動対応を安心して要請することができるようにした。

お問い合わせ先
NTTコミュニケーションズ㈱
経営企画部マネージドセキュリティサービス推進室
E-mail：mss-sp-cp@ntt.com