マネージドセキュリティサービス 最前線
第5回 ー 実例ベースで考える ー

～グローバル企業への総合セキュリティサービス提供事例～

グローバル企業のチャレンジと対策

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

多くのグローバル企業がそうであるように、今回取り上げる事例で紹介する企業も、買収にてグローバルへの事業拡大をはかってきた。そして、その最中、セキュリティ事故がおこった。本連載記事では、そうした苦難を乗り越えて、更に成長を続けるグローバル企業のチャレンジと彼らのとった戦略、並びにNTTコムグループの対応について紹介する。

急拡大する事業とセキュリティ事故の発生

この度紹介するのは、NTTコムグループのセキュリティビジネス子会社であるNTTコムセキュリティ社（NCS社）がインシデント対応から、マネージドセキュリティサービス（MSS）を含む総合リスクマネジメントサービスをグローバルに提供している事例である。

欧州某国を本拠地とする装飾品製造販売グループであるA社は買収により企業規模を拡大し、収益1兆円超、営業利益率20%に及ぶ大企業で、直接雇用の社員もグローバルで3万人規模となってきている。営業テリトリは欧州内のみならず、北南米、日本を含むアジア全域とグローバルであり、世界中に直販店のみで1,000を超えるショップを展開している。特に、ここ10年あまりでビジネスを急拡大してきた。ところが、2010年代に入り、ショップの店員が長期間に渡り販売代金を着服し、被害額が1億円近くに及ぶインシデントが発生した。犯行は店員の就業時間ではない時間帯で行われており、A社は入退室管理を厳格化するために、共連れ防止機能の付いた生体認証による入退室管理システムを導入し、社員管理と入出金管理の徹底化を図った。

買収による事業拡大に合わせ、当然ながらグループ入りした各ブランド会社のサプライチェーンの統合による効率化、ERPの統一による財務管理、管理会計の充実を順次進めてきている。多数のショップと3カ所に分散するデータセンターに配置されたITシステムとの接続はインターネットVPNにより実施している。全ショップにはVPN接続ルータとUTM（Unified Threat Management：統合脅威対策アプライアンス）を設置し、某通信事業者により管理されていた。しかしながら、あるショップの店員のPCにフィッシングメールが到達し、記載されたURL（Webサイト）をクリックしたところ、それは悪性のアプリケーション（マルウェア）が仕込まれたサイトであり、マルウェアが自動的にダウンロードされ感染した（ドライブ・バイ・ダウンロード攻撃）。その後バックドアが設置され、外からの攻撃者によるコントロールに従って、当該ショップからの通信路を経て、データセンターのシステムの脆弱性を利用して感染を広げ、そこに格納されている重要顧客のデータの一部が漏出するという重大インシデントが発生した（図1）。このインシデントの発見経緯は、本社IT部門が顧客情報システムのソフトウェアアップデートの際に、深夜帯で無人であるはずの地域のショップとの間で大量データの授受が行われていることを発見し、追跡調査により感染源を特定できたものである。悪性ウェブサイトに仕掛けられたマルウェアは、その時点ではアンチウイルスソフトが防御できないゼロディ型であると共に、疑似サイトも悪性サイトとして認識される以前であったことが、感染、活動並びに情報漏洩を許してしまったのである。

A社のチャレンジとそれを支えるNCS社の総合リスクマネジメントサービス

そこで、A社は包括的にサイバーセキュリティ対策状況を把握するために、NCS社へセキュリティ監査を依頼した。セキュリティポリシー面、サイバーセキュリティを管理す

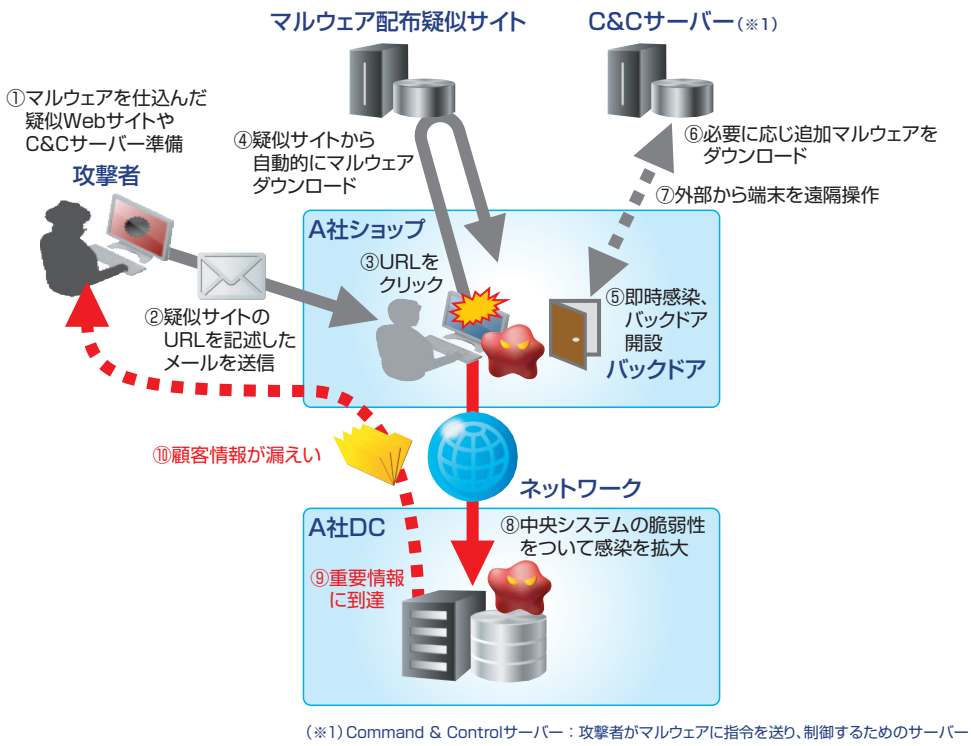

図１　ドライブ・バイ・ダウンロード攻撃によるＡ社のインシデント概要

る組織と責任体制面、社員訓練を含めた運用面、事業継続のための措置面、システムへのアクセス管理・認証面、データ及びアプリケーションのセキュリティ対策面、並びにネットワークとシステムのセキュリティ対策面で監査を実施した。その結果として、セキュリティガバナンス面等で多くの問題点についてCIO※1並びにセキュリティ管理者へレポートをしている。ところが、CIOはこのレポートを取締役会に報告せず放置し、さらに内部犯と疑われる顧客情報の漏洩という、更なるセキュリティインシデントが発生したために、これを契機にセキュリティ監査での指摘点を放置したことが問題となった。経営幹部はCIOとセキュリティ管理者を更迭し、2012年後半よりガバナンスやリスク管理から総合セキュリティ分野まで包含する総合プログラムを開始することとなったのである。

具体的なパートナーとして、GRC（ガバナンス、リスク及びコンプライアンス）監査を既に実施しているNCS社のグローバルに展開するGEM※2コンサルティングチームに白羽の矢があたり、多年に渡る総合契約を結んだ。プログラムは2つに分かれており、GRC面に特化してCISO※3によってリードされるプログラムと、CTO※4によってリードされる具体的なセキュリティ対策ソリューションの展開プログラムに分かれている。前者はグローバルなガバナンス拠点が西欧３カ国を中心にあるが、後者は、製造・流通並びにIT拠点が欧州、北米並びにアジアに展開されており、20カ所の流通拠点・オフィス、３つのデータセンター並びに1,000を超えるショップに渡る。

2013年のプログラムはGRC分野、セキュリティソリューション展開で数億円規模に達している。2013年後半から2014年にかけて、GRCの継続コンサルティング、ソリューション展開、MSS※5でさらに倍増を予定している。さらにソリューションの内容は、セキュリティ機器導入、Webアプリケーションの脆弱性診断、アプリケーションセキュリティ、認証及びアクセス管理、重要データセキュリティに及ぶ。

GRCコンサルティングでは、ICTシステムのライフサイクル全般での、企画／設計時点、開発／構築時点、運用フェーズ並びに何らかのシステムアップデート時点それぞれでの、リスクアセスメント、脆弱性診断や

マネージドセキュリティサービス 最前線

第5回 ー 実例ベースで考える ー

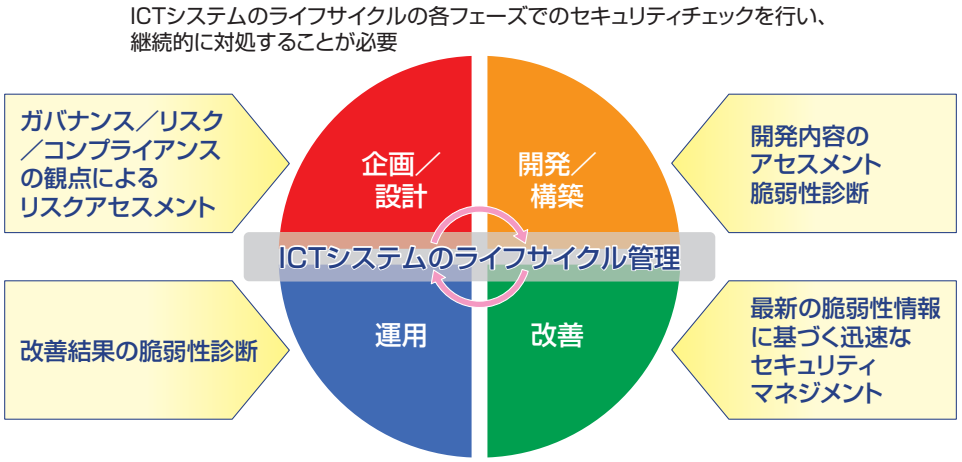

図2　ICTシステムのライフサイクル管理

セキュリティマネジメントについてのプロセスを構築することをサポートしている（図2）。

前述のように、各ショップにはUTMを導入し、某通信会社系MSSにより管理されていたが、NCS社はこれを引き継ぐと共に、データセンター側の顧客管理システム、ERPシステム及びサプライチェーン管理システム等のITシステムを含め、総合的にセキュリティ面からのモニタリングを実施している。総合的なログデータの相関分析はもとより、システムの脆弱性が露呈した時の緊急パッチ等の対策、攻撃者による遠隔操作にて発生する異常な通信の有無、システムの変更時のアセスメント等を総合的に実施することにより、リスクレベルを最小化している。

本事例において学ぶべきポイント

本事例で学ぶべき点は、①URLフィルタリングやアンチウイルス機能まで登載したUTMの設置にも関わらずゼロディ攻撃は成功する点、②マルウェア感染後重要データ漏洩の事実を早期に発見するのは非常に困難、③感染を極力最小化するとともに異常を早期に検知するにはグローバルなICTシステム全体を網羅的に管理することが重要、④そのためには膨大なデータを相関分析し異常を炙り出す仕組みと高度に訓練された分析者がキー、⑤内部犯の可能性をも排斥するリスク管理を常時実施することが重要、⑥ICTシステムの脆弱性を早期に発見・回避するライフサイクル管理が必要、という点である。NTTコムグループのセキュリティビジネスをグローバルに展開する子会社であるNCS社はグローバルに展開している強みから、セキュリティ監査から入り、GRCの総合コンサルティングを多年に渡り実施し、さらにセキュリティソリューションの構築を経て、MSSの継続的提供というフルサービスを実施している。

MSSでは、 NTT研究所の研究成果をも盛り込んだ自社独自開発のSIEM※6エンジンにより、セキュリティ対策機器のみでは検知不能な、あるいは誤検知となるような事象を自動分析している。さらに高度な分析能力を持つリスクアナリストが脅威レベルの判定・確認を実施している。サイバーセキュリティ脅威の変遷に熟知している分析者、自動分析機能並びに既知の攻撃を防御するセキュリティ機器の総合的な組み合わせによって、総合リスクマネジメントを実現しているのである。

※1 CIO：Chief Information Officer（最高情報責任者）
※2 GEM：Global Enterprise Methodology
※3 CISO：Chief Information Security Officer（最高情報セキュリティ責任者）
※4 CTO：Chief Technology Officer（最高技術責任者）
※5 MSS：Managed Security Service（マネジドセキュリティサービス）
※6 SIEM：Security Incident and Event Management（セキュリティイベント情報管理システム）

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