連載
マネージドセキュリティサービス最前線
― セキュリティ脅威の傾向と対策① ―

サイバー攻撃に備える

与沢 和紀
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

いまやサイバー攻撃や不正アクセスは、いつどの企業がターゲットになってもおかしくない。
セキュリティ対策の焦点は、標的型攻撃やゼロディ攻撃にどう備えていくかにシフトしている。
これは情報セキュリティのプロが見た、現場からのレポートである。
＜企業には2つの種類がある。既にハッキングされた企業とこれからハッキングされる企業だ(FBI長官ロバート・ミュラー)＞

連載にあたって

情報セキュリティに関する事件が頻繁に報道されている。通信販売のWebサイトに不正ログインが行われ、クレジットカード情報が流出する。企業のサイトが改ざんされ、閲覧した利用者がウイルスに感染してしまう。海外ではサイバー攻撃によりATMなど社会インフラが停止する事態まで起きている。

本連載※では、情報セキュリティのプロであるわれわれが対応した事例や、話題になった事件を取り上げ、企業がどのようなポイントを踏まえ備えておくべきか考える場としたい。

※編集部注：隔月掲載予定。

最近のインシデント事例に見る、企業が直面する脅威

最近われわれが関わったセキュリティインシデントを紹介しよう。

まずは、全国に店舗を展開し、かつインターネット上での通信販売も積極的に展開するA社のケースである（図1）。

A社はネット販売を拡大するため、データセンターを移設し数百台に上るサーバーの移行を進めていた。その過程で一部のサーバーCPU使用率が異常値を示し、ウイルスに感染しているのではないかとの一報が当社に入った。

当社のエンジニアがただちに解析を進め、その結果、外部からシステムを不正に操作するバックドアや攻撃ツールが多数のサーバーにしかけられていたことが判明した。侵入者はシステムの大部分を掌握し、頻繁にアクセスしていたのである。

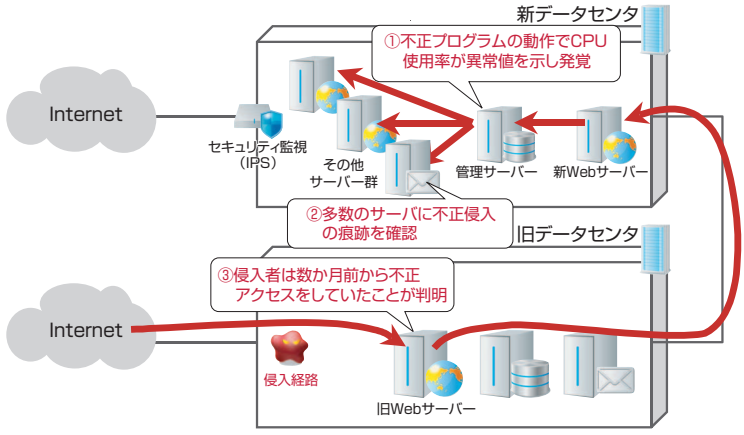

図1　サーバーの脆弱性を突いた不正侵入

さらに複雑に入り組んだ侵入経路を紐解いていくと、侵入者は数か月前、旧データセンターに設置していたWebサーバーの脆弱性を利用して潜り込んだことがわかった。

しかし発覚時までのログは改ざん・消去されており、影響範囲を完全に明らかにすることはできなかった。

続いて、情報サービス関連企業であるB社のケースである（図2）。

B社が見舞われたのは不正なプログラム（マルウェア）による機密情報の流出であった。サーバーから異常値を検出したため調査を行った結果、マルウェアの侵入と情報が漏えいした痕跡のあることが判明した。

B社は先端技術を利用したサービスを政府機関にも提供しているため、その技術情報や取引先に関する情報は貴重な価値を持つものであった。

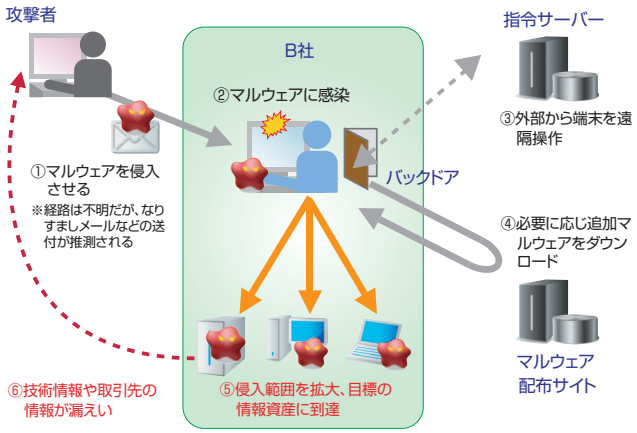

図２　情報サービス関連企業への攻撃

侵入手法については推定だが従業員になりすましメールを送付するなどの手法でマルウェアを社内に潜り込ませたのではないかと考えられる。

事件を機にB社では、従来の対策に加え、当社が提供する、未知のマルウェアにも対処できる新型のマネージドセキュリティサービスの導入を進め、対策の強化を進めている。

高度な知識と強い動機を有し執拗な攻撃者たち

これらの事例からわかるのは、まず攻撃者が高度な知識を有し、手法も巧妙であることだ。A社ではログの痕跡は消され、人員もセキュリティの専門知識も限られる情報システム部門のメンバーだけで事象を把握することは困難であった。

また攻撃者は、何らかの強い動機を持った上で行っている（図３）。読者にはサイバー攻撃を、一部のマニアが自らのスキルを誇示するためにウイルスをインターネット上にばらまくといったイメージで捉えている方もいるかもしれない。

実際、過去はそうだったかもしれない。しかし現在顕著なのは経済的な動機に支えられた攻撃だ。攻撃者は標的から金銭につながる情報を盗み取り、ブラックマーケットを通じて換金したり、何らかの取引を有利に進めたりしているのである。

また最近は社会的、政治的な動機による攻撃も増えている。国際的なハッカー集団が自らの主張を訴えるために攻撃を行うことも珍しくない。

動機	経済的な動機による攻撃	社会・政治的な動機による攻撃	国家が関与する攻撃
攻撃者像	ブラックマーケットで金儲けをしているハッカー集団	特定の主義・主張を軸に集まった国際的なハッカー集団	軍や諜報機関など何らかの国家的な組織
目的	金銭に結び付く情報の収集	社会を騒がせて注目を引き、自らの主張をアピール	国家機密に関する情報収集や社会インフラの停止
影響	ビジネスの停止、ブランドの失墜、ユーザーへの損害賠償	ビジネスの停止、ブランドの失墜	外交・軍事上の不利益 経済活動の停止と損害

図３　サイバー攻撃の動機

さらに背後に国家の存在が疑われる攻撃もしばしば行われている。韓国で大規模なサイバー攻撃があったことは記憶に新しい。B社の事例も、同社が政府や防衛関連の情報も扱う企業であることを考えるとこうした攻撃の可能性は否定できない。

重要となる多層型防御と相関分析

最近の攻撃者たちは対象をよく研究し、持続的にアタックを続ける、標的型攻撃を繰り広げている。また脆弱性が知られ対策が流布される前のタイミングを狙うゼロディ攻撃もしばしば起こる。

これらはFW（ファイアウォール）などを軸に脅威に備える従来型の入口対策だけでは対処しきれない。

重要となる考え方に多層防御がある。特定の手段に依存せず、FWやIDS/IPS（不正侵入検知・防御装置）、ウイルス対策、ログ監視など個々の対策を組み合わせて脅威の緩和、早期検出をはかることである。

また新たなモデルとして、Proxyサーバーやデータベースなどのログ情報とセキュリティ機器のログ情報を連続的に分析し、悪意のある挙動をいちはやく検出するセキュリティ相関分析も注目を集めている。

次回以降、企業が直面した脅威にスポットを当てるとともに、セキュリティ対策の具体像についても紹介していきたい。

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