JPCERT CC®

経営者が知っておくべきセキュリティリスクと対応について

一般社団法人 JPCERT コーディネーションセンター

2013 年 04 月 09 日

本報告書は、Delta Risk Limited Liability Company が作成し、JPCERT/CC が翻訳、一部修正したものです。

目次

1.1 プロローグ

深夜、午前 2 時。電話が鳴り響いた。あなたは、妻や子供たちを起こさぬように気遣って受話器をとる。電話は、最高情報セキュリティ責任者（CISO）からで、彼は、最高情報責任者（CIO）と会議中だった。理由は、エンジニアリング部門のネットワークに接続されたプリントサーバーを介して大量のデータが盗まれたという情報を、情報セキュリティオペレーションセンターが受け取ったことを知らせるためである。CISO によると、会社が過去 10 年にわたって取り組んできた技術のほぼすべてに関する計画書や設計、販売用資料が社内中のネットワークから盗まれたと考えられる。最新の技術も漏洩し、研究開発部門も同じ記憶装置を使用していたため、同部門が保存したデータもすべて漏洩した可能性がある。何者の仕業かは誰にもわからないが、事故に対応した社員は一時ディレクトリに 500 個以上の暗号化圧縮ファイルを確認している。ファイルはすべて標準的な CD-ROM の容量ほどの大きさで、ネットワークを介して転送するために事前に一時ディレクトリに用意されていたのだ。アウトソース先のセキュリティオペレーションセンターは、カナダのサーバーへファイルを大量転送している最中に外向きのインターネット回線が危うく溢れそうになったことで、情報の窃盗行為を発見した。接続内容を監視する準備に手間取り、ようやくそれに着手した時、それに気づいた攻撃者は活動を中止したが、残されたファイルはすでにほんのわずかだった。

最高経営責任者（CEO）であるあなたは、この事故に対処しなければならない。どのようにして起きたのか。攻撃してきたのは誰なのか。なぜもっと早い段階で発見し阻止できなかったのか。実際にどの位の量のデータが奪われたのか。正確なところ、我々は何を失ったのか。

CISO の説明はこうだ。「このような先進的で執拗な脅威攻撃は APT と呼ばれ、非常に巧妙なソーシャルエンジニアリング手法によって偽装されているため、経営陣が悪意のあるコードを含む電子メールを受け取ったとしても、何の疑問も抱くことはないだろう。こうした攻撃は『標的型攻撃』と呼ばれている。電子メールに添付されたファイルを開いた際、またはリンク先をクリックした際に、経営陣のコンピューターにソフトウエアがダウンロードされる。そのソフトウエアがコンピューターシステムの様々な脆弱性を利用して攻撃を行う。多くの場合、攻撃により内部で使われている認証情報が奪われ、遠隔管理ツールによって操作される。こうした攻撃者はしばしば、企業が所有するセンシティブな（取り扱いに注意を要する）、競争優位性のある知的財産、事業やプロジェクトに関する経理情報、営業情報、および企業の合併・買収に係わる文書を狙って収集する。今回のケースでは、攻撃者は当社が開発している内容を正確に把握しており、当社が開発した技術に関

する極めて限定的な情報をシステムから収集したのだ。しかも攻撃者は当社の利用者全員の認証情報も取得している。彼らは再び攻撃してくると思われるが、その時には攻撃に気付くことはできないだろう。現在、セキュリティベンダーと共同で作業を行っているが、ベンダーも解決策を見出せないでいる。」

「取締役会には何と報告すればいいのだ。」「顧客にはどのように説明しよう。」

・・・・・・・・・・・・・・・・

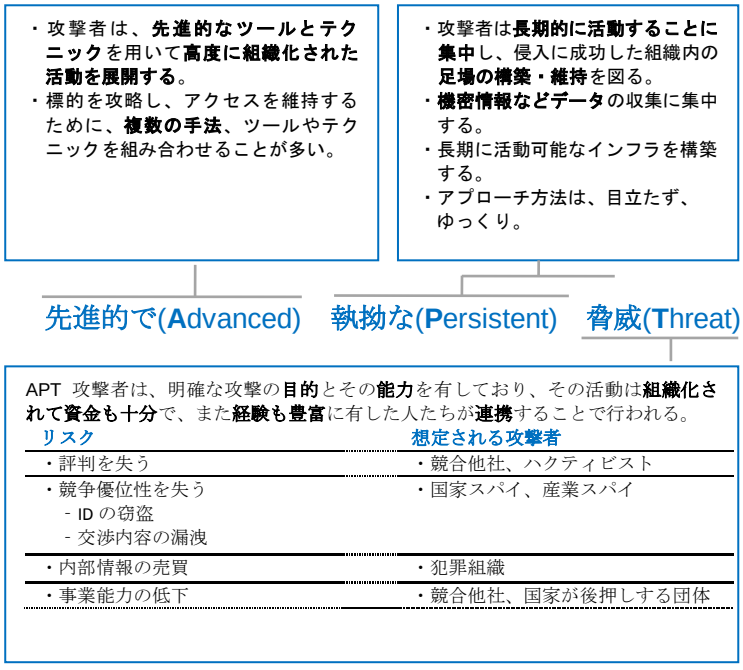
APT の定義

先進的(Advanced)な、執拗な (Persistent)、脅威(Threat)の用語を以下のように定義する。

先進的：攻撃者は目的達成のために必要な最小限のツールしか使用しない。そのため、一連のイベント自体が「先進的」と見なされる。

執拗な：攻撃者は ネットワーク上に長期にわたって居座り続ける。例えば、繰り返しアクセスを図り、複数年にわたってアクセスを維持することもある。

脅威： 攻撃者は長期的な 活動を実施するために 技術だけではなくリソースが必要である。そのため、攻撃者には国家が支援する能力者や先進的なサイバー犯罪者が含まれる場合がある。



1.2 CEO、経営者としての責任、および APT

「先進的で執拗な脅威」は APT（Advanced Persistent Threat）、あるいは「標的型攻撃」としても知られ、近年様々な分野で活動が広がりつつある。この用語は、サイバースペースを利用して、金銭や知的財産、その他企業の競争上の強みとなる情報を入手し、将来にわたり容易に攻撃を続けるための足場をネットワーク内に構築する、一連の侵入行為を表すのに使われる。本報告書は、CEO および経営幹部に APT がもたらすリスクの概要を説明し、経営幹部がとるべき適切な対応について示唆することを目的としている。

CEO および経営幹部は次のことを理解しておかなければならない。経営者は、会社の知的財産およびその他の企業秘密を最大限の注意をもって守らなければならない。米国では、CEO は損失や損失の隠蔽について責任を問われ、また経営する会社の長期的な存続性を確保するための、株主に対する忠実義務の怠慢についても責任を問われることがある。
CEO および経営幹部は財産管理の責任を果たさなければならない。これは、富を生み出すだけでなく、株主、従業員および国家の利益のために会社の長期的存続性を確保できるように会社を守る責任があるということだ。CEO が責任を果たせない場合、次世代の人々や国家の将来が、CEO および会社が受けた損失に苦しむことになる。

その影響は重大である。

サイバー攻撃によって米国経済が受ける損失は、推定年間 80 億ドルであり、また毎年 900 万人近い米国居住者が「なりすまし犯罪」の被害に遭っている[1]。

米ポネモン研究所（Ponemon Institute）によると、データ侵害事件への対応に要するコストの平均は、2009 年に 670 万ドルを上回り、2010 年には 720 万ドルに増大している。2010 年の調査結果によると、最も低額なケースでは 78 万ドルで、最も高額なケースでは 3,500 万ドルを超える。漏洩したデータ 1 件当たりの企業負担は平均 214 ドルとなっている[2]。
次の図は、米ポネモン研究所が調査した 2009 年、2010 年のデータ侵害の対処費用を元に作図したものである。

[1] 2011 年 4 月にロードアイランド大学で開催された CYBER SECURITY SYMPOSIUM　議事録 http://cybersecurity2012.uri.edu/proceedings2011.pdf
[2] ポネモン研究所およびシマンテックによる 2010 年年次調査：米国におけるデータ侵害による損害額（U.S. Cost of a Data Breach）

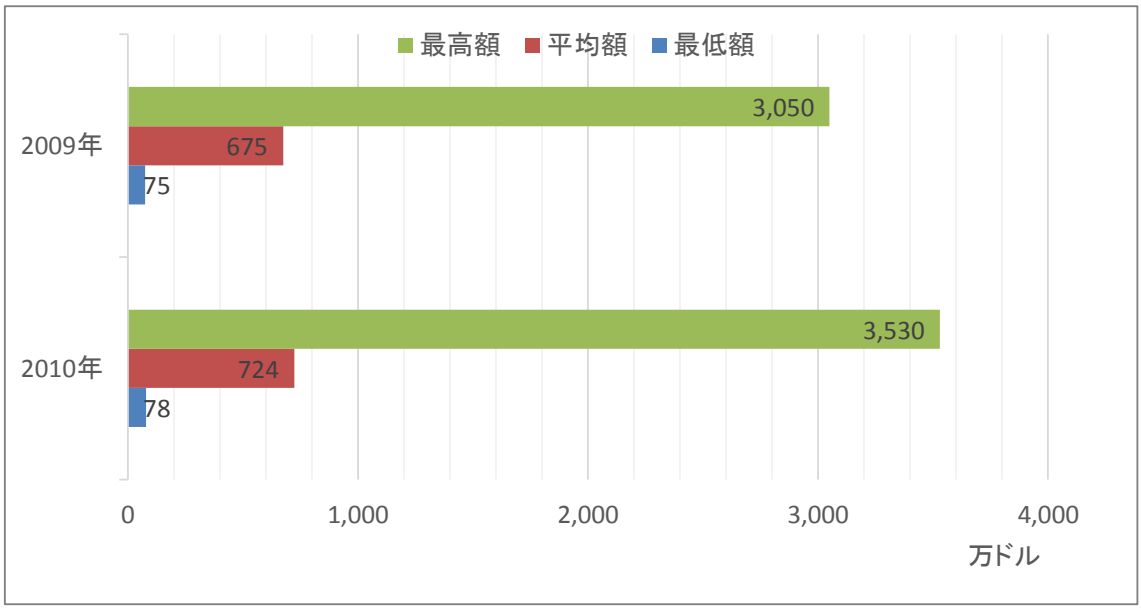


図 1：データ侵害事件への対応に要したコスト

昨今、グーグル（Google）、アマゾン（Amazon）、シティバンク（Citibank）、 JP モルガン（JPMorgan）、ロッキード・マーティン（Lockheed Martin）といった巨大企業における大規模なサイバーセキュリティ侵害が大々的に報道されている。ノーテル（Nortel）が長年にわたって侵害されていたことが情報公開され、同社の企業価値に大きな影響を及ぼした。また、同社首脳部は事態の対処の仕方に対して刑事責任を問われる可能性がある。今日、CEO および経営幹部は、IT セキュリティが重大なリスクの要因となっており、財務業績と同様に効果的な取り組みが必要であるとの認識を高めている。IT サービスや IT セキュリティサービスのアウトソース化により、こうしたリスクの分析がさらに難しくなっている。CEO および経営幹部は、CIO や他の IT 責任者を戦略計画およびリスクマネジメントに組み入れる必要がある。

企業を守る闘いにおいて、CIO がすべての機会や変化に遅れずに対応することがかつてないほどの負担になっていることが問題となっている。最新のツールを購入しただけで効果的なセキュリティ対策が実現できるわけではない。これは IT 責任者が対応する努力を怠っているということではない。むしろ、企業における情報や技術の利用法が 5 年前に比べ格段に複雑になり、モバイル化が進み、アウトソーシングの度合いが高まっているということなのだ[3]。

[3] Mark Boltz, “Top Three Security Concerns Every CEO Should Know（すべての CEO が知っておくべきセキュリティに関する上位 3 つの懸念）”, Chief Executive Magazine, 2011 年 8 月 16 日号

今日、IT セキュリティの全社的な取組をどのように進めるかについて、検討課題や優先事項を決めるのは、CEO、取締役会、および経営幹部の責務である。CEO 直属の経営陣は、こうした優先事項の実施や作業の監督において責任を負わなければならない。こうした取組を行わないことによる財務的影響は、もたらされる影響のうちのほんの一部でしかない。サイバー侵害は多額の財務損失のみならず、ビジネス、業績、顧客の信頼に影響を与えかねない信用喪失をももたらすだろう。その上、情報開示を怠った場合は、CEO だけでなく取締役や上級社員に対しても個人としての責任が問われることもある。

1.3 APT リスクに対する経営陣の責任に関する事例

ウォール・ストリート・ジャーナル（Wall Street Journal）の 2012 年 2 月 14 日付けの記事によると、攻撃者は 10 年以上前にノーテル（Nortel）のコンピュータネットワークに侵入し、技術文書、研究開発レポート、事業計画、従業員の電子メールなどの文書を長年にわたりダウンロードしていた。ノーテルは 2011 年に、所有する特許資産をアップル（Apple）、マイクロソフト（Microsoft）、グーグル（Google）などの企業に売却した。ノーテルの経営陣は全体の期間を通じて、特許資産が侵害され、盗まれた可能性があることを把握していた。

これは過失および詐欺行為とみなされるのであろうか。恐らくみなされるであろう。この件について、CEO および経営幹部は綿密な取り調べを受けており、責任があると認定される可能性がある。処罰は金銭的賠償にとどまらず、民事および刑事訴訟にも及びかねない。CEO は知的財産の喪失に関してその売却前に開示を行わなかったことにより、刑務所に収監される可能性もある。また、こうした事実を把握していたにもかかわらず開示しなかったこと、あるいは単に知的財産保護のための措置をとらなかったことに対し、取締役および経営陣にも責任が及ぶことになるだろう。

最高経営責任者（CEO）Frank Dunn、最高財務責任者（CFO）Douglas Beatty および経理責任者 Michael Gollogly は、既知の侵害を開示しなかったことは会計基準違反には当たらないと主張している。Dunn、Beatty および Gollogly の 3 氏は各々、公開市場に影響を及ぼす詐欺に関する 2 件の訴因および財務書類の改ざんに関する 1 件の訴因で起訴されている。刑法の下では、詐欺に対する有罪判決を受けた場合、最高で 14 年間、刑務所に服役することになる[4]。

[4] James Bagnall, “Were Senior Executives Scapegoats for Nortel’s Demise（上級幹部はノーテル瓦解のスケープゴートだったのか）”, Financial Post, 2012 年 1 月 14 日号,
http://business.financialpost.com/2012/01/14/were-senior-executives-scapegoats-for-nortels-demise/

■関連記事からの抜粋

シールズ氏とコンピュータセキュリティ管理担当者数名はまもなく、ハッカーは前 CEO を含め経営幹部 7 名のパスワードを取得していたらしいことを突き止めた。同氏らは、ハッカーは少なくとも 2000 年には、中国を拠点とするインターネットアドレスからノーテルのネットワークに侵入していたと特定した。

シールズ氏は「ノーテルのネットワーク内にはほとんど障壁がなかったため、ハッカーは社内システムにほぼ完全にアクセスできた。いったんネットワーク内部に入ってしまえば、あとはスカスカの状態だった。」と語る。

シールズ氏はその約 6 ヶ月後に、ハッカーが依然としてシステムに存在する兆候が見られると述べた。ネットワーク上のコンピューター数台がほぼ毎月、パスワードハッキングの時に関与していた上海のインターネットアドレスの 1 つに短時間に少量ではあるが一連のデータを送っていた。セキュリティ専門家によると、あるコンピューターが外部ホストに極めて短時間接触するなどの非日常的な通信が観測された時は、スパイウェアが存在することを示すことも多いという。

ノーテルの捜査に詳しい人物は「スパイウェアは極めて隠密裏に活動する。こうした通信を行うコンピューター内には何かが仕込まれているのだが、発見するのは非常に困難だ。」と述べる。

現代の CEO は、こうした APT がもたらす、極めて重大なリスクについて明確に理解し、脅威を軽減するための戦略の策定と実施に積極的に取り組む必要がある。本報告書では、CEO および主要な経営幹部が受ける脅威、彼らが果たすべき役割・責任について概要を説明し、社内の APT 行為を発見し軽減するための 10 のステップを紹介する。

1.4 サイバースペースはリスクが高まっていると理解する

サイバースペースはますます危険な場所となってきている。サイバースペースは 1970 年代に生み出され、1980 年代に発展し、1990 年代に商業化された 21 世紀の生活を大きく特徴づける存在であり、インターネットに接続可能な機器を日常的に利用する世界の多くの人々に大きな恩恵をもたらしている。現在では、エネルギー網のような国家的・世界的インフラから、スマートフォン、ラップトップ、ゲーム機、そして単純な電気器具といった消費者製品まで、あらゆるものがインターネットを介して結びついている。こうした恩恵とそれに伴う IT 管理の複雑性、そして接続性およびセンシティブデータに係わるリスク

はすべて、その本質的な特性から生じている。情報への欲求の高まり、膨大な数のデバイスやそれを機能させるための複雑な連携の仕組み、そしてユーザーからの使いやすさを求める声、これらがすべてインターネットの開放性を強く求め、それが今では安全性を脅かしている。新たに接続されたデバイス、不慣れな新規ユーザー、新デバイス用に開発された新しいプロトコル、および新しいアプリケーションがそれぞれ、ネットワーク防御の視点で「攻撃対象領域」と呼ばれるものを急激に広げている。攻撃対象領域とは、機能やサービス、ソフトウエア等、外界に面して攻撃に晒される可能性のある部位であり、攻撃者はそれらを介して内在する脆弱性を悪用して、狙ったネットワーク内にいる間に標的の侵害を極めて高い確率で成功させ、所定の目的を遂行しようとする。

サイバースペースのこうした本質的な特性により、様々なレベルのリスクが発生する。インターネットの急速な普及は、防御する側に対して重大な困難をもたらす一方で、攻撃者には新たな優位性が与えられている。

初期のインターネットは、大規模なコンピューター（メインフレーム）同士をオープンなプロトコルにより接続するもので、こうしたプロトコルはコンピューターを結んで情報を交換することのみを目的としていた。セキュリティへの配慮は必要なかった。接続可能なコンピューター資源を利用できたのは一部の政府機関や研究員に限られ、コンピューター間で交換されるデータは主として試験的なものであった。

1980 年代半ばから後半にかけて、より小型のコンピューター（デスクトップコンピューター）がサーバー（非メインフレーム）に接続されるようになる。このようなネットワーキング・モデルは「クライアント - サーバー型」と呼ばれた。ハッカーが出現し始めたことから、セキュリティが若干重用視されるようになった。当時のハッキングはネットワークアーキテクチャを把握する手段であったが、そのような初期の攻撃が注目されるにつれて、急速に悪意のあるものに変化していった。

1990 年代半ばから後半にかけては、大規模なデータセンターが重要な存在となってきた。データセンターは情報の保管と共に、世界のより広い地域からのアクセスを可能にすることが求められた。これらは急激に成長したため、設備の設置面積を縮小する手段を探す必要が出てきた。その結果として仮想化技術が生まれ、インターネットとコンピューター利用における新しい、重要な技術世代が始まる。仮想化により、設備やサーバーに対する要求は 10 分の 1 近くまで縮小し、データセンターはより大容量のストレージ、より高い処理能力を提供しながらコストダウンを実現している。

現在、企業の「クラウド（コンピューティング）」へのアウトソース化が驚くべきペースで進んでいる [5]。運用費用のより大幅な削減、IT インフラへの設備投資の縮小、そして使い勝手の良さが動機となって、クラウドは多くの中小企業および大企業にとって最適な IT プロバイダーとなりつつある。クラウドは、データセンターのサーバーやアプリケーションの「レンタル」である。プロバイダーは、あらゆる応用分野からの要求に応え、ハードウェア上の仮想的なスペースやアプリケーションを地理的な制約を越えて提供してくれる。利用者は、必要なものを必要なときに借りることができるのである。販売、事務処理、財務、または製造に必要なアプリケーションはほぼすべて利用可能である。クラウドプロバイダーによって認証されたユーザーは、Microsoft Word、SAS、セールスフォース・ドッ Salesforce.com などのアプリケーションをオンライン上で利用することができる。企業は、世界中に配置された巨大なデータセンターで動作するサービスを使って活動を持続することが可能となるのである。このような多様性と、冗長化された広帯域通信網によって、クラウドプロバイダーは事実上稼働率 100%の高度な可用性を保証し、利用者はサーバーやインフラへの設備投資の配分を縮小できる。また、熟練した IT スタッフが要らなくなり、クラウドからレンタルできるアプリケーションを購入する必要もなくなるため、運用費用を削減することができる。

こうした革新は、携帯型機器やソーシャルメディアをはじめとする消費者重視のアプリケーションへの飽くなき渇望と相まって、計り知れない恩恵を生み出しているが、同時に極めて大きな未知のリスクももたらしている。我々のサイバースペースへの依存は、他にほぼ例を見ないものであり（食糧、水、住居を除く）、さらなる依存・相互接続性への欲求は、現代の他の産業分野におけるレベルを上回っている。実に、約 1,780 兆ドルもの資金が毎日インターネットを通じてやり取りされているのだ。クレジットカード決済、株式の売買、営利企業の取引の多くがインターネットを通じて行われている。

あなたの会社は IT なくして存続することができるだろうか。会社の極めて重要な資産がサイバースペースに置かれ、そこで利用されているのである。そこには対応できていないリスクが存在することもわかっている。デルタリスク社の調査においては、複数の CISO および CIO に対して、コンピューター（サーバー、デスクトップ、ラップトップ）、インフラデバイス（ルーター、ファイアウォール、スイッチなど）、およびモバイル機器などの資産が現在の環境下でどこにあるかを 100%確実に答えられるか質問した。ほとんどの場合、答えられるのは少数だ（せいぜい 5%程度）。次に、社内の重要なデータがどこにあるか把握しているかと質問した。実に奇妙なことだが、企業はどの情報が企業の事業およ

[5] Christian Harris, “Cloud Adoption Trends 2012（2012 年クラウド採用動向）”, BCW IT Leadership,2012 年 6 月 12 日, http://www.businesscomputingworld.co.uk/cloud-adoption-trends-2012-infographic/

び存続性のために重要であるかは把握しているのに、実際にこうした情報が IT インフラ内のどこに存在するかというインベントリーを作成していないし、そもそも把握もしていない。資産管理ができていなければ、そのような資産を効果的に守ることは不可能である。

CEO、取締役会および経営陣は現在、今までに経験したことのない難しい問題に直面している。組織を構成する様々な要素と従業員を結びつけるシステムが複雑化し、開放性や相互接続性が求められ、システム間の連携が急増することで、ヒューマンエラーが急速に増えつつある。システムの複雑性がヒューマンエラーと相まって、明確な 意図を持った攻撃者に多大な機会を与えている。

これが攻撃者のもつ競争優位性であり、彼らはこれを悪用するだろうし、実際に悪用してもいる。

1.5 APT（Advanced Persistent Threat）について理解する

APT は通常、特定の組織体を執拗かつ効果的に攻撃する能力と意思の両方を兼ね備えた、外国政府などの集団を表す。この用語は一般に、サイバー脅威、特にインターネットを使ったスパイ行為を指すが、他の伝統的なスパイ行為や攻撃による脅威にも同様に使われる。その他に認識されている攻撃手段としては、感染したメディア、サプライチェーンの侵害、ソーシャルエンジニアリングなどが挙げられる。個々のハッカーなどの個人は、たとえ特定の標的にアクセスまたは攻撃しようと意図しても、先進的かつ執拗に活動できる資源を持つことはほとんどないため、通常 APT とは呼ばれない。

特定の、あるいは一連のインシデントの背後にいる実行者に対して、世界的に行われるすべての APT による攻撃活動を総称して「the APT」と単数扱いで呼ぶこともある。APT による攻撃には、会社組織や非政府組織に直接かかわる集団や、国家が後押しするサイバースパイなどを含めることもある。

今日、データ奪取を目的とするスパイ行為の中で最も広く活発に利用されている手法は、サイバースペースを介したものである。米前国家情報長官かつ米国家安全保証局（NSA）前長官は、サイバースパイ行為は「史上最大の富の移転」を引き起こしていると述べている[6]。現在、サイバースペースは人々が情報を創出し、操作し、保存し、交換する共同創作作業の場となっている。攻撃者は、単に公開メディアを探すだけでも膨大な量のデータを収集できるが、それに加え、求める情報を所有している人物を正確に見つけるために、

[6] Booz Allen Hamilton の副会長、Michael McConnell の 2012 年 6 月 4 日ウェストポイント上級会議（West Point Senior Conference）での発言。

公開のメディア情報から自動的にデータを収集し、可視化ツールを使って素早く相互の関連付けを行う手法も有している。その後、こうした攻撃者は正確に標的を定めてサイバー攻撃を行う。ほとんどの企業は攻撃を受けたことさえ気づかないだろう。CIO が管理する IT システムが複雑化することより、管理作業においてヒューマンエラーが起きる可能性は非常に高くなっており、それが損失へと結びつく可能性も同様に高まっている。実際のところ、APT の被害にあった企業に対応している著名なインシデント対応組織は、扱ったケースの 94%において、当該企業は侵害を受けたことを、他者（一般には政府、警察、他の被害者など）から連絡を受けるまで知らなかったと述べている。また、同インシデント対応組織の報告によれば、最初にコンピューターの侵害が起きてから検知されるまでに平均で 416 日間を要している。普通に考えれば、攻撃者が目当てとする知的財産について、標的を定め、アクセス権限を取得し、場所を突きとめ、持ち去るには十分すぎる期間である[7]。

1.6 APT による攻撃を理解する

APT による攻撃は様々な形態をとることができる。従来、関係者を通じて情報を入手することに頼っていたスパイ組織・犯罪組織は、今やインターネットに接続されたコンピューターを利用することで遙かに優れた成果をあげるようになっている。従来手法による攻撃の例としては、競合他社（産業スパイ）、詐欺集団（犯罪行為）によるもののほかに、伝統的な国家的スパイ行為などが挙げられ、これらは公開情報と人を介した情報入手という形をとってきた。しかし、現代のサイバースパイは、表だった動きはほとんどせずに、ほぼ検知されるリスクがない状態で、長期間に渡ってアクセスを持続しながら情報を収集する能力を有している。このような攻撃の例を以下に挙げる。

競合他社：欧州のマルチメディア技術の企業（企業価値：160 億ドル）は 2006 年に、高解像度（HD）デジタル符号器／デジタル復号器（コーデック）に巨額の投資をした。同社は HD をマルチメディアの製造、動向、販売において今後主流になると位置づけた。同社は HD の使用の促進を図り、新製品の推進のためにどの企業もするように、以前に同社のコーデックを機器に組み入れてくれた革新的な大企業と連携した。こうした機器にはテレビ、セットトップボックス、ケーブル機器、映画の大型デジタル映像を製作会社から配給会社へ転送する機器などがある。同社は国際電気通信連合（ITU）において、HD コーデックとブルーレイ（同分野での伸びてきている主要な強力なライバル）との間の選択を議決することになっていた理事会の議席を 3 席確保し

[7] David DeWalt, “Former McAfee CEO, David DeWalt, Joins Mandiant’s Board and Talks Targeted Attacks（マカフィーの前 CEO、David DeWalt 氏がマンディアント(Mandiant)の取締役に就任。標的型攻撃について語る）”, Mandiant, Blog, 2012 年 5 月 8 日

た。HD 側企業とブルーレイ側企業の間の闘いが拡大するにつれて、サイバースペースが急速に競争のツールとなってきた。160 億ドルの価値のある欧州のマルチメディア企業は 2 年足らずの間にその知的財産の大半を奪われ、最高技術責任者（CTO）、最高情報責任者（CIO）および知的財産担当副社長は（現実社会およびサイバー上で）生命の危機にさらされ、知的財産担当副社長は 1 年半の間に 3 回転居した。そして 3 年間に、同社の株価と企業価値は 90%近くを失った。現在、同社はブランドを変更し、限定的な分野における技術開発に焦点を絞っている。同社の現在の価値は、たったの 1 億 6000 万ドルである。[2] 大量の知的財産が、攻撃対象に標的を定めた、先進的かつ執拗なサイバー攻撃によって持ち去られたのである。サイバースペースと現実社会の両面から攻撃を受けたことで、同社はもう少しで破産するところであった。

詐欺集団：ロシアビジネスネットワーク（RBN）は多角的なサイバー犯罪組織で、転売目的の個人情報窃盗を専門にしている。また、Storm Worm など、高性能のツールを開発元であるとも言われている。Storm は、ウェブを介した大量窃盗の可能性を初めて実証したもののうちの一つである。数千件もの大量の電子メールを短時間に送信し、その後は息をひそめる。その自動化された簡便な手法は、大量のユーザー侵害の機会が将来もたらされる可能性を示唆している。

ベリサイン（Verisign）社はかって RBN を「悪党中の悪党」と形容したことがある。RBN はウェブホスティングサービスやインターネットアクセスをあらゆる種類の犯罪組織や非合法な活動に提供しており、最大で年間 1 億 5,000 万ドルもの売上を得ている [8]。こうした活動に対して積極的に反対の立場をとる企業のネットワークは時として、RBN のネットワークから発せられる DoS 攻撃（サービス妨害攻撃）の標的にされる。RBN はそのサービスを広範な犯罪活動に販売していることで知られていたが、その追跡は困難であった。RBN は登記された会社組織ではなく、そのドメイン名の登録住所は明かされていない。主催者はニックネームでのみ知られている。RBN は宣伝を行わず、追跡不可能な電子取引でのみビジネスを行っている。

米国銀行協会（ABA）による預金詐欺に関する調査 2011 年版（2011 ABA Deposit Account Fraud Survey）は、小切手支払いや電子決済の詐欺行為による損害、およびこうした損害の削減に向けて金融機関がとった行為について、基本情報をまとめている。調査は預金口座に対する主要な脅威、現在および今後予想される詐欺による損害、およびその他の詐欺関連のトピックを、銀行業界全体の動向と銀行の資産規模別の両

[8] The Economist:A walk on the dark side, http://www.economist.com/node/9723768?story_id=9723768

面から調査している。業界全体の 2010 年の小切手関連の損害額は 8 億 9,300 万ドルと推定され、2008 年の 10 億 2400 万ドル（推定）よりやや減少している。詐欺の件数も低下している。 業界全体のデビットカード詐欺（POS サイン、POS PIN コード、および ATM 取引の合計）による損失は 2010 年に 9 億 5,500 万ドル（推定）に達しており、2008 年の 7 億 8,800 万ドルから増加している。10 行中 7 行以上（73%）が 2010 年に小切手詐欺による損害を受けたと報告している。また、10 行中 9 行以上（96%）が 2010 年にデビットカード詐欺による損失があったとしている[9]。

CEO および経営陣に向けた APT による攻撃に関する報告に、ABA のレポートを引用したのには理由がある。企業経営には金銭の取り扱いが伴う。口座の乗っ取りにより企業が被る損失額は、平均で約 150 万ドルとも言われている。口座乗っ取りの次にやってくるのは、密かでしかし執拗な、より先進的な攻撃方法である。商店に置かれた POS 端末は遠隔の仮想マシンに接続しているかもしれない。取引の処理はそこで行われるが、同じコンピューター上では他の様々な処理が行われているのだ。そしてそのすべてがインターネットに接続している。これまで金銭の異動には、マネーミュールやマネーロンダリングと呼ばれる手法が使われてきたが、これらは、物理的な危険にさらされることのない、サイバー手段を介した方法へと急速に移行しつつある。

スパイ行為：スパイ行為は、長い間 APT による攻撃を実行した者の主たる動機と考えられてきており、軍事秘密・企業秘密の取得において、船舶・航空機のメーカーや企業に人を送り込んで物理的に危険にさらすより、サイバー手段を利用する方がはるかに容易であることが常識化しつつある。

[9] ABA　Deposit Account Fraud Survey, 2011（米国銀行協会［ABA］預金口座詐欺調査 2011 年），
http://www.aba.com/products/Surveys/Pages/2011DepositAccount.aspx

■報告書からの抜粋[10]

経済スパイが一企業に与えた損害

経済スパイや企業秘密の窃取事件について、個々の企業に与えた損害に関する具体的なデータも記録されている。一例を挙げると、バルスパー（Valspar Corporation）の従業員が、塗料に関する2,000万ドル相当の特許情報を不法にダウンロードしたと報道された。理由は、中国での転職先に持参するためだった。この窃盗額は、当該従業員が逮捕された2009年度のバルスパーの利益の8分の1にあたる。

1.7 CEO および経営陣が把握しておくべきこと

まず、これまで行われてきたセキュリティ対策は役に立たないと認識すべきである。2004年頃より以前には、国家的スパイ・企業スパイのサイバー活動の規模については、ほとんど知られていなかった。ファイアウォールとウイルス対策ソフトを導入し、オペレーティングシステムへのパッチを欠かさなければ十分なセキュリティが確保され、こうした対策を実施していれば、ネットワークは安全であると信じられていた。ネットワークを守る手法は境界防御と呼ばれた。これは城郭に堀を築くのと同じ発想であり、訪問者を受け入れる際には、跳ね橋を下し、検査してから関門を通す。2004 年より以前には、ネットワークもこれに似た形で防御するのが普通だった。ファイアウォールをネットワークの周囲に構築し、ユーザーは認証情報（通常はユーザー名とパスワード）を提示することでそこを通り抜けることができた。いったん内部に入ってしまえば、堀の内側のあらゆるものに全面的にアクセスできた。侵入検知システムは、攻撃の可能性のある不審なネットワーク通信を検出し、その通信が企業という城の内部に入っていくのを食い止めた。これは一般に、外側が堅くて内側が柔らかいことから「クラムシェル（貝殻）」型防御と呼ばれる。また、多くの企業は、これらのファイアウォールや侵入検知システムの運用に関する IT セキュリティ業務を外部にアウトソースしていた。こうした状況では、どのような通信に企業のネットワークの内部に入ることを許すかという極めて重要な決定を、部外者に任せなければならない。

今日では、企業は同時に多くの重大な侵入が発生し、膨大な量のデータが閲覧、喪失、改ざんされる可能性に備える必要がある。こうした脅威に対する防御は以前とは全く異なり、多種多様な内容が含まれる。重層型の防御は依然として必要ではあるが、それだけで十分とは言えない。企業の情報セキュリティチームは、ネットワークおよび企業の存続性を確保するために、状況認識、効果的なインシデント対応、実際に起きた損害の評価を行う高

[10] ONCIX Report to Congress on Foreign Economic Espionage 2009 – 2011（2009～2011 年の海外の経済スパイ活動に関する米連邦議会への ONCIX 報告）

度な処理能力を有する必要がある。情報発信、広報、取締役会への連絡などのコミュニケーション体制は前もって計画・準備しておくべきである。

APT による攻撃を実行した者が関与するインシデントは、ほとんどの場合 CEO にとって青天の霹靂である。これは不思議なことではない。APT は長い時間をかけて、システムに気付かれないように少しずつ入り込んでくる。活動を実行する時期が来ると、APT は必要なデータを窃取（または改ざん）し始める。外部組織（同業他社、警察、情報共有機関）から通知されるような場合を除けば、社内に APT 対策に重点を置いた情報セキュリティチームを持たない限り、これを事前に発見することはほぼ不可能である。IT セキュリティを外部委託している場合は、APT による攻撃に係わるリスクマネジメントは一段と困難になる。外部のセキュリティプロバイダーは、どのような資産や業務が APT の対象になるかについて把握していないからである。

CEO たるものは、インシデントの発生を想定して準備を整えておかねばならない。CISO が午前２時に電話をしてきて「我々が過去 10 年にわたって開発してきた知的財産がすべて海外のハッカーによって盗まれた」と伝える時に備えて、CEO であるあなたは３つの項目についての方針を用意しておかなければならない。

1) 取締役会、顧客、取引先、マスコミへの対応。
2) 他社の経営陣との対応。経営上直面する問題を把握し、他に影響を受けた当事者がいないか確認する。
3) 社内チームとの対応。根本的原因を特定し、運用を維持しつつシステムを回収し、新たな攻撃に対する計画を立てる。APT は会社への攻撃を維持すると考えるべきである。

十分に準備された CEO および経営幹部のチームは、問題に関する知識に確信を持ち、APT に係わる危機管理計画を持っていなければならない。そのために CEO は、関係する各利害関係者がどのような動機を持つかを理解する必要がある。

取締役会および外部の利害関係者に対処する：取締役会は株主に対して受託者責任がある。取締役の社内での役割は、CEO の行為を監視し、会社が確かに成長し富を生み出すようにすることである。取締役は、企業の存続性と株主価値を継続的に生み出す能力を確保するために、危機の際に CEO がとったすべての適切な処置について知っていることを法律により義務付けられている。顧客や取引先は、取引を続けられるか、会社が供給する製品に問題はないか知りたいと思うだろう。

同業他社に対処する：同業他社の関心事は CEO と全く同じである。彼らもまた攻撃を受けているのだ。実際、ある技術を使った製品を生産する企業が攻撃された場合、一般的にその技術に係わるすべての同業他社はそれ以前に攻撃を受けたか、近い将来（数日中に）攻撃を受けている。攻撃されている同業他社の多くは、そのことに気づいていない可能性があり、そうであれば教えてあげるのが親切というものだ。どうするにせよ、難しい判断を迫られている。

社内チームに対処する：ここからは事態が少し微妙になってくる。各企業の経営幹部には通常、様々な競合する立場・責任があり、問題と解決策に対する見解も様々であろう。CEO は断固とした指導的立場をとり、幹部間の一致協力を確保する必要がある。このような指導なしには、社内チームは今後受ける猛攻撃から無事に会社を守ることはできない。

CISO は通常、技術面の専門家であり、何としてでもネットワークを守るよう期待される。危機に直面している最中、積極的な人物であれば将来行うべき防御の参考にするためにネットワーク活動を監視しようとするかもしれないし、あるいはインターネットとの接続を切断するべきだと主張するかもしれない。CISO には、アウトソース先の外部セキュリティベンダーとの間で体制を構築し運用する責任がある。CISO は会社の収益性のために報酬を得ているのではないし、売り上げを伸ばすためでも、サービスを止めずに提供し続けるためでもない。彼の役目はネットワークを守ることである。

一方 CIO は、経理・財務と IT について担当していることが多い。CIO の職務は一般に事業重視であり、ネットワークを落とさずに、高い稼働率（たとえば 99.999%）を維持することである。CIO は事業運営に参画していることもあり、損益が優先事項となりがちである。CIO と CISO の関心事は、本質的に対極的な立場にある。危機の際に、大方の CIO は稼働時間と可用性を維持することを求める。そうすることで、CISO は侵害を許した本質的な問題点に取り組む機会を奪われてしまうこともある。CIO はオペレーティングシステムを再インストールして、システムを再構築しろと主張するだろう。CISO が、入れ直したオペレーティングシステムにも最初の侵害で利用された脆弱性が含まれる可能性を指摘したとしても、CIO は最低のコストで最高の可用性を維持することを求める。

社内にはまた、最高リスク管理責任者（CRO）や他のリスクマネジメント担当者・部門が存在することもある。CRO は通常、事業、継続性、運営、財務および IT に係わるリスクを特定、移管（保険を介して）、軽減、または単に容認する責任がある。しかし、リスク責任者は一般的に、IT に係わるリスクの評価・軽減についてほとんど、あるいはまるで意

識しないしその知識もない。APT がゲームの流れを変え、IT リスクは対処しなければならない企業リスクのうちの変動する（または見えない）要素に急速に変化してきている。

万全な CEO であるためには、この 3 つの主要な権限を持つポストについて、彼らの職掌と性格を考慮した上で、行動を管理する用意ができていなければならない。最近では、こうした指導力を取締役会に移管するという動きもある。米カーネギーメロン大学の CyLab などの機関は、IT セキュリティとプライバシーに関して、取締役会レベルでのより強力な関与を求めている。[11]

来るべき事態に備え、社内体制を整備するために重要な点を次に示す。

1.8 APT リスクに対応するための 10 のステップ

CEO および取締役会：対 APT 防護活動に対し強力な統制と権限を提供する。

1) APT リスクを理解し、方向性を示すための機会を作る。APT とリスクに関する簡単な説明会を開催する。また、IT リスクマネジメントを通常処理の一部に組み入れる。
2) 適切な APT リスク軽減策を確実に実行できるように、必要に応じてリソースを割り当てる。
3) 取締役会レベルで、情報セキュリティに係わる戦略、管理、投資を確実に監視する。

リスク管理責任者（もし存在するなら、最高リスク管理責任者）：効果的な IT リスクマネジメントの推進を確保する。

4) こうしたリスクを理解するプロセスを作成し、各事業部門が確実に関与するよう、通常の企業リスク軽減プロセスへ組み入れる。
5) APT リスクに関して、短期および中期における集中的取り組みを監督する。これにはリスクの測定と、その軽減措置および責任を持つ担当部署の特定が含まれる。

[11] Governance of Enterprise Security: CyLab 2012 Report（企業のセキュリティガバナンス：2012 年 CyLab 報告書）

最高情報責任者（CIO）：社内 IT 担当者を監督し、危機の際には CISO と協働する。

6) 社内 IT 計画およびその展開が、明確に APT リスクに対応し、それを軽減するものであることを確認する。
7) APT 攻撃が起きた際の、ネットワークおよび IT システムの運用に係わる意思決定を行うプロセスを確保する。

最高情報セキュリティ責任者（CISO）：「実働」レベルの技術面の専門家・管理者。

8) 進行中の事象の特定、APT 活動の軽減、短期的な対応の改善の監督を行う取組を指揮する。
9) 現有および必要とされる対 APT 防護機能とを比較し、APT 対抗策を確立するための計画およびリソース要件を作成する。
10) 長期的な対 APT 活動に責任を持ち、対応体制を構築する。

参考文献

・Armerding, Taylor, “The 15 worst data security breaches of the 21st Century（21 世紀におきた最悪のデータセキュリティ侵害ワースト）”
CSOOnline,2012 年 2 月 15 日

・Bagnall, James, “Were Senior Executives Scapegoats for Nortel’s Demise（上級幹部はノーテル瓦解のスケープゴートだったのか）”
Financial Post, 2012 年 1 月 14 日

・Boltz, Mark, “Top Three Security Concerns Every CEO Should Know（すべての CEO が知っておくべきセキュリティに関する上位 3 つの懸念）”
Chief Executive Magazine, 2011 年 8 月 16 日
http://chiefexecutive.net/top-three-security-concerns-every-ceo-should-know

・Coates, Sam, “Lib Dem fury at secret Gove plan to bring back O-levels（Lib Dem 氏は O-level を復活させる秘密の Gove 計画に激怒）”
The Times, 2012 年 6 月 21 日
http://www.thetimes.co.uk/tto/news/

・DeWalt, David, “Former McAfee CEO, David DeWalt, Joins Mandiant’s Board and Talks Targeted Attacks（マカフィーの前 CEO、David DeWalt 氏がマディアント［Mandiant］の取締役に就任。標的型攻撃について語る）”
Mandiant, Blog, 2012 年 5 月 8 日
https://blog.mandiant.com/archives/2562

・Edwards, Cliff, Karen Gullo and Michael Riley, “Sony Faces Lawsuit Regulators’ Scrutiny over Playstation User Data Breach（PlayStation ユーザーデータ流出問題で、ソニーに対して裁判監督当局の調査”
Bloomberg, 2011 年 4 月 28 日
http://www.bloomberg.com/news/2011-04-28/sony-faces-lawsuit-regulators-scrutiny-over-playstation-user-data-breach.html

・Gorman, Siobhan, “Chinese Hackers Suspected in Long-Term Nortel Breach（ノーテルの長期にわたる侵害については中国のハッカーの疑いも）”
Wall Street Journal, February 14, 2012 年 2 月 14 日版

・Governance of Enterprise Security Survey: CyLab 2008 Report（企業のセキュリティガバナンス調査：2008 年 CyLab 報告書）

・Governance of Enterprise Security: CyLab 2010 Report（企業のセキュリティガバナンス：2010 年 CyLab 報告書）

・Governance of Enterprise Security: CyLab 2012 Report（企業のセキュリティガバナンス：2012 年 CyLab 報告書）

・Harris, Christian, “Cloud Adoption Trends 2012（2012 年クラウド採用動向）”
BCW IT Leadership, 2012 年 6 月 12 日
http://www.businesscomputingworld.co.uk/cloud-adoption-trends-2012-infographic/

・McConnell, Michael, Vice Chairman, Booz Allen Hamilton, at the West Point Senior Conference（ウェストポイント上級会議での Booz Allen Hamilton の副会長、Michael McConnell 氏の発言）
2012 年 6 月 4 日

・Mello, Jr., John P., “Sony Low-balling Loss Estimates from Breach, Could Cost Company $2 Billion（ソニーはデータ侵害による損害額を意図的に低く見積もる。損害額は 20 億ドルにも）”
Government Security News, 2011 年 5 月 25 日
http://www.gsnmagazine.com/article/23426/sony_low_balling_loss_estimates_breach_could_cost_

・Office of the National Counterintelligence Executive, “Foreign Spies Stealing US Economic Secrets in Cyberspace（サイバースペースで海外のスパイによって米国の経済的機密が奪われる）”
2011 年 10 月
http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

・Oltsik, Jon, Senior Principal Analyst, U.S. Advanced Persistent Threat Analysis, Enterprise Strategy Group（Jon Oltsik、シニアプリンシパルアナリスト、米国 APT 分析、エンタープライズストラテジーグループ）
2011 年 11 月 1 日
http://www.esg-global.com/default/assets/File/APT_infographic.pdf

・The Ponemon Institute, LLC, Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies（サイバー犯罪による年間損害額の調査、第 2 版、米国企業に対するベンチマーク調査）
Sponsored by ArcSight, 2011 年 8 月
http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

・The Ponemon Institute and Symantec, 2010 Annual Study: U.S. Cost of a Data Breach（2010 年調査：米国のデータ侵害による被害額）

・Rush, Wayne, “Nortel Executives Knew of Data Breach, Chose to Do Nothing - CSO Online - Security and Risk（ノーテル幹部はデータ侵害を知っていて何もしなかったー CSO オンラインーセキュリティとリスク）”
CSOOnline, 2012 年 2 月 14 日
http://www.csoonline.com/article/700193/nortel-executives-knew-of-data-breach-chose-to-do-nothing

・“Showing Incident 1518（インシデントの紹介 1518）”
Data Loss db, 2012 年 4 月 17 日

・“Showing Incident 3661（インシデントの紹介 3661）”
Data Loss db, 2012 年 4 月 27 日

・Sims, David, “How Bad was the Google Aurora Attack?　Bad.（グーグルの Aurora に対する攻撃はどの位ひどかったのか。ひどかった）”
Communication Solutions Community, 2010 年 1 月 18 日
http://communication-solutions.tmcnet.com/topics/security/articles/72929-how-bad-the-google-aurora-hack-attack-bad.htm

・Proceedings of the CYBER SECURITY SYMPOSIUM
（2011 年 4 月にロードアイランド大学で開催されたサイバーセキュリティシンポジウム議事録）
Ann B. Carlson, Ph.D.,2011 年 4 月 11 日
http://cybersecurity2012.uri.edu/proceedings2011.pdf

・Westby, Jody R., Governance of Enterprise Security: CyLab 2010 Report（企業のセキュリティガバナンス調査：2010 年 CyLab 報告書）
Carnegie Mellon CyLab, 2010 年 6 月 15 日
http://www.federalnewsradio.com/docs/070810_cmu_rept.pdf

・Westby, Jody R., Governance of Enterprise Security: CyLab 2012 Report: How Boards & Senior Executives Are Managing Cyber Risks（取締役会および上級幹部はどのようにサイバーリスクに対応しているか）
Carnegie Mellon CyLab, 2012 年 5 月 16 日
http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf