KPMG
cutting through complexity

FAS Group Newsletter

～特別編集号～

巨額の「のれん」の減損は、
なぜ起こったか、どう防ぐか

経営不振企業のM&A

サイバー攻撃の脅威に備える

2013年12月

サイバー攻撃の脅威に備える

株式会社 KPMG FAS
ディレクター　伊藤　益光

昨今、米国家安全保障局（NSA）による盗聴疑惑が世間を賑わせています。報道によると、米国の情報機関がドイツのメルケル首相をはじめとする国家元首35名の電話を盗聴していたとのことです。これにより、EUはますます個人情報保護を強化する方向に動きそうです。近々に施行が予定されているEUデータ保護規制に影響がありそうです。また、2011年にNSAは日本政府にも、光ケーブルを使ってやり取りされる電子メールや電話の個人情報の傍受に協力するよう要請したそうですが、日本は法的制約と情報要員の不足を理由に断ったそうです。こうした要請の背景には、米国によるテロ対策の強化が挙げられます。このように映画やドラマの世界でしか起こり得なかった事件が、現実の世界でも起こりつつあります。万一、社会インフラの制御システムがサイバー攻撃を受けた場合、社会に甚大な被害が及びます。例えば、電気、ガス、水道、鉄道、交通、航空、石油、化学など社会インフラを担う企業は、最新のサイバー攻撃を理解し、備える必要があります。本稿では実際に世界各国で発生したサイバー攻撃の動向をご説明し、企業が取るべき対策について考察していきます。

伊藤（いとう）　益光（ますみつ）
ディレクター

日米にて17年以上のリスクコンサルティング経験を有し、2013年10月1日より、サイバーセキュリティアドバイザリーグループを発足し、KPMGジャパンのサイバーセキュリティプラクティスをリードしている。公認会計士、公認情報システム監査人（CISA）

【ポイント】

- **日々サイバー攻撃は進化しており、映画やドラマでしか起こらないと思われていた事件が現実化している。**
- **制御システムはクローズドからオープンな環境に移行しているため、ハッキングの脅威が増している。但し、対応にはその特性と固有のセキュリティ要件の考慮が必要である。**
- **サイバー攻撃対策はテクノロジー一辺倒であってはならず、人とプロセスが極めて大事である。また経営者の関与はキーとなる。**
- **高度化するサイバー攻撃に対抗するためには、自社だけの努力では限界があるので、業界や政府と情報連携が必要である。**

1　映画やドラマの世界が現実に

ある男子高校生が、コンピュータ上で管理されている成績を勝手に書き換えたり、様々なシステムにハッキングをして楽しんでいました。ある日、ネット上でゲームが楽しめるジョシュアというホストコンピュータに接続します。そこで彼は米国とソ連との世界全面核戦争をシュミレーションするゲームを見つけます。そのホストコンピュータが北米航空宇宙防衛司令部（NORDIC）に繋がっており、本当の核戦争の危機を引き起こして行くという映画がありました。

TCP/IPプロトコルが開発され、インターネットの原型が産声を上げた翌年の1983年にヒットした「ウォーゲーム」という映画です。また、日本でも、天才ハッカー高校生が自らのハッキングテクニックを駆使しながら、日本の治安当局と連携して国際テロ組織に立ち向かうという「ブラッディマンディ」という少年漫画を原作とするテレビドラマが登場しました。

これらでは、ハッキングが身近なもので、使い方を誤れば大変な事態になるということが、リアリティをもって描かれています。現実の世界でも映画やドラマさながらの事件が発生しています。以下、いくつか代表的な事件を見て行きます。

(1) イランの原子力発電所への攻撃

2010年7月にStuxnetと呼ばれる不正プログラムにより、イランのブシェール原子力発電所の稼働が妨害された事件

Stuxnetは、イランの核保有能力にとって重大なウラン濃縮用の遠心分離機を攻撃するため設計されたといわれ、1,000台の装置を制御不能とし、その活動を一時停止させました。サイバー戦争・テロを予期させるような衝撃的な事件でした。

(2) NASAの人工衛星の乗っ取り

2007年、2008年にNASAの気象観測衛星が乗っ取られた事件

地球観測衛星ランドサット7号は、2007年10月と 2008年7月に、それぞれ 12 分間にわたって不正侵入されています。地球観測衛星テラ AM-1 は2008年6月に2分間アクセスされ、その年の10月には 9 分間にわたって攻撃者の制御下にあり、その気になれば完全に衛星を支配できたようです。

(3) 米国の原子力発電所への攻撃

2003年1月に米国オハイオ州のデイヴィス・ベッセ原子力発電所がウィルスに感染し、SCADA（Supervisory Control And Data Acquisition：制御監視）システムが停止した事件

これは、SCADAシステムのネットワークに接続した外部委託先のコンピュータがワーム型不正プログラムのSQL Slammerに感染し、施設内のネットワーク・パフォーマンスを低下させ、安全管理システムや監視システムを約6時間にわたって停止させたものです。

(4) ZOTOB

2005年8月にダイムラー・クライスラーの米国にある工場が、ZOTOBなどの不正プログラムによって操業停止に陥った事件

全米13の工場の製造ラインが停止し、5万人の自動車工場の作業員は50分間作業できない状態に陥り、部品サプライヤーへの感染も疑われ、およそ1,400万ドル（約14億円）の損害をもたらしました。

2　制御システムの特性と固有のセキュリティ要件

制御システムは、情報システムと比べ、大きく異なる特性を有します。第一の特性として、可用性が重視されることです。制御システムは24時間365日の稼働を前提としています。エネルギーの供給、公共インフラや工場の製造ラインなどは連続稼働が必須で、万一システムが止まった場合、被害は甚大なものになります。現実的に1年に数回程度しか定期点検の時間がないため、OSやアプリケーションの修正パッチを当てることは困難です。

第二の特性として、長期運用が前提とされていることです。通常、情報システムでは3年～5年程度の間隔でシステムのリプレースが行われますが、制御システムは20年以上という長期運用が前提となっているケースが多いのです。長年にわたって可用性を維持しなければならないため、古いOSやアプリケーションを使用し続ける結果、セキュリティの脆弱性が放置されたままとなり、より多くの攻撃に晒される可能性が高くなります。

第三の特性として、データの送受信はリアルタイムであるということです。制御システムの稼働状況やサービス提供状況をリアルタイムに監視し、把握する必要があるため、セキュリティ対策を実施するにしても、ネットワークやハードウェアに対する影響は最小限に抑える必要があります。上述のとおり、古いOSやアプリケーションを使用し続けているので、パフォーマンスを維持するためには相当の配慮が必要となります。

第四の特性として、管理部門が情報システム部門ではないことです。制御システムは情報システム部門ではなく、工業の技術部門が管理していることが多いため、セキュリティの脅威を常時認識し、対応している情報システム部門とはセキュリティへの感度が違うことが多いようです。これは制御システムがクローズドな環境で運用されていたので安全だという意識もあり、セキュリティ対策を後回しにしてきた経緯があるためです。

しかしながら、経済産業省の2008年度の調査では、工作機械や半導体製造装置、各種産業機械などの製造装置の制御システムについて、全体の約70%弱がUSBポートを備えており、60%強がEthernetの接続ポートを備えています。さらに、80%強がWindows系、20%弱がUNIX系のOSを採用していることが明らかになっています。このことから、制御システムのオープン化が進んでいることがわかると思います。オープン化が進むということは、標準的な仕様の採用を意味しており、コストや運用の効率化に資する反面、セキュリティの脆弱性が表に出やすいことになります。従って、慎重なセキュリティ対策が必要となります。

以下は、情報システムと制御システムの特性を比較した表です。

図表1　情報システムと制御システムの特性比較

セキュリティ項目	情報システム	制御システム
ウィルス対策／モバイルコード	一般的 広く使用	効果的な配備は一般的でない／不可能
サポート技術の寿命	2～3年 多様なベンダー	最大20年 単一ベンダー
外部委託	一般的 広く使用	運用は外部委託されることもあるが、サービス提供者は多くない
パッチの適用	定期的 計画的	まれ、非計画的 ベンダー固有
変更管理	定期的 計画的	厳格に管理され複雑
時間に厳しい処理	一般に遅延を許容	遅延は許さない
可用性	一般に遅延を許容	24時間365日（連続稼働）
セキュリティ意識	民間部門でも公共部門でも中程度	物理的セキュリティ以外は貧弱
セキュリティテスト／監査	優れたセキュリティプログラムに含まれる	停電に備えたテストを時折実施
物理的セキュリティ	安全（サーバ室）	遠隔／無人 安全

出所：「重要インフラ制御システムとITサービス継続に関する調査」情報処理推進機構セキュリティセンター

以上のような特性から、情報システムに比べセキュリティ対策が大変取りづらくなっています。

3 企業は何をすべきか？

日々刻々と進化するテクノロジーを前に、完璧なセキュリティ対策など有り得ません。いかに事前に攻撃を察知し、適切な対応をしていくかということ以外に道はありません。現在のセキュリティツールなどのテクノロジーで、大抵の攻撃は防げるという人もいるでしょう。しかしながら、重大なセキュリティ侵害が発生した事件は、テクノロジーでは防ぎきれない未知の脆弱性をついた攻撃から発生しています。つまり、最終的にセキュリティ侵害を発見しているのは「人」です。このことから、テクノロジーでカバーできない領域は、組織体制やプロセスで補うしかありません。すなわち、組織、プロセス、テクノロジーをうまく組み合わせたセキュリティ対策が必要になるといえます。

また、組織、プロセス、テクノロジーは、セキュリティプロセスの各段階、すなわち予防、検知、対応の三つのアクションに分けてそれぞれ対策を考える必要があります。

以下、KPMGオランダで実施したサーベイから導き出した、セキュリティのフレームワークについて解説していきます（図表2を参照）。

サーベイ回答者の75%が単にサイバー攻撃のテクノロジー的な側面のみを見るべきではないと回答しています。さらに、90%が、サイバー攻撃は取締役会レベルで議論されるべきであると回答しており、その内55%については、その点に強い同意を示しています。つまり、経営者の強い関与を必要としています。しかしながら、回答企業の20%のみが攻撃に対して有効に対処出来ると答えているに過ぎず、またそれらの企業においても実際には対処プランは用意されていません。フォレンジック調査ノウハウを有している企業は約30%であり、一元管理されたイベントモニタリング機能を有している企業は55%のみです。このような状況に鑑みれば、企業が、サイバー攻撃に対して十分に対応出来ているとは思えません。また、たとえ企業が、テクノロジー的な面でサイバー攻撃に適切に対処する能力を有していたとしても、実際にどのように必要かつ適切な情報を経営者と共有し、対処プランを実行しているかは明確ではありません。

本サーベイの発見事項の一つに、一般的に予防的コントロールの導入が最も進んでおり、発見、対応の順で企業の重要性の認識が甘くなっている、ということがありました。また、企業による対応策の内容についても、対外的な対応策ではなく社内対策に偏っているという結果が出ています。対応策について、業務プロセスの評価・分析が最も一般的で、それからフォレンジック調査（痕跡の調査）とペネトレーション・テスト（侵入テスト）が続いています。

以下、それぞれのアクションについて注目すべき観点をご説明します。

(1) 予 防

予防のスキームは、ガバナンスと組織編成を検討することから始まります。その検討にあたっては、例えば「サイバー攻撃対応の責任者は任命されているか?」や「ハイリスク業務を担当する主要な従業員に対して、意識向上の為のトレーニングを実施しているか?」等の疑問を一つ一つ解決していくことが必要です。

次のステップとして、実際に企業がサイバー攻撃の事実を適時発見出来る体制にあるかを評価するにあたり、サイバー攻撃が発生した状況を再現するシミュレーションやスキャニング（セキュリティの脆弱性の検査）、ペネトレーション・テスト等を用います。最後に、最終端末(エンドポイント)の保護やネットワークのセグメンテーション等を徹底することで、サイバー攻撃の防止効果を強化します。

(2) 検知

企業活動において重要となるアクションのログ管理や、セキュリティに関連する事象を一元的にモニタリングすることで、発見手段の技術的な側面を強化することができます。

また、モニタリングとデータマイニングは、大量のデータからの異常パターンの検出、攻撃対象となる箇所の特定、システム性能の監視を行う上で、非常に有用なツールとなります。このような方法を効果的に用いることで、情報セキュリティは、単発的な検知機能ではなく、より継続的なプロセスとして機能します。企業は、サイバー攻撃に対して受け身ではなく積極的に未然防止を図ることができるのです。

図表2 セキュリティフレームワーク ー 適切な手法の上位

	Prevent（予防）	Detect（検知）	Respond（対応）
ガバナンスと組織	サイバー攻撃対応組織（63%） 教育、研修（61%）	24時間体制の危機管理組織（48%）	フォレンジック（30%）
プロセス	サイバー攻撃対応演習（机上演習含む）（29%） 定期的スキャンと侵入テスト（74%）	セキュリティ事故のフォローアップ手順（73%）	サイバー攻撃対応計画（25%）
テクノロジー	クライアント端末保護（69%） ネットワークセグメント分離（84%）	重大イベントのログ取得（68%） セキュリティ監視センター（41%）	緊急切断機能（41%）

出所：変化する視点 - KPMG Advisory N.V. 2012 年発行 "Shifting viewpoints call for action" の日本語訳版
（注）：（ ）内の%は対応できていると回答した企業の割合

(3) 対応

前述のとおり、実際の攻撃に対する準備が出来ている企業は、ほとんどありません。企業がガバナンスやリスク対策を強化するためには、24時間体制の危機戦略を用意し、セキュリティ上の各種問題に対しての具体的な対応手続を整備することが望まれます。

また、フォレンジック調査体制を整備し、攻撃受けた際に即時対応出来る仕組みを持つことで、対処メカニズムをより洗練させることができます。フォレンジック調査チームは、有事にどのような行動を採るべきかを判断する為のサイバー犯罪への対処計画を整備することが求められます。そして、企業は、攻撃を受けた際に影響のあるテクノロジーを即座に遮断できる体制にしておかなければなりません。

サイバー犯罪の対応計画を整備するにあたっても、情報セキュリティを“ワン・タイム・ソリューション”ではなく、継続的なプロセスとして考えることが重要です。当然、サイバー攻撃を100%事前に排除することはできないので、検知や対応についても予防と同様に重要であり、往々にしてこの部分の改善余地が最も大きいものです。

サイバー攻撃の検知および対応方法を確立することは、その企業にとって重要というだけではありません。サイバー攻撃の可能性を取引パートナーに積極的に通告し、攻撃内容や攻撃者の目的等の情報を共有することが、攻撃者が最終目標を達成する前に、連鎖的なサイバー攻撃を破る重要なカギとなるのです。

4 最後に

サイバー攻撃は、多くの企業をその対策に奔走させる重大な問題です。そして、その対策を実行するにあたっては、第一義的に経営者の姿勢が重要であり、経営者は組織的なアプローチを模索する必要があります。

セキュリティ網全体において最大の弱点の一つとなり得るのが人的要因です。ソフトウェアのバグを作りだすのも人、ソーシャルエンジニアリングによる従業員を踏み台にしたハッキングも人に起因し、セキュリティ事故の対応をするのも人です。従って、経営者による積極的な関与と活動は、企業全体として事の重要性を理解する上で非常に重要であるといえます。さらに、セキュリティ・モニタリングの効果的な活用に注力し、サイバー攻撃発生時に迅速に対応できるよう体制を構築すべきです。もし攻撃を受けることがあった場合には、資産と風評への被害を最小限に抑えるため、企業は迅速かつ効果的に対処しなければなりません。

しかしながら、単なる一企業の努力だけでは、限界があるのも確かです。現状のサイバー攻撃の傾向や兆候、手口を知ることは、サイバー防御体制をとる上で非常に強力な武器になります。そのためには、企業間のみならず、政府を巻き込んだ官民の情報共有が重要です。

効果的なサイバーセキュリティ戦略には関係当事者間の分け隔てないシームレスな協力が要求されます。まず、政府や経済界、そして学術界それぞれにおける知識や専門性を共有することが必要です。現在、IPA（独立行政法人情報処理推進機構）は、サイバー攻撃による被害拡大防止のため、2011年10月25日、経済産業省の協力のもと、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として、サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information Sharing Partnership of Japan ）を発足させました。その後、全5業界、45の参加組織による情報共有体制を確立し、現在、サイバー攻撃に関する情報共有の実運用を行っています。

このような関連情報共有を国内のみならず国境を越えて実行していく事が、今後の重要な課題となると考えています。

KPMG FAS グループ

〒100-0005
東京都千代田区丸の内 1−8−1
丸の内トラストタワーN館
TEL : 03-5218-8600
E-mail : fasmktg@jp.kpmg.com

kpmg.or.jp