標的型攻撃となりすましに対するリスクマネジメントを考える

大型情報漏洩事件に学ぶ

サイバー空間の事業機密防衛とは

サイバー攻撃はターゲットを明確に絞った攻撃型が主流になっているが、なりすましによる内部からの情報漏洩も後を絶たない。企業は事業機密をどのように防衛していくべきか。事業機密防衛の各分野のスペシャリストが語る「動向と対策」についてレポートする。


「ルールのない仮想空間では専守防衛の対応策が重要」と語る橋本豪氏

制作／レクシスネクシス・ジャパン企画制作部

本セミナーは9月26日の午後、東京・丸の内ビルディングで開催された。登壇した講師は、西村あさひ法律事務所の外国法パートナー・橋本豪氏、サイバー空間の監視技術の活用を提唱するハミングヘッズ株式会社顧問の石津広也氏、生体認証技術の活用を提唱する株式会社ディーエス代表取締役の三吉野健滋氏の3名だ。

会場には企業法務担当者、経営者、弁護士など約80名が集まった。

仮想空間における脅威への法的対応策

最初に登壇したのは、ニューヨーク州弁護士である橋本豪氏。橋本氏はサイバー関係の法律実務に長く携わった経験に基づき、次の項目に沿って講演を進めた。

①仮想空間とは何か
②仮想空間でのセキュリティとはどのようなことか
③仮想空間におけるビジネスを取り巻く現状は？
④企業におけるセキュリティはどうあるべきか
⑤事業機密防衛にどう取り組むか

橋本氏は、まず「サイバースペースはどう定義できるか」「グローバル化、インターナショナル、ボーダーレス化の概念の相違点」といったことから、分かりやすく説いていく。

「〝インターナショナル〟とは国家間のことですが、〝グローバル〟となると国家の概念は弱まります。現在のグローバル化はリアルな現実世界とバーチャルな仮想空間が連関しつつ進んでいます。このなかで仮想空間のあり方を考えることが大切です。例えば、インターナショナルでは意味を持ち得た国内法をベースとした考えが、仮想空間では意味をなさなくなります。グローバル化が進行する仮想空間では、不正競争防止法や不正アクセス禁止法などが根本的解決をもたらさない法律となるのです」

橋本氏は「外来語を日本語の概念で解釈せず、原語の意味に立ち返ることで見えてくるものがある」とする。

セキュリティという言葉にもそのことがいえる。セキュリティは「安全・安心」と訳せるが、原語には「心配せずに〝自由〟にできる」という能動的な意味が加わる。

「情報セキュリティには『情報が守られる』だけでなく、『情報に関して自由にできる』という面が加わるということです」

例えば、現実世界の企業セキュリティには、ガードマン、金属探知機、身体検査などのセキュリティと、普段の人間関係を通じた情報収集・解析の両面があるが、仮想空間の企業セキュリティにおいてガードマンや金属探知機、身体検査などが意味を持つとは限らない。すなわち、「企業にとっては現実世界と仮想空間を連携させたセキュリティシステムの構築が重要となります。現実世界のグローバル化ではこれまで海外進出を前提としたグローバル化が検討されてきましたが、仮想空間はそもそもグローバルですから、海外からの侵入にも対処が必要なのです」と説く。

「そこで大事なのは人です。現実世界であろうが仮想空間であろうが、人が何らかの手を下すことで事態は進展します。機密防衛の観点においても人に帰着する面が大きいのです」

日本社会は予定調和的に競争・紛争の解決が図られる社会だ。一方、海外取引では日本と異なるルールが適用される。そこに、ルールが存在しないか、あるいは不十分な仮想空間での取引が浸透していく。

「日本の考え方が通用しない新たなフィールドでの競争・紛争の対処が求められています。国という殻のないところでは、みずから進んで自分のビジネスを守ることが大切です」

橋本氏は能動的対処・態勢を伴う事業機密防衛の重要性を改めて強調した。

ルールなき空間に専守防衛の姿勢で臨む

さらに橋本氏の講演は仮想空間と国際法の関係に及んだ。

これまでの国際法は、法的な主体が明確にあった。ところがグローバル化した社会に仮想空間が浸透し、法的な主体や公法・私法の境界線が不鮮明になってきた。

「サイバー戦争」という概念をとっても、それが戦争かどうかという考え方が生まれる。

従来の戦争は国際法のなかで戦時国際法、平時国際法という枠組みで規定され、伝統的国際法の下では開戦宣言など手続面の規定があり、戦時国際法には交戦法規と中立法規が規定されていた。しかし、仮想空間における戦争には古典的な武力行使はなく、武力行使をめぐる規定は国際関係、国家間関係にのみ適用される。

そのため、仮想空間での戦争は、国際法上の戦争の対象にはならないともいえる。すなわち、仮想空間での戦争では、従来の戦争とは異なる法規のなかで捉える必要があるということだ。

それに対して、米国大統領府は「仮想空間に攻撃があった場合、あらゆる手段を使って反撃できる」と発表した。仮想空間での脅威に、現実世界で軍事力・武力をもって対抗することがあり得るということだ。

では、そこにルールはあるのか。

「武力による自衛も手段の一つということは、自力救済も正当な手段ということ。また、仮想空間において国連憲章2条に当たる一般的な抑止規定もなく、国家による脅威か非国家による脅威かも明確な規定はありません。すなわち、仮想空間における紛争に解決のルールはないということです」

橋本氏はそう語り、最近のサイバー攻撃の一例を挙げた。ウィルス、マルウェア、ボット、ゾンビコンピュータを活用したDDoS攻撃と標的型攻撃が主流になっていることをターゲット社、ホームデポ社などの例で紹介するとともに、現在の法制度による対応の限界を指摘する。

そのなかで日本企業のとるべき道は？　橋本氏はこう語る。

「仮想空間での紛争が現実世界に跳ね返ってくることがあり得るなか、当面は「専守防衛」しかありません。しかし、日本ではメンタリティや技術の問題もあります。ですから、内部的な対策と外部に対する防御のバランスをとって対応することが大切です」

内部的には、重要な事業機密情報を洗い出し、それを重点的に防衛するインフラをつくる。また、法務、コンプライアンス、ITなどの各部門と横断的に協働できる組織をつくることが大切だとする。

「専守防衛といっても、分厚い城壁を築いて座して待つわけではありません。先制攻撃はできなくても、先回りして防衛することはできないか、と考えるべきです。そのために、自国政府の提供する情報に注意し、国際的な団体、横断的な団体も含めた業界団体内の情報交換を密にするなど外部インフラの活用も重要になります」

橋本氏はこの講演で、現実空間と仮想空間で急速に進むグローバル化、特に仮想空間でのルールの不十分さに着目。ルールの不十分さのために、仮想空間での紛争が現実空間に跳ね返る可能性を指摘した。そのとき、日本企業として重要なのは「専守防衛の考え方で、内部的にも外部的にもインフラを活用する。技術に頼らず、人による情報収集・解析も活用したい」と締めくくった。


「専守防衛」の手法の解説に熱心に耳を傾ける参加者

Windows API監視技術を用いた抜本対策を急げ

二人目の登壇者はハミングヘッズ株式会社顧問の石津広也氏。Windows API監視技術を用いた仮想空間の情報機密漏洩対策の重要性と手法を語った。講演内容は、①企業に迫る脅威と事故事例②なぜ事故を防げなかったのか③抜本対策とはどのようなものか④標的型攻撃と情報漏洩対策の具体的な方法である。

APIとは、Windows上でプログラムが動作するために、必ず守らなければならないルールのようなもの。同社はいわば、そのルールの入口のところで、情報の不正入手・活用を遮断することによって、情報漏洩対策を実現している企業である。

企業はいま、仮想空間においてさまざまな脅威にさらされている。高度化・複雑化するIT犯罪手法によって証跡確保の困難さが生まれ、セキュリティ対策の高コストとも相まって情報窃盗に対する法的な対応が十分にできない状況も生まれている。

一方、IT犯罪を防ぐ法整備は、不正アクセス禁止法、ウィルス作成罪の制定、不正競争防止法などがある程度で、公訴時効も3年（不正競争防止法は7年）と短い。サイバー犯罪の主流となってきた海外からの情報窃盗に有効ではないとの指摘も強まっている。

そのなかで企業は、事故後の信用回復が難しく、流出情報は消せず、実施対策のすべてを公開することもできず、さらに関連被害、二次的な犯罪を止めることの難しさにも直面している。まさに事故が起きてからではお手上げの状態で、事故を起こさないことが何より重要となる。

ところが、現実には、大規模な事故が相次いでいる。

「国内でも、インターネットバンキング不正送金が2014年度上半期で18億5200万円にのぼり、うち30・9％が法人口座の被害だとする調査結果も公表されました。身近な例でも、教育大手企業の顧客情報流出事故で対応費用が200億円、半導体大手企業のフラッシュメモリ機密漏洩事故で損害が1000億円以上といった報道がなされています」と石津氏は語る。

こうした事故に対して石津氏は、事故原因の本質はどこにあるか、なぜ事故を防げなかったのかを事例ごとに解説した。そのうえで、

「標的型攻撃を自社のみに仕掛けられたらどうするか、内部情報漏洩では新しい技術や大量のログを全部チェックできるのかといった問題があります。それらに対応するにはアンチウィルスソフトを常に最新にして従業員教育を徹底するだけではなく、API監視技術を活用する抜本対策が重要なのです」と説く。

石津氏は抜本対策について、標的型攻撃と内部情報漏洩の二つに分けて解説した。

「標的型攻撃に対しては、把握していないプログラムは動かさず、意図しないデータ送信は止めることなどが必要です。内部情報漏洩に対しては、データが外部に出る際に必ず暗号化し、顧客に提出するデータのみ社外で読めるようにすることなどが必要です。いずれも、万が一のために詳細なログを取得・保存しておくことが大切になります」

そして、それぞれに対応する製品『Security Platform』『Defense Platform』を紹介した。いずれもAPI監視技術を活かし、プログラム動作段階で監視する。標的型攻撃に対しては不正な割込み処理や勝手なデータ送信などを停止し、内部情報漏洩に対しては社内LANから出た情報は自動暗号化し、USBやCD、メールなど対象を問わず書出し行為を止める。

セミナーでは、製品の特徴をより詳細に述べたが、共通するのはAPIの確実な監視制御だ。

石津氏は「システムと法務が一体となった対策が重要です」と締めくくった。

「プログラムの動作の入口段階で監視・制御し、不正動作させないことが重要」と語る石津広也氏

サイバー空間では、これまでのルールが通用しないこと。新しいインフラとインテリジェンスが求められることを再確認した。

生体認証スマートフォンの劇的な普及とセキュリティ対策への影響

最後の登壇者はPC向け指紋認証でメーカーシェア35・0％（富士キメラ総研2013ネットワークセキュリティビジネス調査総覧より）を占める株式会社ディーディーエス代表取締役・三吉野健滋氏。「なりすまし防止には指紋による生体認証が第一。指紋認証がスマートフォンで普及すれば、面倒なID／パスワードから解放される」ことを力説した。

生体認証は世界でどの程度、普及しているのか。三吉野氏は、その標準化の動向を紹介したうえで、生体認証によるなりすまし対策が企業にとってコスト要因ではなく新たな収益機会を生むことを強調した。

インターネット、スマートフォンの利用が普及し、広告ビジネスでは従来のマス広告からネットによるone to one Markeingにシフトしている。また、DRM（＝デジタル著作権管理）の重要性も増してきた。一般にも、写メールによる「モバイル画像通信」が浸透している。そのなかで重要になるのが、「いつでもどこでも手軽に本人確認できること」と三吉野氏は説く。そのとき、増える一方のID／パスワードでは限界がある。ID／パスワードの不正入手・流用による情報漏洩事故も後を絶たない。三吉野氏は、その事故例を列挙し、「対策としての指紋認証はアップルとサムスンによる指紋認証機能付きスマートフォンが牽引している」と語る。

例えば、アップルは、iPhone6から指紋認証機能＋NFC（Near Field Communication：近距離通信）により、クレジット決済などさまざまな機能を搭載した。それを受けて、他メーカーでも指紋センサ搭載端末の普及を進めている。

世界の動向として注目されるのは、標準化団体のFIDO（Fast Identity Online）が指紋認証の普及を加速化させていることだ。約120社で組織する同団体は「パスワードからの解放」を目的とし、端末では生体認証を、ネットワーク上ではPKI（Public Key Infrastructure＝公開鍵）認証を採用することで、互換性と相互運用性を確保する方向での標準化を進めている。その動きにより、「生体認証の利用が一般消費者市場でも一気に拡大する」と、三吉野氏は語る。

では、生体認証で世界はどう変わるのか。生体認証がインフラとなれば、不正ログインの続出によってシステムの限界に直面した企業も、生体認証による新たなサービスを展開し、なりすましを回避できる。新たなサービスは、決済、電子マネー、著作権課金、高額電子送金、マイナンバーの応用など、さまざまなビジネスで出現する。

社会全体では、生体認証の普及は所有（鍵・カード）と記憶（ID／パスワード）から、キーレス、パスワードレス、カードレス、ウォレットレス社会を実現し、セキュリティのパラダイムシフトをもたらす。まさに、パーソナライゼーションによる利便性が実現する。三吉野氏はそのビジネスの事例とともに、応用・展開例を紹介した。

「生体認証は新たなビジネスの創出につながる」と語る三吉野健滋氏

PC／スマートフォンへの標準搭載によるインフラ化が実現すれば、使用権限許可からユーザ特定へ、セキュリティによるなりすまし防止、本人確認と利便性の融合が実現し、セキュリティの概念が劇的に変化する。特に「マイナンバー制」が導入されれば、生体認証が最も重要かつ有効なセキュリティ対策となる。

「マイナンバー制度は50年に一度の大変革で、生体認証を適用しないという選択肢はありません。そこで生体認証が加速化すれば、セキュリティ対策は、なりすましへの〝対症療法〟から〝根本治療〟となり、よりマイナンバー制度の普及が加速します。そのとき、セキュリティ対策はリスク対策ではなく効率化ビジネスとなります。なりすまし対策はセキュリティではなく、新たなビジネスの創出につながるのです」と力説した。