Deloitte.

製薬業界における
サイバーリスクとインサイダーリスク

要旨

製薬企業にとって、新薬の化学構造式ほど重要なものはないだろう。最近の報道にあるように、企業規模や業種を問わず、ハッカーによる不正アクセス、機密情報の窃取が行われている状況は、企業にとっての大きな脅威である。さらに、インサイダーによる機密情報の窃取がより深刻な問題であると専門家は警告する。本稿では、企業に対するサイバー犯罪とインサイダーによる企業機密の窃取に関する最近の事例を取り上げ、企業を標的とする先端のサイバー犯罪集団が用いるスピアーフィッシングやゼロデイ・エクスプロイトなどの手口や、古典的ではあるが特定が難しい従業員の買収による企業機密の窃取について紹介する。また、サイバー犯罪の犠牲者の多くが、集団訴訟や規制当局からの査察の対象となる昨今の動きについても触れていく。このようにデータ漏洩の事例を概観するだけでも、現在急速に変化しつつある規制環境や、増大しつつある訴訟リスク、あるいは保険に関する重要な注意点を容易に理解することができるだろう。最後に、知的財産保護の対策を強化するにあたって製薬企業が検討すべきポイントを提言することで本稿を締め括りたい。

トーマツ

デロイト トーマツ コンサルティング株式会社

“価値あるものを持っていれば、誰でも標的にされる。誰に狙われるのかを敢えて知る必要はない。”

シスコシステムズ
最高セキュリティ責任者（CSO）
ジョン・スチュワート[1]

はじめに

英国政府の試算によると、同国の製薬、バイオ、ヘルスケア産業における知的財産の窃取による損害額は、2011年で18億ポンドにのぼる[2]。また、米国政府が同年の知的財産や機密情報の窃取による米国経済への影響を5千億ドルと試算したとの報道もある[3]。オバマ政権は、米国企業に対する攻撃の多くを指揮したとして中国を公式に非難し、これに関与したとされる中国人民解放軍エリートハッカー部隊のメンバー名を公表するという異例の対応に出た[4]。

ボストン・サイエンティフィックや複数の米国製薬企業へのサイバー攻撃に関与したとされる中国のハッカー集団は、日本企業を狙ったエクスプロイト（プログラム上の脆弱性を利用した悪意あるプログラム）も開発していた[5]。セキュリティリスクに対するソリューションを提供する**ファイア・アイ社の2013年の調査報告によると、日本は同社が監視する高度ハッカー集団における4番目の標的国であった**[6]。もし、日本の製薬業界が英国（市場規模は日本の約半分）と同レベルの被害を受けたとすると、損害額は年間3千億円程に達するだろう[7]。

2014年の医薬品市場規模は、全世界で1.1兆ドルに達すると推計されている[8]。新たな治療法に対する高いニーズと特許期間中の新薬から得られる利益性の高さを背景に、新薬の開発競争は熾烈を極める[1]。そのため、犯罪組織が製薬企業の知的財産を狙うのは当然だ。盗まれた知的財産は競合の手に渡るのだが、その価値の試算は困難である[9]。

米シンクタンク Center for Strategic and International Studies（CSIS）が推計した2014年のサイバー犯罪による損失額にも、3億7500万ドルから5億7500万ドルと大きな幅がある。報告書には、知的財産の窃取に起因する損害額の試算は困難であり、過小評価となる可能性が高い旨が特記されている[10]。

ただし、ハード面での損失はある程度特定可能である。サイバー攻撃の分析を専門とするPonemon Instituteは、2014年の攻撃からの平均復旧費用を3500万ドルと試算する[11]。同社が**2014年に実施したサイバー犯罪調査では、10業界26社の日本企業が投じた国内のシステム復旧費用は、平均で約2億4100万円**と報告されている[12]。同社は、「転ばぬ先の杖」という諺は堅固なサイバー攻撃対策にも言えることであり、強力なセキュリティの構築が、復旧費用抑制のための唯一かつ最も重要な手段であるとしている[2]。

備えのない状態でサイバー攻撃を受けたならば、経営層はパニックに陥るであろう。なぜなら、**その事実が公になれば、顧客や被害者による訴訟、法令に基づく罰金、政府や自治体などによる査察、顧客や信頼を喪失といった事態が容易に想像できる**ためである。とは言え、旧態依然とした経営陣は、サイバー攻撃を受けない限り、進んで外部コンサルタントに大金をつぎ込むことはないだろう[3]。ただし、サイバー攻撃は企業にとって現実的なリスクであり、日本企業も例外ではない。

---

1. Economist Intelligence Unit, "Cyber Theft of Corporate Intellectual Property: The Nature of the Threat", March 2012.
2. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
3. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html
4. http://usnews.nbcnews.com/_news/2013/03/11/17273068-cybersecurity-threatens-us-china-relationship-white-house-official-says?lite; http://www.reuters.com/article/2014/05/19/us-cybercrime-usa-china-idUSBREA4I0942014051
5. http://www.FireEye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
6. http://www2.FireEye.com/rs/fireye/images/FireEye-advanced-threat-report-2013.pdf
7. http://databank.worldbank.org/data/home.aspx; http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf, p.22.
8. http://en.wikipedia.org/wiki/Pharmaceutical_industry#cite_note-40 (Link to IMS cite dead).
9. http://csis.org/files/attachments/140609_McAfee_PDF.pdf, p2.
10. http://csis.org/files/attachments/140609_McAfee_PDF.pdf
11. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
12. http://www.ibtimes.com/uk-joins-investigation-ebay-data-breach-did-company-do-enough-protect-user-data-1589452

日本の医薬品の研究開発に対する投資額は、2011年で120億ドルにのぼり、世界第3位の規模である[13]。欧州製薬業団体連合会によれば、新薬の上市には平均150万ドルの開発費用と、12～13年の開発期間を要する[14]。ただし開発成功確率は低く、1万の候補化合物のうち、製品となるのは平均1～2件に過ぎない[15]。このような状況下で、新薬候補、中でもまだ特許で保護されていないもののドラッグデザインを盗み出せば、その価値は莫大だ。非倫理的な競合企業にとっては、知的財産の盗用は開発リスクや費用を回避し、新薬上市による利益を得るための近道となる[4]。生産過程が複雑で高度な技術を要する非製薬業界では、盗用した知的財産を開発しようという企業は限られるが、一方で製薬業界は世界中に生産拠点と市場があるため、盗用した知的財産の開発を進めるのは至極簡単なことである[5] 。

サイバー攻撃

製薬企業が高度なインターネット犯罪の標的であることを示す論拠は多い[17]。英国政府は、製薬企業が知的財産の盗用を目的としたサイバー犯罪の主な標的であるとしている[18]。同政府の試算によれば、英国におけるサイバー犯罪による知的財産の損失額は92億ポンドにのぼり、うち18億ポンドが製薬、バイオ、ヘルスケア業界における損害である[19]。米国企業のサイバー攻撃に関する調査からは、先端のサイバー犯罪集団は製薬関連の知的財産を主なターゲットにしていることが分かっている[20]。

専門家は、中国が化学・製薬産業の発展が盛り込まれた5カ年計画達成のためにサイバースパイを活用していると指摘する[21]。ボストン・サイエンティフィックやアボット、ファイザーに買収されたワイスといった米国の主要な製薬・医療機器メーカーへのサイバー攻撃は、中国の高度なハッキンググループによるものとされる。メリーランド州にある米食品医薬品局（FDA）のコンピューターセンターも同グループのハッキング被害を受けており、国内で流通しているほぼ全ての医薬品の機密データ（化学構造式や治験データなど）が流出した[22]。

2014年2月、**米国立標準技術研究所**は、任意のサイバー・フレームワークを公表した。

このフレームワークは、企業がサイバー攻撃に備えて講じるべき様々なポリシーや手段を総体的に解説したものである。

- **把握**: 企業が有する資産（重要データ、システム、資産、機能など）および資産に対するリスクの把握
- **防御**: サイバー攻撃に打ち勝つ、攻撃を防ぐための防御手段の実装
- **検知**: 不正アクセスを検知し、リアルタイムで社内担当者にアラートを出せる常時監視体制の構築
- **対応**:サイバー攻撃を食い止め、被害を最小限に抑えるための対策
- **復旧**: ウイルスなどの駆除と被害を受けた資産の復元、および企業活動の継続

出所：
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

“名指しするが、中国は過去5年でダン・アンド・ブラッドストリート社のリストにある全企業へのハッキングを行った。”

元ブッシュ政権
サイバーセキュリティ
特別顧問
リチャード・クラーク[16]

13. http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf
14. http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf
15. http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf
16. Michael Riley & John Wolcott, “China-based Hacking of 760 Companies Shows Cyber Cold War” Bloomberg. Retrieved from: http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html
17. http://www.ft.com/cms/s/0/a6b09006-e5c9-11e3-aeef-00144feabdc0.html#axzz3CngrmgdR
18. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
19. 同上.
20. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf; http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf
21. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html; see also, http://www2.deloitte.com/content/dam/Deloitte/ch/Documents/life-sciences-health-care/ch_Studie_Pharmaceutical_China_05052014.pdf
22. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html

ハッキングは、世界中の製薬企業が抱える重大な問題であり、これは大企業に限ったものではない[23]。シスコによると、2011年の製薬・化学企業を標的としたマルウェアの数は、他業界平均の4倍以上であった[24]。また、シマンテックはマルウェアの半数以上が従業員2,500人未満の企業を標的としており、18%が250人未満の企業に対するものであったとしている[25]。さらに、シスコの2014年サイバーセキュリティ調査によると、回答企業の90%で内部PCからのマルウェア関連ドメインへのDNSリクエストが確認されており、内部情報漏洩の強い兆候が示されている[26]。ファイア・アイ社は、不正アクセス事例の分析から、侵入者は平均で発覚の241日前からネットワークにアクセスしていると警告する[6]。経営陣には、企業の大小に関係なく、既に会社情報が漏洩している可能性は非常に高いことを警告したい。

最近の報道から、現代のサイバー攻撃におけるトレンドが見て取れる。今も単独ハッカーや政治的ハッキンググループは存在するが、それらはもはや重大な脅威ではなく、代わって国家的あるいは組織的なサイバー犯罪が主たる脅威となっている。Mandiant社は、その著名な報告書の中で、米国政府や米国企業を狙った数々の高度なサイバー攻撃は、中国人民解放軍61398部隊によるものであると指摘している[7]。同部隊は、独自に開発したゼロデイ・マルウェアと攻撃を中継する巨大なインフラにより、世界中でハッキングを行っていたとされる[8]。米国の知的財産権委員会も、米国に対するサイバー攻撃の7割は中国を拠点とするハッカーによるものであり、その多くが中国政府からの資金援助を受けていると非難している[27]。一方で、米国政府はフランス、イラン、東欧を拠点とする犯罪組織やロシア政府を後ろ盾とした犯罪組織についても、高度なサイバー攻撃の犯人であるとしている[28]。

強固なサイバーセキュリティ戦略を立案する上で、高度なハッカー集団は不正アクセスの際に2つのツールを利用することを理解しておく必要がある。

1つ目のツールはゼロデイエクスプロイト（適切なパッチ等が提供される前に脆弱性に対して行われる攻撃）である。ハッカー集団は、まだ世に知られていない新たなエクスプロイトを開発または購入している[9]。実際、このようなツールは非常に高額であり、新たな「ゼロデイ」エクスプロイトを政府や犯罪組織に販売することのみを生業にするハッカーが存在するほどだ[29]。このようなハッキングツールの流通には、闇市場が大きな役割を果たす。シスコは、昨年ロシア当局が悪名高いBlackholeエクスプロイトパッケージの作者である「Paunch」を逮捕したことで、インターネット上で流通するエクスプロイトキットが87%も減少したと報告している[30]。Paunchは、自ら作成したゼロデイ・マルウェアへの定期アクセス権を販売し、月額5万ドルを稼いでいたと言われる。彼の「顧客」がコンピューターに不正アクセスする目的は様々であるが、中には銀行から8億2200ドル相当のルーブルを盗み出したとされるものもある[31]。

このように一瞬の後退局面はあったものの、標的のファイアウォールやアンチウイルスソフトをすり抜ける、新たな「ゼロデイ」エクスプロイトは今も流通し続けている。このような現実を受け、**セキュリティ業界では、不正アクセスは不可避であり、必要なのは、それを検知し、対応するための投資であるという新たな認識**が生まれた[32]。

23. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf
24. Cisco Systems, “Cisco 4Q11 Global Threat Report,” 2012, http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_4Q11.pdf
25. Symantec, “2011 Internet Security Threat Report,” April 2012, 14, available at http://www.symantec.com/threatreport.
26. Cisco Systems, “Cisco 4Q11 Global Threat Report,” 2012, http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_4Q11.pdf
27. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf, p.3.
28. http://www.voanews.com/content/china-russia-israel-france-iran-cyber-threat/1608419.html
29. https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate
30. http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html
31. http://krebsonsecurity.com/tag/paunch/
32. http://www.newyorker.com/magazine/2013/05/20/network-insecurity; https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf, p.1

不正アクセスに用いられる2つ目のツールは、スピアーフィッシング（本物の送信者からのように偽装し、マルウェアを含むEメールをターゲットに送りつける手法）などの無防備なユーザにマルウェアを実行させたり、ネットワークへのアクセスを許可させる手法である[33]。Francophoneと呼ばれるフランス企業を対象とした攻撃は、未解決ではあるが、よくある筋書きに沿ったものである：

- オンライン請求書へのリンクを役員秘書にメールで送信（ハッカーが社内セキュリティを回避するために役員秘書を利用）
- 流暢なフランス語を話すメンバーが別オフィスの幹部になりすまし、その秘書に電話をかける
- 秘書に電話口でリンクにアクセスし、ダウンロードしたファイルを開くように指示する
- 秘書が警告を無視してクリックを続けた結果、ゼロデイ・マルウェアが実行され、ネットワークへのアクセスが可能となる
- ネットワーク内で虚偽の銀行取引に必要な情報を収集する

あるケースでは、不正に入手した認証情報を使って企業の非常事態チームに電話を掛け、その通話を偽のバックアップコールセンターに転送させる手口が取られた。結果、殆どの電話は会社へと再転送されたものの、虚偽の銀行取引に関する銀行からの確認電話は犯人側に転送され、最終的に承認されてしまった[34]。

世界中のスピアーフィッシング事例に基づくシマンテックの分析によると、**最も標的になりやすいのは役員秘書、シニアマネージャー、広報担当者である**[35]。また、ネットワークへの不正アクセス用マルウェアの拡散に「Watering Hole（水飲み場攻撃）」が用いられるケースが増えていると専門家は警鐘を鳴らす[10]。「水飲み場」は、信用できる組織が運営するサイトがハッキングあるいは不正操作され、訪問者が無意識にマルウェアをダウンロードするよう改ざんされたものを指す[11]。

例えば、2014年2月に米国退役軍人クラブのサイトが不正アクセスを受けたケースでは、サイト上のJavaScriptエクスプロイトにより、訪問者のInternet Explorer 10ブラウザが実行ファイルをデータとしてメモリにダウンロード、実行し、訪問者のコンピューターから情報が漏洩するよう改ざんされていた[36]。このサイトは現役軍人が閲覧する可能性が高く、軍関係者のコンピューターを秘密裏にハッキングするには巧妙な手口と言える。その攻撃の特性から、専門家は「オペレーションDeputy Dog」と呼ばれるキャンペーンを立ち上げた中国外の組織が犯人であると結論付けている[37]。「オペレーションDeputy Dog」はInternet Explorer向けのゼロデイエクスプロイトで、日本企業も狙ったものである[38]。これらのマルウェアのコーディング・プロファイルの分析から、米国政府や企業を狙った高度なハッキング・グループが日本企業をも標的としていたことが明らかになった。

“外部のハッカーのみではない。インサイダーも、知的財産が絡むサイバー犯罪の3分の2以上に関与している。（中略）動機はご都合主義か、金か、復讐か、はたまたこの3つが組み合わされたものなのかは定かではないが、インサイダーは自身の信頼ある地位を利用して企業の最も価値あるデジタル資産へアクセスする。” [39]

インサイダーによる知財窃取

大きく話題に取り上げられてはいるものの、外部からのネットワーク攻撃は最大の脅威とは言えない。その被害規模は知り得ないが、企業の知的財産を最も多く窃取しているのはハッカーではなく、インサイダーだということは一般的な認識である。

33. http://www.darkreading.com/vulnerabilities-and-threats/social-engineering-leads-apt-attack-vectors/d/d-id/1100142?
34. http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack
35. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
36. http://www.FireEye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
37. http://www.FireEye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
38. http://www.FireEye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
39. http://www.krollcybersecurity.com/insider_threat_wp_022213_tht_042_2013_final.pdf

eBayに対する調査機関に英国の情報コミッショナー事務局が新たに加わった。このEコマース大手が最近の情報漏洩の対応で、デュー・デリジェンスを行っているかを確認するためだ。（中略）情報コミッショナー事務局は米連邦取引委員会やFBI、コネチカット、フロリダ、イリノイ州政府による同様の調査にも参画している。

International Business Times（2014年5月23日）[12]

2012年、二酸化チタン（紙やプラスチックに使われる白色の顔料）の製造方法を窃取したとしてデュポンの元社員が起訴された[40]。元デュポンの技術者であったTze Chaoは、同社の競合である重慶市の中国国営化学メーカー、パンガン・グループに企業機密を渡したことを認めている[41]。

最近でも、デュポンは韓国化学メーカー、コーロン社を相手取ったケブラー®（芳香族ポリアミド系樹脂）の生産技術機密流用に関する訴訟を行っていたが、米連邦控訴裁判所が新たな公判を命じたことで手痛い失敗を犯した。デュポンは、コーロンと同社の幹部がデュポンの元技術者5人をコンサルタントとして雇い入れたが、それは単なる口実に過ぎず、実際は元社員からデュ　ポンの製造プロセスの秘密情報を集めていたと訴え、9億3100万ドルの支払いを命じる判決を勝ち取った[42]。コーロンとその幹部に対する刑事告訴は続いており、被告人が帝人の米国法人から企業機密を窃取したとの訴えも含まれている。

このような訴訟は枚挙に暇がなく、近年の例では、米司法省が中国企業のスパイとして企業機密を盗用したとしてダウやモトローラ、フォードのインサイダーを起訴している[43]。

ただ、注意しなければならないのは、中国企業からのスパイに絡む訴訟は大きな注目を集めてはいるものの、スパイの数どころではないインサイダーが企業内にはびこっていることである。従業員は日々の行動の中で企業情報を社内ネットワーク外で操作しており、自宅へ持ち帰ることもあれば、Googleクラウドなどに保存することもある。転職の際に、このような企業情報が競合のネットワークに持ち込まれたり、時には競合製品に利用された事例も存在する[44]。

知的財産の窃取を回避するため、企業には以下のような取り組みが必要である。

- 従業員に対し、セキュリティなどの手順に関する定期的な教育プログラムを提供する
- 機密情報が（強力にではなくとも）十分に保護されていることを確認する
- 新たに従業員を雇用する際には、適切な選考プロセスを用いる
- 疑わしい事象があった場合に従業員が報告できるよう、心理的負担が少なく、簡便な手段を確立する
- 疑わしい動きがないか、コンピューターネットワークを定期的に監視する
- セキュリティ（コンピューターネットワークセキュリティを含む）担当者が必要なツールを持っているか確認する。

出所：Federal Bureau of Investigation, The Insider Threat

40. http://online.wsj.com/news/articles/SB10001424052970203986604577256003717724564
41. http://abcnews.go.com/blogs/politics/2012/02/chinese-espionage-aleged-to-target-dupont/
42. http://www.courthousenews.com/2014/04/10/66975.htm; http://www.crowell.com/files/US-v-Kolon-Indictment.pdf
43. http://www.cnbc.com/id/100481542#.
44. http://www.symantec.com/content/ko/kr/enterprise/collateral/white_papers/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf

外部への対応

「データ漏洩」という言葉には、善人の防御が悪意をもって破られるようなニュアンスがあるが、一方で、新たな法律上のパラダイムが生まれつつある。それは、**企業は顧客やパートナーに対し、自社のネットワークとそこに含まれる第三者のデータを保護する責任を負う**というものだ。この理論に基づくと、サイバー攻撃による情報漏洩は、データ保護の失敗を意味する。結果として、サイバー被害を受けた企業が、ありとあらゆる査察や訴訟の対象となるのである。

政治的ハッカー集団アノニマスのメンバーである23歳のコーディ・クレシンガーとその仲間は、2011年にソニーのPlayStationシステムと同社のネットワークをハッキングした。この事件では、1億件の顧客情報が盗まれたにも関わらず、クレジットカード情報の漏洩はなかった[45]。なぜなら、この政治的ハッカー集団の目的が情報の不正利用ではなく、ソニーがハッカーのジョージ・ホッツを提訴したことへの憤りを表明することであったためである[46]。このアノニマスによる不正アクセスを公表した結果、ソニーは65件あまりの集団訴訟に直面した。いくつかの訴訟は統合され、放棄された訴訟も1件あったが、それでもソニーは1500万ドルの賠償金と訴訟に伴う弁護士費用を支払わなければならず、加えて、英国の情報コミッショナー事務局から25万ポンドの罰金を科されることとなった[47]。

2014年に発生した米ディスカウントストア、ターゲットのケースでは、エアコンと冷蔵庫の保守業者が認証コードの不正利用により社内ネットワークにアクセスし、結果、何百万人もの顧客のクレジットカード情報が漏洩した[48]。情報漏洩を受け、ターゲットは、米司法省の査察、上院委員会での聴取、複数の検事総長からの問い合わせに追われることとなった[49]。また、100件以上の集団訴訟が39か所の地方裁判所に寄せられ（連邦司法審議会に取りまとめを依頼している）[50]、さらに、漏洩したカード情報による不正請求の債務を負った銀行からの集団訴訟も進行中だ[51]。

このような捜査や訴訟に加え、保険適応範囲の課題もソニーやターゲットの経営陣を苦しめた。ソニーの場合、商業一般保険を引き受けていたチューリッヒ保険から訴訟や当局による措置に関する交渉、補償を拒否されている。この点に関し、チューリッヒ保険は、ニューヨーク州裁判所から保険契約の補償範囲に関する確認判決を勝ち取っている[52]。

ターゲットの経営陣の二人は、個人的な苦境にも立たされた。サイバー攻撃に十分な防衛手段を講じず、事件後の対応も誤ったとして、ターゲットの経営陣に対して少なくとも2件の株主代表訴訟が起こされた[53]。この種の訴訟は通常、会社役員賠償責任保険の補償対象となる[54]が、ターゲットの加入する保険の対応は明らかにされていない。

いずれにしても、サイバーセキュリティ関連の過失に対する株主代表訴訟が起こった場合の補償範囲について、今の段階から保険会社と確認しておくべきだろう[55]。

---

45. http://www.wired.com/2011/09/sony-hack-arrest/
46. 同上.
47. http://www.zdnet.com/sony-settles-psn-hack-lawsuit-for-15-million-7000031961/
48. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
49. http://online.wsj.com/news/articles/SB10001424052702304020704579276901918248632
50. http://www.law360.com/articles/522775/target-presses-panel-to-send-data-breach-cases-to-minn
51. http://www.chicagobusiness.com/article/20140325/BLOGS11/140329865/chicagos-trustwave-sued-over-target-data-breach
52. http://www.insurancejournal.com/news/east/2014/03/17/323551.htm
53. http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/
54. http://www.businessinsurance.com/article/20140608/NEWS07/306089968
55. http://www.rmmagazine.com/2014/04/02/do-insurance-for-data-breaches/

悪意あるアクセスから企業のネットワークを完全に守りきることは不可能であるという認識は、予防から検知へというサイバーセキュリティにおけるパラダイムシフトをもたらした。

さらに、増加する一方のサイバーセキュリティ関連規制と報告義務も企業の頭痛の種だ。カルフォルニア州はデータ漏洩の報告に先進的に取り組んでおり、2003年に定めた法令では、情報が漏洩した全個人にその事実を通知し、さらに500人以上のデータ漏洩については通知のサンプルを検事総長にも送付するよう求めている[56]。最近、同州はハードドライブに保存されていた3万人の従業員の社会保障番号が過失により第三者に売り渡された際、通知に4ヶ月もかかったとして、カイザーパーマネント社を提訴している[57]。

この秋には、フロリダ州政府も信用調査連合会への報告義務の追加と罰金の上限を年50万ドルとする変更を可決し、報告義務を厳格化している。米国証券取引委員会（SEC）の企業金融局も、2011年のガイドラインでSEC提出書類にサイバーリスク情報を記載するよう求めている[58]。

また、EUも今年に入って電子プライバシー保護指令（ePrivacy Directive）を改訂し、通信事業者に対して、サイバーセキュリティ対策に加え、情報漏洩に際する利用者への通知義務を課している[59]。ただし、暗号化されたデータは通知義務の対象外となる[60]。EUのデータ保護指令第29条作業部会は、全企業に情報漏洩の通知を指導しており、状況により発見から24～72時間以内の通知を推奨している[61]。EUの電子プライバシー保護指令の対象は、現在のところ通信事業者のみであるが、英国情報コミッショナー事務局の裁量権はより幅広いものである。

ソニーとeBayのデータ漏洩では、英国外の事件であるにも関わらず、事務局の調査が入った例である[62]。日本では、特定業界を対象としたデータ漏洩の報告ガイドラインは存在するが（金融庁が定める金融業界のガイドラインなど）[63]、それ以外にも、海外の個人データが日本で漏洩した場合には外国当局の規制対象となる可能性があることを認識すべきである。

打ち手はあるのか？

製薬業界の研究開発部門は、世界のイノベーションと経済発展を牽引する重要な機能である[13]。当然、製薬企業経営陣は自社の知的財産や顧客データなどの財産を保護する必要性を認識しているが、そこには課題も存在する。つまり、セキュリティ対策の費用対効果の最大化と、サイバー攻撃の阻止、セキュリティコストの抑制、職場の生産性維持の適正なバランスの確保である。ある意味、この課題の解決策を導くには、自社が保有するデジタル資産と、各々の資産に対するセキュリティ対策を慎重かつ徹底的に精査するしかないだろう。しかし、専門家は企業が行うセキュリティ対策の見直しには共通する問題があると指摘する。

56. http://oag.ca.gov/ecrime/databreach/reporting
57. http://www.infolawgroup.com/2014/01/articles/breach-notice/california-attorney-general-files-lawsuit-based-on-late-breach-notification/
58. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
59. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
60. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
61. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf, p.2; http://www.infosecurity-magazine.com/news/eu-businesses-prep-for-regulations-requiring-24/
62. http://www.theguardian.com/technology/2014/may/23/uk-data-watchdog-ebay-investigation-cyberattack; http://ico.org.uk/news/latest_news/2013/ico-news-release-2013
63. http://www.bahagram.com/files/WLG_Guide_to_Data_Breach_Notifications-Review_Proof.pdf

デロイトでは、サイバーセキュリティ対策において、以下の3点が重要と考える。

1. 資産の特定

自社が有する、不可欠かつ重要なデジタル資産を特定する。これは、事業運営および製品開発に必要不可欠な資産を指す。その上で、次の項目を確認しておく必要がある：

- 特に重要な資産はどれか？
- データの格納場所は？
- 資産と資産が格納されているネットワークへのアクセス権は誰に付与されているのか？
- データを狙う外部者にとって、魅力的なのはどのデジタル資産か？
- 法令・規制による保護義務を有する資産は？

2. 検知システムの構築

前段で特定された最重要資産は、隔離、保護される必要がある。しかし、不正アクセスの検知は、ファイアウォールやアクセス認証、アンチウイルスソフトといった従来のセキュリティ手段とは一線を画するものである。これらはみな、ゼロデイエクスプロイトやソーシャル・エンジニアリングによる高度なハッキングを防ぐには不十分であるため、企業は不正アクセスが発生し得るものとして備えておかなければならない。従って、**たとえマルウェアがゼロデイエクスプロイトであっても、不正アクセスが発生している段階で確実に検知し、セキュリティチームに警告を出すことができる先進的な検知システムにセキュリティ予算を投じるべき**である。

3. 対応と復旧

対応と復旧は、米国立標準技術研究所（NIST）のサイバー・フレームワークでは技術的に別のプロセスとして扱われているが、実際は密接に関連している。円滑な対応には事前の計画が不可欠であり、対応の段階で被害内容が確認されるまでは復旧に着手できない。事前に対応策が用意されていなければ、現実にデータ漏洩が発生した際に、状況と把握に著しい労力を費やすこととなる。その後、リスクに晒されるビジネスプロセスを把握し、世間に公表すべき、当局に報告すべき情報を特定することになるが、この作業も混乱を極めるだろう。そのため、深刻なデータ漏洩に際しては、回復作業を指揮する外部コンサルタントの活用が一般的である。

以上のことから、事前の備えの重要性を認識し、有事の際の対応・復旧支援を委託するベンダーを予め選定しておくことをお勧めしたい。**堅固なログシステムなどの対策をベンダーと共に構築することにより、犯罪学や損害の軽減措置に対する理解を深めることも可能である。そうすることで、何が起こったのかを迅速に突き止め、被害を最小限に食い止められる企業となれる。**

また、情報漏洩に関する規制当局や、基準や規制に準じたセキュリティ対策を法務部門が把握していることを確認しておくことも重要である。そうすることで、規制当局からの問い合わせにも備えることができる。

さらに、データ漏洩に関する通知には特に十分な準備を進めておきたい。迅速に通知を行うには、事前に実施計画を準備しておく必要がある。迅速に通知できるか否かは、犯罪学的観点からサイバー攻撃の目的を理解できるか否かにかかっている。それが理解できれば、綿密なサイバー攻撃への対応計画の立案が可能となり、経営陣が通知の対象と内容を迅速に決定する体制を整えることができる。

なお、インサイダーについては、他企業や他業界の失敗例からの「学び」が多く存在する。

1. トレーニングや教育プログラムの実施

従業員による知的財産の窃取は、読みもしない機密保持契約書にサインさせただけでは防ぎ得ない。従業員には、企業機密などの重要情報は社外に持ち出せないことを認識させねばならない。具体的には、USBやクラウドに企業のデータを保存することがルール違反であることを認識させることが重要である。

また、スピアーフィッシングのリスク軽減のためにも、社員教育は大切である。不審なリンクをクリックしたり、不明なソースから実行ファイルなどを会社のネットワークにダウンロードしてはならないこと、また、不測の事態が発生した場合の連絡先を従業員に周知しておくべきである。

2. アクセス権付与のルール構築と徹底

多くの場合、企業の内部統制は曖昧なものである。スノーデンがあれほどの情報にアクセスできたのはこのためだ。企業は重要データにとどまらず、ハードウェアや、場合によってはネットワークへのアクセス権も制限するべきであり、経営陣やITスタッフものその対象とすべきである。

暗号化はあくまでもデータの読み込みを防ぐためのものである。

3. 人事制度・勤怠管理による知的財産窃取の抑制

知的財産窃取の可能性が高いのは、特定層の従業員である。具体的には、企業や上層部に不満を持った者や退職を控えた者が、機密性の高い会社資料をコピーしたり、自宅に持って帰ったり、第三者に提供したりする可能性が高い。事件発覚後の取り調べで、犯人が事件を起こす前から勤怠問題やセキュリティ違反など数々の問題を抱えていたにも関わらず、見過ごされていたことが明らかになるケースは多い。退職を控えた従業員では、正式な通知の前後数週間に、大量の資料をコピーすることが多い。

そのため、ログの取得やアクセス制限を導入し、これらの高リスクな従業員を監視するとともに、個々の従業員の過去から現在に至るデータのやり取りを確認できるようにすべきである。もちろん、監視を行うにあたっては、対象従業員やプライバシー関連法に配慮し、弁護士とも協議する必要がある。

結論

製薬企業が保有する知的財産の価値は、有形資産にも匹敵し得るものである。長期的な視点から、高度なセキュリティ体制を構築することで得られる恩恵は、投資額をはるかに上回るものとなるだろう。

コンタクト

丸山 満彦
パートナー
サイバーリスクサービス
デロイト トーマツ リスクサービス株式会社
090 6492 3648
mitsuhiko.maruyama@tohmatsu.co.jp

松尾　淳
パートナー
ライフサイエンス & ヘルスケア
デロイト トーマツ コンサルティング株式会社
080 2003 8644
jmatsuo@tohmatsu.co.jp

Ash Mahmood
シニアヴァイスプレジデント
公認不正検査士（CFE）
デロイト トーマツ
ファイナンシャルアドバイザリー株式会社
080 4182 6048
ash.mahmood@tohmatsu.co.jp

Christian Boettcher
ディレクター
ライフサイエンス & ヘルスケア
デロイト トーマツ コンサルティング株式会社
080 9097 7376
chrboettcher@tohmatsu.co.jp

William “Bud” Roth
シニアマネジャー
サイバー/ナショナルセキュリティ
パブリックセクター
デロイト トーマツ コンサルティング株式会社
080 4651 5850
wroth@tohmatsu.co.jp