米国で注目されるM&Aサイバーデリジェンス

ニューヨーク駐在員　公認会計士　吉田哲也　　EYニューヨーク事務所　藤崎剛之助

▸ Tetsuya Yoshida

当法人パートナー。日本で多国籍企業の監査に従事した後、2016年7月より ニューヨーク事務所に日系企業担当ダイレクターとして駐在。多数の日系企業の米国事業展開のサポートに従事。

▸ Go Fujisaki

米国EY TAS部門シニア・マネージャー。EY TAS日本オフィスで国内およびクロスボーダー M&A案件に従事した後、2016年1月よりニューヨーク事務所。日系企業を中心に、多数のM&A案件支援に従事。

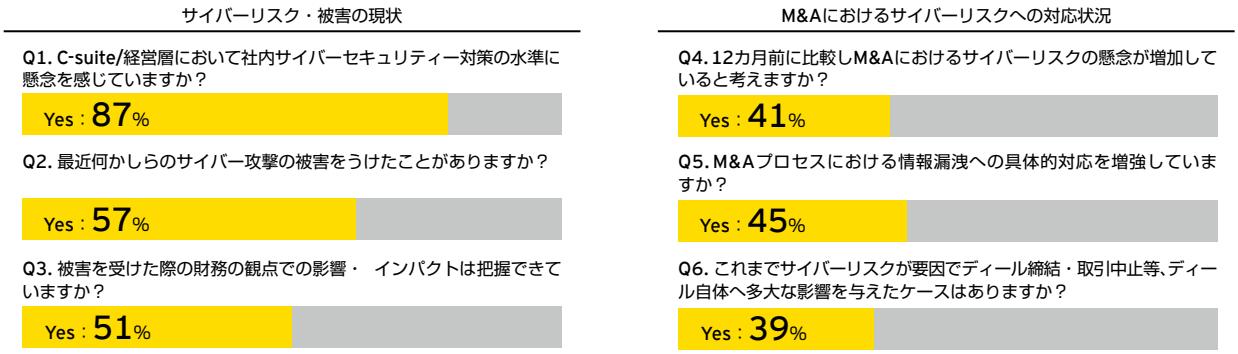
Ⅰ　はじめに

近年注目を浴びるサイバーリスクですが、米国では特にM&Aの一連のプロセスにおけるサイバーリスクへの対応策としてサイバーデリジェンスが注目されています。M&Aのプロセスにおいては、知的財産や製造ノウハウ、個人情報、価格情報、調達先情報といった重要情報がアドバイザーなどを含む外部第三者に開示されることに加え、ITや事業の企業の境界を越えた統合や分割が行われます。このため、M&Aの一連のプロセスにおけるサイバーリスクは高く、これに注意を払われなかった結果、競争優位性の喪失、顧客対応コストの発生、訴訟や課徴金といった影響がもたらされる可能性があります。

Ⅱ　サイバーデリジェンスが注目される背景

M&Aにおいては、ターゲット企業のサイバーリスクへの対応が十分でないようなケースは、ハッカーの格好の標的となると考えられます。EYが実施したGlobal Information Security SurveyやGlobal Capital Confidence Barometerでの調査結果（<図1>参照）によると、何かしらのサイバー攻撃の被害を受けた企業は回答者全体の57%になり、87%の経営層は社内のサイバーセキュリティ対策に懸念を感じています。また、41%は12カ月前に比較して懸念が増加していると回答しており、45%はM&Aプロセスにおける情報漏洩（ろうえい）への具体的対応を増やしています。M&Aの活況と歩調を合わせてサイバーリスクへの意識が高まっており、この早期発見と対応のためのツールとしてサイバーデリジェンスが注目されているといえます。

▶図1　サイバーリスクに関するアンケート結果

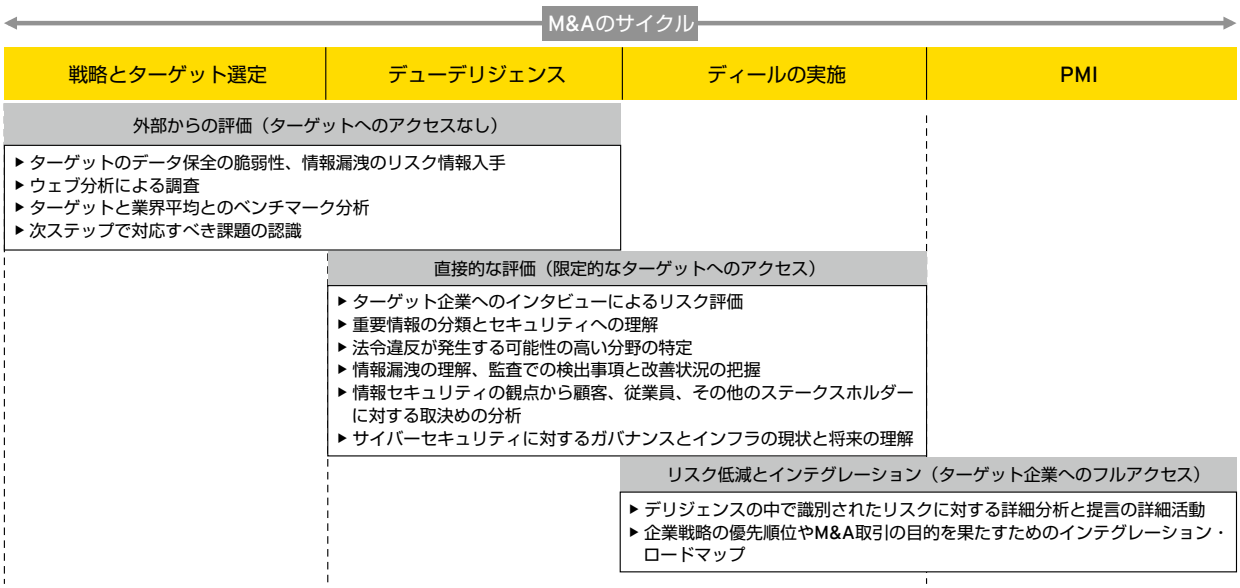


出典：EY Global Information Security Survey 2016, EY Global Capital Confidence Barometer Apr 2017

▶表1　過去3年以内の大型M&Aにおける情報漏洩事案

会社	買収規模	事案
A社（豪、通信）	700M USD	アジアのケーブル・オペレーターを買収する2週間前にターゲット企業でハッカーによる情報漏洩が生じていたが、クロージング後まで事態を把握できなかった。
B社（米、情報）	200M USD	旅行サイトの運営会社を買収した後に、ターゲット企業において140万件の顧客情報が盗まれていたことが発覚した。

▶図2　サイバーデリジェンスの手続



実際に過去3年以内に行われた大型M&Aでは、<表1>のような情報漏洩事案が発生しています。EYがサポートした大型アパレル企業によるeコマース・プラットホーム獲得のための小規模アパレル企業買収案件における調査でも、ターゲット企業のプラットホームがマルウェアを拡散していたようなケースが発見されており、オンラインリテールやホテル・チェーン、知的財産を有するような企業を買収ターゲットとするケースでのリスクは高いといえます。

Ⅲ　サイバーデリジェンスの手続

サイバーデリジェンスでは<図2>に示すように、「戦略とターゲット選定」「デューデリジェンス」「ディールの実施」「ポスト・マージャー・インテグレーション（PMI）」というM&Aの各ステップで、潜在的なリスクや価値の創造の機会に影響を与えるようなファクターを把握します。

ターゲット企業へのアクセスが困難である「戦略とターゲット選定」「デューデリジェンス」の初期段階では、ターゲット企業のウェブ分析による調査、外部からのインターネットアクセスに対する脆弱性の理解、潜在的な成長戦略に対するサイバーリスクの財務的インパクトをモデル化することよりサイバーリスクへの暫定的な理解を進めます。

「デューデリジェンス」と「ディール実施」の段階では、インタビューや文書の閲覧を通じてターゲット企業のサイバーセキュリティに対するインフラへの投資が十分か、サイバーリスクに対する姿勢はどのようなものか、また顧客やサプライヤーとの契約違反の有無や訴訟の結果が財務的に与える影響について理解することが重要です。買収後のターゲット企業の情報漏洩の発覚や、クロージング直前でのデータ盗難を防止するためには、この段階の調査で明らかになった問題への十分な対応が必要になります。なお、ターゲット企業のセキュリティリスクを把握することは、相手企業との交渉ポジションの強化につながることもポイン

トといえるでしょう。

「PMI」の段階では、ターゲット企業へのフルアクセスが可能となった中で、リスクの詳細分析とM&Aの目的達成のため具体的な統合活動が進められます。統合の過程で、マルウェアのターゲット企業ネットワークから買収企業ネットワークへの侵入や、不十分なアクセス管理のためにターゲット企業を退職した従業員からの不正なアクセスの発生といったリスクに対応します。

また、トランザクションの完了後もサイバーリスクに対するモニタリングと対応を継続することは、M&Aの目的を達成するためには必須といえるでしょう。

Ⅳ　おわりに

今後、日本企業の米国マーケットへの投資は継続することが予想されます。日本では、M&Aの際のデューデリジェンスの切り口としてビジネス、財務・税務、法務、環境といったリスクについては認識されているといえますが、サイバーリスクとその対応は必ずしも認識されているとはいえない状況にあると考えられます。M&Aを展開する日本企業にとって、サイバーデリジェンスは注視すべきテーマであるといえるでしょう。

（注）本稿は米国EY TAS 部門パートナー、Doree Keating（Transaction Support - Cyber Due Diligence, Email: doree.keating@ey.com）による執筆内容をもとに作成しています。

お問い合わせ先
EYニューヨーク事務所
ジャパン・ビジネス・サービス
E-mail：tetsuya.yoshida@ey.com
E-mail：go.fujisaki@ey.com