リスクマネジメント

最新のグローバルリスク
サイバーリスクの脅威
―その把握と対策―

平賀 暁
マーシュブローカージャパン株式会社
代表取締役会長

『CFO FORUM』第44号では、世界経済フォーラム発行の〝第八回グローバルリスク報告書二〇一三年版〟の概要とデジタル・ワイルドファイアー（ネット上の山火事のような事態）が最重要のリスクケースの一つとして挙がっていることを説明した。今回は企業のみならず、政界・自治体・学界など広範にわたり影響力を持ち世界全体を震撼させるサイバーリスクの実態を把握し、企業として最低限意識すべき事柄をいくつか紹介する。

過去二年の報告書で取り上げられたサイバーリスク

そもそも、サイバーリスクは二〇一二年版の報告書において大きく取り上げられている。我々の日常生活のほとんどがコンピュータ・システムに依存しており、遠隔かつ匿名で破壊的なサイバー攻撃を仕掛ける能力を急速に身に着けてきた、悪意のある個人・組織などからインターネット経由で影響を受け易い状況にあることが示唆された。サイバー攻撃の目的は大きく三つに分けられる。①データの改変や改竄を目的とした妨害工作、②システム内にアクセスして機密情報などを盗用するスパイ工作、③ウェブサイトのハッキングやウィルスの流し込み、あるいはボットネット（注）を構築して、コンピュータ所有者に気付かれずに遠隔操作によって第三者を攻撃する破壊工作である。

二〇一三年版はそれらの目的以外に、意図しない情報や誤った情報の爆発的な流布、テロリズムからサイバー攻撃やグローバルガバナンスの破綻まで、サイバーリスクがさまざまな技術および地政学リスクの中心に位置していることが示されている。図の「グローバルリスクマップ2013年」がそれである。昨年および今年の一〇大技術リスクのうち四つ（重要システムの故障、サイバー攻撃、大規模なデータの不正利用や盗用、誤った電子情報の大々的な流布）がシステムや情報に帰するものである。企業として想定されるリスクとしては、コンピュータセキュリティ漏洩による他社への法的責任、個人情報漏洩による他社への法的責任、データや情報の喪失や損傷、システム中断に伴う売上や利益の喪失あるいは中断をさせないような防御、防衛体制を敷くための臨時費用の捻出、中断に伴うステークホルダーからの評判やブランド力の低下、などが挙げられる。

（注）ウィルスなどによって多くのパソコンやシステムに遠隔操作できる攻撃用プログラム（ボット）を送り込み、外部からの指令で一斉に攻撃を行わせるネットワークのこと。

外部のみならず内部によるサイバー攻撃の脅威

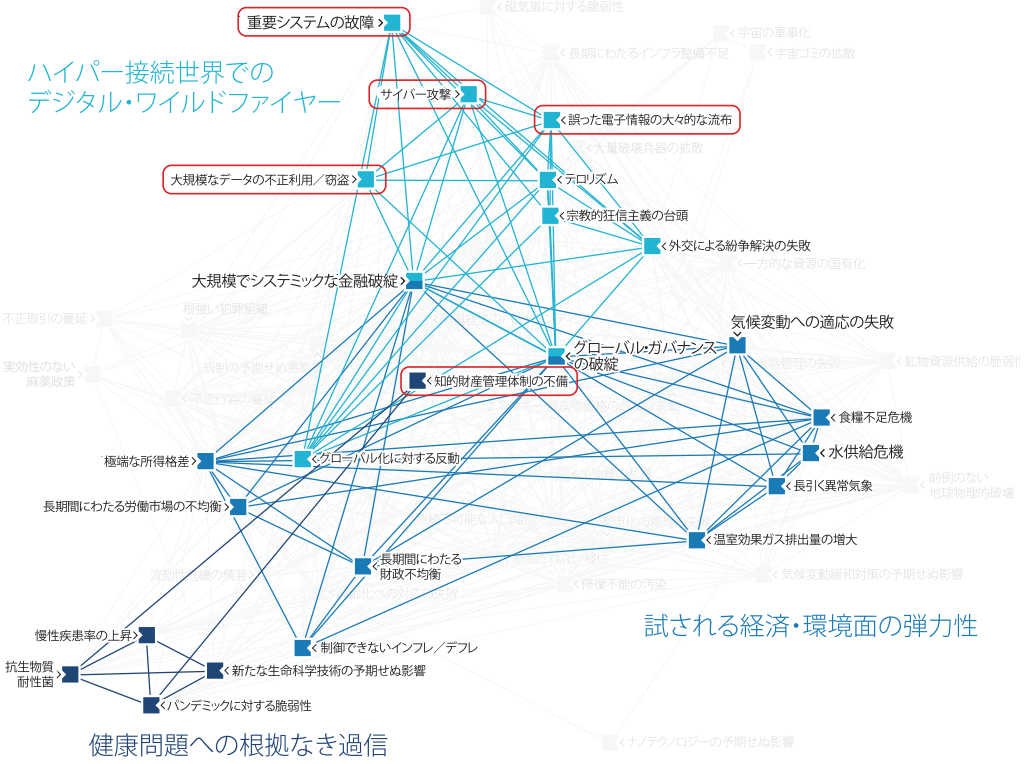
サイバー攻撃は外部から受けるものという意識が働きがちだが、実際には内部すなわち社内からも十分に発生しうることも忘れてはならない。不道徳な社員や注意力の散漫なスタッフのコンピュータ操作によって、データが盗用されたり間違った情報が外部に流出するリスクも、決して頻度は低くないばかりか、一度発生すればその経済的損失は計り知れない。ただし、これらの内部から発生するサイバー攻撃は、リスクコントロールの観点からすれば、無差別に攻撃する外部の者による犯行に比べれば、対策に講じるコストも莫大ではなく、社員のビジネスマナー教育や、システムのアクセス制限や監視体制を敷くことによって対応が可能である。

サイバーリスクの転嫁手段としての保険の普及度合い

インターネットや情報メディアの急速な発展によって、情報の伝達スピードは一昔前とは比べ物

にならないほどの速さとなり、一度発信された情報を受け取った人々は、それらを正しいものだと思い込む傾向が強い。間違った情報を発信した当事者が、仮に間違いに気付き、訂正を加えたとしても、それが浸透する前に間違った情報が予想以上に拡散してしまうことは過去にも数多く起きている。

●グローバルリスクマップ2013年（サイバーリスクに関する事象をハイライト）



出所：世界経済フォーラム

それらのリスクを全て保険に転嫁することは不可能であり、特に日本国内では未だ〝サイバーリスク保険〟なる保険商品はあまり流通していない。既存の企業向け財物保険や賠償責任保険などで斯様なサイバーリスクがカバーされていると期待する向きも多いが、一般的にはサイバー被害は従来の保険契約ではカバーされないというスタンスを取る場合が多い。米国の連邦高裁の昨年九月の判決では、従来の身元信用保険で応訴費用を支払う義務はないとの保険会社の主張は退けられたが、その後はかなりの保険会社が該当する保険商品の約款にサイバーリスクは対象外であることを明記し始めてきている。日本でも最近紹介され始めてきたサイバーリスク保険は、その拠出される保険会社からの保険限度額から、大企業より中堅・中小向きのプログラムになっている。

比して米国では年商一、〇〇〇億円以上の企業もかなり加入してきており、かつ前年度に比べても二〇一二年度は全業種三〇億円程度、リスクが集積しやすい通信、メディア、テクノロジー業界では六〇億円、金融機関は五〇億円弱とそれぞれ買い増しの事実がある。当然ながらリスクの発生頻度や程度から鑑みて、業種によってリスクコストはかなりのばらつきがあることは明らかであり、コスト検証を十分にする必要はある。保険購買を優先させるのではなく、まずは軽減・コントロールできる施策を打つこと。前述の教育や監視もコントロールの一手段である。

先月中旬に世界経済フォーラムが主催したサイバーリスクの実態把握と対策検討の会議が東京で開かれ、日本国内の政財界、学術界の有識者が一堂に会した。民間主導でサイバーリスク転嫁が難しいのであれば、政府管掌による制度設計もあり得るとのこと。財界、学術界などの各界と各国政府が、共通認識としてサイバーリスク対策を講じないことには、抜本的な解決の糸口は見つからないだろう。