サイバーセキュリティとリスクマネジメント
―事業中断による財務インパクトとリスク転嫁手段の検証の重要性―

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

情報システム技術の革新とさまざまな分野での利用によって、情報通信は国家・社会・経済・文化などほとんどすべての日常活動の支えとなってきている。とはいえ、より効果的・効率的なシステムを導入すれば、それを破壊・改竄・盗用しようとする負の力が新たに出現するのも世の常である。

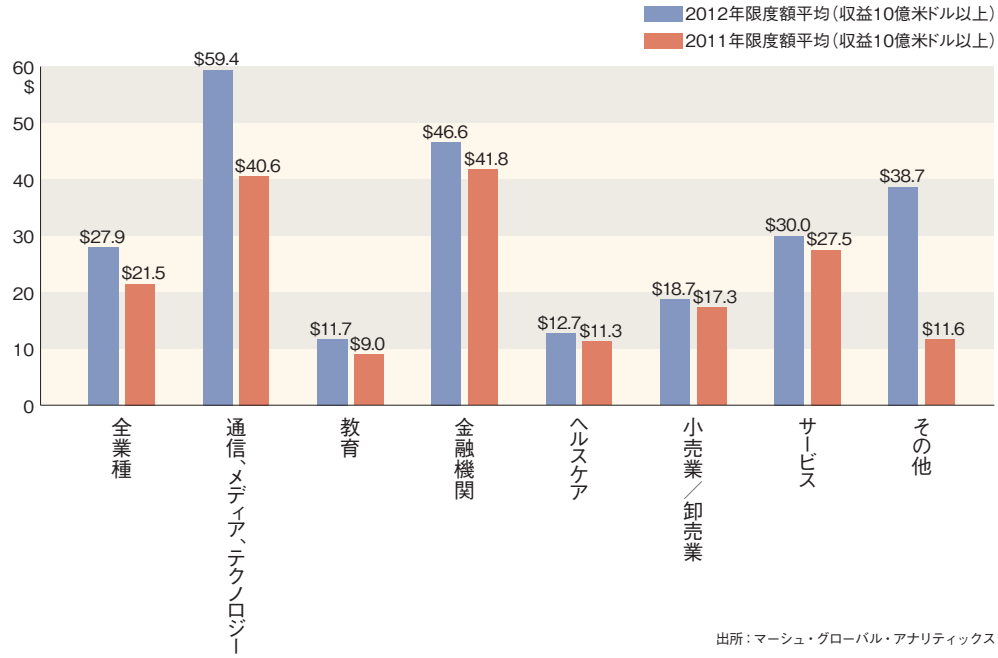
国や地域を越えて頻発・複雑化するサイバー攻撃に対して、国際的に連携しようという方針を一〇月上旬に日本政府が漸く発表した。情報セキュリティ政策会議で一〇月二日に〝サイバーセキュリティ国際連携取組方針〟が出され、サイバー攻撃に対する海外との情報共有やセキュリティに関する技術協力や提携について初めて対外的に明らかにした。これは世界経済フォーラムの年次総会で毎年紹介される〝グローバルリスク報告書〟において、数年前にサイバーリスクに対する国家間の協調を促してから漸く実現する運びとなった。政府にとって肝要なのは、国家機密データを保管するサーバーに侵入され、データが破壊や盗用されることのないように根本的な対策を協力して作り上げていくことだ。一方、企業は斯様なリスクにどのように対峙すれば良いのだろうか？既に被害を受けている企業は後を絶たず、後手に回って対策を講じている企業が多いことは否めない印象だ。サイバー攻撃による負の財務インパクトは図り知れず、CFOあるいは財務担当責任者は被害にあった場合の深刻度（SeverityやDamageabilityと呼ばれる）を認識しておくことが求められる。

企業、とりわけ製造業にとってサプライチェーンの途絶は、事業そのものを停滞させることになり経済的損失ばかりか企業の存続にまで大きな影響を与えかねない。英国の事業継続協会（Business Continuity Institute: BCI）の調査報告書『サプライチェーン・レジリエンス2012』に記載されている〝途絶の影響を受けた企業の主要原因別割合〟によれば、ITや通信の計画外の機能停止はサプライチェーンの混乱を悪化させる最大の原因であり、五二％の企業が影響を受けたと回答している。悪天候や地震、製品汚染、輸送網の途絶などの混乱を引き起こすさまざまな潜在的な要因の中で、ITおよび通信の機能停止が他の阻害要因を押さえて上位を占めている。さらに、データの漏洩やサーバーへの攻撃に起因する比較的小規模なシステム障害が、火災や暴動と同様に事業に大きな損害を与える可能性があると指摘している。

特筆すべきポイントとして、サイバー攻撃は必ずしも第三者による行為とは限らないということだ。最近は専ら外部からの侵入者や破壊者がサイバー攻撃を仕掛けるという意識が強いが、果たして、内部（つまり社員や関係者）の者による過失あるいは故意による犯行もシナリオの一つとしては想定しておかねばならない。それらを食い止める手立てはシステムそのものに防御策を講じたり、社員教育を徹底してモラルの欠如に至らないような継続的な啓蒙活動が必要であることは言うまでもない。それでも巧妙な手口による犯行や内部犯罪を根絶させることは不可能である。そのためにリスク転嫁の一つであるサイバー保険の導入も視野に入れる、あるいは研究しておくことを強くお勧めする。これは昨今、欧米では一般的になりつつあるサイバーリスク対策の一つである。詳細については本編では割愛するが、現在の一般的なサイバー保険契約では、法廷費用

や臨時費用を含むシステムやコンピュータの機能停止またはサイバー攻撃によって生じた減収の補償も可能である。従来型の保険ではカバーできないシステムやデータ使用に起因するリスクによる直接損害や損害賠償を補償する。欧米企業の二〇一一年度と二〇一二年度のサイバー保険を導入した際の賠償限度額の推移は図の通りだ。高まるリスクに備えるために限度額がより高額化してきていることと、それを支える保険会社が高額な限度額の引受に対して以前より前向きな姿勢が窺える。

●サイバー保険を導入した際の賠償限度額の推移



出所：マーシュ・グローバル・アナリティクス

いつ起こるかわからない巨大損害に企業として備えるために、次の四点をぜひ実践していただきたい。

一、サプライチェーンの分断（含むグローバル）による予想最大損失シナリオと財務的インパクトの把握

二、株主価値を守る上で、死守せねばならない財務指標を毀損させないため辛うじて許容できる損失額の把握

三、災害時の優先的に復旧すべき事象の事前決定および社内共有

四、有事に真の意味で機能する事業継続復旧プランの構築と、その定期的な訓練や見直し

多くの企業が情報システム技術の利用に伴う情報サイバーリスクを認識している。しかし、ソーシャルメディア・ネットワークに起因するリスクについては、いまのところ明確な認識には至っておらず、また、社員に対しても的確な指示やそれに類する企業の指針を制定していないのが実情だ。無防備な状況では、次のようなリスクに企業が晒される危険がある。

一、著作権付・商標付の情報がソーシャルメディアユーザーに共有されることによる高価値の知的財産の不当利用に対する損害

二、社員個人のソーシャルメディアでの中傷的な発言等による人格権侵害リスク

三、決算発表などの企業にとって重要な時期の事業活動に関する不正確な情報や作為ある情報の拡散

四、企業の業務慣行について、瞬時に広がる風評・悪評

単純にソーシャルメディアとネットワークから企業が撤退しても、顧客や他人がその企業について話題にしなくなるわけではない。また、企業内のシステムで社員による利用を遮断しても個人のPCや携帯電話などの端末を使ってネットワークにアクセスすることは可能である。したがって、ソーシャルメディア・ネットワークに関する指針の制定は斯様なリスクを軽減する上でも、可及的速やかに行うことが肝要であろう。