保険・年金フォーカス

サイバーリスク保険の普及

サイバーリスクは、保険でどこまでカバーできるのか?

保険研究部 主任研究員　篠原　拓也
(03)3512-1823　tshino@nli-research.co.jp

1――はじめに

近年、世界的に、サイバーリスクが高まっている。各国の政府・自治体、企業、個人において、サイバーテロへの対策が、重要な課題として認識されている。ハッカーは、ネット上で、常に新たなウィルスを開発したり、ハッキング技法を編み出したりして、様々なサイトに、不正アクセスやサイバー攻撃を仕掛けている。このため、企業等は機密情報や、顧客等の個人情報の流出などで、いつ、どのくらいの規模の損失が発生するか、予測できない状況となっている。

そこで、このサイバーリスクに備えるために、欧米では、サイバーリスク保険が導入されている。その普及の伸びは大きく、サイバーリスク対策の重要性の認識が浸透しつつあることを物語っている。日本でも、一部の損保会社が、企業向けに、サイバーリスク保険を販売している。

本稿では、サイバーリスクの状況と、それに備えるサイバーリスク保険について、近年の動向を見ていくこととしたい。

2――サイバーリスクとは

まず、サイバーリスクについて、その内容や、近年の発生状況を概観することとしたい。

1｜サイバーリスクは様々な形で進化し、政府や企業等にとって、大きな脅威となりつつある

インターネットの拡大を通じて、世界中で、コンピューター、スマートフォン、タブレットが接続されている。様々な情報が、デジタルデータ化される。そして、日々、膨大な量のデータが、通信されている。政府・自治体、企業、個人にとって、これらの情報を通じた、事業運営や活動が不可欠となりつつある。中でも、企業は、機密情報や顧客情報を多く抱え、その保護や管理に力を入れている。

一方、それらを狙った、サイバー犯罪は様々な形で進化し、中には、政府や企業等にとって、大きな脅威となるものも出てきている。悪意をもって他人のコンピュータのデータやプログラムを盗み見たり、改竄(かいざん)・破壊などを行うことが、その中心となっている。主なサイバーリスクとして、次の図表のようなものが挙げられる。

図表 1. 主なサイバーリスク

	内容	最近発生した事例（国内）
不正アクセス	利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともある。	日本年金機構が不正アクセスを受け、約 125 万件の個人情報が流出。（2015 年 6 月公表）
標的型攻撃	特定の組織を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取しようとする攻撃。この攻撃では、標的の組織がよくやり取りをする形式のメールを送りつけ、そこについている添付ファイルやリンクをクリックさせ実行させ、そこからマルウェア配布サイトに誘導するなどの手口がよく使われる。	国内の大学で、学内のコンピュータのマルウェア感染により、3000 名以上の個人情報が流出。（2015 年 6 月公表）
標的型諜報攻撃	国の経済や安全保障等に影響を及ぼす組織情報を窃取する活動を背景にし、特定目標組織を継続的に情報偵察する一連の攻撃。目標特定のための情報偵察、業界等分野ごとに散弾的な攻撃、特定した目標を継続的に諜報するための攻撃、がある。	宇宙航空研究開発機構に対する攻撃により、ウィルス感染した端末が業務中に表示した画面情報が流出。（2012 年 3 月公表）
不特定目標攻撃	不特定目標に対し、主に金銭目的のために個人情報を窃取する攻撃。	迷惑メール、Web サイト閲覧によるウィルス感染が多発
DDoS 攻撃[1]（ディー・ドス攻撃）	Web サーバやメールサーバなどに対して、複数のコンピュータから大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークに過大な負荷をかけ、使用不能にする。同様の攻撃方法である DoS 攻撃は、1 台のコンピュータから実行するもの。DDoS 攻撃の場合は、第三者のコンピュータを感染させておくなどして、攻撃者の指示によって、複数のコンピュータが一斉に攻撃する。	成田国際空港や中部国際空港などに、大量のデータが送りつけられ、ウェブサイトの閲覧に、障害が発生。（2015 年 10 月発生）
フィッシング詐欺	実在の金融機関（銀行やクレジットカード会社）、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、住所、氏名、銀行口座番号、クレジットカード番号などの重要な情報を入力させて詐取する行為のこと。	メールを送りつけ、実在の銀行を語るフィッシングサイトに誘導する事案が発生。（2012 年頃より頻発）
なりすまし	他の利用者のふりをすること。または、中間者（Man－in－the－Middle）攻撃など、他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられる。	国内のネット通販事業会社で、なりすましによる不正アクセスにより、最大 15 万件以上の顧客情報が流出した可能性。（2013 年 10 月公表）
ランサムウェア	金銭目的の不正プログラムのこと。感染すると、端末の一部機能を使用不能にしたり、ファイルを暗号化して使用できなくしたりする。そして、それらを使用可能とするための、身代金を要求してくる。	個人・法人を問わず、被害が多発。1,000 万円以上の高額の身代金を要求するケースも発生。（2015 年頃より頻発）

※ 「国民のための情報セキュリティサイト」（総務省，http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html）、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド　改訂第 2 版」（独立行政 法人情報処理推進機構セキュリティセンター，2011 年 11 月）、「ランサムウェアの説明動画の公開について」（警察庁，平成 28 年 1 月 29 日）をもとに、一部改変の上、筆者作成

2｜サイバー犯罪による損害額は、世界全体で年間 4,000 億ドル以上

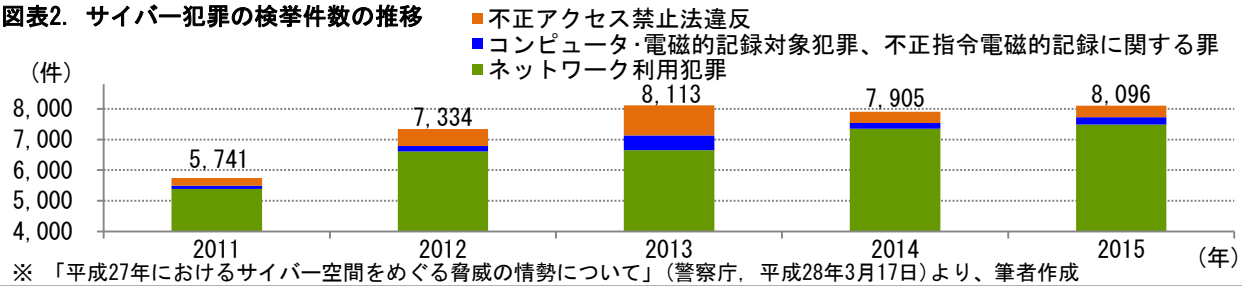
サイバー犯罪は、世界的に拡大している。2014 年に公表された調査報告[2]によれば、年間の損害は、4,000 億米ドル以上とされている[3]。同報告は、国別の損害額も示している。国内総生産（GDP）に対する損害額の比率で見ると、ドイツが 1.60%と高い。次いでオランダが 1.50%、ノルウェーが 0.64%と、一部のヨーロッパ諸国で高くなっている。主要国では、アメリカは 0.64%、中国は 0.63%、イギリスは 0.16%、フランスは 0.11%などとなっている。日本は、0.02%と、他国に比べて低水準とされている。

[1] DDoS は、Distributed Denial of Service の略。DDoS 攻撃は、分散型サービス拒否攻撃を指す。
[2] “Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II”（Center for Strategic and International Studies, June 2014）より。
[3] 損害額の見積もりは、幅をもって示されている。少なくとも 3,750 億米ドル、最大で 5,750 億米ドルとされる。

3｜日本国内でも、サイバー犯罪は増加している

しかし、日本国内でも、ここ数年、サイバー犯罪の件数は増加した。警察庁の発表によると、2015年のサイバー犯罪の検挙件数は、8,096件に上った。特に、ネットワーク利用犯罪が増加している。

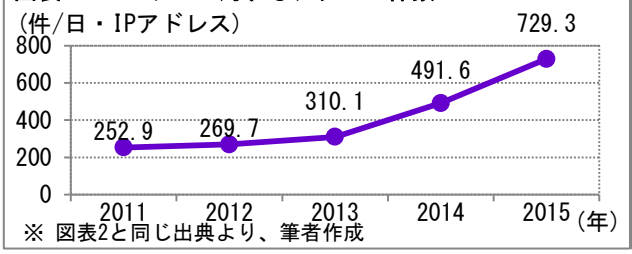
図表2. サイバー犯罪の検挙件数の推移



※ 「平成27年におけるサイバー空間をめぐる脅威の情勢について」（警察庁，平成28年3月17日）より、筆者作成

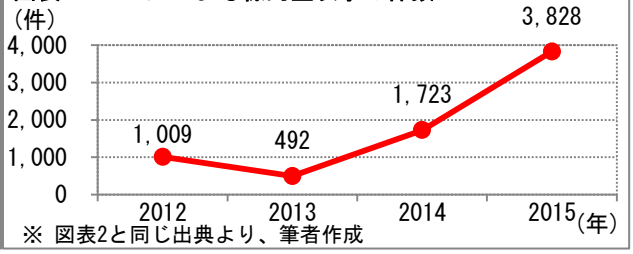
また、インターネットとの接続点に設置されたセンサーに対するアクセスの件数（1日・1IPアドレスあたり）は、2015年に急増している。ルーターや、監視カメラ等の組込み機器を標的とした、探索行為等が増加している。それと同時に、メールによる標的型攻撃の件数も、大きな伸びを見せている。

図表3. センサーに対するアクセス件数



※ 図表2と同じ出典より、筆者作成

図表4. メールによる標的型攻撃の件数



※ 図表2と同じ出典より、筆者作成

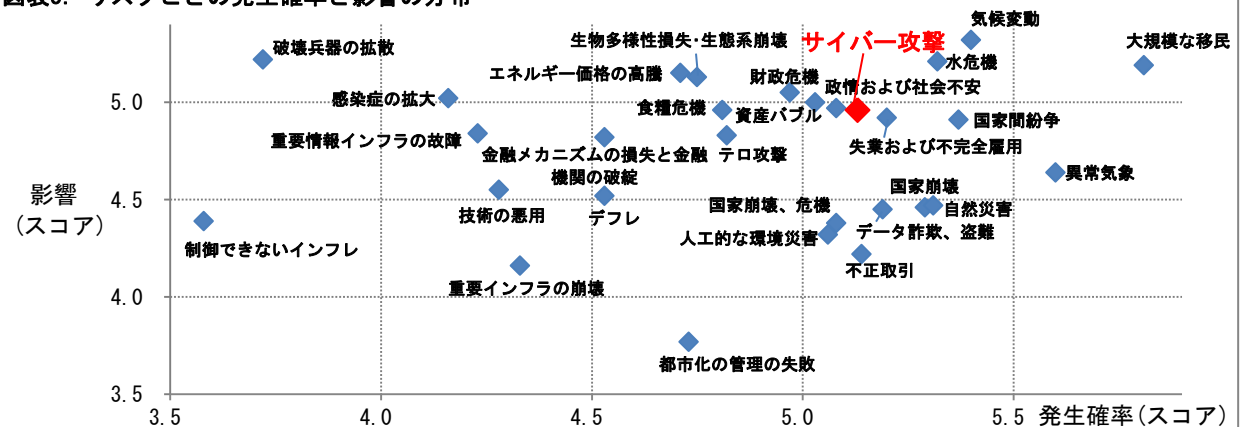
3――サイバーリスクの特徴

サイバーリスクには、他のリスクには見られない特徴がある。簡単に、それらを見ていこう。

1｜サイバーリスクは、他のリスクに比べて、発生確率が高く、影響が大きいとされている

前章で見たとおり、近年サイバーリスクは国内で増加している。一方、仮に発生した場合、100万件を超える個人情報が流出して、その対応に追われることもあるため、政府や企業に与える影響は大きい。世界経済フォーラムが、2016年1月に公表した、グローバルリスクについての報告書でも、サイバー攻撃は、発生確率、影響とも、他の様々なリスクの平均よりも高い、と位置づけられている。

図表5. リスクごとの発生確率と影響の分布



＊ 発生率と影響は、担当者が評価したスコアであり、各リスク間の相対的な位置づけを示している

※ “The Global Risks Report 2016 11th Edition”（World Economic Forum）のFigure 1をもとに、筆者作成

2｜サイバーリスクは、予想損害額の見積もりが難しい

サイバーリスクによる損害は、様々な形で現れる。例として、企業が攻撃を受けて、機密情報や、顧客情報が漏洩(ろうえい)して、損害を被るケースを考えてみよう。

個人情報の漏洩に対して、被害者への損害賠償のための賠償金が必要となる。もし、顧客との間で訴訟が発生すれば、そのための費用もかかる。原因調査や、再発防止策の策定のためにも、弁護士相談や、臨時雇用職員の人件費、社告のための費用など、様々な負担が発生する。また、その対応のために、通常の業務の一部を一定期間停止することになれば、その間の機会利益の喪失や、工場ライン等の事業維持の費用も発生する。

機密情報については、その流出に伴ない、市場での優位性を失うことや、風評被害を被ることもあり、その場合の損害は計り知れない。

これらの損害は、事案ごとに発生の仕方が異なる。従って、過去の事例のうち、将来の予想の参考になる要素は限られる。このため、サイバーリスクは、予想損害額の見積もりが難しいと言える。

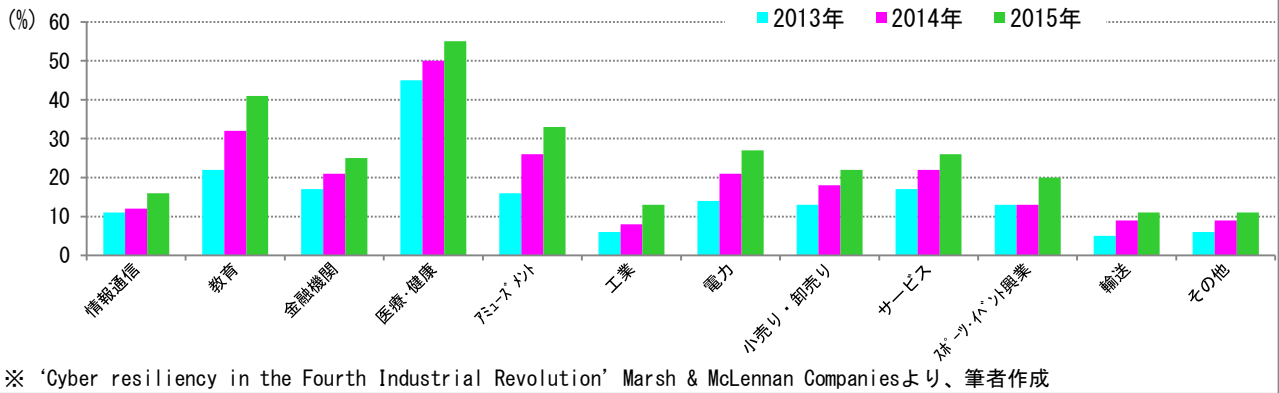
4――日米のサイバーリスク保険の動向

アメリカでは、サイバーリスク保険の販売が進んでいる。日本でも、損保会社で、サイバーリスク保険の取り扱いが始まっている。これらの動向を、見てみよう。[4]

1｜アメリカでは、今後もサイバー保険への加入が進む見通し

アメリカでは、1997 年に AIG 社がサイバーリスク保険を販売した。その後、約 20 年の間に、サイバーリスクの認識が徐々に拡がってきた。近年、この保険の加入率は上昇している。保険仲介大手の Marsh & McLennan 社が、アメリカの自社顧客に対して行った調査[5]によれば、2014～15 年にかけて、サイバー保険の顧客が 27%増加した。2013～14 年にかけての 32%、2012～13 年にかけての 21%に続き、高い増加率を維持している。この結果、保険加入率は、約 2 割となっている。ただし、これは、まだ 8 割の顧客が未加入とも言え、今後もサイバー保険への加入の動きが進むものと考えられる。なお、産業別の加入率を見ると、医療・健康分野(55%)、教育分野(41%)などが、高率となっている。

図表6. サイバー保険の加入率（産業別）



※ ‘Cyber resiliency in the Fourth Industrial Revolution’ Marsh & McLennan Companiesより、筆者作成

[4] なお、保険業界では、保険会社自身が直面するサイバーリスクについて、リスク管理の議論が進められている。例えば、2016 年 8 月には、保険監督者国際機構(IAIS)が、このテーマについて、イシューペーパー‘Issues Paper on Cyber Risk to the Insurance Sector’を公表している。

[5] ‘Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies “The Role of Cyber Insurance in Risk Management”’ Matthew P. McCabe (Marsh, LLC, March 2016)より。

2｜日本でも、サイバーリスク保険の取り扱いが始まっている

日本では、サイバーリスク保険の開発がアメリカよりも遅い。2012 年に、AIU 保険会社が、このリスクに対する保険を発売した。しかし、その後 2 年以上の間、あまり販売は進まなかった[6]。

その後、世界的なサイバー犯罪の増加を受けて、2015 年に、複数の損保会社で、企業向けのサイバーリスク保険の取り扱いが始まった。これらの保険は、サイバー被害に遭った場合の様々な費用を補償する。サイバーリスクには、国境がないため、海外での損害賠償請求訴訟に関する、賠償金・争訟費用も、補償対象としている点が、これらの保険の特徴といえる。ただし、第 2 章で見たとおり、日本では、サイバー犯罪は増加しているものの、その損害額は他国に比べて低水準にあり、サイバーリスクについての企業側の認知は、まだ道半ばといえる。今後、海外でビジネスを展開する企業等を中心に、サイバーリスク対策の必要性の認識が高まるに連れて、この保険のニーズも高まるものと思われる。

図表 7. 日本で取り扱われているサイバー保険

	AIU	東京海上日動	三井住友海上 あいおいニッセイ同和損保	損保ジャパン日本興亜
商品名	CyberEdge （サイバーエッジ）	サイバーリスク保険	サイバーセキュリティ 総合補償プラン*	サイバー保険
発売時期	2012 年 12 月	2015 年 2 月	2015 年 9 月	2015 年 10 月
補償内容 （主なもの）	損害賠償責任（損害賠償金、争訟費用等） 危機管理対応（事故原因調査・被害拡大防止のための費用、データ復元費用、コンサルティング費用等） 情報漏洩対応（見舞金・見舞品費用、社告のための費用、行政対応費用等） 事業中断対応（事業中断に伴う喪失利益、営業継続費用等）**			
海外訴訟	海外での損害賠償請求訴訟に関する、賠償金・争訟費用も、補償対象			

＊　三井住友海上の場合。あいおいニッセイ同和損保では、ｻｲﾊﾞｰｾｷｭﾘﾃｨ保険（IT 業務賠償責任保険［拡張補償プラン］）の商品名で販売。
＊＊　事業中断対応については、オプションでの補償として取り扱われている場合もある
※　各社の発売時のプレス資料、募集パンフレット等を参考に、筆者作成

5――おわりに（私見）

現在、エンタープライズ・リスク・マネジメント(ERM)が徐々に浸透する中で、企業等の事業運営において、様々なリスクが取り上げられ、その発生確率・影響の評価や、リスクへの対応策の検討が進められている。これまで、サイバーリスクは、新たなリスク(エマージング・リスク)の１つと捉えられてきた。今後、このリスクは、増大して、より一般化し、深刻なものとなる可能性が高い。そのため、企業等は、これまで以上に、サイバーセキュリティの備えを充実させることが、必要となろう。

そのためのツールとして、サイバーリスク保険の活用が考えられる。日本では、この保険の拡販が進められており、そのニーズは高まるものと思われる。また、現在は、保険加入が企業に限られているが、今後は、個人事業主等にも、サイバーリスク保険を提供することが考えられる。

サイバーリスクの動向とともに、それに備える保険の普及の状況についても、引き続き、注目していく必要があろう。

[6] サイバーリスク保険の国内での普及については、「日本でさっぱり売れない『サイバーセキュリティ保険』、普及への壁」清嶋直樹（日経ｺﾝﾋﾟｭｰﾀ，2015 年 3 月 18 日）などで取り上げられている。