地域分析レポート

米国サイバーセキュリティー対策の行方

2017年11月14日

ジェトロ海外調査部米州課
仁平 宏樹

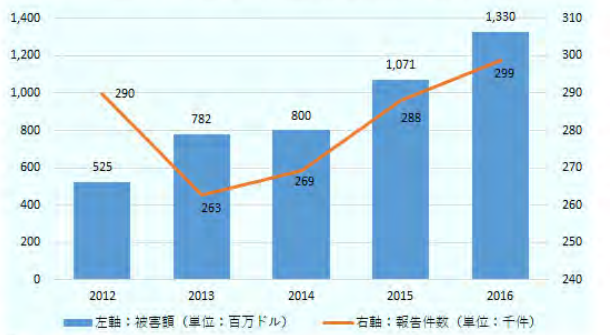
米国では企業や政府の事業活動を脅かすサイバーリスクの深刻度が増している。サイバー犯罪被害額は米国全体で13億ドルに達し、情報漏えいコストは平均735万ドルにも及ぶ。9月には、大手信用調査会社エクイファックスがサイバー攻撃により米国民の半数に近い1億 4,550 万人の個人情報が流出した可能性を公表した。日に日に高度化するサイバー攻撃に対して、企業では政府との脅威情報の共有やセキュリティー対策への投資が進む。連邦議会と政府は政府機関のサイバーセキュリティー強化を図る考えだ。

＜増え続けるサイバー犯罪＞

米国の国家サイバーセキュリティー意識向上月間である10月4日、全米商工会議所主催の「第6回サイバーセキュリティーサミット」に登壇したエレイン・デューク国土安全保障長官代行は「インターネットに接続されたデバイスの数が増え、敵の能力が向上するにつれてサイバー脅威が拡大している」と語ったが、サイバー脅威の拡大による被害は統計上でも如実に表れてきている。

米国インターネット犯罪センター（IC3）によれば、2016 年のサイバー犯罪による被害額は 13 億ドル（前年比 24%増）を超え、報告件数も約 30 万件（同 4%増）と近年右肩上がりが続く（図 1）。被害額は IC3 に寄せられた事案に基づく値であることから潜在的には 90 億ドル近い被害が出ていると指摘する専門家もいる。

図1：サイバー犯罪報告件数および被害額の推移



資料：IC3より作成

州別では、カリフォルニア州が被害額、報告件数ともに 1 位で千人に 1 人が何らかのサイバー犯罪被害に遭っている計算だ。人口が集積するニューヨーク州やフロリダ州、テキサス州などに被害が集中している（表 1）。

表1：サイバー犯罪被害上位5州（2016年）　（単位：人/人口、10万ドル/被害額）

順位	州名	人口	被害額	件数
1	カリフォルニア	39,250,017	2,551	39,547
2	ニューヨーク	19,745,289	1,062	16,426
3	フロリダ	20,612,439	888	21,068
4	テキサス	27,862,596	771	21,441
5	バージニア	8,411,808	491	8,068
全米		323,127,513	1,330	298,728

注:　人口は2016年1月推計値
資料:　IC3「2016 IC3 Annual Report」を基に作成

サイバー犯罪種別では、「ビジネスメール詐欺（Business E-mail Compromise（BEC））」と呼ばれる電子メールを使って企業から海外送金等により金銭を搾取する手口が急増している。報告件数は前年比 53%増の 1 万 2,000 件、被害額は 43%増の 3 億 6,000 万ドルで被害額と

しては最大だ。

連邦政府では、2016 年 9 月にインターネットに接続し情報をやり取りする IoT 機器を標的にした大規模なサイバー攻撃が起きたこともあり、IoT（注）サイバーセキュリティー対策について関心を強めている。10 月 19 日に米国商務省所管の国立標準技術研究所（NIST）が主催した「IoT サイバーセキュリティー会議」では、産学官の関係者から、NIST が開発したサイバーリスクの管理と低減を図るサイバーセキュリティーフレームワークを IoT サイバーリスクに対応したものに刷新を求める声や、政府に IoT 機器のリコール権限を付与する提案等がなされている。就任前からサイバーセキュリティー対策強化の意向を示していたトランプ大統領は 2017 年 5 月 11 日、政府のサイバーセキュリティー強化と重要インフラをサイバー攻撃から守ることを目的に、連邦政府機関の責任者に対してサイバーセキュリティーフレームワークを用いてリスク管理計画を示す報告書を国土安全保障長官と行政管理予算局長に報告することを義務付ける大統領令を発出した（2017 年 5 月 11 日大統領令第 13800 号）。

議会においても、超党派による政府機関が購入する IoT 機器の最低限のサイバーセキュリティー運用基準を示した法案（ Internet of Things（IoT）Cybersecurity Improvement Act of 2017）や IoT サイバーセキュリティー対策を盛り込んだスマートシティーや自動運転関連法案の検討が進められている。政府、議会双方とも政府機関のサイバーセキュリティー強化で方向性は一致しており、IoT へのサイバーセキュリティー対策も含め迅速な政策決定が期待される。

＜政府と企業の脅威情報共有には課題も＞

米国では、サイバー攻撃の事前予防措置として、政府主導でサイバー脅威や脆弱（ぜいじゃく）性に関する情報共有プラットフォームが構築されてきた。1998 年当時のクリントン大統領が重要インフラへの物理・サイバー攻撃の可能性を懸念し、情報共有の組織づくりを推奨したのが始まりと言われる。これを受け、金融サービス、通信、電力、緊急時対応の 4 分野で情報共有分析センター（ Information Sharing and Analysis Center: ISAC ）が設立され、現在までに航空産業や不動産、自動車産業など 23 センターまで拡大を見せている。2015 年 2 月にはオバマ前政権が、センターごとに運営され、情報共有も参加者に限られていた ISAC を補完し、法務や会計などの分野横断または地域間、企業規模間、そして民間企業と政府機関が自主的に、可能な限りリアルタイムで情報共有できる情報共有分析機関（Information Sharing and Analysis Organization: ISAO）の設立を提唱する大統領令を発出。同年 10 月には情報共有のガイドラインづくり等を担う非政府組織の ISAO 標準化機構（Information Sharing and Analysis Organization Standards Organization）が設立され、新たな枠組みが動き出した。

同機構によれば、金融分野の情報共有から開始した後、業界の垣根を越えて法務やエネルギー分野とも情報共有するグローバル・レジリエンス・フェデレーション（Global Resilience Federation）やサイバーセキュリティー対策をリードするバージニア州を含む中部大西洋地域横断的に取り組みを進めるミッドアトランティック・サイバー・センター（Mid-Atlantic Cyber Center）など現在までに27のISAOが組織されている。

一方、政府と企業の情報共有に当たっては課題も聞かれる。情報共有に当たって、サイバー脅威を他の団体や政府と自発的に情報共有した企業は、2015年末に成立したサイバーセキュリティー情報共有法 （Cybersecurity Information Sharing Act（CISA））に基づき法的に保護される。また、国土安全保障省（DHS）は、自動的に匿名化されたサイバー脅威情報を迅速に共有できる仕組みAutomated Indicator Sharing（AIS）を2016年3月に構築した。しかしながら、依然としてプライバシー保護や賠償責任への懸念からAISから情報を受信するだけの企業や、そもそも情報を受信するために必要なサーバー構築技術を有していない企業が多いようだ。また、AISに参加するための政府手続きの迅速化を求める声や、政府側がサイバー脅威情報に犯人情報が含まれることを理由にその多くを機密扱いとし、結果的に企業が受け取る情報が制限されているとの指摘もある。

これらの課題は、前述の「第6回サイバーセキュリティーサミット」でも主要なテーマの一つとして意見交換がなされ、登壇者の一人デイブ・マッカ―ディ米国ガス協会会長兼CEOは「エネルギー企業は犯人情報に興味はない。（興味があるのはサイバー）脅威だけだ」と述べている。このほか、IBMでは脅威情報を5分以内に発表する取り組みを進めており、企業、政府機関とも脅威情報は可能な限り速く共有すべきだと同社は主張する。

＜「不可抗力」にはサイバー保険で対処を＞

自動車事故や自然災害と同様、「不可抗力」と言えるサイバーリスクには、発生後の補償も欠かせない。情報セキュリティーに関する独立調査機関ポネモン・インスティテュートがIBMの支援を受け実施した12回目の最新調査（2017年）によれば、米国のサイバー攻撃による情報漏えいコストは平均735万ドル（前年比5%増）に上り、世界平均362万ドルの2倍超だ。なお、米国48州にある情報漏えいに関する独自規制が、企業のコストを押し上げるとIBMは分析する。

そこで注目されるのが、サイバー保険だ。

米国におけるサイバー保険は1990年代半ばから商品化され、急速に変化するサイバーリスクに対応するため補償範囲を拡大してきた。

サイバー保険と既存の保険との差異は何か。全米保険協会によれば、サイバーインシデントに対して従来の財物保険や個別約款でも限定的な補償が受けられる場合があるものの、総合賠償責任保険の標準約款では、機密情報へのアクセスまたは開示によって生じる個人の侵害や広告侵害への補償は免責とされてきた。これでは十分にサイバーリスクに対応していないため、サイバー保険が開発されてきたのだという。

サイバー保険は、個別のニーズや使用する技術、関連するリスクに応じて企業ごとにテーラーメイドで作られ、契約者への損害と第三者への賠償責任も補償可能だ。補償対象には、データ損失・破壊や事業中断が含まれる（表 2）ほか、近年、企業しか利用できなかったサイバー保険を個人向けに販売を開始した保険会社もあるという。

表2：サイバーセキュリティー保険の補償対象

項目	補償内容
データ損失・破壊	ウイルス等の結果生じる貴重な情報資産の損害と破壊を補償。
事業中断	サービス拒絶のような事業継続を制限する企業ネットワークへの攻撃の結果生じる事業所得の損失を補償。臨時費用や法定費用、関連会社への妨害も含む。
賠償責任	以下の結果生じる、企業が被る弁護士費用、和解金、裁判費用、場合によっては懲罰的損害賠償金を補償。 ・クレジットカード、財務や健康関連情報などのデータ盗難によるプライバシー侵害 ・コンピューター攻撃の結果生じるコンピューターウイルスの感染またはその他負債で、第三者に財務上の損失を与えるもの ・第三者によるネットワークシステムの利用を不可能にするセキュリティーの欠陥 ・掲示板やチャットでのビジター投稿など、企業のウェブサイト上での、著作権または商標権侵害、名誉毀損（きそん）、中傷、その他の「メディア」活動の申し立て。サイトにある他企業のバナー広告も含む。
経営責任	新たに開発され、テーラーメイドで作られる D&O 商品には、広範なリスク補償を提供している。つまり、特に除外されない限り、役員の賠償リスクは補償される。サイバーリスクを含む取締役が直面するすべての賠償責任を補償。
サイバー恐喝	企業のネットワークに対する脅威の「解決」に要する費用を補償。恐喝者を突き止め、交渉するために雇うセキュリティー会社の費用も補償。ランサムウエア攻撃による被保険者の身代金の支払いは、典型的に個々の契約条件による。
危機管理	インシデント発生後の、企業の評判を再建するための広報支援または広告宣伝の費用を補償。消費者への通知費用やインシデント対応費用も利用できる。
犯罪懸賞金	企業のコンピューターシステムを攻撃した犯人の逮捕や有罪判決につながる情報に対して犯罪懸賞金を支払う費用を補償。
データ漏えい	データ漏えいの結果生じる費用や賠償責任を補償。規制上求められる法令順守や顧客の懸念に対処するための経営者向けサービスを利用できる場合もある。
個人情報盗難	顧客または従業員の個人情報が盗難された場合、個人情報盗難コールセンターの利用が可能。

注：　上記のほか、個々の契約内容により、内部と外部両方からの攻撃や被保険者を対象にしたウイルス等も対象となる場合がある。
資料：　全米保険協会「Threat and opportunity」を基に作成

サイバー保険市場も拡大が続く。調査会社 PwC の推定によれば、世界のサイバー保険市場（年間保険料）は、2018 年には 50 億ドル、2020 年までには少なくとも 75 億ドルまで成長することが見込まれる。また、米国企業の 3 分の 1 は何らかのサイバーセキュリティー関連の保険に加入しているという。

米国の同市場については、格付け会社フィッチ・レーティングスが 2016 年に 13.5 億ドルに達し、前年比 35%の増加を見せたとしている。

サイバー保険の加入を後押しするのは、サイバーリスクがビジネスに実害をもたらしている事実と経営層にサイバー保険の必要性が浸透しつつあることが要因のようだ。再保険会社パートナー・リーと調査会社アドバイゼンがサイバー保険加入者を対象に、同保険加入の理由を調査したところ、「他社のサイバー攻撃による損失の報道」が最大の理由となり、「サイバー攻撃に関する何らかの損害を経験」も理由の上位に位置している。

こうしたことから、当面、サイバー保険市場は好調を維持するものと考えられるが、もっとも懸念材料もない訳ではない。サイバーリスクの複雑さから、保険業界幹部はサイバー保険の需要に対応する同市場の引き受け能力には避けられない限界がある事実を認めているという（全米保険協会「Threat and opportunity」（2016 年 10 月））。

冒頭のエクイファックスは、1 億 4,550 万人の個人情報流出公表の翌日、株価が 14%下落、約 20 億ドル超の時価総額を失った。さらに、同社の CEO は辞任に追い込まれ、サイバーリスクの歴史上、最も高価な違反回復費用でその額は数十億ドルに及ぶとの現地報道も見られる。同社がサイバー保険に加入していたかどうかは定かではないが、経済的損失が莫大（ばくだい）であることは確かだ。

注： 本稿では、M2M の機械同士の閉じられたシステム内での相互連携ではなく、さまざまなモノをインターネット等のネットワークと接続することをいう。

執筆者紹介

ジェトロ海外調査部米州課

仁平 宏樹（にへい ひろき）

2008 年茨城県庁入庁。2017 年から日本貿易振興機構に出向し、海外調査部米州課勤務。

日本貿易振興機構（ジェトロ）発行
〒107-6006 東京都港区赤坂 1-12-32
アーク森ビル 6 階
Tel: 03-3582-5511

お問合せは

海外調査部 海外調査計画課 出版班まで
Tel: 03-3582-3518
E-mail: SENSOR@jetro.go.jp