米国におけるサイバー保険の現状

中沢 潔
JETRO/IPA New York

1　サマリー

Y2K 問題（ミレニアム・バグ）をきっかけに、米国では、1997 年に米保険大手 AIG 社が最初のサイバー保険（単独の保険商品）の販売を開始した。補償対象は、不正アクセス、ネットワークセキュリティ、ウイルス感染から始まり、2000 年台半ばには、IT フォレンジック（サイバー被害の調査）やクレジットモニタリング（ID 詐欺の損害補償）、顧客への情報通知コスト等に対する補償のほか、規制に対する弁護費用や罰金などに対応する補償も誕生した。2010 年台以降、大手企業を狙った大規模なデータ漏洩・侵害事件が増加する中、単独の保険商品としてサイバー保険を販売する保険会社の数も 60 社以上に増加している。

2015 年における世界のサイバー保険の市場規模は 17 億ドル（年間の総計上保険料ベース）で、米国の市場規模はその 90%（15 億ドル）を占める世界最大のサイバー保険市場である（日本は 2015 年度に 136 億円。）。米国企業全体におけるサイバー保険の加入率は 20～35%にとどまっている（日本の加入率は 2 割に満たない。）。業界別では、ヘルスケア、教育分野の企業の加入率が 40～50%で高率となっており、金融、小売業界がそれに続く。今後は、製造、エネルギー業界においてもサイバー保険への加入が大幅に増加するとの見通しを示しており、米国のサイバー保険市場は 2020 年までに年間保険料収入ベースで 56 億ドル規模に成長すると予測されている。

業界を問わず米国で情報漏洩被害に遭った企業の平均被害総額は 735 万ドル（前年比 5%増）で、情報漏洩インシデントの 47%は悪意のあるサイバー攻撃によるものであることが明らかになっている。

米国土安全保障省（DHS）は、保険会社により補償内容と保険料が大きく異なっていることに対し、企業のサイバーリスクをより正確に評価するための実質的なデータを保険会社に提供しある一定の基準のサイバーセキュリティ対策を行っている企業に対しては保険料を軽減するといった措置を積極的に講じることを推奨することを目的として、「サイバーインシデントデータ分析リポジトリ（CIDAR）」の構築を提案している。また、非営利の米外交シンクタンクである外交問題評議会（CFR）は、送電網に対するサイバー攻撃など、大規模で破滅的な影響を及ぼす恐れのあるサイバーインシデントに備えて政府がより積極的にサイバー保険の補強・普及につながる政策を施行すべきとし、連邦政府が公的に支援するサイバー保険プログラムを新設することを提案している。

保険業界では、WannaCry に感染した企業／組織のコンピューターシステムは、Microsoft 社がセキュリティパッチ（MS17-010）を 2017 年 3 月に公開していたにもかかわらず、その更新が行われていなかったことから、企業／組織がこうした既知のセキュリティ脆弱性問題への対応を怠った場合に、サイバー保険ポリシーにおいて過失怠慢による損害賠償補償を対象とするかについて再検討・議論されている。その他、個人を対象とする新たなサイバー保険の登場等の商品の多様化の動き、米国商工会議所によるセキュリティ格付け原則の発表等セキュリティリスク評価の統一性、正確性を高めようとする動きが出ている。

しかし、米国のセキュリティサービス企業の中には、こうした指針や基準が定められていない現況では、特に IT セキュリティ分野の関連予算が限定的な小規模企業にとって、非常に複雑で割高なサイバー保険への加入をサイバーセキュリティ対策として選択することは時期尚早であり、代わりにアプリケーションやネットワークの安全性を強化するシステム投資に注力することで情報漏洩の発生を予防する方が適切とする声もある。他方で、業界関係者及び組織の最高情報セキュリティ責任者（CISO）の間では、サイバー保険に加入する大きなメリットは、様々なサイバー被害・被害の補償にとどまらず、保険会社によるリスク管理プロセスにおけるセキュリティ向上計画の策定や従業員に対するデータセキュリティに関する研修サービス、詳細にわたるセキュリティの脆弱性評価などを通じて企業がセキュリティ対策を包括的に見直しサイバーセキュリティ対策や規制コンプライアンスを強化できることにあり、（サイバー保険に加入することで）結果的に企業は将来起こり得るセキュリティインシデントに伴うリスクを最小限に抑制できるとみる声もある。この際、CISO には、セキュリティ対策への投資対効果を示すためにファイアウォールの記録やマルウェア検出状況に関する報告を行うのではなく、コスト削減等の組織のビジネス戦略目標に照らして、ビジネスリスクを軽減し最も重要な資産やデータを守る具体的な方法及びビジネスに付加価値をもたらすセキュリティ対策について経営者に分かり易い言葉で率直な考えを提示する高いコミュニケーション能力が必要と考えられる。

日本においても、業種や売上高、補償限度額などによって変化する保険料に対する投資対効果が不明瞭であることが企業におけるサイバー保険の普及の妨げになっている要因の一つに挙げられており、企業がサイバーリスク評価やサイバー被害によるコスト推定を適切に行える環境を整えることが重要であると考えられる。

（参考）「サイバーセキュリティ経営ガイドライン」（改訂）
http://www.meti.go.jp/press/2017/11/20171116003/20171116003.html

2　米国におけるサイバー保険の誕生・発展の経緯

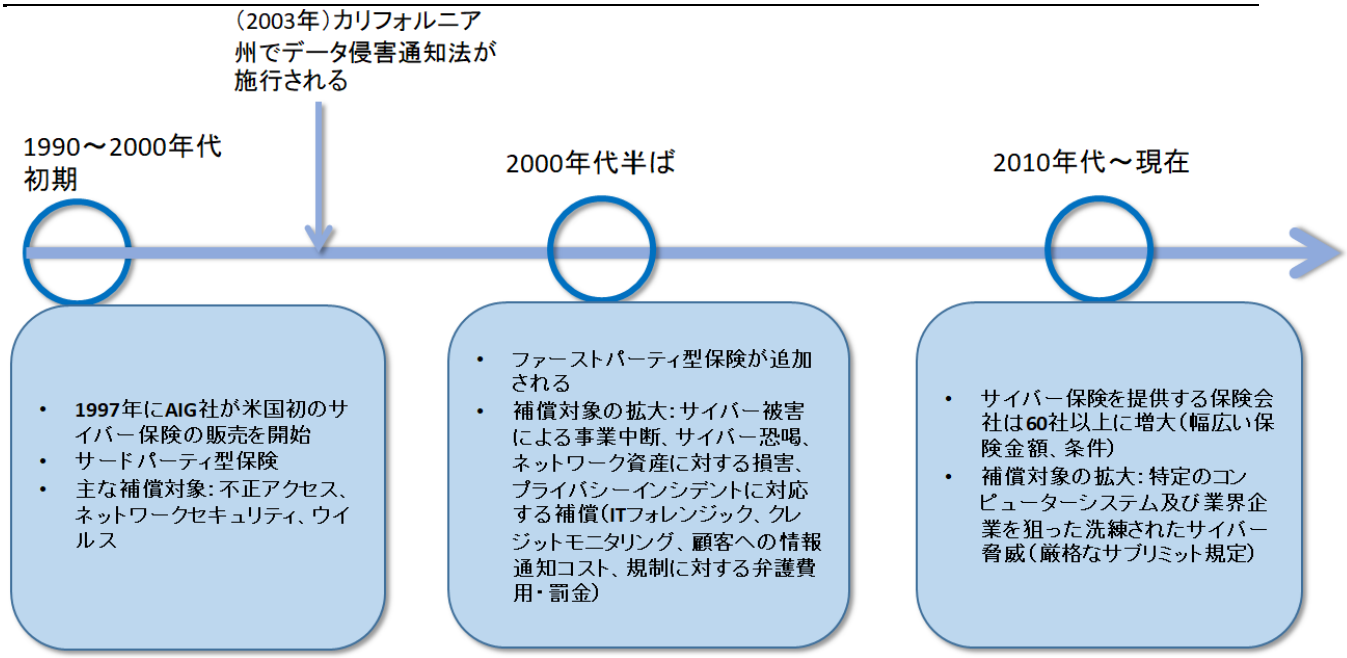
（1）　サイバー保険の起源

「サイバーリスク保険（cyber risk insurance）」又は「サイバー賠償責任保険（cyber liability insurance）」とも称されるサイバー保険は、サイバー攻撃による被害を受けた企業・組織の復旧にかかるコストを補償し、そのリスク負担を軽減することを目的に提供されている保険である。サイバー保険は、1980 年代から提供されているオンラインコンテンツ又はソフトウェア関連の様々な IT リスクをカバーするテクノロジーサービスプロバイダ向け情報システム保険である「Technology Errors and Omissions（テクノロジーE&O）」保険を起源とし、Y2K 問題（ミレニアム・バグ）をきっかけに単独の保険商品としての需要が高まり、米国では、1997 年に米保険大手 American International Group（AIG）社が最初のサイバー保険の販売を開始した[1]。

これらの最初のサイバー保険は、オンラインメディアやデータ処理のエラーを含むソフトウェア及びメディアリスクを補償する専門職業責任保険から発展したもので、2000 年代はじめにかけて、不正アクセスやネットワークセキュリティ、ウイルス関連のリスクを補償する保険も提供され始めたが、これらの保険は概して第三者に対する賠償責任（サードパーティ型）保険で、悪質な内部の従業員によるサイバーリスクや罰科金といった大部分の専門職業責任保険が補償する内容の多くを対象外としていたほか、サイバー攻撃に関する調査等、被保険者が直接受けるサイバー被害による費用を補填するファーストパーティ型補償も存在しなかった。サイバー被害による事業中断やサイバー恐喝[2]、ネットワーク資産に対する損害等を含むファーストパーティ型サイバー保険が登場するのは 2000 年代半ばに入ってからである。

図表 1：米国におけるサイバー保険の発展の推移

[1] http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878
http://www.insurancejournal.com/magazines/features/2014/09/22/340633.htm
[2]ランサムウェアなど、機密情報の流出・データの暗号化や削除・サービス拒否などといった悪意のある攻撃を行って、その攻撃を停止する条件として金銭の支払いを要求するサイバー犯罪を指す。



出典：各種資料を基に作成

（2） データ侵害通知法とサイバー保険の発展

米国におけるサイバー保険成長の背景には、個人情報の重要性への認識の高まりを受けて 2003 年 7 月にカリフォルニア州が米国初のデータ侵害通知法（Security Breach Notification Law）を施行したことが大きく影響している。同法は、データ侵害を受け、個人情報が漏洩した可能性があると判断される場合、各消費者にその旨を通知することを義務付け、不十分なサイバーセキュリティ対策等により発生したデータ侵害について企業に責任を負わせるもので、2005 年以降、他の多くの州も追従して同様の法を制定、これまでにアラバマ州とサウスダコタ州を除く全米 48 州で個別に州法が制定・施行されている[3]。全米におけるこうした法の拡大は、データ侵害を受けた場合の通知にかかるコストなどを補償するプライバシーインシデントの賠償責任及びデータ漏洩の調査に対応する新たなファーストパーティ補償が誕生し、企業のサイバー保険に対する関心を高めるきっかけとなった[4]。

また、こうした州法の制定に伴い、IT フォレンジック（サイバー被害の調査）やクレジットモニタリング（ID 詐欺の損害補償）、顧客への情報通知コスト等に対する新たなファーストパーティ補償のほか、規制に対する弁護費用や罰金などに対応する新たなサードパーティ補償も誕生した。2010 年代以降、大手企業を狙った大規模なデータ漏洩・侵害事件が増加する中、単独の保険商品としてサイバー保険を販売する保険会社の数も 60 社以上に増加している[5]。

3 サイバー保険市場の現状

[3] https://www.huntonprivacyblog.com/2017/04/17/new-mexico-enacts-data-breach-notification-law/
[4] http://locktoncyberriskupdateblog.com/2016/05/31/the-basics-of-cyber-insurance/
[5] http://prowritersins.com/the-history-of-cyber-insurance/

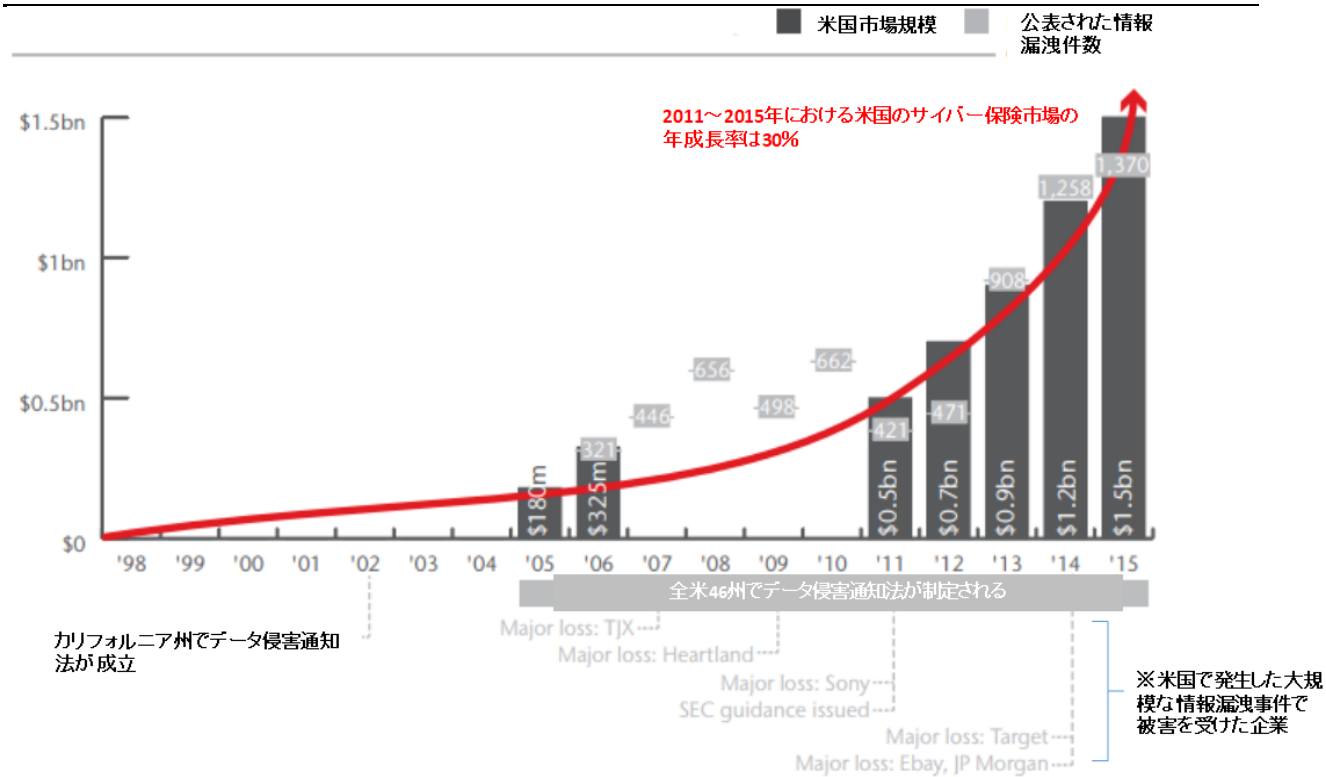
（1） 米国におけるサイバー保険の市場動向

英国ロンドンに本社を置く保険ブローカー及び人材コンサルティング事業を手がける大手 Aon 社が 2017 年 6 月に発表したグローバルサイバー市場に関する調査報告書によると、2015 年における世界のサイバー保険の市場規模は 17 億ドル（年間の総計上保険料ベース）で、米国の市場規模はその 90%（15 億ドル）を占める世界最大のサイバー保険市場である[6]（図表 2 参照）。

ほぼ全ての企業が加入している財物補償保険や損害賠償責任保険などの歴史の長い成熟した保険と比較すると、企業のサイバー保険への加入率は低く、米国企業全体におけるサイバー保険の加入率は 20～35%にとどまっているが、その加入率は企業規模や業界により大きく異なる[7]。企業規模別では、小規模企業に比べ、サイバーインシデントに伴う潜在的なコストに対するリスク意識の高い中規模・大企業の方が、役員などの企業のトップ層が積極的にサイバーリスク対策に取り組んでいる割合が高く、サイバー保険への加入率も高いことが明らかになっている[8]。また、業界別では、保険ブローカー及びリスク管理サービス大手 Marsh 社が主に米国の自社顧客に対して行った調査によると、2015 年時点でヘルスケアや教育分野の企業の加入率が 40～50%で高率となっている（図表 3 参照）。

図表 2：米国におけるサイバー保険の推定市場規模推移

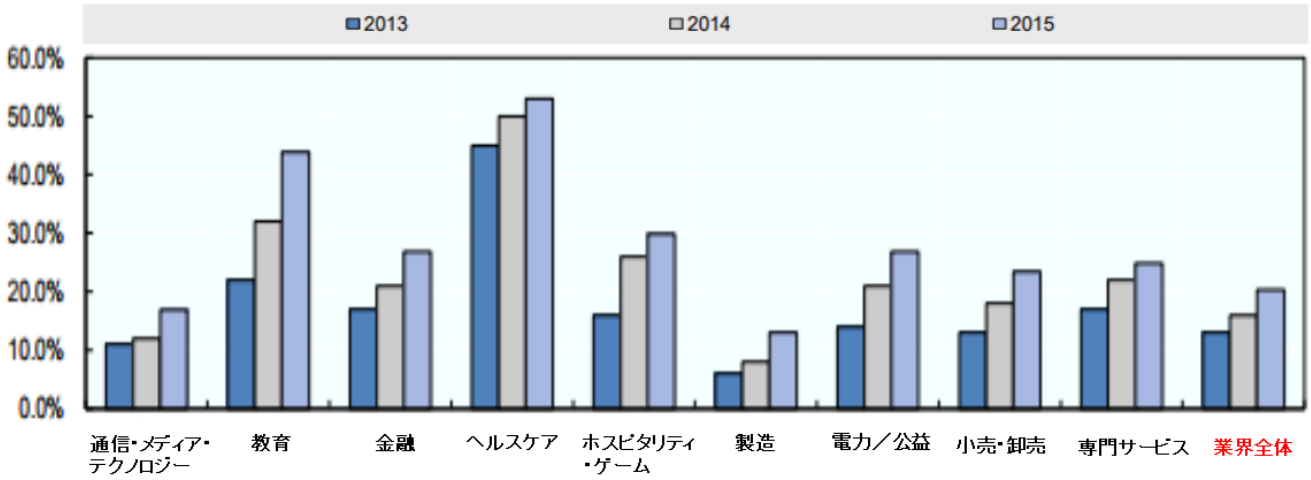
[6] http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[7] https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf
[8] PricewaterhouseCoopers（PwC）社による「企業取締役調査（2016 年）」によると、サイバー攻撃のリスクを監視・理解するために積極的に取り組む企業役員の割合は、大企業では 68%であったのに対し、小規模企業では同率は 32%にとどまっている。また、Aon 社の調査では、2015 年時点で、年間売上高 1 億～10 億ドル未満の中規模企業が米国のサイバー保険市場（年間の総計上保険料ベース）全体の 43%、年間売上高 10 億ドル以上の大企業が同 38%を占めていることが明らかになっている。



※サイバー保険は単独商品として提供されている保険を対象とする。

出典：Aon

図表 3：米国におけるサイバー保険の業界別普及率の推移



※保険ブローカー大手 Marsh 社が主に米国の自社顧客に対して行った調査結果に基づく。

出典：OECD

米国でサイバー保険に加入する企業は、当初、テクノロジー・メディア・通信（TMT）業界の企業や専門サービス企業が主であったが、近年の Sony 社、Target 社、Ebay 社、Yahoo 社といった大手企業を狙ったサイバー攻撃による大規模な個人情報の流出事件が相次いで発生したことも影響し、特に、個人識別情報

（Personally Identifiable Information：PII）や膨大な金融取引データを保持・処理する金融、小売業界の大企業を中心にサイバー保険に加入する企業の割合がその後増加しており、米国のサイバー保険に加入する企業の 29%、21%をそれぞれこれらの業界の企業が占める。また、医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act：HIPAA）における医療情報のプライバシー及びセキュリティルールの策定[9]に伴い、ヘルスケア業界における企業の加入割合も大幅に増加傾向にあり、これらの金融、小売業界に次いで高い割合（15%）を占めている。Aon 社は、サイバーインシデントのもたらす影響への懸念から、今後、製造、エネルギーといった PII を保持しない業界企業においてもサイバー保険への加入が大幅に増加するとの見通しを示しており、米国のサイバー保険市場は 2020 年までに年間保険料収入ベースで 56 億ドル規模に成長すると予測している。

（2） サイバー保険を提供する主要保険会社とサイバー保険の内容

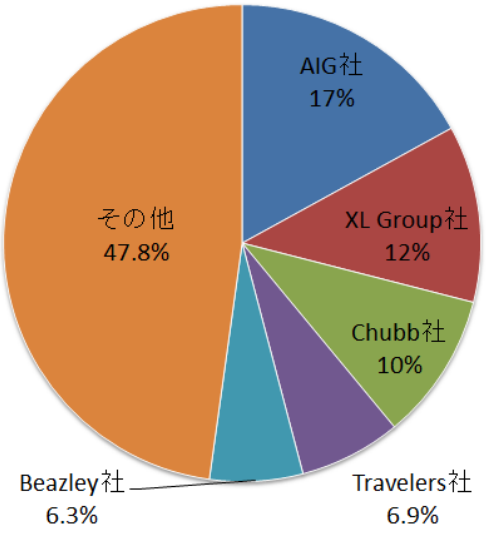
a. サイバー保険を提供する米国の主要保険会社

プライバシー、データ保護、情報セキュリティ政策を専門とする米シンクタンク Ponemon Institute 社が実施した情報漏洩コストに関する調査（2017 年）[10]によると、業界を問わず米国で情報漏洩被害に遭った企業の平均被害総額は 735 万ドル（前年比 5%増）で、こうした情報漏洩インシデントの 47%は悪意のあるサイバー攻撃によるもの[11]であることが明らかになっている。企業のサイバーリスクが高まる中、サイバー保険は、サイバー攻撃又はデータ侵害を受けた際に企業が負う必要のある様々な費用を補填し負担を軽減するなど、企業のリスク軽減戦略において重要な役割を担う一つの手段として近年高い注目を集めており、単独の保険商品としてサイバー保険を提供する保険会社も増えている。

国際信用格付企業大手 Fitch Ratings 社が 2017 年 6 月に発表した米国のサイバー保険市場シェアとパフォーマンスに関する調査報告書によると、2016 年末時点で、130 社以上の損害保険会社が提供する同国のサイバー保険市場のうち、およそ 40%を①AIG 社（17%）、②XL Group 社（12%）、③Chubb 社（10%）の 3 社の主要損害保険会社が占めている[12]。

図表 4：サイバー保険を提供する米国の主要損害保険会社の市場シェア（元受保険料ベース）

[9]同ルールは、データ漏洩の可能性が認められた場合、関連企業に対し、顧客（個人）及び（一定の状況において）米保健社会福祉省（HHS）下の公民権局（OCR）とメディアに通知することを義務付けている。
[10] https://www.ibm.com/security/data-breach/
[11] 他の要因としては、人的エラーによるもの（28%）や IT／ビジネスプロセス障害を含むシステムエラーによるもの（25%）が挙げられる。
[12] https://www.fitchratings.com/site/pr/1025547



出典：Bloomberg[13]

b. 米国で提供されている基本的なサイバー保険の補償内容

ビジネスに深刻な影響を及ぼすサイバー脅威が増加する中、こうした脅威に対するコストを補償するサイバー保険のポリシーも発展を遂げてきた。しかし、他の保険に比べてまだ歴史の浅いサイバー保険に関して、多数の保険会社は情報セキュリティに関する専門的事項やデータ漏洩への具体的な対処法を明確に特定できずにおり、また、標準化された補償項目や保険契約のアンダーライティング（underwriting）プロセス[14]も確立されていないことから、保険会社によりサイバー保険の内容はかなり異なっている。米国でサイバー保険のポリシーは、通常、各企業のサイバーリスクに応じてカスタマイズし提供されているが、企業（被保険者）は、サイバーインシデントの発生時におけるデータ漏洩の影響や関連コストを予測し真に必要な補償を把握するために最適な保険会社を選定する必要がある[15]。

現在米国で提供されている最も基本的なサイバー保険のポリシーの一つは、個人情報やクレジットカード情報、健康／医療情報、企業秘密情報等の個人情報の不適切な開示又は流出に対するリスクを補填するデータプライバシー補償と、被保険者のコンピューターシステムのセキュリティがハッカーやマルウェア、DoS（Denial of Service）攻撃等により破られ情報が漏洩した場合のデータセキュリティリスク補償が含まれる[16]。サイバー保険のポリシーによっては、十数種類以上の保険契約を含むものもあるが、大部分の基本的なポリシーは、3 種類のサードパーティ補償（①プライバシー侵害に対する第三者損害賠償責任、②プライバシー侵害に対する規制当局損害賠償責任、③コンピューターのシステムセキュリティ違反に対する第三者損害賠償責任）と、④データ侵害などのインシデント発生時に被保険者が調査・対策のために支払うコストを補償するファーストパーティ補償の 4 種類の補償を含むことが多い[17]。

[13] https://www.bloomberg.com/news/articles/2017-07-06/the-next-wannacry-cyber-attack-could-cost-insurers-2-5-billion
[14] 保険の引受けにあたって、リスクを認識・評価し、保険契約者を選択、契約条件を設定、料率を決定する一連のプロセスを指す。
[15] http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover
[16] サイバー保険は、一般に、データ、ネットワーク、賠償責任、評判といった無形資産を対象とする補償であり、サイバー攻撃により損害を受けたサーバーやハードウェア等の有形資産の補償は含まれない。
[17] http://locktoncyberriskupdateblog.com/2016/05/31/the-basics-of-cyber-insurance/

図表 5: 米国で提供されている基本的なサイバー保険ポリシーの補償内容

	主な補償内容	
サードパーティ補償	①プライバシー侵害に対する第三者損害賠償責任	・プライバシー法の侵害及び企業のプライバシーポリシー遵守を不注意により怠った場合の損害(ポリシーによっては、不正な情報収集、個人情報の盗難、秘密漏洩、プライバシー権侵害などを含む場合もある) ・プライバシー侵害に係る情報には、氏名、住所、社会保障番号、クレジットカード番号、健康/医療情報などの個人を特定できる情報のほか、企業の機密/専有情報が含まれる
	②プライバシー侵害に対する規制当局損害賠償責任	・データ侵害に対する連邦政府/州の規則で定められている罰科金の補填 ・データ侵害に係るセキュリティインシデントは、通常、複数の州の顧客のデータが関与し、各州の定める法・規則はそれぞれ異なるため、同補償は複数の規制当局の関連規制に遵守する必要のある被保険者にとって特に重要である
	③コンピューターのシステムセキュリティ違反に対する第三者損害賠償責任	・被保険者の(又は第三者が被保険者に代わり運用している)コンピューターシステムがサイバー攻撃を受けた場合の損害 ・第三者によるコンピューターシステムへの不正アクセス、コンピューターシステムにおけるマルウェア/スパイウェア/ウイルス感染、DoS 攻撃、被保険者のコンピューターシステムが他のコンピューターシステムの攻撃に用いられた場合など ・サイバー攻撃により被保険者が受けた金銭/財産の損失や紛失/破損データの復旧にかかる費用は対象外
ファーストパーティ補償	④データ侵害などのインシデント発生時における被保険者のコスト補償	・(被保険者である企業のインシデント対応計画を過去に共同で策定した)プライバシー法の専門弁護士に対する法定費用 ・インシデントの発生原因を探るためのシステム/データ調査にかかるフォレンジック費用 ・各州のデータ侵害通知法等で義務付けられている顧客(個人)や規制当局へのデータ漏洩に関する通知にかかる費用 ・データ漏洩に関する顧客からの問い合わせに応じる特別コールセンターの設置にかかる費用 ・個人識別情報(PII)や決済カード情報、健康/医療情報等のデータ侵害時に通常提供される顧客の ID/クレジットカード情報のモニタリングサービスにかかる費用 ・データ侵害の発生後に企業(被保険者)が直面する評判低下のリスクを軽減するためのメディア等に対する広報 PR(情報危機管理)費用

出典:各種資料[18]を基に作成

c. 米国のサイバー保険の特徴

企業が最適なサイバー保険を選択する上では、米国のサイバー保険の特徴を理解し、主に以下のような点に留意する必要がある。

- *主要保険会社はサイバー保険を単独の保険商品として提供*— 保険専門の米格付け企業 A.M.Best 社によると、2016 年に米国の損害保険会社が計上したサイバー保険関連の元受保険料総額(13 億ドル)のうち、サイバー保険を従来の損害賠償責任保険や利益保険、会社役員賠償責任保険と切り離し、特定のサイバーリスクに対応した単独の保険商品として提供している主要保険

[18] http://locktoncyberriskupdateblog.com/2017/03/13/cyber-insurance-basics-privacy-liability-coverage/
https://www.irmi.com/online/insurance-glossary/terms/r/regulatory-defense-and-penalties-coverage.aspx
http://locktoncyberriskupdateblog.com/2017/10/23/cyber-policies-101-system-security-liability-coverage/
http://locktoncyberriskupdateblog.com/2016/07/11/cyber-insurance-basics-breach-event-cost-coverage/

会社のサイバー保険からの保険料がおよそ 70%を占める。独立したサイバー保険を提供する保険会社が増えている背景には、補償内容を必要性に応じてより詳細に調整できるため効率的であるとの認識が高まっていることに加え、統合型保険では、除外項目をポリシーに詳細に記載しなかったために、後に保険会社が被保険者による高額訴訟に巻き込まれるケースが生じていることなどがある[19]

- *保険会社により大きく異なる補償内容と保険料―* 著しく進化するテクノロジーやサイバーセキュリティに対する各保険会社の理解には差があり、保険のポリシーや保険料は、被保険者（企業）の業界、サービス内容、保存・収集・処理されている機微なデータの種類、個人識別情報（PII）や保護されている医療情報（PHI）の量、情報漏洩リスク、コンピューター／ネットワークセキュリティ、プライバシーポリシー、年間総収益等、多数の要素を考慮して決定されるため、一定の基準で各社のサイバー保険の内容や保険料を比較することは困難である[20]

- *サイバーリスク分析・評価ツールを提供する企業の存在―* サイバー保険においては、企業の受けたサイバー被害について信頼できるデータが不足していることや、顧客企業の過去及び将来のサイバーインシデントへの対応力を見通すことができないことが、保険会社による保険料の設定や企業による補償範囲の決定を困難にしている（同点については次章で後述）。こうした保険会社及び企業の課題に対応するため、企業のサイバーセキュリティリスクやセキュリティ体制を評価・格付けする自動ツールを提供する企業（BitSight Technologies 社、SecurityScorecard 社、PivotPoint Risk Analytics 社）や、予測サイバーセキュリティリスク分析を基に保険会社によるサイバー保険に特化した保険料の設定を支援するソリューションを提供する QuadMetrics 社（2016 年に米予測分析のソフトウェア企業大手 FICO 社が買収）といったスタートアップが市場で注目を集めている[21]

- *最大補償額とサブリミット（内枠限度）、補償除外項目―* データやネットワークのセキュリティ侵害及びその損失を補償するサイバー保険の最大補償額は、通常、各被保険者（顧客）につき、500 万～1 億ドルの範囲に制限されている[22]。また、保険会社は、例えば、プライバシー侵害に対する賠償責任補償で最大 1,000 万ドルの補償を行うポリシーでも、プライバシー侵害に対する規制当局への賠償責任補償は同額より低い額を設定するなど、リスク管理のため、各ポリシーにおける契約でサブリミットを設定していることが多いことから、こうした条件や金額が企業のニーズ及びリスクに応じたものであるか十分注意しなければならない[23]。さらに、サイバー保険のポリシーでは、刑事上の罰金が科されるサイバー犯罪や暗号化されていないデータなどは補償対象外となっている場合も多く、企業はこうした除外項目にも特に注意する必要がある[24]

- *ブローカー及びプライバシー法専門弁護士の重要性―* 企業が組織のサイバーリスクを正確に把握し最適なポリシーを選定する上で、ブローカーは重要な役割を果たす。ブローカーは、アンダーライティングプロセスにおいて、財務、人事、IT といった企業の主要ビジネス部門の人員から、サイバーリスクやサイバーセキュリティ対策について様々な情報を収集し、保険会社が引受審査を通じて

[19] http://www3.ambest.com/ambv/bestnews/presscontent.aspx?refnum=25414&altsrc=9
[20] https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/
[21] https://techcrunch.com/2016/06/13/cyber-insurance-is-changing-the-way-we-look-at-risk/
[22] https://www.bloomberg.com/news/articles/2017-05-09/cyber-crime-fears-drive-growing-demand-for-anti-hacker-insurance
[23] https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2017-10-18/7-things-you-might-not-know-about-cybersecurity-insurance
[24] https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2017-10-18/7-things-you-might-not-know-about-cybersecurity-insurance

最適なポリシーを提案できるよう仲介する。ブローカーは保険会社の代理人ではなく、被保険者（顧客）の利益を代表するという点で、保険業界内における他の職種とは異なっており、一流のブローカーは、顧客と協力してリスクにさらされている資産と、その資産について既存の保険又は新たな特化型保険を通じて最適に対処する方法を把握することが可能である。また、データプライバシー侵害イベント発生時に、州法、連邦法、国際法といった様々な法規制に適切に対処するためには、プライバシー法専門弁護士が必要である。重大なデータプライバシー案件を数多く扱ってきた弁護士は、管轄や法の定義に関する豊富な経験[25]と検討中の法改正の内容や規制担当者の解釈に関する知識を有し、必要なベンダ、規制当局、該当する保険の問題に精通しており、インシデント発生時に関連する法と契約をタイムリーに遵守できる対応計画を作成し、企業が規制当局の調査や訴訟問題に迅速に対応できるよう支援する[26]

- *第三者ベンダのサイバーリスク補償*— 2013 年に米小売大手 Target 社から大量の顧客の決済カード情報が流出した事件で、攻撃者が同社と取引のある空調システム企業のネットワークを経由して同社の顧客情報管理システムに不正侵入したことが明らかになったことなどを受け、第三者ベンダのサイバーリスクを補償するポリシーに対する需要が高まっている[27]

（3） 日本のサイバー保険市場の現状

日本では、データベースの巨大化に伴う情報漏洩被害の拡大に伴い、2012 年に米 AIG 社傘下の AIU 保険会社がサイバー保険の販売を開始したが、あまり販売は進まず、その後、世界的なサイバー犯罪の増加を受けて、2015 年から複数の大手保険会社で企業向けのサイバー保険の取り扱いが開始された。これらの保険は、情報漏洩による損害賠償や争訟費用、サイバーインシデントに伴う利益損害等を補償するもので、米国等でビジネスを展開する企業のニーズを考慮し、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特徴的である[28]。

図表 6: 日本で取り扱われているサイバー保険の概要

[25]例えば、各州で制定されているデータ侵害通知法では、「個人識別情報（PII）」の定義に差があることから、企業は州ごとに異なる義務付けに従う必要がある。https://www.law360.com/articles/922786/cybersecurity-is-the-next-frontier-of-state-regulation、https://www.cio.com/article/2384003/government/national-data-breach-notifications-would-replace--patchwork--of-state-statutes.html

[26] https://www.symantec.com/content/dam/symantec/docs/white-papers/what-every-ciso-needs-to-know-cyber-insurance-en.pdf

[27] https://www.welivesecurity.com/2015/10/14/10-key-facts-need-know-cyber-insurance/

[28] https://swri.jp/article/117
http://www.nli-research.co.jp/report/detail/id=53844&pno=3?site=nli

	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

出典：ニッセイ基礎研究所

米国と比較すると、企業におけるサイバー犯罪による損害額は低水準にある日本[29]であるが、近年、国内外で大規模な情報漏洩問題が発生したことや、標的型攻撃の登場、2017 年 5 月 30 日から施行されている罰則規定を定めた改正個人情報保護法などを背景に、日本国内におけるサイバー保険の市場規模は、2013 年度には 90 億円弱であったのが 2014 年度には 105 億円（前年比 18%増）、2015 年度には 136 億円（同 30%増）規模に成長している[30]。

図表 7：日本国内におけるサイバー保険市場規模の推移

※日本ネットワークセキュリティ協会「2015 年度情報セキュリティ市場調査報告書」より

出典：IT Leaders

しかし、IT 専門調査会社の IDC Japan 社が 2017 年 4 月に発表した国内企業の情報セキュリティ対策実態調査結果によると、国内企業のサイバー保険への加入率は 17.2%にとどまっており、企業におけるサイバ

[29]Ponemon Institute 社によると、2016 年度において米国の企業が受けたサイバー犯罪による平均被害額は 1,736 万ドルであるのに対し、日本は 839 万ドルである。https://software.microfocus.com/en-us/asset/2016-cost-cyber-crime-study-risk-business-innovation-ponemon-institute-cyber-security-analysis
[30] https://it.impressbm.co.jp/articles/-/14548

一保険の普及率は限定的といえる。他方で、ランサムウェアなどのセキュリティ被害が重大化する中、加入を予定・検討している企業はおよそ 40%に上っており、同社は国内企業のサイバー保険への加入率は今後さらに高まると予想している[31]。

4 米国におけるサイバー保険に関連した最近の主な動き

(1) 連邦政府によるサイバー保険関連の政策動向

a. 米国土安全保障省(DHS)による「サイバーインシデントデータ分析リポジトリ(CIDAR)」構築イニシアチブ

米国土安全保障省(Department of Homeland Security:DHS)は、サイバー保険は、情報漏洩や事業中断、ネットワークの損傷といったサイバーインシデントによる企業損失を軽減するもので、同市場の活性化は、補償範囲の拡大やセキュリティ対策の度合いによる保険料設定により、様々な予防措置やセキュリティ対策としてのベストプラクティスを実践する企業が増え、サイバー攻撃による被害件数の減少につながると考えている。また、DHS の国家保護・プログラム理事会(National Protection and Programs Directorate:NPPD)は 2012～2014 年にかけて、学術機関の研究者や重要インフラ業者、保険会社、最高情報セキュリティ責任者(CISO)、企業のリスク管理者などを招集し、サイバー保険市場の成長を促す上での課題について意見交換を推進してきた[32]。そして、これらの意見交換を通じて、歴史の浅いサイバー保険市場においては、特にサイバーインシデントの発生件数と企業及び経済への損害額などを含む企業のサイバーインシデントに関する実質的なデータが不足していることが、保険会社や被保険者となる企業が様々なサイバー攻撃が企業の財政に及ぼす影響やこうしたリスクを緩和するために必要な投資について予測することを困難にしている(結果として保険会社は補償範囲が限定され割高の保険料が設定されたポリシーを提供せざるを得ない)とし、サイバー保険の普及・成長を妨げる主要因の一つとして認識された[33]。

この課題に対応するため、DHS は、匿名化された企業のサイバーインシデントデータを業界で共有し、企業のリスク管理者及び保険会社がサイバー脅威のトレンドの特定やサイバーリスクの算定に利用できる「サイバーインシデントデータ分析リポジトリ(Cyber Incident Data and Analysis Repository:CIDAR)」の構築を提案し[34]、2014 年以降、CIDAR に格納するサイバーインシデントデータの収集を開始している。このデータは、攻撃の種類、重大性、インシデントの時系列、攻撃者の目的、要因、特定の制御障害、危殆化された資

[31] https://www.idcjapan.co.jp/Press/Current/20170425Apr.html
[32] https://www.dhs.gov/cybersecurity-insurance
[33] DHS は、業界有識者との意見交換を通じて、保険会社により提供されているサイバー保険が限定的である理由として、①サイバーインシデントの発生件数と企業及び経済への損害額などを含む企業のサイバーインシデントに関する実質的なデータが不足していること、②実質的な過去のインシデントデータの不足やサイバー攻撃に用いられるテクノロジーの変化が速いことから、サイバーリスク損害発生確率を評価するための予測モデルの構築が困難であること、③電力会社や金融機関など、同一のソフトウェア、企業リスク管理戦略又は IT インフラを用いる業界企業の場合、一企業のいずれかのシステムの脆弱性を突いた攻撃が業界全体のサイバーリスク(aggregation risk)負担につながること、の 3 点を主要因として特定している。https://bipartisanpolicy.org/library/cyber-insurance-a-guide-for-policymakers/
[34]DHS は、様々な重要インフラ業界の最高情報セキュリティ責任者(CISO) と 最高セキュリティ責任者(CSO)、保険会社、その他のサイバーセキュリティ専門家から構成されるワーキンググループ(Cyber Incident Data and Analysis Working Group:CIDAWG)を立ち上げ、サイバーインシデントデータリポジトリの価値、必要な分析を行うためにリポジトリで共有すべきサイバーインシデントデータポイント、データ共有を自発的に促す手法、想定されるリポジトリの構造と機能について調査・検討している。https://www.hsdl.org/c/dhs-cyber-incident-data-and-analysis-working-group/

産、検知・緩和手法、攻撃による被害額を含む 16 種類のカテゴリに分かれており、ウェブベースのポータル上で、従業員数や収益情報を基に、各企業のサイバーセキュリティ対策の比較などを行えるようになる予定である。DHS でパフォーマンス管理ディレクタを務める Matt Shabat 氏は、CIDAR の目的は、企業のサイバーリスクをより正確に評価するための実質的なデータを保険会社に提供し、ある一定の基準のサイバーセキュリティ対策を行っている企業に対しては保険料を軽減するといった措置を積極的に講じることを推奨することと説明する[35]。一方で、企業のサイバーリスクを算定するために十分なデータを収集するには、10～15 年の期間を要する見込みであり、データが完全に集まるまでは、CIDAR はハッカー攻撃のトレンドや企業のリスク管理の価値を分析するために利用できるという。Shabat 氏によると、DHS では、2017 年末までに連邦官報（Federal Register）に CIDAR のデータファイルと分析ツールを用いた最初の成果を公表したい考えである[36]。

米国では、2015 年後半、企業が政府機関とサイバー攻撃に関する情報共有を行った際に発生し得る民事訴訟の免責等により、企業による情報共有を容易にするためのサイバーセキュリティ情報共有法（Cybersecurity Information Sharing Act：CISA）が成立するなど、政府がサイバー脅威情報の官民情報共有を積極的に推進している。しかし、匿名化が困難なことから、サイバーインシデントに関する詳細データを政府と共有することに消極的な姿勢をみせる企業は多く、CIDAR が様々な企業から幅広くデータを収集できるかについては懐疑的な見方もされている。他方で、CIDAR 構築イニシアチブに期待を寄せる業界関係者の声は多く、非構造化データを可視化・分析するセキュリティソフトウェアプラットフォームの開発を手がける米 Varonis 社のグローバルフィールドエンジニアリング部門バイスプレジデントを務める Ken Spinner 氏は、「業界ベースの情報共有センター（Information Sharing and Analysis Center：ISAC[37]）が設置されてから 10 年以上が経過しており、セクター間で情報共有を行う一元化されたサイバーインシデントデータリポジトリの構築は理にかなった次なる措置であり、セキュリティインシデントや犯罪戦術のパターン研究にも資するだろう」と述べている。また、米サイバーセキュリティ企業 Lieberman Software 社のプレジデント Philip Lieberman 氏は、「サイバー保険は客観的に試験・立証できる最低限のセキュリティ要件に関する明確な定義があって初めて意味を持つが、これまでこうした定義は存在しない」とした上で、DHS が CIDAR においてサイバーインシデントに関する質の高いデータを十分に収集できれば、企業のサイバーセキュリティの改善につながるとの考えを示している[38]。

b. 連邦政府が公的に支援するサイバー保険プログラムの新設を求める声

米連邦政府は、民間企業のサイバーセキュリティを強化するインセンティブとして、サイバー保険を活用することを検討・議論してきたが、非営利の米外交シンクタンクである外交問題評議会（Council on Foreign Relations：CFR）は、送電網に対するサイバー攻撃など、大規模で破滅的な影響を及ぼす恐れのあるサイバーインシデントに備えて政府がより積極的にサイバー保険の補強・普及につながる政策を施行すべきとし、連邦政府が公的に支援するサイバー保険プログラムを新設することを提案している。

米国では、2001 年 9 月 11 日の同時多発テロ事件を受けて、民間の保険市場では対応できない損害[39]が発生した場合を想定し、①商用施設における一定規模以上のテロ損害に対する復興費用を政府が支援する「テロリズムリスク保険プログラム（Terrorism Risk Insurance Program：TRIP）」と、②製品開発に失敗し

[35] https://gcn.com/articles/2017/04/24/cyber-incident-data-repository.aspx
[36] https://www.techrepublic.com/article/dhs-cyberinsurance-research-producing-insights-about-security-trends/
[37] 各重要インフラにおける業界の民間事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織。
[38] http://searchsecurity.techtarget.com/news/450427533/DHS-cyberinsurance-research-could-improve-security
[39] 英大手保険会社 Lloyd's of London 社は、米国東海岸の送電網に対するサイバー攻撃が発生した場合の経済損失は 1 兆ドル、保険会社の損失は 710 億ドルに上ると推定している。

た場合のリスク補償を行って政府公認の企業によるテロ対策技術の開発を推進する「効果的な技術促進によるテロ対策支援法（Support Anti-terrorism by Fostering Effective Technologies Act）」が新たに定められた。CFR は、連邦政府が公的に支援するサイバー保険プログラムにおいて、これらの 2 つのプログラム（法）規定を拡大し、テロ攻撃だけでなく、テロリスト、国家、犯罪者等による大規模なサイバー攻撃も対象とすることを提案しており、これにより保険会社は政府の公的支援を受けて莫大な被害額が予想されるサイバーインシデントに対するポリシーを提供できるようになることで、サイバー保険市場の拡大につながることが期待されている。

また CFR は、同サイバー保険プログラムに加入する企業に対し、米国立標準技術研究所（National Institute of Standards and Technology：NIST）のサイバーセキュリティ・フレームワークに基づくサイバーセキュリティ計画を策定することや、悪意のある危険な IP アドレスやフィッシングメールの送信者アドレス等の匿名化されたサイバー脅威情報を官民で共有する情報基盤である DHS の「自動指標共有（Automated Indicator Sharing：AIS）[40]」における情報共有、及びサイバー攻撃を受けた場合にその原因を特定するための徹底した調査・情報収集を義務付けることも推奨しており、こうした取組みは企業のサイバーリスク評価やサイバーセキュリティ対策の向上に資するとしている[41]。

（2） その他のサイバー保険関連の主な動き

a. ランサムウェア「WannaCry」騒動とサイバー保険市場への影響

Microsoft Windows のセキュリティの脆弱性を突いたワーム型ランサムウェア「WannaCry（別名「WannaCrypt」「WanaCrypt0r」「Wanna Decryptor」「WCry」など）[42]」は、2017 年 5 月 12 日にサイバー攻撃による感染が確認されて以降、短期間で世界中に拡散し、英国民保健サービス（NHS）や米物流大手 FedEx 社、ルノー・日産社、など、世界 150 カ国以上における医療機関や政府機関、企業のおよそ 30 万台のコンピューターに被害をもたらした。Trend Micro 社の 2017 年上半期セキュリティ脅威レポートによると、その被害額は最大 40 億ドルに上るとみられている[43]。

図表 8：WannaCry に感染したコンピューターに示された暗号化データの身代金として仮想通貨ビットコインを要求するメッセージ（脅迫状）のスクリーンショット

[40] https://www.dhs.gov/ais
[41] https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program
[42] WannaCry は、主に Windows の Server Message Block（SMB）サーバーの脆弱性を利用して感染したとみられている。なお、同脆弱性については、2017 年 3 月 14 日に Microsoft 社がセキュリティパッチ（MS17-010）を公開していた。
[43] https://www.trendmicro.com/vinfo/gb/security/research-and-analysis/threat-reports/roundup

出典：Popular Science[44]

しかし、①最も被害の大きかったのはアジアと欧州地域であり米国での感染範囲が比較的限定的であったこと[45]と、②同ランサムウェアが要求する身代金額が感染したコンピューター1 台当たり 300～600 ドルと少額であり、サイバー保険では免責金額（被保険者の自己負担額）とされ補償されないことの 2 大理由から、WannaCry による米国のサイバー保険業界における財務上の影響は当初想定されていたよりも軽いとみられている[46]。一方で、米セキュリティソフトウェア企業 Symantec 社のバイスプレジデント兼ゼネラルマネージャーを務める Pascal Millaire 氏は、ランサムウェアによる身代金額は比較的少額であるケースが多いものの、ランサムウェア攻撃に対するサイバー保険補償が効果を発揮するのは、事業中断に伴う利益損失と臨時費用が発生した場合や情報漏洩、訴訟問題などが起きた場合であり、今回の WannaCry 攻撃によるこれらの関連コストや、ランサムウェアにより数千・数万件に上る企業がこうしたコスト補償を保険会社に請求するような将来起こり得る最悪のシナリオを想定して、保険会社がサイバー保険の保険料や条件を見直す可能性も否定できないとの考えを示している[47]。

Millaire 氏によると、具体的には、WannaCry に感染した企業／組織のコンピューターシステムは、Microsoft 社がセキュリティパッチ（MS17-010）を 2017 年 3 月に公開していたにもかかわらず、その更新が行われていなかったことから、保険業界では、企業／組織がこうした既知のセキュリティ脆弱性問題への対応を怠った場合に、サイバー保険ポリシーにおいて過失怠慢による損害賠償補償を対象とするかについて再検討・議論されているという。従来、サイバー保険に加入する企業は、顧客データの漏洩を懸念する小売、

[44] https://www.popsci.com/time-to-start-thinking-about-how-to-survive-next-ransomware-attack
[45] アジアや欧州地域と比較して米国における WannaCry の感染被害が少なかった主な理由として、業界関係者の間では、米国企業はセキュリティ対策への意識が高く、サイバー攻撃に起因する情報漏洩などが争訟問題に発展するのを恐れ、既知のセキュリティの脆弱性問題を検知するセキュリティプログラムを導入し、ソフトウェアのアップデートを欠かさず実施している組織が多かったことや、更新サービスを受けられない海賊版の Microsoft Windows OS がほとんど利用されていないこと、WannaCry は「MalwareTech」と名乗る英国のセキュリティ研究者が動作を停止させるキルスイッチを早期に発見したことにより有効だった時間が 7 時間程度と比較的短かったが、この時間帯が米国では深夜から朝でありネットワーク活動が少なかったこと等が考えられている。https://www.usatoday.com/story/tech/news/2017/05/15/ransomeware-attack-wannacry-malware/101710900/
[46] https://www.ft.com/content/25bf97e8-3a27-11e7-821a-6027b8a20f23
[47] http://www.eweek.com/security/wannacry-ransomware-raises-stakes-for-cyber-security-insurance

金融業界の企業が中心であったが、WannaCry 騒動を機に、ハッキングやランサムウェアによる事業中断に伴うサイバー被害を恐れ、サイバー保険に関心を持つ企業は製造業や重工業の企業など幅広い業界で増えつつあり、保険会社はこれを市場拡大の機会と捉えている。このように、事業中断に対するサイバー保険補償へのニーズが高まる中、保険会社が最悪のシナリオに照らして保険約款の見直しや改訂を行うかについて、今後の動向を注視する必要がある。

b. 個人を対象とする新たなサイバー保険の登場

サイバー保険は、膨大な個人識別情報（PII）や医療・健康情報、オンライン決済／取引情報、企業機密情報などを有する大企業を中心にニーズが高まり、その後、サイバー攻撃に伴う大規模な情報流出事件が相次いでメディアで取り上げられる中、中小企業でも高い関心を集めつつあるが、サイバー保険のパイオニア企業である AIG 社は 2017 年 4 月、個人を対象とする包括的なサイバー保険「Family CyberEdge」の提供を新たに開始した。

同保険は、多額の自己資本を持つ富裕層向け保険を提供する AIG 社のプライベート・クライエント・グループ（Private Client Group）部門の顧客を対象とする住宅所有者保険の補足保険として位置づけられる商品で、ランサムウェアといったサイバー恐喝やネット上での嫌がらせ（cyberbullying）等の被害におけるデータ復旧、危機・評判管理、サイバー恐喝により支払いを要求された金銭などの補償を行う。また AIG 社は、調査／コンプライアンス／サイバー防衛分野で業界を主導する米 K2 Intelligence 社[48]と共同で、プライベート・クライエント・グループの保険契約者に対し、様々なサイバーリスクをより主体的に管理する方法についてアドバイスを行うほか、Family CyberEdge の保険契約者に対し、様々なデバイス、ホームネットワーク、無線アクセスポイント、オンラインアカウントのセキュリティ評価に加え、契約者の家族に対するサイバーセキュリティ強化に関するベストプラクティスに関する指導、個人情報の利用状況に関するオンラインモニタリング／評価、ID 保護サービスを提供する米 CyberScout 社によるなりすまし／不正取引の検知等に関する専門ツール及びリソースの提供など、幅広い支援も行う。なお、Family CyberEdge の年間保険料は、最大補償額に応じて 597～1,723 ドルとなっている[49]。

AIG 社のプライベート・クライエント・グループプレジデントを務める Jerry Hourihan 氏によると、同社が住宅所有者保険を提供する顧客の多くの家屋は、20 台程度のハッキングリスクのある WiFi 対応デバイスに接続しており、「（コネクテッドホームが増える中で）顧客のサイバーリスクへの理解をサポートすることが我々の重要な務めである」と述べる[50]。個人向けサイバー保険は、AIG 社のほか、英国の Hiscox 社やドイツの再保険サービス企業 Munich Re 社の傘下にある Hartford Steam Boiler 社といった保険会社も提供を開始しており、各社は個人向けサイバー保険市場が今後大きく成長する可能性を見出している[51]が、住宅所有者保険や自動車保険のように加入が義務付けられていないサイバー保険が広範な消費者層に普及するかなど、今後の行方が注目される。

[48] AIG 社は 2015 年、K2 Intelligence 社の少数株を取得している。
[49] http://www.insurancebusinessmag.com/us/news/cyber/aig-to-offer-comprehensive-personal-cyber-insurance-64367.aspx
https://www.computerworld.com/article/3190209/cybercrime-hacking/how-one-personal-cyber-insurance-policy-stacks-up.html
[50] https://www.ft.com/content/72e11ca6-98ad-11e7-8c5c-c8d8fa6961bb
[51] http://fortune.com/2017/04/08/cyber-security-insurance-cybersecurity-aig-2017-tools-news/

c. 米国商工会議所によるセキュリティ格付け原則の発表

米国商工会議所（U.S. Chamber of Commerce：USCC）は 2017 年 6 月、「公正かつ正確なセキュリティ格付けに関する指針（Principles for Fair and Accurate Security Ratings）」を発表した[52]。上述のように、米国では、企業によるサプライチェーンのセキュリティリスクや保険会社による潜在的な顧客企業のサイバーセキュリティリスクに関する理解を支援するため、企業のサイバーセキュリティリスクやセキュリティ体制を評価・格付けするソリューションを提供するセキュリティ格付け企業が近年注目を集めている。しかし、これらの格付け企業は、（時には対象企業が把握していない）幅広い情報源から企業のセキュリティデータを収集し、それぞれ独自のアルゴリズムを用いて分析、格付けを行っているため、企業の複雑なセキュリティプログラムについて導き出された格付け評価結果が必ずしも第三者により明白に立証できるものでなく、信頼性に欠けることが問題として認識されていた。

この問題に対応するため、JP Morgan 社、Goldman Sachs 社、Morgan Stanley 社、Starbucks 社、Microsoft 社、Verizon 社を含む多様な業界における 40 社以上の USCC のメンバー企業は、セキュリティ格付け企業と密接に協力し、セキュリティ格付け評価の統一性と信頼性を高めるための一連の基本原則を策定した。同原則は、以下の 6 項目から構成される。

- **透明性の確保**— セキュリティ格付け企業は、対象となる企業が評価結果がどのように出されたかを明確に理解できるよう、評価に用いる方法やデータの種類に関する情報を必要に応じて提供しなければならない
- **紛争解決**— 評価対象となる企業は、格付け評価結果に対し異議を唱え、修正や用いられたデータの提示を求める権利を有しており、問題が解決するまで紛争中の評価結果についてはその旨を記録しなければならない
- **正確性及び妥当性の確認**— 格付け評価は立証可能であるかデータを重視していること、又は専門家の意見として記録される必要があり、セキュリティ格付け企業は、評価方法や評価モデルの過去の実績を実証し、必要に応じて修正情報を反映しなければならない
- **モデルガバナンス（データ品質や検証）の確保**— 格付け評価方法及び（又は）データセットに変更を加える場合、セキュリティ格付け企業は顧客企業に対し、当該変更が既存の評価結果に及ぼす影響について予め通知しなければならない
- **独立性の保障**— セキュリティ格付け企業との商用契約は企業のセキュリティ評価に直接的な影響を与えるものではなく、セキュリティ評価を受けた企業は（格付け企業の顧客であるかにかかわらず）、評価結果に異議を唱えることができる
- **守秘義務**— 格付け評価結果に対し対象企業が異議を唱えた場合、セキュリティ格付け企業は評価結果を公表したり、対象企業のシステムを危険に晒す可能性のある機密情報を第三者に提供したりしてはならない

米セキュリティ格付け企業は、同原則を概ね好意的に受け止めており、例えば BitSight 社のシニアバイスプレジデントである Jake Olcott 氏は、「多数の大手企業がセキュリティ格付け評価の問題に対応するために共同で策定した同原則は、セキュリティ評価サービス市場が将来的な企業間（B2B）のリスク管理にとって重要かつ不可欠なものとして認識されていることを示すものである」とコメントしている。同氏は、企業のビジネスエコシステムの拡大や第三者ベンダのセキュリティリスク問題の増加、サイバーセキュリティ人材不足、ビジネスエコシステムのサイバーリスクを迅速かつコスト効率の高い方法で評価することの困難さ等を背景に、セキュリティ格付けの重要性は高まっており、2020 年までに同格付けは信用格付けと同等に重視されるようになると考えている。その上で、こうした原則は、同一及び異なるセキュリティ格付け企業の間で正確

[52] https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

で一貫した評価プロセスを確立し、セキュリティ評価に対する信頼性を高めるために重要な役割を果たすとみられている[53]。

5　今後の展望と日本への示唆

(1)　米国のサイバー保険(市場)の展望

北米の保険業界で 20 年以上アンダーライティング業務に従事し、現在サイバー保険等のスペシャルティ保険及び再保険製品のアンダーライティングサービスを提供する米 Argo Pro 社のシニアバイスプレジデントを務める William Kelly 氏は、2022 年までの今後 5 年以内に米国のサイバー保険の内容(及びその市場)に影響を及ぼす可能性の高い事象として、以下を挙げている[54]。

- *補償範囲の拡大*― サイバー保険の補償範囲は拡大し続けており、今後は傷害、器物・環境損害、ソーシャルエンジニアリング[55]による損失など、様々なデジタル通信への接続に係る損害責任が補償対象となる可能性がある
- *州レベルでの新たなサイバーセキュリティ規則*― ニューヨーク州金融サービス局(New York State Department of Financial Services)は 2016 年 12 月、同州でサービスを提供する全ての金融サービス企業に対し、個人／機密情報を保護するためのサイバーセキュリティプログラムの策定・実施を義務付けるサイバーセキュリティ規則を発表しており[56]、サイバー保険ポリシーの策定に影響する様々な業界を対象としたセキュリティ規則を新たに施行する州は今後増える可能性がある
- *幅広い業界に拡大するサイバーリスク*― サイバー保険は一般的に、個人情報を扱う金融機関、保険会社、医療機関、ホテル、小売業者などの業界企業が加入する保険と認識されているが、今後は製造業や公共インフラ分野など、事業中断に伴い大規模な損害が予想される業界を標的にした様々なサイバー攻撃が増える可能性がある
- *多数の企業が依存するデジタルシステムの障害発生率の増加*― 2016 年 10 月に発生した Spotify や Twitter といった大手ウェブサイトを下支えする米 Dyn 社のドメインネームシステム(DNS)に対する大規模な分散型サービス妨害(DDoS)攻撃など、多数の企業が依存するデジタル通信システムがより複雑化する中で、こうしたシステムを標的にしたサイバー攻撃が今後増加し、事業中断に伴う企業の損害も増える可能性がある
- *IoT デバイスの普及に伴うサイバーリスクの増加*― モノのインターネット(Internet of Things:IoT)時代においてインターネット接続機器が増加する中、デバイスのセキュリティリスクが人間の健康や安全にも危険を及ぼすようになっており、こうした IoT デバイスのリスクをいかに補償するかがサイバー保険における重要な課題の一つである

[53] http://www.securityweek.com/consortium-promotes-principles-fair-and-accurate-security-ratings
[54] https://d1hks021254gle.cloudfront.net/wp-content/uploads/2017/02/2017-Cyber202211.pdf
[55]人間の心理的な隙や行動のミスにつけ込み、パスワードなどの個人が持つ重要な情報を、情報通信技術を使用せずに盗み出す方法を指す。
[56]具体的に同規則は、サイバーセキュリティプログラムの策定や定期的なリスク評価の実施、最高情報セキュリティ責任者(CISO)の選任等のセキュリティ対策に関する社内体制の確立のほか、所定の技術手段(ペネトレーションテスト、アクセス特権の制限、多要素認証等)の導入、サイバーインシデント対応計画の策定、サイバーセキュリティイベント発生時における 72 時間以内の報告義務などの要求事項に 2017 年 8 月末までに対応するよう義務付けている。
http://www.dfs.ny.gov/about/press/pr1612281.htm
http://www.jonesday.com/deadline-to-comply-with-new-yorks-cybersecurity-regulation-is-approaching-08-17-2017/

2018 年 5 月末から欧州連合（EU）の一般データ保護規則（General Data Protection Regulation：GDPR）の施行が開始されることで、EU 市民の個人情報を保持する世界中の企業でサイバー保険への加入が進むことが予想されているが、個人識別情報（PII）を保護する法規制をいち早く施行した米国は、現在世界最大のサイバー保険市場であり、今後も同市場は急成長することが見込まれている[57]。しかし、データ分析ソフトウェアの開発を手がける米 FICO 社が 2017 年 5 月に発表した企業のサイバーセキュリティ対策に関する調査結果[58]によると、調査を実施した米国企業の半数はサイバー保険に加入していないほか、データ漏洩等のサイバー被害が 2018 年に増加すると考える企業の割合は全体の 60%を超えるにもかかわらず、サイバー保険に加入する計画はないと回答した企業幹部の割合はおよそ 30%に上ることが明らかになっており、サイバー保険への加入に二の足を踏む企業は少なくない。これらの企業がサイバー保険への加入を躊躇する主な理由として、保険会社によるサイバー保険の保険料設定において、組織内のサイバーセキュリティ上のリスク要因を正しく反映していないとしてリスク評価プロセスが不透明であることが挙げられており、保険料の設定方法に関する明確な指針やサイバーリスクを評価する上での業界基準を設定することが企業によるサイバー保険への加入を促進する上で重要な要素の一つと考えられている[59]。

米国のセキュリティサービス企業の中には、こうした指針や基準が定められていない現況では、特に IT セキュリティ分野の関連予算が限定的な小規模企業にとって、非常に複雑で割高なサイバー保険への加入をサイバーセキュリティ対策として選択することは時期尚早であり、代わりにアプリケーションやネットワークの安全性を強化するシステム投資に注力することで情報漏洩の発生を予防する方が適切とする声もある[60]。他方で、業界関係者及び組織の最高情報セキュリティ責任者（CISO）の間では、サイバー保険に加入する大きなメリットは、様々なサイバー被害・被害の補償にとどまらず、保険会社によるリスク管理プロセスにおけるセキュリティ向上計画の策定や従業員に対するデータセキュリティに関する研修サービス、詳細にわたるセキュリティの脆弱性評価などを通じて企業がセキュリティ対策を包括的に見直しサイバーセキュリティ対策や規制コンプライアンスを強化できることにあり、（サイバー保険に加入することで）結果的に企業は将来起こり得るセキュリティインシデントに伴うリスクを最小限に抑制できるとみる声もある[61]。

（2） 日本におけるサイバー保険の普及に向けた課題

重大なセキュリティ被害に遭う企業の割合が増加する中、日本でもサイバーセキュリティの重要性は高まっており、企業のサイバー保険への加入率も上昇傾向にある。しかし、上述のように、国内企業のサイバーセキュリティ保険への加入率は 2 割に満たない状況であり、米国と比較すると、依然としてその普及は限定的といえる。

企業がサイバーセキュリティ保険を選定する上では、サイバーセキュリティ対策における投資戦略の中で自社のセキュリティリスクを正しく把握した上で、サイバーセキュリティ保険が投資に見合う価値があるかどうかを判断し、セキュリティ対策の強化につなげることが重要となる。しかし、サイバー攻撃の被害を受けても情報漏洩に関する通知や情報開示を義務付ける規制のない日本を含むアジア太平洋地域では、多数のサ

[57] http://opengovasia.com/articles/6968-cyber-insurance-market-to-triple-in-wake-of-recent-cyber-breaches-as-explained-by-david-barton-of-forcepoint-2
[58]同調査は、金融サービス、通信、ヘルスケア、小売、e コマース、メディアサービス企業における 350 人の経営幹部及びシニアセキュリティ担当者に対する電話インタビューを通じて実施された。
[59] https://www.insurancejournal.com/news/national/2017/05/31/452647.htm
[60] https://www.wordfence.com/blog/2017/09/cyberinsurance/
[61] https://www.esecurityplanet.com/network-security/cyber-insurance-6-facts-you-should-know.html
http://www.wealthmanagement.com/technology/ten-experts-weigh-cyber-liability-insurance

イバー被害に関する事例はほとんど明るみに出ない。AIG 社の中国、オーストラリア、韓国向け損害賠償・金融保険種目担当責任者である Jason Kelly 氏は、サイバーインシデント事例に関する情報の透明性に欠けることが原因で、自社がサイバー攻撃の標的になるまでその実質的な損害を目の当たりにすることのない企業の経営層の間では、（実際、アジア太平洋地域における企業を標的にしたハッキング攻撃は急速に増加傾向にあるにもかかわらず）他の地域と比較するとサイバーリスクは小さいという誤った認識が広がっている可能性があると指摘する[62]。IDC Japan 社の調査においても、特に企業規模が小さくなるほどサイバーセキュリティに関する経営者の関与が欠如し、決められたセキュリティ予算のない場当たり的な投資やファイアウォールなどの従来型のセキュリティ対策への投資を継続する企業が多いことが明らかになっており[63]、経営者が責任を持って事業リスクやコスト効果を考慮した戦略的なセキュリティ投資戦略の策定に関与することが求められる。クラウド型 Web セキュリティサービスを提供する米 Zscaler 社の欧州・中東・アフリカ地域情報セキュリティシニアディレクターを務める Chris Hodson 氏は、CISO の果たす役割は特に重要であり、CISO には、セキュリティ対策への投資対効果を示すためにファイアウォールの記録やマルウェア検出状況に関する報告を行うのではなく、コスト削減等の組織のビジネス戦略目標に照らして、ビジネスリスクを軽減し最も重要な資産やデータを守る具体的な方法及びビジネスに付加価値をもたらすセキュリティ対策について経営者に分かり易い言葉で率直な考えを提示する高いコミュニケーション能力が必要との見方を示している[64]。

また、日本においても、業種や売上高、補償限度額などによって変化する保険料に対する投資対効果が不明瞭であることが企業におけるサイバー保険の普及の妨げになっている要因の一つに挙げられており[65]、企業がサイバーリスク評価やサイバー被害によるコスト推定を適切に行える環境を整えることが重要であると考えられる。

（参考）「サイバーセキュリティ経営ガイドライン」（改訂）
http://www.meti.go.jp/press/2017/11/20171116003/20171116003.html

62 https://www.aig.com/knowledge-and-insights/k-and-i-article-state-of-cybersecurity-asia
63 http://businessnetwork.jp/Detail/tabid/65/artid/5327/Default.aspx
64 https://www.csoonline.com/article/3225345/risk-management/how-to-engage-with-the-c-suite-on-cyber-risk-management.html
65 http://techtarget.itmedia.co.jp/tt/news/1609/30/news06_2.html