米国におけるサイバー保険の動向

グループリーダー 主席研究員　牛窪　賢一

目　　次

要旨

米国では、わが国や欧州よりもサイバー保険の利用が進んでおり、全世界のサイバー保険市場のおよそ 85%（収入保険料ベース）が米国 1 国内のリスクで占められているとの推計もある。本稿では、サイバー保険に関心のある広範な保険関係者の参考となるよう、直近 1 年間を中心に米国におけるサイバー保険の動向を整理する。

サイバーリスクについては損害データの蓄積が進んでおらず、サイバー保険の引受においても適切なリスクの評価や保険料率の算出が難しいなどの課題がある。この課題に対応するため、保険会社やモデリング会社等を中心に、データの標準化、データの共有化、サイバーリスクモデルの構築等が進められてきている。

今後も、サイバー攻撃による被害の拡大や、個人情報保護に関する規制の強化等の動きを受け、サイバー保険の需要は拡大していく可能性が高い。ただし、保険会社が提供するサイバー保険が、将来に向けてその商品内容や保険料率の水準等から企業の期待に応えられない場合、キャプティブや保険リンク証券（ILS）にその需要の一部を奪われる可能性も考えられる。

保険会社は、モデリング会社やサイバーセキュリティ専門会社等と連携のうえ、データの蓄積やリスクモデルの精緻化等を進め、これらを商品のカスタマイズや料率設定に活かすことを通じて、これまで以上に企業の期待に応えていく必要があろう。

１．はじめに

2017 年 5 月、ワナクライ（WannaCry）と呼ばれるランサムウェア[1]によるサイバー攻撃が世界的に確認された。ワナクライはマイクロソフトのソフトウェアの脆弱性を通してコンピュータに入り込み、ファイルを暗号化して、それを解除するための身代金を要求した。150 カ国以上の国で計 30 万台以上のコンピュータが被害を受けたとされ、サイバー攻撃の脅威を改めて実感させるものとなった。ワナクライ以外でも、サイバー攻撃は進化・多様化しており、サイバーリスク[2]に対する関心は世界的に高まっている。

サイバーリスクに対する懸念が広がる一方、個人情報保護に関する規制の強化も世界的な流れとなっている。わが国では、2017 年 5 月 30 日に改正個人情報保護法が全面施行された。米国でも、サイバーセキュリティ関連法の強化が進められており[3]、EU では 2018 年 5 月に一般データ保護規則（General Data Protection Regulation：GDPR）が適用開始される予定である[4]。

サイバー攻撃の増加やこれに伴うサイバーリスクへの関心の高まりと、上記のような規制強化の動きは、企業によるサイバーセキュリティ対策の強化を促すと同時に、サイバー保険に対する需要の拡大につながる可能性が高い。

米国では、わが国よりも早い段階から、官民挙げてサイバーリスク対策が推進されてきた。サイバー保険の利用も進んでおり、全世界のサイバー保険市場のおよそ 85%（収入保険料ベース）が米国 1 国内のリスクで占められているとの推計もある。当研究所では、このように世界で最も進んだ米国のサイバー保険を巡る動向について、2015 年 1 月[5]および 2016 年 7 月[6]に損保総研レポートで取り上げた。その後 1 年の間にも、サイバー保険市場は拡大、変化しており、関連情報も多数発信されている。このような状況を踏まえ、本稿では、サイバー保険に関心のある広範な保険関係者の参考となるよう、直近 1 年間を中心に米国におけるサイバー保険の動向を整理することとした。

なお、本稿における意見・考察は筆者の個人的見解であり、所属する組織を代表するものではないことをお断りしておく。

---

[1] ランサムウェアは、コンピュータに保存されたファイルを暗号化して閲覧できないようにしたり、パソコン等をロックしたりするウィルスであり、元に戻すことと引き換えに身代金を要求する。

[2] サイバーリスクについて定型化された定義はないが、本稿では、「インターネットやテレコミュニケーション・ネットワーク等のテクノロジー・ツールを含む電子データの保管、利用およびその伝達によって生じるリスク」の意味で使用している。

[3] 後記 6.を参照願う。

[4] なお、個人情報保護に関連する規制の動向については、当研究所で現在進めている 2017 年度上期調査「主要国における個人情報保護規制の動向と保険業界の対応」（2017 年 4 月～9 月調査、11 月報告書刊行予定）でも紹介する予定である。本稿（損保総研レポート第 120 号）では、この上期調査の範囲と一部重なることや紙面の都合もあり、関連規制については概略ふれる程度にとどめた（後記 6 参照）。

[5] 山下潤「米国のサイバー・インシュアランスの動向」損保総研レポート第 110 号（損害保険事業総合研究所、2015.1）

[6] 牛窪賢一「サイバーリスクとサイバー保険－米国の動向を中心として」損保総研レポート第 116 号（損害保険事業総合研究所、2016.7）。第 116 号では、サイバー保険の動向のほか、サイバー保険拡大の背景（サイバー攻撃による被害の状況、米国のサイバーセキュリティ国家戦略、企業向け規制および規制への企業の対応、保険会社向け規制の状況等）も広く取り上げており、このレポートも適宜参照願う。

２．サイバー保険の概要と市場の概況

本項では、米国におけるサイバー保険と関連サービスの概要、ならびにサイバー保険市場の概況について説明する。

（1）サイバー保険と関連サービスの概要

a. サイバー保険の概要

サイバー保険[7]は、コンピュータ・ウィルスやコンピュータへの不正アクセス、ヒューマンエラー等に起因して生じる損害を補償する保険である。形態は、①サイバーリスク専用のサイバー保険（以下「専用型サイバー保険」または「専用型保険」とする）、②E&O 保険[8]等の従来型の保険商品にサイバーリスクを補償する特約を付帯するもの、またはサイバーリスクに対する補償が明示されていないが約款上含まれると解釈されるもの（以下「サイバー補償を含む従来型保険」または「従来型保険」とする）、の 2 種類に大別される。

サイバー保険は、各企業のニーズに合わせてカスタマイズされることが多く、商品によって補償内容も異なる。サイバー保険の補償内容は、通常、第三者への損害賠償と、各種対応に要する自社の費用の 2 種類の損害に対する補償により構成される。主な補償内容としては図表 1 のものが挙げられる。

図表 1 のほか、企業の評判や信頼、ブランド等の失墜による損失等のレピュテーショナル・リスクまで補償の対象とする保険会社もあるが、このような保険会社はまだ少ない[9]。

米国ではほとんどの州において、個人情報を含むデータ漏えいが生じた場合、その企業等に、データ漏えいにより影響を受ける可能性がある顧客等への通知を義務付ける「データ漏えい通知法」が制定されている。このような規制や、実際にデータ漏えいの被害が多く発生していることなどを背景として、データ漏えいに伴う損害への企業の関心は高く、米国のサイバー保険では、データ漏えい時の損害に対する補償に特に重点が置かれている。

ただし、企業の関心は、データ漏えい等に伴う第三者への賠償責任に対する懸念から、その企業の事業に大きな影響を及ぼし得る物理的な財産損害や事業中断損害を引き起こす可能性があるサイバー攻撃に移ってきたとの見方もある[10]。

---

[7] サイバーリスクを補償する保険商品の多くは、Cyber Insurance、Cyber and Privacy Insurance、Cyber Liability & Data Breach Insurance 等の名称で呼ばれているが、本稿では、これらを総称してサイバー保険と呼んでいる。

[8] Errors and Omissions Insurance の略であり、過失怠慢賠償責任保険等と訳される。職務遂行上の過失や怠慢によって顧客等の第三者に損害を与えたことに起因して法律上の賠償責任を負うことで生じた損害を補償する保険である。

[9] PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査 2016」

[10] このような動きを反映し、サイバー保険に加入する企業の業種は、従来中心となっていた顧客の個人情報を多く抱える小売、金融サービス、ヘルスケア等に加え、製造業にも広がってきた。保険コンサルティング会社の Advisen が実施した米主要企業を対象とするサンプル調査によれば、2016 年の製造業者を

図表１　サイバー保険の主な補償内容

項目	補償の内容
データ漏えい等に関する賠償費用	データ漏えい等に伴い第三者に対して与えた損害に関し、これを賠償するための費用
データ修復費用	データの損壊に対する修復のための費用
顧客への通知、信用モニタリング等の費用	米国では、データが漏えいした場合に顧客等への通知を義務付けている州が多い。こうした通知の費用や、情報が漏えいした可能性のある顧客等の信用モニタリング等にかかる費用
フォレンジック調査費用	被害内容や被害の復旧方法、再発防止策等を明らかにするためのフォレンジック（forensics）調査のための費用
訴訟、罰金、恐喝	機密情報や知的財産の流出にかかわる訴訟費用、法律上の罰金、ランサムウェアによる恐喝に伴う費用等
事業中断に伴う損失	ネットワークやシステムの停止、事業中断等に伴う損失

（出典：各種資料をもとに作成）

b. 保険関連サービスの概要

多くの保険会社は、サイバー保険の引受のほか、企業に対しサイバーリスク管理のアドバイス等のサービスも提供している。例えば、保険会社は、企業のサイバー被害対応計画の策定や被害を想定した予行演習等を支援している。

また、サイバー保険に加入している企業に対し、企業が被害を受けた後の対応も支援している。例えば、データ侵害に関しては、データの修復、被害内容や被害の復旧方法等を明らかにするためのフォレンジック調査、企業の責任に関する法的な分析、顧客への通知と信用モニタリング等を含め、企業が対応するために役立つ支援サービスを提供している。

被害前の準備や被害後の対応に関するこのようなサービスは、自社のリソースが不足している中小企業に特に役立つとされている。保険会社によるこれらのサービスは、Symantec などのサイバーセキュリティ専門会社等と連携して提供されることも多い。

保険ブローカーも、顧客に対し、保険商品の案内のほか、一般的なサイバーリスクに関する情報の提供や各社のサイバーリスクに関する評価の支援、被害を受けた後の対応に関する支援等のサービスを提供している。関連サービスの内容は、ウェブサイトでの情報提供やセミナー、リスク評価ツールの提供等様々である[11]。

企業による保険会社や保険ブローカー等の保険関連サービスの利用は広がりつつある。ただし、被害を受けた後の対応に関する支援サービスは役立つが、被害を受ける前のリスク評価に関する支援サービスは役立っていないと考える企業が多いとの調査結果もある[12]。企業向けに提供される保険関連のサービスは、総じて以前よりも有効

契約者とするサイバー保険料は、前年比 89%増加し、サイバー保険料全体の 13%を占めることになった（2015 年は 9%）。工場のコンピュータ制御による自動化が進む中で、製造業者もサイバー被害対策への関心を高めていることがこの背景にある。

[11] 例えば、2017 年 5 月に発生したワナクライ攻撃の後、大手保険ブローカーの Willis Towers Watson は、顧客への警報を発信し、ランサムウェア攻撃の被害軽減のための方法等を紹介している。

[12] The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey” (2017.5)

に機能するようになってきたが、データの不足等を背景として、依然として事前のリスク評価は難しいという課題が窺える。

（2）サイバー保険市場の概況

本項では、サイバー保険市場の規模、引受を行っている保険会社、サイバー保険の収益性、サイバー保険の課題について説明する。

a. サイバー保険市場の規模

サイバー保険市場の規模については、正確な統計データがなく、また関係組織等の将来予測にも幅がある。再保険ブローカーの Aon Benfield[13]によれば、世界全体でのサイバー保険の市場規模[14]は概ね 25 億ﾄﾞﾙから 30 億ﾄﾞﾙ、世界全体のサイバー保険料の約 85%は米国内のリスク[15]によると推計されている。

全米保険庁長官会議（National Association of Insurance Commissioners：以下「NAIC」）[16]の公表データ[17]によれば、2016 年のサイバー保険の元受収入保険料は前年比約 30%増加[18]し、13 億 4,000 万ﾄﾞﾙとなっている[19]。この内訳は専用型保険：約 9 億ﾄﾞﾙ、従来型保険：約 4 億ﾄﾞﾙであった。ただし、NAIC のデータは、米国のサイバー保険市場のすべてをカバーしているわけではないため、実際のサイバー保険市場はこれよりも大きいと考えられている。

格付会社のフィッチ社（Fitch Ratings）によれば、米国のサイバー保険市場（元受収入保険料ベース）は、2022 年には 140 億ﾄﾞﾙにまで拡大すると予測されている。この背景として、ランサムウェアを含むサイバー攻撃の活発化により、企業のサイバーリスク対応への関心が高まること、およびサイバーセキュリティに関する規制の強化が進むこと等が、サイバー保険の需要の拡大につながるとしている[20]。

---

13 Aon Benfield, “Cyber Update: 2016 Cyber Insurance Profits and Performance” (2017.5)
14 専用型サイバー保険のみの数値とされている。
15 米国内のサイバーリスクは、概ね 20 億ﾄﾞﾙから 25 億ﾄﾞﾙに相当し、米国内の保険会社のほか、バミューダやロンドン等の保険会社によっても引き受けられている。
16 NAIC は、各州の保険庁長官によって構成される組織であり、直接的な監督権限は持たないが、各州の保険規制・監督の均質化・調和化を図るための取組を行っている。後記 6.(2)も参照願う。
17 2016 年より、保険会社が NAIC に提出する年次報告書に、サイバー保険の引受状況の記載が義務付けられた。具体的には、サイバー保険引受による元受計上保険料、元受既経過保険料、損害調査費用を含む保険金支払額に関する情報、残存契約件数、保険金支払件数等の情報を記載することが求められている。この情報収集の狙いは、保険会社によるサイバー保険の引受が円滑に進むように、保険規制当局が、サイバー保険市場の規模や成長性、保険金支払や収益性の状況をモニターするのに役立てることにある。また、この情報収集は、保険会社がサイバー保険の引受に伴い、万が一、巨額な保険金支払が生じ、保険会社の支払能力に致命的な影響を及ぼすことがないよう、保険規制当局が監視するためのものでもある。
18 ここ数年における米国のサイバー保険市場は、概ね年 25%～50%増のペースで急拡大していると推計している業界関係者が多い。
19 米国における 2015 年の企業向け損害保険の正味収入保険料は 2,471 億ﾄﾞﾙであり（Insurance Information Institute, “The Insurance Fact Book 2017”）、サイバー保険の保険料規模（NAIC の公表データに基づく数値）は、企業向け損害保険全体の 1%に満たない。
20 Fitch Ratings, “Global Attacks Spur Demand for Cyber Insurance” (2017.5)

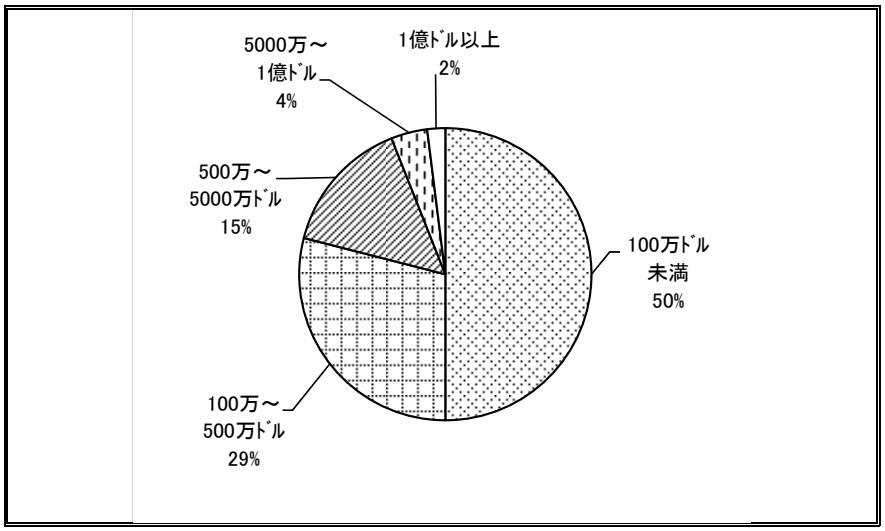
b. 引受を行っている保険会社

前記 a の NAIC の公表データによれば、2016 年にサイバー保険の引受を行った保険会社は 138 社であった。2016 年の元受収入保険料 13 億 4,000 万ﾄﾞﾙについて、上位 5 社の市場シェアは 52%であり、上位 10 社の市場シェアは 70%となっている[21]。

この元受収入保険料の保険会社別の内訳をみると、年間保険料 1 億ﾄﾞﾙ以上の保険会社は 3 社（138 社の 2%）存在し、これらを含め保険料 500 万ﾄﾞﾙ以上の保険会社は 29 社（同 21%）であった。一方、138 社のうちの 109 社（同 79%）は年間保険料 500 万ﾄﾞﾙ未満にとどまっている（図表 2 参照）。

なお、市場を先導している保険会社としては、AIG、Chubb、XL Group、Zurich Insurance、Beazley Group 等が挙げられる[22]。

図表 2　サイバー保険の元受収入保険料規模による保険会社数の構成比



（注）NAIC データの 2016 年の 138 社による合計 13 億 4,000 万ﾄﾞﾙの保険会社別構成比（年間の収入保険料規模による保険会社数の割合）

（出典：Aon Benfield, “Cyber Update: 2016 Cyber Insurance Profits and Performance” (2017.5) をもとに作成）

c. サイバー保険の収益性

前記 a の NAIC の公表データを利用した Aon Benfield の分析によれば、米国の保険業界全体でのサイバー保険の収益性については、2015 年は損害率[23]41.5%、事業費率 31.3%、コンバインド・レシオ 72.8%、2016 年は損害率 57.7%、事業費率 29.6%、

[21] 2015 年における上位 5 社のシェアは 61%、上位 10 社のシェアは 80%であった。2016 年における上位社のシェアは、まだ高水準にあるものの、新規参入の増加等により低下してきたと考えられる。

[22] フィッチ社によれば、2015 年における上位保険会社の市場シェアは、AIG22%、Chubb12%、XL Group12%であった。

[23] なお、NAIC に報告されたデータは暦年ベースであり、事故年ベースでみた場合は、損害率が上昇する可能性がある。

コンバインド・レシオ 87.3%と推計されており、2016 年は前年に比べ収益性が低下する結果となっている[24]。

フィッチ社は、2015 年および 2016 年におけるサイバー保険の収支結果は、保険会社にとって比較的良好だったとみている。しかし、サイバー保険市場が成熟し、サイバー被害が顕在化するまでにはまだ時間がかかるため、現時点では、サイバー保険の収益性について評価できる段階に至っていないとしている。

d. サイバー保険の課題

サイバー保険の普及に関しては課題も多い[25]。特に重要なのは、サイバー被害に関する有効なデータの不足である。この要因としては、サイバー被害の範囲が単にデータ漏えいにとどまらず、事業中断、財産の物理的損害および企業の評判低下による損失まで含まれ非常に広いこと、データの標準化が進んでいないこと、企業はサイバー攻撃を受けても気づかなかったり、被害を受けても公表したがらない場合もあること等が挙げられる。データ漏えいによる損害のデータは、ある程度蓄積されてきたが、システム障害やこれに伴う事業中断等による損害のデータはまだ少ない状況にある。

また、技術の発展に伴いリスクそのものが大きく変化していることや、サイバー保険による補償の範囲も企業のニーズに合わせて変化していることもあり、適正なリスクの評価や保険料率の設定は、他の保険商品に比べ非常に難しいものとなっている。

このため、リスクの出し手である企業のニーズと、受け手である保険会社との間にはギャップが生じやすい。例えば、大企業が自社のリスクに見合うよう支払限度額の引上げを希望しても、保険会社がこれに応じられない場合がある。また、エネルギー、製造、交通業界等の企業にとって、サイバー攻撃が物理的損害や人身傷害を引き起こすリスクも見過ごせないが、これらのリスクを引き受けている保険会社はまだ少ない。

さらに、保険料率がリスクに見合っていない場合も想定されることから、保険会社のエクスポージャーにつき懸念を示す向きもある。フィッチ社は、サイバーリスクの評価や料率設定には不確実な要素が大きく、個別の保険会社がサイバー保険の引受を積極的に拡大したり、サイバーリスクの集積が高水準になったりする場合、格付けにマイナスの影響を及ぼす可能性があるとしている[26]。フィッチ社によれば、過去の保険金支払によるデータの蓄積がまだ少ないため、保険会社にとっては、保険数理的に

---

[24] Aon Benfield, “Cyber Update: 2016 Cyber Insurance Profits and Performance” (2017.5). なお、2016 年の収益性について専用型保険と従来型保険に分けてみた場合、専用型保険は損害率 59.8%、事業費率 28.7%、コンバインド・レシオ 88.5%、従来型保険は損害率 53.4%、事業費率 34.4%、コンバインド・レシオ 87.9%と推計されている。

[25] サイバー保険を巡る課題については、損保総研レポート第 116 号も参照願う。

[26] S&P 社、Moody’s 社、フィッチ社、A.M.ベスト社等の米国の格付会社は、損害保険会社の格付評価において、保険会社自身が抱えているサイバーリスク、およびサイバー保険の引受に伴うリスクの 2 つの視点からサイバーリスクを重視しており、抱えているリスクが大きく、その管理が不十分な保険会社は、格付けに影響を及ぼす可能性があるとしている。A.M.ベスト社の格付評価における基本的な考え方は損保総研レポート第 116 号を参照願う。

強固な料率設定とサイバーリスクに関する補償の条件等を確立することが優先的な課題だとされている。

３．サイバー保険への企業の加入状況

サイバー保険への企業の加入状況については、企業向けのアンケート調査等から大まかな傾向を把握できる。ただし、調査対象となる企業の規模の違い等によって調査結果には幅がある。

本項では、米国の保険代理店・ブローカー協議会（CIAB）、リスク保険マネジメント協会（RIMS）、データ分析会社 FICO 等の調査結果を取り上げて説明する。

（1）保険代理店・ブローカー協議会の調査

本項では、米国の保険代理店・ブローカー協議会（The Council of Insurance Agents & Brokers：CIAB）による、保険代理店やブローカーの顧客企業を対象とした調査について紹介する。この調査は半年ごとに実施されており、中小企業から大企業まで幅広く対象としているため、概ね米国の企業の平均的な状況を示していると考えられる。

a．加入率

2017 年 4 月に実施された調査（公表は 5 月）[27]では、何らかのサイバーリスクの補償を有している企業の割合は 32%となっている（2016 年 10 月調査の 29%に比べ 3%上昇した）。また過去半年間にサイバー保険に加入した企業のうち、72%が従来型保険ではなく専用型保険を選択しており、専用型保険への加入が進んでいることが窺える。保険ブローカーも、専用型保険への加入を企業に推奨しているとされている。

b．支払限度額

2017 年 4 月の調査では、サイバー保険の支払限度額は 600 万ﾄﾞﾙの設定が最多となっている。2016 年 10 月の調査では 300 万ﾄﾞﾙが最多であったため、支払限度額は拡大傾向にあると考えられる。

また、企業が手配可能な最大支払限度額は、複数の保険会社のサイバー保険を組み合わせることで 2016 年 10 月調査では 5 億ﾄﾞﾙであったが、2017 年 4 月調査では 6 億ﾄﾞﾙまで引き上げられたとされている。

なお、サイバー保険市場のキャパシティについては、企業の 81%が問題ないと回答しており、全体的には、支払限度額の設定に満足している企業が多いことが窺える。ただし、中小企業向けの保険引受はある程度定型化が進み、緩和気味にある一方、個人情報の取扱が重要である小売、ヘルスケア、金融サービス等の大企業に対しては、

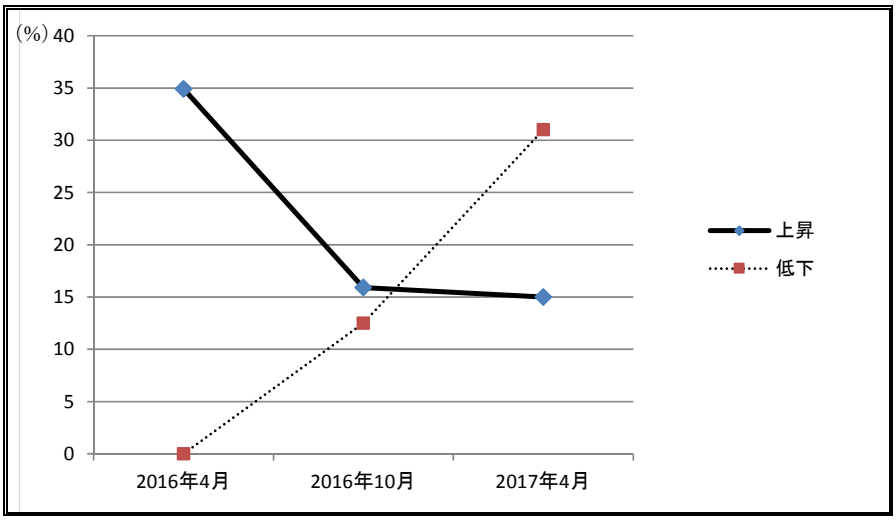
[27] The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey” (2017.5)

保険会社の引受審査が厳しくなっているとの指摘もある。

c. サイバー保険の保険料率の動向

サイバー保険の保険料率は、2015 年から 2016 年前半までは、総じて堅調に推移してきた[28]。しかし、2017 年 4 月の調査では、保険料の変化に関する回答の割合が、横ばい 54%、低下 31%、上昇 15%の結果となり、保険料率は低下傾向に変化した可能性が示された（図表 3 参照）。

図表 3　サイバー保険の保険料水準の変化



（注）保険代理店・ブローカー協議会の調査において、保険料が上昇した、または低下したと回答した企業の割合

（出典：The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey” (2017.5) ほかをもとに作成）

（2）RIMS の調査（大企業中心の調査）

リスク保険マネジメント協会（Risk and Insurance Management Society : RIMS）[29]が会員企業のうちの 272 社を対象として行ったアンケート調査[30]について紹介する。なお、調査対象となった企業の 56.5%は、年間売上高 10 億ﾄﾞﾙ以上の大企業である。

a. 加入率

2016 年のアンケート調査によれば、サイバーリスクを第三者に移転している企業の割合は 69%となり、2015 年の 59%から 10%上昇した。

---

[28] The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey” (2016.4)
[29] RIMS は、本部をニューヨークに置き、米国およびカナダを中心として世界 60 カ国以上に計 11,000 人以上のリスクマネジメントのプロフェッショナルを会員として擁する、世界最大のリスクマネジメント団体である。
[30] RIMS, “RIMS 2016 Cyber Survey” (2016.10)。2016 年 8 月～9 月に実施された調査である。

サイバーリスクを第三者に移転している企業のうち、専用型サイバー保険に加入している企業の割合は80%となり、2015年の51%から29%の上昇となった。このデータからも、サイバー保険は、従来型保険ではなく、専用型保険が主流になってきたことが窺える。

サイバー保険への加入率が上昇している要因としては、企業にとってサイバー攻撃によるデータ漏えいの被害額がここ数年拡大傾向にあること等が挙げられている[31]。

b. 補償対象リスク

サイバー保険でどのリスクを補償対象としているかとの質問に対する回答（重複回答）は次のとおりであり、データ漏えい費用の補償が中心となっていることが窺える。

○ データ漏えい費用：91%
○ データ修復費用：80%
○ サイバー攻撃による金銭搾取（cyber extortion）：78%
○ ネットワーク・事業の中断に伴う損失：76%
○ 罰金・制裁金：63%
○ 専門職業人賠償責任：50%
○ 企業の評判低下による損失：42%
○ 事業上の機密事項の盗難：27%

一方、サイバーリスクで想定される被害の中で、その企業にとって最も重要なものは何かとの質問に対する回答の構成比は、データ漏えいによるプライバシー侵害：26%、事業中断：23%、企業の評判低下：23%、法的支払義務・罰金・制裁金：14%、情報セキュリティ対応：10%、その他：4%であった。

企業の評判低下や事業中断に伴う損失については、企業が重要視している割には、補償の手配が進んでいないことが窺える。

c. 支払限度額

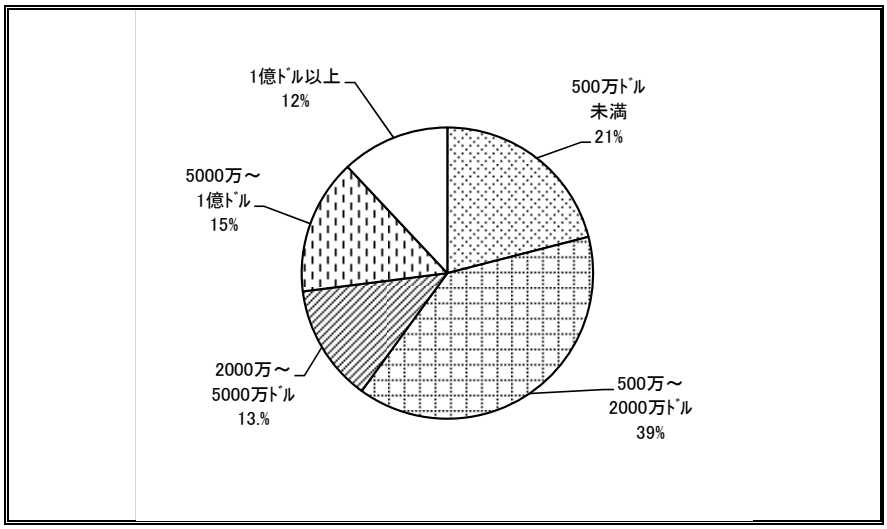
サイバー保険の支払限度額は、500 万～2,000 万ﾄﾞﾙに設定している企業の割合が39%を占め、この水準が最多となっている（図表4参照）。

500万ﾄﾞﾙ未満の割合は、2015年の23%から2016年は21%へと低下した反面、500万～2,000万ﾄﾞﾙの割合は、2015年の35%から2016年は39%へと上昇した。この変化の一因としては、500万ﾄﾞﾙ未満であった一部の企業が支払限度額を引き上げ、500万～2,000万ﾄﾞﾙの層にシフトした可能性等が考えられる。

[31] またこの調査では、契約上の義務を果たすためにサイバー保険に加入していると回答した企業の割合が2015年は8%であったのに対し、2016年は25%まで上昇している。このデータからは、取引先等との契約上の義務を果たすためにサイバー保険に加入する企業が増えている状況が窺える。

一方、支払限度額を 1 億ﾄﾞﾙ以上に設定している企業の割合は 2015 年の 11%から 2016 年は 12%へとわずかながら上昇している。

図表 4　サイバー保険の支払限度額（2016 年）



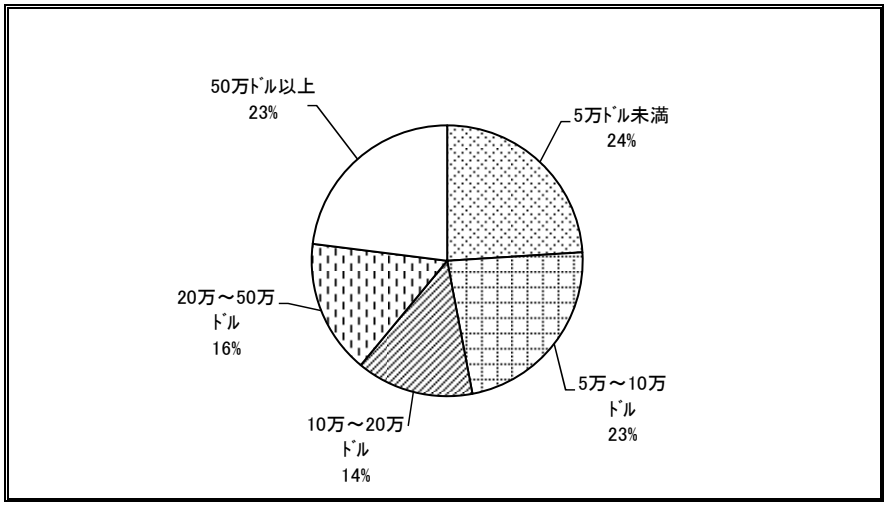
（出典：RIMS, “2016 RIMS Cyber Survey” (2016.10)をもとに作成）

d. 保険料の水準

2016 年において企業が支払った年間の保険料は、50 万ﾄﾞﾙ以上の企業の割合が 23%を占める一方、5 万ﾄﾞﾙ未満の企業が 24%を占め、これを含め 10 万ﾄﾞﾙ未満の企業が 47%となっている（図表 5 参照）。

2015 年の調査では 10 万ﾄﾞﾙ未満の企業が 45%であったため、2016 年は 10 万ﾄﾞﾙ未満の比較的少額の保険料の企業の割合がわずかながら上昇する結果となっている。

図表 5　サイバー保険の年間保険料（2016 年）



（出典：RIMS, “2016 RIMS Cyber Survey” (2016.10)をもとに作成）

（3）その他の調査

a. FICO の調査

シリコンバレーを拠点とするデータ分析会社 FICO の調査[32]は、対象企業が大企業から中小企業まで幅広く、平均的な企業規模は RIMS の調査対象に比べ小さい。

2017 年 5 月に公表された調査結果によれば、米国でサイバー保険に加入している企業の割合は RIMS の調査よりも低く、米国の企業の 50%以上がサイバー保険に加入しておらず、そのうちの 27%は今後も加入予定がないと回答している。

サイバー保険の加入率が低いことおよび今後の加入にも前向きでない企業が多い理由の 1 つとして、サイバー保険の保険料の設定に対する企業側の不信感が挙げられている。FICO によれば、回答企業の多くは、保険会社によるリスク評価および保険料決定のプロセスに何らかの改善余地があると考えており、例えば、保険会社が保険料の設定について明確なガイドラインを提供すること、保険料の調整を行う理由を明確に説明すること、サイバーリスクを対象とする業界標準を設けることなどが必要とされている。

b. Hiscox 等の調査

他の調査でも、サイバー保険の加入に前向きでない企業が一定存在すること、およびその理由が挙げられている[33]。2017 年 2 月に公表された、スペシャルティ保険に強みを持つ保険会社 Hiscox の調査によれば、米国の企業の 55%がサイバー保険に加入している一方、26%はサイバー保険に加入する予定はないと回答している。加入の予定がない理由としては、その企業ではサイバー保険に加入する必要性がないこと、サイバー保険は複雑過ぎて何が補償対象となるのか理解できないこと等が挙げられている。

Deloitte が公表したレポート[34]においても、サイバー保険への加入に前向きでない企業が一定存在するとし、その理由として、サイバーリスクやサイバー保険の内容を理解していない企業が多いこと、加えてサイバー保険の補償内容に関する標準化が進んでいないこと等が挙げられている。似たようなサイバー保険であっても、保険会社が異なればそれぞれ補償内容等が異なるため、購入側にとって保険料の比較が困難なことが問題とされている。

---

[32] FICO の依頼により、調査・コンサルティング会社 Ovum が 2017 年 3 月から 4 月に実施した電話による聞き取り調査であり、米国、カナダ、イギリス、北欧等の 350 社の IT の責任者である役員等を対象としている。対象企業の業種は、金融サービス、ヘルスケア、テレコミュニケーション、小売、電子商取引、メディア・サービス等である（FICO, “What the C-suite Needs to Know About Cyber-readiness” (2017)）。

[33] Insurance Journal, “Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance” (2017.5.31)

[34] Deloitte, “Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market” (2017)

なお、この Deloitte のレポートでは、企業の加入を妨げている要因を克服するために、保険業界は、保険契約における用語の標準化、リスク・インフォームド・モデル[35]の構築、ターゲットとする業界やエクスポージャーの大きさ等を明確にした保険引受、企業のサイバーリスク管理に対する従来以上に包括的な支援サービスの提供等が必要とされている。

４．サイバー保険における保険金支払の動向

本項では、米国のサイバー保険で最も重視されているデータ漏えいに伴う保険金支払に関するサンプル調査[36]である、ネット・デリジェンス（NetDiligence）社[37]の調査結果の概要を紹介する。

この調査で抽出対象となった 2016 年におけるサイバー保険の保険金請求件数は 176 件であり、このうち保険金支払が確認された 172 件の支払保険金の総額は 1 億 1,434 万ﾄﾞﾙとなった（2015 年の調査では 160 件の保険金請求につき、支払保険金の総額は 7,550 万ﾄﾞﾙであった）。

2016 年における保険金の平均支払額は、2015 年よりもわずかながら低下し 66 万 5,000 ﾄﾞﾙとなった。中央値は 6 万ﾄﾞﾙであった。2016 年は、少額の保険金支払が前年に比べわずかながら増加しており、これは中小企業もサイバー攻撃の標的として狙われることが増えたことの表れと考えられる。

（1）漏えいデータ件数と保険金支払額

1 事故あたりの漏えいデータ件数と、漏えいデータ 1 件あたりの保険金支払額については、次の結果となった。

○　1 事故あたりの漏えいデータ件数

図表 6 のとおり、2016 年の 1 事故あたりの漏えいデータ件数は約 204 万件となり、2015 年の 317 万件から減少した。2016 年の中央値は、この平均値に比べて非常に少ない 1,339 件（2015 年は 2,300 件）に過ぎず、平均値は、漏えいデータ件数の多い事故の影響で統計上引き上げられているが、中央値をみると、比較的少ない件数のデータ漏えい事故も多数発生していることが窺える。

---

[35] 保険申込者であるその企業のサイバーリスクに対する安全策や損害軽減策等のリスク管理策を見極めたうえで保険料率を決定し引受を行うモデルを意味する。

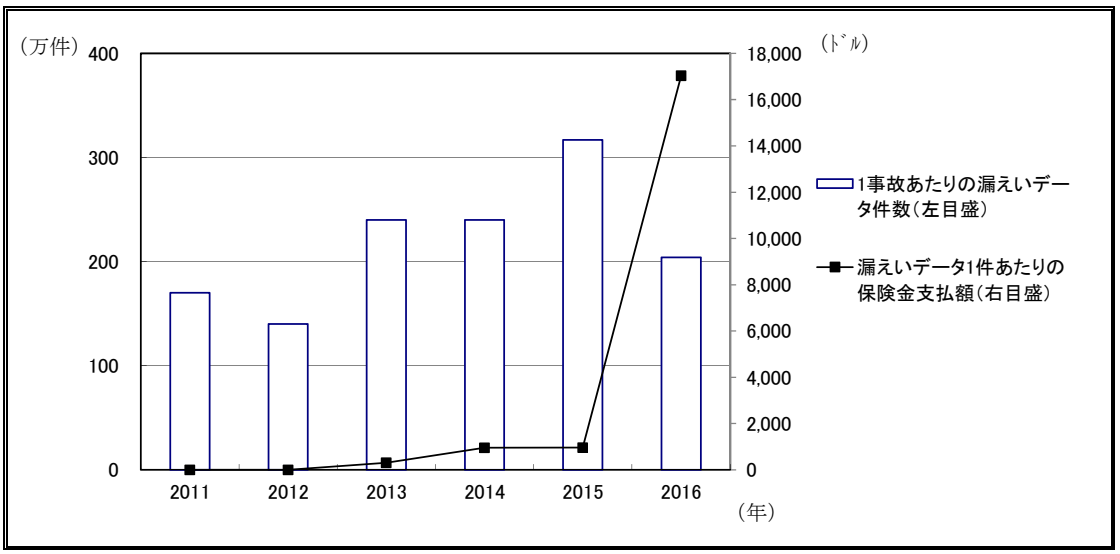
[36] NetDiligence, “2016 Cyber Claims Study”. サイバー保険の引受を行っている AIG、Zurich、Beazley を含む主要 17 社において、同期間中に保険金請求がなされた 176 件に関する調査を実施したものである。この調査における支払保険金のデータは、まだ支払総額が確定しておらず、調査時点までの金額を示している。また、このサンプリング調査は、米国の同時期におけるサイバー保険金支払全体の一部を占めるに過ぎない。

[37] NetDiligence 社は、サイバーリスクの評価やデータ侵害に関する情報の提供等を行うサービス会社である。

○　漏えいデータ１件あたりの保険金支払額

2016年の漏えいデータ１件あたりの保険金支払額は１万7,035ﾄﾞﾙとなり、2015年の 964ﾄﾞﾙから大幅に拡大した。さらに、数年単位でみると、この数値は急激に拡大してきていることがわかる（図表６参照）。ただし、2016年に、漏えいデータ 1 件あたりの保険金支払額が急拡大した要因としては、漏えいデータが 10 件未満と少ないながら保険金支払額が大きい事故が３件あったことが大きく影響している。一部の事故のために平均値は高くなっているものの、中央値は漏えいデータ１件あたり約 40ﾄﾞﾙにとどまっている。

図表６　１事故あたりの漏えいデータ件数と、漏えいデータ１件あたりの保険金支払額



（出典：NetDiligence, “2016 Cyber Claims Study” をもとに作成）

（2）保険金支払額の内訳

2016年の保険金支払総額１億1,400万ﾄﾞﾙのうち、保険金の使途の分類が確認できた7,600万ﾄﾞﾙの構成比をみると、75%が危機対応サービス（フォレンジック調査、顧客への通知、信用・IDモニタリング等の費用）であり、20%が法的解決または法的防御のための費用、5%が罰金となっている。

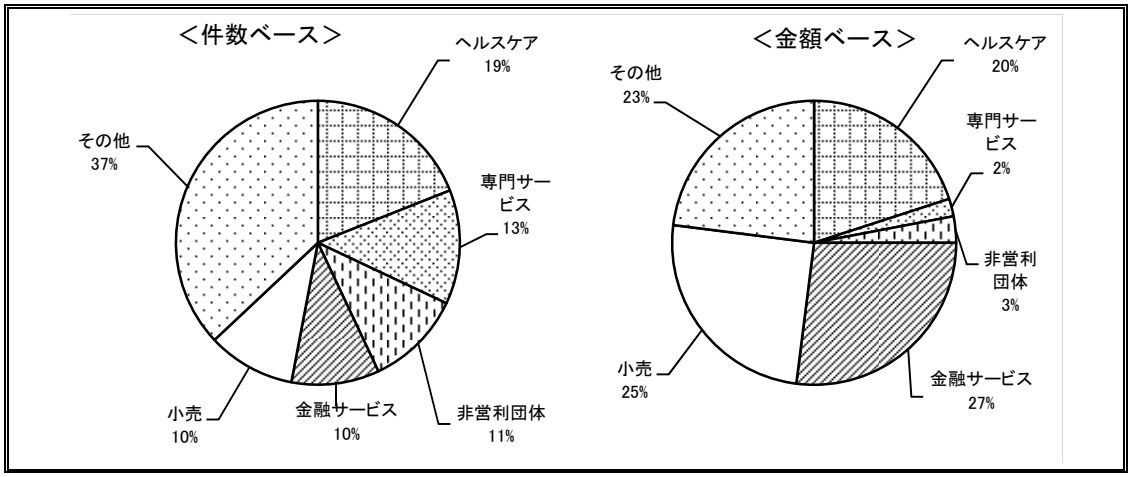
本項では、さらに 2016 年の保険金請求および保険金支払の内訳につき、業種別、企業の収入規模別、損害の原因別に紹介する。

a. 業種別

2016 年の保険金請求件数 176 件の業種別内訳につき件数ベースでみると、ヘルスケア 19%、専門サービス 13%、非営利団体 11%、金融サービス 10%、小売 10%等が上位を占めている（図表７参照）。ヘルスケアの割合は 2015 年の 21%に比べ低下したものの、前年に続き 2016 年も最多の業種となっている。

一方、保険金の金額ベースでみると、金融サービス 27%、小売 25%、ヘルスケア 20%の割合が高い結果となった。2015 年は 44%を占めて最大であったヘルスケアの割合は 2016 年には低下し 3 位となっている。金融サービスや小売、ヘルスケアの割合が他の業種に比べ高いのは、これらの業界では顧客の個人情報を多く抱えており、ハッカーやマルウェア[38]・ウィルスの攻撃により、大きな被害が発生しているためである。

図表 7　2016 年の保険金の内訳（業種別）



（注）件数ベースは保険金請求 176 件に対する割合。金額ベースは、保険金支払 172 件に対する割合。
（出典：NetDiligence, “2016 Cyber Claims Study” をもとに作成）

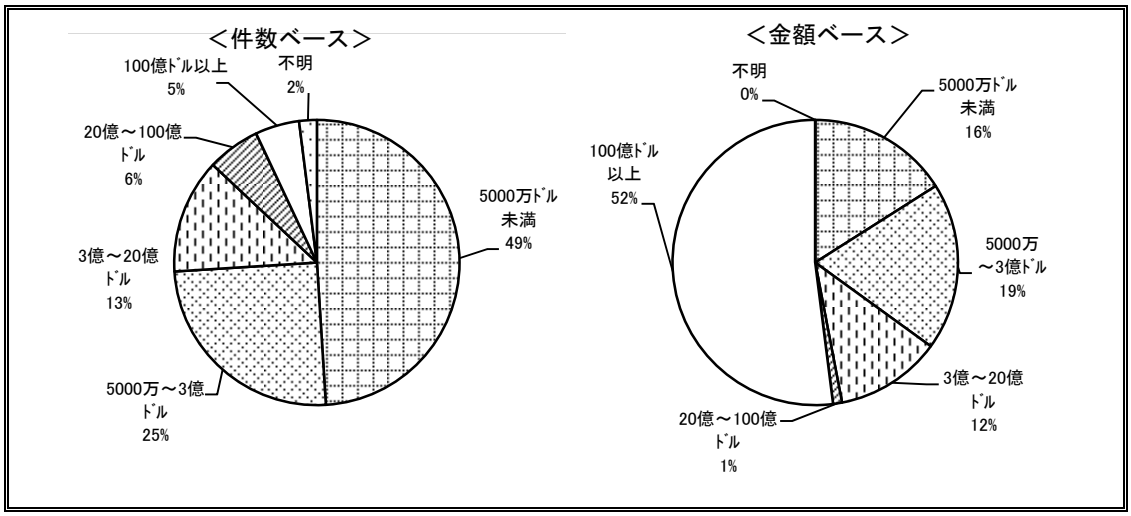
b. 企業の収入規模別

2016 年の保険金請求につき企業の収入規模別に件数ベースでみると、収入規模 5,000 万ﾄﾞﾙ未満の企業が 49%となり、これを含め 20 億ﾄﾞﾙ未満の企業が全体の 87%を占めている（図表 8 参照）[39]。2015 年における 20 億ﾄﾞﾙ未満の企業の割合は 71%であったため、2016 年は、比較的規模の小さい企業による保険金請求が増えたと考えられる。

2016 年の保険金の金額ベースでは、件数ベースで 87%を占めた収入規模 20 億ﾄﾞﾙ未満の中小企業は金額ベースでは 47%にとどまっている。一方、件数ベースでは 5%を占めるに過ぎない収入規模 100 億ﾄﾞﾙ以上の大企業が金額ベースでは 52%を占める結果となった。これには、企業規模が大きくなるにつれ、1 件あたりの保険金支払額も大きくなる傾向が反映されている。

[38] マルウェアは、不正かつ有害な動作を行うソフトウェアの総称である。
[39] ネット・デリジェンス社は、2015 年および 2016 年において大企業よりも中小企業の割合が高い要因として、企業の総数自体において大企業よりも中小企業の方が多いことに加え、中小企業の方がサイバーリスクに対する認識が低く、また適正なデータ保護や従業員に対する研修を実現するためのリソースに乏しいため、大企業に比べサイバーリスク対策が進んでいないことを挙げている。

図表 8　2016 年の保険金の内訳（企業の収入規模別）



（注）件数ベースは保険金請求 176 件に対する割合。金額ベースは、保険金支払 172 件に対する割合。

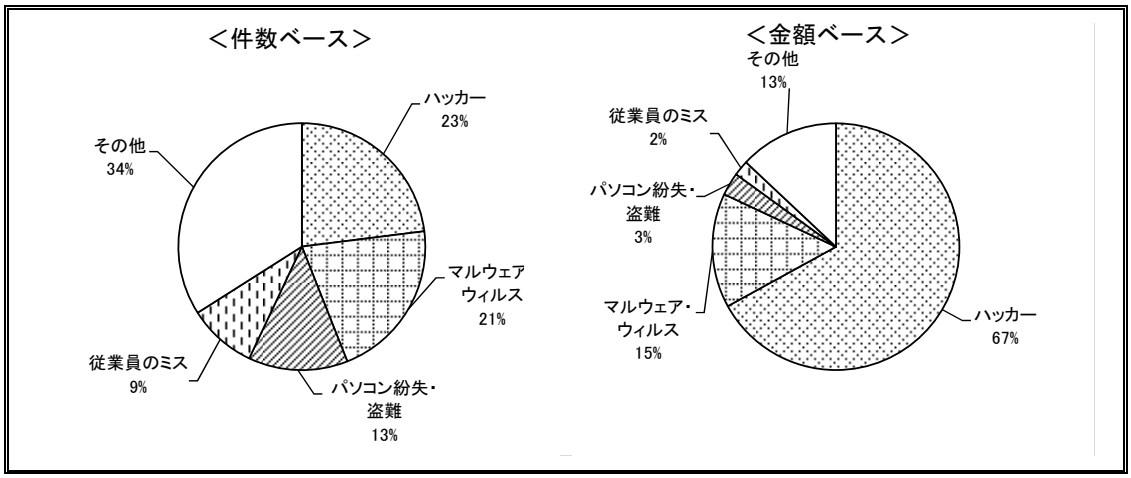
（出典：NetDiligence, “2016 Cyber Claims Study” をもとに作成）

c. 損害の原因別

2016 年の保険金請求につき損害の原因別に件数ベースでみると、ハッカー23%、マルウェア・ウィルス 21%、パソコンの紛失・盗難 13%、従業員のミス 9%等となっている（図表 9 参照）。

一方、保険金の金額ベースでみると、ハッカー67%、マルウェア・ウィルス 15%等が大きな割合を占めており、パソコンの紛失・盗難や従業員のミスに比べ、悪意のある外部からの攻撃による被害が大きかったことがわかる。2016 年におけるこの傾向は、概ね 2015 年と同様であった。

図表 9　2016 年の保険金の内訳（損害の原因別）



（注）件数ベースは保険金請求 176 件に対する割合。金額ベースは、保険金支払 172 件に対する割合。

（出典：NetDiligence, “2016 Cyber Claims Study” をもとに作成）

（3）その他の特徴

2016 年の保険金支払件数のうち、30%は企業等の内部者の行為に起因する損害であり、この割合は 2015 年の 32%からわずかながら低下した。2016 年におけるこの保険金支払のうち 77%は、従業員等の悪意のないミスによるものであり、残りの 23%は、従業員等の悪意によるものであった。

2016 年におけるランサムウェアによる保険金請求は 6 件確認され、1 件あたりの平均保険金支払額は 3 万 2,000ﾄﾞﾙであった[40]。フィッシング詐欺[41]およびソーシャル・エンジニアリング[42]に関連する保険金請求は 8 件確認され、平均支払額は 12 万 3,000ﾄﾞﾙであった。

５．サイバー保険を巡る新たな動き

サイバー保険を巡る比較的新しい動きとして、本項では、サイバーリスクモデルの構築、キャプティブの利用、保険リンク証券（ILS）の利用について取り上げる。

（1）サイバーリスクモデルの構築

前記 2.(2)d のとおり、サイバーリスクの評価や保険料率の設定には非常に困難な要素が存在する。しかし、サイバー保険市場が急速に拡大する中で、このような状況を改善するため、大手モデリング会社やサイバーリスク分析の専門会社等が中心となって、サイバーリスクモデルの構築に本格的に取り組むようになってきた。

大手モデリング会社の RMS（Risk Management Solutions：以下「RMS」）、AIR Worldwide（以下「AIR」）、シリコンバレーを拠点とするサイバーリスク分析の専門会社であるサイエンス社（Cyence）[43]などは既にサイバーリスクモデルを開発し公表している[44]。しかし、総じてサイバーリスクモデルの構築はまだ始まったばかりの段階であり、自然災害リスクモデルよりも 20 年程遅れているとの見方もある。

サイバーリスクモデルの構築には、信頼できるデータの蓄積が必要であるが、サイバーリスクは自然災害リスクと異なり、リスクに関する統一的な公式データがなく、

---

[40] 6 件のうち、5 件はマルウェア、ウィルスに分類され、1 件はハッカーに分類されている。6 件のうち 5 件は、収入規模 5,000 万ﾄﾞﾙ未満の中小企業によるものであった。

[41] 実在の金融機関やショッピングサイト等を装った電子メールを送信し、これらのホームページとそっくりの偽りのサイトに誘導し、銀行口座番号やクレジットカード番号、パスワード、暗証番号等の重要な情報を入力させて搾取する行為を指す。

[42] コンピュータやネットワークの管理者や利用者等から、パスワードなどの保安上重要な情報を、情報通信技術を使用せず、人間の心理的な隙や行動のミスにつけ込んで盗み出す方法であり、例えば、巧みな話術による誘導や盗み聞き、盗み見等の手段が該当する。

[43] Cyence は 2016 年にサイバーモデルを開発し公表した。これは、保険会社がリスクを評価するために必要な様々な公開情報源からデータを収集し、保険会社を支援するものである。

[44] Guy Carpenter と Symantec もサイバー集積モデルにつき共同開発を進めることを 2016 年 5 月に公表している。

政府機関等が保有する公的な被害データや保険関連データについても、データの基準がばらばらであり、統一的に分析することが困難になっている。このような問題を解決するため、RMS や AIR はデータの標準的なフォーマットを構築している。

ここでは、サイバーリスクモデルの構築やデータ標準化を進める RMS の事例を取り上げて説明する[45]。

RMS は、2016 年 2 月にサイバー集積管理システム（Cyber Accumulation Management System：CAMS）を公表した。これは、サイバーリスクの集積を理解するための最初のモデルであると同時に、共通のデータ標準フォーマットを提供するものである。

さらに RMS は、2017 年 5 月に第 2 世代のサイバー集積管理システムを公表した。これは、モデル構築後短期間ながらサイバーリスクを取り巻く環境が大きく変化したとの認識に基づき、従来のモデルをアップデートして進化させたものである。この構成要素の概要は次のとおりである。

○　共通データ標準（A Common Data Standard）

ケンブリッジ大学リスク研究センター（University of Cambridge Center for Risk Studies）と連携して、サイバーリスクの特定、定量化、報告のための標準フォーマットを策定した。この標準フォーマットは、サイバーリスクの集積を理解し計測するために必要な共通言語と共通アプローチを提供する。

○　サイバー損失プロセスモデル（Cyber Loss Process Models）

サイバー保険の予想最大損失額（Probable Maximum Loss：PML）を定義することは、経済全体に連鎖的に影響を及ぼす大規模な損失が現実に発生した経験がないため非常に難しい。そこで RMS は、保険会社や再保険会社の保険引受ポートフォリオに重要なサイバー脅威、ストレステストを適用するリスクモデルを構築した。保険会社はこのモデルの利用によって、経済全体に連鎖的に影響を及ぼす大規模な損失がどの程度の水準となるのか探ることが可能になる。

○　オープン分析プラットフォーム（Open Analytics Platform）

サイバー保険のエクスポージャーや収益性について分析する枠組みを提供する新しいユーザー・インターフェースであり、効率的なデータ管理とデータ分析への継ぎ目のないアクセスを可能とする。

RMS は、上記のようなデータ標準化やサイバーリスクモデルの構築の取組みはまだ初期の段階にあり、解決すべき課題が多く残されていると認識している。

[45] RMS, Center for Risk Studies University of Cambridge, “2017 Cyber Risk Landscape”

（2）キャプティブの利用

サイバー保険の市場は拡大しているものの、市場で入手できるサイバー保険では、企業が希望する条件や支払限度額に合わない場合もある。このため、サイバーリスクの管理のためにキャプティブ[46]の利用を検討する企業もある。

保険会社がサイバーリスクの引受に消極的な場合、企業は従来の保険商品に頼らずキャプティブを利用して、サイバー被害に伴う自社の業績の変動を軽減することが可能となる。ただし、キャプティブを利用してサイバーリスクを効率的に管理するためには、自社のサイバーリスクに対する理解や適正なリスク評価が欠かせない。このような企業のニーズに対し、大手保険ブローカーやサイバーセキュリティ専門会社、モデリング会社等が支援サービスを提供しようとする動きがある。

ここでは、大手保険ブローカーAon が提供する、サイバーリスク補償のためのキャプティブ関連のサービスの例を紹介する。Aon グループのリスクコンサルティング事業を担う Aon Global Risk Consulting は、2017 年 1 月、サイバー・キャプティブ・プログラムを開発した。企業は、このプログラムの利用によってサイバーリスクの特定、定量化等の支援を受け、キャプティブ[47]を通じた自己保有と 4 億ﾄﾞﾙまでのリスク移転を行うことが可能になる。

Aon は、企業は伝統的な保険市場ではサイバーリスクの包括的な補償を入手しづらいことから、キャプティブを通じた包括的なリスク移転の手段を企業に提供できるよう、このプログラムを開発した。Aon は、多くの企業がサイバー攻撃により財産損害や事業中断の被害を受ける可能性がある状況に直面しており、サイバーリスクに対する従来以上に包括的な補償が必要と認識していた。企業は、自社にとっての重要な問題や脅威を認識したうえで、包括的な補償を手配することができるとしている。

Aon のサイバー・キャプティブ・プログラムは主に以下の内容で構成されている。

○ Aon サイバー強靭性レビュー（Aon Cyber Resilience Review）

Aon が企業のサイバーリスクの特定、評価、定量化を支援する。Aon が提供する下記のソリューションを企業が利用するためにはこのレビューを受ける必要がある。企業は、自身のリスクプロファイルを理解することを通じて、リスクのどの程度をキャプティブで保有し、どの程度を Aon のプログラムに移転するかの判断が容易になる。

○ Aon サイバー企業ソリューション（Aon Cyber Enterprise Solutions）

米国、ロンドン、バミューダに所在する Aon のサイバー専門チーム、財産チーム、PL（生産物賠償責任）チームが緊密に協力して構築したソリューションであ

[46] キャプティブは、一般の企業がその子会社として設立する、自社のリスクを引き受ける保険会社を意味する。企業は、効果的なリスクの保有や管理等を目的としてキャプティブを利用する。
[47] バミューダ所在のシングル・ペアレント・キャプティブ（一つの親会社等によって所有されるキャプティブ）の利用が想定されている。

る。企業のキャプティブは、このソリューションの利用によって、再保険またはエクセス保険[48]ベースで 4 億ﾄﾞﾙまでの包括的なサイバーリスク補償を得ることができる。

主な特徴は以下のとおり。

・適用地域は全世界、全業種対応
・1 契約の支払限度額は 2,500 万ﾄﾞﾙ超過で 4 億ﾄﾞﾙまで適用可能
・補償の範囲は、サイバー攻撃による財産損害から事業中断損害に至るまで非常に広範（例えば、保険による補てんが認められる国においては、個人情報保護法違反による罰金まで補償の対象となる）

（3）保険リンク証券（ILS）の利用

サイバーリスクをカバーするため、保険リンク証券（Insurance-Linked Securities：以下「ILS」）[49]の利用も検討されている[50]。米国土安全保障省（DHS）の前秘書官 Tom Ridge 氏は、サイバーリスクは非常に巨大で重要なリスクであり、ILS を利用した資本市場へのリスク移転が重要な役割を果たす可能性があるとしている。

ILS を利用したリスクの移転は、単純化していえば、企業がリスクの出し手となる場合、従来の保険市場を通さず、直接、資本市場の投資家にリスクを移転することになる。また、元受保険会社がリスクの出し手になる場合は、従来の再保険市場を通さず、直接、資本市場の投資家にリスクを移転することになる。したがって、ILS を利用したサイバーリスクの移転が実現し活発化すれば、従来の保険市場や再保険市場にも大きな影響が生じる可能性がある。

ただし、ILS によるリスク移転が有効に機能するためには、サイバーリスクの損害に関するデータが蓄積され、洗練されたリスクモデルが構築されることが欠かせないとの見方が多い[51]。

---

[48] エクセス保険とは、損害が一定割合または一定額を超えない場合は補償されず、それを超えた場合には、超えた分だけを補償する方式をいう。

[49] 保険リンク証券は、ある特定の保険リスクの損害実績に連動してその価値が変動する証券化商品である。この証券の販売・購入を通じて、その保険リスクの全部または一部を資本市場の投資家に移転することができる。投資家にとっては、従来の株式市場や債券市場とは相関性の低い保険リスクが新たな投資対象となることによって、リスクの分散が図れる等のメリットがある。サイバーリスクの引受は、再保険会社にとっても、データの不足等からリスクを的確に評価することが難しく、またサイバーリスクの性質上、再保険会社にリスクの集積の問題が生じやすい。このため、今後サイバー保険市場が急成長したときに、元受保険会社が適正な再保険料で再保険を手配することが難しくなる可能性があり、そのような場合、保険リンク証券を利用した巨大な資本市場へのリスク移転が重要になると考えられる。保険リンク証券の仕組みや特徴等については、鈴木久子「Insurance Linked Securities（ILS）がもたらす変化－資本市場による保険リスクの引受け－」損保ジャパン日本興亜総研レポート Vol.70（損保ジャパン日本興亜総合研究所、2017.3）を参照願う。

[50] 2016 年 5 月には、クレディ・スイスがオペレーショナル・リスク等を移転する ILS を発行しており、この ILS では、不正行為や会計処理の誤り等の伝統的なオペレーショナル・リスクのほか、事業中断を引き起こす IT システムの障害等のサイバーリスクも移転の対象となった。

[51] JLT Re, “JLT Re VIEWPOINT Unlocking the potential of the cyber market” (2017)

これらのほか、サイバーリスクを対象とするILSの発行を妨げる要因として次のような指摘もある[52]。

○　株式市場や債券市場等とのリスク相関の可能性があること（投資家側の視点）

ILSの一種であり、1990年代に開発され、その後発行が拡大してきた異常災害債券（キャット・ボンド）の場合は、異常災害が発生するリスクと株式市場や債券市場のリスクとは相関性が低く、投資家にとって分散投資の効果を得やすいとみられている。これに対し、広範なサイバー攻撃が生じた場合には株式市場や債券市場の投資価値にも影響を及ぼす可能性があり、サイバーリスクを対象とするILSに投資するリスクは、株式市場や債券市場のリスクと相関性が低いと言い切れない可能性がある。

○　ベーシスリスクの存在（リスクの出し手側の視点）

ILSの設計の仕方によっては、リスクの出し手が実際に受ける損害と、ILSによって得られる金額に差が生じ、リスクの出し手が損害を十分にカバーできないベーシスリスクが生じる可能性がある。ただし今後、情報共有を高度化し、それに応じて補償条件や支払限度額、免責条項等が明確化されてくれば、ベーシスリスクに関する懸念も低下していくと考えられている。

上記のような問題があるほか、異常災害債券（キャット・ボンド）の市場[53]は財産関連リスクの移転が中心であり、これとは性質が異なるデータ漏えい等のサイバーリスクがILSの対象として活発に移転されるようになるには、まだしばらく時間がかかる可能性が高いと考えられる[54]。

６．サイバー保険に関連する規制の動向

一般的に、サイバー保険市場の成長は、サイバーセキュリティに関する規制の動向の影響を受ける。規制が強化され、企業にとってコンプライアンス・リスクが高まれば、サイバー保険に対する需要が拡大する可能性が高い。

前記2.(1)aのとおり、米国ではほとんどの州においてデータ漏えいが生じた場合、顧客等への通知が義務付けられており、企業にとってこの通知義務は非常に大きな費用となり得る。

---

[52] スイス再保険会社「Sigma No.1/2017 サイバー空間：複雑なリスクに取り組む」

[53] ILSやキャット・ボンド等の分野に強みを持つ分析・情報サービス会社であるArtemisによれば、2017年6月19日現在、キャット・ボンドの発行残高は287億ﾄﾞﾙ、2017年1月以降の発行額は91億ﾄﾞﾙとなっている。

[54] 一方、RMSのように、今後サイバー攻撃による物理的被害が、保険会社や再保険会社の財産保険のポートフォリオに大きな影響を及ぼす可能性があり、このようなサイバーリスクの移転がILSを利用する契機となる可能性があるといった見方もある。

本項では、サイバー保険の需要に影響を及ぼす可能性のある規制の動きとして、①ニューヨーク州のサイバーセキュリティ規則、②NAIC の保険データセキュリティ・モデル法策定の動き、および③テロリスク保険制度の補償対象に関するガイダンス発行の動きを取り上げ、それらの概要を説明する。

ただし、これらの規制が及ぶ範囲は、①ニューヨーク州の監督下にある保険会社や金融機関、②米国内で事業を行う保険会社、③テロによる損害（サイバーリスクに関してはサイバーテロによる損害が該当）に対する補償、というようにそれぞれ限定的であるため、サイバー保険の需要に及ぼす直接的な影響はそれほど大きなものにはならない可能性がある。

（1）ニューヨーク州のサイバーセキュリティ規則

ニューヨーク州では、金融サービス局（New York Department of Financial Services：NYDFS）のサイバーセキュリティ規則（Cybersecurity Regulations）が米国で初めて導入され、2017 年 3 月 1 日より施行されている。この規則は、NYDFS の監督下にある 3,000 以上の保険会社や金融機関を対象とする。

この規則の対象となる保険会社や金融機関は、自社の情報システムや顧客情報を保護するためのサイバーセキュリティ・プログラムを策定・維持することが義務付けられた。また、文書でのサイバーセキュリティ方針を採用し、情報システムに関する年 2 回の脆弱性評価と、リスクベースでの年次評価を実行すること、さらに、サイバーセキュリティ・プログラムの実行と監督に責任を持つ最高情報セキュリティ責任者（Chief Information Security Officer）の任命も義務付けられた。

この規則には、既存のニューヨーク州データ侵害通知法が組み込まれており、重要なサイバーセキュリティ被害については 72 時間以内の消費者への通知が求められている。さらに、この規則では、保険会社や金融機関が重要なデータ侵害を受けた場合、消費者に加え、規制当局にも通知することが求められる。

保険会社や金融機関のシステムには、膨大な顧客の個人情報が蓄積されており、サイバーリスクは非常に大きい。さらに、今回のニューヨーク州のサイバーセキュリティ規則の施行によって、保険会社や金融機関にとってコンプライアンス・リスクも大きくなっている。

フィッチ社によれば、ニューヨーク州のサイバーセキュリティ規則の施行は、サイバー保険および D&O 保険等の引受を行っている保険会社にとって、保険料の伸びと損害の拡大の両方につながる可能性がある。例えば、保険会社や金融機関の取締役または役員がこの規則に違反したことが発覚した場合、訴訟にさらされる可能性があり、これは D&O 保険を含む専門職業人賠償責任保険の補償対象となる可能性がある[55]。

[55] ハッキング攻撃が、データ保護に対する過失怠慢（errors and omissions）によって引き起こされ、第三者への賠償責任を生じさせる場合は E&O 保険の補償対象となる可能性もあるとされている。

なお、ニューヨーク州で事業を行う保険会社や金融機関の数は多く、また規制の調和化を図る観点からも、将来的には同様の規則が他の州でも導入される可能性があるとされている。

（2）NAIC の保険データセキュリティ・モデル法

NAIC[56]では、保険データセキュリティ・モデル法の策定を模索する動きが続いている[57]。

NAIC のサイバーセキュリティ作業部会（Cybersecurity Task Force）は、2016 年 4 月に保険データセキュリティ・モデル法の討議草案を公表した。業界からの多くのコメントを受けて修正し、2016 年 8 月に討議草案の第二弾を公表した。これに対しても業界から、侵害の通知に関する損害基準が定められていないことや個人情報の定義が広すぎる等の懸念が表明された。さらに修正を経て、2017 年 4 月にも改定版が公表されている。この改定版は、前記(1)のニューヨーク州金融サービス局（NYDFS）のサイバーセキュリティ規則の内容を概ね踏襲した内容となっている[58]。

2017 年 6 月末現在、NAIC の保険データセキュリティ・モデル法が成立する時期は流動的であるが、このモデル法が成立した場合は、多くの州の保険庁がこの内容を採用する可能性がある。その場合、保険会社にとってサイバーセキュリティに関するコンプライアンス・リスクが従来以上に高まることが考えられる。

（3）テロリスク保険制度

米国には公的なテロリスク保険制度（Terrorism Risk Insurance Program）[59]が存在し、民間保険会社の補償に加えて、政府支援も行われている。米国で企業保険を販売するすべての保険会社がこの制度に参加し、テロ被害に対する補償を提供することが義務付けられている。多くの保険会社は企業向けの財産保険等で補償するリスクの一部としてテロによる損害への補償を提供している。

---

[56] NAIC は、全米保険庁長官会議の略称。各州の保険庁長官によって構成される組織であり、直接的な監督権限は持たないが、各州の保険規制・監督の均質化・調和化を図るための取組を行っている。モデル法の策定もその一環として重要な役割を担っている。

[57] NAIC は、2014 年 11 月にサイバーセキュリティ作業部会（Cybersecurity Task Force）を設置し、保険会社自身のサイバーセキュリティ対策等について本格的に検討を開始した。検討の結果、2015 年 4 月に「効果的なサイバーセキュリティのための原則：保険規制ガイダンス」が、2015 年 12 月に「サイバーセキュリティ消費者保護のためのロードマップ」が採択されている。これらの概要については損保総研レポート第 116 号を参照願う。

[58] この内容については、当研究所が現在進めている 2017 年度上期調査との重複や紙面の都合もあり、説明を割愛する。

[59] 2001 年 9 月 11 日の同時多発テロを受け、2002 年 11 月にテロリスク保険法（Terrorism Risk Insurance Act：TRIA）が発効し、これによりテロリスク保険制度が創設された。米国のテロリスク保険制度の詳細については、中江俊「米国テロリスク保険の概要－テロリスクの特性と課題を中心に－」損保総研レポート第 107 号（損害保険事業総合研究所、2014.4）、杉山優紀「米国テロリズム保険制度の動向」損保ジャパン日本興亜総研レポート Vol.66（損保ジャパン日本興亜総合研究所、2015.3）等を参照願う。

テロリスク保険制度では、テロ行為[60]による民間保険会社の保険損害額が一定の規模を超えた場合に政府補償が実行される。この保険制度では、補償対象となる保険商品が予め決められている。例えばD&O保険は補償対象であるが、D&O保険以外の専門職業人賠償責任保険は補償対象外とされており、サイバー保険については、これまで補償対象となるのかどうか明確な規定がなかった。

2016年12月、米財務省はガイダンスを発行し、専用型サイバー保険は、テロリスク保険制度の補償対象に含まれることを公式に明らかにした。

2017年1月に公表されたAonのレポートによれば、専用型サイバー保険がテロリスク保険制度の補償対象となることが明確化されたことで、今後、専用型サイバー保険の普及が進むと予測されている。また多くの保険会社は、サイバーテロによる被害を含む広範な補償を提供するために、自社が引き受けるサイバー保険商品においてサイバーテロによる被害の免責条項を削除することになるとの見通しが示された。

テロリスク保険制度による政府補償は、民間保険会社によるサイバー保険の引受において支払限度額の拡大を促すとの見方や、サイバー保険分野に新規参入する保険会社が増加し、これがサイバー保険市場の拡大につながるとの見方もある。

一方､テロリスク保険制度のもとでも重要な補償のギャップは残るとの見方もある。例えば、サイバーテロの被害による電力会社の配電網の機能を回復させるための費用や多数の企業の事業中断に伴う費用は、テロリズム保険制度で補償対象とならない可能性があるとの懸念を示す向きもある[61]。

7．おわりに

今後、IoTや自動運転車、ドローン等の開発・利用が進展する中で、企業や保険会社にとって、サイバーリスクの脅威は益々大きくなり、複雑化していくと考えるのが自然であろう。サイバー保険に対する企業からの期待も大きくなると考えられる。

欧州大陸やイギリスでは､サイバー保険に加入している企業はまだ米国に比べ少ないとみられている。しかし、今後は、2018年5月のGDPRの適用に伴い、企業のデータセキュリティに対する関心が高まり､サイバー保険の普及率も向上するとの見方がある。例えば、GDPRでは、データ侵害が生じてから72時間以内に規制当局に報告することや､顧客等のデータ主体にも報告することが義務付けられる。企業にとってコンプライアンス・リスクが高まることで、サイバー保険の需要拡大につながる可能性が高いと考えられる。

ただし､保険会社が提供するサイバー保険が､将来に向けてその商品内容や保険料率の水準等から企業の期待に応えられない場合、キャプティブや保険リンク証券（ILS）

[60] 連邦議会が戦争と宣言した場合の被害は補償対象外となるなど、一定の条件を満たし、かつ財務長官および国土安全保障省長官が承認したテロ行為だけが補償の対象となる。
[61] A.M. Best, “News of the Alternative Risk Markets from A.M. Best” (2017.4)

にその需要の一部を奪われる可能性も考えられる。保険会社は、モデリング会社やサイバーセキュリティ専門会社等と連携のうえ、データの蓄積やリスクモデルの精緻化等を進め、これらを商品のカスタマイズや料率設定に活かすことを通じて、これまで以上に企業の期待に応える必要があろう。

サイバー保険市場は、米国でもまだ成長途上にあり、欧州でも今後拡大が見込まれている。変化の大きい市場であるため、本稿では取り上げなかった欧州の動きも含め、引き続き注視することとしたい。

＜参考資料＞

・PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査 2016」
・牛窪賢一「サイバーリスクとサイバー保険－米国の動向を中心として」損保総研レポート第 116 号（損害保険事業総合研究所、2016.7）
・杉山優紀「米国テロリズム保険制度の動向」損保ジャパン日本興亜総研レポート Vol.66（損保ジャパン日本興亜総合研究所、2015.3）
・スイス再保険会社「Sigma No.1/2017 サイバー空間：複雑なリスクに取り組む」
・鈴木久子「Insurance Linked Securities（ILS）がもたらす変化－資本市場による保険リスクの引受け－」損保ジャパン日本興亜総研レポート Vol.70（損保ジャパン日本興亜総合研究所、2017.3）
・中江俊「米国テロリスク保険の概要－テロリスクの特性と課題を中心に－」損保総研レポート第 107 号（損害保険事業総合研究所、2014.4）
・福留竜太郎「米国 NAIC のソルベンシー近代化構想の進展」損保総研レポート第 102 号（損害保険事業総合研究所、2013.1）
・山下潤「米国のサイバー・インシュアランスの動向」損保総研レポート第 110 号（損害保険事業総合研究所、2015.1）
・A.M. Best, “A.M. Best Special Report: U.S. Cyber Insurance Market Topped $1 Billion in 2016; More Writers Move to Standalone Policies”（2017.6）
・A.M. Best, “GDPR: Implications for European Insurers and the Cyber Insurance Market” (2017.7)
・A.M. Best, “News of the Alternative Risk Markets from A.M. Best” (2017.4)
・A.M. Best, “WannaCry Ransomware Attack- More to Come” (2017.5)
・Aon Benfield, “Cyber Update: 2016 Cyber Insurance Profits and Performance” (2017.5)
・Aon Inpoint, “Global Cyber Market Overview: Uncovering the hidden opportunities” (2017.6)
・Aon Risk Solutions, “Cyber Survey 2016”
・Business Insurance, “Captives increase options for cyber cover”（2017.3）
・Business Insurance, “Finding the right insurance coverage helps mitigate ransomware exposures”（2017.6）
・Business Insurance, “Insurers reluctant to cover cyber property exposures” (2017.6)
・Business Insurance, “Unstated cyber risks may hit multiple policies”（2017.7）
・Deloitte, “Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market” (2017)
・EY, “Global Forensic Data Analytics Survey 2016”
・FICO, “What the C-suite Needs to Know About Cyber-readiness” (2017)
・Financial Services Sector Coordinating Council, “2016 Cyber Insurance Buying Guide”（2016）
・Fitch Ratings, “Global Attacks Spur Demand for Cyber Insurance”（2017.5）
・Fitch Ratings, “U.S. Cyber Insurance Premiums Total $1B Per New Supplemental Filing”（2016.8）
・Insurance Information Institute, “The Insurance Fact Book 2016”

・Insurance Information Institute, “The Insurance Fact Book 2017”
・Insurance Journal, “New York Sees Its Cyber Rules for Insurers as Model for Other States” (2017.4.10)
・Insurance Journal, “Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance” (2017.5.31)
・ITRC, “Data Breach Reports 2016 End of Year Report”
・JLT Re, “JLT Re VIEWPOINT Unlocking the potential of the cyber market” (2017)
・Marsh & McLennan, “Captives at the Core: The Foundation of a Risk Financing Strategy” (2017.5)
・Marsh & McLennan, “Cyber Risk Report 2017”
・Marsh & McLennan, “MMC Cyber Handbook 2016”
・National Underwriter, “Eating it up”（2016.5）
・National Underwriter, “Is a Captive Right for You?”（2017.5）
・NAIC, “CIPR Newsletter”（2015.12）
・NetDiligence, “2015 Cyber Claims Study”
・NetDiligence, “2016 Cyber Claims Study”
・OECD, “Supporting an Effective Cyber Insurance Market” (2017.5)
・Ponemon Institute, “2016 Cost of Data Breach Study: United States”（2016.6）
・Ponemon Institute, “2017 Cost of Data Breach Study: United States”（2017.6）
・Ponemon Institute, “2017 Global Cyber Risk Transfer Comparison Report”（2017.4）
・PwC, “Insurance 2020 & beyond: Reaping the dividends of cyber resilience”（2015.9）
・RIMS, “Cyber Survey”（2015.5）
・RIMS, “RIMS 2016 Cyber Survey”（2016.10）
・RMS, Center for Risk Studies University of Cambridge, “2017 Cyber Risk Landscape”
・RMS, Center for Risk Studies University of Cambridge, “Managing Cyber Insurance Accumulation Risk” (2016.2)
・SANS Institute, “Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey”（2016.6）
・Symantec, “Internet Security Threat Report” (2017.4)
・The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey”（2016.4）
・The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey”（2017.5）
・The Wall Street Journal, “Cyber Insurance Becomes a Must for More Manufacturers”（2017.4）

＜参考ウェブサイト＞

・金融 ISAC　http://www.f-isac.jp/index.html
・損害保険事業総合研究所　https://www.sonposoken.or.jp/
・損害保険ジャパン日本興亜　http://www.sjnk.co.jp/
・損保ジャパン日本興亜総合研究所　http://www.sj-ri.co.jp/
・東京海上日動火災保険　http://www.tokiomarine-nichido.co.jp/

・日本損害保険協会　http://www.sonpo.or.jp/
・米国土安全保障省（DHS）　https://www.dhs.gov/
・米財務省　http://www.ustreas.gov/
・米ホワイトハウス　https://www.whitehouse.gov/
・三井住友海上火災保険　http://www.ms-ins.com/
・AIG　http://www.aig.com/home_3171_411330.html
・AIR Worldwide　http://www.air-worldwide.com/
・A.M. Best　http://www.ambest.com/
・Aon　http://www.aon.com/
・Artemis　http://www.artemis.bm/
・Business Insurance　http://www.businessinsurance.com/
・Chubb　https://www2.chubb.com/us-en/
・Deloitte　https://www2.deloitte.com/us/en.html
・EY Global　http://www.ey.com/
・FICO　http://www.fico.com/
・Financial Stability Board（FSB）　http://www.financialstabilityboard.org/
・Fitch Ratings　http://www.fitchratings.co.jp/
・FRB　http://www.federalreserve.gov/
・Insurance Information Institute　http://www.iii.org/
・Insurance Journal　http://www.insurancejournal.com/
・Insurance Services Office（ISO）　http://www.verisk.com/iso.html
・KPMG　https://home.kpmg.com/
・Marsh & McLennan　https://www.marsh.com/us/home.html
・Moody's Investor's Service　http://www.moodys.co.jp/pages/HomePage.aspx
・National Association of Insurance Commissioners（NAIC）　http://www.naic.org/
・OECD　https://www.oecd.org/
・Property Casualty Insurers Association of America（PCI）　http://www.pciaa.net/sitehome.nsf/main
・PwC　http://www.pwc.com/
・RIMS　https://www.rims.org/Pages/Default.aspx
・RMS　http://www.rms.com/
・Symantec　https://www.symantec.com/
・S&P　http://www.standardandpoors.com/en_US/web/guest/home
・Travelers　https://www.travelers.com/
・Willis and Towers Watson　https://www.towerswatson.com/en