米国を中心とするサイバー保険市場の動向

特命部長兼グループリーダー 主席研究員　牛窪　賢一

目　　次

要旨

新型コロナウイルス感染症の影響で在宅勤務が拡大したこともあって、企業へのサイバー攻撃は世界的に拡大している。このため、サイバー保険市場にも大きな変化が生じており、例えば、収入保険料・支払保険金の増加、損害率の上昇、保険料率の引上げ・引受条件の厳格化等の動きが顕著になっている。このような状況を踏まえ、本稿では、直近1年程度における米国を中心とするサイバー保険市場の動向について紹介する。

大手保険会社の中には、顧客企業によるサイバーセキュリティ対策をより厳しく評価したり、新たなツール等の提供によりリスク軽減を積極的に支援したりする動きが見られ、また保険会社同士の共同取組も開始されている。

インシュアテック企業の中には、より広範なサイバー関連リスクを補償対象とし、サイバーリスクの評価やサイバーセキュリティ関連サービスまで含む包括的なサービスの提供により事業を拡大している企業もある。また、財産保険にサイバーリスクの補償を加えた、より包括的な補償の提供に注力する保険ブローカーも見られる。

今後、在宅勤務でのパソコン等の利用に加えて、IoT等のデジタル化が進む中で、企業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られる。そのため企業は、これまで以上に包括的な補償やリスク移転・軽減の手段を求めるようになるのではないだろうか。そうだとすれば、従来型の大手保険会社にとっても、このような包括的な商品・サービスの提供が新たな収益機会となる可能性が考えられる。

どのような引受戦略を採用するにせよ、保険会社にとっては、サイバーリスクを適正に評価し、それを商品設計や保険料率に的確に反映することを通じて、保険の利便性と収益性をバランスよく維持することが必要である。そのためには、サイバーセキュリティ技術に強みを持つインシュアテック企業等との提携も含めて、データの蓄積、モデルの精緻化、技術力の活用等を積極的に推進することが重要になろう。

１．はじめに

近年、デジタル化の進展等に伴い、サイバーインシデント[1]による被害が世界的に拡大してきた。このような被害を補償するサイバー保険[2]の市場は年々成長を続けており、特に米国ではわが国よりも早くから官民挙げてサイバーリスク対策が推進されてきたこともあって、サイバー保険の利用が進んでいる。また欧州でも、欧州連合（European Union：EU）において 2018 年 5 月に、個人データの保護等を目的とした法規制である一般データ保護規則（General Data Protection Regulation：GDPR）が施行されたことなどを契機としてサイバー保険への関心が高まり、市場も拡大してきている。

当研究所では、このような重要性に鑑み、2019 年度上半期に欧米主要国におけるサイバー保険の関連動向について調査[3]し、2021 年 1 月にも損保総研レポート[4]でその後の動向について取り上げた。

さらに 1 年が経過したが、その間にも技術の進化に加えて新型コロナウイルス感染症の影響もあって[5]、サイバー攻撃は増加かつ巧妙化している。サイバー保険市場においても、加入率の上昇、収入保険料・支払保険金の増加、損害率の上昇、保険料率の引上げ・引受条件の厳格化等、大きな変化が生じている。また、サイレント・サイバーリスク[6]を巡る動きにも進展が見られる。

大手保険会社であるアクサの 2021 年の調査[7]によると、米国では、保険業界関係者にとって最も懸念されるリスクとしてサイバーセキュリティリスクが第 1 位となっている[8]。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関係者の参考となるよう、直近 1 年程度における米国を中心とするサイバー保険市場の動向について紹介する。

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 サイバーインシデントとは、サイバーセキュリティを脅かす事件や事故、およびサイバーセキュリティを堅持するにあたり好ましくない事象・事態を意味する。発生要因には、コンピュータシステムの変更時の不具合等の主に自社内の管理態勢の不備に起因するものと、サイバー攻撃のように主に外部要因に起因するものがある。

2 サイバーリスクを補償する保険商品の多くは、Cyber Insurance、Cyber Liability Insurance、Cybersecurity 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ぶ。

3 損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）

4 林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」損保総研レポート第 134 号（損害保険事業総合研究所、2021.1）

5 新型コロナウイルス感染症による損害保険業界への影響については、濵田和博「主要国におけるパンデミックに係る事業中断保険の現状」損保総研レポート第 138 号（損害保険事業総合研究所、2022.2）、損害保険事業総合研究所「欧米主要国の保険業界における新型コロナウイルス感染症への対応」（2021.3）、濵田和博「新型コロナウイルスの損害保険業界への影響」損保総研レポート第 132 号（損害保険事業総合研究所、2020.7）、牛窪賢一「米国における新型コロナウイルスと事業中断保険を巡る動向」損保総研レポート第 132 号（損害保険事業総合研究所、2020.7）等を参照願う。

6 後記 4.(1)を参照願う。

7 AXA, “AXA Future Risks Report 2021”（2021.9）

8 世界全体での結果は、第 1 位：気候変動リスク、第 2 位：サイバーセキュリティリスク、第 3 位：パンデミック・伝染病リスクとなっている。

２．サイバー保険市場の概況

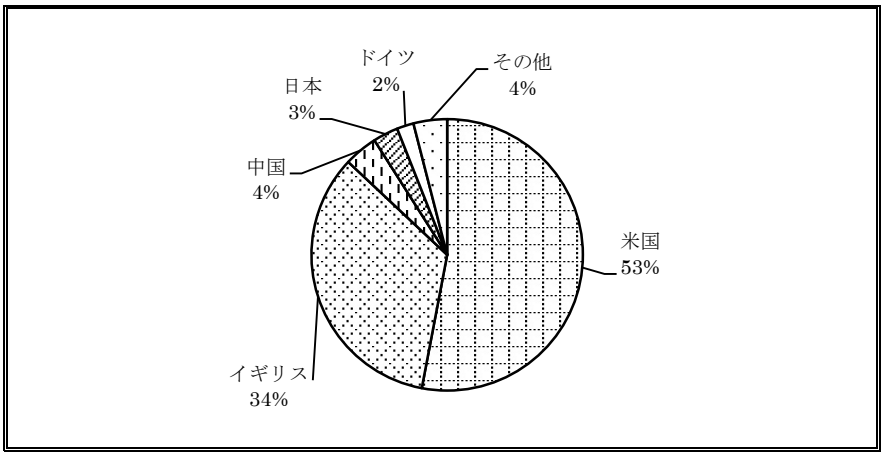
本項では、世界のサイバー保険市場規模について紹介したうえで、米国を中心とするサイバー保険市場の概況について説明する。

（1）世界のサイバー保険市場規模

サイバー保険の市場規模に関する統一的な統計データは存在せず、複数の関連組織等がそれぞれの推計結果等を公表している。例えば、イギリスの情報サービス会社であるGlobalDataによると、2020年におけるサイバー保険の市場規模は世界全体で約70億ﾄﾞﾙと推計されており[9]、2025年には200億ﾄﾞﾙになると予測されている。

これとは別の保険監督者国際機構（International Association of Insurance Supervisors：IAIS）のデータ[10]によると、世界の主要13カ国・地域におけるサイバー保険の市場規模は約60億ﾄﾞﾙと推計されており、このうち第1位の米国が約53%、次いでイギリスが約34%を占め、中国（4%）、日本（3%）等が続くとされている（図表1参照）。

図表１　世界におけるサイバー保険市場の構成割合（注）



（注）世界の主要13カ国・地域における構成割合を示している。

（出典：IAIS, “Global Insurance Market Report”（2021.11）をもとに作成）

（2）米国を中心とするサイバー保険市場の概況

本項では、サイバー保険市場の概況として、2020年前後における米国の動向を中心に、加入率の上昇、収入保険料の増加、主要保険会社の業況（保険会社ごとに異なる業況）、サイバー攻撃と保険金支払の増加、損害率の上昇、および保険料率の引上げと引受条件の厳格化について説明する。

---

[9] OECDによると、世界のサイバー保険市場の規模は、2018年時点でおよそ40億ﾄﾞﾙから50億ﾄﾞﾙと推計されていた（OECD, “Encouraging Clarity In Cyber Insurance”（2020.2））。

[10] IAIS, “Global Insurance Market Report”（2021.11）

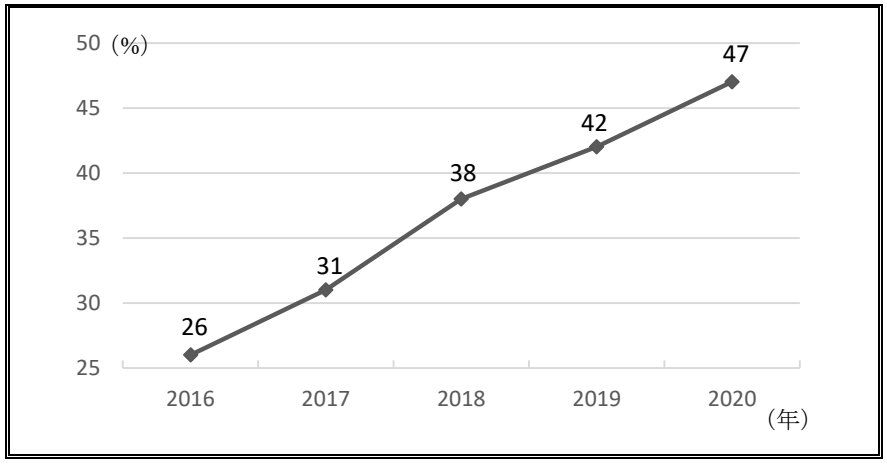
a. 加入率の上昇

米国会計検査院（United States Government Accountability Office：以下「GAO」）の報告書[11]によると、ここ数年、企業のサイバー保険への加入率は上昇している。その一例として、大手保険ブローカーであるマーシュのデータを挙げて、2020 年における同社の顧客のサイバー保険への加入率は、サイバー攻撃の増加等を背景として、前年の 42%から 5 ポイント上昇し、47%にまで高まっているとしている（図表 2 参照）。

一方、マーシュをはじめとする保険業界関係者は、大企業に比べて中小企業の加入率は低いとし、その要因として中小企業には以下のような特徴があり、サイバーリスクやサイバー保険に対する理解が十分に進んでいないことを挙げている。

○ サイバーリスクを過小評価している。
○ 現在自社が加入している企業向け保険でサイバーリスクが補償対象となっているものと誤解している。
○ サイバー保険の補償内容[12]の理解が難しい。
○ 手頃な保険料での加入が難しいと考えている。

図表 2　マーシュの企業顧客におけるサイバー保険の加入率



（出典：GAO, “Cyber Insurance; Insurers and Policyholders Face Challenges in an Evolving Market”（2021.5）をもとに作成）

b. 収入保険料の増加

米国の全米保険監督官協会（National Association of Insurance Commissioners：以

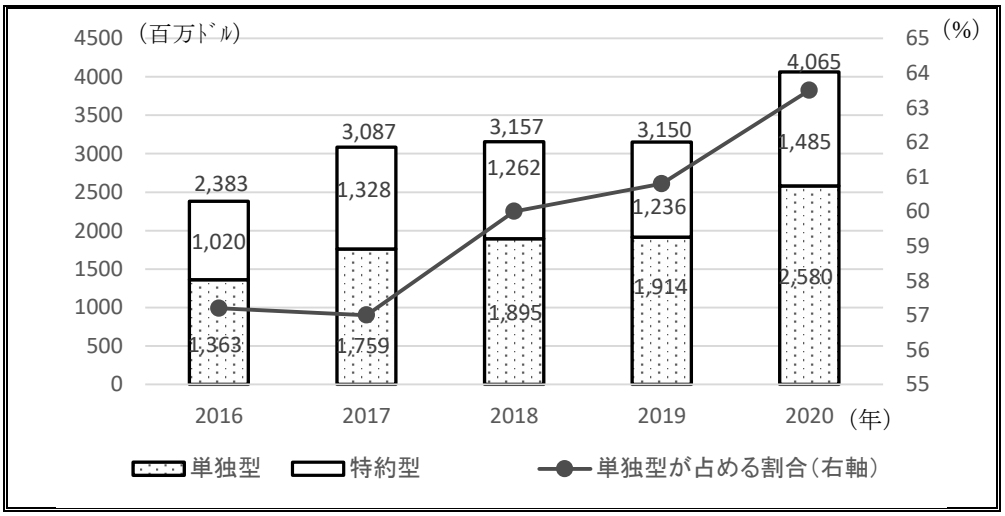
[11] GAO, “Cyber Insurance; Insurers and Policyholders Face Challenges in an Evolving Market”（2021.5）

[12] サイバー保険の補償内容は、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、保険会社や商品によって異なる。補償内容は通常、データ漏えい等に伴う第三者への損害賠償費用、および各種対応に要する自社の費用により構成される。

下「NAIC」）の報告書[13]によると、2020 年における米国のサイバー保険の元受収入保険料は、サイバー脅威の拡大に伴い、前年比 29.1%増加し、40 億 6,500 万ﾄﾞﾙとなった（図表 3 参照）。この内訳は、単独型サイバー保険[14]が前年比 34.8%増の約 25 億 8,000 万ﾄﾞﾙ、特約型サイバー保険[15]が前年比 20.1%増の約 14 億 8,500 万ﾄﾞﾙであり、サイバー保険全体に占める単独型の割合は 63.5%まで高まっている。単独型サイバー保険の伸び率が高いことは、保険会社が、サイバーリスクを他種目の保険の補償と合わせて包括的に提供するよりも、サイバーリスクに特化した保険を提供するケースが増えていることを意味しており、GAO[16]は、この背景について以下の点を挙げている。

○ 保険契約者は、単独型サイバー保険への加入により、何が補償対象となるかをより明確にし、サイバー関連の損害を確実に補償して欲しいと考えており、保険会社も保険金請求に関する紛争や訴訟を軽減することができると考えている。
○ 保険契約者は、特約型サイバー保険よりも単独型サイバー保険の方が、サイバーリスクに特化したより高額の支払限度額の補償を得られると考えている。

図表 3　米国におけるサイバー保険の元受収入保険料（注）



（注）各州の認可保険会社による引受分に加え、当該州で認可を受けていないサープラスライン保険会社による引受分も含まれている（2020 年の元受収入保険料 40 億 6,500 万ﾄﾞﾙの内訳は、それぞれ 27 億 5,400 万ﾄﾞﾙ、13 億 1,100 万ﾄﾞﾙであった）。

（出典：NAIC, “Report on the Cybersecurity Insurance Market”（2021.10）をもとに作成）

[13] NAIC は、全米各州の保険監督官によって構成されている組織であり、各州の保険規制・監督に関する支援や調和化等のための活動を行っている。毎年、サイバー保険を契約している保険会社からデータを収集しており、2021 年は 141 の保険会社グループが、2020 年におけるデータを提出した（NAIC, “Report on the Cybersecurity Insurance Market”（2021.10））。
[14] サイバーリスクを補償する専用の保険種目である。
[15] 従来型の保険種目にサイバーリスクの補償を特約として付帯するものである。
[16] GAO, “Cyber Insurance; Insurers and Policyholders Face Challenges in an Evolving Market”（2021.5）

c. 主要引受保険会社の業況（保険会社ごとに異なる業況）

2020 年に米国でサイバー保険の引受を行っている保険会社の数は、前年の 192 社から 8 社増加して 200 社となった。サイバー保険の元受収入保険料上位 20 グループの業況は図表 4 のとおりである。2020 年における上位 20 グループの市場シェアは約 84%、上位 10 グループの市場シェアは約 68%であり、前年とほぼ同水準であった。サイバー保険市場は、上位保険会社による集中度が高い状態が続いていると言える。

単独型および特約型の区分による上位 5 グループの業況は図表 5 および図表 6 のとおりである[17]。単独型サイバー保険の引受保険会社としては、アクサが第 1 位、AIG が第 2 位となっている。ただし両社には保険料の伸び率で大きな差があり、アクサは保険料を前年比 27.6%増加させたのに対し、AIG はほぼ横ばいとなっている。このような保険料の伸び率の違いは、業界全体の損害率が悪化傾向にある[18]中で、積極的な引受を続けるのか慎重になるのか、保険会社によって取組のスタンスに差が生じていることの表れと考えられる[19]。

特約型サイバー保険の引受保険会社としては、チャブ[20]が第 1 位であり、第 2 位以下とは大きな開きがある。ただし、第 2 位の CNA と第 3 位の Hartford はチャブ以上に高い伸び率となっており、引受に積極的なスタンスが窺える。

2020 年は主要な保険会社による市場からの撤退はなかったものの、保険会社によっては、引受時における支払限度額を半分にまで抑制しているケースもある[21]。サイバー関連の技術を有する新興の保険会社等が、縮小分の一部を補っているものの、サイバーリスクに対するキャパシティは、業界全体としては減少しているとされている[22]。

---

17 S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）
18 後記 e を参照願う。
19 アクサと AIG の動向については後記 3.(1)a を参照願う。
20 米国では、特定の業種や特定の企業規模に絞って引受を行う保険会社も多いが、チャブは基本的にすべての業界、すべての規模の企業を対象としてサイバー保険を提供している。後記 3.(1)a も参照願う。
21 後記 f を参照願う。
22 Judy Greenwald, “Cyber Cover Costs Expolde, Capacity Limited”（Business Insurance, 2021.11）

図表 4　サイバー保険引受状況（2020 年）　（単位：百万ﾄﾞﾙ）

	保険会社グループ	元受保険料	市場シェア（注）	損害率
1	Chubb	404	14.7%	61.0%
2	AXA	293	10.6%	98.2%
3	AIG	228	8.3%	100.6%
4	Travelers	207	7.5%	85.5%
5	Beazley	178	6.5%	47.9%
6	AXIS	134	4.8%	46.2%
7	CNA	120	4.3%	105.7%
8	Fairfax	109	3.9%	55.7%
9	Hartford	103	3.7%	25.4%
10	BCS	87	3.1%	59.1%
11	Tokio Marine	78	2.8%	51.1%
12	SOMPO	73	2.6%	114.1%
13	Zurich Insurance	64	2.3%	40.4%
14	Liberty Mutual	42	1.5%	30.0%
15	Apollo Global MGMT	39	1.4%	29.6%
16	Berkshire Hathaway	37	1.4%	25.8%
17	Markel Corp	30	1.1%	38.0%
18	Everest Re	28	1.0%	48.0%
19	Cincinatti FNCL	25	0.9%	24.6%
20	Swiss Re	24	0.9%	42.6%

（注）認可保険会社による引受分だけの（サープラスライン保険会社分を含まない）元受収入保険料合計に対する市場シェアである。

（出典：NAIC, “Report on the Cybersecurity Insurance Market”（2021.10）をもとに作成）

図表 5　単独型サイバー保険引受状況（上位 5 グループ）　（単位：百万ﾄﾞﾙ）

	保険会社グループ	元受保険料			損害率（注）
		2019 年	2020 年	伸び率	2020 年
1	AXA	230	293	27.6%	98.2%
2	AIG	226	227	0.1%	101.3%
3	Beazley	141	169	19.3%	41.9%
4	Travelers	144	168	16.6%	81.9%
5	Fairfax	65	108	66.8%	55.8%

（注）単独型サイバー保険だけの損害率である。特約型サイバー保険も含む損害率は前掲図表 4 を参照願う。

（出典：S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）をもとに作成）

図表 6　特約型サイバー保険引受状況（上位 5 グループ）　（単位：百万ﾄﾞﾙ）

	保険会社グループ	元受保険料			損害率（注）
		2019 年	2020 年	伸び率	2020 年
1	Chubb	355	404	13.7%	61.0%
2	CNA	79	101	28.9%	105.7%
3	Hartford	50	92	84.6%	25.4%
4	AXIS	48	44	▲8.4%	46.2%
5	Travelers	35	39	12.5%	85.5%

（注）特約型および単独型の両方を合わせた損害率である（前掲図表 4 の損害率と同じ数

値)。なお、特約型サイバー保険だけの損害率は入手できなかった。

（出典 : S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）をもとに作成）

d. サイバー攻撃と保険金支払の増加

サイバー攻撃は世界的に増加し、手口も巧妙化している。この背景には、新型コロナウイルス感染症に関連して在宅勤務が増加したことによる影響もある。特にランサムウェア[23]攻撃による被害が拡大しており、サイバー保険の保険金支払の増加につながっている。大手保険ブローカーであるエーオン[24]によると、米国での 2020 年におけるサイバー保険 1 件あたりの保険金支払額は、前年の 4 万 8,710ﾄﾞﾙから 50%以上増加し、7 万 4,350ﾄﾞﾙとなっている[25]。以下、直近の保険金支払の特徴・変化について説明する。

（a）ランサムウェア攻撃の概要

NAIC では、ランサムウェアによる攻撃の概要、およびその対策等について、図表 7 のとおりウェブサイト上で公開している。一般的に、ランサムウェアによる被害は身代金の支払、および関連費用だけに留まらず、データ漏えいや事業中断損害[26]等も被害者にとって大きな負担となる。

また、ドイツのアリアンツ傘下の Allianz Global Corporate & Specialty（以下「AGCS」）の報告書[27]では、近年のランサムウェアの特徴として図表 8 の点を挙げている。

---

[23] 「ransom（身代金)」と「software（ソフトウェア)」を組み合わせた造語であり、コンピュータ等に感染し、ファイル暗号化等によりデータを使用不能にした後、解除を条件に身代金を要求するウイルスを指す。

[24] Aon, “US Cyber Market Update: 2020 US Cyber Insurance Profits and Performance”（2021.6）

[25] 一方、保険契約件数に占める保険金支払件数の割合は、前年とほぼ変わっていないとされている。

[26] サイバーセキュリティの専門会社である Coveware によると、2020 年第 4 四半期には、平均 21 日間の事業中断期間が報告されている。この事業中断の損害としては、期間中の喪失利益や給与等の継続的な営業費用等があり、これらはサイバー保険で補償対象とすることができる（Dan Burke, “Cyber Security Controls: Now Critical for Your Cyber Insurance Renewal”（Woodruff Sawyer, 2021.2)）。

[27] Allianz Global Corporate & Specialty, “Ransomware trends: Risks and Resilience”（2021.10）

図表 7　NAIC によるランサムウェア対応に関する説明（抜粋）

○ランサムウェアの多くは、正規の機関等を装ったフィッシングメールによって配信され、企業のシステム等に侵入する。パソコン、タブレット、スマートフォン等あらゆる機器が感染の入口となる可能性がある。 ○ランサムウェア攻撃では通常、ハッカーの要求が満たされるまで、被害者のデータやシステムは暗号化されて凍結される。ハッカーは被害者に、データやシステムへのアクセスを回復するために身代金を支払うよう要求する。身代金は通常、ハッカーが匿名で利用できるビットコイン等の暗号資産での支払が求められる。 ○被害者となった企業は、身代金等の金銭だけでなく、ランサムウェアの被害が公表されることで、レピュテーションや顧客の信頼も損なう可能性がある。 ○個人、企業、病院、および政府機関等、誰もがランサムウェアのターゲットになる可能性がある。2021 年の時点で、ランサムウェア攻撃の被害者の 50%から 75%は中小企業だと言われている。中小企業は、一般的にセキュリティへの投資が少なく、システムへの侵入が容易であるため、狙われやすい。 ○各州の保険監督当局は、企業や個人がランサムウェア攻撃の被害を受ける可能性を懸念しており、サイバー保険への加入等の対策を講じるよう呼びかけている。多くのサイバー保険では、身代金、恐喝対応関連費用、および復元費用等が補償される。ただし、身代金を支払う前に保険会社に通知することが重要であり、そうしないと補償されない場合がある。 ○FBI は、身代金を支払うことにはリスクが伴うと警告している。身代金を支払っても、データが復元される保証はなく、またハッカーは被害者の情報を共有しているため、身代金を支払った被害者は再び狙われることが多いとしている。

（出典：NAIC ウェブサイトをもとに作成）

図表 8　近年におけるランサムウェアの特徴

	特徴等
「サービスとしてのランサムウェア ransomware as a service)」化	○ハッカー集団は、ランサムウェアなどのハッキングツールを事業の対象として、第三者に販売・レンタルし、様々な支援サービスも提供しているため、犯罪者による攻撃が拡大する要因となっている。
二重恐喝の増加	○犯罪者は、被害者のデータファイルやシステムを暗号化することによる恐喝に加えて、それらに含まれる機密データや個人データを公開するなどと脅迫する事例が増加している。
ハード・ソフト双方のサプライチェーンへの攻撃	○重要インフラなどの物理的サプライチェーンに加え、ソフトウェア・IT サービス事業者がターゲットとなっており、犯罪者はそれらを利用してマルウェア (注) のさらなる拡散を図ろうとしている。

（注）「malicious（悪意のある）」と「software（ソフトウェア）」を組み合わせた造語であり、コンピュータウイルスやスパイウェアなど、ユーザーのデバイスに不利益をもたらす悪意のあるプログラムやソフトウェアを指す。

（出典：Allianz Global Corporate & Specialty, “Ransomware trends: Risks and Resilience”（2021.10）ほかをもとに作成）

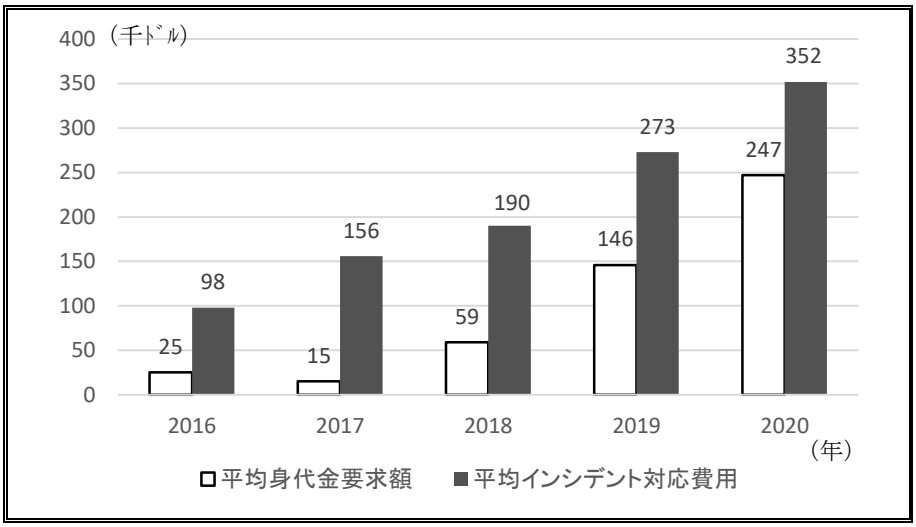
（b）2020 年までの傾向

FBI によると、2020 年には 2,474 件のランサムウェア被害の報告があり、損失額は 2,900 万ﾄﾞﾙ以上に上ったとされ、これは、2018 年に比べ 8 倍の増加となっている。また、サイバーリスクを専門とする情報サービス会社である NetDiligence[28]によ

[28] 米国の主要保険会社等がデータを提供し、NetDiligence が集計している（NetDiligence, “Cyber Claims Study 2021 Report”（2021））。

ると、中小企業を対象とするランサムウェアによる平均身代金要求額と平均インシデント対応費用は年々増加傾向にあり、2020 年も拡大している（図表 9 参照）。

図表 9　ランサムウェアの身代金要求額とインシデント対応費用



（出典：NetDiligence, “Cyber Claims Study 2021 Report”（2021）をもとに作成）

（c）2021 年に入ってからの変化

コンサルティング会社の Accenture[29]によると、2021 年上半期の世界におけるサイバー攻撃件数は、前年同期比で 125%増加しているとされ、サイバー攻撃は 2021 年に入ってからも加速していることが窺える。

しかし、Corvus[30]の報告書[31]によると、ランサムウェアへの対応費用は減少してきたとされている。世界的に犯罪が急増し、身代金の要求も高額化する中で、システムのバックアップや e メールのセキュリティに対する企業側の意識が高まってきたことが、ランサムウェアへの対応費用の減少につながっているとしている。

ランサムウェアによる平均支払額は増加傾向にある[32]ものの、支払を行った企業等の数は減少傾向にあり、ランサムウェアの身代金要求に対し実際に支払を行った企業等の割合は、2020 年第 3 四半期には 44%であったが、2021 年第 3 四半期には 12%まで低下している（図表 10 参照）。なお、企業等のセキュリティが高まった要因として、以下の 2 つの傾向が挙げられている[33]。

---

[29] Accenture, “Triple digit increase in cyberattacks: What next?”（2021.8）

[30] 2017 年に設立されたマサチューセッツ州ボストンに本社を置く企業向け保険を提供するインシュアテック企業である。

[31] Corvus, “Corvus Risk Insights Index Q4 2021”（2021.11）。この報告書では、同社の保険金請求データ、および第三者から取得したデータ等を利用して分析しているとされており、分析の対象は米国のサイバー保険市場が中心になっているものと推測される。

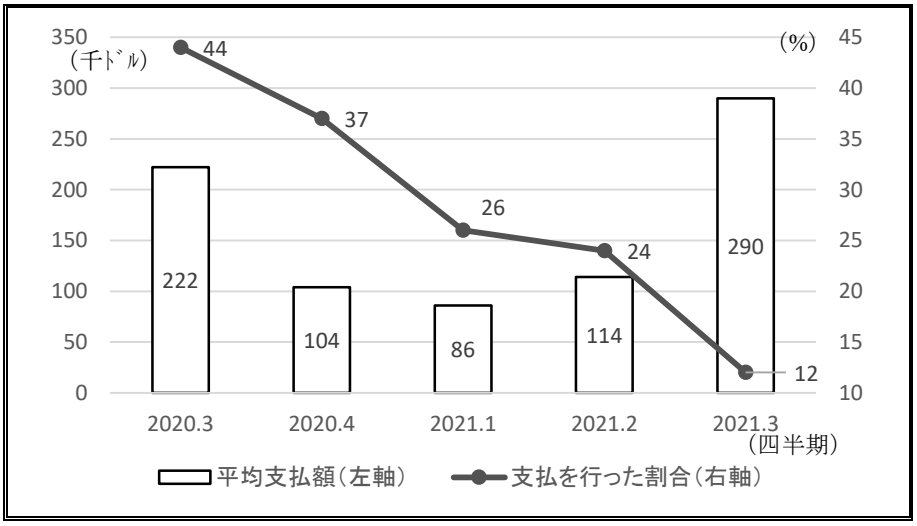
[32] 2021 年第 3 四半期に大幅に増加した背景には、身代金要求が高額化していることがあるとされている。

[33] Scott Ikeda, “Cyber Insurance Claims Spike With Major Attacks, but Ransomware Costs Down

○ 脆弱なリモートデスクトッププロトコル（Remote Desktop Protocol：以下「RDP」）[34]システムが、徐々に安全性が高いシステムに置き換えられている。パンデミックが始まる前には、企業等の 10%が RDP システムを使用していたが、リモートワークが定着した現在では 4%以下にまで低下している。

○ パンデミックが始まって以来、e メールセキュリティツールの使用が 158%増加した。質の高い e メールツールを使用することで、サイバー攻撃に対する被害を抑制する効果が表れてきている。

図表 10　ランサムウェアによる平均支払額と支払を行った割合



（出典：Corvus, “Corvus Risk Insights Index Q4 2021”（2021.11）をもとに作成）

e. 損害率の上昇

サイバー保険での保険金支払額の増加に伴い、サイバー保険の損害率も大きく上昇している。2020 年の米国におけるサイバー保険の平均損害率は前年の 44.9%から 22.1 ポイント上昇し、67.0%となった。特に単独型サイバー保険の損害率が前年の 47.1%から 25.7 ポイント上昇し、72.8%となっている（図表 11 参照）[35]。

前掲図表 4 のとおり、上位 20 グループの損害率は、24.6%から 114.1%まで、保険会社によって大きな差が生じている[36]。元受収入保険料の上位社の中では、単独型サイバー保険で第 1 位のアクサと第 2 位の AIG の損害率がともに 100%前後となっている。

Sharply From 2020”（CPO Magazine, 2021.11）

[34] RDP は、デスクトップコンピュータをリモートで使用するための技術的な規格であり、Microsoft によってリリースされた。

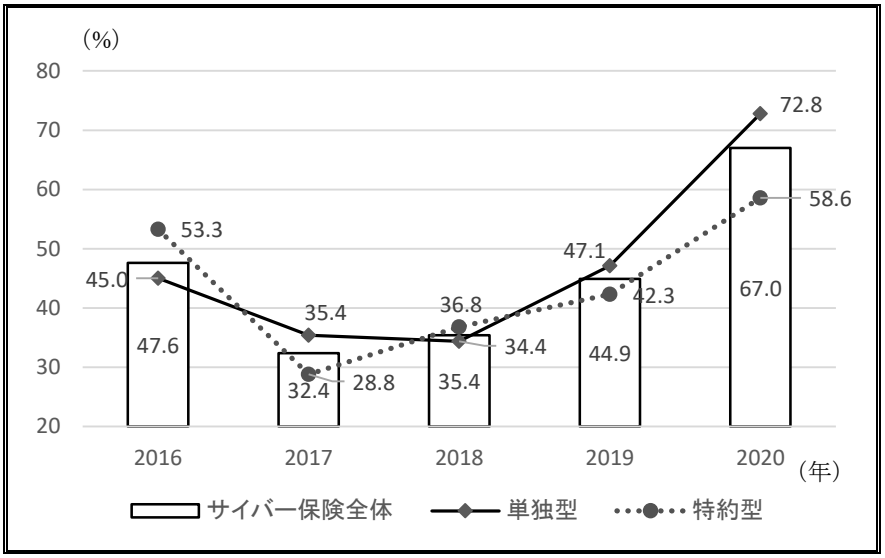
[35] エーオンは、この損害率に基づき、2020 年のコンバインドレシオを 95.4%（内訳は単独型 100.1%、特約型 88.9%）と推計している。

[36] ただし NAIC は、サイバー保険市場はまだ未成熟で発展途上にあるため、保険会社によって損害率の差が大きいことは予想外のことではないとしている。

特約型サイバー保険では、第 1 位のチャブの損害率は 61.0%であるものの、第 2 位の CNA は 105.7%となっており、市場シェア上位の保険会社の多くが、収益性の面で課題を抱えていると考えられる。

なお、チューリッヒ保険における 2020 年の損害率は 40.4%であり、業界の平均を大幅に下回っている。格付機関である S&P の報告書[37]では、この好業績の一因として、同社がサイバーセキュリティ技術の専門会社と提携したことによる効果が挙げられている[38]。

図表 11　米国のサイバー保険市場における平均損害率の推移



（出典：Aon, “US Cyber Market Update: 2020 US Cyber Insurance Profits and Performance”（2021.6）をもとに作成）

f. 保険料率の引上げと引受条件の厳格化

サイバー保険の損害率の上昇ペースが速いため、多くの保険会社が、保険料率の引上げや引受条件の厳格化等の対応を行っている。Marsh McLennan Agency[39]によると、サイバー保険の更改時における保険料の上昇率は、2020 年から 2021 年にかけて加速し、2021 年第 3 四半期は 27.6%となっている（図表 12 参照）。また、他の企業向け保険種目と比較しても、サイバー保険の料率上昇が際立って高いことがわかる（図表 13 参照）。

[37] S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）
[38] チューリッヒ保険は、イスラエルを拠点とするサイバーセキュリティ専門会社である CYE と提携し、世界中の顧客に対し CYE の AI に基づくサイバーリスク評価等の技術を利用した包括的なサービスを提供することを 2020 年 2 月に公表している（Insurance Journal, “Zurich Insurance Partners with Cyber-Security Specialist CYE”（2020.2））。
[39] Marsh McLennan の子会社である。Marsh McLennan については後記 3.(3)b(b)を参照願う。

NAIC[40]によると、2021 年におけるサイバー保険の保険料率は、全体的に 15%から 50%の上昇になると見込まれており、保険料率が上昇する中でもサイバー保険に対する需要は高まっているため、このような傾向は 2022 年も続く可能性が高いとされている。

多くの保険会社は、サイバー補償に関する免責条項の追加、免責金額の引上げ、サブリミットの設定等によって、引受条件を厳格化している。また、サイバー保険の支払限度額は、リスクが高い一部の業種を対象として従来の 1,000 万ﾄﾞﾙから 500 万ﾄﾞﾙに引き下げられている。

GAO[41]によると保険会社は、医療や教育などのリスクが高い業種や公共団体等の支払限度額を引き下げたり、ランサムウェアによる損害のサブリミットを追加設定したりしている。なおこのような引受条件の厳格化には、保険会社がサイレント・サイバーリスク対応として補償対象・範囲を明確にしようとする側面があることも GAO は指摘している。

上記のほか保険業界関係者は、サイバー保険の引受に関する最近の特徴的な動きとして以下の点を挙げている。

○ 保険会社は保険契約締結の前に、より多くの情報を企業に求め、企業が多要素認証（Multifactor Authentication : MFA）[42]やインシデント対応計画等、最新のサイバーセキュリティ対策を実施しているか確認している[43]。

○ 大手保険会社は、サイバー保険の引受可否や適正な保険料算定のために、顧客のコンピュータネットワークにおけるサイバーセキュリティリスクを評価するためのツールを引受プロセスに組み込むようになってきている[44]。

○ サイバー保険の引受に関して、企業が求められるセキュリティ管理やガバナンスの要件は、以前に比べはるかに厳しくなっている。企業が保険に加入するためには、強固なサイバーセキュリティシステムが必要になってきた[45]。

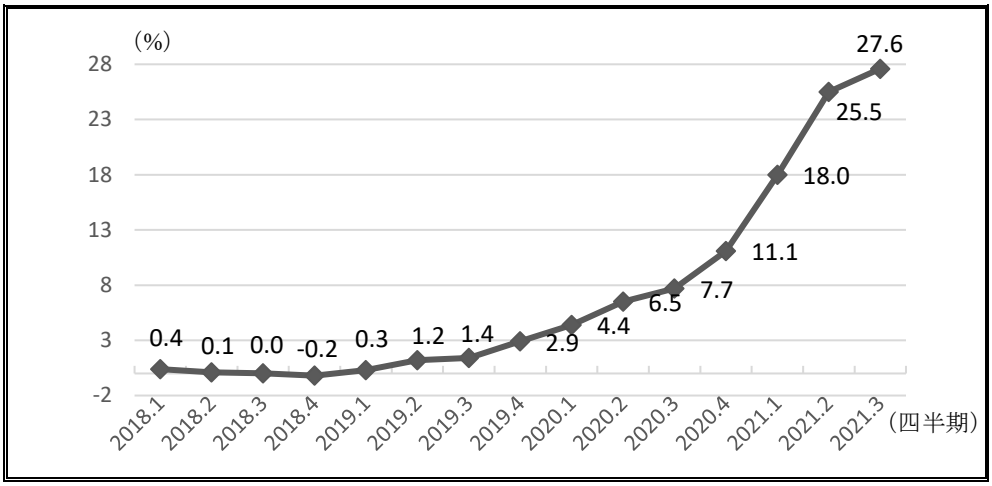
○ 公共団体や非営利団体がハッカーに狙われやすいのは、古いシステムで運用されているコンピュータネットワーク、最小限のサイバーセキュリティ、IT 部門の人員不足などが原因であることが多い。サイバー保険の加入や更新を検討している公共団体は、厳しい条件に直面しており、保険料は前年の 2 倍になるケースもある[46]。

---

40 NAIC, “Report on the Cybersecurity Insurance Market”（2021.10）
41 GAO, “Cyber Insurance; Insurers and Policyholders Face Challenges in an Evolving Market”（2021.5）
42 認証の 3 要素である知識情報、所持情報、および生体情報のうちの 2 つ以上を組み合わせて認証することを意味する。
43 Judy Greenwald, “Cyber Cover Costs Expolde, Capacity Limited”（Business Insurance, 2021.11）
44 NAIC, “Report on the Cybersecurity Insurance Market”（2021.10）
45 S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）
46 S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）

なお S&P の報告書[47]によると、補償内容やリスクアペタイト[48]等に関する引受スタンスは、保険会社によってかなり異なっている。例えばチューリッヒ保険は、前掲図表 4 のとおり損害率が 40.4%と低いこともあり、引受スタンスを比較的安定させており、補償範囲やリスクアペタイト等の大幅な変更は想定していないとしている。

図表 12　サイバー保険の更改時における保険料率の上昇率



（出典：Marsh McLennan Agency, “Cyber Risk Perceptions Survey Findings 2020-2021”（2021.11）をもとに作成）

図表 13　主要企業向け保険種目の保険料率の上昇率[(注)]　（単位：%）

	保険種目	2021 年第 2 四半期	2021 年第 3 四半期
1	サイバー保険	25.5	27.6
2	会社役員賠償責任保険（D&O 保険）	13.4	13.6
3	雇用慣行賠償責任保険	8.9	10.3
4	洪水保険	4.5	6.8
5	建設保険	6.4	6.3
6	事業中断保険	6.7	5.9
7	海上保険	4.0	5.3
8	医療過誤保険	5.4	5.0

（注）保険契約の更改時における平均上昇率である。

（出典：Marsh McLennan Agency, “Cyber Risk Perceptions Survey Findings 2020-2021”（2021.11）をもとに作成）

３．大手保険会社・インシュアテック企業等の動向

前記 2.(2)c のとおり、サイバー保険の引受においては従来型の大手保険会社が中心となっている。ただし、サイバーセキュリティに関する専門的な技術力を有する新興のイ

[47] S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）
[48] 保険会社等が進んで受け入れるリスクの種類や大きさ等を意味する。

ンシュアテック企業等もサイバー保険市場において一定の役割を担っている。例えば、保険商品に加えてリスク評価を含むセキュリティ関連サービスを包括的に提供するインシュアテック企業が事業を拡大する動きが見られる。また、サイバーリスクを評価するプラットフォームを提供するサイバーセキュリティ専門会社がサイバーセキュリティリスクの格付（以下「サイバーリスク格付」）を市場に定着させようとする動きもある。本項では、これらの概要を説明する。

（1）大手保険会社の動向

本項では、主な大手保険会社の事例について説明したうえで、共同取組としてのCyberAcuView の創設、および官民連携に向けた動きについて紹介する。

a. 主な大手保険会社の事例

本項では、チャブ、AIG、およびアクサの事例を取り上げて説明する。

（a）チャブ

チャブは 1998 年から引受を行っているサイバー保険分野の先駆者であり、20 年以上にわたってサイバー保険および関連サービス提供の経験を蓄積してきた。同社が提供しているサイバー保険の代表的な商品であるサイバーエンタープライズリスクマネジメント（Cyber ERM）は、企業のエクスポージャーとニーズに合わせてカスタマイズ可能なソリューションであり、図表 14 のような特徴を持っているとされている。

さらにチャブは 2021 年 11 月、サイバー攻撃が進化する中で企業顧客のリスク軽減を一層支援するために、新たなサイバーリスクサービスを提供することについて公表した[49]。このサービスの概要は図表 15 のとおりである。

図表 14　チャブが提供するサイバー保険（Cyber ERM）の特徴等（抜粋）

○規模、業種、リスクの種類を問わず、全世界で適用可能な補償 ○顧客独自のニーズに対応する革新的で高度にカスタマイズ可能なソリューション ○最低保険料の設定はなく、保険料は、補償範囲と支払限度額に基づき、あらゆる規模のリスクに対して段階的に設定可能 ○小規模なリスクの引受については、オンライン見積りとリアルタイムの保険証券発行が可能 ○進化する規制やセキュリティ基準に対応し、将来の変化も考慮した革新的な補償内容 ○典型的なサイバーインシデントの流れに沿った説明により、企業の意思決定を支援

（出典：Chubb ウェブサイトをもとに作成）

[49] MarketScreener, “Chubb：Enhances Cyber Risk Service Offerings to Further Support Clients in Helping to Reduce Potential Losses”（2021.11）

図表 15　チャブが新たに提供するサービスの概要

サービス名	特徴等
サイバー脆弱性警告システム	○顧客が使用しているソフトウェアに関連する脆弱性を e メールで警告する。
多要素認証（MFA）(注1)評価・導入サービス	○顧客が多要素認証（MFA）プログラムを選択・設計・レビューできるようにし、また導入時における潜在的なリスクを特定し対処できるようにする。
パッチ管理サービス	○ソフトウェアの既知の脆弱性に対処するアップデートのためのソリューションの選択・実装を支援する。
境界型 e メールセキュリティサービス	○悪意のあるメールを受信トレイから排除するためのメールフィルタリングおよびサンドボックス(注2)の選択・設計・実装を支援する。
サイバーサービスオリエンテーション	○契約者は、チャブのアドバイザーチームとのバーチャルセッションに参加し、サイバーリスクや関連サービスにつき質問・確認できる。

（注１）前記 2.(2)f を参照願う。

（注２）ユーザーが通常利用する領域から隔離・保護された領域を意味し、不正なプログラム等による被害を防ぐために使用する。

（出典：MarketScreener, “Chubb：Enhances Cyber Risk Service Offerings to Further Support Clients in Helping to Reduce Potential Losses”（2021.11）をもとに作成）

（b）AIG

AIG は、前掲図表 4 のとおり 2020 年の損害率が 100.6%と高かったことから、引受条件の厳格化に取り組んでいる。例えば保険契約者によっては、サイバー保険の支払限度額の 50%をランサムウェアによるサブリミットとして設定することとし、またランサムウェアによる損害の 50%を保険契約者に負担してもらう方式[50]での引受も実施するとされている[51]。

AIG はエクスポージャーを抑制するため、引受前の手続として 2021 年から顧客のセキュリティ対策に関する 25 項目の質問[52]を追加して企業のセキュリティ対策をより厳しく評価するようになり、同社が求めるレベルに顧客の管理態勢が達していない場合には、ランサムウェアによるサブリミットの設定に留まらず、保険の引受自体を拒絶することもあるとされている[53]。

（c）アクサ

アクサはグループ傘下のアクサ XL を中心として欧米、アジア等でのグローバル保険プログラムの提供に注力しており、このプログラムのメリットとして、漏れや重複のない広範で一貫性のある補償によって、異なる国・地域に存在する自社の資産を境

[50] 英語では“co-insurance”と呼ばれている。
[51] Dan Burke, “Cyber Security Controls: Now Critical for Your Cyber Insurance Renewal”（Woodruff Sawyer, 2021.2）
[52] その企業の業種、売上高、従業員数、営業地域、および保有データの状況等の基本的情報に加えて、使用しているウイルス対策ソフトウェア、パスワード、および多要素認証（MFA）等の状況、ならびに自社のシステム等に攻撃を受けた場合の影響の大きさ（5 段階評価）等が挙げられている。
[53] Ian Smith, “Cyber insurers recoil as ransomware attacks ‘skyrocket’”（Financial Times, 2021.6）

界線なく保護することができること、アクサグループが提供する世界各地の専門的なリソースを活用できること等を挙げている[54]。

なお、アクサグループ傘下のアクサ・フランスは2021年5月、フランス国内でランサムウェアによる身代金支払をサイバー保険の補償対象外とすることを公表した[55]。この補償に関する引受停止措置は、2021年4月にパリで開かれた上院の会議において、フランスの司法当局とサイバーセキュリティ当局の関係者等が、身代金の支払を補償対象とする保険について批判したことを受けて公表されたものであり[56]、既存の保険契約には影響しないとされている[57]。

b. 大手保険会社による共同取組としてのCyberAcuViewの創設

米国の保険業界においてサイバー保険の収支が悪化する中、サイバー保険の引受を行う大手保険会社のチャブ、AIG、トラベラーズ、Beazley、AXIS、Hartford、およびLiberty Mutualの7社は、保険業界でサイバーリスクの軽減に取り組むコンソーシアムであるCyberAcuViewを設立したことを2021年6月に公表した[58]。

CyberAcuViewは、設立メンバー7社が100%出資しており、ニューヨークを拠点としてサイバー関連データを収集・分析し、メンバーとなっている保険会社やその保険契約者を支援する。具体的には、以下のような方法でサイバーリスクの軽減に取り組むとしている。

- ○ サイバーリスクへのレジリエンスを高めるため、業界のベストプラクティスを提供する。
- ○ サイバー犯罪に対処するため、規制当局、法執行機関、その他のセキュリティ関連機関と積極的に連携する。
- ○ システミックリスクに対処するソリューションを開発し、またサイバー保険市場

---

[54] Anoop Khanna, “Cyber protection and global insurance programmes”（Asia Insurance Review, 2021.11）

[55] Frank Bajak, “Insurer AXA to Stop Paying for Ransomware Crime Payments in France”（Insurance Journal, 2021.5）

[56] Scott Ikeda, “Ransomware Attack Reported at Insurance Giant AXA One Week After It Changes Cyber Insurance Policies in France”（CPO Magazine, 2021.5）。なお欧米主要国では、ランサムウェアによる身代金支払を保険で補償することに対し、犯罪を助長するとの考え方から批判的な見方がある。イギリスのアビンドンに拠点を置くサイバーセキュリティの専門会社であるSophosの調査によると、サイバー保険に加入している組織は、加入していない組織に比べて身代金を支払う可能性が2倍以上になっているとされている。また多くの場合、ランサムウェアの犯罪者は、ターゲットに関する情報を事前に収集し、被害者が身代金支払を補償する保険に加入していることを把握しているとされる。

[57] アクサの動き等を契機として、保険会社の間で身代金支払に対する補償を停止する動きが世界的に広がれば、ランサムウェア攻撃が減少するとの見方もある（Life Insurance International, “Axa’s announcement to stop coverage of ransomware payments prompts broader cyber insurance debate”（2021.6））。

[58] Insurance Journal, “7 Major Cyber Insurers Form Company to Coordinate Cyber Analysis, Risk Mitigation”（2021.6）

の効率性を向上させるためサイバー保険の約款文言を見直す。

○ サイバー攻撃の傾向や損害の原因を分析して可視性を高め、保険会社によるリスク管理、および損害防止策に関する保険契約者への啓発等を支援する。

CyberAcuView の CEO には、AIG の元サイバー部門責任者が就任しており、保険業界全体のリソースを組み合わせることで、サイバー関連動向の理解を深め、将来の攻撃を予測・軽減し、社会全体のサイバーレジリエンスを高めることができるとしている。また CyberAcuView には、元保険庁長官や FBI 出身者等も取締役として加わる予定とされている。

なお、米国の格付機関である AM Best の報告書では、ランサムウェア等のサイバーリスク環境が著しく悪化しているため、米国のサイバー保険市場の見通しは厳しく、保険業界はサイバーリスクに対する方針等を全面的に見直す必要があり[59]、今回の共同取組の公表はそのような評価を踏まえたものとされている。

c. 官民連携に向けた動き

サイバー保険の収支が悪化する中で、官民の連携が有効との見方もある[60]。例えばチャブは、ランサムウェア攻撃の増大により、多くの保険会社が大幅な保険料率引上げや補償範囲の縮小等を実施・検討していることを受け、このような問題に対処するため、図表 16 のとおり官民の連携が効果を発揮する可能性があるとしている。

また 2021 年 5 月、サイバーセキュリティに関するサミットがホワイトハウスで開催され、保険業界からはトラベラーズと Coalition[61]等が、大手テクノロジー企業やバイデン政権関係者等とともに参加した[62]。ジョー・バイデン大統領は、連邦政府だけではこの課題に対応できないとして、サイバーセキュリティの水準を高めることへの協力を民間企業に求めた。図表 16 には、保険業界の役割やサイバーセキュリティに対する自社の取組について、会議後にトラベラーズが言及した主な内容も記載している。

---

[59] AM Best によると、保険会社は、サイバーリスクに関するアペタイト、リスク管理、モデル構築、ストレステスト、および保険料率設定等のあらゆる面で早急に見直す必要があるとしている（AM Best, “Market Segment Report: Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk”（2021.6））。

[60] Ian Smith, “Cyber insurers recoil as ransomware attacks ‘skyrocket’”（Financial Times, 2021.6）

[61] Coalition の概要および取組等については、後記(2)a を参照願う。

[62] Insurance Journal, “What Insurance Firms Promised at White House Cybersecurity Summit”（2021.8）

図表 16　官民連携に関するチャブとトラベラーズの考え方

	概要
チャブ	○今日の世界では、個人も企業もデジタルで相互に接続している。サイバーリスクは、パンデミックリスク同様、潜在的な被害規模が大きいこと、時間的・地理的な境界がないこと等の特徴を有しており、民間の保険会社だけでは対応が難しい面がある。 ○国家によるサイバー攻撃や、国家以外の犯罪者集団等による社会的混乱や金儲けを目的としたサイバー攻撃への対応・管理方法は複雑であり、政府との連携が役立つ。 ○民間部門と公的部門が協力できることは多く、例えば情報共有もその１つである。
トラベラーズ	○保険会社は、サイバーリスクの評価、サイバー攻撃対策の強化に関するアドバイス、サイバー脆弱性のモニタリング等を通じて、組織が効率的かつ効果的にサイバーリスクを管理できるよう支援している。 ○企業等にデータ漏えいが発生した場合、保険会社は技術的な専門知識と金銭的な支援を提供し、復旧を促す。また保険業界が協力することで、サイバーリスクの傾向を把握・共有し、セキュリティのベストプラクティスの採用を促進することができる。 ○例えば、企業が多要素認証（MFA）のような安価なリスク軽減策を導入すれば、ランサムウェア攻撃の大部分を防ぐことができるという調査結果があり、そのようなベストプラクティスを採用することで、企業および国をより安全にすることができる。 ○サイバー被害から企業や個人を守るために、政府、サイバーセキュリティ専門会社、および他の保険会社等と協力して対応したい。

（出典：Mark Hollmer, “Chubb CEO Greenberg Stresses Need to Address Ransomware and ‘Systemic’ Cyber Risk”（Insurance Journal, 2021.7）、Insurance Journal, “What Insurance Firms Promised at White House Cybersecurity Summit”（2021.8）をもとに作成）

（2）インシュアテック企業による包括的サービス提供の事例

本項では、サイバー保険に関する包括的なサービスを提供する代表的なインシュアテック企業である Coalition および Zeguro の事例を取り上げて説明する。

a. Coalition による事業の展開

Coalition は 2017 年に米国のサイバー保険市場へ参入したインシュアテック企業であり、カリフォルニア州サンフランシスコに本社を置き、保険代理店として企業向けにサイバーセキュリティツールやサイバー保険を提供している。実際の保険引受は、保険会社である Swiss Re Corporate Solutions および Argo Group が行っている。Coalition はサイバー保険の販売に際し保険契約者のシステムを調査する等の独自の技術で保険契約者のリスク評価を行っている。調査によってセキュリティの不備が見つかった場合はコンサルティングを行い、リスクの軽減を図る。また、リスクが一定の基準を超える場合は引受対象としないとしている。

Coalition のリスク管理プラットフォームは、企業も Coalition のウェブサイトにメールアドレスを入力して登録するだけですぐに利用することができる。このツールは、その企業におけるサイバーリスクを評価して診断結果を提示し、問題を修正する方法も示すため、企業はすぐにリスク管理を開始することができるとされている[63]。

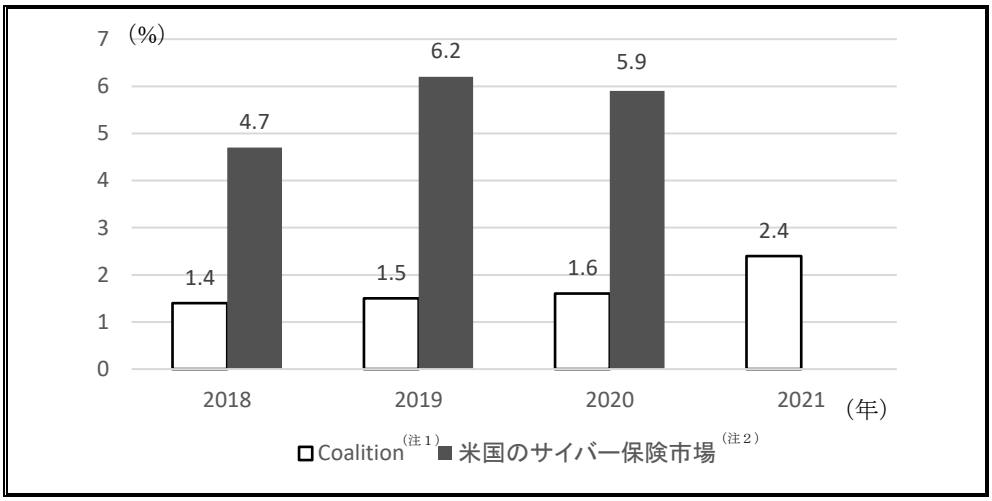
[63] Coalition は前記(1)c のホワイトハウスにおいて、バイデン大統領や政府、その他の民間企業と協力して米国のサイバーセキュリティの課題に取り組むこと、および中堅・中小企業の安全を守るために、利用

Coalition の顧客数は過去 1 年間で倍増して 5 万を超え、また総取扱保険料は前年比 9 倍の 3 億 2,500 万ﾄﾞﾙ以上となったとされる。これは、同社の保険引受およびリスク管理に関するビジネスモデルがうまく機能していることの表れだとしている。同社によると、同社の保険契約件数に占める保険金支払件数の割合は、米国のサイバー保険市場の平均に比べて 3 分の 1 以下だとしている（図表 17 参照）。

Coalition の CEO は、「Coalition のサイバー保険の特徴は、一般的な補償に加えて、サイバー攻撃によって生じる可能性のあるあらゆる財物損壊も補償対象としている点にある。これは、従来のサイバー保険よりも補償範囲が広いが、データ分析力を最大限に活用することで収益性の確保も可能になっている」としている。

パンデミックとそれに続くサイバー攻撃の急増が、同社の大きな成長の原動力となっている。Coalition は、2021 年 9 月に 2 億 500 万ﾄﾞﾙを調達[64]し、これまでの調達総額は 5 億ﾄﾞﾙ以上となった。今回調達した資金は、新たな地域やサイバー保険以外の保険種目への事業展開、および従業員数の拡大等に使用する。従業員は現在 265 名で、2021 年末までに 315 名に増加する見込みとしている。さらに Coalition は 2021 年 12 月、新たにキャプティブを立ち上げ、サイバー保険のリスクテイクを開始することを公表した。具体的な取組内容は明らかにしていないが、これにより同社は、キャパシティの管理能力と長期的な成長力の強化を図るとしている[65]。

図表 17　保険契約件数に占める保険金支払件数の割合



（注１）2021 年のデータは、公表時点での見込と推測される。

（注２）NAIC の統計データによる市場平均であり、2021 年のデータは未公表である。

（出典：Coalition, “Cyber Insurance Claims Report H1 2021”（2021）をもとに作成）

しやすい技術とインセンティブを幅広く組み合わせて対応すること等を約束した。また、保険契約者のためのリスク管理プラットフォームを、どの企業にも無償で提供することを公約し、直ちに実行に移したとされる。

64 この資金調達では、複数の投資ファンド等が主導し、同社の既存投資家も参加した。

65 Coalition ウェブサイト

b. ミュンヘン再保険傘下の HSB と連携する Zeguro

Zeguro は 2016 年に設立され、カリフォルニア州サンフランシスコに本社を置き、中小企業向けにサイバー保険を含むサイバーセキュリティに関する包括的なサービスを提供しているインシュアテック企業である[66]。同社は米国の全州でライセンスを取得し、ミュンヘン再保険グループ傘下のハートフォードスチームボイラ検査保険（Hartford Steam Boiler Inspection and Insurance Company：以下「HSB」）等のアンダーライターとしての機能を担ってきた[67]。

Zeguro は、サイバーセキュリティと保険の専門家からなるチームを有し、顧客がデジタル時代の急速に進化するサイバー脅威に耐えられるよう支援する。Zeguro のサイバーセキュリティ・プラットフォームは、顧客のリスクを特定し、Zeguro の技術や研修等を通じてリスクを軽減する。加えて、データ関連の法規制や契約上の義務を遵守するための支援も行っているとしている。

ミュンヘン再保険のウェブサイトでは、HSB が提供する中小企業向けのサイバー保険について説明されており、その中で Zeguro の技術により提供される Cyber Safety™についても紹介されている。Cyber Safety™は、中小企業がサイバー攻撃を事前に防止できるように設計されたツールを含む包括的なサービスであり、主な機能は図表 18 のとおりである。

図表 18　Cyber Safety™の主な機能

項目	概要
ウェブサイトのモニタリング	○ウェブサイトの脆弱性につきスキャン調査する。 ○脆弱性を改善するための推奨事項を記載した報告書を取得できる。 ○調査結果を IT 担当者と共有し、セキュリティ改善のための措置を講じることができる。
セキュリティ研修	○Cyber Safety™に含まれる研修モジュールの利用により、従業員のサイバーセキュリティに対する意識を向上させることができる。 ○登録した従業員に対してサイバーセキュリティのスキル評価を行い、各従業員の長所と短所に基づいてカスタマイズされた研修を提供する。
セキュリティ方針の策定・管理	○Cyber Safety™に含まれるコンプライアンス文書のひな形を利用して、企業のサイバーセキュリティ方針を策定することができる。 ○これらの方針は必要に応じてカスタマイズし、データ漏洩対応計画や情報セキュリティ基準等にも対応させることができる。 ○1 つのダッシュボードですべてのセキュリティ方針等を一括して管理することができる。

（出典：Munich Re ウェブサイトをもとに作成）

[66] Zeguro ウェブサイト

[67] HSB は 3 年間にわたり Zeguro と提携のうえ、顧客にサイバー保険を提供してきた。しかし、2021 年 10 月、HSB は、Zeguro が開発した中小企業向けサイバーセキュリティ・プラットフォームを含む同社の中核事業を買収することを公表した。この買収により HSB は、Zeguro の技術を利用してサイバーセキュリティサービスを強化するとしている。なお、今後 Zeguro 本体は事業を継続しないとされている（Carrier Management, “Updated: Munich Re’s HSB Is Acquiring Zeguro’s Cybersecurity Digital Platform, Plus Six Employees”（2021.10））。

（3）サイバーリスク格付の定着に向けた動き

サイバーセキュリティリスクの評価は、企業等のリスク管理の観点から重要であることに加えて、保険会社にとっては、保険引受の際に、引受可否の判断、保険料率の決定のために重要な要素となる。企業等の関心が高まる中で、サイバーリスク格付に注目する動きがある[68]。

本項では、サイバーリスク格付の概要およびサイバーリスク格付プロバイダーの取組事例について説明する。

a. サイバーリスク格付の概要

サイバーリスク格付は、企業等のセキュリティ対策を含む総合的なサイバーセキュリティ・パフォーマンスをデータに基づいて定量的に評価し、その結果を簡単な記号で表したものである。サイバーリスク格付では、企業等のインターネット接続に関する外部から観察可能なデータを使用して、いくつかのセキュリティリスク要素に基づいて企業のサイバーセキュリティ態勢につき評価する。

デジタル化が進む社会において、サイバーリスク格付は今後、現在の信用格付のような地位を占めるようになると、調査会社である Gartner は予測している。格付機関と呼ばれる信用格付プロバイダーと同様に、現在、市場には多数のサイバーリスク格付プロバイダーが存在する。サイバーリスク格付は、リスクを適正に反映している場合は有効に機能すると考えられる反面、現時点では、サイバーリスク格付がリスクを適正に反映していないのではないかという懸念がある。これは、セキュリティリスク評価のための普遍的なスコアリング方法が現在のところ存在せず、プロバイダーによって異なる分析結果が提供される可能性があるためとされている。

調査・コンサルティング会社である Forrester は、サイバーリスク格付の市場について調査するため、この分野の主なプロバイダーとして 7 社[69]を選定し、それらを評価した。この調査では、格付モデルの精度、透明性等の要素を基準として、SecurityScorecard と BitSight の 2 社が市場のリーダー的な存在であるとされ、またサイバーリスク格付に関する課題として以下の点が挙げられた。

○ 企業が自社の格付が妥当でないと感じた場合、異議申立のプロセスは確立されておらず、評価結果を覆すことは困難である。
○ サイバーリスク格付プロバイダーは、リスク評価において、一般に公開されてい

---

68 Forrester, “The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021”（2021.2）。サイバーリスクについては損害データの蓄積が十分でなく、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の算出が難しいなどの課題があり、保険会社やモデリング会社等も、データの蓄積やモデルの構築等に取り組んでいる。

69 BitSight、SecurityScorecard、Black Kite、Panorays、Prevalent、RiskRecon、UpGuard の 7 社を指す。これらの事業者はいずれも、サイバーリスク格付関連の収益が年間 100 万ﾄﾞﾙ以上とされている。

る情報を利用している。このような情報はリスク評価に有用であるものの、公開情報の範囲が狭かったり、定期的に更新されていなかったりすることによって、情報が十分でないまま、企業の格付が決まってしまう可能性がある。

○ サイバーリスク格付プロバイダーは、格付を受ける企業からの情報を活用していない。このような方法では、企業は、評価を高めるために有効なデータを提供することができず、組織のセキュリティ態勢を示すことができない。

b. サイバーリスク格付プロバイダーの取組事例

本項では、サイバーリスク格付プロバイダーの代表的な事例として、SecurityScorecard と BitSight の 2 社を取り上げ、それらの業務・取組等の概要を説明する。

（a）SecurityScorecard

SecurityScorecard は、サイバーセキュリティ分野の専門家等によって 2013 年に設立され、ニューヨークに本社を置き、現在 1,100 万社以上の企業を継続的に格付している[70]。特許取得済みの格付技術は 2 万 5,000 件以上を有しており、同社の格付は、企業における自社のリスク管理やサイバー保険の引受等に利用されている。

SecurityScorecard は、世界中の企業を継続的にモニタリングし、非侵入型の独自の手法を用いて、10 種類の重要なサイバーセキュリティ要素[71]にわたってセキュリティ態勢を評価し、最終結果として「A」から「F」までの評価を提供している。これらの評価は、一般に公開されている客観的なデータに基づいて日々更新されており、信用格付と同様に、企業のセキュリティ態勢を外部からの視点で評価している。

SecurityScorecard は、サイバーリスクは進化し続けるリスクであり、継続的な精査が必要としたうえで、保険会社におけるサイバー保険の引受プロセス上の課題として以下の 3 つを挙げている。

① 企業のサイバーリスクをどのように評価するか
② サイバーリスクに詳しくない保険会社の従業員や代理店および保険ブローカーが容易に理解できる共通のサイバーリスクの分類法をどのように定めるか
③ 顧客に対し、顧客のサイバーリスクについてどのように伝えるか

---

[70] SecurityScorecard ウェブサイト

[71] 例えば、インターネット上でドメイン名を管理するためのシステムである Domain Name System（DNS）の健全性、IP レピュテーション（IP アドレスのレピュテーション・信用等の確認）、ウェブアプリケーションのセキュリティ、ネットワークのセキュリティ、情報漏えいの状況、ハッカーチャッター（ハッカーサイト上で話題となっているかどうか等の確認）、エンドポイントのセキュリティ（社員の作業端末のセキュリティレベルの測定）、パッチの適用状況（サポート切れや脆弱な製品の検出）等が挙げられている。

これら3つの課題はすべて、SecurityScorecardのサイバーリスク格付を含むソリューションを保険会社の引受プロセスに組み込むことで解決するとされている。具体的には、SecurityScorecardが保険会社に対し、サイバー保険への加入を検討している企業のサイバーリスクを自動的に評価するツールを提供する。このツールの利用により保険会社は、その企業のサイバーリスク格付(単純なAからFによる評価)、および10種類のサイバーセキュリティ要素のそれぞれにおけるスコアを得ることができる。

なお、SecurityScorecardは2021年11月、世界的なセキュリティ専門家の不足に対応するための、高度なサイバーセキュリティの教育・研修等のための包括的なオンラインコミュニティであるSecurityScorecard Academyの創設を公表した。同社は、これを通じて、企業の最高情報セキュリティ責任者（Chief Information Security Officer：CISO）等を対象として、2023年末までに2万5,000人以上に研修を実施するとしている。

（b）BitSight

BitSightは、2011年に設立され、マサチューセッツ州ボストンに本社を置き、世界中に2,300社の顧客を有し、サイバーリスク格付と分析サービス等を提供している。BitSightのサイバーリスク格付プラットフォームは、高度なアルゴリズムを適用し、250から900の範囲のサイバーリスク格付を毎日策定し、企業等におけるセキュリティ・パフォーマンス管理・リスク軽減、および保険会社によるサイバー保険の引受等につき支援している。

BitSightは保険会社に対し、サイバー保険の申込企業における過去のセキュリティ状況や業界またはポートフォリオのベンチマークとの比較を含む客観的な報告書を提供するため、保険会社は個々の企業のサイバーリスクを適切に評価し、引受能力を強化することができる。また保険会社は、保険契約企業のポートフォリオ全体のリスクをダッシュボードで一覧表示し、セキュリティ状況に急激な変化があった場合は警告通知を受け取ることもできるとされる。

さらに、BitSightのサイバーリスク格付により、保険会社は被保険者のセキュリティ状況が時間とともにどのように変化してきたかを履歴として把握することができ、保険金請求が発生する前に、保険契約企業のセキュリティ状況を改善することができる。このようにして保険会社は、他の保険会社に対し競争上の優位を確保できるとされている[72]。

BitSightは2021年11月、Marsh McLennan[73]と提携することを公表した[74]。

---

[72] BitSightウェブサイト

[73] 保険ブローカーであるマーシュの親会社であり、リスク・保険・人材・経営戦略分野における総合サービスを提供している。

[74] Zacks Equity Research, “Marsh & McLennan (MMC) Unites With BitSight, Hikes Cyber Security”

Marsh McLennan のサイバーリスク分析センター[75]は、BitSight のサイバーリスク格付プラットフォームを活用し、顧客がサイバーセキュリティのパフォーマンスをよりよく理解し、より多くの情報に基づくリスク管理の意思決定を行えるようにする。サイバーインシデントの増加に伴い、Marsh McLennan が提供するサービスへの需要は急速に高まっている。130 カ国に及ぶ同社の顧客は、BitSight を利用することで、情報をシームレスに受け取り、潜在的なリスクを迅速に特定し、それに応じたリスク軽減等の戦略を講じることができる。また、BitSight と Marsh McLennan は、共同調査・分析も開始するとされている。

なお BitSight は、格付機関 Moody's との提携も 2021 年 9 月に公表しており、市場でのサイバーリスク格付の定着を目指すとしている。Moody's は BitSight に 2 億 5,000 万ﾄﾞﾙを出資し、両社は統合的なサイバーセキュリティリスク・プラットフォームを構築する。また BitSight は、サイバーリスク定量化の専門会社である VisibleRisk を買収するとされている[76]。

4．サイレント・サイバーリスクを巡る動向

サイレント・サイバーリスクへの対応に関しても過去 1 年で進展が見られた。本項では、これまでの経緯につき概説したうえで、エクスポージャーの定量化と財務力格付への影響、ロイズの動向[77]、および保険ブローカーLockton が開発した商品の事例について紹介する。

（1）経緯

サイレント・サイバーリスクとは、従来から存在する損害保険（以下「従来型保険」）の約款において補償対象と明示されておらず、免責の対象ともされていないサイバーリスクを指す。サイバー被害は従来型保険で伝統的に補償されてきた財物損壊や賠償責任をもたらす可能性があるため、こうした損害は、サイバーリスクを補償するために設計されたサイバー保険だけでなく、サイバーリスクを考慮せずに設計された従来型保険においても補償しているとみなされる可能性がある。サイバー被害の増加・多様化に伴って、サイレント・サイバーリスクのエクスポージャーも増大することが懸念されてきた。

（2021.11）

[75] Marsh McLennan グループ傘下のマーシュ、ガイカーペンター、マーサー、およびオリバーワイマンという 4 つのビジネスユニットのサイバーリスクに関するデータ分析・軽減策等を統合したものであり、その創設が 2021 年 10 月に公表されている。

[76] Steve Harvey, “The BitSight and Moody's Partnership: A New Era For Cybersecurity”（BitSight, 2021.9）

[77] 本稿では全体的に米国の動向を中心に紹介しているが、サイレント・サイバーリスクについてはロイズの動向も注目に値するため本項で取り上げている。

サイレント・サイバーリスクへの対応は、米国やイギリスを中心に、従来型保険にサイバー関連の免責条項を導入することなどで進められてきた。米国ではISO[78]が免責条項を開発し、多くの保険会社がこれを採用してきた。イギリスでは、金融機関の健全性規制を担う健全性監督機構（Prudential Regulation Authority：以下「PRA」）が中心となってサイレント・サイバーリスク問題に取り組み、保険会社に対応を講ずるよう求めてきた[79]。

サイレント・サイバーリスクへの対応について保険会社は、ここ数年、サイバーリスクの引受を単独型サイバー保険に移行したり、従来型保険に、サイバーリスクに関する免責条項やサブリミットを導入したりすることで、エクスポージャーの削減に努めてきた。また、サイバーリスクを補償対象とする場合は、それを約款に明記し、その分の適正な保険料を請求する方向で対応を進めてきた。このようにして欧米主要国の大手保険会社の多くは、2020年までに対応を完了したとしている[80]。

しかし、サイレント・サイバーリスクの問題は未だ解消されておらず、依然として保険業界にとって重要な課題の1つであるとの見方もある[81]。単独型サイバー保険市場の規模が拡大し、洗練されてきたことや、新型コロナウイルス感染症の影響もあってサイバー攻撃が増加してきたことも、様々な従来型保険におけるサイレント・サイバーリスクの再評価を促す一因となっている。

（2）エクスポーポージャーの定量化と財務力格付への影響

AM Bestは2021年10月、保険会社向けにサイバーリスク分析等のサービスを提供するCyberCubeおよびエーオンと共同で報告書を公表した[82]。本報告書は、米国の損害保険市場に蓄積されているサイレント・サイバーエクスポージャーを定量化し、格付への影響を示すことを目的としている。報告書では、保険会社によるサイレント・サイバーリスク対応はまだ十分進んでおらず、企業向け損害保険におけるサイバー補償のさらなる明確化やサイバーリスクに見合う適切な保険料の設定が必要であることが示された。

---

78 ISO（Insurance Services Office）は米国においてモデル約款の提供や保険料率の算出、その他各種データ提供等を行う組織であり、情報サービス会社であるVerisk Analyticsの傘下にある。

79 米国とイギリスでの対応については、金奈穂「サイレント・サイバーリスクを巡る動向－米国・イギリスを中心に－」損保総研レポート第126号（損害保険事業総合研究所、2019.1）も参照願う。

80 林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」損保総研レポート第134号（損害保険事業総合研究所、2021.1）。なお、欧米主要国の主な監督当局・団体等の対応状況も同レポートで整理されており、それ以降の新たな動きは少ないため、本稿では取り上げていない。

81 例えば、後記(2)のAM Bestによる報告書のほか、ニューヨークを拠点とするUSI Insurance Servicesは、会社役員賠償責任保険（D&O保険）等を中心として問題は残っており、保険会社はさらなる努力が必要であるとしている。なおD&O保険では通常、取締役や役員の不正行為による損害を補償するため、取締役や役員のサイバーインシデントへの関与に伴う損害等が補償対象となる可能性がある。また財産保険においては、サイバーインシデントに起因する財物損壊や事業中断等が補償対象となる可能性がある。

82 Steve Evans, “Silent cyber in US property insurance has $12.5bn loss potential: Report”（Artemis, 2021.10）

本報告書によると、米国の損害保険市場には、サイレント・サイバーエクスポージャーが蓄積されており、100 年に 1 度の大規模なインシデントが発生した場合、損害保険会社は業界全体で 125 億ﾄﾞﾙの損失を被る可能性がある。米国の企業向け損害保険におけるサイバーエクスポージャーの現状は管理可能なレベルにあるものの、このエクスポージャーが高水準にある保険会社の一部では、財務力格付に影響を及ぼす可能性があるとしている。

CyberCube は、米国の中小企業向け損害保険に関するサンプルポートフォリオを分析し、モデル化された特定のサイバー損害シナリオの下でストレスを与え、損害の可能性を定量化した。AM Best はこの分析結果をもとに、米国の損害保険会社 579 社の財務内容への影響を評価し、この規模の損害が発生した場合、自己資本比率（Best's Capital Adequacy Ratio：BCAR）の低下により、18 社の財務力格付が引き下げられる可能性があるとした。

米国では、サイバーリスクが今後も急速に高まると予想されることから、損害保険市場におけるサイレント・サイバーエクスポージャーも急速に拡大すると考えられている。AM Best は、125 億ﾄﾞﾙの損害は自然災害の損害と比べると小さいように見えるが、これらのエクスポージャーが保険会社のリスク管理や、保険料の設定において考慮されていないことが多いことを考えると、影響は予想外に大きくなる可能性があるとしている。

なお本報告書では、ホームオーナーズ保険等の住宅用保険は分析対象とされていない。住宅用保険においてもサイレント・サイバーリスクの問題は脅威であり、今後数年以内に大きな損害をもたらす可能性があるとしている。

（3）ロイズの動向

本項では、保険会社におけるサイレント・サイバーリスク対応について見るうえで米国と同様に重要と考えられるイギリスでのロイズの動向について紹介する。ロイズは 2020 年 1 月以降 4 段階で、サイレント・サイバーリスク対応を進めてきた。また 2021 年 3 月と 9 月にも約款上の規定に関する新たな方針を示しており、本項ではこれらの概要について説明する。

a. ロイズにおける対応の概要

2019 年 1 月に PRA が保険会社に対し、意図しないサイバーエクスポージャーの削減を求めたことを受け、ロイズは 2019 年 7 月、シンジケートの保険会社が様々な保険種目においてサイバーリスクを補償対象とするか、免責とするか明記することを求める指令を発出した[83]。各保険種目において準拠しなければならない期日を 4 段階に分け

[83] Lloyd's, "Market Bulletin Y5258"（2019.7）

て実施することとし、第1段階の2020年1月の財産保険等から開始された[84]（図表19参照）。2021年1月からは第3段階として会社役員賠償責任保険（Directors and Officers liability insurance：以下「D&O保険」）等に、7月からは第4段階として医療過誤保険等に適用され、同年にはすべての対応が完了したことになる。

このような課題に対応するため、ロイズ市場協会（Lloyd's Market Association：以下「LMA」）やロンドン国際引受協会（International Underwriting Association：IUA）等の業界団体等は、サイバーリスクに関するモデル免責条項[85]を公表しており、多くの保険会社がこれらを適用している。

図表19　ロイズにおけるサイレント・サイバーリスクへの対応

段階	開始時期	対象となる主な保険種目
第1段階	2020年1月	財産保険、海上保険等
第2段階	2020年7月	傷害保険、信用保険、金融保証保険等
第3段階	2021年1月	D&O保険、専門職業人賠償責任保険等
第4段階	2021年7月	医療過誤保険等

（出典：LMAウェブサイトほかをもとに作成）

b. シングルペリル型保険とD&O保険での扱い

LMAは、サイバーリスクの補償内容を顧客に明確に伝えるための要件を定めて公表しており、2021年3月にシングルペリル型保険（および再保険）[86]、および同年9月にD&O保険（および再保険）に関する図表20の方針を示した。すなわちロイズは、これらの保険に関して、マネージング・エージェント[87]が保険約款でサイバーリスクを補償対象とするか免責とするか明示することなく、引受を行うことができるとの考え方を示している[88]。

---

84 2020年1月以降に開始されるすべての財産保険等は、サイバーリスクを補償対象とするか、免責とするか、約款に明記しなければならないとされた。

85 モデル免責条項の内容については、林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」損保総研レポート第134号（損害保険事業総合研究所、2021.1）を参照願う。

86 一般的に、シングルペリル型は単一の災害（例えば地震等）を対象とするものをいい、マルチペリル型は複数の災害（例えば、ハリケーンと地震）を対象とするものをいう。

87 ロイズ市場における保険引受は、これに参加する各メンバーが行っている。メンバーが保険を引き受けるためには、いずれかのシンジケートに参加する必要があり、メンバーは当該シンジケートが引き受けるリスクについて、それぞれの出資割合に応じた保険責任を負担する。メンバーに代わって保険の引受業務等のシンジケートの運営を行うのがマネージング・エージェントである。

88 これらの方針変更の背景には、サイバーリスク以外のリスクも広く補償対象としているのに、サイバーリスクだけを補償対象として約款に明記することは、保険契約者に混乱をもたらす可能性があるとの考え方がある。

図表 20　特定の保険種目等に関するサイレント・サイバーリスクへの対応

公表時期	種目等	概要
2021 年 3 月	シングル ペリル型 保険	○この保険は、特定の単一のペリル（例えば地震等）による損害をトリガーとする。 ○この保険は、原因が何であれ、またサイバーインシデントが指定されたペリルに関連しているかどうかにかかわらず、保険対象となるペリルの結果として生じるすべての損害に対して保険金を支払うことを前提としているため、マネージング・エージェントは約款でサイバーリスクの補償につき明示することなく、引受を行うことができる。 ○ただし、マネージング・エージェントがこれらのシングルペリル型保険の下でサイバーリスクを除外または制限しようとする場合には、適切な除外表現を適用する必要がある。
2021 年 9 月	D&O 保険	○この保険は、取締役や役員の不正行為をトリガーとする。 ○この保険は、原因が何であれ、またサイバーインシデントが不正行為に関連しているかどうかに関わらず、不正行為の結果としての損害に対して保険金を支払うことを前提としているため、マネージング・エージェントは約款でサイバーリスクの補償につき明示することなく、引受を行うことができる。 ○ただし、マネージング・エージェントがこれらの D&O 保険でサイバーエクスポージャーを除外または制限しようとする場合は、適切な除外表現を適用する必要がある。

（出典：LMA, “Lloyd's Market Association Bulletin LMA21-008-PD”（2021.3）、LMA, “Lloyd's Market Association Bulletin LMA21-035-PD”（2021.9）をもとに作成）

（4）保険ブローカーLockton による商品提供の事例

保険ブローカーである Lockton は、保険業界にサイレント・サイバーリスク問題が存在することを踏まえて、同リスクに対応する商品を世界中に提供するとしており、本項では、同社によるサービスの概要について説明したうえで、この商品の特徴等について説明する。

a. Lockton によるサービスの概要

Lockton[89]は、1966 年に米国のミズーリ州カンザスシティで設立され、現在はイギリスのロンドンに本社を置く。企業が財務内容を保護し、レピュテーションを維持し、組織を成長させるために、情報提供、改善（コンサルティングとロスコントロール）、および保険ソリューションの開発という 3 つのステップによるアプローチでサービスを提供しているとする（図表 21 参照）。

Lockton は、保険会社が通常提供している商品よりも広い補償範囲の商品を開発し、顧客に推奨している。また、3,000 社を超える顧客の保険契約データ、比較分析等により、継続的にパフォーマンスを測定し、最良のサイバー保険を長期的に提供し続けることができるとしている。

[89] Lockton は、世界最大級の非上場の独立系保険ブローカーであり、世界各地に 50 名以上のサイバー関連の技術者を擁し、175 社以上の保険会社と取引関係がある。年間 300 件以上のインシデントに対応し、これまでの保険金請求の成功率は 99%に達しているとしている。

図表 21　Lockton の 3 ステップアプローチの概要

3 ステップ	概要
情報提供	○サイバーリスク分析の専門会社である Corax と提携し、サイバーセキュリティ、リスクの定量化、同業他社のベンチマーク等の情報を顧客に提供する。 ○損害原因の分析、リスク管理システムの見直し、ソリューションプランの策定、およびプランの実行等を支援する。 ○Lockton のアドバイザーが、サイバー保険の補償範囲、保険金請求方法、および保険市場の動向等に関する情報を提供する。
改善（コンサルティングとロスコントロール）	○顧客の一般社員から役員までを対象として、サイバーに関する認識とベストプラクティスに関する教育を行い、セキュリティガバナンスの枠組、方針、および手順等の策定を支援する。 ○顧客が自信を持ってサイバーリスクを評価し、対処できるよう、顧客のサイバーセキュリティの状況、データ漏えいのシナリオ等を調査する。
保険ソューションの開発	○Lockton は、保険会社が必要と考えるサイバー保険を顧客に販売することが仕事ではないと考えている。 ○顧客固有のリスクに合った保険を開発し、グローバルな保険会社との関係を活かして、その保険を引き受けてくれる保険会社を探す。 ○そのために、独自の契約形態や保険会社の約款に付帯する特約を開発し、補償範囲を広げている。

（出典：Lockton ウェブサイトほかをもとに作成）

b. サイレント・サイバー財産保険の特徴等

Lockton は、Silent Cyber Property Solution（以下「サイレント・サイバー財産保険」）と呼ばれる、市場での一般的な商品よりも補償範囲が広い単独型の商品を開発し、提供する[90]ことを公表した[91]。

サイレント・サイバー財産保険は、サイバー攻撃やサイバーテロの結果として生じる財物損壊および事業中断の両方を補償対象とすることができる独自の財産保険である。この保険では、追加費用、賃貸料の喪失、損害防止費用、残存物取片づけ費用、消防費用、および臨時費用等も補償し、さらに事業中断損害等を補償対象として追加することも可能であり、保険契約者は、1 インシデントあたり 1 億 5,000 万ﾄﾞﾙまでの補償を受けることができるとされている。

Lockton によると、「サイバー攻撃やサイバーテロが発生した場合、財物損壊や事業中断等により被る損害と、従来の財産保険で受けられる補償との間には大きなギャップがあり、企業にとって非常に大きな負担となる。サイバー攻撃が増加する中で、企業がこのようなリスクに備える必要性は益々高まっている。多くの保険契約者は、サイバー攻撃やサイバーテロによる財物損壊および事業中断損害等が既存の損害保険で補償対象となると考えているが、近年はオールリスク型の保険であっても、サイバーリスクに関する免責条項が付帯されるケースが増えているため、実際には補償対象になっていないことが多い。」とされている。多くの保険会社がサイレント・サイバーリスク対応の観点から財産保険の契約においてサイバーリスクを免責とする傾向がある中で、

[90] この保険は、中国やイスラエル等の一部の国・地域を除き世界中で提供される。
[91] Insurance Journal, “Lockton Launches Silent Cyber Property Solution for Businesses”（2021.10）

Lockton による本商品の提供は、そのような動きに対抗する戦略とも考えられる。

５．おわりに

これまで見てきたとおり、米国では多くの保険会社が、サイバー保険における損害率の悪化傾向に伴い、保険料率の引上げや支払限度額の引下げ等の引受条件の厳格化を進めている。顧客企業によるサイバーセキュリティ対策をより厳しく評価したり、新たなツール等の提供によりリスク軽減を積極的に支援したりする動きも見られる。また、サイレント・サイバーリスクへの対応の観点から、単独型サイバー保険の引受による明確なサイバーリスク補償の提供を進めると同時に、従来型保険においてはサイバーリスクを免責として約款に明記することが主流となっている。このような状況下で大手保険会社同士の共同取組も開始されている。

一方、インシュアテック企業の中には、より広範なサイバー関連リスクを補償対象とし、サイバーリスクの評価やサイバーセキュリティ関連サービスまで含む包括的なサービスの提供により事業を拡大している企業もある。また、財産保険にサイバーリスクの補償を加えた、より包括的な補償の提供に注力する保険ブローカーも見られる。

今後、在宅勤務でのパソコン等の利用に加えて、IoT 等のデジタル化が進んでいく中で、企業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られる。そのため企業は、これまで以上に包括的な補償やリスク移転・軽減の手段を求めるようになるのではないだろうか。そうだとすれば、従来型の大手保険会社にとっても、このような包括的な商品・サービスの提供が新たな収益機会となる可能性が考えられる。

ただし、引受戦略の中心を広範な補償、または限定的な補償のどちらに置くべきなのかは、保険会社の引受能力等により異なる可能性がある。いずれの場合でも、保険会社にとっては、サイバーリスクを適正に評価し、それを商品設計や保険料率に的確に反映することを通じて、保険の利便性と収益性をバランスよく維持することが必要である。そのためには、サイバーセキュリティ技術に強みを持つインシュアテック企業等との連携も含めて、データの蓄積、モデルの精緻化、技術力の活用等を積極的に推進することが重要になろう。

サイバー保険市場は、米国でもまだ成長途上にあり、欧州やわが国でも今後拡大していく可能性が高い。変化の大きい市場であるため、引き続き注視することとしたい。

＜参考資料＞

・牛窪賢一「米国におけるサイバー保険の動向」損保総研レポート第 120 号（損害保険事業総合研究所、2017.7）
・牛窪賢一「米国における新型コロナウイルスと事業中断保険を巡る動向」損保総研レポート第 132 号（損害保険事業総合研究所、2020.7）
・金奈穂「サイレント・サイバーリスクを巡る動向－米国・イギリスを中心に－」損保総研レポート第 126 号（損害保険事業総合研究所、2019.1）
・損害保険事業総合研究所「欧米主要国の保険業界における新型コロナウイルス感染症への対応」（2021.3）
・損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）
・日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」（2020.12）
・濵田和博「主要国におけるパンデミックに係る事業中断保険の現状」損保総研レポート第 138 号（損害保険事業総合研究所、2022.2）
・濵田和博「新型コロナウイルスの損害保険業界への影響」損保総研レポート第 132 号（損害保険事業総合研究所、2020.7）
・林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」損保総研レポート第 134 号（損害保険事業総合研究所、2021.1）
・Accenture, “Triple digit increase in cyberattacks: What next?”（2021.8）
・Allianz Global Corporate & Specialty, “Ransomware trends: Risks and Resilience”（2021.10）
・AM Best, “Market Segment Report: Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk”（2021.6）
・Anoop Khanna, “Cyber protection and global insurance programmes”（Asia Insurance Review, 2021.11）
・Aon, “US Cyber Market Update: 2020 US Cyber Insurance Profits and Performance”（2021.6）
・AXA, “AXA Future Risks Report 2021”（2021.9）
・Carrier Management, “Updated: Munich Re’s HSB Is Acquiring Zeguro’s Cybersecurity Digital Platform, Plus Six Employees”（2021.10）
・Coalition, “Cyber Insurance Claims Report H1 2021”（2021）
・Corvus, “Corvus Risk Insights Index Q4 2021”（2021.11）
・Dan Burke, “Cyber Security Controls: Now Critical for Your Cyber Insurance Renewal”（Woodruff Sawyer, 2021.2）
・Forrester, “The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021”（2021.2）
・Frank Bajak, “Insurer AXA to Stop Paying for Ransomware Crime Payments in France”（Insurance Journal, 2021.5）
・GAO, “Cyber Insurance; Insurers and Policyholders Face Challenges in an Evolving Market”（2021.5）
・IAIS, “Global Insurance Market Report”（2021.11）
・Ian Smith, “Cyber insurers recoil as ransomware attacks ‘skyrocket’”（Financial Times, 2021.6）
・Insurance Journal, “7 Major Cyber Insurers Form Company to Coordinate Cyber Analysis, Risk

Mitigation”（2021.6）
・Insurance Journal, “Lockton Launches Silent Cyber Property Solution for Businesses”（2021.10）
・Insurance Journal, “What Insurance Firms Promised at White House Cybersecurity Summit”（2021.8）
・Insurance Journal, “Zurich Insurance Partners with Cyber-Security Specialist CYE”（2020.2）
・Judy Greenwald, “Cyber Cover Costs Expolde, Capacity Limited”（Business Insurance, 2021.11）
・Life Insurance International, “Axa’s announcement to stop coverage of ransomware payments prompts broader cyber insurance debate”（2021.6）
・Lloyd’s, “Market Bulletin Y5258”（2019.7）
・LMA, “Lloyd's Market Association Bulletin LMA21-008-PD”（2021.3）
・LMA, “Lloyd's Market Association Bulletin LMA21-035-PD”（2021.9）
・Mark Hollmer, “Chubb CEO Greenberg Stresses Need to Address Ransomware and ‘Systemic’ Cyber Risk”（Insurance Journal, 2021.7）
・MarketScreener, “Chubb：Enhances Cyber Risk Service Offerings to Further Support Clients in Helping to Reduce Potential Losses”（2021.11）
・Marsh McLennan Agency, “Cyber Risk Perceptions Survey Findings 2020-2021”（2021.11）
・NAIC, “Report on the Cybersecurity Insurance Market”（2021.10）
・NetDiligence, “Cyber Claims Study 2021 Report”（2021）
・OECD, “Encouraging Clarity In Cyber Insurance”（2020.2）
・S&P Global, “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20”（2021.6）
・Scott Ikeda, “Cyber Insurance Claims Spike With Major Attacks, but Ransomware Costs Down Sharply From 2020”（CPO Magazine, 2021.11）
・Scott Ikeda, “Ransomware Attack Reported at Insurance Giant AXA One Week After It Changes Cyber Insurance Policies in France”（CPO Magazine, 2021.5）
・Steve Evans, “Silent cyber in US property insurance has $12.5bn loss potential: Report”（Artemis, 2021.10）
・Steve Harvey, “The BitSight and Moody's Partnership: A New Era For Cybersecurity”（BitSight, 2021.9）
・Zacks Equity Research, “Marsh & McLennan (MMC) Unites With BitSight, Hikes Cyber Security”（2021.11）

＜参考ウェブサイト＞

・イギリス健全性監督機構（PRA） https://www.bankofengland.co.uk/prudential-regulation
・欧州保険・年金監督局（EIOPA） https://eiopa.europa.eu/
・経済協力開発機構（OECD） http://www.oecd.org/
・全米保険監督官協会（NAIC） http://www.naic.org/
・損害保険事業総合研究所 https://www.sonposoken.or.jp/

・日本損害保険協会　https://www.sonpo.or.jp/
・米国会計検査院（GAO）　https://www.gao.gov/
・米国財務省　https://home.treasury.gov/
・米国損害保険協会（APCIA）　http://www.pciaa.net/
・米国独立代理店・ブローカー協会（IIABA）　https://www.independentagent.com/
・米国保険情報協会（I.I.I.）　http://www.iii.org/
・保険監督者国際機構（IAIS）　https://www.iaisweb.org/
・保険サービス事務所（ISO）　https://www.verisk.com/insurance/brands/iso/
・ロイズ市場協会（LMA）　https://www.lmalloyds.com/
・ロンドン国際引受協会（IUA）　https://www.iua.co.uk/
・Accenture　https://www.accenture.com/us-en
・AIG　https://www.aig.com/
・AM Best　http://www.ambest.com/
・Allianz　https://www.allianz.com/
・Aon　https://www.aon.com/
・Artemis　https://www.artemis.bm/
・Asia Insurance Review　https://www.asiainsurancereview.com/
・AXA　https://www.axa.com/
・BitSight　https://www.bitsight.com/
・Business Insurance　https://www.businessinsurance.com/
・Carrier Management　https://www.carriermanagement.com/
・CBInsights　https://www.cbinsights.com/
・Chubb　https://www.chubb.com/US-EN/
・CNA　https://www.cna.com/web/guest/cna/home
・Coalition　https://www.coalitioninc.com/
・Corvus　https://www.corvusinsurance.com/
・Coveware　https://www.coveware.com/
・CPO Magazine　https://www.cpomagazine.com/
・CyberAcuView　https://cyberacuview.com/
・CyberCube　https://www.cybcube.com/
・Digital Insurance　https://www.dig-in.com/
・FBI　https://www.fbi.gov/
・Financial Times　https://www.ft.com/
・Forrester　https://www.forrester.com/bold
・Gartner　https://www.gartner.com/en
・GlobalData　https://www.globaldata.com/

・Guy Carpenter　https://www.guycarp.com/

・Hartford　https://www.thehartford.com/

・Insurance Journal　https://www.insurancejournal.com/

・Insurance Post　https://www.postonline.co.uk/

・Lockton　https://global.lockton.com/apac/en

・Lloyd's　https://www.lloyds.com/

・Marsh　https://www.marsh.com

・Marsh McLennan Agency　https://www.marshmma.com/

・Munich Re　https://www.munichre.com/en.html

・NetDiligence　https://netdiligence.com/

・PropertyCasualty360　https://www.propertycasualty360.com/

・PwC　http://www.pwc.com/

・S&P Global　https://www.spglobal.com/ratings/en/

・SecurityScorecard　https://securityscorecard.com/

・Sophos　https://www.sophos.com/

・Swiss Re　https://www.swissre.com/

・Travelers　https://www.travelers.com/

・USI Insurance Services　https://www.usi.com/

・Verisk Analytics　https://www.verisk.com

・Willis Towers Watson　https://www.willistowerswatson.com/

・Woodruff Sawyer　https://woodruffsawyer.com/

・Zacks Equity Research　https://www.zacks.com/

・Zeguro　https://zeguro.com/

・Zurich Insurance　https://www.zurich.com/