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

主席研究員　林　圭一

目　　次

要旨

わが国を含む世界各国で、情報通信ネットワーク上のサイバーセキュリティの脆弱性を狙う、巧妙な手口のサイバーインシデントが急増している。サイバーインシデントについては、ランサムウェア攻撃による被害の増加や新型コロナウイルス感染拡大に伴う影響が大きな特徴となっている。このような被害を補償するサイバー保険については、保険事故の増加によって損害率が悪化していることを受けて、米国大手損害保険会社を中心に引受基準を厳しくする動きがある。一方で、インシュアテック企業等の新たな参入の動きも見られ、これらの企業は独自の技術を利用して保険契約者のリスクを評価し、保険の提供とともに、リスク軽減のための支援にも積極的に取り組んでいる。

日本損害保険協会の2020年の調査によると、わが国の企業のサイバー保険加入率は7.8%にとどまっている。それに対し欧米主要国ではサイバー保険の活用が進んでおり、特に米国においては企業の加入率は50%以上となっている。

当研究所では、サイバーリスクへの対応やサイバー保険のあり方などの重要性に鑑み、2019年度上半期調査により、「欧米地域におけるサイバー保険関連動向」（2019年9月）を公表した。本稿では、その後のサイバーインシデントとサイバー保険市場の動向について米国を中心に紹介する。

これらの動向は、今後わが国においても、サイバーリスクへの対応やサイバー保険のあり方、さらには情報通信ネットワークに関係する社会基盤のレジリエンス強化に向けた対応等の検討を行う際に参考になるものと考えられる。

１．はじめに

情報通信ネットワーク上の不正アクセスをはじめとする迷惑行為・犯罪行為が世界各地で国境を越えて数多く発生している。わが国においてもサイバーインシデント[1]の発生が増加している。警察庁の調査[2]によると 2020 年上半期において標的型攻撃メール[3]の件数は昨年比で 48%増加して 3,978 件となった。また、サイバー攻撃[4]への布石と思われる、企業のネットワークや IoT[5]機器への不正アクセス件数は 1 つの IP アドレス[6]につき前年の 2 倍以上の 1 日あたり 6,218 件、インターネットバンキングの不正送金は昨年の 4.8 倍の 885 件発生している。

サイバー攻撃の目的は主に機密情報の盗取、金銭の奪取、業務の妨害の 3 つが挙げられる。2019 年以降サイバー攻撃の手口がさらに巧妙化し、機密情報と金銭の両方を狙うケースが多くなってきている。特にランサムウェア[7]による攻撃の急速な進化など犯罪組織のサイバー攻撃技術が高度化したことによって被害が拡大しているとされている[8]。

世界的なサイバーインシデントの増加を背景として、わが国においてもサイバーリスク対策の検討が活発化している。金融庁は 2020 年 10 月 13 日に金融機関 110 社[9]に対しサイバーセキュリティ演習[10]を実施すると発表した。インターネットバンキングやキャッシュレス決済サービス等を通じた不正送金・不正出金の犯罪が増加していることを踏まえ、万一被害が発生した場合を想定して、システム、顧客対応体制、および顧客対応手順を確認し、2021 年初めにもフィードバックするとしている。

また経済産業省は日本経済団体連合会・日本商工会議所・経済同友会の主要経済 3 団体と連携し、2020 年 11 月 1 日にサプライチェーン全体でサイバーセキュリティ対策の推進を行うことを目的とした「サプライチェーン・サイバーセキュリティ・コンソーシアム」（Supply Chain Cybersecurity Consortium：以下「SC3」）を設立した。主要経済

---

1 サイバーインシデントとは、外部からの攻撃または内部不正等による情報セキュリティを脅かす事件や事故を意味する。具体的にはコンピュータウイルスによる感染、ネットワークへの不正アクセス、電子情報の盗難・漏えい等が挙げられる。

2 警察庁「令和２年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2020.10）

3 特定の企業や組織を狙って、機密情報や知的財産、各種アカウント情報を窃取しようとする攻撃を指し、メール送付の添付ファイルやリンクのクリックによってランサムウェア等に誘導する手口が多いとされる。

4 外部から企業内ネットワーク等のシステムに利用権限を持たない者が不正な手段で接続・侵入し、システムの機能不全や停止、データの改ざんや盗取、乗っ取り・遠隔操作等を行うことを意味する。

5 Internet of Things の略で、モノ（家電、車、建物・設備、インフラ等）をインターネット経由でサーバーやクラウドサービス等につなげる仕組を指す。双方向通信により、実効的・効率的なサービスの提供が実現するとされている。

6 コンピュータやスマートフォン等に割り当てられたインターネット上の住所を意味する。

7 Ransom（身代金）と Software（ソフトウェア）を組み合わせた造語で、身代金目的のコンピュータウイルスを意味する。

8 NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）

9 詳細は非開示とされているが、銀行、信用金庫、信用組合等のほか、証券会社、損害保険会社、生命保険会社、外国為替証拠金取引事業者、資金移動事業者、キャッシュレス決済事業者、暗号資産（仮想通貨）交換事業者、監査法人等が参加したとされている（金融庁ウェブサイト）。

10 サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の 3 つの視点（Delta）と防御（Wall）の視点から、組織内部門間および組織外部との連携の実効性等を確認し、業界全体のサイバーインシデント対応能力の向上を図る。参加金融機関は在宅勤務等の環境下で行うとされている（金融庁ウェブサイト）。

3団体は連名で、2020年11月19日に「サプライチェーン・サイバーセキュリティ確保に向けた共同宣言」を公表した。産業界が一体となって推進運動を進め、わが国の産業に対する信頼の維持・強化につなげるとしている。

本稿では、このような状況を踏まえて、サイバーインシデントの発生状況、およびサイバー保険[11]の動向について、世界のサイバー保険市場の 70%以上を占めるとされる米国を中心に各種公開情報等から紹介する。当研究所では 2019 年度上半期にも欧米地域におけるサイバー保険関連動向等について調査してきたため、本稿ではその後の1年程度の状況に焦点を当てて紹介する。

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

2．世界におけるサイバーインシデントの動向

本項では世界におけるサイバーインシデントの動向について、概況、ランサムウェア攻撃による被害の動向、および新型コロナウイルス感染拡大に関係するサイバーインシデントの動向の順に説明する。

（1）概況

米国の情報セキュリティ専門会社である McAfee とシンクタンクである米国の戦略国際問題研究所（Center for Strategic and International Studies：以下「CSIS」）の共同調査[12]によると、2020年にはサイバーインシデントは世界経済に1兆ﾄﾞﾙ[13]を超える経済損失をもたらすものと見込まれている。この経済損失は世界の GDP の 1%超に相当し、2018年の 6,000 億ﾄﾞﾙの 1.6 倍以上となっている。また、サイバーインシデントの被害を受けた企業の 92%が、この経済損失以外に直接的な金銭では測れない影響[14]も受けたとされている。

米国の情報セキュリティ専門会社である Check Point の調査[15]によると、サイバー攻

---

11 サイバー保険とは、サイバーインシデントによって保険契約者に生じた第三者に対する損害賠償責任のほか、損害復旧費用や喪失利益等を補償する保険である。付帯サービスとして、サイバーセキュリティ強化やサイバーインシデント発生時の緊急対応等についてのコンサルティング等も用意されている。

12 従業員 1,000 人以上の企業における 1,500 人の意思決定者に対するインタビュー調査であり、2020 年 4 月から 6 月までの期間に実施された。回答者数の内訳は、米国（300）、カナダ（200）、イギリス（200）、フランス（200）、ドイツ（200）、オーストラリア（200）、日本（200）となっている（McAfee, “The Hidden Costs of Cybercrime”（2020.12））。

13 CSIS は政府関係者へのインタビューとあわせ、被害に関する公表資料の調査および国際通貨基金（International Monetary Fund：IMF）の所得データをもとに国民所得水準による調整値の概算を利用して費用計算したとしている。

14 2019 年に被害が発生した企業・組織から、システムの停止・中断による業務の中断時間が平均約 18 時間、業務効率の低下が 1 週間平均約 9 時間あったこと、これに加えブランド棄損・風評被害等があったことが報告されている。

15 2020 年 1 月から 6 月までの期間を対象とする調査である（Check Point, “Cyber Attack Trends: 2020 Mid-Year Report”（2020.7））。

撃の手口は近年さらに巧妙化しており、特にランサムウェアによる攻撃や新型コロナウイルス感染拡大に便乗した攻撃の増加が重要な特徴となっている（図表１参照）。

世界経済フォーラム（World Economic Forum：以下「WEF」）はグローバルアジェンダ[16]で Check Point の本調査を引用し、新型コロナウイルスの感染拡大に便乗したフィッシング[17]やランサムウェア等によるサイバー攻撃数が 2020 年 2 月までは週 5,000 件未満で推移していたが、4 月下旬には週 20 万件に激増したことを紹介している（図表 2 参照）。

このような状況を踏まえ、サイバーリスク軽減のための保険金支払機能とサイバーセキュリティの強化に寄与し事故防止に役立つ付帯サービス等を兼ね備えたサイバー保険の活用が検討される必要があるとされている[18]。

また、全米保険庁長官会議（National Association of Insurance Commissioners：以下「NAIC」）の直近の報告書[19]によると、2019 年の特徴として、個人情報の中でも健康診断や病歴情報等のセンシティブ情報の窃取を目的とする保険会社等へのサイバー攻撃が増加しているとされている。犯罪組織等が利用するダークウェブと呼ばれる闇サイトで、個人の健康診断・病歴情報等が有利に取引されている[20]ため、その種の情報を多く保有する保険会社や企業・団体等がサイバー攻撃を受けているとされている。

図表１　直近のサイバー攻撃の特徴・主な手口

特徴	概要
脅迫攻撃の巧妙化（二重脅迫等）	○攻撃側が、ランサムウェア攻撃によってデータを暗号化し、脅迫するだけでなく、暗号化前に大量のデータを盗取しておき、身代金要求に応じない場合には、情報漏えいさせると脅迫するという二重の脅迫を仕掛ける手法が増加している。
モバイルデバイス（注１）への攻撃	○攻撃側が、新たな感染経路として公式アプリストアに有害アプリを紛れこませ、モバイルデバイスを感染させるような高度な手法が増えた。 ○大手グローバル企業のモバイル管理システムに侵入し、管理下のモバイルデバイスの 75%以上にマルウェアを拡散させた手口も確認された。
クラウド（注２）サービスへの進入攻撃	○パンデミックによって多くの企業・組織等が利用することが増えたため、汎用クラウドサービスへ攻撃・侵入し、機密情報を盗取する手法が増加している。

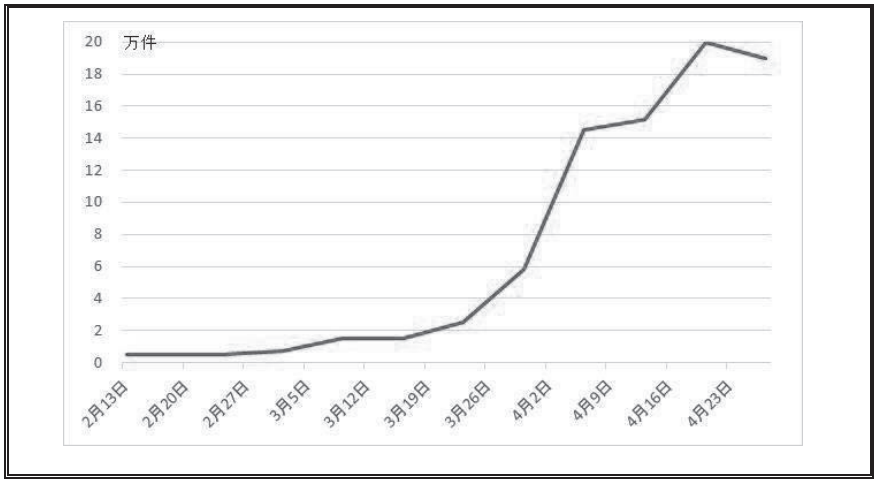
（注１） 持ち運び可能な電子機器端末の総称である。

（注２） ネットワークを介して遠隔から利用するシステムやデータベースを意味する。

（出典：Check Point, “Cyber Attack Trends: 2020 Mid-Year Report”（2020.7）をもとに作成）

16 地球規模の課題等を意味する（Moti Sagey, “Remote work carries massive cyber risks. These top IT tips can help keep your workers secure”（WEF, 2020.9））。
17 正規のメールやウェブサイトを装い、暗証番号やクレジットカード番号等を盗み取る詐欺手法を意味する。
18 WEF, “Cyberinsurance”（2020.11）ほか
19 NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）
20 ダークウェブと呼ばれる闇サイトで、クレジット情報は平均 5.4 ﾄﾞﾙ程度なのに対し、病歴情報は平均 250ﾄﾞﾙ程度で取引されていることが背景にあるとしている。

図表 2　2020 年新型コロナウイルスに便乗したサイバー攻撃数の推移



（出典：Check Point, “Cyber Attack Trends: 2020 Mid-Year Report”（2020.7）をもとに作成）

（2）ランサムウェア攻撃による被害の動向

近年、増加するランサムウェア攻撃による被害は、世界全体でサイバーインシデント数の 40%以上を占めるとされている[21]。2019 年には世界の企業・組織で 50 万件以上、身代金被害額だけで 63 億ﾄﾞﾙ以上が報告されており、その他の関連する被害を含めると被害総額は 1,000 億ﾄﾞﾙを超えている。これらの被害のうち、事業中断による被害が最も大きく、全体の 60%以上を占め、身代金要求額の 6 倍以上になると見込まれている。これは、被害に遭った企業が機密情報や様々なデータ、基幹系システムやその他のデバイスを使えなくなることで大規模な事業中断につながるためとされている。またシステム復旧費用は身代金と同額程度になるとされている。

情報セキュリティ専門会社である Acronis が実施した調査[22]によると、2020 年 7 月から 9 月において、新型のランサムウェアの一種である MAZE[23]がランサムウェア攻撃による被害の半数近くを占めており、金銭を目的とする二重脅迫の手口が悪質化・巧妙化する傾向が高まっていると指摘されている。

また、情報セキュリティ専門会社である Sophos がランサムウェア被害に遭った企業に対して実施した調査[24]によると、サイバー犯罪組織はランサムウェア攻撃に以前

---

[21] Allianz Global Corporate & Specialty, “Managing the Impact of Increasing Interconnectivity: Trends in Cyber Risk 2020”（2020.11）ほか

[22] Acronis は 2020 年 7 月から 9 月までを対象期間として自社のネットワークの 10 万以上のシステム端末から情報を収集して調査し、「世界におけるサイバーリスクの脅威」を公表している（Acronis, “Cyberthreats Report 2020”（2020.12））。

[23] 2019 年 5 月に初めて確認された最も悪質とされるランサムウェアの一種であり、情報の盗取、バックアップ情報の削除、情報の暗号化、身代金の要求、情報漏えいの脅迫というプロセスを一貫して行うとされている。

[24] ランサムウェアについて 26 か国 5,000 人の企業 IT 管理者を対象に 2020 年 1 月と 2 月に実施した調査である。企業・組織の規模は 50%が従業員 100 人から 1,000 人まで、50%が従業員 1,001 人から 5,000 人

よりも多くの労力が必要となったことから、標的数を絞るようになってきていると分析している（図表 3 参照）。また、企業の規模に関係なくサイバーセキュリティが脆弱で金銭を得やすいと思われる企業が狙われている。サイバー犯罪組織はランサムウェアによる身代金奪取等によって資金力を強化していることから、今後はより高度な戦術[25]で緻密に狙いを定めてサイバー攻撃を仕掛けることが予想されるとしている。

図表 3　ランサムウェア被害に関する調査結果の概要

項目	調査結果の概要
システム・情報の暗号化	○ランサムウェアに攻撃を受けた企業のうち、73%がシステムを暗号化された。
システムの復旧・回復状況	○システム・情報を暗号化された企業の 94%はシステムを復旧することができた。
自力による復旧・回復	○システム・情報を暗号化された企業のうち、56%がバックアップ情報等によってシステムを復旧することができた。
身代金支払による復旧・回復	○システム・情報を暗号化された企業の 26%が身代金を支払うことでシステムを復旧することができた。 ○ただし、システム・情報を暗号化された企業の 1%は身代金を支払ったにもかかわらず、復旧できなかった。
システム・情報の平均復旧費用	○身代金を支払った場合は、支払わない場合と比較して 2 倍の費用がかかることが判明した。 ○ランサムウェア対応の平均費用（ダウンタイムによる損失、人件費、デバイス費用、ネットワーク費用、逸失利益、身代金等）は以下のとおりである。 ・身代金を支払わなかった企業： 732,520 ﾄﾞﾙ ・身代金を支払った企業： 1,448,458 ﾄﾞﾙ
サイバー保険に対する理解	○サイバー保険に加入している企業は 84%であったが、このうちの 5 社に 1 社は契約内容を理解していない。 ○ランサムウェアを対象とする保険に加入している企業は、サイバー保険加入企業の 64%であった。
身代金の保険金支払	○ランサムウェアを対象とするサイバー保険に加入し、身代金を支払った企業の 94%は身代金を保険金として受け取った。

（出典：Sophos, “The State of Ransomware 2020”（2020.5）をもとに作成）

（3）新型コロナウイルス感染拡大に便乗するサイバーインシデントの動向

医療分野の研究開発機関や病院等の医療機関を対象とするサイバー攻撃が増えており、ワクチンや治療薬の開発への影響に加え、患者への医療行為を行うことができない等、経済損害以外にも深刻な影響が発生している[26]。国際刑事警察機構

までであり、公共団体と民間企業から匿名で回答を受領したとしている。また調査対象企業の 51%がランサムウェア攻撃を経験したと回答している（Sophos, “The State of Ransomware 2020”（2020.5））。

[25] サイバー犯罪組織の間で、分業による連携やランサムウェアの貸与・売買取引がされること、および AI 活用等が挙げられている。

[26] UN, “Cybercrime, UNODC COVID-19 Policy Documents”（2020.4）、ICRC, “Cyber attacks Statement”（2020.7）

（International Criminal Police Organization：ICPO）や欧州刑事警察機構（European Police Office：EUROPOL）は、様々なウェブ詐欺、新型コロナウイルス感染拡大に乗じた医療用品取引詐欺や個人情報窃取等の詐欺が増加しているとして警戒を呼び掛けている。具体的には、個人情報が盗取されて失業保険の不正請求が行われた事例、マスクと消毒液の取引の偽装でフランスの製薬会社が約 725 万ﾄﾞﾙをだまし取られた事例等が挙げられている[27]。

また、ソーシャルエンジニアリング攻撃と呼ばれる在宅勤務等の環境にある従業員の不安な心理を利用した攻撃が増加している。これにより、企業のネットワークに接続するためのパスワードやその他重要情報の窃取を目的とする、標的型フィッシング攻撃や悪意のあるウェブサイトへ誘導する攻撃等が大幅に増加したとされている。直接企業の管理下にない、個人所有の自宅コンピュータ等から企業のシステムへの接続が許可されていることに乗じて、サイバー犯罪組織がセキュリティの脆弱な個人を狙ったとされている[28]。

３．サイバー保険市場の動向

本項ではサイバー保険市場の動向について、世界全体の市場規模、および米国保険会社におけるサイバー保険の収支状況の順に説明する。

（1）世界全体の市場規模

経済協力開発機構（Organisation for Economic Co-operation and Development：以下「OECD」）によると、世界のサイバー保険市場の保険料規模は 2019 年時点でおよそ 40 億ﾄﾞﾙから 50 億ﾄﾞﾙとされている（図表 4 参照）。さらに、サイバーインシデントの増加、保険加入ニーズの増加を背景に、2020 年には 50 億ﾄﾞﾙを超える規模[29]に成長していると推計されている[30]。保険監督者国際機構（International Association of Insurance Supervisors：以下「IAIS」）は、サイバー保険市場は 2025 年には約 200 億ﾄﾞﾙ規模に拡大すると予測している[31]（図表 5 参照）。

保険ブローカーであるエーオンは、2019 年時点で米国のサイバー保険市場は全世界の約 70%を占める最大市場であり、今後も米国を中心に同市場が成長すると予測して

---

27 ICPO, “COVID-19 cyberthreats”、EUROPOL, “How Criminals Profit From The COVID-19 Pandemic”, “Internet Organized Crime Threat Assessment”、S&P Global Ratings, “Cyber Risk In A New Era: Insurers Can Be Part Of The Solution”（2020.9）ほか

28 Check Point, “Cyber Attack Trends: 2020 Mid-Year Report”（2020.7）

29 米国では約 42 億ﾄﾞﾙ、欧州では約 6.5 億ﾄﾞﾙ、アジア（豪州を含む）では約 4.5 億ﾄﾞﾙと推計されている。

30 IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12）、NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）

31 IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12）

いる[32]。

一方、保険ブローカーであるマーシュ・アンド・マクレナン等によると、欧州およびアジア大洋州においてもサイバー保険市場は 2016 年から 2018 年にかけて大きく成長している。その理由としては、欧州において 2018 年に一般データ保護規則（General Data Protection Regulation：GDPR）[33]が施行されたこと、アジア大洋州においても同様のルール策定の動きがあることが指摘されている。加えて、サイバーインシデントの増加によって、サイバーリスク対策への関心が高まったこと等によるものとされている[34]。同時にサイバーインシデントの増加によってサイバー保険の損害率が悪化したことなどからサイバー保険料率が引上げられたことも影響しているとされている[35]。

2020 年以降は新型コロナウイルス感染拡大という特殊事情、十分なサイバーセキュリティ対策や準備がないまま在宅勤務等へ移行するなど労働環境・IT システム環境の大規模な変化が生じることによって、サイバーインシデントの脅威が広がっていることから、サイバー保険市場はより急速に成長する可能性があるとされている[36]。

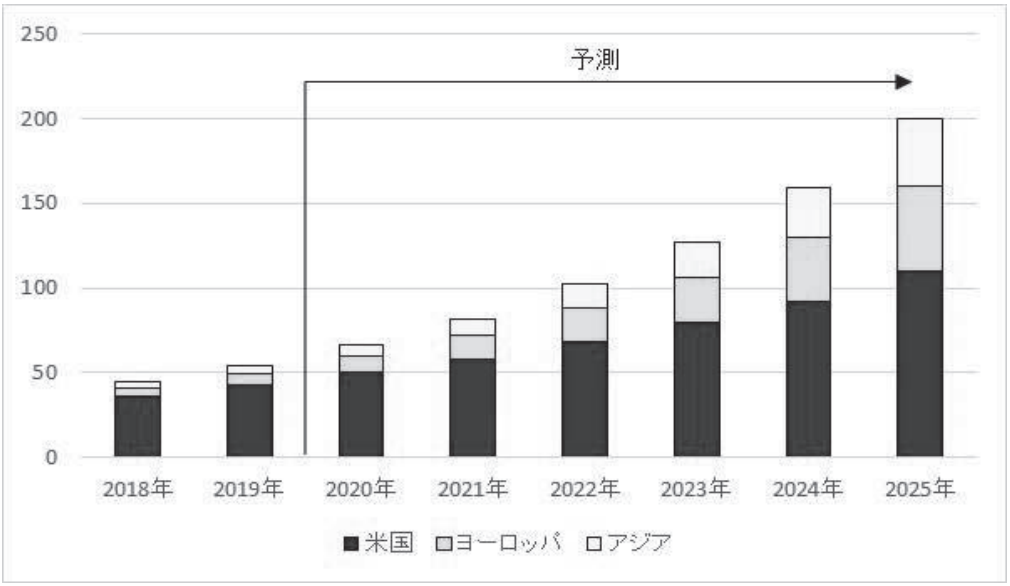
図表 4　世界のサイバー保険市場の地域別の総収入保険料（推計）

地域	2016 年		2018 年	
	総収入保険料	シェア	総収入保険料	シェア
米国	約 25 億ﾄﾞﾙ～30 億ﾄﾞﾙ	85%～90%	約 32 億ﾄﾞﾙ	70%～80%
欧州	約 1.5 億ﾄﾞﾙ～4 億ﾄﾞﾙ	5%～9%	約 5 億ﾄﾞﾙ～10 億ﾄﾞﾙ	10%～20%
アジア大洋州	約 0.5 億ﾄﾞﾙ程度	1%～2%	約 2.5 億ﾄﾞﾙ～5 億ﾄﾞﾙ	5%～10%
世界全体	約 25 億ﾄﾞﾙ～35 億ﾄﾞﾙ	100%	約 40 億ﾄﾞﾙ～50 億ﾄﾞﾙ	100%

（出典：OECD, “Enhancing the Role of Insurance in Cyber Risk Management”（2017.12）、“Encouraging Clarity In Cyber Insurance”（2020.2）、NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）をもとに作成）

[32] Aon, “US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance”（2020.6）
[33] 個人情報および個人情報所有者の権利の保護を目的とした法規制であり、個人情報の取扱に関して厳しい義務を課している。
[34] Aon, “Cyber Insurance Market Insights”（2020.10）、“Cyber Insurance Market Update”（2020.6）
[35] Marsh, “Global Insurance Market Index”（2020.11）ほか
[36] 在宅勤務等の際の従業員の個人所有コンピュータ等を介して機密情報を奪う、または企業ネットワークへ侵入するサイバー攻撃が大幅に増加している（IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12））。

図表 5　世界のサイバー保険市場の成長予測　（単位：億ﾄﾞﾙ）



（出典：IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12）をもとに作成）

（2）米国保険会社におけるサイバー保険の収支状況

a. 保険料の状況

NAIC の報告書[37]によると、米国の 2019 年におけるサイバー保険の保険料収入は前年比ほぼ横ばいであったとされている（図表 6 参照）。ただし、2019 年の認可保険会社[38]の元受収入保険料は単独型サイバー保険（以下「単独型」）[39]、特約型サイバー保険（以下「特約型」）の合計約 22 億 6,200 万ﾄﾞﾙとなっており、前年対比約 2 億 3,000 万ﾄﾞﾙ（11.4%）増加している。現在中小企業の加入率はおよそ 50%とされているが、サイバーインシデントの増加やサイバーリスクの認識の高まり等を背景に、今後サイバー保険の加入ニーズはさらに高まるものと予想されている。

一方、大手保険会社の元受収入保険料に占めるサイバー保険の割合は、AIG、チャブで 2%以下、トラベラーズ、リバティミューチュアル、チューリッヒ保険で 1%以下となっており、まだまだ極めて低い状況にある。また、単独型の元受収入保険料は上位 10 社でおよそ 80%、15 社でおよそ 87%を占める状況にある（図表 7 参照）。

---

37 NAIC が認可保険会社およびサープラスライン保険会社からの報告に基づき集計した（NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12））。

38 米国では、各州の認可保険会社のほかに、認可保険会社が引き受けないリスクの高い契約や特殊なリスク等の契約を州外から引き受けるサープラスライン保険会社がある。

39 NAIC の報告書では、サイバー保険は、主としてサイバーリスクを対象とする「単独型サイバー保険」と、財産保険や賠償責任保険など従来型の保険にサイバーリスクの補償を特約付帯した「特約型サイバー保険」に分類されている。

図表 6　米国におけるサイバー保険元受収入保険料の規模　（単位：百万ﾄﾞﾙ）

年	認可保険会社		サープラスライン保険会社		合計	
	保険料	増減率	保険料	増減率	保険料	増減率
2015 年	1,416	-	-	-	1,416	-
2016 年	1,675	18.3%	709	-	2,383	68.3%
2017 年	1,891	12.9%	1,197	68.9%	3,087	29.5%
2018 年	2,029	7.3%	1,128	−5.8%	3,157	2.2%
2019 年	2,262	11.4%	888	−21.3% (注)	3,150	−0.2%

（注）NAIC は 2019 年のサープラスライン保険会社の保険料減少の要因を報告受領時点で特定できていないとしている。

（出典：NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）をもとに作成）

図表 7　米国におけるサイバー保険（単独型）元受収入保険料上位 15 社（2019 年）　（単位：百万ﾄﾞﾙ）

保険会社グループ	元受収入保険料	市場シェア	損害率
アクサ	230	18.2%	65.7%
AIG	226	17.9%	55.4%
トラベラーズ	144	11.4%	34.1%
Beazley	142	11.2%	21.3%
Fairfax	65	5.1%	51.6%
Axis Capital	50	3.9%	11.8%
Bcs	45	3.5%	39.7%
チューリッヒ	44	3.5%	86.9%
Tokio Marine	35	2.8%	19.0%
リバティ	30	2.3%	49.8%
Sompo	23	1.8%	35.7%
Apollo Global	19	1.5%	0.9%
WR Berkley	17	1.4%	2.8%
CNA	16	1.3%	33.0%
アリアンツ	15	1.2%	0.0%
合計	1,100	87.0%	-

（出典：NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）をもとに作成）

b. 保険金支払の状況

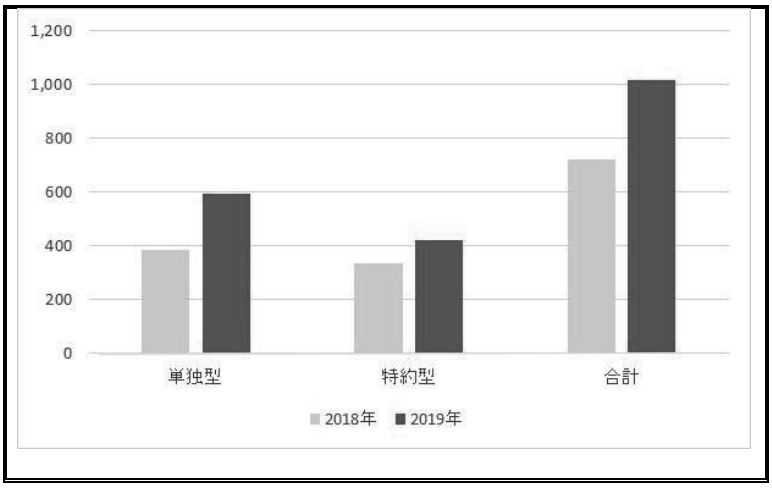
NAIC およびエーオンの公開情報[40]によると、米国保険会社のサイバー保険における事故件数と支払保険金はこのところいずれも増加している。認可保険会社におけるサイバー保険の保険金支払の状況[41]は、単独型が約 6 億ﾄﾞﾙで前年比約 55%増加、特約型が約 4 億ﾄﾞﾙで前年比約 25%増加となり、合計約 10 億ﾄﾞﾙで前年比約 41%増加とな

[40] NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）、Aon, “US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance”（2020.6）

[41] 保険金支払に関しては認可保険会社の情報のみが公開されている。

っている（図表 8 参照）。

図表 8　米国保険会社の保険金支払状況　　（単位：百万ﾄﾞﾙ）



（出典：NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）、Aon, “US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance”（2020.6）ほかをもとに作成）

（a）企業・組織の規模別の状況

サイバーリスクを専門とする情報提供会社である NetDiligence が集計した 2019 年における保険会社[42]の保険金支払情報[43]によると、企業の事業規模別では、年間売上が 20 億ﾄﾞﾙ未満の中小企業が保険金支払件数の 98%を占め、残り 2%が年間売上 20 億ﾄﾞﾙ以上の大企業であるとされている[44]。

一方、NetDiligence が集計した 2019 年におけるサイバーインシデントによる損害額約 1 億 9,500 万ﾄﾞﾙの内訳は、中小企業が約 49%、大企業が約 51%という割合になっている。企業・組織の規模が大きいほど、1 件あたりの平均損害額も大きくなっている（図表 9 参照）。

特にランサムウェアによるサイバー攻撃の平均損害額が大きくなっており、例えば、中小企業の平均損害額は 2018 年の約 4 万 7,000ﾄﾞﾙから 2019 年には約 17 万 5,000ﾄﾞﾙにまで増加している[45]（図表 10 参照）。

---

[42] アクサ XL、Beazley、Berkley Cyber Risk、CFC Underwriting、チャブ、Great American Insurance、Hiscox、Markel、Philadelphia Insurance Companies、QBE、Sompo International、Swiss Re、Tokio Marine HCC、トラベラーズ、および United States Liability Insurance の 15 社の提供情報としている。

[43] NetDiligence は、2015 年から 2019 年までの 3,597 件の保険金支払に基づいて分析しているとし、このうち 869 件は 2019 年の保険金支払であるとしている。

[44] NetDiligence, “Cyber Claims Study 2020 Report”（2020.10）

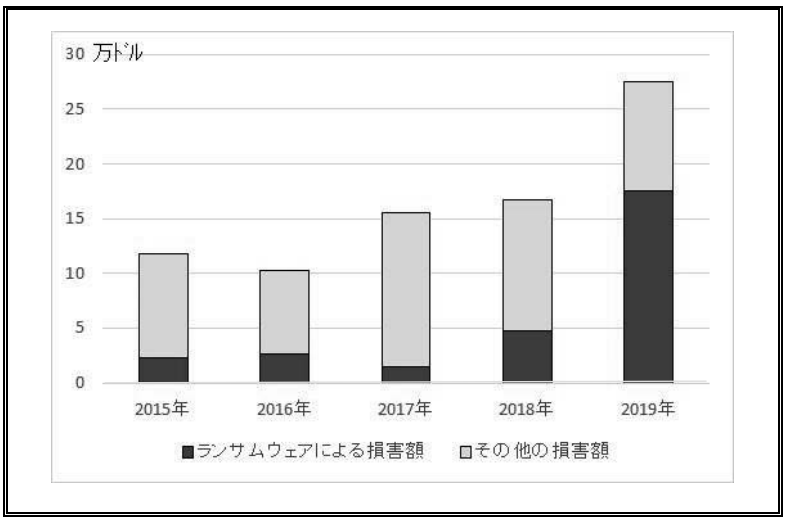
[45] S&P グローバルも複数の保険会社からの情報として、ランサムウェア攻撃による保険金支払が 2019 年は前年比およそ 2 倍から 3 倍の規模に増加しており、この傾向は 2021 年も続くとしている（S&P Global Market Intelligence, “Cyber insurers tighten underwriting, raise prices as ransomware wave hits”

図表 9　企業・組織の規模別の保険金支払件数と平均損害額

企業・組織規模		保険金支払件数	平均損害額
中小企業	年間売上 5,000 万ﾄﾞﾙ未満	1,590	9.1 万ﾄﾞﾙ
	年間売上 5,000 万ﾄﾞﾙ以上 3 億ﾄﾞﾙ未満	594	17.3 万ﾄﾞﾙ
	年間売上 3 億ﾄﾞﾙ以上 20 億ﾄﾞﾙ未満	199	35.9 万ﾄﾞﾙ
	不明	970	2.1 万ﾄﾞﾙ
大企業	年間売上 20 億ﾄﾞﾙ以上 100 億ﾄﾞﾙ未満	28	360 万ﾄﾞﾙ
	年間売上 100 億ﾄﾞﾙ以上 1,000 億ﾄﾞﾙ未満	15	2,030 万ﾄﾞﾙ
	年間売上 5,000 万ﾄﾞﾙ以上 3 億ﾄﾞﾙ未満	3	2,330 万ﾄﾞﾙ

（出典：NetDiligence, “Cyber Claims Study 2020 Report”（2020.10）をもとに作成）

図表 10　中小企業における平均損害額の推移



（出典：NetDiligence, “Cyber Claims Study 2020 Report”（2020.10）をもとに作成）

（b）企業・組織の業種別の状況

中小企業における 2019 年のサイバー保険の保険金支払件数の業種別構成割合では、医療 29%、専門サービス[46]20%、製造 8%の順となっている。また、大企業においては、金融サービス 50%、医療 22%、テクノロジー[47]7%の順となっており、金融サービスの割合が大きい。医療、専門サービス、小売、製造、金融サービスの 5 業種が全体に占める割合は、中小企業の約 70%、大企業でも約 80%となっている（図表 11、12 参照）。

これは、医療や専門サービス、小売、金融サービスといった業種が個人情報やセンシティブ情報を多く保有していることもあり、多く狙われたものと考えられる。

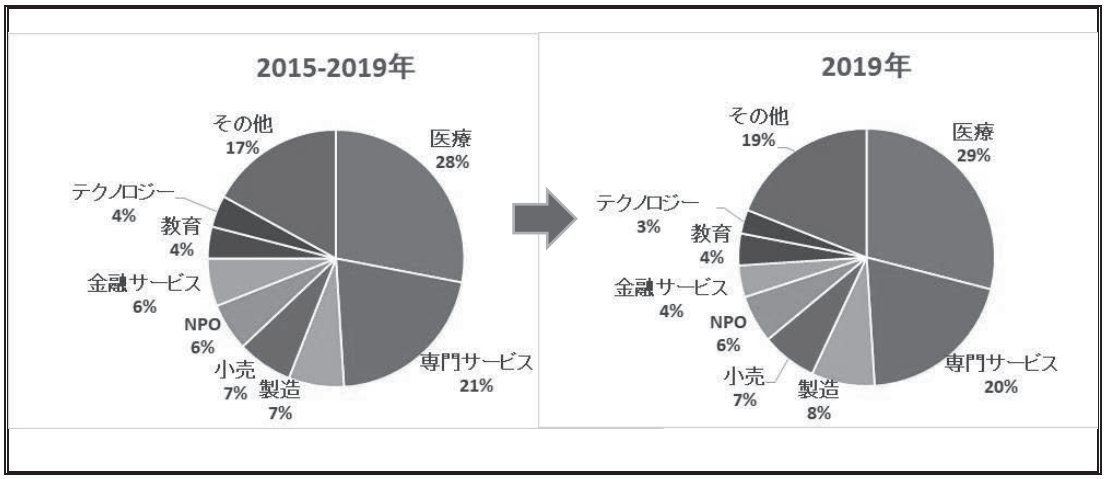
（2020.10））。

[46] 法律事務所、建築設計事務所、設備管理会社、警備会社等の専門サービス事業者を意味する。機密情報等を多く持つ、または高層ビル・大型商業施設・原子力発電所・ダム等の重要施設の管理・使用を行っているために狙われる可能性が高いとされている。

[47] 科学・技術に関係する業種を意味する。

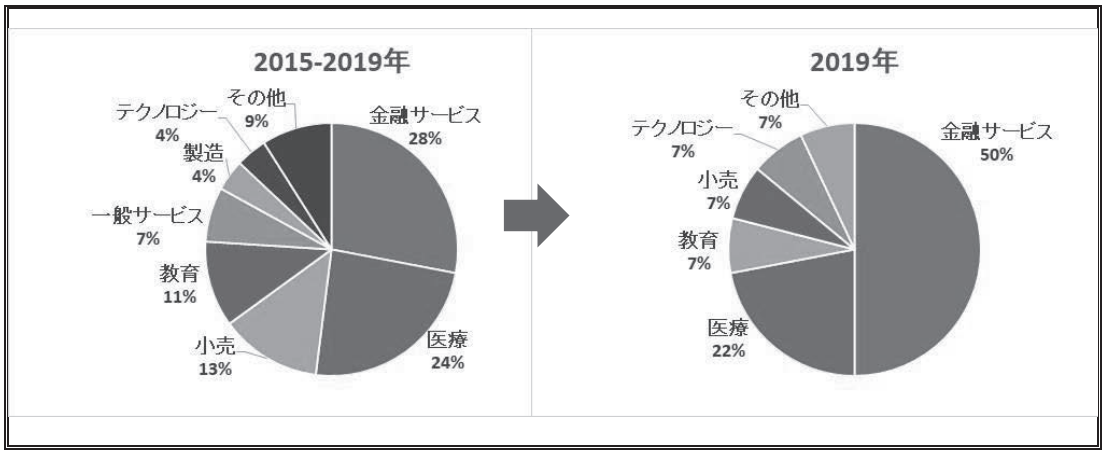
特に医療業界が狙われるのは、人命にかかわる医療行為は緊急性が高く、かつセンシティブ情報を多く保有していること等から身代金支払につながりやすいためと考えられている。

図表 11　中小企業の業種別の保険金支払件数割合



（出典：NetDiligence, “Cyber Claims Study 2020 Report”（2020.10）をもとに作成）

図表 12　大企業の業種別の保険金支払件数割合



（出典：NetDiligence, “Cyber Claims Study 2020 Report”（2020.10）をもとに作成）

c. 損害率・コンバインドレシオの状況

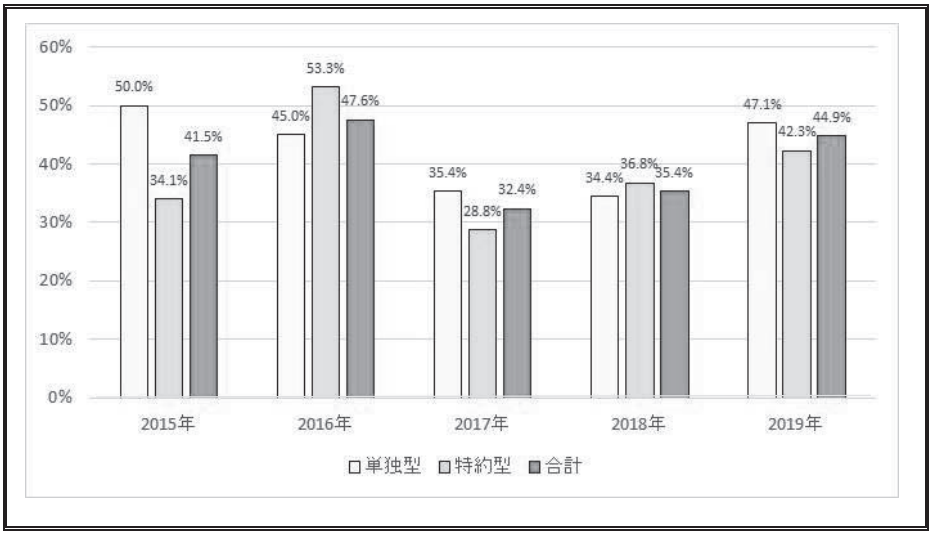
米国の認可保険会社のサイバー保険の損害率は 2019 年に単独型 47.1%、特約型 42.3%、合計 44.9%となっており、前年比 9.5%上昇している（図表 13 参照）。損害率上昇の主な要因は、保険料の増加以上に保険事故件数が増加したためとされており、2018 年に 0.42%であった事故率[48]が 2019 年には 0.56%に上昇し、1.3 倍以上に

48 契約件数における事故発生割合（事故件数／契約件数）を意味する。

なっている[49]。2019 年は特にランサムウェアを原因とする保険金支払が事業者の規模や業態にかかわらず増加したこと[50]、健康管理・病歴等に関する個人情報の盗取を原因とする保険金支払が増加したこと等が背景にあるとされている。

損害率に事業費率を加えたコンバインドレシオを見てみると、2019 年は単独型 76.2%、特約型 71.9%、合計 74.5%となっている。損害率の上昇に伴いコンバインドレシオも前年比 9.2%上昇し、サイバー保険の収益性は悪化している。ただし、サイバー保険以外の損害保険種目との比較においては、依然として収益性の高い良好な水準にとどまっているとされている[51]（図表 14 参照）。

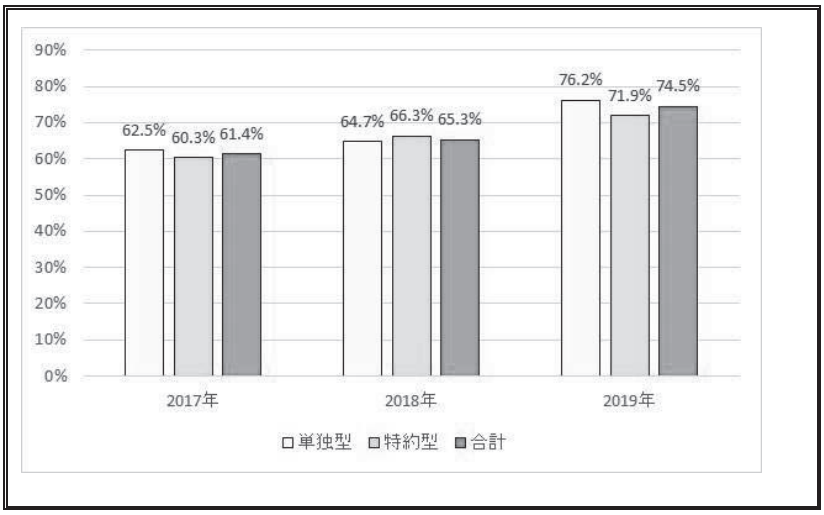
図表 13　米国認可保険会社のサイバー保険損害率推移



（出典：Aon, “US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance”（2020.6）をもとに作成）

[49] Aon, “US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance”（2020.6）
[50] NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）
[51] Aon, “US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance”（2020.6）

図表 14　米国認可保険会社のサイバー保険コンバインドレシオ推移



（出典：Aon, “US Cyber Market Update: 2019”、“US Cyber Insurance Profits and Performance”（2020.6）をもとに作成）

d. 引受条件見直し等の状況

サイバー保険の引受を行っている多くの保険会社は、ランサムウェアによる保険金支払が急増していることから保険料率の引上げを進めている。元受収入保険料に占めるサイバー保険の割合が比較的高い保険会社である Beazley によると、直近では 15%から 25%の料率の引上げが一般的となっており、このような状況が 2021 年も続くとしている。また、引受限度額の引下げやサブリミットの設定、免責金額の引上げ等を含め、引受基準を厳格化する保険会社も多い。保険会社がサイバー保険の引受判断を行うために、企業のサイバーセキュリティやリスク管理に関し多くの質問を行うことや、情報セキュリティ専門会社等と連携して企業のサイバーセキュリティ上の脆弱性の把握に努めることも多くなったとされている[52]。

4．その他の動向

本項では、直近の特徴的な変化等として、サイバー保険市場へのインシュアテック企業の参入、サイレント・サイバーリスクへの対応、ならびに再保険市場と保険リンク証券（Insurance-Linked Securities：ILS）発行の動きについて説明する。

（1）サイバー保険市場へのインシュアテック企業の参入

本項では、サイバー保険市場に参入した主なインシュアテック企業の事例として、Coalition、At-Bay 等の特徴について紹介する。

[52] S&P Global Market Intelligence, “Cyber insurers tighten underwriting, raise prices as ransomware wave hits”（2020.10）

a. Coalition

ランサムウェア被害の増大を背景に、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 Coalition は、カリフォルニア州サンフランシスコに本社を置き、保険代理店としてサイバー保険を販売している。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、自社の技術を利用して積極的に事業展開しており、取扱保険料を 2019 年の約 5,000 万ﾄﾞﾙから 2020 年秋までに約 1 億ﾄﾞﾙへと大幅に拡大し、保険契約者も約 2 万 7,000 社にまで増大させている。保険契約者層は中小企業のほか、教会、農業従事者、ゴルフリゾート、各種ベンチャーキャピタル等が多いとしている[53]。

既存大手保険会社の保険商品と差別化を図るため、Coalition はサイバー保険の販売に際し保険契約者からの告知ではなく、保険契約者のデバイスをスキャン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。具体的には、保険契約者のデバイスを週に 6 万 5,000 回スキャン調査するなど、サイバーインシデントの予防対策を実施している。スキャン調査によってシステム上のセキュリティ不備を見つけた場合は、修正・代替手段確保等のコンサルティングを行い、サイバーリスクの軽減を図るとしている。また、リスク評価の結果、リスクが一定の基準を超えている場合は引受謝絶するとしている。

Coalition は、保険契約者に対し、サイバーインシデントの予防としてサイバーリスクを管理・軽減するための無料ツールと、サイバーインシデントによる被害発生後の業務復旧を支援するためのサイバー保険を組み合わせて提供している。サイバーインシデントによって被害が発生した場合には、専門家チームが 24 時間 365 日体制で対応するとしており、専門知識を持つ広報・法務・危機管理の専門家と連携してネットワーク・システム・業務の迅速な復旧を支援する。Coalition は、引受判断だけではなく、保険契約者のサイバーリスク軽減対策に自ら介入し、サイバーリスクが軽減されていることを確認し、監視を継続することで一般的なサイバー保険よりも幅広い補償の提供が可能となるとしている（図表 15 参照）。また、Coalition は、サイバーセキュリティは国境がない世界的な問題であるとして、2020 年 5 月にはカナダにも進出している。

[53] Jeff Kauflin, “Ransomware Has Catapulted This Insurtech Startup To $100 Million In Revenue”（Forbes, 2020.11）、Coalition ウェブサイトほか

図表 15　Coalition の主要補償項目と一般的なサイバー保険との比較 (注)

補償項目	一般的なサイバー保険	Coalition の補償
サーバー等への侵入・侵害対応費用	○	○
デジタル資産の復元費用	○	
危機管理・広報対応	○	
事業継続追加費用	×	
構外利益・構外事業中断損害	×	
ネットワーク・情報上の賠償責任	○	
規制対応・法的防御費用・罰金	○	
コンテンツの賠償責任	○	
資金移動詐欺損害	△	
サイバー恐喝損害	△	
システムの交換入替費用	×	
システムのアップグレード費用	×	
人身傷害・財産損害	×	
公害・汚染対応費用	△	
レピュテーション回復対応費用	△	
個人所有デバイスに起因する損害	×	
フリーアプリ等に起因する損害	△	

（注）○：補償対象、△：補償対象となる場合がある、×：補償対象外。

（出典：Coalition のウェブサイトをもとに作成）

b. At-Bay

At-Bay は 2016 年に設立され、カリフォルニア州マウンテンビューに本社を置き、インシュアテック企業として米国のサイバー保険市場に参入した。実際の保険引受は保険会社である Hartford Steam Boiler Inspection and Insurance が行っており、At-Bay は支払限度額 1,000 万ﾄﾞﾙまでの保険代理店として、サイバー保険をインターネットやブローカーを介して販売している。保険事業拡大のために 2020 年 12 月にマイクロソフトのベンチャーファンド、ミュンヘン再保険ベンチャーズ、および情報セキュリティ専門会社のチェックポイント社とイスラエル企業のジョイントベンチャー企業等から 3,400 万ﾄﾞﾙの資金調達を行った。At-Bay は中小企業を対象にサイバー保険の販売を行っており、保険契約者のネットワーク等を継続して監視することでサイバーセキュリティ上の問題点の警告やコンサルティングを行うとしている[54]。

保険契約者のサイバーセキュリティ上の問題点を積極的に洗い出し、改善のための指摘・提案を行うこと等により、保険契約者のネットワークへの侵入や情報漏えいを予防し、他社との差別化を図っている。また、独自の保険契約者向け提供ツールとして、セキュリティスコア算定機、および情報漏えい費用算定機という 2 種類のツールを用意しており、これらはサイバーインシデントの予防に役立っているとしている（図表 16 参照）。

[54] Zack Whittaker, “Cyber insurance startup At-Bay raises $34M Series C, adds M12 as a new investor”（TechCrunch News, 2020.12.8）、At-Bay ウェブサイトほか

図表 16　保険契約者向けツール

ツール	機能
セキュリティスコア算定機	○保険契約者のサイバーセキュリティを評価し、スコア化してレポートを作成するためのツールである。 ○リスク軽減のための検討にも利用することができる。
情報漏えい費用算定機	○情報漏えいに関し、保険契約者である企業の経営者・リスクマネージャー等に、保険契約者ごとの環境や管理状況に応じた損害シナリオの想定から潜在的な財務への影響等を計算し、理解してもらうためのツールである。

（出典：At-Bay のウェブサイトをもとに作成）

c. その他の新規参入企業等

その他の代表的な新規参入企業としては Corvus や Slice labs 等が挙げられる。

Corvus は、マサチューセッツ州ボストンに本社を置き、2017 年 1 月から事業展開している。実際のサイバー保険の引受は保険会社である Hudson Insurance Group が行っており、Corvus は支払限度額 100 万ﾄﾞﾙまでの保険代理店としてサイバー保険を販売している。企業向けに加入手続がシンプルなスマートサイバー保険等のスマート保険シリーズをインターネット上で販売している[55]。

Slice labs はニューヨークに本社を置き、2016 年にミュンヘン再保険会社等から出資を受け、事業を開始した。実際の保険引受は主にアクサが行っており、保険代理店として保険クラウドサービスというプラットフォームを利用し、中小企業向けにオンデマンド・テーラーメイド型のサイバー保険を販売している。顧客企業は、インターネット上で自社の URL、所在地、業種、年間売上高、従業員数を入力すると簡単に保険料見積を受領できる[56]。

また直近の新規参入の例では、カリフォルニア州サンフランシスコに本社を置き、2020 年 11 月に事業を開始した Resilience が挙げられる。保険会社等への出資の実績がある Intact Ventures[57]によって設立された。実際の保険引受は主に Homeland Insurance が行い、Resilience は保険代理店として保険契約者のリスクを軽減する特許取得済みの分析技術に基づくサイバーセキュリティツールとともにサイバー保険を選ばれたブローカーを介して中小企業向けに提供するとしている。

（2）サイレント・サイバーリスクへの対応

サイレント・サイバーリスク[58]は、保険商品の設計段階では考慮されなかったリス

---

[55] Anthony R. O'Donnell, "Corvus Insurance Launches Automated Ransomware/Business Interruption Cost Calculator"（Insurance Innovation Reporter, 2020.4）

[56] CBInsights, "Slice Labs" Information（2020.12）

[57] インターネットダイレクト販売を中心に保険展開する Intact Insurance Specialty Solutions を傘下に持つ投資会社である。

[58] サイレント・サイバーリスクに関しては、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）、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）をあわせて参照願う。

クであり、財産保険や賠償責任保険などの従来型の損害保険商品の約款において明確に免責とされていない[59]ことから、補償の対象とみなされる可能性がある。そのため、保険会社にとって、引受リスク量の正確な把握や収支管理等を行うためには、主に各保険商品からサイレント・サイバーリスクを除外する、サイレント・サイバーリスクが約款上免責であることを明確にする、保険契約者に対して明確で適正な商品・サービスを提供する等の取組が課題とされている[60]。

a. 欧米の監督当局・団体等における対応

サイレント・サイバーリスクに関する課題について、イギリスの保険監督当局である健全性監督機構（Prudential Regulatory Authority：以下「PRA」）が 2019 年に通達を発信して以降、各国・各地域の監督当局および団体、保険会社で対応がなされている（図表 17 参照）。

これらを契機に 2019 年から 2021 年にかけて、世界の保険会社は従来型の損害保険商品においてサイバーリスクのエクスポージャーを特定し明確化する対応、またはサイバーリスクを明確に免責にする対応等の実施が求められることとなった[61]。

[59] IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12）

[60] OECD, “Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation”（2020.10）

[61] 多くの保険会社にとって、従来型の損害保険商品においてサイバーリスクのエクスポージャーを特定し定量化することは事実上困難であるため、従来型の損害保険商品からサイバーリスクを明確に免責とする方法が現実的とされている。

図表 17　欧米の主な監督当局・団体等の対応

当局・機関・団体等	対応状況
PRA	○2019 年 1 月にサイバーリスクを管理するための活動計画の策定についての通達を発信した。
欧州保険年金監督機構（European Insurance and Occupational Pensions Authority：EIOPA）	○2019 年 9 月に「保険会社のためのサイバーリスク引受上の課題と機会」を公表した。 ○2019 年 12 月に「金融安定化報告」を公表した。 ○いずれもサイバーリスクの引受方針の中で、サイレント・サイバーリスクについて、保険会社はタスクフォースチームを設置し、従来の保険種目におけるサイレント・サイバーリスクを含むサイバーリスク、エクスポージャーを分析し、サイバーリスクの免責の明確化、あるいは現実的な災害発生シナリオに基づくリスク評価を行い、サイバーリスクの明確な把握とその極小化を行う等の解決策を策定するよう言及した。
ロイズ保険市場協会（Lloyd's Market Association）	○2019 年 7 月にロイズ保険市場協会が市場通達 Y5258 を発信し、再保険の出再・受再のためにすべてのシンジケートがすべての保険契約におけるサイバーリスクのエクスポージャーを正確に把握の上、再保険者および保険契約者等へ明確に通知すること等が必要であるとした。 ○2020 年 1 月に市場通達 Y5258 のフォローの位置づけで市場通達 Y5277 を発信した。
OECD	○2020 年 2 月に「サイバー保険の適用範囲の明確化の促進・公共政策と規制の役割」を公表した。 ○サイバー保険の適用範囲における明確性の促進が必要であるとした。
欧州・米国保険対話プロジェクト（EU-US Insurance Dialogue Project）(注)	○2018 年の欧州・米国保険対話プロジェクトにおいて 2017 年から 2019 年までの取組の中で重要議題として取り上げられた。 ○2020 年 2 月にサイバー保険ワークグループでフォローアップ議論がなされている。
NAIC	○各州の監督当局が各認可保険会社に対し、引受を行っているサイバーリスクの情報について年次報告書を通じ明確に報告するよう求めていることを NAIC は 2019 年 9 月に公表している。
IAIS	○2020 年 12 月に「持続可能な保険市場発展のためのサイバーリスク引受上の課題および監督上の考慮事項の明確化」を公表した。 ○2021 年から 2024 年の戦略計画で、サイバー保険市場の拡大の中でサイレント・サイバーリスク対応を注視していくとしている。

（注）欧州連合（European Union：EU）および米国の関係機関が、保険の規制および監督等について相互に理解と協力を深めることを目的として 2012 年 1 月に開始されたプロジェクトである。

（出典：NAIC, "Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement"（2019.9）、EU-US Insurance Dialogue Project, "The Cyber Insurance Marketworking Group Summary Report"（2020.2）、OECD, "Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation"（2020.10）、および IAIS, "Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development"（2020.12）ほかをもとに作成）

b. 欧米の保険会社等における対応

ロンドン国際保険引受協会（International Underwriting Association of London）

[62]やロイズ市場協会（Lloyd's Market Association）等の業界団体や再保険会社等は、保険会社がサイバーリスクを従来型の損害保険商品において明確に免責とするためのモデル免責条項等を公表している。例えば、ロイズ保険市場協会は、2019 年 11 月に免責条項についてノンマリン種目用 2 種類およびマリン種目用 2 種類の合計 4 種類を公表した（図表 18 参照）。その後も各種目にあわせた形態のモデル免責条項・特約条項が 20 種類以上公表されている。また同協会以外にも各国・各地域の団体等がモデル免責条項・特約条項等を公表している。

これらモデル免責条項に基づき、世界の保険会社がサイレント・サイバーリスクの約款上の免責の明確化等の対応を、2019 年から 2020 年にかけて進めてきたとされている。主な保険会社は 2020 年までに対応を完了したとしている[63]（図表 19 参照）。

図表 18　ロイズ保険市場協会のノンマリン種目用モデル免責条項（2 種類）の概要（注１）

条項項目	LMA5400	LMA5401
電子機器へのアクセスまたは使用による不正、悪意または犯罪行為に関連した損失や損害	×	×
サイバーインシデントに起因する電子機器へのアクセスや使用によるエラーや不作為に関連した損失や損害	×	×
サイバーインシデントに起因する電子機器へのアクセスや使用ができない、またはできなかったことに関連した損失や損害	×	×
データの使用不能または機能低下による損失や損害	×	×
データの交換・復旧	×	×
データの金銭評価上の損害	×	×
サイバーインシデントに起因する火災・爆発による物的損害の補償	○（注２）	×
サイバーインシデントに起因する火災・爆発による事業中断損害の補償	×	×
補償される損害により電子機器が使用不能、機能不全になった場合の物的損害または事業中断損害の補償	×	×

（注１）○：有責、×：免責

（注２）ただし他の免責条項が優先される場合がある。

（出典：Lloyd's Market Association "LMA5400 Cyber and Data endorsements"（2019.11）をもとに作成）

図表 19　欧米の保険会社のサイレント・サイバーリスクに係る約款対応状況

保険会社	対応状況
アリアンツ	2019 年契約更改の際に全契約につき対応を完了した。
AIG	2020 年 1 月までに企業向けのすべての財産保険、および賠償責任保険で対応完了した。
チューリッヒ	2019 年から開始し 2020 年までに対応を完了した。
FM グローバル	2019 年 7 月に企業向け財産保険の約款改定を実施し、対応を完了した。

[62] ロンドンマーケット（除くロイズ）における保険会社の業界団体である。会員保険会社の事業の発展に資する各種取組を行っている。

[63] Stuart Collins, "Commercial Risk News"（2019.11）、IAIS, "Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development"（2020.12）

（出典：Stuart Collins, “Commercial Risk News”（2019.11）、IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12）をもとに作成）

（3）再保険市場と保険リンク証券（ILS）発行の動き

スイス再保険によると、従来の保険種目で元受保険会社が出再割合を 10%から15%程度としている場合でも、サイバー保険の場合は 40%程度出再しており、特に単独型の場合は 95%程度出再していると推定されている[64]。また同社は、「現在サイバー保険の再保険市場の引受キャパシティは 15 億ﾄﾞﾙ程度であり、同キャパシティは再保険会社上位 10 社によって引き受けられている。同キャパシティは全世界のサイバー保険引受の 50%に過ぎず、万一、巨大なサイバー保険事故が発生した場合にはさらに同キャパシティが小さくなることが懸念される。」と指摘している。

再保険市場以外のサイバーリスクの移転手段に関しては、S&P グローバルとエーオン[65]が、従来の保険市場を通さず、資本市場の投資家にリスクを直接移転することが可能である保険リンク証券（Insurance-Linked Securities：以下「ILS」）[66]があり、解決すべき課題は多いものの、利用できる可能性は高いと述べている。

既に 2020 年 11 月の段階で、エーオンが Hudson Structured Capital Management Limited（以下「HSCM」）[67]と協力して、サイバーリスクの引受キャパシティを拡大するために、大規模なサイバー保険事故に対応する ILS の開発を実現したと報じられている。この新たな仕組によって、ランサムウェア等の各種マルウェアによるサイバー攻撃等によるシステムの破壊やネットワーク中断、クラウド中断等の大規模なサイバー保険事故が発生した場合に最大 7,000 万ﾄﾞﾙまで補償され、元受保険会社および再保険会社の損害を軽減することが可能となるとしている[68]。さらに HSCM は、エーオンのサイバー分析チームの独自のモデルを利用し、ILS におけるサイバーリスクの移転に適したプラットフォームを開発した[69]。

このように、サイバー保険市場の拡大にあわせて ILS の利用が活発化するきっかけとなる可能性があるとされている。

---

64 Swiss Re, “Could cyber risk be a growth engine for reinsurance?”（2019.8）

65 Ben Dyson, “Cyber insurance-linked securities will come ‘sooner than later’”（S&P Market Intelligence, 2019.9）、（Aon, “Insurance-Linked Securities”（2018.9））。

66 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。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。

67 バミューダに拠点を置く投資会社である。

68 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。

69 Aon, “Aon secures $70 million alternative capital capacity led by HSCM to transfer systemic cyber risk”（2020.11）ほか

５．おわりに

本稿では米国を中心とするサイバー保険市場の動向等を見てきた。NAIC および保険ヨーロッパ（Insurance Europe）は、サイバー保険の機能について、サイバーレジリエンスの観点から保険業界・保険会社の役割は単なる保険提供にとどまるのではなく、企業等がサイバー攻撃やサイバーインシデント被害から迅速に回復できるよう事業継続の支援を行うことや個人・企業等がサイバーリスクを十分理解できるようにするための支援を行うことが重要であるとしている[70]。

保険会社が、今後サイバー保険の引受を拡大し、収益の成長を持続可能なものにするためには、手口の巧妙化や高度化等のサイバー攻撃が大きく変化していることにあわせて保険商品・サービスを見直し、開発すること、ならびに保険引受やリスク管理に関する方針を明確にすること等が必要とされている。米国のサイバー保険市場に参入したインシュアテック企業の対応にも見られるように、顧客企業のサイバーインシデント予防対策、危機管理対策、およびシステム復旧対策等への支援を通じ、顧客企業にとって最善の保険サービスを提供することが重要であるとされている[71]。

サイバーインシデントやサイバー保険をめぐる状況の変化は速く、また保険会社への影響も大きいと考えられるため、今後も引き続き注視していくこととしたい。

[70] NAIC, “Cybersecurity, Center for Insurance Policy & Research”（2020.4）、Insurance Europe, “Insurer’s role in EU cyber resilience”（2019.10）

[71] S&P Global, “Cyber Risk In A New Era: Insurers Can Be Part Of The Solution”（2020.9）

＜参考資料＞

・飯野由佳子「中小企業向けの BI 保険と BCP 関連サービス－米国・イギリスを中心に－」損保総研レポート第 130 号（損害保険事業総合研究所、2020.1）
・牛窪賢一「インシュアテックにおける新たなビジネスモデル－ブロックチェーンを利用した補償等の展開と課題－」損保総研レポート第 128 号（損害保険事業総合研究所、2019.7）
・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）
・笠原康弘「諸外国の保険業界における IT 活用の動向」損保総研レポート第 133 号（損害保険事業総合研究所、2020.11）
・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）
・経済産業省「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」（2020.6）
・警察庁「令和２年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2020.10）
・杉浦友「スマートシティの政策課題と保険会社への影響」損保総研レポート第 131 号（損害保険事業総合研究所、2020.5）
・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）
・日本経済団体連合会、日本商工会議所、経済同友会「サプライチェーン・サイバーセキュリティ 確保に向けた共同宣言」（2020.11）
・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「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）
・安田昶勲「GDPR 施行後の現状と保険業界における課題」損保総研レポート第 129 号（損害保険事業総合研究所、2019.11）
・Acronis, “Cyberthreats Report 2020”（2020.12）
・Airmic, “Silent Cyber White Paper”（2020.12）
・AJ Gallagher USA, “2020 Market Conditions Report: Cyber Liability”（2020.3）
・Allianz Global Corporate & Specialty, “Managing the Impact of Increasing Interconnectivity: Trends in Cyber Risk 2020”（2020.11）
・Amanda Russo, “Next Generation Tech Creates Watershed Moment for Cybersecurity Industry”（WEF, 2020.11）
・Anthony R. O’Donnell, “Corvus Insurance Launches Automated Ransomware/Business Interruption Cost Calculator”（Insurance Innovation Reporter, 2020.4）
・Aon, “2020 Cyber Security Risk Report”（2020.2）

・Aon, “Aon secures $70 million alternative capital capacity led by HSCM to transfer systemic cyber risk”（2020.11）
・Aon, “Cyber Insights for Insurers”（2020.5）
・Aon, “Cyber Insurance Market Insights”（2020.10）,
・Aon, “Insurance-Linked Securities”（2018.9）
・Aon, “US Cyber Insurance Profits and Performance”（2020.6）
・Aon, “US Cyber Market Update”（2019.10）
・Ben Dyson, “Cyber insurance-linked securities will come ‘sooner than later’”（S&P Market Intelligence, 2019.9）
・CBInsights, “Slice Labs Information”（2020.12）
・Check Point, “Cyber Attack Trends: 2020 Mid-Year Report”（2020.7）
・CrowdStrike, “Asia Pacific & Japan, State of Cybersecurity Survey 2020”（2020.7）
・Cyber Risk Management Company, “Cyberhedgehog”（2019.2）
・EIOPA, “Cyber Risk For Insurers, Challenges And Opportunities”（2019.7）
・EIOPA, “EIOPA Strategy on Cyber Underwriting”（2020.2）
・EIOPA, “Financial Stability Report”（2019.12）
・EU-US Insurance Dialogue Project, “New Initiatives for 2017 - 2019, Focus Areas for 2018”（2018.10）
・European Police Office, “How Criminals Profit From The COVID-19 Pandemic”（2020.10）
・European Police Office, “Internet Organized Crime Threat Assessment”（2020.10）
・FBI, “2019 Internet Crime Report”（2020.8）
・Hiscox, “Hiscox Cyber Readiness Report 2020”（2020.7）
・IAIS, “Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development”（2020.12）
・IBM, “IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year”（2020.7.29）
・Insurance Europe, “Insurer’s role in EU cyber resilience”（2019.10）
・International Committee of The Red Cross, “Cyber attacks Statement”（2020.7）
・International Criminal Police Organization, “COVID-19 cyberthreats”（2020.10）
・International Criminal Police Organization, “Evolution of Cybercrime Trends and Threats amid COVID-19”（2020.8）
・International Criminal Police Organization, “Global Landscape on COVID-19 Cyberthreat”（2020.4）
・International Criminal Police Organization, “Internet Organised Crime Threat Assessment (IOCTA)”（2020.10）
・Jeff Kauflin, “Ransomware Has Catapulted This Insurtech Startup To $100 Million In Revenue”

（Forbes, 2020.11）
・Jonathan Kent, “HSCM and Aon team up to offer cyber coverage”（The Royal Gazett, 2020.11）
・Luke Gallin, “Aon & HSCM launch $70mn catastrophic cyber product”（Reinsurance News, 2020.11）
・Marsh, “Global Insurance Market Index”（2020.11）
・Marsh, “MMC CYBER HANDBOOK 2021”（2020.11）
・McAfee, “The Hidden Costs of Cybercrime”（2020.12）
・Microsoft, “Microsoft Digital Defense Report”（2020.9）
・Moti Sagey, “Remote work carries massive cyber risks. These top IT tips can help keep your workers secure”（WEF, 2020.9）
・Munich Re, “Cyber insurance: Risks and Trends 2020”（2020.4）
・NAIC, “Cybersecurity, Center for Insurance Policy & Research”（2020.4）
・NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2019.11）
・NAIC, “Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement”（2020.12）
・NetDiligence, “Cyber Claims Study 2020 Report”（2020,10）
・OECD, “Encouraging Clarity in Cyber Insurance Coverage”（2020.2）
・OECD, “Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation”（2020.10）
・OECD, “Enhancing the Availability of Data for Cyber Insurance Underwriting”（2020.2）
・OECD, “Insurance Markets in Figures, COVID-19 may curb the positive premium and investment income growth of insurers”（2020.6）
・S&P Global Market Intelligence, “Cyber insurers tighten underwriting, raise prices as ransomware wave hits”（2020.10）
・S&P Global Market Intelligence, “Cyber Risk In A New Era: Insurers Can Be Part Of The Solution”（2020.9）
・Sam Carter, “Cyber-Catastrophe Insurance-Linked Securities On Smart Ledgers”（Carter Research, 2018.11）
・Sophos, “The State of Ransomware 2020”（2020.5）
・Stuart Collins, “Commercial Risk News”（2019.11）
・Swiss Re, “Could cyber risk be a growth engine for reinsurance?”（2019.8）
・United Nations, “Cybercrime, UNODC COVID-19 Policy Documents”（2020.4）
・WEF, “Cyberinsurance”（2020.11）
・WEF, “Future Series: Cybersecurity, Emerging Technology And Systemic Risk”（2020.11）
・WEF, “Global Technology Governance Report 2021: Harnessing Fourth Industrial Revolution

Technologies in a COVID-19 World”（2020.12）
・WEF, “Partnership against Cybercrime”（2020.11）
・WEF, “Remote work carries massive cyber risks. These top IT tips can help keep your workers secure”（2020.9）
・Willis Towers Watson, “Insurance Marketplace Realities”（2020.11）
・Zack Whittaker, “Cyber insurance startup At-Bay raises $34M Series C, adds M12 as a new investor”（TechCrunch News, 2020.12）
・Zurich North America, “Information Security And Cyber Risk Management”（2020.10）

＜参考ウェブサイト＞

・欧州保険年金監督機構（EIOPA）　https://www.eiopa.europa.eu/
・金融庁　https://www.fsa.go.jp/
・経済協力開発機構（OECD）　https://www.oecd.org/
・経済同友会　https://www.doyukai.or.jp/
・警察庁　https://www.npa.go.jp/
・財務省　https://www.mof.go.jp/
・情報処理推進機構　https://www.ipa.go.jp/
・全米保険庁長官会議（NAIC）　https://content.naic.org/
・総務省　https://www.soumu.go.jp
・通商産業省　https://www.meti.go.jp/
・内閣サイバーセキュリティセンター　https://www.nisc.go.jp/
・内閣府　http://www.cao.go.jp/
・日本経済団体連合会　http://www.keidanren.or.jp/
・日本商工会議所　https://www.jcci.or.jp/
・日本損害保険協会　https://www.sonpo.or.jp/
・防衛省　https://www.mod.go.jp/
・保険監督者国際機構（IAIS）　https://www.iaisweb.org/
・Acronis　https://www.acronis.com/
・AIG　https://www.aig.com/
・AJ Gallagher　https://www.ajg.com/
・Allianz　https://www.allianz.com/
・Aon　https://www.aon.com/
・At-Bay　https://www.at-bay.com/
・AXA　https://www.axa.com/
・CBInsights　https://www.cbinsights.com/
・Check Point　https://www.checkpoint.com/

・Coalition　https://www.coalitioninc.com/

・Corvus　https://www.corvusinsurance.com/

・Crowdstrike　https://www.crowdstrike.com/

・CSIS　https://www.csis.org/

・European Police Office　https://www.europol.europa.eu/

・FBI　https://www.fbi.gov/

・FM Global　https://www.fmglobal.com/

・Gen Re　https://www.genre.com/

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

・Hiscox　https://www.hiscoxgroup.com/

・IBM　https://www.ibm.com/

・Insurance Europe　https://www.insuranceeurope.eu/

・Intact Ventures　https://www.intactfc.com/English/home/default.aspx/

・International Committee of The Red Cross　https://www.icrc.org/

・International Criminal Police Organization　https://www.interpol.int/

・Marsh　https://www.marsh.com

・Resilience Insurance　https://www.resilienceinsurance.com/

・Slice Labs　https://www.slice.is/

・Sophos　https://www.sophos.com/

・Swiss Re　https://www.swissre.com/

・Travelers　https://www.travelers.com/

・United Nations　https://www.un.org/

・United States Cybersecurity & Infrastructure Security Agency　https://www.cisa.gov/cybersecurity/

・United States Department of Defense　http://www.defense.gov/

・United States Department of The Treasury　https://home.treasury.gov/

・WEF　https://www.weforum.org/

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

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