欧米等におけるサイバーリスク・保険の現状・課題および保険業界の取組み

主席研究員　濵田　和博

目　　次

１．　はじめに

２．　サイバーリスクの現況

（1）サイバーインシデントの発生状況

（2）攻撃の態様別の動向

（3）サイバー攻撃のアクターの動向

３．　サイバーリスク関連の規制の動向

（1）国連

（2）EU

（3）米国

（4）オーストラリア

４．　サイバー保険市場の概況

（1）全世界における市場規模

（2）保険事故の動向

（3）再保険会社の対応

５．　サイバーリスク・保険における課題と保険業界等の取組み

（1）中小企業への啓発・普及

（2）AI 等先進技術の影響・活用

（3）戦争免責条項への対応

（4）リスクの定量化・モデリング

６．　おわりに

要旨

生成 AI 等 IT 技術の急速な進化、およびそれらを実装した各種デジタルデバイスの企業・個人への普及、ならびにウクライナ、中東をはじめとする世界各地の地政学リスクの高まりなどを背景として、サイバーリスクは近年ますます拡大・増大している。またそれに伴い、先進国を中心として、サイバーリスク関連の法規制も強化されている。

そのような状況下、サイバーリスクへの対応策の１つとして、サイバー保険の利用が拡大し、世界的に収入保険料が増加している。また再保険会社などによる将来予測においても、今後さらに市場は拡大する見込みが示されている。

一方サイバー保険については、中小企業への啓発・普及、AI 等先進技術への対応、戦争リスクへの対応、リスクの定量化・モデリングなどの課題が認識されており、各国の損害保険業界、損害保険会社は、それらの解決に向け各種取組みを進めている。

わが国の損害保険業界も、顧客企業のニーズを汲み、最新のサイバーリスクの動向や、諸外国の損害保険業界の動向を注視しつつ、それらの課題に適切に対応していくことが重要である。

１．はじめに

生成 AI 等 IT 技術の急速な進化、およびそれらを実装した各種デジタルデバイスの企業・個人への普及、ならびにウクライナ、中東をはじめとする世界各地の地政学リスクの高まりなどを背景として、サイバーリスクは近年ますます拡大・増大している。わが国においても、2024 年 12 月に、日本航空のネットワーク機器を狙ったサイバー攻撃により、一時的に航空券の販売や運航に支障を来す事態が発生するなど、サイバー攻撃による被害が頻発している。

また、社会、企業、個人のサイバーリスク[1]に対する認識も高まっている。例えば、ドイツの大手保険会社アリアンツが 2025 年 1 月に公表した Allianz Risk Barometer[2]によると、主要なビジネスリスクの中でサイバーインシデントは、4 年連続で第 1 位に挙げられている[3]。米国の大手保険会社トラベラーズの「2024 Risk Index」においても、米国におけるビジネスリーダーの最大の懸念事項は「サイバーリスク」となっている[4]。

このようなリスクの増大や、リスク認識の高まりを受けて、サイバーリスクへの対応策としてのサイバー保険への需要は増加しており、その市場規模は拡大を続けている。

サイバーリスクは、社会および損害保険業界にとって重大性・重要性の高いリスクの 1 つである。このため、損害保険事業総合研究所においては、2019 年度上期の調査報告書「欧米地域におけるサイバー保険関連動向」をはじめとして、その後の複数の損保総研レポート等において、様々な角度で取り上げている。

本稿では、サイバーリスクの現況、サイバーリスク関連の規制の動向、サイバー保険市場の概況を説明したのち、サイバーリスク・保険における課題と保険業界等の取組みについて説明する。「サイバーリスク」は、国によって環境や規制など異なる要素も多々あるが、各国、各企業等に所在する IT 機器がインターネットを介して相互に接続しており、リスクが世界的に同時に顕在化する危険性があるなど、その性質上、各国とも共通した問題点を抱える特異なリスクでもある。したがって、他国で挙げられている「サイバーリスクの課題」の多くは、わが国においても同様に対応を検討すべき課題であり（またはその可能性が高く）、各国の先進的な取組みは、わが国でも参考になると考える。このような観点から、本稿執筆時点での最新と考えられる課題や取組みなどに関する情報について、国を限定せずに取り上げた。

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] 本稿では、サイバーリスクのうち、主にサイバー攻撃・犯罪について取り上げる。その他のサイバーリスクが顕在化した事案としては、2024 年 7 月に発生した「CrowdStrike 事件」が挙げられる。サイバーセキュリティ企業 CrowdStrike が顧客に対して配信したソフトウェアアップデート用のファイルの欠陥により、航空会社や病院の運営が中断されるなど、世界的に IT 障害が発生し、大きな損害が発生した。

[2] Allianz Commercial, “Allianz Risk Barometer”（2025.1）

[3] 106 カ国にわたる 3,778 人の顧客企業、保険ブローカー等に対する調査の結果である。

[4] サイバーリスクは、62%の回答者が懸念事項に挙げており、「医療費のインフレ（59%）」、および「従業員福利厚生費の増加（59%）」が続いている。

２．サイバーリスクの現況

（1）サイバーインシデントの発生状況

サイバーインシデントの発生状況につき、世界全体でとりまとめた正確なデータはないが、サイバー保険を積極的に販売している、イギリスに本拠を置く保険会社 Hiscox が、2024 年 11 月に公表した調査結果によると、欧米主要国の回答者[5]の 6 割以上が「過去 12 カ月間にサイバー攻撃が増加した」と回答している（図表 1 参照）。

また大手 IT 企業である IBM が 2024 年 10 月に公表したレポート[6]によると、16 カ国・地域でデータ侵害の影響を受けた 604 社を調査したところ、データ侵害によるコストの平均値は、2023 年の 445 万ﾄﾞﾙから 488 万ﾄﾞﾙに急増し、新型コロナウイルスのパンデミック以降で最も高い増加率（9.6%）となった。この増加の要因として、業務のダウンタイムや顧客の喪失を含むビジネス損失に伴うコストの増加、およびカスタマー・サービスのヘルプデスクへの人員配置や高額な罰金の支払いなど、侵害後の対応コストの増加を挙げている。

図表 1　Hiscox によるサイバーインシデントに関する主な調査結果

項目	イギリス	フランス	ドイツ	米国
過去 12 カ月間にサイバー攻撃が増加した組織	70%	62%	60%	69%
過去 12 カ月間に 1 組織が受けたサイバー攻撃の平均件数	71 件	75 件	49 件	66 件
サイバー攻撃による評判の失墜がビジネスに大きな損害を与えると考えるリーダー	62%	61%	62%	56%

（出典：Hiscox, “Cyber Readiness Report 2024”（2024.11）をもとに作成）

（2）攻撃の態様別の動向

大手コンサルティング会社のデロイトは、2024 年 3 月に公表した報告書において、世界の法執行機関の取組みにより、ランサムウェアによる身代金の支払件数は減少しているが、ランサムウェアは、2024 年も大きな脅威であり続けるとしている。また、ユーザーID を基にした初期アクセス技術が普及しており、2023 年における有効な認証情報の悪用は、全データ侵害の 44.7%を占め、2022 年の 41.6%から増加している。有効な認証情報を保護することはサイバーセキュリティにとって最も重要であるとしている。さらに「業界横断的な脅威ベクトル[7]のトレンド」として、ランサムウェア、大規模なデータ侵害、マルウェア、およびアンダーグラウンドの各動向を挙げている（図表 2 参照）。

---

[5] 欧米主要国の、組織においてサイバーセキュリティ戦略を担当する 2,150 人を対象として、調査したものである。

[6] IBM「データ侵害のコストに関する調査 2024」（2024.10）

[7] 脅威ベクトル（threat vectors）とは、6 つの主な攻撃ルート（ネットワーク、ユーザー、e メール、ウェブアプリ、リモートアクセスポータル、モバイルデバイス）のうちの 1 つ以上を介してコンピューターシステムにアクセスするための手段を指す。

図表２　サイバー攻撃の主な態様ごとの動向

攻撃の態様	動向
ランサムウェア	○ランサムウェアは、世界のあらゆる業界で二重恐喝（注１）に使用されており、2023年には米国が最も多く標的となっている。 ○ランサムウェアによる被害額は、2024年上半期で4億ﾄﾞﾙを超えた。 ○医療と金融サービス分野においては、ランサムウェアに対する支払額が世界的に減少している。 ○洗練されたランサムウェアの運営者は、ゼロデイ攻撃（注２）を最初のアクセス・ベクトルとして使用する傾向が強まっており、被害者の36%がこの方法で身代金を要求されている。有効なクレデンシャル（注３）の侵害は、ランサムウェア攻撃のエントリポイント（注４）として2番目に多かった。
大規模なデータ侵害	○2023年に、全業界合計で82億件以上のデータが侵害され、その平均コストは445万ﾄﾞﾙであった。 ○最も一般的な最初の攻撃ベクトルは、フィッシング（注５）および有効な認証情報の窃取であった。 ○データや、個人を特定できる情報（Personal Identifiable Information：PII）は、それを販売することで利益を得るサイバー犯罪者や、国家安全保障上の課題に関するデータ収集や、様々なスパイ活動を行う国家脅威主体にとって最も価値のあるものである。 ○2023年には、顧客データの安全管理を怠ったプロバイダーに対する集団訴訟の事例が増加している。
マルウェア	○ステルス型のマルウェアが、さらに拡散している。 ○2023年における注目すべきマルウェアの傾向としては、ウェブブラウザ、暗号資産ウォレット、ゲームアカウント、VPN（Virtual Private Network）（注６）およびFTP（File Transfer Protocol）（注６）サービスからクレデンシャルを窃取するために使用されるInfoStealers（注７）が挙げられる。 ○さらに、主に製造業におけるIoTマルウェアの世界的な普及が見られる。
アンダーグラウンド	○2023年の主なトレンドとして、無償および有償のデータベースの配布や、Infostealers、トロイの木馬（Remote Access Trojan）（注８）、ドレイナー型マルウェア（注８）の提供が挙げられる。 ○「Cryptoドレイナー」は、巧妙なフィッシング・ウェブサイトを使用し、ユーザーを騙して暗号資産ウォレットを攻撃者のインフラに接続させている。 ○初期アクセス・ブローカー（Initial Access Broker：IAB）（注９）を介したAaaS（Access-as-a-Service）（注１０）や、FaaS（Fraud-as-a-Service）（注１０）が広く提供されている。

（注１）二重恐喝は、ランサムウェアによりターゲット組織のデータを抽出した後、ファイルを暗号化し、さらにリークサイト上で盗んだデータの公開を脅しに身代金を要求する攻撃手法を指す。

（注２）ゼロデイ攻撃は、発見された脆弱性を解消するための対策が提供される前に行われるサイバー攻撃を指す。

（注３）クレデンシャル（Credential）は、IT・セキュリティにおいてアクセスコントロールを行うための認証に使われる情報を指す。

（注４）エントリポイント（Entry Point）は、プログラムやシステムが実行される際に最初に処理が開始される場所やコードの部分を指す。

（注５）フィッシング（Phishing）は、実在する組織を騙って、ユーザネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を詐取する攻撃を指す。

（注６）VPNは、大規模ネットワークのスケールメリットと管理設備を利用するために、パブリックネットワーク内に構成されるプライベートネットワークを指す。また、FTPは、コンピュータネットワーク上のクライアントとサーバーの間でファイル転送を行うための通信プロトコルの1つを指す。

（注７）InfoStealers とは、情報を盗み出そうとするマルウェアを指す。複雑化したマルウェアには、通常 InfoStealers が含まれている。

（注８）トロイの木馬は、標的のコンピュータに侵入し、遠隔で操作を行うマルウェアを指す。また、ドレイナー（Drainer）は、ユーザーのウォレットから暗号資産等を不正に引き出し（Drain）盗むサイバー犯罪手法の１つを指す。

（注９）初期アクセス・ブローカーは、サイバー攻撃を行う際の最初のステップである、標的への不正アクセス手段を提供する者を指す。

（注１０）AaaS は不正アクセスの、また FaaS は詐欺や不正行為の、手段やツールをサイバー犯罪者が「サービス」として提供するビジネスモデルを指す。

（出典：Deloitte, “Global Cyber Threat Intelligence (CTI): Annual Cyber Threat Trends”（2024.3）をもとに作成）

（3）サイバー攻撃のアクターの動向

サイバー攻撃を行う者（アクター）は、①国家の支援を受けたアクター、②サイバー犯罪者、③ハクティビスト[8]、④内部脅威、の 4 つに大きく分類できる。それぞれのアクターの最近の動向は、図表 3 のとおりである。

図表３　サイバー攻撃のアクターの動向

アクター	動向
①国家の支援を受けたアクター	○国家の支援を受けた「高度サイバー攻撃（Advanced Persistent Threat：APT）(注1)」は、最も重大なサイバーセキュリティ脅威である。 ○政治的動機に基づく脅威アクターと、金銭的動機に基づく脅威アクターの境界線は曖昧になってきている。「重要インフラ」の定義に「金融サービス」を含めると、国家の支援を受けた脅威アクターと金銭的動機に基づく脅威アクターの違いはより曖昧である。国家の支援を受けた脅威アクターが、金銭的動機に基づく脅威アクターと協力し、多方面からアプローチする傾向が見られる。
②サイバー犯罪者	○RaaS（Ransomware as a Service）(注2)、および非常に活発で破壊的な少数のランサムウェアが蔓延している。 ○RaaS と同様に、初期アクセス・ブローカー（IAB）サービスも数多く利用されている。 ○ダークウェブにおいて、チャット・アプリを利用したサイバー犯罪者同士のコミュニケーションも継続的に行われている。 ○サイバー犯罪者によって増殖した、IoT マルウェアを含む多目的マルウェアは、依然として世界的に流行している。
③ハクティビスト	○政治的な動機に基づくハクティビストは、中東紛争に際しても、その動員能力を実証した(注3)。この脅威は、ウェブサイトの改ざんや、標的のウェブポータルに対する分散型サービス妨害（DDoS）攻撃(注4)という形で現れ、窃取した情報が漏えいする場合もある。
④内部脅威	○2023 年を通じて、アクターがダークウェブにおいて、「内部関係者」を積極的に勧誘していることが観察されている。 ○不安定な経済情勢は、個人が金銭的利益を得るために悪意のある活動に従事する動機となり、アクターは内部関係者の勧誘活動においてそれを利用している。 ○アクターはまた、情報収集やスパイ活動の目的で、政府組織、金融機関、携帯通信事業者、その他世界中の大手企業の内部関係者を勧誘している。

[8] 「ハッカー（hacker）」と「アクティビスト（activist）」を組み合わせた造語で、政治的あるいは社会的な主張・目的のためにサイバー攻撃を行う活動家や集団を指す。

（注１）高度サイバー攻撃は、革新的なハッキング手法を使用してシステムにアクセスし、長期間内部に留まる標的型攻撃を指す。

（注２）RaaS は、ランサムウェアの手段やツールをサイバー犯罪者が「サービス」として提供するビジネスモデルを指す。

（注３）イスラエルとイスラム組織ハマスの衝突を受けて、ハマスを支持する「ハクティビスト」集団がイスラエル側を標的としてサイバー攻撃を行った。

（注４）DDoS 攻撃は、標的もしくはその周りのインフラストラクチャに大量のインターネットトラフィック（転送されるデータ量）を与えることで、標的となるサーバー、サービス、ネットワークの通常トラフィックを妨害しようとする攻撃を指す。

（出典：Deloitte, “Global Cyber Threat Intelligence (CTI): Annual Cyber Threat Trends”（2024.3）をもとに作成）

３．サイバーリスク関連の規制の動向

本項では、データ・プライバシー規制や、サイバーセキュリティ報告要件等、サイバーリスク関連の、国連、EU、米国、およびオーストラリアにおける直近の主な規制の動向について説明する。

（1）国連

2024 年 7 月 29 日から 8 月 9 日の日程で、国連本部において「国連サイバー犯罪条約（仮称）」案作成交渉のためのアドホック委員会再開最終会合が開催され、現地時間 8 月 8 日、条約案が承認（合意）され、交渉が妥結した。

同条約案は、「情報通信技術を使って行われる特定の犯罪と、重大な犯罪の証拠を電子的に共有するために、国際的な協力を強化すること」を目的とし、その主な内容は、以下のとおりである。この条約案は、国連総会において 12 月 24 日に採択された。

① サイバー犯罪をより効率的かつ効果的に予防・対処するための対策を推進、強化すること
② サイバー犯罪の予防・対処における国際的な協力を推進、促進、強化すること
③ サイバー犯罪を予防・対処するための技術支援や能力構築を推進し、特に開発途上国の利益のために支援すること

（2）EU

EU では 2018 年以降、一般データ保護規則（General Data Protection Regulation：GDPR）がデータ保護とプライバシーの包括的な枠組みとなっている。また、2024 年 5 月に成立した EU の AI 法は、GDPR を補完し、AI システムに対するデータ・プラ

イバシー要件のギャップを埋めることを意図している[9]。

さらに EU 理事会（Council of the European Union）は、デジタル要素を備えた製品のサイバーセキュリティ要件に関する新しい規則となるサイバーレジリエンス法（Cyber Resilience Act：以下「CRA」）を 2024 年 10 月に採択した。CRA は、デジタルコンポーネントを備えた製品、例えば IoT 製品の安全性をライフサイクル全体およびサプライチェーン全体にわたって確保することを目的としている。

CRA の対象となるデジタル要素を含む製品は、デバイスやネットワークと接続する用途の製品を含め、欧州市場で販売されるハードウェア・ソフトウェア、遠隔データ処理ソリューションであり、すべてのコネクテッド製品が対象となっている。一方、既に他の法令の規制対象となっている一部の製品・サービス[10]については、法令間の調整を図る目的で CRA の対象外としている。

（3）米国

米国商務省（Department of Commerce）は 2024 年 9 月、先端的な AI 開発者とクラウド事業者に対して、技術の安全性とサイバー攻撃対応に万全を期すために連邦政府へ詳細な開発状況を報告する義務を提案すると表明した。先端的な AI の開発者やクラウド事業者は、サイバー攻撃に対する防衛策や、いわゆる「レッドチーム演習（危険なサイバー攻撃への耐性を診断するための疑似攻撃）」結果の報告も求められる。

商務省は、この提案のもとで集まった情報は、安全性や信頼性、サイバー攻撃へのレジリエンス、敵対的な外国や非政府勢力による悪用リスクの低減といった面で、AI 技術を確実に厳格な基準に適応させるうえで重要になると説明した。

バイデン大統領は 2023 年 10 月、米国の安全保障や経済、公衆衛生を脅かす AI システムの開発者に、安全性の試験結果を連邦政府と共有した後で公開することを定めた大統領令（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence）を発している。

また、米国証券取引委員会（Securities and Exchange Commission：以下「SEC」）の定めた、新たなサイバーセキュリティ関連の開示規則も、2023 年 12 月から発効している。この規則により、上場企業は、サイバーインシデントを「重大」であると判断した場合、4 営業日以内に、当該インシデントを開示しなければならない。企業はまた、SEC への提出が義務付けられている「年次報告書」を通じて、サイバーセキュリティ戦略、リスク管理、ガバナンス慣行に関する情報を開示する必要がある。SEC は外国企業にも同様の定期的な開示を義務付けている。

---

[9] AI 法についての詳細は、佐藤智行「保険事業における AI 利用に関する海外主要規制・監督機関等の主な取組み」損保総研レポート第 147 号（損害保険事業総合研究所、2024.6）を参照願う。

[10] 軍事・国家安全保障目的の製品や、海洋、医療、自動車、航空等に関する製品として既に規制対象となっているものなどを指す。

（4）オーストラリア

オーストラリアは、2024 年 11 月、同国初の単独のサイバーセキュリティ法（Cyber Security Act）を可決した。同法は、同国のサイバーセキュリティ戦略（2023-2030 Australian Cyber Security Strategy）に基づく、サイバーセキュリティ立法パッケージ[11]の一部である。同法に定める主な措置は、以下のとおりである。

○ 新たに独立した諮問機関である「サイバーインシデントレビュー委員会（Cyber Incident Review Board：以下「CIRB」）」を創設した。CIRB は、重大なサイバーセキュリティインシデントの事後レビューを実施し、企業や公共部門に、推奨事項や情報を提供する。CIRB には、重大なサイバーセキュリティインシデントが発生した場合、関係者に情報の提供を義務付ける権限も与えられている。

○ 重大なサイバーセキュリティインシデントに対する政府全体の対応を主導する国家サイバーセキュリティコーディネーター（National Cyber Security Coordinator）を新たに設置する。

○ 重要なインフラを所管する組織、およびオーストラリアで事業を営む、基準[12]を超える年間売上をあげる民間企業に、サイバー身代金支払いに関する報告義務[13]を導入する。身代金を支払った場合、支払い後 72 時間以内に、内務省（Department of Home Affairs）とオーストラリア信号局（Australian Signals Directorate：以下「ASD」）[14]に報告する必要がある。

４．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、全世界における市場規模、保険事故の動向、および再保険会社の対応について説明する。

（1）全世界における市場規模

世界全体のサイバー保険市場に関して正確な統計はないが、スイス再保険によると、世界全体のサイバー保険市場は、2017 年から 2022 年にかけて年平均 32%という高い

---

11 サイバーセキュリティ法のほか、Intelligence Services and Other Legislation Amendment (Cyber Security) Act、および the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act で構成される。

12 基準となる売上高は、今後明記される見込みであるが、300 万豪ﾄﾞﾙ（約 3 億円）となる可能性が高い（Corrs Chambers Westgarth, “Australia introduces Comprehensive Cyber Security Legislation”（2024.11））。

13 身代金を支払った場合のみに報告義務が生じ、ランサムウェアの感染や、身代金の要求を受けただけでは、報告義務はない。

14 ASD は、諜報活動の 1 つである信号情報（signals intelligence）、オーストラリア軍事作戦への情報支援、サイバー戦争の遂行、情報セキュリティの確保を担当するオーストラリア政府の法定機関である。

成長率を達成した。2019 年までは、北米と欧州において、サイバー保険を契約する企業が増加したことで、収入保険料は大幅に増加した。その後 2020 年から 2022 年にかけては、ランサムウェアの急増により大きな損失が発生したため、保険会社による保険料率の引上げが実施され、それが主な保険料増加要素となった。

2022 年には、保険料率引上げと収益性見通しの改善により、サイバー保険市場に新規参入する保険会社が増加した。これにより保険会社間の競争が激化し、2023 年には保険料率水準、および市場の成長率が低下した。

スイス再保険は、2025 年の市場保険料を 166 億ﾄﾞﾙ（2024 年比 8%増）と予測している。一方で、サイバーリスクの補償ギャップは依然として大きく、サイバー保険料の地域間分布にも不均衡があるとしている。北米における収入保険料が、世界全体の 70%を占め、次いで欧州（19%）、アジア太平洋（8%）となっている。これは、サイバー保険市場の成熟度が地域により異なることを示しているだけでなく、欧州とアジア太平洋の多くの経済圏でサイバー市場が未開拓であり、成長のポテンシャルがあることを裏付けているとしている。

（2）保険事故の動向

多くの国でサイバー保険を販売している Allianz Commercial[15]が、自社のサイバー保険の保険金請求データを分析した結果を、2024 年 10 月に公表している[16]。これによると、2024 年上半期の大規模[17]なサイバー保険の保険金請求の発生頻度は 14%増加し、重大度（severity）は 17%増加している[18]。大きな特徴の 1 つは、これら大規模損害の 3 分の 2 に、「データ・プライバシー侵害」が関連していることである。サイバー保険金請求における「データ・プライバシー侵害による損害」の比重が高まっているのは、①サイバー攻撃が個人データを標的とする傾向に変化していること、および②個人データの不正な収集や、不適切な処理など「非攻撃的なデータ・プライバシー（non-attack data privacy）」関連の集団訴訟が急増していることによるものであるとしている。これら「非攻撃的なデータ・プライバシー」関連の保険金請求の増加は、IT 技術の発展、個人データの商業的価値の増大、規制および法的環境の変化の結果である。米国では、データ使用などに関するプライバシー侵害に関連して、大手米国企業および国際企業に対する集団訴訟が提起される傾向が強まっている。

また、注目すべき傾向として、データ流出を含むランサムウェア攻撃の増加も挙げられている。これは、サイバー攻撃者の戦術の変化と、これまで以上に大量の個人記録を

---

15 Allianz Commercial は、Allianz Global Corporate & Specialty（AGCS）の大規模法人向け保険事業と、Allianz Property & Casualty の中規模企業向け保険事業を統合した保険会社であり、200 を超える国・地域で事業を展開している。

16 Allianz Commercial, “Cyber security resilience 2024”（2024.10）

17 ここでは、100 万ﾕｰﾛ（約 1 億 6,500 万円）超の保険金請求を指す。

18 2023 年は、発生頻度は対前年で 14%増加し、深刻度は 17%増加した。

共有する組織間の相互依存関係の増大によるものである。

Allianz Commercial は、データ侵害とランサムウェア攻撃の増加により、2024 年は、サイバー保険の保険金請求が大幅に増加するとしている[19]。

（3）再保険会社の対応

2024 年 9 月に開催された、翌年の更改等再保険関連の諸問題を論議する「モンテカルロ保険会議（Rendez-Vous de Septembre）」において、スイス再保険は、最近「サイバーは実際に重大なリスクであり、適切な保険が必要である」との認識が高まっており、今後数年間、年成長率は 2 桁の大幅な伸びを示すとの予測を示した。一方大手再保険会社スコール（SCOR）は、「サイバー保険のキャパシティは、リスク集積の脅威によって制限されるだろう」とし、「サイバーリスクは他のリスクと全く異なり、すべてが相互に関連している」と述べ、グローバルビジネスのデジタル化との関連性が強まっていることを強調した[20]。

５．サイバーリスク・保険における課題と保険業界等の取組み

本項では、サイバーリスク・保険における課題と保険業界等の取組みとして、中小企業への啓発・普及、AI 等先進技術の影響・活用、戦争免責条項への対応、およびリスクの定量化・モデリングについて説明する。

（1）中小企業への啓発・普及

中小企業は、大企業に比してサイバーセキュリティ管理が厳格ではない場合が多いため、その脆弱性を突いて、世界各国でサイバー攻撃の対象となってきている。例えば、Hiscox が、2023 年 10 月に公表した「年次サイバー準備報告書（Cyber Readiness Report 2023）の調査結果によると、従業員 10 人未満の中小企業に対するサイバー攻撃が過去 3 年間で 23%から 36%に増加している。

その一方で一般的に中小企業は、サイバーリスクの深刻さについて認識が低く、対策を講じていない割合が高い。例えば、中小企業向けのサイバー保険を取り扱う大手保険代理店 Cowbell が、2024 年 3 月に公表した調査[21]によると、調査対象となったイギリスの中小企業経営者 500 人のうち 32%が、サイバー攻撃により自社の事業遂行能力に影響を受けないと考えており、また回答者の 10%は、サイバーリスクに対する対応を

[19] Mirko Zorz, “The future of cyber insurance: Meeting the demand for non-attack coverage”（Help Net Security, 2024.10）

[20] Matthew Lerner, “US casualty tops reinsurers’ concerns as renewal negotiations begin”（Business Insurance, 2024.9）

[21] この調査は、2023 年 9 月 1 日から 15 日までの期間に、イギリスの中小企業の経営幹部および上級管理職 500 人を対象に実施された。

強化する必要性を感じていないと回答している。多くの中小企業がサイバーリスクの理解・軽減に関心が薄いということは、これらの中小企業をサプライチェーンに含む大企業に危険を及ぼす危険性も高い。また、Cowbell の調査によると、イギリスの中小企業の 77%が社内においてサイバーセキュリティ対策を講じていない。

2023 年 4 月にイギリスの科学技術イノベーション省（Department for Science, Innovation and Technology : DSIT）が公表した「サイバーセキュリティ侵害調査 2023（Cyber security breaches survey 2023）」によると、イギリスにおいてサイバー保険に加入している零細企業はわずか 6%、中小企業で 11%であるとのことである。

スイス再保険は、サイバー保険の最も大きな成長機会は中小企業にあるとし、サイバー脅威に対するレジリエンスを強化するために、保険業界は地理的範囲を拡大するだけでなく、リスク移転商品とサービスを顧客セグメントの特定のニーズに合わせて調整し、それらを配布する効率的な方法を見つける必要があるとしている[22]。

a. 保険業界の取組事例

イギリスの大手保険会社アビバは、小規模企業がサイバー保険に加入しやすいよう、手頃な保険料水準でサイバーインシデントに関する補償や、データ侵害対応サービスを提供する新たなサイバー保険商品「Aviva Cyber Respond」の販売を 2023 年に開始した[23]。この新商品の保険料は、年間 50 ﾎﾟﾝﾄﾞ（約 1 万円）と低額に設定されている。この保険は、個人情報詐欺監視サービス、信用監視サービス、評判管理サービスのほか、24 時間の電話による対応と、IT フォレンジック[24]の専門家のサポートなどのサービスが付帯されており、小規模企業がサイバーレジリエンスを高めることができるよう設計されている。

またアビバは、中小企業のサイバーレジリエンス構築支援に必要な情報をブローカーに提供するため「アビバ認定サイバー保険・リスクプロフェッショナル（Aviva's Certified Cyber Insurance and Risk Professional：以下「ACCIRP」）」と呼ばれるトレーニングプログラムを実施している[25]。ACCIRP は、以下の単位で構成されている。

① サイバーリスク入門
② サイバーに関する用語
③ 顧客がサイバー保険を必要とする理由

---

[22] Swiss Re, "Reality check on the future of the cyber insurance market"（2024.11）
[23] Terry Gangcuangco, "Aviva to roll out cyber product for UK micro-SMEs"（Insurance Business, 2023.10）
[24] 「フォレンジック」とは、元々犯罪捜査における分析や鑑識を意味する言葉であるが、サイバーセキュリティの分野では、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組みを指す。
[25] Stuart Collins, "Europe's insurers will move to clarify cover for AIrisks"（Commercial Risk, 2024.11）

④　サイバー保険による補償
⑤　保険事故対応・管理
⑥　アンダーライティングの要素
⑦　顧客からの反論、および販売方法

（2）AI 等先進技術の影響・活用

生成 AI を含む AI の進歩と、AI への企業・個人の依存度の高まりは、サイバーセキュリティの状況に大きな影響を与えている。AI により、サイバー犯罪者は、より大規模かつ迅速に攻撃を実行することが可能となっている。一方 AI は、企業等のサイバー攻撃の防止、脅威の検出の強化、インシデント対応戦略の改善能力向上などサイバーセキュリティにプラスの影響も与えている。

a. AI の利用によるリスク

2024 年 10 月、ニューヨーク州金融サービス局（New York State Department of Financial Services：以下「DFS」）は、金融サービス会社を含む、サイバーセキュリティ規制（23 NYCRR Part 500）における対象事業体に対して、AI から生じるサイバーセキュリティのリスク、ならびに AI の進歩および AI への依存度の高まりを踏まえた関連リスクを軽減するための戦略に関する業界レター（ガイダンス）[26]を発行した。このガイダンスは、金融機関等、DFS の規制対象組織（Covered Entities：以下「対象エンティティ」）に向けて書かれたものであるが、その多くは、金融機関以外にもあてはまる内容である。このガイダンスでは、サイバーセキュリティに特有の、AI の使用がサイバーセキュリティに与える主なリスクとして 4 つ取り上げている（図表 4 参照）。なお、図表 4 において、①および②は、脅威アクターによる AI の使用によって引き起こされるリスクであり、③および④は、対象エンティティによる AI の使用、または AI への依存によって引き起こされるリスクである。

[26] New York State Department of Financial Services, “Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks”（2024.10）

図表４　AIの使用に関連する主なリスク

リスク	内容
①AIを利用したソーシャルエンジニアリング（注１）	○ソーシャルエンジニアリングは、長年サイバーセキュリティ上の課題であるが、AIによって脅威アクターが高度にパーソナライズされた、より洗練されたコンテンツを作成できるようになっている。 ○脅威アクターは、リアルで双方向な、音声、動画、テキスト（ディープフェイク）を作成するためにAIをますます利用しており、eメール（フィッシング）、電話（ヴィッシング（注２））、テキスト（スミッシング（注３））、ウェブ会議、オンライン投稿を通じて特定の個人を標的にしている。 ○これらのAIを利用した攻撃は、多くの場合、従業員に自分自身や雇用主に関する機密情報を漏らすように仕向ける。 ○ディープフェイクにより認証情報が共有されると、脅威アクターは非公開情報（Nonpublic Information）を含む情報システムにアクセスが可能となる。 ○AIを利用したソーシャルエンジニアリング攻撃は、機密情報の漏えいに加えて不正な口座への多額の資金送金などの犯罪にもつながる。 ○ディープフェイクは、個人の外見や声を模倣して、生体認証技術を回避するために使用されている。
②AIを利用したサイバーセキュリティ攻撃	○AIの大きなリスクの１つは、脅威アクターが、従来のサイバー攻撃の有効性、規模、速度を増幅できることである。 ○AIは、膨大な量の情報を高速にスキャン・分析できるため、脅威アクターはAIを利用してセキュリティの脆弱性を特定できる。 ○脅威アクターは、AIを使用して、より多くの情報システムに、より早く侵入し、偵察を行い、マルウェアを展開して非公開情報にアクセスして盗み出す最適な方法などを見つけることができる。 ○AIは、マルウェアの新たな変種の開発速度を速め、防御セキュリティを回避できるようにランサムウェアを変えることにより、検出を逃れることも可能となる。 ○AI対応の製品・サービスが急増に伴い、現在、または近い将来において、脅威アクターに技術的スキルがなくても、サイバー攻撃ができる可能性があると広く考えられている。AIはサイバー攻撃の速度と規模を加速させている。
③膨大な量の非公開情報の漏えいまたは盗難	○AIを使用する製品では、通常大量のデータの収集・処理が必要であり、非公開情報が含まれている場合も多い。大量の非公開情報を保持することは、AIを開発・展開する対象エンティティに、追加のリスクを生じることになる。また、脅威アクターがこれらの対象エンティティを標的にして、金銭的利益やその他の悪意のある目的で非公開情報を抽出しようとする動機が強くなる。 ○脅威アクターは、盗んだ生体認証データを使用して正規のユーザーを模倣し、非公開情報やその他の機密情報を管理する情報システムにアクセスすることが可能となる。また、生体認証データを使用して、非常に精巧なディープフェイクを生成することもできる。
④サードパーティ、ベンダー、その他のサプライチェーンへの依存による脆弱性の増大	○AIを使用する組織や、AIを組み込んだ製品を使用する組織にとって、サプライチェーンの脆弱性は、重要な懸念事項の１つである。 ○AIを利用したツールやアプリは、膨大な量のデータの収集・維持に大きく依存している。そのデータ収集プロセスでは、ベンダーやサードパーティ・サービス・プロバイダー（以下「TPSP」）との連携が頻繁に必要になる。そのサプライチェーンには、脅威アクターが悪用できる潜在的なセキュリティの脆弱性が存在する。 ○TPSP、ベンダー、サプライヤーがサイバーインシデントによって侵害された場合、対象エンティティの非公開情報が公開され、サプライチェーン内の他のすべてのエンティティに対するより広範な攻撃の入り口になる可能性がある。

（注１）ソーシャルエンジニアリングは、マルウェアなどを用いずにパスワードなどの情報を盗み出す手法を指す。

（注２）ヴィッシング（Vishing）は、電話（Voice）によるフィッシング攻撃を指す。
（注３）スミッシング（SMiShing）は、携帯電話のショートメッセージサービス（SMS）によるフィッシング攻撃を指す。
（出典：New York State Department of Financial Services, “Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks”（2024.10）をもとに作成）

b. AIの活用によるサイバー攻撃対策

AI 等先端技術は、サイバー攻撃に対する防御を強化する強力なツールとして活用することもできる。例えば、「SOAR（Security Orchestration, Automation and Response）」は、セキュリティ運用の自動化および効率化を実現する技術として、近年注目を浴びている[27]。SOAR は、組織内の各種セキュリティ機器および外部サービスから収集された脅威情報を 1 つのプラットフォームに統合する技術であり、一般的には、以下の 3 要素で構成されている。

① インシデント対処の自動化
② インシデント管理機能
③ 脅威インテリジェンスの活用

また生成 AI は、脅威レベルと脆弱性に関する詳細なレポートを迅速に作成することができるため、企業等がサイバーセキュリティ戦略・投資において、より良い意思決定を行うことを可能にする。

サイバーインシデント発生後、これらのツールは攻撃を再構築して調査を支援し、将来の侵害を軽減するための予防策を提案することができる。また生成 AI は、暗号化キーの強化からアクセス制御の強化まで、より強力なセキュリティ・プロトコルの開発を支援することもできる。企業等は、技術革新とサイバーセキュリティを相反する力ではなく補完する力としてとらえるべきである。両者を同時に進めることで、成長と発展のための安全な環境を育むことができる[28]。

c. AI、または AI を活用したサイバー攻撃による損害に対する補償

AI は、サイバーリスクにおいては、新たなリスクを生み出しているというより、むしろサイバーセキュリティやデータ・プライバシーなどの既存のリスクを増幅させている。例えば、誤情報が広められるリスクの場合、AI とソーシャルメディアの発達により、以前に比べ影響を及ぼす範囲やスピードが急激に増している。また、それにより

[27] 佐々木美稲「SOAR とは？セキュリティ運用の自動化により得られる３つのメリット」（NRI Secure, 2024.10）
[28] Hiscox, “Cyber Readiness Report 2024”（2024.4）

リスクプロファイルも変わってきている。

欧州保険市場においては、損害保険は現在、AI に関連する損失に対して「黙示的な」補償を提供していると広く考えられているが、保険会社は今後、AI 関連の補償を明確にする方向に動く可能性が高いとのことである[29]。スイスの大手保険会社チューリッヒ保険は、AI が根本的に保険リスクを変える可能性があるため、AI が各業界や保険契約者に与える影響について十分に理解する必要があるとしている。また、リスクマネージャーや保険契約者は、現在の損害保険契約が AI による損害を補償するかどうかについて疑問を持ち始めている。AI に対する補償については、チューリッヒ保険の顧客諮問委員会（customer advisory boards）でも論議されているが、AI が与える影響については、まだ体系的な見解が出ていない。またこれは、ここ 2 年間で急速に高まった問題であり、対応方法や顧客への説明方法を考える必要があるとしている。

大手保険ブローカーのマーシュによると、一般的に保険市場では AI の補償に制限は課されていないという。現状では、AI が免責とされることはないと思われるが、一部のリスクは増幅されているおそれがある。現在の保険商品がそれを補償しているかどうかを理解するには、常にリスクを具体的に見る必要がある。損害保険業界は、保険契約が AI リスクにどのように対応するかについて考える必要がある[30]。また、今後は保険契約の約款文言をさらに明確にする必要がある。

AI の機能によっては、「物理的な損害」も考慮する必要がある。例えば、生産プロセスを自動化している場合に、そこで AI に発生した事故による損害が、サイバー保険（または財産保険）で補償されるかどうかを確認する必要がある。

d. 保険業界の取組み事例

米国に本拠を置く大手保険会社 AXA XL は、2024 年 10 月、北米、欧州、アジアにおいて、独自の生成 AI モデルの開発、トレーニング[31]を行う企業に対する補償を、特約により提供すると発表した[32]。この特約は、自社のサイバー保険（Cyber Risk Connect policy）に生成 AI 補償特約（endorsement）を付帯して補償を提供する。この特約は、生成 AI が、ビジネスにもたらす以下の 3 つの主要なリスクを補償する。

① データポイズニング（攻撃者による AI トレーニングデータの改ざん・汚染）
② EU の AI 法（Artificial Intelligence Act）の故意でない（non-intentional）違

[29] Stuart Collins, “Europe’s insurers will move to clarify cover for AI risks”（Commercial Risk, 2024.11）
[30] AI は、サイバー保険だけでなく、賠償責任保険や財産保険など、多くの保険分野に影響を及ぼす可能性がある。
[31] AI モデルの「トレーニング」とは、コンピュータープログラムを段階的に実行して知能を獲得するプロセスを指す。
[32] Camille Joyce Lisay, “AXA XL launches insurance coverage for Gen AI risks”（Insurance Business, 2024.10）

反

③ 機械学習で使用されるデータに関連する著作権・知的財産の侵害など使用権の補償

（3）戦争免責条項への対応

サイバー保険における「戦争免責条項」への対応は、国家の関与が疑われる、または戦争の手段として使用されるサイバー攻撃が増加する中、損害保険業界として、補償が困難なシステミックリスクを除外するという観点、および補償の範囲を明確化して顧客との保険金支払いに関するトラブルを回避する観点などから重要な課題である。

本項では、サイバー保険における戦争免責条項への対応として、「従来の戦争免責条項」の適用を巡る行方、ロイズの「サイバー戦争免責条項」への対応、および再保険者の「サイバー戦争免責条項」への対応について説明する。

a. 「従来の戦争免責条項」の適用を巡る裁判の行方

米国において、2017 年の国家の関与が疑われるサイバー攻撃により生じた損害に係る保険金請求に対し、損害保険会社が、従来の戦争免責条項を根拠として保険金支払いを拒絶し、訴訟となった事例として「Merck 対 Ace American など」の概要および第 1 審の判決内容を、2022 年 12 月の損保総研レポートで取り上げた[33]。

同裁判は、その後、保険金支払いを命じた第 1 審を不服として、被告保険会社 Ace American などは控訴したが、控訴審（Appellate Division in New Jersey）も、「免責とするには、軍事行動の関与が必要」として、保険会社に保険金支払いを求めた。さらに被告保険会社は上告したが、上告審（New Jersey Supreme Court）の判決前に、原告・被告間で和解が成立した。この判決前の和解により、「従来の戦争免責条項」の適用可否などの論点につき、上告審による最終的な判断は得られなかった。なお、Merck の受けた損害額は 14 億ﾄﾞﾙとされるが、今般の和解による損害保険会社の支払額は、公表されておらず不明である。

b. ロイズの「サイバー戦争免責条項」への対応

前記 a.の事案をきっかけとして、ロイズなどにおいて、国家の関与するサイバー攻撃を免責とする「サイバー戦争免責条項」が論議され、ロイズ市場協会（Lloyd’s Market Association：LMA）は、2021 年 11 月に、「サイバー戦争免責条項」のモデル案を公表した。

2022 年 8 月、ロイズ（Loyd’s of London）は、「市場通告（Market Bulletin）Y5381」を発出し、2023 年 3 月 31 日以降、サイバー保険の新規・更改契約において、国家の

[33] 事案の詳細については、濵田和博「国家の関与するサイバー攻撃とサイバー保険の戦争免責条項について」損保総研レポート第 141 号（損害保険事業総合研究所、2022.12）を参照願う。

関与するサイバー攻撃に起因する損害について免責条項の付帯を義務付ける指示を出した。市場通告 Y5381 の趣旨は、ロイズが国家の関与するサイバー攻撃によってもたらされるシステミックリスクをロイズ市場が適切に管理できるようにすることであった。

ロイズは、2024 年 5 月に、改めて「国家の関与するサイバー攻撃に関する文言の要件を更新する」として、「市場通告 Y5433」を発出した。市場通告 Y5381 の発出後、ロンドン保険市場参加者は、国家の関与するサイバー攻撃から生じるエクスポージャーに対応するため、多くの特約を開発した。限定的ではあるが、ロイズは適切な根拠が提供される場合、市場通告 Y5381 に規定された要件の一部を満たさない条項の採用に同意した事例もある。ロイズはエクスポージャーのモニタリングを可能にするため、このような様々なタイプの条項を分類している。

今回の市場通告Y5433では、現状のサイバー戦争免責条項を7つのタイプに分類し、タイプごとに「使用状況の監視」や「使用不可」など監視アプローチや、対応方法を通知している。

なお、ロイズは、サイバー保険市場におけるシステミックリスクは、国家の関与するサイバー攻撃のみから発生するものでもなく、国家の関与するサイバー攻撃すべてがシステミックリスクをもたらすわけではないことを認識しているとしながら、国家が支援するサイバー攻撃の動機・目的は、他国の機能の混乱である可能性があり、そのような攻撃は、システミックな障害を引き起こすように設計されている可能性があるという見解を持っている。

c. 再保険会社の「サイバー戦争免責条項」への対応

再保険会社によって、「サイバー戦争免責条項」に関する方針は異なるようであるが、ミュンヘン再保険は、元受会社に導入を要請しているようであり、2024 年 1 月の再保険の更改において主要な再保険プログラムにおいて「サイバー戦争免責条項」を導入済みであるとの情報がある[34]。

大手保険ブローカーのエーオンは、「戦争免責条項については、市場で一貫性が欠けている。多くの保険会社や再保険会社は、依然として契約ごとに文言を交渉している」としている[35]。

（4）リスクの定量化・モデリング

米国の格付会社 AM Best は、保険会社の格付プロセスにおけるサイバー保険関連の

[34] Abbie Day, “Munich Re secures cyber war exclusions at 1.1 as wording tension dissipates”（Insurance Insider, 2024.1）
[35] Aon, “U.S. Cyber Insurance: Market Trends and Opportunities”（2024.4）

ストレステスト[36]、およびモデリングにおける問題点につき指摘している[37]。伝統的に、ストレステストの尺度の１つは、巨大損害（catastrophic loss）に対するエクスポージャーであり、これは、予想最大損害額（Probable Maximum Loss：以下「PML」）で表される。サイバー保険は、新しい保険種目であるため、PML の計算方法は、各保険会社で異なっている。

またサイバー保険のモデリングに関して、AM Best は、現時点で巨大損害が発生していないため、まだ理論的な段階にあり、モデリングの結果を検証できないことも課題として挙げている。今後サイバー保険市場が発展し、サイバー保険に対する保険会社や再保険会社のリスクアペタイトが高まるにつれて、今後数年で保険事故等に関するデータが増加し、モデルは改良されていくと予想しつつも、現時点では不確実性が多く、変動要素も多数あるとしている。

世界の保険会社約 80 社の CEO で構成される、保険業界のシンクタンクであるジュネーブ協会（Geneva Association）は、極めて巨大なサイバーリスクを定量化する方法を改善することは、サイバー保険の規模と範囲をさらに拡大し、補償ギャップを解消するうえで極めて重要であるとしたうえで、サイバー保険市場の成長に伴い、集積リスクを管理するための引受手法も進化してきているとしている。また、より質の高いデータや洞察が様々な情報源から収集され、サイバーリスクの状況を把握するのに役立っていると指摘している[38]。

Allianz Commercial は、今日の複雑な相互接続性[39]とサービスプロバイダーへの依存により、サイバーリスクのモデリングは重要になっているとして、顧客のリスクを評価する際、被保険者のエクスポージャーだけをモデリングしているわけではなく、拡張ネットワーク、クラウド、ソフトウェア、デジタルサービスプロバイダーもモデリングしている[40]。

６．おわりに

本稿では、サイバーリスクの現況、関連法規制の動向、および保険市場の概況とともに、最近のサイバー保険における課題と保険業界の対応について説明してきた。

サイバー保険の重要性やニーズは、今後一層高まると予想され、損害保険業界は、そ

---

[36] 「ストレステスト」とは、想定される将来の不利益（ストレス）が生じた場合の財務等への影響に関する分析を指す。

[37] AM Best, “Global Tensions Elevate the Risks for Cyber Coverage”（2024.11）

[38] Geneva Association, “Cyber Risk Accumulation: Fully tackling the insurability challenge”（2023.11）

[39] 「相互接続性」とは、共通に使用される通信手順などを規定することにより、ネットワークを構成する交換機，コンピュータ，端末などのすべての装置が相互に通信ができることを指す。

[40] Mirko Zorz, “The future of cyber insurance: Meeting the demand for non-attack coverage”（Help Net Security, 2024.10）

れらに適切に応えるとともに、サイバー保険を持続的かつ健全に発展させる必要がある。そのためには、損害保険会社は、サイバーリスクに関する定量データの収集・分析およびモデリングの構築等による適切なリスク管理が重要である。また、顧客企業に対しては、サプライチェーンも含めたサイバーリスクの予防に向けた技術的な対策提供サービスに加えて、従業員教育など、提供するサービスのさらなる充実も図るべきである。さらに、今後の保険商品・サービスを検討するうえでは、中小企業など企業規模や、業種特性など、様々な目線で検討することも必要であると考える。

技術革新に伴い、サイバーリスクを巡る状況も常に「進化」していることから、わが国の損害保険業界も、最新のサイバーリスクの動向や他国の損害保険業界の動向を注視しつつ、適切に対応することが重要である。

＜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「米国を中心とするサイバー保険市場の動向」損保総研レポート第 138 号（損害保険事業総合研究所、2022.2）
・浦上純「世界における主要な補償ギャップの現状と対策についてー最新のサイバーリスク動向を含めてー」損保総研レポート第 143 号（損害保険事業総合研究所、2023.6）
・金奈穂「サイレント・サイバーリスクを巡る動向ー米国・イギリスを中心にー」損保総研レポート第 126 号（損害保険事業総合研究所、2019.1）
・佐々木美稲「SOAR とは？セキュリティ運用の自動化により得られる３つのメリット」（NRI Secure, 2024.10）
・佐藤智行「保険事業における AI 利用に関する海外主要規制・監督機関等の主な取組み」損保総研レポート第 147 号（損害保険事業総合研究所、2024.6）
・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）
・濵田和博「国家の関与するサイバー攻撃とサイバー保険の戦争免責条項について」損保総研レポート第 141 号（損害保険事業総合研究所、2022.12）
・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）
・IBM「データ侵害のコストに関する調査 2024」（2024.10）
・Abbie Day, “Munich Re secures cyber war exclusions at 1.1 as wording tension dissipates”（Insurance Insider, 2024.1）
・Allianz Commercial, “Allianz Risk Barometer”（2025.1）
・Allianz Commercial, “Cyber security resilience 2024”（2024.10）
・AM Best, “Global Tensions Elevate the Risks for Cyber Coverage”（2024.11）
・Aon, “U.S. Cyber Insurance: Market Trends and Opportunities”（2024.4）
・Aon, “U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance”（2024.8）
・Beth Musselwhite, “UK business leaders struggle to recognise cyber risk as a financial threat: Resilience”（Reinsurance News, 2024.12）
・Camille Joyce Lisay, “AXA XL launches insurance coverage for Gen AI risks”（Insurance Business, 2024.10）
・Chantal Kapani, “Are SMEs paving the way for cyber attacks on larger companies?”（Insurance Times, 2024.5）
・Check Point Research, “2024 Cyber Security Report”（2024）
・Corrs Chambers Westgarth, “Australia introduces Comprehensive Cyber Security Legislation”（2024.11）
・CyberCube, “Projecting Cyber Insurance Growth: A 10-Year US Market Outlook”（2024.9）

・Deloitte, “Global Cyber Threat Intelligence (CTI): Annual Cyber Threat Trends”（2024.3）
・Geneva Association, “Cyber Risk Accumulation: Fully tackling the insurability challenge”（2023.11）
・GOV.UK, “Official Statistics: Cyber security breaches survey 2024”（2024.4）
・Hiscox, “Cyber Readiness Report 2024”（2024.4）
・Howden, “Cyber Insurance: Risk, resilience and relevance”（2024.6）
・IAIS, “Global Insurance Market Report (GIMAR)”（2024.12）
・Joe Toppe, “Email cyberattacks spike 24% in 2023”（PropertyCasualty360,2024.11）
・Matthew Lerner, “US casualty tops reinsurers’ concerns as renewal negotiations begin”（Business Insurance, 2024.9）
・Mirko Zorz, “The future of cyber insurance: Meeting the demand for non-attack coverage”（Help Net Security, 2024.10）
・Munich Re, “Cyber Insurance: Risks and Trends 2024”（2024.4）
・Munich Re, “War exclusions on the cyber market – Taking the next step”（2023.4）
・NAIC, “Report on the Cyber Insurance Market”（2024.10）
・New York State Department of Financial Services, “Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks”（2024.10）
・Resilience, “Midyear 2024 Cyber Risk Report”（2024.8）
・Sarah, “Jolly EC takes action against member states over NIS2 cybersecurity rules”（2024.11）
・Stuart Collins, “Europe’s insurers will move to clarify cover for AI risks”（Commercial Risk, 2024.11）
・Swiss Re, “Reality check on the future of the cyber insurance market”（2024.11）
・Terry Gangcuangco, “Aviva to roll out cyber product for UK micro-SMEs”（Insurance Business, 2023.10）
・The insurer, “Munich Re retains “vast majority” of cyber business after war exclusion”（2024.9）
・WTW, “War exclusions in cyber policies: the important details”（2023.6）

＜参考ウェブサイト＞

・アーンスト・アンド・ヤング　https://www.ey.com/
・外務省　https://www.mofa.go.jp/
・東京海上日動　https://www.tokiomarine-nichido.co.jp/
・Allianz　https://www.allianz.com/
・AM Best　http://www.ambest.com/
・AON　https://www.aon.com/
・Artemis　https://www.artemis.bm/
・Business Insurance　https://www.businessinsurance.com/
・Center for Strategic and International Studies (CSIS)　https://www.csis.org/
・IAIS　https://www.iaisweb.org/

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

・Lloyd's of London　https://www.lloyds.com/

・LMA　https://www.lmalloyds.com/

・Marsh　https://www.marsh.com/au/home.html

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

・NAIC　https://content.naic.org/

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

・PwC　https://www.pwc.com/

・Reinsurance News　https://www.reinsurancene.ws/

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

・Travelers　https://www.travelers.com/

・WTW　https://www.wtwco.com/en-US