# 企業のサイバーセキュリティリスクとサイバー保険

富永　健司


## ▌要　約▐

1. 近年、社会のデジタル化の進展等を背景として、サイバー空間（仮想空間）とフィジカル空間（現実空間）との融合が進む中、サイバー空間におけるセキュリティリスクが高まっている。金融を通じたサイバーセキュリティリスクへの対応策としてサイバー保険が挙げられる。
2. 保険監督者国際機構（IAIS）の調査によれば、現状、サイバー保険の元受収入保険料の国・地域別シェア（2020年時点）は、米国が53%と最も高く、次いで英国が 34%となっている一方、日本のシェアは 3%と相対的に低水準となっている。日本損害保険協会の調査においても、サイバー保険に加入していると回答した国内企業は調査対象の 7.8%に留まっており、国内でサイバー保険の普及に向けてさらに取り組みを推進する余地があることが示唆される。
3. 国内上場企業等のサイバーセキュリティ関連事故は、多種多様な業種の企業において発生しており、同事故が発生した後の資金面の備えを提供するサイバー保険の必要性は総じて高いと推察される。
4. サイバー保険の普及に向けた主な課題として、（1）企業のサイバーセキュリティに対する意識及びサイバー保険の認知度向上、（2）企業によるサイバーセキュリティ対策のさらなる強化、（3）損害保険会社におけるサイバー保険ビジネスの持続可能性向上、が挙げられる。日本及び世界において企業に対するサイバー保険のさらなる普及と共に、サイバーセキュリティリスクへの対応の進展が注目される。


**野村資本市場研究所　関連論文等**


・富永健司「自然災害リスクと金融の役割―CAT ボンドの活用可能性を中心に―」『野村サステナビリティクォータリー』2023 年夏号。
・板津直孝「サイバーセキュリティに関わる SEC の開示規則案―広範囲に及ぶインシデントの懸念と情報開示―」『野村サステナビリティクォータリー』2023 年春号。
・江夏あかね・門倉朋美「米国証券市場におけるサイバーセキュリティリスク対処に向けた SEC 規則案の公表」『野村サステナビリティクォータリー』2023 年春号。

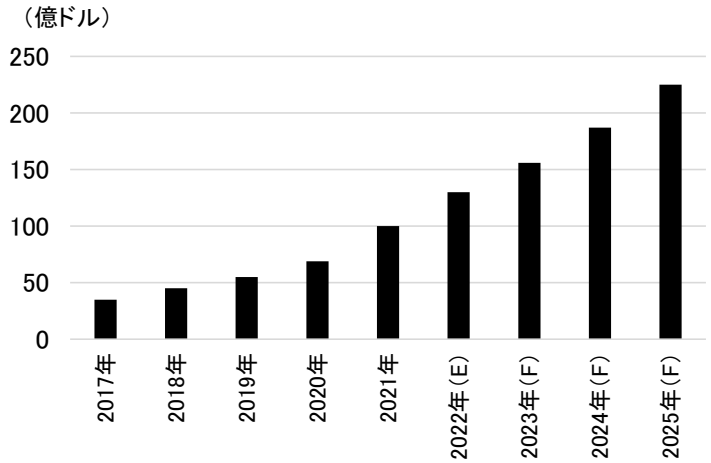
# Ⅰ　重要性が高まるサイバーセキュリティリスクへの対応

近年、社会のデジタル化の進展等を背景として、サイバー空間（仮想空間）とフィジカル空間（現実空間）との融合が進んでいる[1]。昨今では新型コロナウイルス禍への対応を通じて、人々のデジタル技術の活用が加速したことで、サイバー空間はより一層、人々の生活にとって身近な空間となっている。他方、サイバー空間においては、ランサムウェア[2]による被害、標的型攻撃[3]による機密情報の窃取等のセキュリティ上の脅威が深刻化している。

サイバー空間におけるセキュリティリスクが高まっていることに鑑みると、企業にとってサイバーセキュリティの強化に向けた取り組みは重要な経営課題であると言える。企業による、金融を通じたサイバーセキュリティリスクへの対応策としてサイバー保険への加入が挙げられる。世界ではサイバー犯罪[4]の増加等を背景として、同保険の市場規模が拡大しつつある。スイス・リー・インスティチュートによれば、サイバー保険市場の規模は、2022 年に約 130 億ドル（推定値）となり、2017～2022 年の期間に約 3 倍に拡大した。同社は、同保険市場の規模が 2025 年に 225 億ドルに達すると予想している（図表 1）[5]。

本稿では、サイバー保険の概要と世界及び日本の同保険市場の概況を示し、今後の課題について論考する。

**図表 1　サイバー保険の収入保険料**




（注）　E は推定値、F は予想値を示す（推定値及び予想値は、スイス・リー・インスティチュートによる）。
（出所）スイス・リーウェブサイト、より野村資本市場研究所作成

1　警察庁「令和 5 年警察白書」2023 年 8 月 25 日。
2　感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラム（警察庁ウェブサイト）。コンピューターウイルス等の悪意あるプログラムを指すマルウェアの一種。
3　機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。
4　インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等、情報技術を利用した犯罪（警察庁ウェブサイト）。
5　Swiss Re, “What you need to know about the cyber insurance market,” August 28, 2023.

# Ⅱ　サイバー保険の概要とサイバー保険市場の概況

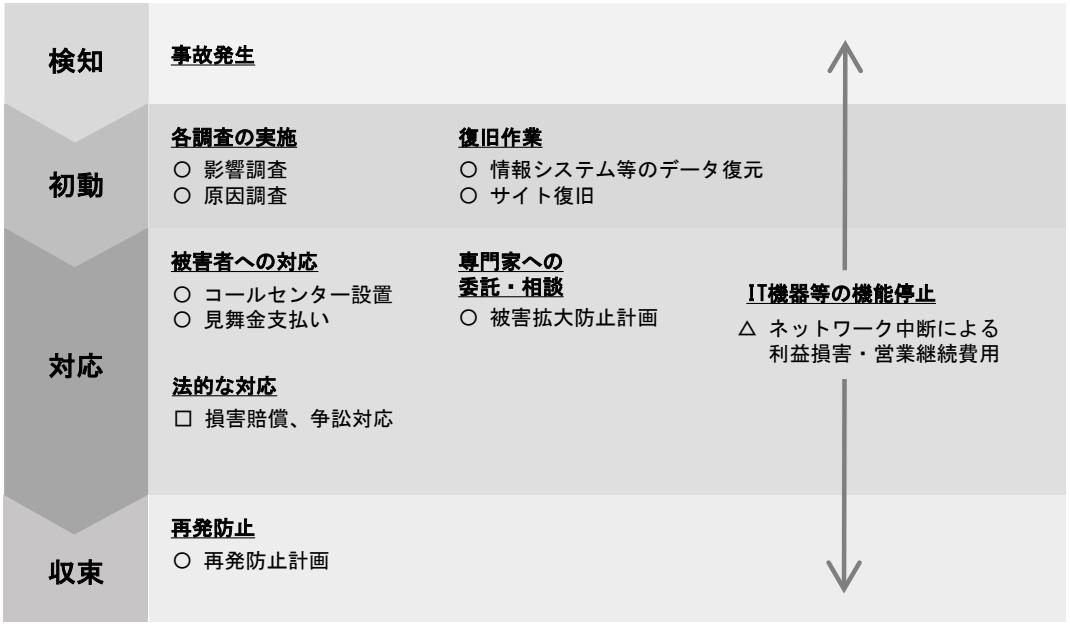
本章では、サイバー保険の概要、世界及び日本のサイバー保険市場の概況を示す。

## １．サイバー保険の概要

サイバー保険とは、サイバーセキュリティリスクに起因して発生する様々な損害に対応するための保険である[6]。同保険の補償内容は、（1）損害賠償責任、（2）事故対応費用、（3）利益損害・営業継続費用、に大別される（図表 2）。（1）は、被保険者が法律上負担する損害賠償金や、争訟費用等による損害が対象となる。具体的には、顧客や取引先等の第三者に対する損害賠償責任を補償する。（2）は、サイバー事故に起因して一定期間内に生じた費用が対象となる。具体的には、事故原因調査、法律相談等に関連する各種費用を補償する。（3）は、ネットワークを構成する IT（情報技術）機器等が機能停止することによって生じた利益損害（喪失利益・収益減少防止費用）や営業継続費用が対象となる。

具体的な事故の例としては、情報漏洩又はその恐れ、ネットワークの所有・使用・管理に起因する他人の業務阻害、サイバー攻撃に起因する他人の身体傷害・財物損壊等が挙げられる。

図表 2　サイバー攻撃への対応の流れ（一例）




（注）　○は事故対応費用、△は利益損害・営業継続費用、□は損害賠償責任。
（出所）一般社団法人 日本損害保険協会「サイバー保険」、より野村資本市場研究所抜粋

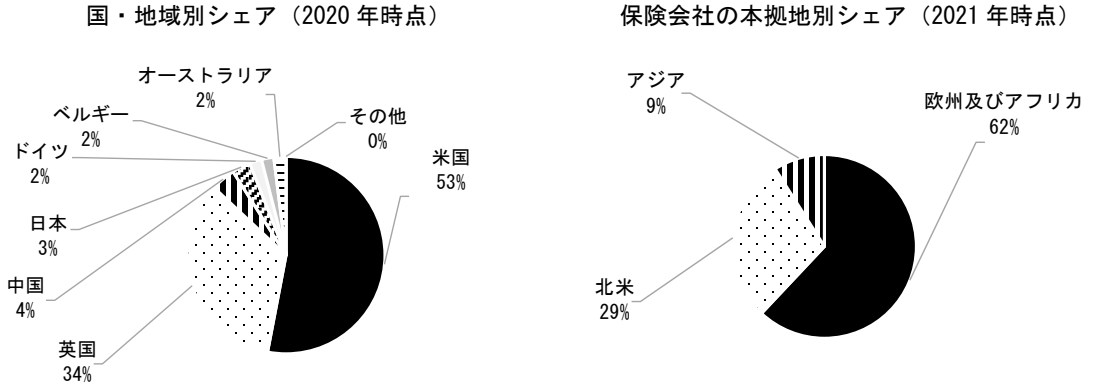
6　一般社団法人日本損害保険協会「サイバー保険」。

## ２．世界のサイバー保険市場

保険監督者国際機構（International Association of Insurance Supervisors、IAIS）[7]は 2023 年 4月、サイバー保険市場の調査レポートを公表した[8]。IAISは、同レポートの中で、世界的なサイバーセキュリティリスクの脅威や IT への依存度の増大を背景として、損害保険においてのサイバー保険の存在感が今後も高まるとの見方を示している。本節では、同調査レポート及びその他の関連調査等を用いて、世界のサイバー保険の状況について示すこととする。

IAIS の調査によれば、世界のサイバー保険の元受収入保険料は、2020 年時点で計 60 億ドル（13 か国・地域による報告）、2021 年時点で計 137 億ドル（19 か国・地域による報告）だった。保険料の国・地域別シェア（2020 年時点）は、米国が 53%と最も高く、次いで英国が 34%、日本は 3%となっている（図表 3）。他方、サイバー保険を提供する保険会社が本拠を置く地域別に保険料の内訳を見ると、2021 年時点で、62%が欧州及びアフリカ、29%が北米となっている。これは、米国外に本拠を置く保険会社・グループが、米国内において、相対的に多くのサイバー保険を提供していることが主因である。実際、米国においてサイバー保険を提供する上位の保険会社・グループを見ると、米国外が本拠の保険会社・グループが多く含まれている（図表 4）。

**図表 3　サイバー保険の元受収入保険料**




（出所）International Association of Insurance Supervisors (IAIS), “Global Insurance Market Report,” December 2022 、IAIS, “Global Insurance Market Report Special Topic Edition Cyber,” April 2023、より野村資本市場研究所作成

[7] 保険分野の監督に関する原則、基準、ガイダンス等の策定及び実施の支援を行う基準設定機関。200 以上の国・地域の保険監督当局がメンバーとなっている。

[8] International Association of Insurance Supervisors, “Global Insurance Market Report Special Topic Edition Cyber,” April 2023.

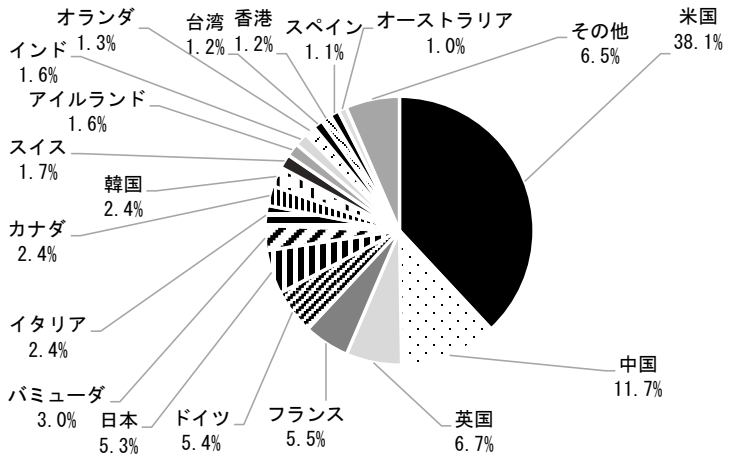
図表 4　米国のサイバー保険の引き受けを行う保険会社上位 20 社（2021 年）

| 順位 | 企業・グループ名 | 本拠地 | 保険料 |
|---|---|---|---|
| 1 | チャブ・グループ | スイス | 4.7 |
| 2 | フェアファックス・フィナンシャル・グループ | カナダ | 4.4 |
| 3 | アクサ・グループ | フランス | 4.2 |
| 4 | 東京海上ホールディングス | 日本 | 2.5 |
| 5 | アメリカン・インターナショナル・グループ（AIG） | 米国 | 2.4 |
| 6 | トラベラーズ・カンパニーズ | 米国 | 2.3 |
| 7 | ビーズリー・グループ | 英国 | 2.0 |
| 8 | CNA フィナンシャル・コーポレーション | 米国 | 1.8 |
| 9 | アーチ・インシュアランス・グループ | 米国 | 1.7 |
| 10 | アクシス・キャピタル・ホールディングス | バミューダ | 1.6 |
| 11 | チューリッヒ・インシュアランス・グループ | スイス | 1.5 |
| 12 | リバティ・ミューチュアル・グループ | 米国 | 1.4 |
| 13 | SOMPO ホールディングス | 日本 | 1.3 |
| 14 | BCS フィナンシャル・コーポレーション | 米国 | 1.3 |
| 15 | ハートフォード・ファイア・アンド・キャス・グループ | 米国 | 1.2 |
| 16 | ミュンヘン・リー・グループ | ドイツ | 1.2 |
| 17 | スイス・リー・グループ | スイス | 1.0 |
| 18 | アリゲニー・コーポレーション | 米国 | 0.9 |
| 19 | ダブリュー・アール・バークレー・コーポレーション | 米国 | 0.8 |
| 20 | バークシャー・ハサウェイ・グループ | 米国 | 0.7 |

（注）　本拠地は親会社の本拠地。保険料の単位は億ドル。
（出所）National Association of Insurance Commissioners, “Report on the Cyber Insurance Market,” October 18, 2022、より野村資本市場研究所作成

サイバー保険市場の相対的な規模を考える際の一つの目安として、世界の保険全体の元受保険料のシェアが挙げられる。サイバー保険の元受収入保険料の上位国である米国、英国等において、サイバー保険市場におけるシェアは、世界の保険全体の元受収入保険料についてのシェアを上回る傾向が見られており、保険市場全体と比べて、相対的にサイバー保険の引き受けが浸透している可能性があると言える（図表 5）。

図表 5　世界の元受収入保険料の国・地域別シェア




（注）　2021 年時点。
（出所）IAIS, “Global Insurance Market Report,” December 2022、より野村資本市場研究所作成

IAIS の調査によれば、2021 年時点のサイバー保険の純支払保険金は 42 億ドルであり、このうち約 3 分の 2 が米州、約 3 分の 1 が欧州及びアフリカ地域で発生した。対象を 100 万ドル超の保険料を報告した国・地域に限定すると、各保険会社・グループの元受収入保険料に占める純支払保険金の平均的な割合は約 48%だった。他方、同国・地域における回答者について、損害保険事業全体の純支払保険金の割合は約 38%である。IAIS は、これらの数値は直接的な比較はできないものの、損害保険事業の中で、サイバー保険事業の収益率が低い水準に留まっていることが示唆されるとの見方を示している。

サイバー保険の支払限度額の最大値は平均で 5,000 万ドル（範囲は 245 万～1.22 億ドル）、平均的な支払限度額は 359 万ドル（範囲は 29 万～1,114 万ドル）だった[9]。また、サイバー保険は、損害保険事業全体と比べて、再保険の割合（出再割合）が高い。具体的には、対象を 100 万ドル超の保険料を報告した 9 か国・地域に限定すると、サイバー保険の出再割合が平均で約 54%であるのに対して、損害保険事業全体の同割合は約 29%に留まる。サンプル全体では約 88%がサイバー保険に対して再保険を付していると回答した。

サイバー保険を提供するほとんどの保険会社は、データの機密性、損害賠償責任、データ漏洩、ネットワークセキュリティ、事業中断、サイバー恐喝、コミュニケーション及びメディア関連の責任等に関連するリスクについて、サイバー保険の補償対象としている（図表 6）。

サイバーセキュリティに関する具体的な脅威に関する設問では、ランサムウェア攻撃（身代金を払うまで会社のシステムへのアクセスを妨害）の割合が最も高い。その他、プライバシーの侵害（個人情報の紛失又は盗難）、外部のサプライヤーやパートナーのサイバー障害による事業中断、在宅勤務の従業員（フィッシング[10]やソーシャルエンジニアリング[11]の攻撃）等の回答割合が相対的に高くなっている（図表 7）。

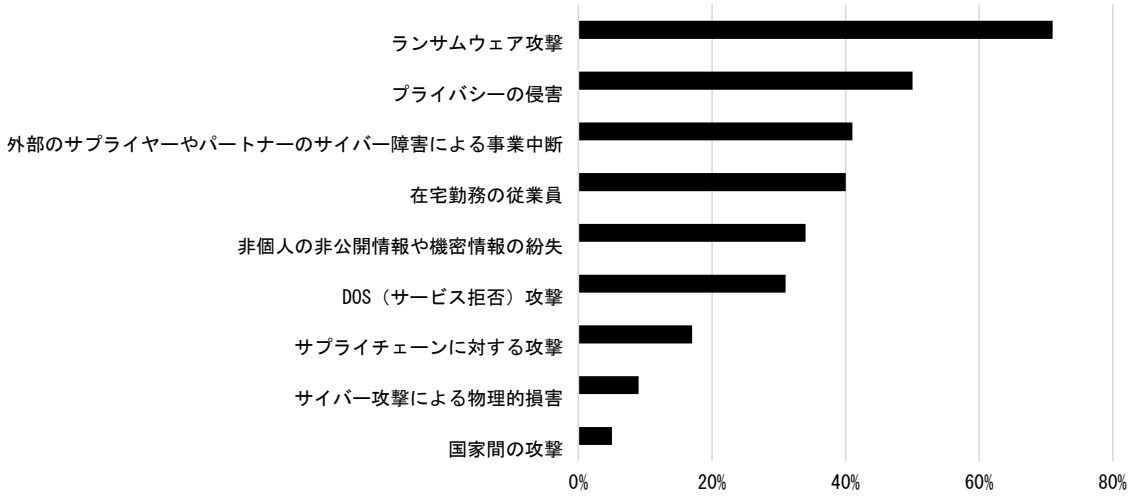
**図表 6　サイバー保険の補償対象となるリスク例**

| リスクの種類 | 回答割合（%） |
|---|---|
| データの機密性 | 88 |
| 損害賠償責任 | 88 |
| データ漏洩 | 88 |
| ネットワークセキュリティ | 84 |
| 事業中断 | 84 |
| サイバー恐喝 | 84 |
| コミュニケーション及びメディア関連の責任 | 84 |
| 技術障害 | 68 |
| サイバー詐欺及び窃盗 | 68 |
| 連鎖的な事業中断 | 52 |
| その他 | 12 |

（出所）IAIS, “Global Insurance Market Report Special Topic Edition Cyber,” April 2023、より野村資本市場研究所作成

[9] International Association of Insurance Supervisors, “Global Insurance Market Report Special Topic Edition Cyber,” April 2023.
[10] 銀行等の実在する企業を装って電子メールを送り、その企業のウェブサイトに見せかけて作成した偽のウェブサイト（フィッシングサイト）を受信者が閲覧するよう誘導し、当該サイトでクレジットカード番号や識別符号を入力させて金融情報や個人情報を不正に入手する行為（警察庁「令和 3 年警察白書」2021 年 7 月）。
[11] 人間の心理的な隙や行動のミスにつけ込み、情報通信技術を使用せずに、ID・パスワード等を搾取する方法（警察庁「令和 3 年警察白書」2021 年 7 月）。

図表 7　サイバーセキュリティに関する脅威




（注）　ランサムウェア攻撃は「身代金を支払うまで会社のシステムへのアクセスを妨害」、プライバシーの侵害は「個人情報の紛失又は盗難」、在宅勤務の従業員は「フィッシングやソーシャルエンジニアリングの攻撃」、DOS 攻撃は「正規ユーザーのネットワークへのアクセスを制限」との例が設問には含まれている。

（出所）IAIS, “Global Insurance Market Report Special Topic Edition Cyber, ” April 2023、より野村資本市場研究所作成

サイバー保険の引き受けに対して、保険会社は、保険契約の項目の見直し、再保険等を活用した各種のリスク軽減・移転策を実施している。サイバー保険会社によるリスク軽減・移転に関連する動きとして、世界でサイバー保険商品を提供する英損害保険会社であるビーズリーによる大災害債券[12]（Catastrophe bond、CAT ボンド）の発行が挙げられる。

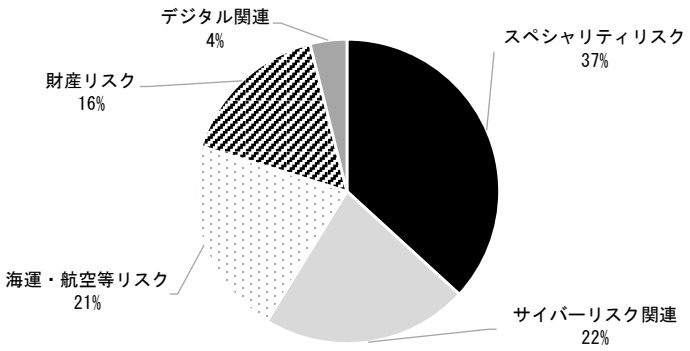
ビーズリーは、英国に本拠を置く保険会社であり、損害保険、海上保険、専門保険、サイバー保険等の幅広い範囲の保険を提供している。同社は、欧州、アジア、米国等でビジネスを展開しており、近年、サイバーセキュリティリスクを対象とした保険を強化している。同リスクに関連する保険引受額は、引受額全体の約 22%を占める（図表 8）。同社のサイバーセキュリティリスク関連の引受額は 2021 年頃より拡大しており、2022 年においては前年比で 4 割増となった。同社は、サイバーセキュリティリスクの重要性の高まりを踏まえて、サイバー保険には高い水準の需要が継続するとの見解を示している。

こうした中、ビーズリーは 2023 年 1 月、世界初となるサイバーセキュリティリスクを対象とする CAT ボンドを、4,500 万ドル発行した[13]（図表 9）。大規模なサイバー事故の発生時に CAT ボンドの元本が減額される条件であるトリガーは、インデムニティ型である。同トリガーは、事前に定めた損害額を超える実損額が補償される仕組みである。具体的には損害額が 3 億ドル超の大規模なサイバーセキュリティリスク関連のイベントが対象となる。

[12] CAT ボンドの詳細については、富永健司「自然災害リスクと金融の役割―CAT ボンドの活用可能性を中心に―」『野村サステナビリティクォータリー』2023 年夏号、を参照。

[13] Beazley, “Beazley launches market’s first cyber catastrophe bond,” January 9, 2023.

図表 8　ビーズリーの引受収入保険料の内訳




（注）　2022 年時点。スペシャリティリスクは、役員・取締役に対する賠償責任、合併・買収、等に関連するもの。
（出所）Beazley, “Annual Report 2022” 、より野村資本市場研究所作成

図表 9　サイバーセキュリティリスクを対象とする CAT ボンド

| スポンサー | ビーズリー |
|---|---|
| 対象 | サイバーセキュリティリスク |
| 発行額 | 4,500 万ドル |
| トリガーの種類 | インデムニティ型 |
| 発行時期 | 2023 年 1 月 |

（出所）Artemis, “Beazley cyber cat bond (Cairney)”、を基に野村資本市場研究所作成

ビーズリーは、当該 CAT ボンドについて、今後 10 年でビジネス需要に対応して成長する見込みのサイバー関連の市場における新たな資金調達手段として革新的なものである、との見解を示している。

ビーズリーによれば、同債券に対しては、保険リンク証券（ILS）に投資を行うファンド等により投資が行われた。具体的には、米国を本拠とする運用会社であるファーマット・キャピタル・マネジメント（Fermat Capital Management）等が含まれている。同社の共同創業者兼マネージングディレクターであるジョン・セオ氏は、サイバー保険市場における適切な投資機会を数年間注視してきたと述べると共に、当該取引はサイバーセキュリティ関連のリスクに対する資本市場からの投資を後押しし、将来のサイバー保険に関連する ILS 市場の基礎となる、との見解を示した。

なお、ビーズリーはサイバーセキュリティリスクを対象とする CAT ボンドについて、2023 年 1 月に続き、同年 5 月に 2,000 万ドル、同年 9 月に 1,650 万ドルの発行を行っている[14]。

[14] Artemis, “Beazley sponsors third cyber catastrophe bond, $16.5m Cairney Ⅲ,” September 15, 2023.

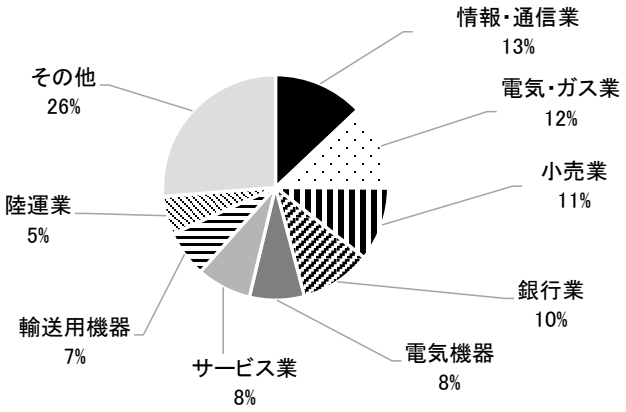
## ３．日本の状況

### １）国内上場企業等のサイバーセキュリティ関連事故

国内の上場企業及びその子会社等のサイバーセキュリティに関連する事故（不正アクセス行為〔ランサムウェアによる攻撃を含む〕、サイバー攻撃、システムの誤設定による情報の不正閲覧、メールの誤送信、個人情報を含む情報機器の紛失、そして、これらの事故に伴う個人情報の漏洩被害等）について、2019 年 1 月～2023 年 6 月の期間において、企業のプレスリリース、日経新聞等のメディアニュースにより発生状況を確認すると、様々な業種の企業において、サイバー事故が発生していることが確認できる（図表 10）。

サイバー事故が、多種多様な業種・企業において発生している実態に鑑みると、同事故が発生した後の資金面の備えを提供するサイバー保険の有効性が示唆される。

**図表 10　国内上場企業のサイバーセキュリティ関連事故の業種別内訳**




（注）　対象は 2019 年 1 月～2023 年 6 月の期間における国内上場企業のサイバーセキュリティに関連する事故（不正アクセス行為〔ランサムウェアによる攻撃を含む〕、サイバー攻撃、システムの誤設定による情報の不正閲覧、メールの誤送信、個人情報を含む情報機器の紛失、そして、これらの事故に伴う個人情報の漏洩被害等）。合計約 256 件。
（出所）企業のプレスリリース、日経新聞等のメディアニュース、各種資料、を基に野村資本市場研究所作成

### ２）日本企業のサイバー保険への加入状況

日本では個人情報保護法が成立・施行された 2003～2005 年頃より、個人情報漏洩に関する保険の提供が活発化した[15]。その後、世界的規模で生じているサイバーセキュリティに対する脅威の深刻化等に伴い、サイバーセキュリティの確保を図ることが必要との認識により、2014 年にサイバーセキュリティ基本法が制定され、サイバーセキュリティに関する社会的な意識が高まった。

こうした中、2012 年頃よりサイバー攻撃による被害を包括的に補償する保険が登

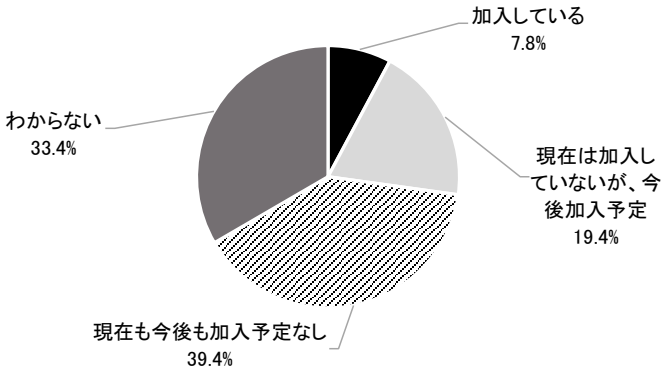
[15] 「個人情報の漏洩防げ　関連市場拡大　シュレッダー好調／保険各社は新商品」『産経新聞』2005 年 5 月 23 日。

場した[16]。具体的な例として、米保険大手 AIG 傘下の AIU 保険によるサイバーエッジ保険等が挙げられる。同社は 2004 年より個人情報漏洩保険を販売していたが、当該保険により、損害賠償に加えて、サイバー事故の調査による費用や逸失利益等を対象とすると共に、補償対象地域を全世界に広げた。2015 年には、東京海上日動火災保険が国内の大手損害保険会社で初めてサイバー保険を発売した[17]。その後、損害保険各社の参入が本格化し、サイバー保険商品の拡充が進んだ。

他方、IAIS の調査によれば、サイバー保険の元受収入保険料の日本のシェアは、前述のとおり、2020 年末時点で 3%に留まる（前掲図表 3）。当該数値は、世界の保険全体の日本のシェア（5%）を下回っており、サイバー保険市場にさらなる拡大の余地があることが示唆される。同様に、日本損害保険協会の調査によれば、サイバーリスク保険については、依然として普及余地があるとの見方が示されている（図表 11）。同協会が公表した国内企業 1,535 社を対象としたサイバーリスク意識・対策実態調査[18]においては、サイバーリスク保険に加入していると回答した企業は全体の 7.8%だった。また、全体の約 2 割が「今後加入予定」と回答した。

サイバーリスク保険に加入しない理由を聞いた設問では、「保険の補償内容や保険料についてよく知らないため」との回答割合が 40.7%と最も多く、次に「サイバー攻撃に伴う損害額（必要な補償額）がわからないため」が同 24.5%だった。また、同調査では、「サイバー被害を受ける可能性が低いため」との回答割合が 18.8%だった結果を受けて、危機意識の低さがうかがえるとの指摘がなされている。こうした結果を踏まえると、国内においては現状、サイバー保険の普及に向けて、さらに取り組みを推進する余地があるものと考えられる。

**図表 11　サイバーリスク保険への加入状況**




（出所）一般社団法人 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 年 12 月、より野村資本市場研究所作成

16 「大手損保各社、サイバー保険を相次ぎ投入―認知度高まり市場活性化」『日刊工業新聞』2015 年 4 月 15 日。
17 「サイバー保険、現場に解　東京海上日動の教学大介さん」『日本経済新聞』2023 年 4 月 21 日。
18 一般社団法人日本損害保険協会「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 年 12 月。

日本政府が2021年9月に閣議決定した「サイバーセキュリティ戦略」においては、社会のデジタルトランスフォーメーション[19]と共に、サイバーセキュリティの確保に向けた取り組みを同時に推進することが重要であるとの見方が示されると共に、特に予算の制約がある中小企業を念頭に、安価かつ効果的なセキュリティサービスや保険の普及に取り組むとの方針が示された。

さらに、経済産業省が、国内企業において経営者主導のもとで組織的なサイバーセキュリティ対策を実践するための指針として2023年3月に公表した「サイバーセキュリティ経営ガイドライン Ver3.0」においても、リスクの把握と対応計画策定についての事項の金融の仕組みに関連するものとして、サイバー保険への加入が挙げられている。このようなサイバー保険に対する政策的な動きについても、国内におけるサイバー保険の普及を後押ししていくものと期待される。

## Ⅲ 今後の課題

近年、社会のデジタル化の進展等を背景として、サイバー空間におけるセキュリティリスクが高まる中、企業にとってサイバーセキュリティの強化に向けた取り組みは重要な経営課題となっている。日本政府が、社会のデジタルトランスフォーメーションと共にサイバーセキュリティの確保にむけた取り組みを同時に推進することが重要との認識を示す中、サイバー保険の重要性が高まっている。サイバー保険の普及に向けた今後の主な課題としては、（1）企業のサイバーセキュリティに対する意識及びサイバー保険の認知度向上、（2）企業によるサイバーセキュリティ対策のさらなる強化、（3）損害保険会社におけるサイバー保険ビジネスの持続可能性向上、が挙げられる。

### １．企業のサイバーセキュリティに対する意識等の向上

前述の IAIS の調査に基づくと、サイバー保険の元受収入保険料の国・地域別シェア（2020 年時点）は、米国が全体の 53%と最も高く、次いで英国が 34%となっている一方、日本のシェアは 3%と相対的に低水準となっている。日本損害保険協会の調査においても、サイバーリスク保険に加入していると回答した国内企業は調査対象の 7.8%に留まっており、国内で同保険の普及に向けてさらに取り組みを推進する余地があることが示唆される。同調査からは、国内企業のサイバー保険の加入率向上に向けて、サイバーセキュリティに対する意識向上、サイバー保険の認知度向上等の課題が窺える。取り組みを進める際に重

[19] 企業が外部エコシステム（顧客、市場）の破壊的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第3のプラットフォーム（クラウド、モビリティ、ビッグデータ／アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネス・モデルを通して、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること（経済産業省　デジタルトランスフォーメーションに向けた研究会「DX レポート～IT システム『2025 年の崖』の克服と DX の本格的な展開～」2018 年 9 月 7 日）。

要となるのは、サイバーセキュリティに関連する事故の実態を把握・理解し、自社の事業に照らしたリスク認識を行うことである。

現状、国内上場企業等のサイバーセキュリティ関連事故は、多種多様な業種の企業において発生しており、同事故が発生した後の資金面の備えを提供するサイバー保険の必要性は総じて高いと推察される。投資家においては、サイバーセキュリティをエンゲージメントのテーマとして挙げる動きもでてきている[20]。企業と投資家の同テーマに関する対話において、サイバー保険をトピックとして議論していくことも重要なポイントとなる可能性がある。

## ２．企業によるサイバーセキュリティ対策のさらなる強化

サイバー保険は、企業にとってサイバー攻撃を受けた際の財務負担を軽減する役割が期待される一方、必ずしも全ての被害を補償するものではない点については留意が必要であろう。例えば、ランサムウェアやサイバー恐喝等により生じた身代金の支払いについては、補償の対象とならないことがある[21]。その意味では、企業は、サイバー攻撃をできる限り回避するための対策の強化に継続して取り組む必要がある。具体的には、対応方針の策定、リスク管理体制の構築、資源（予算、人材等）の確保、対応計画の策定を含む多面的な取り組みが必要と言える[22]。

## ３．損害保険会社におけるサイバー保険ビジネスの持続可能性向上

保険及び再保険会社によるサイバー保険の引き受けにおける主要課題としては、サイバーセキュリティリスクに関するエクスポージャーの計測がある。IAIS によれば、同エクスポージャーの計測上の課題として、5 点を挙げている[23]。

1 点目は、サイバーセキュリティリスクの進化である。サイバーセキュリティ関連では、日々新たな脅威が発生し、構造的な変化によって損害の発生状況が変わる可能性がある。そのため、過去のデータのみによるリスク計測は将来の損害を過小評価する恐れがある。

2 点目は、限定的なサイバーセキュリティ関連の損害データである。サイバーセキュリティリスクは、比較的新しいリスクであること、開示が限られていること、分類方法が多様であること、等の理由により、サイバーセキュリティ関連の損害データを入手・分析することが困難と考えられる。

---

[20] Principles for Responsible Investment, “Engaging on cyber security: Results of the PRI collaborative engagement 2017-2019,” April 22, 2020. 詳細は、江夏あかね「機関投資家から見たサイバーセキュリティ―サステナブルな情報化社会実現に向けた論点整理―」『野村サステナビリティクォータリー』2022 年秋号を参照。

[21] 国内では、一般に、ランサムウェアの被害に遭い、データ復旧のために支払った身代金はサイバー保険の補償対象にならない（日本損害保険協会「サイバー保険」）。

[22] 経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」2023 年 3 月 24 日。

[23] IAIS, “Cyber risk underwriting Identified challenges and supervisory considerations for sustainable market development,” December 2020.

3 点目は、保険契約者の脆弱性評価の問題である。保険契約者のサイバーセキュリティリスクの評価は、技術・工学的な評価ではなく、ガバナンス及びプロセスに重点が置かれており、契約者のシステム及びリスクの理解が必要であり評価が複雑になる可能性がある。

4 点目は、集積リスク（accumulation risk）である。あるイベント及び環境において、保険リスク又は補償対象が集中することで、複数の保険契約において、複数年及び地域で、多額の保険金の支払いが発生する可能性がある。こうしたリスクは、一般に集積リスクと分類されるが、企業等による共通のソフトウェアおよびハードウェアの使用による IT サービスの集中化、IT システムと保険契約者の相互接続性等が主因と考えられる。

5 点目は、非明示的エクスポージャー（non-affirmative exposure）である。非明示的エクスポージャーは、サイバーセキュリティ関連の損害の補償を明示的に含まないかつ除外もしない保険契約から発生する。具体的には、サイバー攻撃が火災につながることで発生した損害が、火災保険によって補償されるといったケースがある。IAIS によれば、多くの保険会社は、従来型の保険にサイバーセキュリティ関連事故による損害を補償対象から除外する文言を含める等のリスク軽減策を講じているが、こうした除外文言についての法的な有効性は必ずしも明確ではない[24]。

損害保険会社は、以上のような課題を踏まえて、サイバー保険ビジネスの持続可能性の向上を図っていくことが必要である。こうした取り組みを進めるにあたり、サイバー保険の引受能力向上の観点から、再保険や CAT ボンドといったリスク移転策の活用についても検討が必要と言える。

このように、サイバー保険の普及等を通じてサイバーセキュリティの確保・向上を進めるためには、企業、損害保険会社を含めた市場参加者による多面的な取り組みが求められる。日本及び世界において企業に対するサイバー保険のさらなる普及と共に、サイバーセキュリティリスクへの対応の進展が注目される。

[24] IAIS, “Global Insurance Market Report Special Topic Edition Cyber,” April 2023.