

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

主席研究員 浦上 純

目 次

1. はじめに

2. 世界における補償ギャップの概況

- (1) 補償ギャップを生み出すリスクの評価
- (2) 年金リスクにおける補償ギャップの現状と対策
- (3) 医療費リスクにおける補償ギャップの現状と対策
- (4) 自然災害リスクにおける補償ギャップの現状と対策

3. サイバーリスクにおける補償ギャップの現状

- (1) サイバーリスクにおける補償ギャップの定義
- (2) サイバーインシデントによる経済損失額
- (3) サイバーインシデントによる保険損害額
- (4) サイバーリスクにおける補償ギャップの縮小に向けた課題

4. サイバーリスクに対する補償ギャップ縮小に向けた取組

- (1) サイバーインシデント対策
- (2) サイバー保険の普及に向けた取組

5. おわりに

＜補足資料＞ 調査報告書「諸外国における自然災害による被害の縮小や
保険普及に向けた取組の現状、課題、対策」（2023.3）の概要

要旨

近年、気候変動、IT 技術の進化、および人口動態の変化等、人類を取り巻く環境の様々な変化により、事故やイベントの発生時において、それに伴う経済損失額やあらかじめ備えておくべき必要補償額と、実際の補償額との差（補償ギャップ）が拡大しているとされている。

本稿では、2023 年 3 月に公表された GFIA の報告書に基づいて、年金リスク、医療費リスク、自然災害リスク、およびサイバーリスクの 4 つを取り上げ、それぞれについて、その概要および補償ギャップの規模感、それぞれのリスクにおける課題、ならびに補償ギャップの縮小に向けた対策について説明する。また、特に近年その脅威が増大しているサイバーリスクについては、最新のデータ・情報を交え、損害保険会社の取組事例等を紹介する。

4 つのリスクに共通していることは、補償ギャップの縮小に向けて、民間の保険会社による取組が重要であることに加えて、政策立案者による支援、後押しはいずれも不可欠であることが挙げられる。また、サイバーリスクにおける補償ギャップの縮小においては、損害保険業界として、特に「サイバー保険の普及推進」、「サイバーインシデントの被害縮小に向けた活動推進」、および「官民連携取組」を進める必要があるものと考えられる。わが国損害保険業界においても、サイバーリスクの領域を、保険事業の成長や収支安定化としての側面だけではなく、現在、世界で最も懸念されているリスクにおける補償ギャップの縮小に向けて貢献を図る絶好の機会としてとらえ、さらなる取組を推進していくことが求められている。

1. はじめに

近年、経済の発展とともに、気候変動、IT 技術の進化、および人口動態の変化等、人類を取り巻く環境の様々な変化により、事故やイベントの発生時において、それに伴う経済損失額やあらかじめ備えておくべき必要補償額と、実際の補償額との差（補償ギャップ）が拡大しているとされている。

より具体的には、地球温暖化に伴う気候変動の影響により、自然災害が頻発化・甚大化し、世界各地で大規模な損害が発生しており、またデジタル化の進展や新たなテクノロジーの導入により、データの利用も指数関数的に増加する中で、サイバーリスク¹の脅威も飛躍的に増大している。加えて、高齢化社会の進展、新興国における富裕層の台頭、および中産階級の拡大など、人口動態や社会構造の変化が消費者のニーズや経済システムにまで影響を及ぼしている。その結果、個人にとっては、自らの財産、収入、健康を十分に守ることができない状況に陥る可能性が増え、企業にとっても、資産の安全性や将来的な業績の見通しに対して懸念を抱く状況となっている²。

こうした中、国際保険協会連盟（Global Federation of Insurance Associations：以下「GFIA」）³は 2023 年 3 月、世界的に発生している補償ギャップの実態と、それを埋めるための対策をまとめた報告書⁴を公表した。同報告書では、昨今の情勢を踏まえ、世界において補償ギャップを生み出している最も懸念すべき 4 つのリスク領域として、「年金」、「医療費」、「自然災害」、および「サイバー」を選定している。

本稿では、これらの年金リスク、医療費リスク、自然災害リスク、およびサイバーリスクを取り上げ、それぞれの補償ギャップの現状と対策について説明したのち、特にサイバーリスクについては、直近の情報を中心に、補償ギャップの観点で、その現状や縮小に向けた取組についてより詳しく説明する⁵。

なお、サイバーリスクに関しては、当研究所でもこれまで、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し⁶、さらに 2021 年 1 月および 2022 年 2 月には米国を中心とするサイバー保険市場の動向を、また、2022 年 12 月には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、損保総研レポートで取り上げている⁷。

¹ ジュネーブ協会では、サイバーリスクについて、「データやサービスの機密性、可用性、完全性を損なう情報通信技術の使用から生じるあらゆるリスク」と定義している。

² GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3)

³ 意見発出、情報交換活動の強化、および国際監督規制の議論における保険業界のプレゼンス向上を目的に 2012 年に設立された、各国の保険協会を通じ、（再）保険会社の利益を代表している団体である。

⁴ GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3)

⁵ 詳細は、GFIA 報告書の原文、または日本損害保険協会作成の日本語仮和訳「グローバルプロテクションギャップとそれを埋めるための提言」（2023.6）を参照願う。

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）

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）、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）、濱田和博「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）

また、自然災害リスクについては、当研究所では自然災害リスクに関する補償ギャップに焦点を当て、その縮小に向けた諸外国の保険会社や国際機関の取組について調査を行い、2023 年 4 月に報告書⁸を刊行していることから、内容の重複を極力避けるため、GFIA の報告書の内容を中心に記載している。

最後に、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。

2. 世界における補償ギャップの概況

本項では、2023 年 3 月に公表された GFIA の報告書に基づいて、世界における補償ギャップの概況について説明するとともに、その規模、拡がりの速度、人々の生命や生活への影響度合、および保険業界との関連性等の観点で、特に重要性が高いとしているリスクのうち、年金リスク、医療費リスク、および自然災害リスクにおける補償ギャップの現状について、その他の文献によるデータや情報も交えて、概要を説明する。なお、サイバーリスクについては、後記 3.以降で説明する。

(1) 補償ギャップを生み出すリスクの評価

GFIA は、近年の経済や社会の様々な環境変化、気候変動、技術革新、および人々の意識の変化を踏まえて、「年金」、「サイバー」、「医療費」、「自然災害」、「金融市場」、「障害・罹患・死亡」、「モビリティ」、「個人・企業賠償責任」、「家屋・財産（除く自然災害）」、「事業継続」、「サプライチェーンの混乱」、「戦争・テロリズム」、および「環境賠償責任」の 13 領域を、補償ギャップの観点で影響が大きく、また（再）保険業界にも密接な関係があるリスクであるとしている。報告書では、各領域のリスクに対して、①経済的な重要度、②リスクの増大傾向、③官民による補償の程度、④民間保険会社による保険手当の可能性、および⑤人間の生活に与える影響度合の、5 つの基準に基づいて評価を行っている（図表 1、図表 2 参照）。

この評価分析によると、年金リスク、サイバーリスク、医療費リスク、および自然災害リスクが、補償ギャップの観点でその深刻性が際立っている。年金リスクと医療費リスクは、経済的に重要性が高く、かつ人口動態の変化に大きく影響されるとし、特に医療費リスクについては、医療技術の進歩や気候変動等の影響も受けるため、変化の激しいリスク分野であるとしている。また、自然災害リスクは気候変動の影響を最も受けるリスクである一方で、実際に支払われた保険損害額は、経済損失額全体の 40%未満に留まっているとしている。さらに、サイバーリスクについては特に地政学的に不安定な現在の状況において、政府、企業、個人に対する重要性が高まっており、

⁸ 損害保険事業総合研究所「諸外国における自然災害による被害の縮小や保険普及に向けた取組の現状、課題、対策」（2023.3）

「今世紀最大のリスク」となる可能性がある」と指摘している。

調査時点での 4 つのリスクにおける補償ギャップの概算金額については、年金リスクが 1 兆ドル超、サイバーリスクが 9,000 億ドル超、医療費リスクが 8,000 億ドル超、自然災害リスクが 1,000 億ドル超であると推定している（補償ギャップの定義、および算定方法については後記（2）以降を参照願う）。加えて、各リスクにおける補償ギャップ額の地域別割合についても、図表 3 のとおり公表しており、地域によってリスクの影響度合は異なっている。なお、これら 4 つの補償ギャップは、少なくとも合計で約 2 兆 8,000 億ドルとなり、世界の GDP⁹の約 3%に相当している。

図表 1 補償ギャップに関するリスクの重要性を評価するための 5 つの基準（注 1）

リスク	対象		評価基準				
	個人	企業	①経済的な重要度	②リスクの増大傾向	③官民による補償の程度	④保険手当の可能性（注 2）	⑤人的影響
年金	○		4	3	2	○	4
サイバー		○	3	4	0	△	2
医療費	○		4	3	2	○	4
自然災害	○	○	2	3	3	○	3
金融市場	○	○	3	1	1	△	0
障害・罹患・死亡	○		3	1	2	○	4
モビリティ	○	○	2	1	3	○	3
個人・企業賠償責任	○	○	2	1	3	○	2
家屋・財産（除く自然災害）	○	○	2	1	3	○	3
事業継続	○	○	4	2	2	×（個人） △（企業）	0
サプライチェーンの混乱		○	2	3	1	△	1
戦争・テロリズム	○	○	2	3	4	×	4
環境賠償責任		○	1	4	0	△	2

（注 1）表中の数字は、それぞれの大きさ（あるいは可能性）を、0（小）～4（大）のスケールで示している。

（注 2）○は保険手当可能、△は部分的に保険手当可能、×は保険手当不可能を表している。

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them”（2023.3）をもとに作成）

図表 2 各評価基準の分析に関する補足説明

基準	内容（抜粋）
①経済的な重要度	○WHO の調査（注 1）によると、医療費の年間支出総額は、世界の GDP の約 10%を占めている。 ○年金の年間支出総額は、世界の GDP の 12%から 14%を占めており、そのうち 70%は政府の支出である。 ○パンデミックは事業継続に深刻な影響を与えるものであり、世界銀行の分析（注 2）によると、全世界の企業の売上高は、2020 年 10 月から 2021 年 1 月までの 4 カ月間で、パンデミック発生前と比べて平均で 27%減少した。

⁹ 国際通貨基金（IMF）の統計によると、2021 年の世界の GDP 合計は、93 兆 9,539 億ドルである。

基準	内容（抜粋）
②リスクの増大傾向	○特にサイバーリスクと環境賠償責任のリスクは、今後 10 年間で大幅に増加するものと予測される。 ○世界の 65 歳以上の人口は、2010 年には総人口の 7.6%であったが、2020 年には 9.3%に拡大している。 ○2015 年から 2019 年にかけて、医療費の年間支出総額は 18%増加した。
③官民による補償の程度	○モビリティ、個人・企業賠償責任、家屋・財産（自然災害を除く）は、民間保険会社が広く補償を提供しているリスクである。 ○年金、医療費、自然災害、障害・罹患・死亡、事業継続に関する民間保険会社の商品は存在するが、価格、認知度、規制環境により普及状況は様々であり、民間事業者と政府との共同負担の仕組みも存在する。
④保険手当の可能性	○サイバー、金融市場、サプライチェーンの混乱、環境賠償責任は、民間保険会社が一定部分の補償を提供することができるが、それぞれに異なる課題があり、保険の手当により完全に補償できるとまでは言えない。 ○一部のリスクは保険による手当に馴染まないため、その対応に向け、保険業界として、公共部門とその役割について検討する必要がある。
⑤人的影響	○単なる経済損失としてではなく、苦痛・幸せに直結する、人への影響度合を考慮すると、年金、医療費、障害・罹患・死亡、戦争・テロリズムは、より深刻なリスクであると言える。

（注 1）World Health Organization, “Global spending on health: Weathering the storm”（2020.12）

（注 2）World Bank, “Tracking an Unprecedented Year for Businesses, Everywhere”（2021.2）

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them”（2023.3）をもとに作成）

図表 3 各リスクにおける補償ギャップ額の地域別割合（注 1）

リスク	全世界		北米	南米	欧州	アジア	アフリカ・中東
	補償 ギャップ額（注 2）	補償 ギャップ率（注 3）					
年金	1 兆ドル超	—	20%	7%	29%	29%	15%
サイバー	9,000 億ドル超	約 99%	41%	4%	23%	28%	5%
医療費	8,000 億ドル超	—	5%	18%	5%	53%	20%
自然災害	1,000 億ドル超	約 60%	58%	—	—	—	—

（注 1）本図表では、地域別割合が 40%以上の場合は濃色で、20%以上の場合は淡色で網掛けしている。
また、「—」は出典に記載がないことを示す。

（注 2）補償ギャップの推定値に幅がある場合には、下限値を記載している。

（注 3）当該リスクによる経済損失額に占める補償ギャップ額の割合を指す。

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them”（2023.3）をもとに作成）

（2）年金リスクにおける補償ギャップの現状と対策

a. 補償ギャップの定義、現状、および課題

年金リスクにおける補償ギャップの定義、現状、および課題をまとめると、図表 4 のとおりである。

図表 4 年金リスクにおける補償ギャップの定義、現状、および課題

項目	内容（抜粋）
定義	○報告書では、年金リスクにおける補償ギャップの定義を、「次世代の退職者が合理的な生活水準（65%から 70%の所得代替率^{（注1）}）を維持するために必要な生涯収入の現在価値と、実際の退職時の貯蓄額およびその時点で予測されている年金制度からの流入額の現在価値との合計額との差」とするジュネーブ協会^{（注2）}の定義を採用している。 ○スイス再保険では、2021年に公表した報告書^{（注3）}において、補償ギャップの定義を、「現役時の収入の 65%に退職後の平均余命期間を乗じた金額から、現役時代の年金拠出金に、年金基金の収益と退職時の貯蓄額を加えた金額との差」であるとしている。
現状	○年金リスクにおける補償ギャップの総額を、約 51 兆ドルと試算しているが、この金額は生涯の累計であることから、他のリスクにおける補償ギャップと比較検証するために、一般的な労働期間とされる 40 年で割り戻し、将来のギャップ額を補てんするために必要となる年間のギャップ額を、約 1 兆ドルと試算している^{（注4）}。 ○スイス再保険が行った試算によると、新興国^{（注5）}の補償ギャップ総額だけで、年間で 5 兆 4,000 億ドル、受給期間の累積では 106 兆ドルに上るとしている^{（注6）}。
課題	○年間 1 兆ドルと推定された年金リスクにおける補償ギャップは、以下の要因等によってさらに拡大することが予想されている。 ・世界の 65 歳以上の人口比率が、2000 年の 6.8%から 2020 年には 9.3%に上昇し、退職後の平均余命の伸び^{（注7）}とともに、年金の受給者数の増加が見込まれる。 ・出生率が低下している国・地域では、年金制度への資金流入を支える労働人口が減少する傾向にある。 ・1人あたりの実質 GDP は、2050 年まで継続的に増加すると予想されており、生活水準の向上に伴い、年金額を充実させる必要性が加速している。 ○都市化の進展に伴い、核家族化が進み、家族による老後支援の弱体化が懸念される。 ○低金利を特徴とするマクロ経済環境による将来の年金基金や民間保険の資金準備の弱体化や、インフレ率の上昇によって、将来の退職所得水準の低下を招く可能性がある。

（注 1）現役時代の手取収入額と比較した、年金の受給開始時点における年金受給額の割合を示す。

（注 2）規制、リスク管理、気候変動等の保険業界にとって重要な課題について調査・研究を行っている世界の（再）保険会社約 70 社の CEO で構成される保険業界のシンクタンク組織である。

（注 3）Swiss Re Institute, “Emerging markets: the drive for sustainable retirements in an ageing world” sigma No2/2021（2021.5）

（注 4）この補償ギャップは、年金制度の仕組（賦課方式か積立方式か）、資産所有の役割、国民の経済事情、平均寿命、規制環境、（長期）医療の必要性、家族の役割などの違いにより、国によって異なるとしている。

（注 5）明確な定義はないものの、日欧米などの先進国に対して現在の経済水準はまだ低いものの、高い成長性を秘めた国々を言い、主に中南米、東南アジア、中東、東欧などの諸国を指す。

（注 6）スイス再保険では、試算にあたり新興国の総 GDP の 80%を占める 17 カ国について、国家統計機関等、入手可能なデータリソースを用いて、2019 年の価値ベースで調査している。

（注 7）OECD 諸国において、労働市場から退いた定年後の平均余命は、男性の場合、1970 年が 12 年だったのに対し、2020 年では 20 年、また女性の場合も、1970 年が 16 年だったのに対し、2020 年では 24 年と、いずれも 8 年間延びている。

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them”（2023.3）ほかをもとに作成）

b. 補償ギャップの縮小に向けた取組・提言

GFIA は、年金リスクにおける補償ギャップの縮小には、官民による緊密な連携が必要としたうえで、政府機関は適切な規制環境を構築するうえで重要な役割を果たすこと、また民間保険会社はそれを補完すべく、新商品を導入すること等を通じて貢献することが重要であるとし、それぞれが実行可能な取組として、図表 5 に示す 4 点を挙げている。

図表 5 年金リスクにおける補償ギャップの縮小に向けた取組概要

取組	内容（抜粋）
革新的で柔軟な商品の開発	○保険会社は、市場環境と顧客のリスクアペタイトに合わせ、革新的で柔軟な商品を開発し、下記のソリューションを提供していくことが重要である。 ・変動金利と固定金利の配分を顧客のリスクアペタイトにより調整可能な商品 ・再生可能エネルギー等の新しいタイプの投資対象と関連する年金商品 ・リバースモーゲージ^(注1)等、不動産などの非流動資産を流動資産として取り扱う年金商品
老後資金の必要性に対する消費者意識の醸成	○年金制度は概して複雑であり、国民の金融リテラシーが十分ではないことも想定されるため、年金制度に対する国民の理解に改善の余地がある。 ○政府は、老後に向けた貯蓄の重要性について国民を啓発する役割を担っており、特に若者への啓発活動を推進する必要がある。 ○民間保険会社は、老後資金の準備を促す役割を果たすべく、明確で透明性の高い貯蓄プランに関する情報を提供することが重要である。
年金制度への加入促進	○OECD 加盟国では 38 カ国中 19 カ国が強制加入の年金制度を導入しているが、加入者がその国の生産年齢人口 ^(注2) に対して 75%を超えているのは 12 カ国に過ぎず、強制加入制度であっても加入率は必ずしも高くはない。 ○その要因として、制度に登録されていない非正規労働者は、年金制度に拠出していないことや、制度対象外の業種が存在すること等が挙げられる。 ○年金加入を促進する手段として、自動加入方式と呼ばれる、年金制度には自動加入となるが、希望者は脱退（オプトアウト）が可能な制度が普及している。 ○米国では企業年金制度である 401k プラン ^(注3) の加入率向上を目的として、2006 年 8 月に「年金保護法（Pension Protect Act）」 ^(注4) が施行された結果、2021 年までに自動加入方式を導入した企業の割合は、22%から 74%に増加した。
税制優遇措置の導入	○従業員や雇用者に対する年金拠出を奨励するための税制優遇措置等のインセンティブは、年金制度を維持していくうえで不可欠な要素である。 ○政府は、従業員と雇用者の双方にメリットを付与することに加え、定年退職年齢の引上げを推進する政策の立案や、契約条件の適時的変更など個人年金制度の資金繰り悪化を招くような運営を認めないこと等も重要である。

(注1) 自宅を担保に生活資金を借り入れし、自らの持ち家に継続して住み続け、借入人が死亡したときに担保となっていた不動産を処分し、借入金を返済する仕組みを指す。

(注2) 15 歳から 64 歳までの人口を指す。

(注3) 米国における確定拠出型の企業年金制度で、1978 年米国内国歳入法（Internal Revenue Code of 1978）の条項名（第 401 条（k）項）にちなんで名付けられた。公的年金の上乗せとなる老後資金の積立を目的としており、そのため課税上の特典が与えられている。

(注4) 企業年金の財政基盤強化を主眼としており、自動化に関する法制度も整備された。

(出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3) ほかをもとに作成)

(3) 医療費リスクにおける補償ギャップの現状と対策

a. 補償ギャップの定義、現状、および課題

医療費リスクにおける補償ギャップの定義、現状、および課題をまとめると、図表 6 のとおりである。

図表 6 医療費リスクにおける補償ギャップの定義、現状、および課題

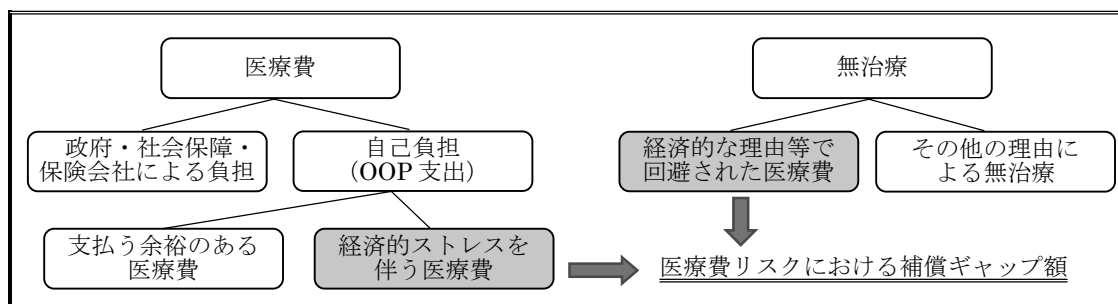
項目	内容（抜粋）
定義	○報告書では、医療費リスクにおける補償ギャップの定義を、図表 7 のとおり、「個人が負担した医療費のうち、経済的ストレスを伴う医療費と、経済的な理由等で回避されたと推定される医療費との合算値」としている。 ○医療費は本来、政府・社会保障や保険会社が負担する部分と、個人の自己負担部分（Out-of-Pocket：以下「OOP 支出」）に分かれているが、補償ギャップ額の対象とする OOP 支出を OOP 支出総額とした場合には、保険加入よりも自己資金での支払（自家保険）を好むという自主的な選択の要素も含まれることから、補償ギャップの定義においては、家計を圧迫するような経済的負担を強いる（経済的ストレスを伴う）費用^{（注1）}のみを含めるべきである。 ○経済的な理由等で回避されたと推定される医療費とは、健康維持のために本来支出されるべき費用でありながら、経済的な事情や医療インフラへのアクセス等の問題により、実際には支出されなかった費用としている。 ○スイス再保険では、医療費リスクにおける補償ギャップの定義を、2018 年に公表した報告書^{（注2）}の中で、「経済的ストレスを伴う医療費と、手頃な価格でないことを理由に治療を受けていない推定医療費との合算値」であるとしており、GFIA の定義付けもこれに準じたものとなっている。
現状	○報告書によると、2020 年の補償ギャップの規模は、8,000 億ドルから 4 兆 2,000 億ドルであると推定しており、これは世界の GDP の 1%から最大 5%近くにも及ぶとしている。 ○下限値としている 8,000 億ドルは、経済的ストレスを伴う OOP 支出のみを対象としている。 ○上限値は、これに加えて回避された医療費も含まれたものであり、この費用は公表されておらず、定量化が困難であるものの、推定で最大 3 兆 4,000 億ドル程度あるとされている。
課題	○公的機関や民間事業者が、毎年多額の資金を投じ、医療技術や新しい治療法等において進歩が見られているものの、高齢化、罹患率の上昇、新興国における人口増と中間層の増加による医療ニーズの高まりなどを受け、補償ギャップは年々拡大している。 ○経済的ストレスを伴う OOP 支出は、2009 年から 2019 年にかけて、全世界で毎年 4%から 5%のペースで拡大しており（図表 8 参照）、今後もこのペースで OOP 支出と回避された医療費のいずれもが拡大すると仮定すると、2030 年までに補償ギャップ額は、6 兆ドルから 6 兆 5,000 億ドルに達する可能性があるものと予想している。

（注 1）具体的には、習慣的な支出を控えたり、親族や金融機関からお金を借りたりすることにつながるような、「ストレスを伴う」OOP 支出を対象としており、WHO では、家計収入の 40%を超える医療費支出を目安として提示している。

（注 2）Swiss Re Institute, “The health protection gap in Asia: a modelled exposure of USD 1.8 trillion” (2018.10)

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3) ほかをもとに作成)

図表 7 医療費リスクにおける補償ギャップ額のイメージ



(出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3)、Swiss Re Institute, “The health protection gap in Asia: a modelled exposure of USD 1.8 trillion” (2018.10) をもとに作成)

図表 8 所得水準別の OOP 支出の伸びと医療費全体に占める割合 (2009 年~2019 年)

地域 (注)	OOP 支出の年平均伸び率		医療費全体に占める OOP 支出の割合	
	OOP 支出全体	経済的ストレスを伴う OOP 支出	2009 年	2019 年
低所得国・低中所得国	4.8%	2.2%	61%	57%
中高所得国	5.7%	10.2%	36%	32%
高所得国 (除く米国)	1.8%	2.8%	16%	16%
米国	3.2%	2.0%	13%	11%
全世界	3.5%	4.9%	19%	18%

(注) 世界銀行が開発した所得指標 (アトラス法) に基づき算出された、1 人あたりの国民総所得 (GNI) に応じて、低所得国 (1,085 ドルまで)、低中所得国 (1,086 ドルから 4,255 ドルまで)、中高所得国 (4,256 ドルから 13,205 ドルまで)、高所得国 (13,206 ドル以上) の 4 つに区分されている。

(出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3) をもとに作成)

b. 補償ギャップの縮小に向けた取組

GFIA は、医療費リスクにおける補償ギャップの縮小に向けて、公的医療インフラや保障の拡充と、民間の医療保険との組合せが必要であるとしたうえで、新たな保険販売チャネルの活用、予防医療を促進するための啓発キャンペーン、補完的な民間医療保険の推進、および付加的なヘルスケア・サービスの確立など、図表 9 に示す取組が重要であるとしている。

図表 9 医療費リスクにおける補償ギャップの縮小に向けた取組概要

取組	内容（抜粋）
新たな保険販売 チャネルの活用	○途上国では、健康保険や医療施設などのヘルスケアに対するアクセスについて、都市部と農村部とで大きな差が発生しており、ILO（国際労働機関）が2015年に行った調査^{（注1）}では、世界の農村人口の56%が健康保険に加入しておらず、都市部の22%と比べて著しく高い。 ○アクセス障壁の解消に向けて、新しい保険販路を構築することは、医療費リスクの補償ギャップ縮小において重要である。 ○タイでは、人口の約15%がセブンイレブンで日常的に買い物をし、かつ店舗の56%が都市部以外にある実態を踏まえ、2013年より同社店舗を通じて、医療保険を含めたマイクロインシュアランスを販売したところ、2017年には前年10%増の400万件もの契約が成立した。 ○米国でも同様の狙いで薬局を保険販売ネットワークに組み込んでいる。
予防医療を 促進するための 啓発キャンペーン	○健康意識を高め、予防を促進し、早期発見を促すことで、病気や深刻な病状を回避したり、管理したりすることが可能である。 ○ドイツでは、歯科予防を促進するため、歯科検診に係る財政的インセンティブ制度^{（注2）}を導入した結果、歯科治療費総額に占める虫歯治療費の割合が1997年は36.2%であったものが、2020年には22.1%に減少したのに対し、歯科予防費用の割合は1997年の49.8%から2021年には62.1%に拡大した。
補完的な 民間保険の推進	○公的保険や社会保障などの公的医療制度を民間医療保険で補完し、公的医療制度では対応できない治療費を民間医療保険でカバーすることは、補償ギャップの縮小に貢献する。 ○公的医療制度と民間医療保険との適切なバランスを見つけることは、世界各国の政府にとって重要な課題であるが、適切な規制枠組と、民間医療保険の選択肢を自国民に適切に提供することが、医療制度の成功のカギである。 ○フランスでは、公的医療制度が一般的な治療費の70%をカバーし、民間医療保険が、自己負担となる30%部分を補完する役割を果たしているが、民間医療保険の普及率は95%に達しており、補償ギャップの縮小に貢献している。
付加的なヘルスケア ・サービスの確立	○付加的なヘルスケア・サービスを提供し、健康管理を人々の日常生活により身近にすることで、シームレスな顧客体験^{（注3）}が生まれ、健康維持にポジティブに働くとし、主なサービスの事例として、以下の3つを挙げている。 ・予防や早期発見を支援し、金銭的なインセンティブを与えるサービス ・医師と対面、またはオンラインで相談できるサービス ・遠隔処方箋および遠隔薬局サービス ○アフリカのある医療保険会社では、保険契約者が健康的なライフスタイルを選択すると報酬が得られる会員制システムを導入しており、保険契約者が専用アプリを通じて、運動、健康食品の購入、健康診断などの行動記録を登録すると、それに応じて各種費用のキャッシュバックを受けることができる。 ○健康増進を目的とした同システム導入による医療費の減少は、保険会社にもメリットがあり、利用者は、非利用者と比較して平均で入院頻度が10%少なく、入院期間が25%短縮され、保険金請求額が14%減少した。

（注1）Xenia Scheil-Adlung, “Global evidence on inequities in rural health protection: New data on rural deficits in health coverage for 174 countries” (ILO,2015.5)

（注2）ドイツでは、年1回の歯科検診の受診を申告することにより、検診費用の60%の払戻を受けることができ、5年連続で受診すると70%に、10年連続で受診すると75%に還元率が高まる。

（注3）顧客が製品やサービスと接触し興味を持った時点から、購入して利用し続けるまでの、すべての企業との接点と、それらに基づき顧客が企業に対して持つ評価を指す。

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3) ほかをもとに作成）

(4) 自然災害リスクにおける補償ギャップの現状と対策

本項では、GFIA の報告書で取り上げている自然災害における補償ギャップの概況のうち、当研究所が 2023 年 4 月に刊行した調査報告書で取り上げていない内容を中心に説明する（調査報告書の概要については、巻末の補足資料を参照願う¹⁰⁾）。

a. 補償ギャップの定義、現状、および課題

自然災害リスクにおける補償ギャップの定義、現状、および課題をまとめると、図表 10 のとおりである。

図表 10 自然災害リスクにおける補償ギャップの定義、現状、および課題

項目	内容（抜粋）
定義	○報告書では、自然災害リスクにおける補償ギャップの定義を、「自然災害による経済損失額と実際に支払われた保険損害額との差」とし、一般に浸透している定義を採用している（注¹⁾）。 ○経済損失額の考え方については、「自然災害に関係するすべての損害および直接的・間接的な経済損失（注²⁾）の合算」としている。
現状	○自然災害による経済損失は、過去 50 年間で年平均 5% 増加しており、1990 年から 1999 年の 10 年平均で 1,190 億ドルであったものが、2010 年から 2020 年の 10 年平均で 2,160 億ドルに増加した（図表 11 参照）。 ○スイス再保険の報告書（注³⁾）によると、自然災害による保険損害額は、2012 年から 2021 年の 10 年平均で 810 億ドル、2017 年から 2021 年の 5 年平均では 1,110 億ドルとなっており、2022 年は 2021 年とほぼ同水準の 1,250 億ドルであったとしている（図表 12 参照）。 ○自然災害の頻度と深刻さが増し、リスクの高い地域の資産の経済価値が高まっているにもかかわらず、ここ数 10 年間、インフレ調整後の「GDP に占める自然災害による経済損失の割合」にあまり変動がないのは、自然災害の影響を受けにくい無形資産（データ駆動型ビジネスモデル（注⁴⁾）における GDP が増加していることにも起因していると、スイス再保険では分析している。
課題	○スイス再保険の報告書（注⁵⁾）によると、経済発展と都市化は同規模の自然災害に対してより高い経済損失を生み出しており、資産価値が 2000 年から 2020 年の間に 3 倍に、世界人口が 1975 年から 2020 年の間に 40 億人から 78 億人に、人口密度が過去 50 年間で 1km²あたり 32 人から 60 人に増加したことが、経済損失の絶対額を増加させているとしている。 ○補償ギャップ率は、欧州や北米では損害額の 30%から 40%に留まる一方、低所得国市場では一貫して大きく、100%近くに達していることから、これらの地域で大規模な自然災害が発生した場合、財政面で国際援助に依存しやすくなっている。 ○補償ギャップを拡大させる要因の 1 つとして、人口と資産が自然災害リスクの高い地域に移動していることを挙げている。

（注 1）自然災害リスクにおける補償ギャップの定義については、損害保険事業総合研究所「諸外国における自然災害による被害の縮小や保険普及に向けた取組の現状、課題、対策」（2023.3）も参照願う。

（注 2）ここで言う間接的な経済損失とは、物的損害に起因する事業中断に伴う経済損失などを指す。

（注 3）Swiss Re Institute, “Natural catastrophes and inflation in 2022: a perfect storm” sigma No1/2023（2023.3）

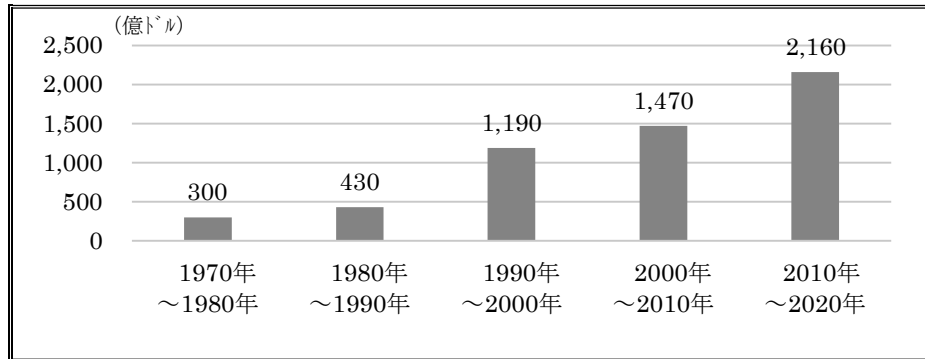
¹⁰⁾ 詳細については、損害保険事業総合研究所「諸外国における自然災害による被害の縮小や保険普及に向けた取組の現状、課題、対策」（2023.3）を参照願う。

(注4) あらゆるデジタル化されたデータを利活用し、企業の経営やビジネスに活かす手法を指す。

(注5) Swiss Re Institute, “Natural catastrophes in times of economic accumulation and climate change” sigma No2/2020 (2020.4)

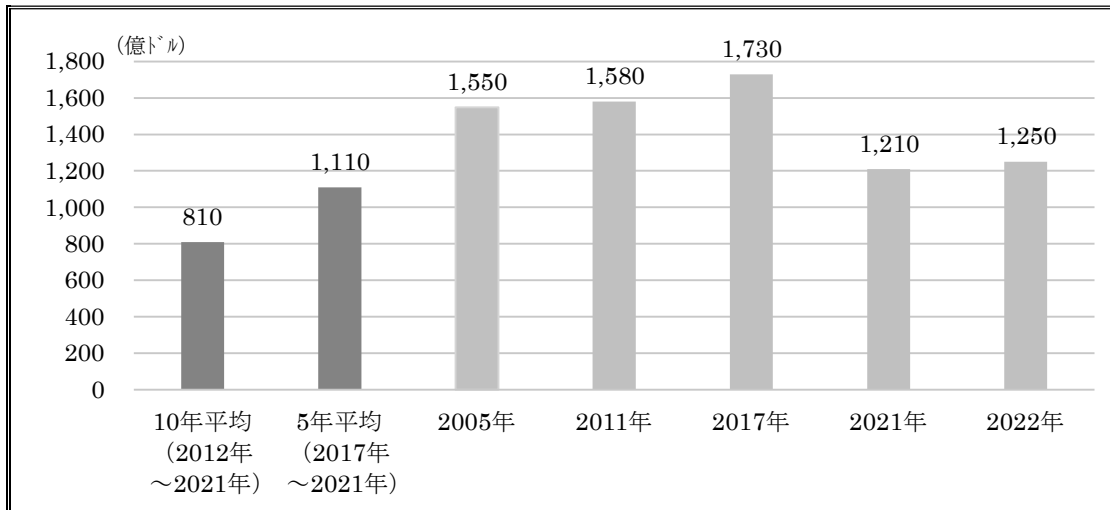
(出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3) ほかにもとに作成)

図表 11 10年ごとの自然災害による年間平均経済損失額



(出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3) ほかにもとに作成)

図表 12 近年の自然災害による保険損害額（10年平均、5年平均、および主要年）(注)



(注) これまでの自然災害による保険損害額のワースト5の年度を、主要年として表示している。

(出典：Swiss Re Institute, “Natural catastrophes and inflation in 2022: a perfect storm” sigma No1/2023 (2023.3) をもとに作成)

b. 補償ギャップの縮小に向けた取組

GFIA は、自然災害リスクにおける補償ギャップの縮小に向けて、官民のステークホルダーが取り得る手段は様々であるとしつつ、革新的なリスク移転商品や新たな販

売チャネルの開発、予防と適応（防災・減災対策）、政府支援プログラム、およびグローバルな再保険へのアクセスの促進など、図表 13 に示す 4 点を有効な取組事例として挙げている。

図表 13 自然災害リスクにおける補償ギャップの縮小に向けた取組概要

取組	内容（抜粋）
革新的なリスク移転 商品や新たな販売 チャネルの開発	○マイクロインシュアランス、パラメトリック保険、CAT ボンド等、地域のニーズに合致した保険商品を検討する必要がある、特にマイクロインシュアランスは新興国での補償ギャップ縮小に向けて、効果的な商品になり得る。 ○先進国・新興国のいずれの市場においても、既存の保険代理店・ブローカーチャネルに加え、デジタル・IT 技術を駆使した新たな商品や販売チャネルを活用することにより、民間保険会社の保険商品へのアクセス性が高まり、自然災害発生時の保険損害額の割合を増やすことが可能である。
予防と適応 （防災・減災対策）	○防災・減災とリスク適応の面で、先進国、途上国のいずれにおいても、政府主導で自然災害リスクのエクスポージャー削減に向けた取組が進められている。 ○土地の利用や建築基準の策定など、様々な状況において予防や適応策^{（注1）}を実施し、リスクの高い地域での建築を奨励しないこと等を通じて、保険金支払の如何を問わず、損失額そのものを減少させることが、補償ギャップに対処するための重要な要素になる。
政府支援 プログラム	○政府は、公的補償制度だけに依存するのではなく、保険業界の枠組に応じて、政府支援プログラム、官民パートナーシップ、自然災害基金への拠出の義務化、およびリスクプールなど、政府の財政負担を軽減し、自然災害からの早期の経済回復と、保険浸透率の向上につながるような施策を検討する必要がある^{（注2）}。 ○市場の違いにより政府が選択できる支援プログラムは様々であるとしつつも、政府が自然災害リスクを対象とする公的保険に対して、いかに積極的な当事者になり得るかが補償ギャップ縮小のカギとなる。
グローバルな再保険 へのアクセス促進	○自然災害リスクの地理的集中を軽減するために、グローバルな再保険市場へのアクセスを促進することは極めて重要であり、国際的なリスクの分散は、よりレジリエンスのある（再）保険リスク・ポートフォリオの構築に役立つ。 ○外国保険会社の国内進出要件、付保規制、グローバル・データ・モデリングの制限等、再保険のクロスボーダー取引の縮小につながり、リスク分散効果の低下をもたらすような法律や規制の見直し検討も視野に入れる必要がある。

（注1）GFIA の報告書では、具体例として、「より良い復興（ビルドバックベター）」や日本の耐震基準等が取り上げられている。

（注2）GFIA の報告書では、自然災害に対する官民合同の保険制度の事例として、フランスの巨大自然災害保険（Cat Nat）が取り上げられている。

（出典：GFIA, “Global Protection Gaps and Recommendations for Bridging Them”（2023.3）ほかをもとに作成）

3. サイバーリスクにおける補償ギャップの現状

サイバーリスクは、Allianz Global Corporate & Specialty¹¹が2023年1月に公表した報告書¹²において、保険会社を含む世界94カ国のリスク管理専門家が懸念するリスクとして、前年に続き、1位に挙げられている。また、GFIAの報告書においても、サイバー攻撃の脅威はこの10年で急激に増大しており、サイバーリスクに対する財政面での補償ニーズが高まる一方で、サイバーリスクに対する保険市場の対応は、まだ発展途上の段階にあることから、サイバーリスクにおける補償ギャップの動向とその対策については、特に注視が必要であるとされている。

そこで本項では、サイバーリスクにおける補償ギャップに関して、より詳細なデータを調査のうえ、サイバーリスクにおける補償ギャップの定義、サイバーインシデントによる経済損失額、サイバーインシデントによる保険損害額、およびサイバーリスクにおける補償ギャップの縮小に向けた課題について説明する。

(1) サイバーリスクにおける補償ギャップの定義

GFIAの報告書では、サイバーリスクにおける補償ギャップの定義を、「サイバー攻撃による一次的な経済損失額と、実際に支払われた保険損害額との差」としている。ここで言う一次的な経済損失とは、人身傷害、物理的な資産の損害、金銭盗難・詐欺、サイバー身代金・恐喝、事業中断、データ・ソフトウェアの損失、規制・法的防御、および事故対応コストなどが該当するとしており、風評被害や事業機会の喪失等の二次的な経済損失は、他のリスクとの比較検証の観点から含めていない。

この定義に基づくGFIAによる試算によると、サイバーリスクにおける補償ギャップは、一次的なサイバー攻撃による経済損失額である9,500億ドルに対して、サイバー保険で支払われた保険損害額は、わずか60億ドルに過ぎなかったとしている¹³。

(2) サイバーインシデントによる経済損失額

a. サイバー攻撃の実態

(a) サイバー攻撃件数の動向

サイバーセキュリティの大手ソリューション事業者であるCheck Point Software Technologiesは、2022年のサイバー攻撃の傾向に関するデータを発表した¹⁴。これによると、2022年に1つの組織が受けた週平均のサイバー攻撃件数は、2021年と比較して全世界で38%増加、日本では29%増加したとしている。

¹¹ アリアンツグループ傘下の事業体であり、企業向け保険の引受を中心に事業展開を行っている。

¹² Allianz Global Corporate & Specialty, “Allianz Risk Barometer: Identifying the major business risks for 2023” (2023.1)

¹³ 経済損失額の算出については、後記3.(2)b.を、また保険損害額の算出については、後記3.(3)b.を参照願う。

¹⁴ Check Point Software Technologies, “Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks” (2023.1)

このサイバー攻撃件数の増加は、より小規模かつ俊敏になったハッカー集団等によってもたらされたとしており、特に新型コロナウイルス感染症の世界的な流行によって浸透しているリモートワーク環境や、オンライン学習に移行した教育機関が、十分なサイバーセキュリティ対策が施されていないことを要因に、集中的に標的にされた可能性があるとしている。また、この世界的なサイバー攻撃件数の増加要因の1つとして、ハッカー集団による医療機関への関心の高まりがあり、2022年の医療機関に対するサイバー攻撃の増加率は、全業界の中で最大の43%であり、攻撃件数も1組織あたり週平均2,314件に上っている。なお、公表データは、世界的なサイバー攻撃件数、業界別、地域別などに分類されており、主な分析の結果は、図表14のとおりである。

また、ミュンヘン再保険によると、サイバー攻撃の加速の度合は、ロシアのウクライナ侵攻に代表される地政学的リスク¹⁵によっても影響を受けるとしている¹⁶。今後、このような紛争や大国の地位争いが、サイバー攻撃の主要な推進力となり、大規模なサイバーインシデント発生の可能性を高めるおそれがあるとしている。

また、特に懸念されることとして、国家が人材や資金を投入して進めたサイバーに関する研究・開発の内容をサイバー犯罪者が悪用して、例えば、人工衛星事業者を標的とする、あるいは、ソーシャルメディアの利用を通じて、サイバー攻撃を行う等の場合には、大きな脅威となるとしている。ミュンヘン再保険では、国家規模のサイバー犯罪集団が特に標的としている業界・組織として、IT企業（22%）、シンクタンク・NGO（17%）、教育機関（14%）等を挙げている（図表15参照）。

加えて、将来のサイバー攻撃に関して言及しており、ChatGPT¹⁷のようなAI（人工知能）¹⁸、メタバース¹⁹、IoT²⁰、オペレーショナルテクノロジー（OT）²¹の拡大などの革新的なテクノロジーの普及によって、サイバー攻撃はますます加速されるであろうと警告している。実際に、ソフトウェアを開発した経験のない人でも、ChatGPTを活用することにより、半年程度でマルウェア²²を作成することができるとの問題も指摘されている²³。

¹⁵ 特定地域が抱える政治的、軍事的、社会的な緊張の高まりが、地理的な位置関係によって、その地域や関連地域の経済、世界経済全体の先行きを不透明にしたり、特定の商品の価格を変動させたりするリスクを指す。

¹⁶ Munich Re, “Cyber insurance: Risks and trends 2023” (2023.4)

¹⁷ 米国サンフランシスコに本社を置き、AIの研究・開発を行っている OpenAI が、2022年11月に公開した AI チャットボットを指す。

¹⁸ 人間が行う「知的活動」をコンピュータプログラムとして実現することを指す。

¹⁹ 超越したという意味の「メタ (meta)」と、「ユニバース (universe)」を組み合わせた造語であり、インターネット上に構築された仮想空間を指す。

²⁰ 様々なモノ（物）がインターネットに接続され、情報交換することにより相互に制御する仕組を指す。

²¹ 社会の重要インフラ環境や産業用環境の機能を制御・運用する技術を指す。

²² 「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。

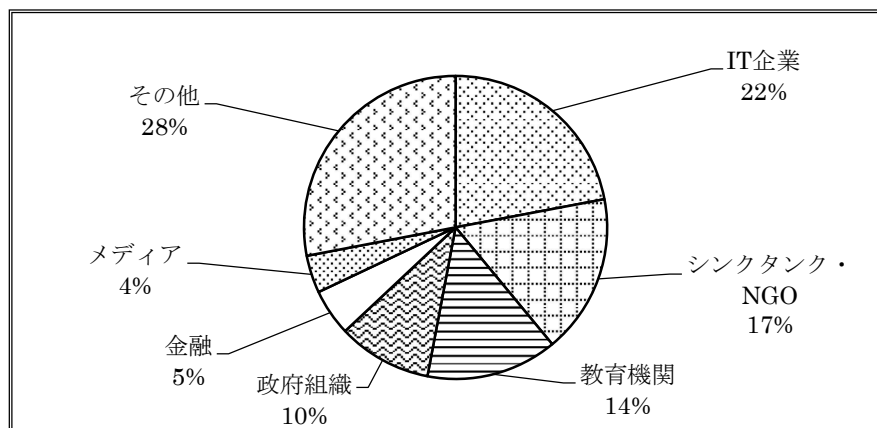
²³ Maria Dinzeo, “Cyberattacks are accelerating with AI's help” (PropertyCasualty360, 2023.6)

図表 14 Check Point Software Technologies によるサイバー攻撃分析

内容
○2022 年第 4 四半期の世界全体のサイバー攻撃件数は過去最高に達し、1 組織あたり週平均 1,168 件の攻撃が発生した。
○2022 年に最もサイバー攻撃を受けた業界・組織のトップ 3 は、「教育・研究機関」、「政府組織・軍」、「医療機関」であった。
○地域別では、アフリカ地域が 1 組織あたり週平均 1,875 件と、最も攻撃を受けており、次いでアジア・太平洋地域で、1 組織あたり週平均 1,691 件の攻撃を受けている。
○2021 年と比較して、2022 年のサイバー攻撃件数の増加率が大きい地域は、北米 (+52%)、中南米 (+29%)、欧州 (+26%) となっている。

(出典：Check Point Software Technologies, “Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks” (2023.1) をもとに作成)

図表 15 国家規模のサイバー犯罪集団が標的としている業界・組織



(出典：Munich Re, “Cyber insurance: Risks and trends 2023” (2023.4) をもとに作成)

(b) ランサムウェアによる攻撃件数の動向

サイバー攻撃の中でも、昨今、深刻な被害を及ぼしているとされるランサムウェア²⁴による攻撃²⁵について、複数の調査・分析機関が直近の動向について公表している。

S&P Global²⁶が 2022 年 10 月に公表した報告書²⁷によると、ランサムウェアによる攻撃件数は、直近 1 年間で約 25%増加したが、その一方で、企業が情報セキュリティ対策にかかる予算も約 26%増加しているとしている。また、報告書ではサイバー攻撃を未然に防げなかった要因として、全体の約 82%においてヒューマンエラー

²⁴ 「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。

²⁵ IBM が 2021 年に行った調査によると、2020 年に発生したサイバーインシデントは、ランサムウェア (23%)、データ漏洩 (13%)、脆弱性の悪用 (10%) の順であったとしている。

²⁶ 米国ニューヨークに本拠を置く金融サービス企業であり、格付会社である S&P Global Ratings や各種インデックスの算出会社である S&P Dow Jones Indices を傘下に持つ。

²⁷ S&P Global, “Cyber Trends and Credit Risks” (2022.10)

が関係しているとしている。

また、SonicWall²⁸による報告書²⁹では、2022 年の世界全体のランサムウェアによる攻撃件数は、前年比 21%減に相当する 4 億 9,330 万件であったとしている。しかしながら、2022 年 6 月を境に、再びランサムウェアによる攻撃件数が増加に転じており、2022 年第 4 四半期は、図表 16 のとおり、2021 年第 3 四半期以来最高の 1 億 5,490 万件に達したとしている。

さらに、Corvus³⁰の調査³¹によると、2021 年はランサムウェアの攻撃件数は大幅に減少しているものの、これは主として米国における攻撃が減少したためであり、米国を除いた件数では 20%近く増加していることから、サイバー攻撃者は、攻撃対象を米国から米国以外に移した可能性があると考えられるとしている。また、同調査では、攻撃件数が減少した一方で、同社の保険契約者における平均身代金支払額は、図表 17 のとおり、2022 年も増加傾向にあり、ランサムウェアの脅威は低下していないとしている。なお、Corvus では身代金支払額が増加している要因として、ランサムウェア攻撃の成功事例が減少傾向にあったことから、攻撃者はより大きな組織を標的とした、あるいは、より大きな身代金要求を突きつけるようになった等の理由が考えられるとしている。

2022 年のランサムウェア攻撃の減少要因について、IT セキュリティの専門企業である Delinea の報告書³²によると、様々なセキュリティ対策が奏功していることに加え、「Conti」³³と呼ばれるランサムウェアを用いた攻撃を行うグループが、2022 年 5 月に解散したとの情報が影響しているのではないかと推測している。また、ランサムウェア攻撃を受けたことをすべての企業が認めているとも限らないため、必ずしも報告件数が発生率の実態を反映しているとは限らないとしている。

なお、Delinea の調査において、ランサムウェアの被害件数から、攻撃の標的とされているのが、大企業から中堅・中小企業に変化していることが確認されている。これは、大企業のセキュリティ対策が進化しているのに対し、中堅・中小企業側のサイバー攻撃に対処するためのセキュリティリソースが不十分であることが原因の 1 つとされている。

²⁸ 米国カリフォルニア州に本社を置くネットワーク機器の製造、販売会社である。

²⁹ SonicWall, “2023 SonicWall Cyber Threat Report” (2023.3)

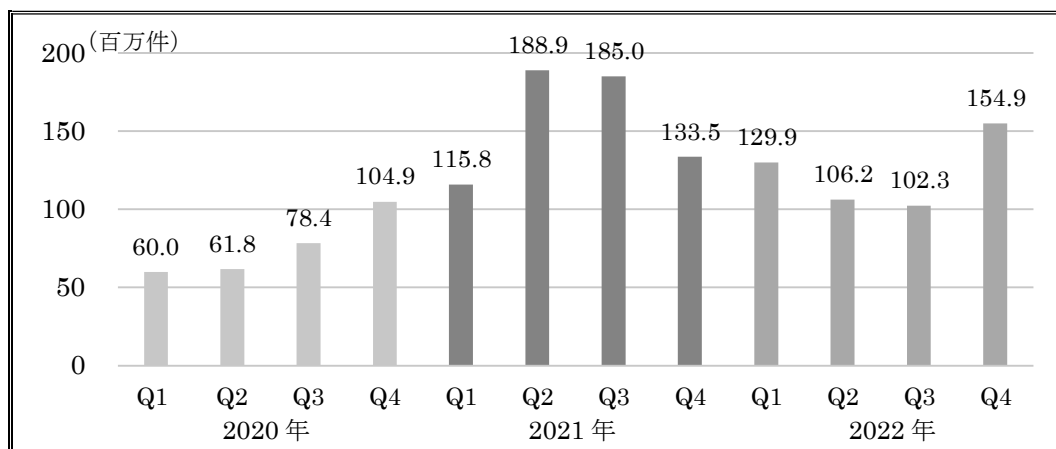
³⁰ 米国マサチューセッツ州ボストンに本社を置き、保険代理店としてサイバー保険を提供する、2017 年に設立されたインシュアテック企業である。

³¹ Corvus, “Q2 2023 Corvus Risk Insights Index” (2023.5)

³² Delinea, “State of Ransomware Survey Report: Making the Hard Choices for Ransomware Readiness and Response” (2023.1)

³³ 2020 年 5 月に初めて確認され、現在全世界で多くの被害を出している標的型ランサムウェアであり、近年流行している二重脅迫を行う攻撃グループが用いるランサムウェアを指す。

図表 16 全世界におけるランサムウェア攻撃件数の推移



(出典：SonicWall, “2023 SonicWall Cyber Threat Report” (2023.3) をもとに作成)

図表 17 保険契約者による年別の平均身代金支払額

	2020 年	2021 年	2022 年
平均身代金支払額	約 15 万ドル	約 19 万 4,000 ドル	約 31 万 6,000 ドル

(出典：Corvus, “Q2 2023 Corvus Risk Insights Index” (2023.5) をもとに作成)

b. 推定経済損失額

サイバーインシデントによる経済損失額については、企業や政府機関がすべてのサイバーインシデントを報告し、数値化している訳ではないことから、経済損失額の総額を明確に示す数値は公表されていない。しかし、いくつかの研究論文では、年間 1 兆ドル以上と推定されており、一般に広く利用されている McAfee³⁴による推定では、サイバーインシデントによる経済損失額（一次的な経済損失）は、2020 年においては 9,450 億ドルであるとし（図表 18 参照）、GFIA の報告書においても、補償ギャップ額の算出にあたっては、McAfee の推定値が使用されている。この試算には、人身事故、ソフトウェアやハードウェアの交換、サイバー身代金の支払、監督当局への罰金などが含まれているが、事業機会の喪失や風評被害などの二次的な経済損失は含まれていない。

また、サイバー攻撃による経済損失額に加えて、2020 年では 1,450 億ドルを超えると推測されているサイバーセキュリティ対策に要した費用を勘案すると、実質、世界経済に対して 1 兆ドルを超える影響を与えているとしている。さらに McAfee によると、被害にあった組織が被った損失費用として認識していないものとして、事業機会の喪失や風評被害に加えて、人員リソースの浪費や従業員のモラル低下等もあるとしており、経済損失額を正しく認識するためには、これらの損失も考慮しておく必要がある

³⁴ 米国カリフォルニア州に本社を置くコンピュータセキュリティ関連のソフトウェアとハードウェアの製作・販売会社であり、コンピュータセキュリティ関連のベンダーとして世界有数の規模を誇る。

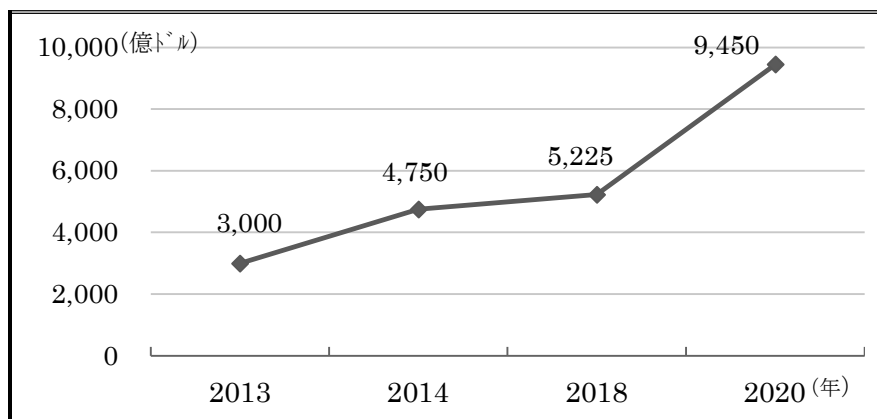
ことを認めている³⁵。

次に、サイバーセキュリティ専門の調査・分析会社である Cybersecurity Ventures では、2022 年 10 月に発行した報告書³⁶において、サイバー犯罪による被害額は、2015 年の 3 兆ドルから、2023 年には 8 兆ドルに達し、2025 年には 10 兆 5,000 億ドルに到達するであろうと予測している。なお、同社がサイバー犯罪の被害額としてもものは、データの損傷・破損、金銭の盗難、知的財産の盗難、個人データ・財務データの盗難、横領、詐欺、サイバー攻撃後の事業中断、フォレンジック調査³⁷、ハッキングされたデータやシステムの復旧・削除に加えて、生産性の低下や風評被害等の二次的な経済損失も含めており、McAfee の推定値とは経済損失額の対象範囲が異なっている。

また、同社ではランサムウェアによる被害額についても統計数値を公表しており、2015 年には 3 億 2,500 万ドルであったものが、2017 年には 50 億ドル、2019 年には 115 億ドル、2021 年には 200 億ドルに達し、2031 年までには 2,650 億ドルに到達すると予測している。

なお、サイバー攻撃による損害については、攻撃を受けている企業や組織が直接被ることもあれば、企業の顧客やサプライヤー等の第三者が被ることもある。Aon が公表している報告書³⁸によると、2021 年、米国ではサイバーインシデントに関する保険金請求の約 25%が第三者の損害に起因していたとしている。

図表 18 サイバーインシデントによる推定経済損失額



(出典 : James Andrew Lewis, Zhanna Malekos Smith, & Eugenia Lostri, “The Hidden Costs of Cybercrime” (McAfee, 2020.12) をもとに作成)

³⁵ James Andrew Lewis, Zhanna Malekos Smith, and Eugenia Lostri, “The Hidden Costs of Cybercrime” (McAfee, 2020.12)

³⁶ Cybersecurity Ventures, “2020 Official Cybercrime Report: Cybercrime to cost the world \$8 trillion annually in 2023” (2022.10)

³⁷ コンピューターなどのデジタル記録媒体に残された法的な証拠となるデータの収集や分析・解析調査を指す。

³⁸ Aon, “US Cyber Market Update: 2021 US Cyber Insurance Profits and Performance” (2022.8)

(3) サイバーインシデントによる保険損害額

a. サイバー保険市場規模

ミュンヘン再保険は、2023 年 4 月に公表した報告書³⁹において、サイバー保険の市場規模は、2019 年に 58 億ドルであったものが、2022 年には 119 億ドルに達したとしており、今後、2025 年には 225 億ドル、2027 年には 333 億ドルにまで拡大すると予測している（図表 19 参照）。

また、世界的な調査会社である Fortune Business Insights が公開しているウェブサイトによると、2022 年のサイバー保険の市場規模は 133 億ドルであり、そのうち、最大のサイバー保険市場である米国が 49 億ドル（全体の 36.8%）を占めたとしている。また、今後、2023 年には 167 億ドル、2030 年には 846 億ドルにまで拡大すると予測している。

さらに、データ分析およびコンサルティング会社である GlobalData の調査結果⁴⁰では、2022 年のサイバー保険の市場規模は 167 億ドルと推定し、2027 年には 334 億ドルに達するであろうと予測している。ここ数年の保険料の伸びは、保険料の大幅な引上げを主因としており、サイバー攻撃の頻度と深刻さに加え、経済全体のリモートワークへの移行が、保険料引上げの要因となっているとしている。また、同社が 2022 年に行ったイギリス国内での保険消費者調査では、イギリスの中小企業の 4 分の 1 以上が、パンデミックによるリモートワークの増加の結果、サイバー保険に新たに加入したと回答している。また、個人のサイバー保険市場についても、市場は小さいながらも、徐々に加入率が高まっており、回答者の 5.9%が個人向けサイバー保険を契約していると回答したとしている。

IAIS⁴¹においても、2023 年 4 月に発行した報告書⁴²の中で、グローバルモニタリング（Global Monitoring Exercise : GME）⁴³によるデータ収集⁴⁴を通じて得た、サイバー保険の地域別の総収入保険料を、図表 20 のとおり、公表している。これによると、米州を拠点とする損害保険会社に保険料が集中している一方で、わが国を含むアジアを拠点とする損害保険会社のサイバー保険の引受保険料は小さいものとなっている。また、IAIS では、サイバー保険の需要高まりの背景として、①サイバー攻撃の拡大に対する消費者の意識の高まり、②テクノロジーへの依存度の高まり、および③複雑な

³⁹ Munich Re, “Cyber insurance: Risks and trends 2023” (2023.4)

⁴⁰ GlobalData, “Cyber Insurance - Thematic Intelligence” (2023.5)

⁴¹ 保険監督者国際機構（International Association of Insurance Supervisors : IAIS）は、わが国（金融庁）を含む 200 以上の国・地域の保険監督当局が加盟する国際基準設定機関であり、公正・安全な保険市場を構築・維持し、保険契約者の保護を図るための効率的で一貫した監督を促進することを目指している。

⁴² IAIS, “Global Insurance Market Report (GIMAR): Special Topic Edition Cyber” (2023.4) を指す。なお、同報告書は IAIS が 2022 年に行った Global Monitoring Exercise (GME) を通じて収集した、2021 年末のデータに基づいている

⁴³ グローバルな保険セクターの動向をモニタリングし、システミックリスクの蓄積の可能性を評価するための IAIS の枠組を指す。

⁴⁴ 19 の国・地域からグローバル展開している大手損害保険会社約 60 社のデータを入手のうえ、取りまとめている。

サイバーリスクの状況などの理由が挙げられるとしている。

図表 19 世界全体のサイバー保険市場の実績と予測^(注)

企業名	2022 年 (実績)	2023 年 (予測)	2025 年 (予測)	2027 年 (予測)	2030 年 (予測)
ミュンヘン再保険	119 億ドル	—	225 億ドル	333 億ドル	—
Fortune Business Insights	133 億ドル	167 億ドル	—	—	846 億ドル
GlobalData	167 億ドル	—	—	334 億ドル	—

(注)「—」は出典に記載がないことを示す。

(出典：Munich Re, “Cyber insurance: Risks and trends 2023” (2023.4)、Fortune Business Insights
ウェブサイト、GlobalData, “Cyber Insurance - Thematic Intelligence” (2023.5) をもとに作成)

図表 20 サイバー保険の地域別の総収入保険料 (2021 年)

地域	総収入保険料	割合
米州	97 億ドル	71%
アジア・オセアニア	1 億ドル	1%未満
欧州・アフリカ	39 億ドル	29%
合計	137 億ドル	100%

(出典：IAIS, “Global Insurance Market Report (GIMAR):

Special Topic Edition Cyber” (2023.4) をもとに作成)

b. 保険損害額の算出方法

GFIA の報告書によると、サイバーインシデントによる保険損害額の算出にあたっては、世界のサイバー保険の保険料総額と損害率に基づいて算出できるとし、ミュンヘン再保険が公表している 2021 年のサイバー保険の保険料 (92 億ドル) に、世界のサイバー保険損害率の近似値として、米国のサイバー保険の損害率 (約 65%) を乗じることで、サイバーインシデントによる保険損害額を約 60 億ドルと推定している。

この考え方に基づくと、2022 年のサイバー保険の保険料 (119 億ドル)⁴⁵に、世界におけるサイバー保険の損害率として、NAIC が 2022 年 10 月に公表した米国のサイバー保険の損害率 (66.4%)⁴⁶を乗じると、2022 年のサイバーインシデントによる保険損害額は、約 76 億ドルに拡大しているものと類推される。

GFIA では、今後、補償範囲・引受方針の見直しや、損害率の変動等の不確定な要素はあるものの、サイバー保険の損害率が 60%から 70%で推移し、サイバー保険市場が毎年 25%から 40%で成長し続ける場合、サイバーインシデントによる保険損害額は、2025 年までに 130 億ドル～250 億ドルにまで増加するであろうと予想している。

⁴⁵ 前掲図表 19 を参照願う。

⁴⁶ NAIC, “Report on the Cyber Insurance Market” (2022.10)

(4) サイバーリスクにおける補償ギャップの縮小に向けた課題

サイバーリスクにおける補償ギャップは、「サイバーインシデントによる経済損失額と、実際に支払われた保険損害額との差」であることから、補償ギャップの縮小に向けて、サイバーインシデントの発生を未然に防ぐ、あるいは発生時の損害額を軽減するにあたり直面している課題と、サイバー保険の普及を推進するにあたり直面している課題の、両面から検討する必要がある。

ミュンヘン再保険が 2022 年 5 月に公表した、世界 14 カ国⁴⁷、7,000 社以上を対象に行った調査⁴⁸において、企業がサイバーの脅威に対する防御を改善するうえで認識している課題について照会したところ、図表 21 に示す回答結果となった。従業員のサイバーセキュリティに対する意識の低さや、IT セキュリティに精通した人材不足が、課題の上位として挙げられている。

また同調査では、サイバー保険の未加入企業に対して、その理由について照会を行っており、回答結果は図表 22 のとおりであった。1 位の「保険料が高い」については、近年のサイバー攻撃の増加による損害率の悪化に伴い、保険料率が年々上昇していたことが、回答結果にも表れているものと推察される。3 位の「商品内容がわからなかった」、4 位の「補償内容やサービスが不十分であった」と合わせて、損害保険会社に対して、サイバー保険についての適切な価格設定、わかりやすい保険商品、および魅力ある付帯サービスが求められていることが窺える。また、3 位の「サイバー保険の存在を知らなかった」については、損害保険業界を挙げて、サイバーリスクならびにサイバー保険に対するなお一層の認識の向上・改善が必要であると思われる。いずれの回答もサイバー保険を今後広く普及させるうえでの課題を示唆しており、それぞれに対処していくことが、サイバーリスクにおける保険補償ギャップ縮小につながる取組になるものと推察される。

また、あわせてサイバー保険に期待する付帯サービスとして、インシデント発生前、発生後それぞれについて意見を求めている。これに対する回答結果は、損害保険会社が今後のサイバー保険の商品開発や付帯サービスの検討にあたって、参考になるものと思われることから、サイバー分野の様々な専門機関とも協業のうえ、サイバー保険の普及取組を進めていく必要があると思われる（図表 23、図表 24 参照）。

⁴⁷ イギリス、イタリア、インド、オーストラリア、カナダ、スウェーデン、スペイン、中国、ドイツ、日本、ブラジル、フランス、米国、および南アフリカの 14 カ国である。

⁴⁸ Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022” (2022.5)

図表 21 サイバーの脅威に対する防御を改善するうえで認識している課題

順位	課題	回答割合
1	従業員のセキュリティ意識が低い	43%
2	ITセキュリティに精通した人材が不足している	30%
3	セキュリティ対策の統合・相互運用性 ^(注) が低い	27%
4	個々の部門間の連携が欠如している	26%

(注) 機器やソフトウェア、システムなどが、共通の仕様やデータ形式、伝送手順などに
対応し、互いに相手にデータを伝達したり、機能呼び出して使用したりできるこ
とを指す。

(出典：Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”
(2022.5) をもとに作成)

図表 22 サイバー保険に加入していない理由

順位	理由	回答割合
1	保険料が高い	29%
2	サイバー保険の存在を知らなかった	25%
3	商品内容がわからなかった	22%
4	補償内容やサービスが不十分であった	18%

(出典：Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”
(2022.5) をもとに作成)

図表 23 サイバー保険に期待する付帯サービス（インシデント発生前）

順位	サービス内容	回答割合
1	ネットワークセキュリティ（ファイヤーウォール等）の構築支援	62%
2	重要なシステムやデータ等のバックアップ	57%
3	マルウェア対策	54%
4	ID やパスワード等の管理	53%
5	従業員のセキュリティ意識の向上支援	48%

(出典：Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”
(2022.5) をもとに作成)

図表 24 サイバー保険に期待する付帯サービス（インシデント発生後）

順位	サービス内容	回答割合
1	データの復元（含むバックアップ）	65%
2	24 時間ヘルプホットライン	54%
3	インシデント後のフォレンジック調査	51%
4	法的なアドバイス	50%
5	恐喝事案の相談	49%

(出典：Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”
(2022.5) をもとに作成)

4. サイバーリスクに対する補償ギャップ縮小に向けた取組

本項では、サイバーリスクに対する補償ギャップの縮小に向けた動きとして、GFIA が報告書で取り上げている情報も踏まえ、サイバーインシデント対策と、サイバー保険の普及に向けた取組に分けて説明する。

(1) サイバーインシデント対策

a. 予防の奨励と支援

GFIA の報告書によると、サイバーインシデントの予防策を奨励・支援することで、企業や組織のサイバーリスクを 70%減少させることができる可能性があるとしており、保険会社は顧客に対して、事前リスク低減サービスを提供し、対策の実施状況に応じて保険料割引を付与するなどの金銭的インセンティブを盛り込むことが重要であるとしている。なお、スイス再保険の調査では、サイバー保険を引き受けている保険会社の約 70%が、既にこの種のスキームを導入済み、もしくは実施予定であるとしている。

米国において最大のサイバー保険の販売実績⁴⁹を誇るチャブでは、400 人以上のリスクエンジニアリングの専門家を抱え、リスク評価⁵⁰、リスクマネジメント⁵¹、リスクパートナーシップ⁵²という 3 つの柱に基づき、顧客にリスクエンジニアリングサービスを提供している。既存の IT インフラのリスク評価、シナリオベースの分析における潜在的な損失の算出、従業員向けのウェビナーによる研修など、より安全なインフラを構築するためのオーダーメイドの提案など様々なサービスを提供している。

また、チューリッヒ保険グループでは、イスラエルに拠点を置くサイバーセキュリティ事業者である CYE との提携により、高度な AI と 945 人以上の専門家からなる広範なグローバルネットワークを組み合わせた事前のリスク低減サービスを提供している。具体的には、「危機管理とインシデント対応の 24 時間サポート」、「戦略的サイバーセキュリティコンサルティング」、「サイバーセキュリティの運用上の支援」、「サイバー研修」、および「事業へのセキュリティ上の各種貢献」等が挙げられている。

また、Check Point Software Technologies⁵³は、自社のウェブサイトにおいて、サイバー攻撃の脅威から身を守るために肝要なのは、「検知」ではなく「予防」を第一に考えることであるとし、次なる攻撃にさらされるリスクを最小限に抑えるために、組織が取り得るベストプラクティスとして、図表 25 のとおり提示している。

⁴⁹ NAIC, “Report on the Cyber Insurance Market” (2022.10)

⁵⁰ チャブによる Global Cyber Facility 評価プロセスでは、客観的基準と主観的基準の両面から、サイバーエクスポージャーに関する評価を行うとしている。

⁵¹ チャブでは、顧客と協力のうえ、エクスポージャーの削減、リスクコントロールの改善、およびクレーム対応など、必要に応じたリスク改善の提案を行うとしている。

⁵² チャブのサイバーインシデント対応チームは、法律、コンピューターフォレンジック、コールセンター、広報、危機管理コミュニケーション、詐欺相談、信用状況のモニタリング、個人情報の流出対応等の分野において経験豊富なサービスプロバイダーで構成されている。

⁵³ Check Point Software Technologies については、前記 3.(3)a も参照願う。

図表 25 サイバー攻撃を未然に防ぐベストプラクティス

取組	内容
サイバーセキュリティ意識向上の研修	○ランサムウェアから組織を守るためには、従業員に対する頻繁なサイバーセキュリティ意識向上の研修が不可欠であり、以下の指示が必須である。 ・悪質なリンクをクリックしない。 ・定型外または信頼できない添付ファイルは絶対に開かない。 ・フィッシング犯に個人情報や機密データを開示しない。 ・ダウンロードする前に正規ソフトウェアであることを確認する。 ・不明な USB を自分のコンピュータに接続しない。 ・信頼できない、または公共の Wi-Fi に接続する際は VPN^(注2) を使用する。
パッチ ^(注1) の最新化	○コンピュータやサーバーを常に最新の状態に保ち、特に「重要」の表示があるセキュリティパッチの適用により、ランサムウェア攻撃に対する組織の脆弱性を抑制する。
ソフトウェアアップデート	○ランサムウェア攻撃者は、アプリケーションやソフトウェアに侵入口を見つけ、その脆弱性に目をつけて攻撃することから、パッチマネジメント ^(注3) の一環として、従業員によるソフトウェアの最新版への更新作業を確実に実施させる必要がある。
検知より予防への優先投資	○多くのサイバー攻撃は未然に防ぐことができることから、サイバー被害を検知・軽減する技術に投資すること以上に、予防のための適切な技術に投資することを検討すべきである。

(注1) コンピュータ等においてプログラムの一部分を更新してバグ修正や機能変更を行うためのデータを指し、脆弱性や問題点を解消するためのプログラムは、セキュリティパッチと呼ばれる。

(注2) 仮想専用ネットワーク (Virtual Private Network) の略称であり、物理的に離れた場所にある拠点間を仮想的な社内ネットワークでつないで安全なデータ通信を実現する仕組を指す。

(注3) システムを構成しているコンピュータを管理して、脆弱性が発見されたときに適切にセキュリティパッチを適用させるための管理活動を指す。

(出典：Check Point Software Technologies, “Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks” (2023.1)、PR Times ウェブサイトをもとに作成)

b. 事故報告の枠組の構築

GFIA の分析では、政府、セキュリティ機関、保険会社は、サイバーインシデントに関する頻度、規模、確率等のデータ推定に課題を抱えており、その結果、保険会社は信頼できる損害予測を行うことができず、一貫した適正なリスクプライシングを行うことができないとしている。これにより、保険会社として積極的なサイバー保険の提供につながりにくく、市場拡大の障壁にもつながっているとしている。

セキュリティが確保された、サイバーインシデントを報告する制度・枠組が整備され、必要な情報が保険会社と共有されることにより、サイバー脅威に対する透明性を高め、保険会社によるリスクモデリングを促進する可能性があることから、世界各国の政府は、図表 26 に示すとおり、インシデント報告を強制する規制の導入を開始している。実際、米国におけるサイバーインシデント報告に関する法規制の導入と施行は、サイバー保険市場の成長と相関しており、その結果、補償ギャップが縮小する可能性があるという分析結果を得ているとしている。

図表 26 主なサイバーインシデント報告に関する法規制

国	年	根拠とする法規制	報告の基準
米国	2021	ランサムウェア・ガイダンス (Ransomware Guidance)	インシデント発生後72時間以内に米国ニューヨーク州金融サービス局 (NYDFS) へ報告
	2022	重要インフラサイバーインシデント報告法2022 (CIRCA)	インシデント発生後72時間以内、ランサムウェア身代金支払後24時間以内に監督当局へ報告
欧州	2016	EUにおける一般データ保護規則 (GDPR)	情報漏えいを認識後72時間以内に監督当局へ報告
	2022	改正ネットワークおよび情報システム指令 (NIS2指令)	重大なインシデント発生を認識後24時間以内に早期警告、72時間以内にインシデント通知、1カ月以内に最終報告書を提出
オーストラリア	2021	重要インフラ安全保障法 (Security of Critical Infrastructure Act 2018) の改正	重要インフラ責任事業者は重大なサイバーインシデント発生を認識後12時間以内に、その他については発生を認識後72時間以内に当局へ報告
インド	2022	サイバーセキュリティ指令 (Cyber Security Directions)	サイバーインシデント発生を認識後6時間以内に報告
日本	2022	個人情報の保護に関する法律施行規則	報告対象事態を認識してからすみやか(概ね3から5日以内)に個人情報保護委員会へ報告、本人に通知

(出典：PwC コンサルティング「「サイバー攻撃被害に係る公表」に関する国内組織実態調査 2023」(2023.4) ほかをもとに作成)

c. 政府による適応措置の促進

世界各国の政府の中には、サイバーセキュリティを国家課題に掲げ、国家サイバーセキュリティ目標を明確に定義したサイバーセキュリティ戦略を導入し、国家サイバーレジリエンスの構築と、安全なデータ使用に関する、国民の教育を目的とした支援活動を立ち上げているところもある。

政府による支援は、国家的なサイバーセキュリティ戦略や予防的な取組から、リスク成熟度モデルや必要なリスク資本に基づく最低基準の形で予防や適応策に関する法制化まで、様々なものが考えられる。民間の損害保険会社は、規制環境と公共のサイバーセキュリティ・インフラに依存しているため、損害保険会社だけでは、サイバーリスクにおける補償ギャップの縮小に向けた取組には限界がある。各国の政府が率先して、サイバー市場に人的資源を投入し、規制の枠組を構築することが、補償ギャップの縮小に向けて効果的な役割を果たすことにつながると考えられる。

(2) サイバー保険の普及に向けた取組

a. 啓発キャンペーンの実施

官民の関係者による啓発活動は、サイバーリスクについて個人を教育し、セキュリティ対策の重要性を説明することで、補償ギャップを解消するものである。特に、中小企業は、セキュリティへの資源投入が少ない一方で、人事や顧客情報、財務データ、生産内容などの機密情報を取り扱っているため、サイバー攻撃に対して特に脆弱である可能性がある。新型コロナウイルス感染症の流行によって、中小企業のデジタル化

が急速に進む中、情報セキュリティのリテラシーと実装が必ずしも追いついていない側面があることから、官民を挙げて啓発活動を推進していくことが求められる。

保険契約者は、サイバーに関するすべての情報・サービスにアクセスできるとは限らないことから、保険会社はサイバー保険の顧客である契約者に対して、購入プロセスを通じて、より密接にサイバーリスクに関する様々な情報を提供することにより、サイバーリスクの軽減につながるものと考えられる。

b. サイバーリスクに対応する新商品の開発

(a) HDI Global によるインセンティブ付きサイバー保険

ドイツに本拠を置く保険会社である HDI Global では、サイバーリスクに対する事前対策サービスやサイバー補償を提供するだけでなく、サイバーインシデント予防に金銭的なインセンティブを与えるスキームを導入している。具体的には、サイバー保険に特約条項を設けており、保険契約者が保険契約と同時に提供される HDI Global の無料予防サービスを利用した場合、免責金額を 25%減額する。さらには、保険契約者は、HDI Global の子会社で IT セキュリティサービス事業者である Perseus⁵⁴を通じて、同社が定めるセキュリティチェックを実施すれば、免責金額をさらに 75%削減することができるとしている。これにより、サイバー保険の普及を行うとともに、サイバーインシデントに対する未然予防を促し、被害軽減に努めることができるとしている。

(b) Intangic MGA によるパラメトリック保険

AXA SA 傘下の AXA XL の支援を受けて最近設立されたロンドンを拠点とする保険総代理店 (Managing General Agent) ⁵⁵である Intangic MGA は、2023 年 3 月より、重大なデータ侵害による損害を最高 1,500 万ドルまで補償するパラメトリック保険の販売を行っている。保険契約締結時に、「企業を標的にした悪意あるサイバー攻撃により発生した損失額」を保険金支払のトリガーとして閾値を定め、契約期間中に閾値を超えた場合に保険金が支払われるとしている。Intangic MGA では、このパラメトリック保険により、すべての関係者がリスク活動をリアルタイムでモニタリングするための測定基盤が確保できるとし、既存のサイバー補償の代替ではなく、財務面での補完機能を果たす役割を担う、サイバー保険市場にとって初めての商品であるとしている。

⁵⁴ HDI Global は 2020 年 2 月、ベルリンに本拠を置き、サイバーリスクの防止と緊急支援を専門とする Perseus Technologies GmbH を買収した。

⁵⁵ 保険料水準の設定、保険契約の締結、保険金の支払など、通常は保険会社が行う業務について、権限の一部を委任された保険代理店・ブローカーを指す。

(c) サイバーCAT ボンドの発行

イギリスに本拠を置く保険会社である Beazley は 2023 年 1 月、大規模なサイバーインシデントに対する CAT ボンドを、4,500 万ドル発行したことを明らかにした。サイバー災害リスクを対象とした流動性の高い保険リンク証券 (ILS) 商品が創設されたのは、保険業界で初めてとなる。この CAT ボンドでは、顧客の請求額が 3 億ドルを超える大規模なサイバーテロが発生した場合、Beazley はあらかじめ定めた条件に応じた金額を受け取ることができるとしている。なお、2023 年 5 月には、さらに 2,000 万ドル分のサイバーCAT ボンドの追加発行を行っている。

Beazley では、サイバーリスクに対する効果的なソリューションとして、この種の CAT ボンドを開発することは、サイバー（再）保険市場へのキャパシティ供給を増加させるものであり、企業や社会からのサイバーリスクに対する補償需要の高まりに対応するにあたって不可欠であるとしている。

c. 官民連携に向けた取組

ジュネーブ協会⁵⁶およびテロリスク（再）保険プール国際フォーラム (International Forum of Terrorism Risk (Re)Insurance Pools : 以下「IFTRIP」)⁵⁷ は、2022 年 1 月に公表した報告書⁵⁸において、持続可能な民間のサイバー再保険市場の発展を促すためには、国家関与のサイバー攻撃に代表される大規模で不確実性の高いサイバーリスクに対しては、被害者救済（補償ギャップの縮小）の観点からも、民間の保険市場だけでは対応しきれないとしている。そのため、公的資金を提供する、官民連携取組のような政府のバックアップが必要であるとし、保険業界が主導的な役割を果たし、官民連携取組を強化することで、リスク吸収能力を高め、民間の損害保険市場の負担を軽減し、さらにサイバー保険市場におけるイノベーションを可能にし、壊滅的なサイバーインシデントやシステミックリスクに対する補償をさらに拡大することができるとしている。

また、同報告書では、政府支援のソリューション設計は複雑であり、政府と民間（再）保険会社間でのリスク負担調整の難しさを踏まえると、国際的な官民連携の協調ソリューションが最適であるものの、まずは国内レベルでの官民連携ソリューションの開発を優先させるべきであるとも提言している。

同様に、GFIA においても、サイバー保険の普及にあたって、サイバー攻撃が潜在的なシステミックリスクである点を踏まえると、官民連携取組は不可欠であるとし、

⁵⁶ 前掲図表 4（注 2）を参照願う。

⁵⁷ IFTRIP は、政府支援によるテロ再保険プール間の緊密な国際協力取組を支援するために、Pool Re の主導により 2015 年 10 月にロンドンで発足し、2016 年 10 月にオーストラリア再保険プール公社 (ARPC) が主催した会議において正式に批准された。

⁵⁸ Geneva Association & IFTRIP, “Insuring Hostile Cyber Activity: In search of sustainable solutions” (2022.1)

民間保険会社によるサイバー保険の安定供給に向けて、政府がサイバーリスクのシステミックリスク部分について積極的な施策を講じることを提言している。また、「企業によるランサムウェア支払の禁止」、「大企業へおサイバーセキュリティ補償の義務付け」、および「サイバー犯罪への法執行の強化」等、政府が取り得る施策に関しても、様々な問題提起を行っている。

5. おわりに

本稿では、現在、世界の人々が直面している主要な補償ギャップとして、年金リスク、医療費リスク、自然災害リスク、およびサイバーリスクの4つを取り上げ、それぞれについて、その概要および補償ギャップの規模感、それぞれの抱えている課題、および補償ギャップの縮小に向けた対策について説明した。また、近年、特にリスクが増大し、損害保険業界において補償ギャップの縮小に向けて特段の役割が期待されているサイバーリスクについては、最新のデータ・情報を調査したうえで、損害保険会社の取組事例を紹介するとともに、損害保険業界が果たすべき役割について整理した。

4つのリスクに共通していることとして、補償ギャップの縮小に向けて、民間の保険会社による取組は重要で、その果たすべき役割は大きいながらも、個別の活動には限界があることから、地域、国、および国際機関等の政策立案者が、適切な措置を講じるかどうかの観点が極めて重要であると考えられる。特にリスクの管理・軽減に最適な環境を設計・構築し、損害保険会社が重要な役割を果たせるようにするためには、政策立案者による支援、後押しが不可欠であることが今回の調査から窺えた。

また、その拡大が最も懸念されるサイバーリスクにおける補償ギャップの縮小に向けて、損害保険業界としての取組は、サイバー保険の提供も含め、まだ発展途上にある。今後、業界として取り組むべきポイントとして、①サイバーリスクに関する啓発活動の実施、サイバーセキュリティ企業との協業、およびパラメトリック保険やCATボンド等の新たなサイバー補償の提供等による「サイバー保険の普及推進」、②顧客へのサイバーセキュリティ評価サービスの提供や、サイバーリスク低減取組に対してインセンティブを与える保険商品提供等による「サイバーインシデントの被害縮小に向けた活動の推進」、ならびに③サイバー攻撃の抑制に向けた政府・自治体への業界としての提言・協業や、サイバーインシデントに関する各種情報の共有化等の「官民連携取組」が重要であると考えられる。

わが国損害保険会社として、サイバーリスクの領域を、保険商品としての収益性の側面だけではなく、現在、世界で最も懸念されているリスクに対する補償ギャップの縮小に向けて貢献を図り、存在感を示す絶好の機会としてとらえ、さらなる取組を推進していくことが求められるものとする。

＜補足資料＞

調査報告書「諸外国における自然災害による被害の縮小や 保険普及に向けた取組の現状、課題、対策」(2023.3) の概要

(1) 自然災害における補償ギャップの現状

2011 年から 2021 年までの通算の、全世界の自然損害による補償ギャップ額は 1 兆 5,286 億ドルであり、経済損失額に占める補償ギャップ額の割合（補償ギャップ率）は 63%となっている（図表 27 参照）。アジア諸国全体における補償ギャップ率は平均で約 90%であり、途上国は先進国より相対的に補償ギャップ率が高くなっている。

また、米国、イギリス、ドイツ、フランス、カナダ、およびオーストラリアにおける、ペリル別の補償ギャップ率は図表 28 のとおりであるが、フランスを除く 5 カ国において、洪水による補償ギャップ率が暴風による補償ギャップ率を上回っている。

図表 27 全世界の補償ギャップの推移（2017 年～2021 年）

（単位：億ドル）

項目	2017 年	2018 年	2019 年	2020 年	2021 年	2011 年～ 2021 年通算
①自然災害による経済損失額	3,737	1,813	1,473	2,026	2,700	24,195
②自然災害による保険損害額	1,555	905	572	899	1,106	8,909
③補償ギャップ額（＝①－②）	2,181	907	901	1,127	1,594	15,286
④補償ギャップ率	58%	50%	61%	56%	59%	63%

図表 28 調査対象国におけるペリル別の補償ギャップ率

ペリル	米国	イギリス	ドイツ	フランス	カナダ	オーストラリア
自然災害全体 ^(注)	25%	25%	40%	33%	33%	34%
暴風	21%	23%	30%	32%	25%	33%
洪水	48%	28%	64%	32%	58%	43%

（注）暴風、洪水、地震、森林火災などを含む自然災害全体を指す。

(2) 諸外国において補償ギャップが生じている原因・課題

自然災害における補償ギャップが縮小していない原因・課題については、経済損失額が減少していない要因、および保険損害額が増加していない要因、あるいはその両面から分析する必要がある。

原因・課題の調査結果は、図表 29 のとおりであるが、経済損失額が減少していない各国共通の要因として、経済の発展とともに、洪水などの自然災害の影響を受けやすい地域において、住民の流入や土地開発・住宅建築が行われていることや、各国の防災・減災に向けたインフラ設備が十分に対応しきれていない点などが挙げられる。

また、保険損害額が増加していない要因として、先進国においては、主に保険制度面・商品構成面での課題が挙げられる。一方、途上国においては、損害保険の普及率

が低いことが共通しており、その背景には、所得水準が低いなどの経済的事情や文化的・社会的要因などがあるものと考えられる。

図表 29 補償ギャップが生じている原因・課題

調査対象国	概要
米国	○補償ギャップの原因は様々であり、①災害発生時には政府の支援があるため保険は不要であるという誤解、②自然災害リスクに対する関心の低さや理解不足、③保険料水準の高さ、および一般のホームオーナーズ保険で洪水や地震が補償されない商品設計の問題などがある。
イギリス	○保険業界と政府で共同運営している洪水再保険会社（スキーム）である Flood Re の適用対象となる保険契約に対して、顧客への意向確認が不十分でありながら、保険会社が洪水除外条項付きで住宅保険を提供したり、更改したりしている可能性がある。 ○洪水リスクの高い世帯や企業に的を絞った、洪水リスクに対する認識向上の取組が不十分である。
ドイツ	○個人向けの建物・家財総合保険では、洪水、地震等は特約の付帯により補償対象とすることができるが、この特約の付帯率は 52%に留まっている。 ○政府による被災者への手厚い支援金の提供が、自身で保険に加入しようとするインセンティブを損ねている。
フランス	○フランスの海外領土での財産保険の普及率が低いため、自然災害発生時の補償ギャップは大きくなる傾向にある。 ○農作物保険および森林保険等の普及率が財産保険ほど高くないこと、ならびに重要な公共インフラの多くが自家保険となっていること等も一因とされている。
カナダ	○洪水リスクが高い地域では保険料が高く、特に低所得世帯にとっては大きな負担となる。 ○各州に災害支援制度があるために、住宅所有者は、リスク低減のための行動や、保険加入に積極的でない。
オーストラリア	○低所得の住宅所有者や賃借人は保険に加入していないケースが多い。 ○洪水リスクが高い地域での開発と人口増加が進んでいる。
インドネシア	○住宅所有者のごく一部しか保険を契約していないなど保険の普及が進んでいない。 ○保険の普及が進まない要因として、宗教的・文化的な考え方、金融機関に対する一般的な不信感、および貧困などが挙げられている。
タイ	○個人物件で財産保険に加入している世帯の割合は、10%未満と推定されている。 ○社会的背景や保険文化の欠如、および古くからの迷信で保険加入は保険事故を誘発すると言われていた。
フィリピン	○国民の年間所得が 1 人あたり 3,000 ドル程度水準に留まっているため、損害保険料を支払う余裕がない。 ○住宅ローン金利が高いこと、歴史的に賃貸住宅を好む文化があることなども、住宅を対象とする財産保険が普及しない要因となっている。
インド	○自然災害が多発し被害額が大きい一方、保険の浸透率が極めて低い。 ○保険の普及が進まない要因として、保険の認知度不足や、国民の保険会社に対する信頼の欠如などが挙げられている。

(3) 諸外国における自然災害に対する補償拡充に向けた取組

諸外国における自然災害に対する補償拡充に向けた主な取組内容の概要は、図表 30 のとおりである。欧米諸国では、保険制度の見直しをはじめ、保険料率の引下げ、低所得者に対する保険料補助、税制面での負担軽減等の検討を行っている。また、各国で民間保険会社によるパラメトリック保険やマイクロインシュアランスを用いた地震、洪水等の自然災害に対する補償拡充の動きや、農作物に対するパラメトリック保険の提供なども開始されている。

図表 30 自然災害に対する補償拡充に向けた取組

調査対象国	主な取組の概要
米国	○連邦緊急事態管理庁（FEMA）が、連邦洪水保険の加入率向上のため、保険制度の見直しを行っている。 ○全米保険監督官協会（NAIC）の会議体において、民間保険会社による洪水保険引受の拡大に向けた検討が行われている。
イギリス	○Flood Re スキームの対象とならない企業物件に対し、スタートアップ企業である FloodFlash が洪水パラメトリック保険を提供しているほか、イギリス保険ブローカー協会（BIBA）も、洪水補償を付帯した会員専用の企業保険スキームを導入している。
ドイツ	○2023 年 1 月末現在、連邦政府と州政府は、自然災害リスクを補償対象とする強制保険制度の導入について議論を継続している。 ○ドイツ保険協会（GDV）は 2021 年 10 月に、適切な防災・減災措置の実施とあわせて、「すべての住宅保険に自然災害補償を追加し、保険契約者がこれを望まない場合は拒否（オプトアウト）できる仕組み」を導入することなどを提言している。
フランス	○官民合同の保険制度である巨大自然災害保険（Cat Nat）の制度改正法案が可決され、認定手続の明確化、干ばつの損害に関する保険金請求期限の延長、被災時の緊急移転費用の補償追加等、制度面や補償面の改正が 2023 年から順次行われる。
カナダ	○2020 年 11 月に公安省は洪水保険および立ち退きに関する作業部会を設置し、公的保険制度モデルのあり方を検討し、2022 年 8 月に報告書を公表した。
オーストラリア	○オーストラリア保険評議会（ICA）は 2022 年に、保険普及推進のため、保険に係る印紙税や州税の廃止を提言している。 ○民間保険会社がマイクロインシュアランスの提供や CAT ボンドの発行等を行っている。
インドネシア	○政府は、2018 年に自然災害に対するレジリエンスを構築するための戦略として「災害リスクファイナンス・保険戦略（DRFI 戦略）」を策定した。 ○国内再保険会社である Maipark は、世界銀行グループの国際金融公社との提携により、地震災害に係るパラメトリック保険である EQ II を開発し、販売を開始した。
タイ	○政府は、2016 年に農業従事者の農作物保険加入義務化に向けた対応を行うよう勧告を受けて以来、農作物保険の普及・拡大について、情宣活動を積極的に行っている。
フィリピン	○政府は、マイクロファイナンス・マイクロインシュアランスを自然災害に対する補償拡充の手段の 1 つとして位置付け、普及促進に向けた取組を行っている。
インド	○国営の保険会社である AIC は、2021 年に農作物に対する気象変化による被害を補償するパラメトリック保険の提供を開始した。

(4) 諸外国における防災・減災に向けた取組

諸外国における防災・減災に向けた主な取組内容は、図表 31 のとおりである。各国とも、自然災害に対する防災・減災取組を国家の重点施策の 1 つとしてとらえ、政府計画への落とし込みや、新たな防災・減災専門組織の設置、自然災害リスク防止基金の創設など、対策を強化している。各国の保険業界においても、業界独自で防災・減災の専門機関を設置し、建築基準の適正化、強化建物規格の普及・促進、および防災知識の啓発・教育への取組や、洪水被害の低減に向けたインフラやハード面の改善、土地利用計画や建築基準法の改正等を中心とした政府に対する要望・提言活動などが進められている。

図表 31 防災・減災に向けた取組

調査対象国	主な取組内容
米国	○連邦緊急事態管理庁（FEMA）が、2022 年からの同庁の計画において、防災・減災を重点取組としており、補助金の拡大などにより自治体の取組を推進している。 ○保険業界の防災・減災の専門機関である「事業・家庭安全保険研究所（IBHS）」が、保険会社や他の専門機関と連携して、建築基準の適正化、強化建物規格の普及・促進、および防災知識の啓発・教育に取り組んでいる。
イギリス	○Flood Re は、制度に参加する住宅保険提供保険会社を通じ、住宅の洪水対策費用として 1 契約者あたり最高 1 万ポンド（約 161 万円）を提供するビルドバックベタースキームを 2022 年 4 月に開始した。 ○アビバをはじめとする保険会社は、洪水被害の低減に向けたインフラやハード面の改善を中心とした要望・提言を政府に行っており、その一部は実現しつつある。
ドイツ	○ドイツ保険協会（GDV）は 2021 年 10 月、建築規制の気候変動への適応、リスクが高い場所での建築禁止、および自然災害ポータルサイトの設置等を、政府に対し提案している。
フランス	○自然災害リスクにさらされた住民の住居等を、国または地方自治体がい取り替えるための基金として、重大自然災害リスク防止基金（FPRNM）が 1995 年に創設されている。
カナダ	○連邦政府が気候変動に対する国家適応戦略を策定し、国民への自然災害に関するデータベースの公表や、緊急情報サービス、ハザードマップの提供等を実施している。 ○カナダ損害保険大手 Intact は、風水災対策を実施した建物の住宅火災保険に対して、一定の保険料割引を提供している。
オーストラリア	○政府や政府機関等が中心となって、ハザードマップの品質向上、ポータルサイトでの情報提供、消費者向け啓発等を実施している。 ○オーストラリア保険評議会（ICA）は 2022 年に、連邦政府に対し、土地利用計画や建築基準法の改正等を提言している。
インドネシア	○2007 年に防災法を制定し、災害対策を所管する主務官庁として、災害対応だけではなく、防災、災害後の復旧・復興も目的とする国家防災庁（BNPB）を設立した。 ○同庁は 5 年ごとに国家防災計画を策定するとともに、国内外の機関が収集した観測情報、災害リスク情報、分析情報を国内で共有・伝達するためのツールを開発している。
タイ	○2011 年の洪水を契機に、政府の防災・減災の政策策定や計画立案、実行管理は、内務省災害防止軽減局（DDPM）に一元化され、災害リスク管理の人材育成を担当する防災アカデミー、災害予警報などの情報発信を担当する国家災害警報センター等が設置されている。
フィリピン	○2009 年 9 月の台風ペンを契機に、それまでの復旧主体の災害対策から、災害リスク管理を重視した防災・減災の取組へと政策を変更した。
インド	○2005 年に災害管理法を制定のうえ、国家レベルで防災に係る取組を開始し、それまでの復旧主体の対応から、予防・緩和・準備主導のアプローチへの転換が示されている。 ○2019 年の国家災害管理計画では、インドのすべての階層を災害に対してレジリエントにし、実質的かつ包括的な災害リスクの低減を達成することを目標としている。

(5) おわりに

調査報告書では、わが国損害保険業界が、世界における補償ギャップの縮小に向けた取組・対応を検討する際に特に重要な視点として、以下の3点を取り上げている。

a. 国際機関・国際イニシアチブへの貢献

- わが国は、国際的な防災の取組指針となる仙台防災枠組において世界を主導する立場にあり、現在政府が進めている、「インフラシステム海外展開戦略 2025」や、「日本政府の気候変動の悪影響に伴う損失および損害支援パッケージ」の中でも、わが国が有する防災・減災の技術・知見・ノウハウや、公的保険制度および各種支援制度等は、他国にとって有益であるとしている。
- わが国損害保険業界がこうした状況を踏まえ、国際機関・国際イニシアチブに対して、これまで以上の提言や取組の支援、技術・ノウハウ提供等の貢献活動を行うことにより、自然災害における補償ギャップの分野でのわが国損害保険業界の貢献度をさらに高め、より一層の存在感を発揮することが可能である。

b. 官民連携取組の推進

- 民間の損害保険業界単独での取組には限界があり、特に法規制面や資金面等において、国や自治体等との連携が不可欠である一方で、国や自治体の取組だけでも十分な実効性が得られないことから、損害保険業界との相互に補完的な取組が不可欠となっている。
- 防災・減災に向けたインフラ整備や、自然災害に対する危険予知に関して、国や専門機関が有するインフラ整備の知見・ノウハウや自然災害の検知技術、自治体が有する住民とのネットワーク、損害保険業界が有する自然災害の被害データ等を相互に共有・活用することで、防災・減災取組のさらなる高度化が期待できる。
- わが国損害保険業界では、各地で自治体との防災・減災取組を積極的に進めており、こうした事例を、アジアを中心とした途上国に展開していくことも肝要である。

c. 損害保険の普及促進

- 各国とも自然災害に対する保険加入による補償の手当てが十分ではなく、特にアジアの途上国においては、損害保険の普及率そのものが低水準に留まっていることから、例えば、パラメトリック保険やマイクロインシュアランス等を活用して損害保険の普及を促進する必要がある。
- 先進国においても保険加入率が依然として低いなどの課題があることから、消費者への丁寧なリスク情報の提供などにより、既存の公的保険制度の拡充や民間保険商品の加入率引上げなどの地道な取組も引き続き不可欠であり、国、自治体、損害保険業界が、相互の情報共有・連携を強化していく必要がある。

<参考資料>

- ・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）
- ・GFIA 著、日本損害保険協会仮訳「グローバルプロテクションギャップとそれを埋めるための提言」（2023.6）
- ・SonicWall「エクゼクティブサマリー：2023 SonicWall サイバー脅威レポート」（2023.3）
- ・損害保険事業総合研究所「諸外国における自然災害による被害の縮小や保険普及に向けた取組の現状、課題、対策」（2023.3）
- ・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）
- ・田代邦幸「第 206 回：米国におけるランサムウェア攻撃および対策状況のトレンド」（リスク対策.com、2023.1）
- ・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）
- ・日本損害保険協会「中小企業におけるリスク意識・対策実態調査 2022 調査結果報告書」（2022.12）
- ・濱田和博「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）
- ・PwC コンサルティング「「サイバー攻撃被害に係る公表」に関する国内組織実態調査 2023」（2023.4）
- ・吉川孝志「Conti ランサムウェアの内部構造を紐解く」（MSBD、2021.4）
- ・Allianz Global Corporate & Specialty, “Allianz Risk Barometer: Identifying the major business risks for 2023”（2023.1）
- ・Aon, “US Cyber Market Update: 2021 US Cyber Insurance Profits and Performance”（2022.8）
- ・Beazley, “Beazley launches market’s first cyber catastrophe bond”（2023.1）
- ・Check Point Software Technologies, “Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks”（2023.1）
- ・Corvus, “Q2 2023 Corvus Risk Insights Index”（2023.5）
- ・Cybersecurity Ventures, “2020 Official Cybercrime Report: Cybercrime to cost the world \$8 trillion annually in 2023”（2022.10）
- ・Daniel Croft, “Worlds’ First Cyber Catastrophe Bond Launched By UK Insurer”（CyberSecurity Connect, 2023.1）
- ・Delinea, “State of Ransomware Survey Report: Making the Hard Choices for Ransomware Readiness and Response”（2023.1）
- ・Geneva Association, “Healthcare in Emerging Markets: Exploring the Protection Gaps”（2019.3）
- ・Geneva Association, “Ransomware: An insurance market perspective”（2022.7）
- ・Geneva Association, “Understanding and Addressing Global Insurance Protection Gaps”（2018.4）
- ・Geneva Association & IFTRIP, “Insuring Hostile Cyber Activity: In search of sustainable solutions”

- (2022.1)
- GFIA, “Global Protection Gaps and Recommendations for Bridging Them” (2023.3)
 - GFIA, “Towards a safer cybersecurity environment: Insurance industry cyber-awareness initiatives” (2021.1)
 - GlobalData, “Cyber Insurance - Thematic Intelligence” (2023.5)
 - IAIS, “Global Insurance Market Report (GIMAR)” (2022.12)
 - IAIS, “Global Insurance Market Report (GIMAR): Special Topic Edition Cyber” (2023.4)
 - IBM, “IBM X-Force Threat Intelligence Index 2021 ” (2021.2)
 - Insurance Journal, “Intangic MGA Launches Cyber Parametric Policy With Backing From AXA XL” (2023.3)
 - Insurance Europe, “2021 Pan-European Pension Survey: Key Findings” (2021.12)
 - James Andrew Lewis, Zhanna Malekos Smith, & Eugenia Lostri, “The Hidden Costs of Cybercrime” (McAfee, 2020.12)
 - Joseph Carson, “Reports of ransomware attacks are declining, but don’t start celebrating yet” (Delina, 2023.1)
 - KPMG, “Closing the Gap: Cyber Security and the insurance sector” (2017.7)
 - Leigh Wolfrom, “Insurance Policy Insights: Building a Sustainable Cyber Insurance Market - The Role of Public Policy and Regulation” (OECD, 2018.4)
 - Lloyd’s, “Closing the gap: Insuring your business against evolving cyber threats” (2017.6)
 - Maria Dinzeo, “Cyberattacks are accelerating with AI's help” (PropertyCasualty360, 2023.6)
 - Munich Re, “Cyber insurance: Risks and trends 2023“ (2023.4)
 - Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022” (2022.5)
 - NAIC, “Report on the Cyber Insurance Market” (2022.10)
 - OECD, “Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation” (2020.2)
 - OECD, “Enhancing the Availability of Data for Cyber Insurance Underwriting: The Role of Public Policy and Regulation” (2020.2)
 - OECD, “Pensions at a Glance 2021: OECD And G20 Indicators” (2021.12)
 - S&P Global, “Cyber Trends and Credit Risks” (2022.10)
 - SonicWall, “2023 SonicWall Cyber Threat Report” (2023.3)
 - Swiss Re, “Asia's health protection gap: Insights for building greater resilience” (2019.1)
 - Swiss Re Institute, “Cyber insurance: strengthening resilience for the digital transformation” (2021.5)
 - Swiss Re Institute, “Emerging markets: the drive for sustainable retirements in an ageing world” sigma No2/2021 (2021.6)

- ・ Swiss Re Institute, “Natural catastrophes and inflation in 2022: a perfect storm” sigma No1/2023 (2023.3)
- ・ Swiss Re Institute, “Natural catastrophes in times of economic accumulation and climate change” sigma No2/2020 (2020.4)
- ・ Swiss Re Institute, “The health protection gap in Asia: a modelled exposure of USD 1.8 trillion” (2018.10)
- ・ Swiss Re Institute, “World insurance: inflation risks front and centre” sigma No4/2022 (2022.7)
- ・ WEF, “The Global Risks Report 2023: 18th Edition, Insight Report” (2023.2)
- ・ World Bank, “Tracking an Unprecedented Year for Businesses, Everywhere” (2021.2)
- ・ World Health Organization, “Global spending on health: Weathering the storm” (2020.12)
- ・ Xenia Scheil-Adlung, “Global evidence on inequities in rural health protection: New data on rural deficits in health coverage for 174 countries” (ILO,2015.5)

<参考ウェブサイト>

- ・ 企業年金連合会 <https://www.pfa.or.jp/>
- ・ 警察庁 <https://www.npa.go.jp/>
- ・ 公安調査庁 <https://www.moj.go.jp/psia/>
- ・ ニッセイ 基礎研究所 <https://www.nli-research.co.jp/>
- ・ 日本損害保険協会 <https://www.sonpo.or.jp/>
- ・ 三井物産セキュアディレクション <https://www.mbsd.jp/>
- ・ リスク対策.com <https://www.risktaisaku.com/>
- ・ Coincheck <https://coincheck.com/ja/>
- ・ Cyber Security.com <https://cybersecurity-jp.com/>
- ・ IBM <https://www.ibm.com/>
- ・ NEC <https://jpn.nec.com/>
- ・ PR Times <https://prtimes.jp/>
- ・ Sompo Cyber Security <https://www.sompocybersecurity.com/>
- ・ SonicWall <https://www.sonicwall.com/ja-jp/>
- ・ Tenable <https://jp.tenable.com/>
- ・ 経済協力開発機構 (OECD) <http://www.oecd.org/>
- ・ 国際通貨基金 (IMF) <https://www.imf.org/>
- ・ 国際保険協会連盟 (GFIA) <https://gfiainsurance.org/>
- ・ 国際労働機関 (ILO) <https://www.ilo.org/>
- ・ 全米保険監督官協会 (NAIC) <https://content.naic.org/>
- ・ 保険監督者国際機構 (IAIS) <https://www.iaisweb.org/>
- ・ Allianz <https://www.allianz.com/>

- ・ Aon <https://www.aon.com/>
- ・ Asia Insurance Review <https://www.asiainsurancereview.com/>
- ・ AXA <https://www.axa.com/>
- ・ Beazley <https://www.beazley.com/>
- ・ Check Point <https://www.checkpoint.com/>
- ・ Chubb <https://www.chubb.com/us-en/>
- ・ Corvus <https://www.corvusinsurance.com/>
- ・ CSIS <https://www.csis.org/>
- ・ Cybercrime Magazine <https://cybersecurityventures.com/>
- ・ Delinea <https://delinea.com/>
- ・ Fintech Finance News <https://ffnews.com/>
- ・ Fortune Business Insights <https://www.fortunebusinessinsights.com/>
- ・ Geneva Association <https://www.genevaassociation.org/>
- ・ GlobalData <https://www.globaldata.com/>
- ・ HDI Global <https://www.hdi.global/>
- ・ IF*TRIP <https://iftrip.org/>
- ・ Insurance Europe <https://www.insuranceeurope.eu/>
- ・ Insurance Journal <https://www.insurancejournal.com/>
- ・ Insurance Post <https://www.postonline.co.uk/>
- ・ Intangic MGA <https://www.intangic.com/>
- ・ KPMG <https://kpmg.com/>
- ・ McAfee <https://www.mcafee.com/>
- ・ Munich Re <https://www.munichre.com/>
- ・ OpenAI <https://openai.com/>
- ・ Reinsurance News <https://www.reinsurancene.ws/>
- ・ S&P Global <https://www.spglobal.com/>
- ・ Swiss Re <https://www.swissre.com/>
- ・ World Bank <https://www.worldbank.org/>
- ・ Zurich <https://www.zurich.com/en>