保険を利用して サイバーレジリエンスの強化を図る

調査研究概要｜2026年3月

Darren Pain, Director of Research, Geneva Association
Sasha Romanosky, Senior Policy Researcher, RAND

サイバーインシデント（不正アクセス、機密情報漏洩など情報セキュリティ上の脅威となる事象）の発生頻度の高まりとともに、その被害額も増加の一途をたどっています。サイバーセキュリティ侵害に起因する一件当たりの年間損失額の中央値は、過去 15 年間で 15 倍に達しており、当初の 19 万ドルから 300 万ドルに迫る勢いで増加しています。大規模なインシデント事案を原因とする損失額も急増しており、2024 年における損失額上位 10%の事象では平均値が 2,800 万ドルを超えており、2008 年に記録した水準のほぼ 5 倍になっています。[1]

各企業では、サイバーリスクを事業運営上の主要な懸念事項の一つとしてますます強く認識するようになっています。とはいえ、こうしたサイバーインシデントの多くは、依然として、フィッシング詐欺に対する脆弱性、脆弱なパスワードの使用、修正プログラム未適用のソフトウェア、設定が不適切なシステムなど、基本的かつ予防可能な脆弱性に起因して発生しています。保険会社は、企業のサイバーセキュリティ対策の強化を図り、企業全体のサイバーレジリエンスを高めるうえで重要な役割を担うことができます。しかしながら、一部の市場や地域では、サイバー保険の普及率は依然として低水準に留まっています。推定値によると、世界的に見ても、中小企業（SME）の内、サイバー保険に加入している企業はわずか 10%程度に過ぎません。国によっては 10%をさらに下回るところもあり、ましてや、零細企業となれば、保険に加入していないところがほとんどではないでしょうか。[2]

サイバーレジリエンス（サイバー攻撃を受けても事業を継続できる能力）と保険

「レジリエンス三角形」を見れば、企業運営が有害な障害・妨害によってどのような影響を受けるか、即ち、障害等の突然の発生により業務やパフォーマンスがどの程度落ち込み、その回復がどのような過程をたどるのかを可視化することができます。各企業のシステム構造にもよりますが、事前に適切な対策を講じることで、一定のショックは業務への影響を抑えながら吸収することが可能です。とはいえ、予期せぬ障害や事故は必ず起きます。その影響の程度は、信頼性の高いバックアップシステムの整備や、機能停止の拡大を抑えるために事業部門の一部を分離する仕組み、さらに対応・復旧に必要な資金や物的資源を確保できるかどうかに大きく左右されます。この三角形モデルは、障害等発生前・発生中・発生後の各段階におけるシステムのレジリエンス確保に向けた企業の施策とその進捗を可視化するものであり、その形状を分析することで、システムの信頼性を確保しつつ、売上や生産量などの業績を企業レベルで維持することが可能となります（図 1 参照）。

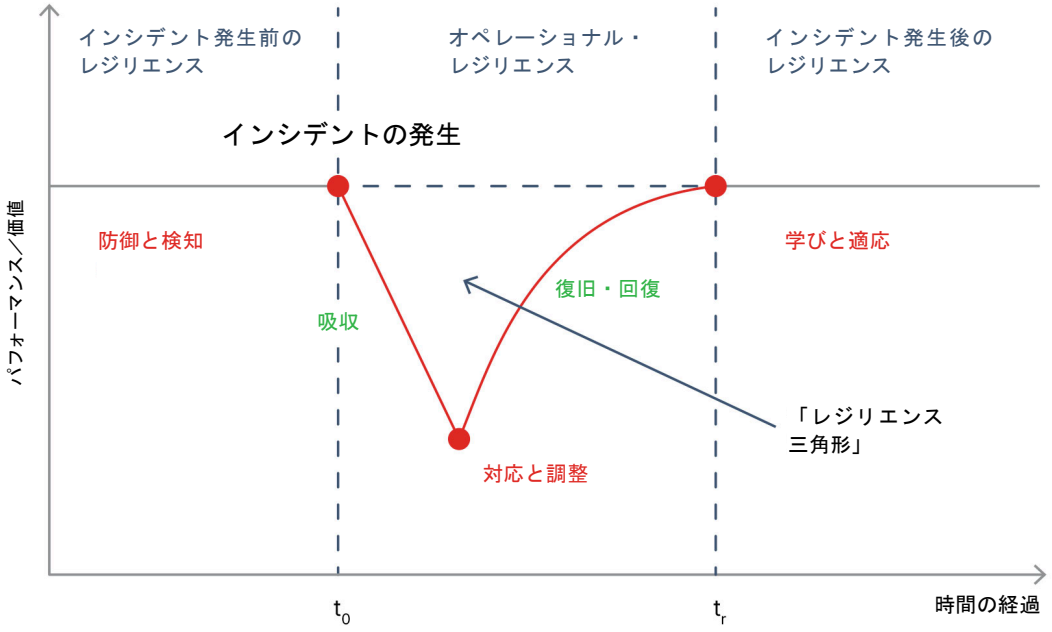
サイバー保険は当初、単なるリスク移転メカニズムの一つでしたが、現在ではサイバー脅威とその影響の管理・軽減を支援する仕組みとして進化しています。保険会社は、被保険企業に対して、一定のセキュリティ基準の策定・遵守を求めるとともに、推奨セキュリティ対策、サイバーリスクの監視と警告、インシデントの際に発生する外部専門家費用の補償など、様々なサービスをパッケージ化して提供することもできます。このように、保険を通じて、インシデント発生前後における企業のオペレーショナル・レジリエンス（サイバー攻撃等が発生しても、重要業務を最低限継続する能力）を高めることができ、レジリエンス三角形モデルの「V字」を浅くする各企業の取り組みを支援することができます。

サイバーセキュリティ対策業者は、自社製品やサービスの不具合に対する個別保証を提供する場合もありますが、サイバー保険会社は、それとは異なり、被保険者である企業がサイバーインシデントに起因するあらゆる損失（第三者が被った損害を含む）を最小限に抑えられるよう、包括的な支援を行っています。助言、ガイダンス、そして補償の間には相互に作用し合う関係があります。より効果的なサイバーセキュリティ対策を優先的に実施することで、保険金請求金額／件数を減らすことができます。同様に、サイバーセキュリティへの投資によって、保険条件の改善やインシデント対応の高度化が実現すれば、発生時の被害を抑えやすくなり、サイバー保険の実効性を高めることになります。

1 Cyentia 2025.

2 Swiss Re 2024.

図 1：レジリエンスの全体像

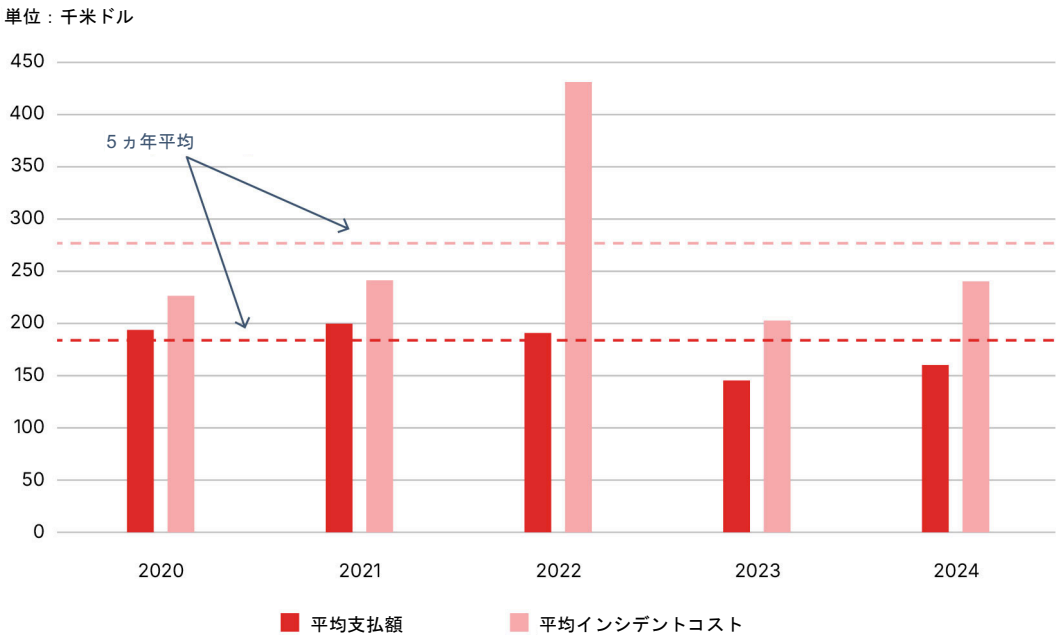


出典：Geneva Association[3]

サイバー保険はどの程度有効か？

実証研究によれば、サイバー保険会社は実際に保険金を支払うだけでなく、被保険企業のサイバーセキュリティの取り組みにも影響を与えています。ある国際的な調査では、サイバー事故報告件数の 92%がサイバー保険の補償対象範囲に含まれていました。[4] これに対し、英国の自動車保険では保険金請求件数の 90%以上、住宅保険で約 70%、訴訟費用保険は 50%強にとどまっています。[5]

図 2：中小企業におけるインシデントコストと保険金等の支払い



出典：NetDiligence

3 グラフは右記より引用。Bruneau et al.2003.
4 Willis Towers Watson 2025.
5 Financial Conduct Authority 2025.

米国、カナダ、英国のデータによると、サイバー保険の平均支払額は、インシデントコスト（インシデント対応費用）全体においてもかなりの割合を占めており、中小企業の場合には 70%近くに達しています（図 2 参照）。各種調査や事例研究の結果からも、サイバー保険会社はその引受プロセスを通じて、保険契約者である企業のサイバーセキュリティ水準の底上げに寄与していることが明らかになっています。例えば、2024 年の調査によれば、サイバー保険に加入しているほぼすべての企業・団体が、サイバー防御対策の強化にも投資を行い、サイバーリスクと保険料／補償内容の間におけるバランスの最適化に向け取り組みを進めています。調査対象企業の 4 分の 3 を超える（76%）企業・団体が、サイバー保険への加入を目的に、サイバーセキュリティへの投資を増やしていると回答しています。[6]

しかしながら、保険にはサイバーセキュリティを効果的に高める可能性がある一方で、保険の供給側と需要側の両方において、こうした機能の発揮を妨げる以下のような市場特性が依然として存在します。

- **リスクの評価・差別化の限界。**近年、引受手法は進化しているものの、保険会社はいまだに被保険企業ごとのサイバーリスク水準を正確に見極めることに苦慮しています。その結果、保険条件がセキュリティ対策の脆弱な企業に対する改善インセンティブとして十分に機能していない場合があります。

- **予防・軽減策の実施を阻む実務上の障害。**被保険者である企業の多くは、保険会社が提供するインシデント発生前のセキュリティ支援サービスを活用していません。最近の調査によると、回答した企業・団体の約 3 分の 1（32.5%）が、サイバー保険契約に含まれる無料のリスク管理サービスの存在を認識していませんでした。[7]

- **インセンティブの不整合と制度や仕組みに起因する組織間の摩擦。**保険会社、ブローカー、保険契約者の間に潜在的な利益相反があれば、事故や不正侵入発生後におけるリスク管理の取り組みを弱体化させることにもなりかねません。例えば、保険契約者は、商業的に価値のある機密情報を保険会社等に漏らすことや、企業の評判が毀損したり法的制裁につながったりする事態を懸念して、損害査定に必要な情報を提供しないことも考えられます。情報共有に対する消極的な姿勢は、透明性と信頼を損なうことになります。

- **大規模なサイバー事象に関する不確実性。**大規模なサイバーイベントに起因して生じうる累積損失の発生確率や規模は依然として不確実性が大きく、これが保険会社および再保険会社のサイバーリスクの引受意欲を引き続き抑制しています。例えば、IT システムの共通障害やマルウェアの連鎖的拡散によって、多数の保険金等請求が同時発生する事例が考えられます。

サイバー保険の普及拡大に向けた取り組み

保険は、一部の極端なサイバーリスクが最終的に保険対象とならない可能性がある場合でも、企業のサイバーセキュリティ水準の向上や、サイバーインシデントへの対応力強化を促す重要な役割を担うことができます。しかしながら、とりわけ中小企業（SME）においてサイバー保険の普及を拡大し、サイバーレジリエンス向上に不可欠なツールとしての役割を強化するには、複数の利害関係者による取り組みを組み合わせて実施する必要があります。このような取り組みには次のようなものがあります。

- **サイバーリスクおよび補償の価値に対する認識向上。**引受プロセスや保険会社との継続的な関与を通じて、契約者のリスクプロファイルを大きく改善できる可能性があります。特に中小企業では、過失や管理不足が主要なリスク要因となっており、改善の余地が大きいと言えます。このことは、保険会社（およびブローカー）が、サイバーリスクや保険に含まれる予防的なセキュリティ対策について、顧客教育への投資を強化する余地があることを示唆しています。先見性のあるサイバー保険会社は既にこうした点を理解しており、契約者との関係においてレジリエンスの向上を重視しています。

- **契約者ニーズに応じた補償内容の提案。**引受手法の進化により、契約者のニーズに適合するきめ細かな補償設計が可能となっています。これには、強制的な業務停止への対応、規制当局による罰金・制裁への備え、さらにはサイバー事故に起因する物的損害や事業中断による損失への補償などが含まれます。近年では、事業中断リスクに対する保険金支払いの迅速化を目的として、パラメトリック型や協定価額型の商品が注目されており、既存契約への特約付加や単独商品として提供されるケースが増えています。

- **中小企業向けの保険商品・手続の簡素化。**顧客体験の簡素化が重要な課題となっています。具体的には、契約内容が理解しやすい保険設計、スムーズな加入プロセス、および引受・保険金請求手続の効率化が求められます。例えば、専門用語を避けた分かりやすい約款を、各国の規制や業界特性に応じて整備することが重要です。透明性の高い約款により、補償範囲や免責事項が明確になり、契約者と保険会社の信頼関係構築や、長期的で安定したサイバーセキュリティパートナーシップの確立につながります。

- **顧客ニーズとリスク特性に応じた販売チャネルの整備。**サイバー保険そのものに加え、顧客と保険会社・ブローカーとの接点のあり方も見直しが必要です。すでに新たな流通モデルが登場しており、例えば 2024 年 5 月にはブローカーの Howden 社が中小企業向けのサイバー保険プラットフォームを立ち上げました。[8] また、一部の保険会社は IT サービスやソフトウェア、セキュリティ製品の購入時に保険を組み込む「組み込み型（エンベデッド）保険」を導入し、特に中小企業における保険普及の拡大を目指しています。

6 Sophos 2024.
7 QBE 2024.
8 Howden 2025.

- **デジタルインフラ事業者との連携強化。**保険会社は、ネットワークやアプリケーション、端末、クラウド環境など複数のソースからデータを自動的に収集・分析する高頻度テレメトリ（測定）への投資を強化する必要があります。これにより、契約者の IT 脆弱性やセキュリティ状態をより正確に把握できます。さらに、AI の活用によって保険料設定の精度向上、損害発生の抑制、レジリエンス強化が期待されます。こうした継続的引受審査（保険会社が契約者のリスクを、契約期間中も常時、リアルタイムで評価・更新する手法）への移行は、インフラ提供事業者やセキュリティ企業との連携強化によって一層促進されます。

- **政府機関との連携・協力。**保険会社は、事故や損失、脆弱性に関する豊富なデータを保有している一方、政府機関は新たな脅威や攻撃手法に関する機密情報や集約データを有しています。これらを安全かつ適切に共有することで、企業は早期警戒、リスク評価の高度化、新たな脅威への備えの強化といった恩恵を受けることができます。また、情報共有に加え、保険会社と政府が連携して基本的なセキュリティ対策の標準化と普及を進めることで、保険加入の要件整備や、将来的な義務化の検討にもつながります。

- **システム全体のレジリエンス強化に向けた取り組み。**大手テクノロジー企業では、脆弱性の発見を促進するために、外部研究者への報奨金制度（バグバウンティ）を活用しています。保険会社が保険料の一部を活用してこうした仕組みを支援することも検討する余地があります。ホワイトハッカーの知見を、自動化された脆弱性検出や防御技術の高度化に活用できれば、セキュリティ向上への効果は大きいと期待されます。一方で、こうした取り組みを実装するには、ソフトウェアベンダー、契約者、保険会社のインセンティブ調整に加え、法規制面の課題への対応も含めた慎重な制度設計が必要となります。

参考文献

Bruneau, M. et al. 2003. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra* 19 (4): 733-752.

Cyentia. 2025. *Information Risk Insight Study 2025*.

Financial Conduct Authority. 2025. *General Insurance Value Measures Data 2024*.

Howden. 2025. *Rebooting Growth: Howden's 2025 Cyber Insurance Report*.

QBE. 2024. *2024 Cyber Insurance Report*.

Sophos. 2024. *Cyber Insurance and Cyber Defenses 2024*.

Swiss Re. 2024. *Reality Check on the Future of the Cyber Insurance Market*.

Willis Towers Watson. 2025. *Boards Risk Costly Cyber Exposure as Confidence Outpaces Preparedness, According to Willis Report*.