保険の2030年アジェンダ

シリーズ 38

フロンティアAIの標的になる中小企業を支えるサイバー保険

AI駆動型攻撃が容易にできるようになり、中小企業を含むサプライチェーン全体がサイバーリスクに直面している。米国サイバー保険のモデルを踏まえ、大企業を起点としたサプライチェーン全体のリスク診断と包括的補償を組み合わせたフロンティアAI時代のサイバー保険が有効であると考えられる。

容易になるフロンティアAIによるサイバー攻撃

2026年4月にAnthropicが発表した「Claude Mythos」に代表されるフロンティアAI[1]の登場は、脆弱性の自律的な探索や攻撃コードの自動生成を可能にし、サイバー脅威を前例のないレベルへ引き上げた。NICT[2]の観測データでは攻撃通信数が年々増加しており、「情報セキュリティ10大脅威 2026」でも「AIの利用をめぐるサイバーリスク」が3位に初ランクインしている。

フロンティアAIの代表的な攻撃事例である高度なフィッシングやAI駆動型マルウェアの本質は、「低コストで容易に実行できるサイバー犯罪」にある。日本では従来、費用対効果の観点から攻撃対象になりにくかったサプライチェーンの約9割を占める中小企業が、今後は標的となる可能性が出てきた。保険業界にとっても大きな課題を抱えることになったといえよう。

現在のサイバー保険は、必然的に事前（予測、予防）、事後（補償、復旧）それぞれの機能毎に見直しが求められることになるだろう。

事前段階におけるリスク評価は、質問票や過去の事故履歴などに基づく静的な審査に依拠する場合が多く、契約後に変化する脆弱性や攻撃環境を継続的に反映する仕組みは限定されている。こうした静的な審査のもとでは、日々進化するAIに対してリスク評価がすぐに陳腐化する。引受時点では把握できなかった脆弱性や攻撃手法が短期間で顕在化し、保険会社は実態よりも低くリスクを見積もるおそれがある。

事後段階において最も重要なポイントは、初動対応である。攻撃が高度化し高速化する中では、初動対応の遅れが損害拡大に直結する。被害は短時間で他の端末やシステムに波及し、事後段階における復旧はより一層、困難になる。

米国サイバー保険MGAの事例

世界のサイバー保険市場の過半数を占める米国[3]では、サイバー保険MGA（Managing General Agent）[4]による事前段階および事後段階での取り組みが進んでいる。その概要を図表に示す。

米国のサイバー保険MGAでは、継続的データ取得による最新リスクスコアリング、専門チームやAIによるリアルタイム監視、AIツール導入による動的な支払い限度額の設定、そして専門チームやAIによる自動検知を通じた迅速な復旧など、統合的にサイバー保険として

図表　米国サイバー MGAの取り組み

区分		アプローチ	会社/サービス	事例概要
事前	予測	・継続的データ取得による最新リスクスコアリング ・兆候検知	Cowbell/ Cowbell Factors	中小企業向けのサイバーリスク評価システム。AIで社内外の**データを継続的に取得・分析して、最新のリスクスコアリングを実施**。セキュリティの脆弱性の可視化を提供。
			Coalition	**データを継続収集し、シミュレーションによりサイバーイベントの財務影響を推計。シナリオを評価**し、保険金支払額の算出に活用。
	予防	・専門チームやAIによるリアルタイム監視	At-Bay/ Stance MDR	専門家チームがAI技術を活用し、**リアルタイムで脅威を監視・検知**。不審な動きを、自動的に遮断し修復を実施。
			At-Bay/ Fraud Defense	ビジネスメール詐欺（BEC）やインボイス詐欺など、検知が難しい巧妙な詐欺を**AIがリアルタイムで検知・ブロック**。
事後	補償	・AIツール導入による動的な支払い限度額	At-Bay	Stance MDRやFraud Defenseの導入により、**補償の増額や自己負担額の軽減**が適用される。
	復旧	・専門チームやAIによる自動検知を通じた迅速な復旧	Coalition/ Wirespeed	MDRプラットフォームを通じて、脅威を**ミリ秒単位で**自動検知・遮断。
			At-Bay/ Response & Recovery	インシデント対応の専門チームが**報告後平均5分以内という迅速な対応**で、被害の優先順位付けと封じ込めを行う。

（出所）各種資料を基に野村総合研究所作成

野村総合研究所　金融ITイノベーション事業本部 事業企画室

NOTE

1) フロンティアAI：現在の生成AIの延長線上にある「最先端AI」。
2) NICT：国立研究開発法人 情報通信研究機構 (National Institute of Information and Communications Technology)。
3) 「2026 Cyber Insurance Market Outlook」より https://www.ajg.com/-/media/files/gallagher/us/news-and-insights/2025/2026-cyber-insurance-market-outlook.pdf
4) MGA (Managing General Agent)
保険会社から実質的なリスク引受権限や、商品開発、保険料の決定などを委任されている機関。
5) NAICS (北米産業分類システム)。
6) 「自社スコアが業界平均より7ポイント低い組織は、8ポイント高い組織と比較して保険金請求確率が11倍高い」という実証結果が示されている。
7) 日本国内では一般社団法人　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2025 調査結果報告書」によれば、中小企業の付保率は8.8%となっている。

提供している。

本稿ではその中でも、中小企業向けにサイバーリスクの動的評価と迅速な保険引受を実現している事例としてCowbellの「Cowbell Factors」を紹介したい。

Cowbell Factorsは、サイバーリスクを客観的に定量化し、必要な補償内容と適切な保険料を算出するためのリスク評価システムである。リスク評価は、ネットワークセキュリティ、クラウドセキュリティ、資金移動リスクなどの8つの指標で構成されている。本システムの重要なポイントを二点ほど指摘する。

一つ目は、見積もりの迅速化である。迅速化を実現している要因は、継続的なデータ取得と、取得データを活用した事前リスク計算にある。継続的なデータ取得においては、外部データ（インターネット上に公開されているインフラをスキャンし得られたIPアドレスやポート等の外部リスクシグナル）やダークウェブの脅威情報等を収集している。

また、事前リスク計算においては、取得したリスクシグナルを基にAIおよび機械学習アルゴリズムによってリスクを数値化している。これらの仕組みにより、見積もりプロセスを5分以内に短縮することが可能となっている。

二つ目は、リスクスコアリングを補償範囲の選定や保険料算定に活用している点である。この実現手法として、同社は巨大なデータプールを活用した「同規模・同業者との比較」というアプローチを採用している。データプールはNAICS[5]の6桁コードを用いた比較対象の粒度を細分化し、米英の中小企業3,800万社からなるリスクデータプールを構築している。これにより精緻なリスク評価[6]と、企業ごとの補償範囲の選定や適正な保険料算出へと結びつけることを実現している。

日本における サプライチェーンサイバー保険の展開

日本では中小企業のサイバー保険付保率は8.8%[7]に留まり、AI技術の普及による攻撃の容易化によるサプライチェーンを通じた被害拡大リスクは高いといえる。中小企業は予算・人材面の制約から独自の対策が困難である一方、大企業にとってもサプライヤーである中小企業の脆弱性は自社の事業継続リスクに直結しており、双方にとって解決すべき課題であるという認識が求められる。

この課題の解決策として、「サプライチェーン統合型サイバー保険」を提案したい。この保険は、大企業を起点としてサプライチェーン全体のリスクを診断し、その結果を基に必要な保険に加入する仕組みである。このモデルの実現には、サイバーリスクを評価する仕組みやそれを基に補償や保険料に落とし込む仕掛けが必要であり、米国の事例が参考になる。

また、サプライチェーン統合型サイバー保険では、大企業が窓口となり、サプライチェーン全体の契約を主導することで、中小企業の予算制約や人材不足の課題解決や事務コストの削減にもつながる。さらに、サプライチェーン全体のリスク評価による料率を設定することで、中小企業が単独で加入する場合と比べて保険料を抑えられる可能性がある。中小企業のサイバーリスクへの有効な手段と考えられる。

Writer's Profile

坂野 敦志 Atsushi Banno
保険デジタル企画部
エキスパートコンサルタント
専門はAI、損害保険システム
focus@nri.co.jp