保険・年金フォーカス

サイバーリスクのモデリング

相互に接続されたシステミックリスクをどうモデリングする?

保険研究部 主席研究員　篠原　拓也
(03)3512-1823　tshino@nli-research.co.jp

1――はじめに

サイバーリスクの脅威が拡大している。マルウェアによるウイルス感染により、ネットワーク端末の機能を使用不能にしたり、ファイルを暗号化して使用できなくしたりして、それらを使用可能とするための身代金を要求する、ランサムウェア攻撃[1]。別人のふりをしてメールを送信したり電子掲示板に書き込みを行ったりする、なりすまし。実在の金融機関等を装ったメールを送付してクレジットカード番号などの情報を入力させて詐取する、フィッシング詐欺。その他、DDoS 攻撃、不正アクセス、パスワードクラッキングなど、企業や個人を問わず、日常的にサイバーリスクにさらされている。

損保会社は、サイバー保険の開発や引き受けを通じて、サイバーリスクへの補償を行っている。その前提となるサイバーリスクの定量化、保険料設定に関して、リスクのモデリング手法についての議論が世界的に行われている。欧米のアクチュアリー会では、このテーマに対する報告書が公表されている。本稿では、その中から、2023 年にヨーロッパアクチュアリージャーナルに掲載された報告書[2](以下、「報告書」と呼ぶ)をもとに、その議論を概観していくこととしたい。

2――サイバーリスクの分類

モデリングを行うためには、それに見合うよう、リスクを適切に分類することが必要となる。まずは、その分類から見ていこう。

1｜サイバーリスクには、特異的、システマティック、システミックの 3 つのタイプがある

ひとくちにサイバーリスクといっても、さまざまなものがある。モデリングにあたっては、被害の規模や拡大に応じて、3 つのタイプ(特異的、システマティック、システミック)に分類されることが一般的とされる。

---

[1] ランサムウェア攻撃では、身代金が支払われても、端末やファイルが使用可能になるとは限らず、それどころか保存データを公開すると再び脅迫して、被害が二重、三重に拡大するケースもある。

[2] “Modeling and pricing cyber insurance - Idiosyncratic, systematic, and systemic risks” Kerstin Awiszus, Thomas Knispel1, Irina Penner, Gregor Svindland, Alexander Voß, Stefan Weber (European Actuarial Journal (2023) 13:1-53, https://doi.org/10.1007/s13385-023-00341-9)

(1) 特異的リスク

企業や個人に個別に影響を与える独立したサイバーリスクを指す。例えば、企業内のネットワークのエラーによって引き起こされるものが該当する。

典型的な特異的リスクは、古典的な保険数理手法の適用が可能となる大規模な保険プールにおける独立したリスクである。

(2) システマティックリスク

異なる企業に同時に影響を与える企業体共通の脆弱性に起因するサイバーリスクである。例えば、同じ業種や地域に属する企業、同じソフトウェア、サーバ、コンピュータ・システムを利用する企業などである。これらのリスクは、共通のリスク要因によってモデル化できる。

古典的な保険数理および金融数学の観点からは、システマティックリスクには金融市場リスク、国民の死亡率の変動リスクなどが含まれる。

(3) システミックリスク

相互に接続されたシステムにおける局所的またはグローバルな感染、あるいは相互作用によって引き起こされるサイバーリスクである。例えば、ワーム型マルウェアやサプライヤー攻撃がある。

これらのリスクは、金融危機において観察される重要なフィードバックメカニズムに類似している。例えば、取引相手のネットワークにおける感染や、流動性の低い市場におけるストレスを受けた市場参加者の投げ売りなどである。システミックリスクには、古典的な保険数理や金融数学とは別の、相互接続性に焦点を当てたモデルの構築が必要となる。

図表 1. サイバーリスクの 3 つのタイプ

	特異的リスク		システマティックリスク		システミックリスク	
	標的型攻撃	個別障害	標的型攻撃	システム障害	非標的型攻撃	大規模障害
データ侵害	個別の標的型データ盗難	個人が意図しないデータ開示	特定システムに対する標的型データ盗難	小規模クラウドプロバイダでの意図しないデータ開示	広範囲に渡るマルウェアやフィッシングによるデータ盗難	大規模クラウドプロバイダでの意図しないデータ開示
業務の中断	標的型ランサム攻撃	偶発的な誤動作によるシステムやシステムやプロセスの混乱	同じソフトウェアに依存するシステムを混乱させる攻撃	ソフトウェア障害によるシステムの混乱	広範囲に渡るランサム攻撃	クラウドの停止によるビジネスサービスの混乱
詐欺	ホエーリング攻撃(経営幹部に対する攻撃)を通じた CEO 詐欺	従業員によるデータベースへの偶発的侵害	小規模クラウドプロバイダの従業員によるデータベース侵害	小規模クラウドプロバイダでの障害発生を起因としたデータベース侵害	広範囲に渡るランサム攻撃やソーシャルエンジニアリング詐欺*	大規模クラウドプロバイダに保存されているデータの偶発的侵害

＊ ソーシャルエンジニアリング詐欺とは、電話でパスワード聞き出す、肩越しに画面をのぞき見る、ゴミ箱に捨てられた資料を漁るといった行為を通じた詐欺

※“Cyber Risk Modeling Methods and Data Sets: A Systematic Interdisciplinary Literature Review for Actuaries”(SOA Research Institute, Sept. 2022)をもとに、筆者作成

2｜モデリングには、CRO フォーラムのサイバーリスク分類は用いにくい

サイバーリスクの分類として、さまざまなものが公表されている。そのなかで、よく知られているものとして、CRO フォーラムが 2016 年に示した分類が挙げられる。この分類は、データを取得したり、仕分けしたりするにはよい。だが、前節の 3 タイプに区分しづらく、モデリングには不向きとされる。

図表 2. CRO フォーラムが公表したサイバーリスクの分類

サイバーインシデント	事象の種類	根本の原因	行為者
1. システムの誤動作・誤用	オペレーショナルリスクのカテゴリー	A. 人間	1. 国家
2. データの機密性		B. 外部要因	2. 組織犯罪者
3. データの正当性・可用性		C. プロセス	3. ハッカー
4. 悪意のある行動		D. システム	4. ハクティビスト*1
			5. 内部関係者

影響の種類			
1. 事業の中断	7. インシデント対応コスト	13. コミュニケーションとメディア	18. 技術職業務過誤賠償責任
2. 物的損害がない状況での偶発的事業中断	8. プライバシー侵害	14. 法的保護(弁護士費用)	19. 専門職務過誤賠償責任
3. データとソフトウェアの損失	9. ネットワークセキュリティとその機能停止	15. 援助カバー－心理的支援	20. 環境被害
4. 金融上の盗難や詐欺	10. 風評被害(法的保護を除く)	16. 製品	21. 物的資産被害
5. サイバー身代金と恐喝	11. 法規制の防衛コスト(罰金と罰則を除く)	17. 役員賠償責任	22. 身体傷害と死亡
6. 知的財産の盗難	12. 罰金と罰則		

*1 政治的あるいは社会的な主張・目的のためにハッキングを行う個人や集団
※“CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk”(CRO Forum, June 2016)をもとに筆者作成

3｜インシデントを特異的やシステミックなどのリスクに区分することが望ましい

サイバーリスクのモデリングのためには、インシデントを特異的やシステミックなどのリスクに区分することが望ましい。例えば、次表の Zeller 氏と Scherer 氏の論文によるものが考えられる。

図表 3. Zeller 氏と Scherer 氏の論文でのサイバーリスク分類

	特異的インシデント 標的型攻撃	個別の障害	システミック事象 非標的型攻撃	大規模障害
データ侵害	標的型データ盗難	個々の意図しないデータ漏えい	広範なマルウェアやフィッシングによるデータ盗難	クラウドサービスプロバイダーでの意図しないデータ漏えい
事業の中断	標的型(D)DoS/ランサムウェア攻撃	偶発的な誤動作による IT システムまたはプロセスの中断	広範なランサムウェア攻撃	クラウドサービスの停止によるビジネスサービスの中断
詐欺全般	標的型(スピア)フィッシング攻撃による CEO 詐欺	従業員によるデータベースの偶発的な侵害	広範なランサムウェア攻撃またはソーシャルエンジニアリング詐欺*2	クラウドサービスプロバイダーに保存されているデータの偶発的な侵害

*2 人間の感情(恐怖心や緊急性等)を利用して攻撃者への送金、顧客の機密情報の漏洩、認証情報の開示など実行するよう仕向ける詐欺
※“A comprehensive model for cyber risk based on marked point processes and its application to insurance” Zeller G, Scherer M (Euro Actuarial J, 12:33-85, 2022)をもとに筆者作成

3――サイバーリスクの特徴

サイバーリスクにはいくつかの特徴がある。

(1) サイバーリスクの発生や被害額のデータは、十分な量または必要な粒度で利用できない

データが望ましい量と粒度で利用可能であれば、統計学の最尤法によって、サイバーインシデントの発生を推定することができる。しかし、実際には、利用可能なデータは限られる。これは、インシデントが発生しているが検知されていないケースや、発生して被害が出ているが被害額がわからないケースなどがあるためだ。さらに、被害を受けた企業や個人が、被害を受けたことを公表しない可能性もあるため、データは不十分なものになりがちとされる。

(2) テクノロジーとサイバーの脅威は急速に拡大しており、サイバー環境は非定常な状態にある

サイバー環境は変化が激しい。過去のデータと将来のリスク発現の関連性は、時間とともに低下する可能性が高い。このため、高度なモデリング技術に支えられた専門家の意見とデータの統計的評価を組み合わせることが重要である。

(3) サイバーインシデントには、独立性の仮定は成り立たない

サイバーインシデントは、複数の保険契約者に同時にもしくは連鎖的に影響を及ぼす可能性がある。これは、サイバーリスクの依存関係という特徴を示している。依存関係には、契約者間の依存性の他に、発生するインシデントの頻度と深刻度の間の依存関係も加味する必要があるとされる。

(4) サイバーインシデントには、地理的な制約がない

サイバーリスクは、突然発生して、甚大な被害をもたらす地震などの自然災害と似ている面がある。しかし、一つ大きな違いがある。自然災害のような発生地域の地理的な制約がない点である。サイバーリスクは、国境や地形などと無関係に発現する。複数の地域、場合によっては全世界で一斉に起こる可能性もある。

4――サイバーリスクのモデリング

サイバーリスクの被害の予測を行うためには、前章までに見たサイバーリスクの特徴や、データの特性を踏まえて、モデリングを行うことが必要となる。報告書をもとに、具体的に見ていこう。

(1) 特異的リスクのモデリング

特異的リスクについては、古典的な保険数理にもとづく価格設定が適用できる。これは、事象間の独立性を前提として、大数の法則が成り立つことを仮定できることによる。標準偏差原理などを用いて、過去のデータに対して一定の安全割増を上乗せすることで、発生率や被害額の見積もりが可能となる。

(2) システマティックリスクのモデリング

システマティックリスクは、同じ業種や地域に属する企業、同じソフトウェア、サーバ、コンピュータ・システムを利用する企業に一斉に被害が生じる可能性がある。これは、株式投資等において、株価等の暴落により投資家が一斉に損失を被る価格変動リスクに似ている面がある。

そこで、現実のリスク指標とは別に、リスク中立確率指標[3]を用いることで、システマティックリス

[3] 市場の投資家がすべてリスク中立者であると想定することで、どんなにリスクのある金融資産でもその期待収益率は無リスク金利、いわゆるリスクフリーレートと同じになるとして、プライシングを行う。このような世界で成立していると考えられる確率は、リスク中立確率と呼ばれる。

クをプライシングすることが考えられる。システマティックな損失は、すべての保険契約者が共同でさらされる共通のリスク要因によって引き起こされる、と仮定することで、その定量化を行う。

(3) システミックリスクのモデリング

システミックリスクについては、相互に接続されたシステムにおけるリスク評価を行う必要がある。その手法については、さまざまな方法が模索されている。

報告書では、ホークス過程、感染ネットワークモデル、ゲーム理論モデルの 3 つが紹介されている。

(a) ホークス過程

ホークス過程とは、不規則な時間間隔で発生する事象について、その時間間隔をモデル化した確率過程で、事象の発生が後続の事象の発生頻度を増加させる「自己励起性」という性質を表すものをいう[4]。時間間隔をモデル化した確率過程としては、定常ポアソン過程がよく知られている。これは、事象の発生確率が観測時間の長さに比例するとの仮定を置いたもの。一般に、瞬間の事象の発生率は強度と呼ばれ、その時間変化は時間を変数とする強度関数として表される。定常ポアソン過程では、この強度関数が時間によらない定数となる。一方、ホークス過程では、強度関数として、定数項に過去の事象からの影響を表す励起関数を加えたものを用いる。励起関数は、過去の事象が未来の事象の発生にどれだけの影響を与えるかを示す関数である。これにより、発生の強度が変化するサイバーインシデントの様子を、モデルとして表現することができる。

(b) 感染ネットワークモデル

システミックリスクの相互接続性を、疫学における感染症の感染ネットワークモデルとしてモデリングすること。

感染ネットワークモデルとして有名なものとして、SIR モデルが挙げられる。これは、ある集団を免疫を有しない未感染者(Susceptible, S)、感染者(Infected, I)、免疫を持つ回復者(Recovered, R)の 3 つの群団に分けて、群団間の時間ごとの推移を微分方程式等で表すもの。

ただし、サイバーリスクの場合、マルウェアの感染から回復した端末が免疫を持つとは限らないため、SIR ではなく SIS モデルとして表すことが適切と言えるかもしれない。

(c) ゲーム理論モデル

保険契約を、保険契約者、保険会社、規制当局の 3 つのプレーヤーの防衛機能に基づくものとして、3 者の戦略の効用を、ゲーム理論を用いて定量化する。

保険契約者の立場からは、保険に加入する場合と、加入しない場合の期待効用を算定する。保険会社の立場からは、競争的な保険市場、独占的な保険市場、寡占的な保険市場のそれぞれについて、サイバー保険の収益(保険料収入から保険金支払を差し引いたもの)を計算する。規制当局の立場からは、社会的厚生関数として、例えば、各保険契約者の期待効用の合計額を算定する。

その上で、3 者がとりうる戦略にもとづくこれらの効用の落ち着き先により、モデリングを行う。

(1)～(3)を組み合わせることで、実際のサイバーリスク環境に応じたモデリングが可能となる。具体的な組み合わせ方については、定まった方法はなく、現在も研究が続いている模様である。

[4] 1971 年にイギリスの統計学者 Alan G. Hawkes 氏により提案された。

5――おわりに（私見）

本稿では、サイバーリスクのモデリングについて紹介していった。サイバーリスクの特徴として挙げられるテクノロジーとサイバーの脅威は急速に拡大しており、サイバー環境は非定常な状態にある。このため、サイバーリスクのモデリング手法の検討は、まだしばらく続くものと考えられる。特に、システマティックリスクやシステミックリスクについては、リスクの同時多発や相互接続をどのようにモデル化するか、さまざまなモデルが考えられる。金融モデル、疫学モデル、ゲーム理論など、さまざまな分野のモデルを活用する取り組みが模索されている。

生成 AI の出現・普及に応じて、サイバーリスクの脅威は高まり、さらなる対応の高度化が求められるものとみられる。そのためには、モデリングを通じた、サイバーリスクの予測がますます有用となろう。今後も、サイバーリスクに関するモデリングの動向をウォッチしていくこととしたい。

（参考文献）

“Modeling and pricing cyber insurance - Idiosyncratic, systematic, and systemic risks” Kerstin Awiszus, Thomas Knispel1, Irina Penner, Gregor Svindland, Alexander Voß, Stefan Weber (European Actuarial Journal (2023) 13:1-53, https://doi.org/10.1007/s13385-023-00341-9)

“Cyber Risk Modeling Methods and Data Sets: A Systematic Interdisciplinary Literature Review for Actuaries”(SOA Research Institute, Sept. 2022)

“A comprehensive model for cyber risk based on marked point processes and its application to insurance” Zeller G, Scherer M (Euro Actuarial J, 12:33-85, 2022)

“CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk”(CRO Forum, June 2016)

「Hawkes 過程の理論と実証 －東京金先物市場への応用－」砂田洋志(山形大学, 2021 年)

「点過程モデリングを用いた金融時系列データの解析」近江崇宏(東京大学, 生産技術研究所, 「生産研究」第 70 巻第 3 号, 2018 年)