EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# サイバー保険 - モデルと手法、AI の活用

ENISA リサーチ＆イノベーション・ブリーフ

2024 年 2 月

## ENISA について

欧州連合サイバーセキュリティ機関（ENISA）は、欧州全体で高い共通レベルのサイバーセキュリティを実現するための欧州連合の機関である。2004 年に設立され、EU サイバーセキュリティ法によって強化された欧州連合サイバーセキュリティ機関は、EU のサイバー政策に貢献し、サイバーセキュリティ認証制度によって ICT 製品、サービス、プロセスの信頼性を高め、加盟国および EU 機関と協力し、欧州が明日のサイバー課題に備えるのを支援する。知識の共有、能力開発、意識向上を通じて、同機関は主要な利害関係者と協力し、コネクテッド・エコノミーに対する信頼を強化し、EU のインフラの回復力を高め、最終的には欧州の社会と市民のデジタルセキュリティを維持することを目指している。ENISA とその活動の詳細については、www.enisa.europa.eu。

## コンタクト

著者への連絡は、rit@enisa.europa.eu。

本紙に関する報道関係のお問い合わせは、press@enisa.europa.eu。

### 著者

Stefan Weber 教授（ライプニッツ大学ハノーファー）、Matthias Scherer 教授（ミュンヘン工科大学）、Corina Pascu（ENISA）、Marco Barros Lourenco（ENISA）。

### 謝辞

Marie Kratz (ESSEC Paris), Martin Eling (University of St.Gallen), Ana Teresa Moutinho (EIOPA), Miguel Caballero (EIOPA), Benedetta Di Lupidio (EIOPA), Gabriela Zeller (Technical University of Munich), Matthias Fahrenwaldt (BaFin).

### 法的通知

本書は、別段の記載がない限り、ENISA の見解と解釈を表している。規則（EU）No 2019/881 に基づく ENISA または ENISA 機関の規制義務を支持するものではない。

ENISA は、本書またはその内容を変更、更新、削除する権利を有する。本書は情報提供のみを目的としており、無料でアクセスできなければならない。本書の全部または一部への言及またはその使用には、出典として ENISA を明記しなければならない。

第三者の情報源は適宜引用している。ENISA は、本書で言及されている外部ウェブサイトを含む外部情報源の内容に関して、いかなる責任も負わない。

ENISA および ENISA を代理する者は、本書に含まれる情報の使用について責任を負わない。

ENISA は本書に関する知的財産権を保持する。

## 著作権表示

欧州連合サイバーセキュリティ機関（ENISA）、2024 年

本書のライセンスは CC-BY 4.0 である。「特に断りのない限り、本書の再利用はクリエイティブ・コモンズ 表示 4.0 インターナショナル（CC BY 4.0）ライセンス（https://creativecommons.org/licenses/by/4.0/）の下で許可されている。これは、適切なクレジットを付与し、変更を示すことを条件に、再利用が許可されることを意味する。

ENISA の著作権下にない写真やその他の素材の使用や複製については、著作権者から直接許可を得なければならない。

ISBN:978-92-9204-633-0, doi: 10.2824/464473

# 目次

**目次 ..... 3**

**エグゼクティブサマリー ..... 5**

**1. はじめに ..... 7**

1.1 問題の説明 ..... 7

1.2 目的と範囲 ..... 8

1.3 方法論と情報源 ..... 8

1.4 レポート構成 ..... 9

**2. サイバーリスクとサイバー保険 ..... 11**

2.1 背景 ..... 11

2.2 サイバー保険業界の課題 ..... 13

2.2.1 価格設定 ..... 14

2.2.2 ポートフォリオ・リスク管理／規制資本 ..... 14

2.2.3 予約する ..... 15

2.2.4 再保険 ..... 15

2.2.5 将来の損失防止 ..... 15

2.3 課題と影響 ..... 16

2.3.1 課題 ..... 16

2.3.2 サイバー保険への影響 ..... 17

**3. データの背景 ..... 18**

3.1 現在入手可能で利用されているサイバー関連データ ..... 18

3.1.1 IT システムへの攻撃 ..... 18

3.1.2 データ侵害 ..... 18

3.1.3 サイバー損害データ（財務的影響） ..... 19

3.1.4 被保険者に関するメタ情報（特異的、システマティック、システミック） ..... 20

3.2 サイバー損害に関するデータの様式化された事実と課題 ..... 21

3.2.1 データの（非）可用性 ..... 21

3.2.2 技術進歩；データの非定常性 ..... 21

3.2.3 損失の累積 ..... 22

3.2.4 リスクの多様性 ..... 22

3.2.5 情報の非対称性 ..... 23
3.3 ビジョン：異なるソースからのデータのプール ..... 23
**4. サイバーリスクの種類 / モデリングアプローチ ..... 24**
4.1 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 ..... 24
4.2 古典的な保険数理アプローチ ..... 24
4.3 伝染モデル ..... 25
4.4 戦略的相互作用 ..... 26
4.5 主要なモデル化の課題とプライシング手法 ..... 26
**5. 統計的手法、機械学習、AI ..... 27**
5.1 サイバー で使われている確率的手法の現状 ..... 28
5.2 ML 法と AI 法の概要 ..... 29
5.3 保険業界で使われている ML/AI の方法 ..... 30
**6. 将来の研究ビジョン ..... 33**
**7. 結論 ..... 59**
**8.保険用語集 ..... 60**
**9.参考文献 ..... 65**

# エグゼクティブサマリー

研究・イノベーション（R&I）は、社会があらゆる分野における進歩、成長、発展を測る重要な指標である。しかし、ますますデジタル化する社会における進歩と成長は、信頼なくしては達成できない。サイバーセキュリティ R&I への投資は、新しく出現する脅威に関する知識を増やし、システム、ネットワーク、データを保護するための新しい技術、ツール、戦略を開発するための鍵となる。これを怠れば、個人、組織、社会全体によるデジタル技術の利用に対する信頼構築に壊滅的な結果をもたらしかねない。

本報告書の主な目的は、サイバーリスクとサイバー保険を紹介し、既存の研究とモデル化アプローチの概要を提供し、今後の研究プロジェクトのギャップを明らかにすることである。本レポートの主要な発見は以下の通りである：

- サイバー保険業界の現状を批判的にレビューし、サイバーリスク・モデリングに関する学術文献を要約する；
- 我々は、この学際的なモデリング作業で最も困難なのは、(i)一方では個々の企業の具体的な脆弱性をしっかりと理解することであり、(ii)他方では企業間の相互関係であり、後者はシステミック・リスクやシステマティック・リスクをもたらすものであると主張する；
- 我々は、ML/AI による高度な統計手法がサイバーリスク・モデリングやサイバー保険に利用できる可能性があることを示す；
- 高度な統計ツールのさらなる開発と利用を阻む大きな障害は、一般に利用可能なデータが不足していることである。そこで我々は、研究を促進するために、一般に利用可能なサイバー関連データプールの創設を提唱する；
- サイバー損害は、モデル化において説明しなければならない統計的特性を示している。特に、ポートフォリオにおける累積リスクにつながる非線形依存性、技術進歩や人的相互作用に起因する非定常な損害プロセス、重い尾を引く損害分布などである；
- サイバー保険は、特に適切なサイバー支援サービスと組み合わせることで、個々の企業にとっての利益とグローバルな IT インフラの回復力の両方を高めることができると主張する；
- 具体的な課題や今後の研究課題については、長いリストが挙げられている。

2023 年、ENISA はサイバー保険サービスの加入に関連する重要サービス事業者（OES）[1] の現在の展望と課題を分析した報告書を作成した。本レポートは、日常業務におけるサイバーリスクを軽減す

[1] ENISA（2023 年）

るツールとしてのサイバー保険の選択、購入、利用に関する情報と統計を提供している。この報告書は、需要側、特に OES がサイバー保険を利用する際の要件についての概要を提供しているが、本研究では、供給側からサイバー保険をより効果的なものにするために、技術的（保険数理的）観点からいくつかの課題に対処するために必要なことを強調している。例えば、サイバー保険をより手頃なものにし、OES のリスク軽減戦略としてより適切なものにするために、サイバーリスクの評価と分析の効率を高める方法である。加えて、本研究では、リスク・エクスポージャーの特定、軽減、定量化という観点から、リスク管理実務の成熟度をいかに向上させるかについて、実践的な提言も行っている。これら 2 つの報告書を合わせて読むことで、サイバーリスクを軽減するツールとしてサイバー保険をより効果的にする方法についての理解が深まるだろう。

# 1. はじめに

本章は、本報告書を読むための手引きとなるものである。専門的ではない方法で、まず、サイバーリスクにさらされている企業と、適切なサイバー保険契約を締結することによってサイバーリスクを（部分的に）受け入れようとする保険会社の視点から、サイバーリスクの問題を紹介する。次に、本報告書の目的と範囲、構成の概要を説明し、作成に使用した科学的手法と情報源について説明する。特に、サイバーリスクの分析と軽減の文脈で既に使用されている、あるいは将来そのような利益をもたらす可能性のある高度な統計的機械学習（ML）と人工知能（AI）の手法に重点を置いている。

## 1.1 問題の説明

デジタル技術は今日すでにバリューチェーンの中心的役割を担っており、その影響力は今後も確実に増していくだろう。しかし同時に、この発展に伴うさまざまなリスク（ここでは「サイバーリスク」という言葉でまとめている）も増大している。このようなリスクと起こりうる結果を認識し、その軽減や移転のために適切な対策を講じることが、企業のリスク管理にかかっている。後者、すなわちサイバーリスクの移転は、いくつかの保険会社や再保険会社が「サイバー保険」という名称で提供している。このような保険がサイバーアシスタンスと呼ばれる IT サービスによって補完されれば、サイバーリスクの一部を軽減し、単なるリスク移転の域を超えることさえ可能である。これは特に、大企業のような特殊な IT 専門知識を持たない中小企業にとって重要である。サイバー・エコシステムと一般的なリスク管理におけるサイバー保険の役割は、ほとんどの企業にとって極めて重要である。

企業のリスク管理の視点を離れ、保険会社の立場からサイバーに目を向けると、いくつかの類似点があるが、顕著な相違点もある。共通点は、企業のリスクを理解する必要性である。保険の文脈では、これは引受プロセスの一部であり、最終的には、年間保険料と引き換えに、関心を持つ企業に提供される保険契約につながる。しかし、このリスク評価では、保険会社は主にサイバーインシデントが引き起こす可能性のある財務的影響に関心を持つ。アクチュアリーの言葉を借りれば、保険会社はサイバー損害の発生確率（「損害の頻度」）とその財務的結果の分布（「損害の重大度分布」）を理解することを目的としている。風評被害など、保険契約でカバーされないサイバーリスクの側面は、保険会社にとっては、影響を受ける企業ほど関係ない。しかし、保険会社は、個々の企業のリスクの理解をはるかに超えなければならない。全体的なポートフォリオ・モデルが必要な理由は、例えばサイバー犯罪者の共通の攻撃ベクトルや IT システムの相互接続性から生じるサイバー損害の複数の相互依存性である。このことは保険会社にとって最も重要なことである。というのも、結果として生じるポートフォリオの損失分布は、個々の保険契約間の依存関係に強く影響され、このポートフォリオの損失分布は、保険会社のリスク管理および規制資本の計算プロセスにおいて理解され、管理される必要があるからである。学術的な観点からは、このことは IT システムのシステム的理解につながる、非常に興味深く、やりがいのある研究の機会を提供するものである。

## 1.2 目的と範囲

本報告書の主な目的は、サイバーリスクとサイバー保険における主要な課題を明らかにすることである。そのために、現在の研究状況を簡単に紹介するが、より詳細な情報については、Awiszus et al.（2022）などの最近の調査記事を参照されたい。サイバーリスクを分類し、保険業界が提供する商品、データ、統計手法、ML/AI における手続きについて説明する。提案された研究の目的は、サイバーにおける課題を表面的な定性的な扱いだけでなく、定量的な分析にも利用できるようにすることである。この文脈において、サイバーリスクとサイバー保険を正しく理解するためには、データ、モデリング、統計、ML/AI、そして特にアクチュアリーや IT 専門家といった学際的な専門知識を結集した多次元的な視点が必要である。

## 1.3 方法論と情報源

サイバーリスクと保険における既存の研究と未解決の課題に関する我々の報告書は、以下のような様々な情報源からの情報を組み合わせている：

- サイバーリスクに関する学術文献（未発表原稿を含む）。
- ML/AI に関する学術文献。
- 政府機関（ENISA など）、研究機関、保険数理協会、規制当局、（再）保険会社などの民間企業による報告書。
- サイバー保険市場で活躍する実務家、IT 専門家、ML/AI 研究者との議論から得た知見。
- サイバー関連のデータベース
- 独自の研究ノウハウを持つ。
- この文書の以前のバージョンに対する様々な専門家によるフィードバック。

既存の科学文献は、研究の現状を記述するための主要なリソースである（(1)参照）。多くの論文は、研究の限界を明確に述べ、将来の研究のためのアイデアを提供している。ML/AI の手法は、より伝統的な保険分野でもすでに適用され、成功を収めている。この一連の研究が分析され、サイバー保険に外挿されている。新しい手法、商品、新しいデータベースなどに関する非常に貴重な情報は、(3)を参照されたい。このようなレポートはしばしば、サイバーリスクとサイバー保険市場について非常にタイムリーな洞察を提供してくれる。さらに、既存の研究機会や未解決の実践的問題について明確に知るために、専門家にインタビューを行った（4）参照。さらに、サイバー関連データに関する数少ない既存のデータベース（(5)参照）は、ML/AI の将来的な応用の可能性についての洞察を与えてくれる。また、モデルや手法と既存のデータセットを比較することで、今後の開発にどのデータが必要で、どのデータベースを構築すべきか、場合によっては付随する規制措置によってサポートされるべきかの示唆を得ることができる。(6)に関しては、本報告書の著者はいずれも数理科学と金融数学の

上級研究者であり、確率論的モデリングと統計的応用において長期にわたる研究経験を有している。両者とも特にサイバー関連の問題に取り組んでおり、保険業界との共同研究も行っている。この専門知識と彼らの個人的な意見も報告書に盛り込まれている。また、ENISA のパネルディスカッションからも更なるフィードバックを得たので、(7)を参照されたい。

## 1.4 レポート構成

レポートの構成は以下の通りである：

- **第 2 章**では、一方ではサイバーリスクの様々な側面について、他方ではサイバー保険とその要件について詳細に紹介している。これは科学的背景を提供し、長い参考文献のリストを通じて読者を導くだけでなく、保険業界の観点から必要な応用と課題を示している。また、この問題の経済的関連性も強調している。本書全体にとって非常に重要なのは、サイバーリスクに関する統一的な分類法であり、これは「通過点」として提供されている。この章では、学術的背景を説明し、保険業界の観点から必要な応用と課題を説明し、最後に次の章で使用されるサイバーリスクの分類法を提供する。
- **第 3 章**では、サイバーに関する既存のデータ、そのデータを分析した学術文献、モデル化する際に考慮しなければならないサイバーリスク特有の定型化された統計的事実の帰結の分析を取り上げる。サイバー関連のデータセットを簡単に説明し、これらのデータを分析した学術文献を引用し、主な結果を要約する。詳細には、モデル化において考慮する必要があるサイバーリスクの結果について議論する。本章の結論として、さらなる研究、特に ML/AI の応用に不可欠な、研究に利用可能なより良いデータセットを作成することを強く主張する。
- **第 4 章では、**サイバー領域のモデリング・アプローチを取り上げる。個別リスク、システマティックリスク、組織的リスクに分けることがなぜ重要なのかを考察する。モデリングの分野では、将来に向けて多くの課題が残されている。
- **第 5 章では、**機械学習（ML）と人工知能（AI）の現状を簡単に概観し、保険数理学と保険業界における既存の（そしておそらく将来的な）応用例について論じている。なぜ今日まで、これらの手法の多くがサイバー保険に導入されていないのか、また、この状況を変えるためにはどのような障害を取り除かなければならないのかが説明されている。
- **最後に第 6 章**では、重要かつ有望な研究課題の長いリストを掲載する。これらの問題は前章までの議論から生まれ、以下のように整理されている：研究課題、目的、貢献者、スコープ：、成果物、革新の機会である。
- 本報告書は、結論**（第 7 章）**、保険関連の専門用語集**（第 8 章）**、厳選した参考文献のリスト（**第 9 章**）で締めくくられている。

- ENISA は、サイバーセキュリティ R&I に関する助言を作成し、利害関係者に提示するためのツールとして利用することを目的として、これらの報告書を作成している。これらの利害関係者は、本報告書の主な対象読者であり、より広範な研究開発コミュニティ（学者、研究者、イノベーター）のメンバー、産業界、欧州委員会（EC)、欧州サイバーセキュリティ・コンピテンス・センター（ECCC)、国内調整センター（NCC）を含む。

# 2. サイバーリスクとサイバー保険

## 2.1 背景

デジタル技術が私たちの生活をますます左右するようになっている。これはもはやデスクトップ・コンピューターやタブレット、スマートフォンに限ったことではなく、今日ではデジタル技術が日常的に使用されている多くのモノを制御している。[2]この状況はしばしば「モノのインターネット」というキーワードで表現される。同様に、私たちの労働環境もデジタル化、ネットワーク化された空間へとますますシフトしており、最近の COVID19 の大流行はこの変化を強力に加速させている。企業とその物流、輸送システム、エネルギー供給、販売チャネルはデジタル・システムによって制御されている。このデジタル・トランスフォーメーションは大規模な効率化をもたらし、今後もそうなるだろう。

しかし、デジタル・システムやデジタル・ネットワークの相互接続による付加価値は、進歩につながるだけでなく、リスクも伴う。複雑なシステムは、個人の日常生活だけでなく、企業や社会全体のレベルでも、多くのプロセスが適切に機能するかどうかに依存しており、そのシステムが破壊される可能性がある。プロセスの中断、遅延、途絶は、まったく異なる次元の損失をもたらす可能性がある。最悪の場合、甚大な経済的影響や人的被害さえ伴う大惨事が発生する可能性もある。デジタル・システムに対するこのような脅威は、サイバーリスクとして知られ、分析、規制、管理されなければならない。

サイバーリスクは、サイバー事象の原因、発生する損失の種類、リスクを評価するために取られるアプローチ、サイバーセキュリティを強化したりサイバー事象の悪影響を軽減したりするために取られる行動など、さまざまな観点から検討することができる。

サイバーリスクの原因には、技術的誤作動、人為的ミス、インサイダーやハッカーによる攻撃などがある。結果として生じる損害には、データの損失や盗難が含まれる。事業運営は中断または中断される可能性がある。重要なインフラが機能制限、損傷、破壊されることもある。サイバー事象によって、人身事故や死亡事故が発生することもある。サイバー事件が積極的なサイバー攻撃である場合、詐欺や恐喝などの犯罪が重要な役割を果たす。[3]

サイバーリスクの分析は難しい。サイバーリスクと脅威を世界規模で事前に調査するために、様々なツールが利用可能である。潜在的な影響を評価するために、ケーススタディで個々の反事実的事象と

---

[2] ネットワーク化されたデジタル機器の数は、2020 年頃には 300 億台と推定されていたが、2030 年には 1,250 億台になると予想されている（Reinhart (2021)を参照）。

[3] Reinhart (2021)は近年の例を挙げている。

その結果を検討するシナリオ分析がしばしば行われる。また、データがあれば、サイバーリスクを統計的に分析することもできる。最後に、サイバーリスクを多層的に検討できるような、より複雑な確率モデルを開発することもできる。

サイバーリスクに対するセーフガードには、システムの更新や、システムの完全性を確保するための追加的なセキュリティ対策が含まれる。潜在的なサイバー事象に備えるため、コンティンジェンシープランの策定は重要な予防策である。最後に、サイバー損害の金銭的影響は、保険ソリューションでカバーすることができる。[4]

サイバーリスクは人々の意識に定着している。近年では、2017 年に WannaCry や NotPetya といった世界的なサイバー事件が発生し、大きな混乱が生じた。アリアンツ・リスク・バロメーター2022（Allianz, 2022）は、ビジネス・ステークホルダーを対象とした調査であり、2022 年のグローバル・ビジネス・リスクの中で、事業の混乱（42%）、自然災害（25%）、パンデミック（22%）、法的・政治的リスク（19%）を抑えて、サイバーリスクが第 1 位にランクされている（回答者の 44%が挙げている）。6 位～10 位、気候変動、火災・爆発、市場の不確実性、熟練労働者の不足、マクロ経済の発展が続いた。戦略国際問題研究所（CSIS、2020 年）によると、世界のサイバーリスクによる推定年間損害額は、2014 年には 4,450 億米ドル、2018 年には 6,000 億米ドル、2020 年には 1,000 億米ドルに増加する。定義や方法論によって、見積もりは分かれる。2025 年には 10,500 億ドルに達すると予測されるなど、6 倍以上の金額が提示されているケースもある。

サイバーリスク管理における重要なプレーヤーは保険業界である。MunichRe (Reinhart, 2021)は、2018 年の世界の保険料は 50 億米ドル、2025 年には 200 億米ドルまで増加すると予測しており、市場シェアは米国が 50%、欧州が 25%である。特に犯罪的サイバー攻撃の分野では、ミュンヘン再保険は中長期的に大幅な増加を見込んでいる。攻撃技術は、特に組織犯罪の分野でさらに開発されているが、国家によっても開発されている。5G、人工知能、自動化、クラウド技術などの技術は、今後攻撃者の標的になると予想される。サイバーリスクの重要性は、ハノーバー再保険とハノーバー保険ハウスのグループ・リスク・マネジメントのケルスティン・アウィスツス博士も強調している：「興味深い問題は、サイバー攻撃を受けるかどうかではなく、いつ（それに気づくか）である。

サイバーリスクの管理において、保険ソリューションはどのような役割を果たすことができるのだろうか？個人や企業の古典的なリスク管理戦略は、リスクの回避、リスクの低減、リスクの意識的受容、リスクの移転である。サイバーリスクにおいても、これらの側面はすべて役割を果たす。行為者は自らのリスクを定義しなければならないが、より高いセキュリティ基準によってリスクを削減するためのコストも負担しなければならない。リスク移転は通常、残存リスクに対する金銭的な保護を提供することでリスク管理を完成させる。

[4] 優れた紹介と調査については、Zeller and Scherer (2022)と Awiszus et al.

保険会社は主にリスク移転ソリューションを提供しているが、契約開始時および契約期間中に最低限のセキュリティ要件を満たすことも顧客に要求している。情報は、リンクされたアドオン・オファリングを通じて得ることができ、最低限の要件はそれらを通じてモニターすることができる。サイバー保険の場合、サイバー支援サービスはこの点で非常に重要である。保険会社はビジネスモデルの幅を広げるためにこれらを利用することができるが、何よりも、より詳細かつ継続的にリスクを監視・管理できる可能性がある。特に、サイバー保険のような比較的複雑で透明性の低い保険種目では、こうした追加情報はプライシングやリスク管理に非常に役立つ。リスク移転分野のサービス、特にサイバー支援分野のサービスは、被保険企業をより強固で弾力的なものにすることで重要な安定化機能を持ち、その結果、福祉を向上させる効果がある。特にサイバー領域では、保険会社は、純粋なリスク移転ソリューションの提供者としての伝統的な役割を超えて、社会的利益をもたらす仕事を担う。特に、保険ソリューションが、IT システムの物理的セキュリティを強化するサイバー支援と組み合わされる場合、このことが当てはまる。

保険の分野では、サイバーとは、コンピュータ・システム、ハードウェア、ソフトウェア、データ、インターネットその他のデジタル・ネットワーク、あらゆる種類の情報技術（IT）、または運用技術（OT）に関連するあらゆるリスクの総称である。現在、以下のような保険が提供されているか、あるいは開発中である：データの喪失または盗難、プライバシー侵害保護、サイバー恐喝、物的損害、（偶発的な）事業中断、製造物責任、風評被害、知的財産の喪失などである。[5]ミュンヘン再保険（Reinhart, 2021）のような保険会社は、サイバー保険はこれまでのところ世界のサイバー損害のごく一部しかカバーしておらず、サイバー保険市場には大きな成長機会があると想定している。しかし、サイバー事象の同時多発的な増加により、この保険格差はしばらくの間続く可能性がある。[6]

## 2.2 サイバー保険業界の課題

保険会社はリスクを評価し管理する際に複雑なタスクに直面するが、サイバー保険の分野でも適切に実施しなければならない。これらのタスクは、プライシング、保険ポートフォリオ管理、積立、再保険、将来の損害防止に関連している。サイバー保険の適切な手法を開発するためには、サイバーリスクのモデルをさらに発展させ、サイバー事象やサイバー損害に関するデータを収集する必要がある。本セクションでは、本レポートで展開するリサーチ・クエスチョンの基礎として、保険の様々な役割について概観する。

[5] これらのリスクは必ずしも切り離すのが容易ではなく、金銭的な影響を測定するのも難しい場合が多い。

[6] ラインハート（2021 年）の専門家の意見によれば、このようになる。

### 2.2.1 価格設定

保険の基本原理は、集団におけるリスクのプールであり、その根本原理はしばしば「少数の不幸に対する多数の貢献」と説明される。理想的には、独立したリスクの均質な集合体をグループ化し、古典的な手続きと保険料原則を用いたシンプルな価格決定ルールを可能にすることである。正味保険料は、基本的に大数の法則に依拠しており、リスク・プレミアムとコストや税金のサーチャージによって調整される。古典的な保険契約のプライシングは、特異的リスクに焦点を当てている。さらに、サイバー保険の分野では、他の種類のリスク、すなわちシステマティック・リスクやシステミック・リスクも考慮しなければならない。

集団におけるリスク・プーリングに基づくプライシングは、均質な集団を前提とする。この目的のためには、意味のあるリスク識別を可能にする関連共変数を決定する必要がある。そうすれば、例えば、集合モデルを用いて集合的な損失分布を記述することができ、これによって契約のプライシングが可能になる。集合体モデルは、集合体を、分布が等しい独立した損害の生産者として解釈する。損害の頻度と重大性はデータから推定しなければならない。

システマティック・リスクやシステミック・リスクが存在する場合には、古典的な保険プライシングを他の手法で補完しなければならない。システマティックリスクは、さまざまな被保険者に共同で影響を与えるランダムな要因過程への依存から生じる。こうしたリスクの評価には、金融数学の手法、すなわちハンス・ビュルマンの「第三種のアクチュアリー」の手法が必要となる。サイバーリスクで中心的な役割を果たすシステミック・リスクがどのように評価されるべきかという問題は、研究においてまだ未解決である。システミックリスクは、フィードバック効果、ローカルおよびグローバルな相互作用、すなわちリスクを増幅させるシステミックなメカニズムによって特徴付けられる。これらを評価するためには、適切な方法で拡散メカニズムをモデル化する必要がある。保険／金融の他の分野では、依存関係は間接的な影響の結果であることが多いが（例えば、金利上昇は多くの企業の信用力に影響を与える）、サイバーリスクでは通常、さまざまな事業体（[7]）に直接損失をもたらすシステミックな事象に直面し、その結果、依存関係が生じる。

### 2.2.2 ポートフォリオ・リスク管理／規制資本

保険会社は、さまざまな保険集団とそのリスクをまとめている。システマティックリスクやシステミックリスクに起因する、異なる構成要素間の複雑な依存関係を考慮しなければならない。サイバーリスクについては、これらのモデル化と見積もりはほとんど未解決の課題であった。さらに、保険会社のバランスシートを見積もり、管理するためには、金銭的なリスク尺度など、ポートフォリオ・レベルでリスクを計測する必要がある。ポートフォリオ・モデルは、保険会社の破綻の可能性から保険契約者やその他の利害関係者を保護することを目的とした保険資本規制の基礎でもある。

---

[7] 例えば、マルウェアやクラウド障害が多くの企業に同時に影響を与えた場合を考えてみよう。

### 2.2.3 予約する

クレーム・リスティングとは、不完全に決済されたクレームに対して、貸借対照表の負債側に財源を確保するプロセスを指す。クレーム・リスティングは、引当金を決定するために、データを用いた様々な方法を用いる。サイバーリスクの分野では、データの利用可能性はまだ低い。一方では、これは古典的な手法がごく限られた範囲でしか適用できないことを意味する。他方で、手法の有効性を決定的に評価することはまだできない。

### 2.2.4 再保険

包括的なリスク・プールは、可能な限り大規模な集合体によって確保することができる。多くの保険会社のポートフォリオをプールすることは、大量のデータと資本を束ね、技術的専門知識を維持する再保険会社によって実現できる。このような第三者へのリスク移転に加え、保険リンク証券を通じて資本市場にリスクを移転することもできる。サイバーリスクの再保険商品とデリバティブの分析は、まだ十分に発展させる必要がある。

### 2.2.5 将来の損失防止

情報の非対称性とシステミック・リスクにより、特にサイバーリスクの分野では、責任制限と免責事項を含む慎重な引受方針が必要となる。同時に、リスクに関する透明性の創出も重要な要素であり、これは、例えば、サイバーアシスタンスにおけるサービスを通じて確立することもできる。このように、保険は物理的世界におけるサイバーリスクの低減にも貢献することができる。健全な保険引受方針とサイバーアシスタンス提供のための効果的な戦略のための優れたベンチマークを包括的に確立しなければならない。

サイバー危機の場合、システミックな安全保障を確立し、レジリエンスを強化するために、国家機関がどのような役割を果たすことができるのか、極めて根本的に問い直す必要もある。これは、過去の金融危機、コロナ・パンデミック時やロシアのウクライナ攻撃におけるサプライチェーンの問題、多様化やシステミックな相互依存が不十分であったために農業やエネルギー供給市場で供給不足を経験したことから学んだ教訓と類似している。歴史的に見ても、平時には適切に機能している市場が、危機の際には人々の繁栄と供給に十分に貢献しないことは明らかである。今日に至るまで、多くの政府介入や補助金が危機の際に開始されてきたが、事前にどのようにレジリエントな構造を作ることができるのか、そのためにどのような政府規制が必要なのかが問われなければならない。このような疑問は、サイバーリスクとサイバー保険についても答えられなければならない。

## 2.3 課題と影響

### 2.3.1 課題

サイバーリスクのリスクマネジメントと保険には、基本的な課題が伴う。デジタル技術は絶え間なく変化しており、リスクもそれに合わせて変化する。しかし、この進歩は予測可能なものではなく、本質的にランダムで不確実なものである。さらに、自然災害におけるリスクとは異なり、サイバーリスクは定常的なものではないと考えられる。セキュリティ技術とサイバー犯罪者の能力は、複雑な進化のダイナミズムの中で変化しており、これが根本的な課題となり、絶え間ない適応を必要とする。統計学的な観点から見ると、非定常過程やデータを扱うことを考慮しなければならない。

もうひとつの困難は、デジタル・エンティティが相互に接続され、相互作用する複雑なネットワーク構造である。異なるノードにおけるリスクは確率的に依存するが、自然災害の分野におけるリスクのような単純な地域／近接構造を持たない。したがって、サイバーリスク評価は、デジタルネットワークのグラフ構造とリスクの伝播ダイナミクスのマッピングに依存する。蓄積リスクは単純な方法では表現できない。このようなモデルのキャリブレーションと検証には、古典的な保険損害リスク管理モデルとは異なるタイプのデータが必要である。

同様に複雑なのは、サイバーリスクが非常に多様な性質を持ちうるという事実である。デジタル技術」という用語は非常に幅広く、様々な実体や現象が含まれる。このような異質性から、個々の課題に適切に適応しなければならない、多元的で広範なモデリング・アプローチが必要となる。

他の多くの保険リスクと同様、情報の非対称性は重要である。物理的なサイバーセキュリティはクレームの頻度や重大性に大きく影響する。適切な保険料を算出し、保険性を損なわないためには、ここでも適切なリスク選択が重要である。これはよく知られている逆選択の問題である。原理的には、保険契約締結後にサイバーセキュリティ強化策へのインセンティブが低下する可能性もある。後者のモラルハザードの問題がサイバーリスクにおいて中心的な役割を果たすかどうかは疑問である。なぜなら、他のさまざまなインセンティブがサイバーセキュリティを積極的に低下させることをあまり好都合なこととはしていないからである。[8]特にサイバーリスクの分野では、情報の非対称性がリスクの複雑さと結びついている。その結果、保険会社は、保険とサイバー支援を組み合わせるなど、これに対処する戦略を開発しなければならない。

最後に、サイバーリスクに関するデータの入手可能性が中心的な問題である。保険業界における研究、規制、応用に適した粒度や十分な量のデータはまだ入手できない。保険会社や再保険会社はデータプールを構築することができるが、欧州でサイバーセキュリティとサイバー保険に関する研究を成功させるためには、しっかりとしたデータベースに裏打ちされた政府の規制も必要である。

---

[8] 保険金が支払われないリスクの例として、評判の失墜を挙げてみよう。

### 2.3.2 サイバー保険への影響

サイバーリスクは、進化的な構造、非定常性、システム的なネットワーク効果の重要性といった特徴を持っている。モデル化とリスク管理において、これらの特徴を考慮しなければならない。この点については、まだまだ開発が必要である。並行して、研究や規制のために、まだ利用可能でないデータセットを構築することも重要である。保険実務においては、リスク移転と物理的保護を結びつけ、並行して継続的にデータを収集することが特に重要である。保険サービスは常に状況の変化に対応していかなければならない。アリアンツ・グローバル・コーポレート＆スペシャリティのサイバー部門グローバル責任者であるスコット・セイスは、サイバー保険の中心的な格言を次のように特徴づけている（Allianz, 2022 参照）：

「優れたサイバー成熟度と優れたサイバー保険は手を携えている。私たちは自宅のために保険に加入するが、これは玄関の鍵を開けっ放しにすることを意味しない。サイバー市場は、保険契約とテクノロジー、リスク・エンジニアリング、レスポンス・サービスを組み合わせたサービス指向の提供へとシフトしている。保険会社は、引受プロセスや保険期間を通じて、絶えず変化するエクスポージャーを理解し、サイバー・セキュリティとレジリエンスへの投資に集中できるよう組織を支援することができる。私たちは、サイバーリスク改善の旅を通して、そのようなパートナーになりたいと考えている。

# 3. データの背景

本章では、サイバーリスクに関する既存のデータベースについて議論し、このデータを保険の文脈や一般的なサイバーリスクのモデル化においてどのように利用できるかを説明する。サイバー関連データを収集し、利用する上での課題について議論し、保険市場の他のセグメントにおける状況と比較する。

## 3.1 現在入手可能で利用されているサイバー関連データ

本報告書を執筆している 2022 年半ばまでには、サイバー損害賠償請求に関する一般に入手可能なデータで、良質な情報を提供するものは不十分である。しかし、サイバー賠償請求に関連する興味深い初期洞察を提供し、すでに研究に利用できるデータセットがいくつか存在する。そのようなデータの情報源は、すでに文献や保険業界で使用され、分析されているものであるが、以下に要約する。

### 3.1.1 IT システムへの攻撃

情報技術の文献では、IT システムやウェブサイトへの攻撃（DDoS 攻撃など）の時系列のモデリングに関する様々な科学論文がある。このような時系列は、例えば実際のシステム／ウェブサイト上で観測された攻撃から生成されたり、いわゆるハニーポット[9] を設置することによって生成されたりする。時系列分析や計量経済学などのツールを適用して、このデータを統計的に分析することで、攻撃のダイナミクスに関する洞察を得ることができる。サイバー保険に関しては、間接的な情報ではあるが、興味深い情報が得られる。サイバー保険にとって、攻撃が「成功」する可能性を特定すること、そして「成功」した攻撃の統計的特性とその金銭的影響を理解することも同様に重要である。多数の）攻撃と（ごく少数の）サイバーインシデントおよびその結果生じる金銭的損失を照合することは困難であり、興味深い（将来の）研究分野である。

### 3.1.2 データ侵害

データ漏洩は、サイバーインシデントの特殊な形態のひとつであり、ハッキング行為、人為的ミス、技術的誤作動など、さまざまな原因から発生する可能性がある。現地の法律や開示されたデータの種類によっては、巨額の罰金や深刻な経済的損失につながることもある。データ漏洩に関するデータソースとしては、非営利法人「プライバシー権クリアリングハウス」（PRC） が組織する「データ漏洩年表」（[10] ）や「オープン・セキュリティ財団データ損失デー タベース」（[11] ）などが知られてい

---

[9] 攻撃を誘発し記録する目的で、特別に生成されたウェブページやウェブサービス。

[10] https://privacyrights.org/data-breaches

[11] 以前は http://datalossdb.org から入手可能だった。

る。保険という観点からは、データ漏えいの情報を金銭的損害に変換することは容易ではない。[12]、データ漏えいに起因する風評被害などは（不可能ではないにせよ）定量化することが難しいからである。しかし、データ漏えいがもたらす財務的影響を理解し、リスクの価格設定という観点か ら評価するためには、このような定量化が必要である。統計的な結果に関して、Edwards ら（2016）と Eling and Loperfido（2017）の研究は、開示された記録の数（頻度）は対数正規分布または対数スキュー正規分布（負の二項分布）で記述できることを示唆している。Eling and Jung (2018)は、データ漏洩損失の（産業間の）横断的依存性を研究している。これらのデータベースの利用を複雑にしているのは、情報のほとんどが事象の口頭説明という形で構造化されていないことである。データ漏えいの統計的法則と、（さまざまな法律における）その金銭的結果についてのより深い理解は、明らかに今後の研究の可能性を秘めている。しかし、これはサイバーリスクの多くの側面の一つに過ぎないことを認識しなければならない。

### 3.1.3 サイバー損害データ（財務的影響）

サイバー損害に関する広範なデータベースは、営利企業 Advisison によって提供されている。2022 年現在、彼らはそのデータセットを「Advisen*'s cyber loss data provides a historical view of more than 90,000 cyber events - including clash events - collected from reliable and publicly verifiable* sources」[13] と説明している。このデータは、特に Romanosky (2016)によって分析されている。この興味深い一連のデータが学界で自由に利用できないという事実は、学界による分析や調査を明らかに妨げている。

Eling and Wirfs（2019）は、サイバーリスクをオペレーショナル・リスクのサブグループと定義し、この観点から、オペレーショナル・リスク・データベース SAS OpRisk Global のデータ[14] から（サイバー損害のサブセットを）分析している。Dacorogna and Kratz (2020)は、フランス国家憲兵隊の非公開データベースを用いた研究について述べている。彼らの初期分析は、ヘビーテールの損失を示唆している。同時に、データをクリーニングし、匿名化して一般に利用可能にすることの難しさについても述べている。Dacorogna et al. (2022)では、詳細な統計分析が行われており、リスク管理への影響や、尾の太さに基づくサイバー攻撃の分類が示唆されている。

---

[12]Ponemon Institute LLC (2016) の出版物は、開示されたレコード 1 件当たりの平均コストは、データ侵害の原因および業種によって異なると結論づけている。データ漏えいの財務的影響とデータ漏えいの大きさの間の直接的なリンクの入門書は、データ漏えいの対数コストと開示されたレコードの対数数を対応付ける Jacob の公式（Jacob (2014)を参照）である。

[13]https://www.advisenltd.com/data/cyber-loss-data/ より 引用

[14] https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf

### 3.1.4 被保険者に関するメタ情報（特異的、システマティック、システミック）

上記のデータベースの多くには、[15] 関係企業名がプレーンテキストで含まれている。これは、当該データベースを他の情報と統合し、最終的に当該企業に関するメタ情報を用いて共変量のエンリッチリストを得る際に、貴重な情報となる可能性がある。この作業には、明らかに手間のかかるデータの前処理が必要であるが、個人のリスク評価などの用途では非常に価値があると思われ、今後の研究でさらに検討されるべき重要な課題である。

学術研究と比較すると、保険会社のデータ状況は若干良好である。なぜなら、保険会社は、例えばポートフォリオ企業のリスク・アンケートを通じて収集したような、非公開の追加情報を自由に利用できるからである。また、保険会社が過去に直面した損害やイベントの履歴を活用することもできる。しかし、引受プロセスにおいて意味のあるリスク分析を行うことは、依然として非常に複雑な作業であり、理想的には、サイバー損失をモデル化するために必要なあらゆるデータを収集し、IT 専門家と緊密に連携して実施する必要がある。以下のような単純と思われる質問がある：企業のサイバーリスクを分析するために、企業に関するどのような情報／共変数を収集すべきか」、あるいは「特定の企業のリスクを定量化するにはどうすればよいか」といった単純と思われる質問に答えることは、いまだに非常に難しい。

遅くとも、ポートフォリオ・リスク管理には、さらなるレベルの情報が必要である。これには、確率的に依存するサイバー損害につながる、検討対象企業間の可能な相互関係の範囲が含まれる。多くの依存関係は、インシデント発生前に予測することは困難であり、インシデント発生後に見過ごされる可能性さえある。例えば、感染したソフトウェアの一般的な使用、ソーシャル・エンジニアリングの類似事例に対する脆弱性、サプライチェーン経由の攻撃、大量電子メール攻撃によるフィッシングの試み、共有クラウドサービスやインフラの障害など、例を挙げればきりがない。リスク間の依存性が地理的距離とともに減少する（同じ河川による洪水など共通の事象へのエクスポージャーが容易に理解できる）例えば NatCat と比較すると、サイバーに関する同様の「距離の尺度」は明らかではなく、国や大陸をまたいで分散する戦略は、相互接続されたサイバー世界では容易に実行できない。多くの場合、グラフ理論的手法に基づいている（本文書のモデリングに関するセクションを参照）が、これらは現在までのところ、ほとんどがおもちゃのモデルのレベルであり、より実証的な研究が望まれる。上記の例が示すように、ネットワーク化されたサイバーリスクの現実的なモデルを作成する作業 は、十分な IT スキルと包括的なデータがなければ不可能であり、また、技術の改善・変 化に応じて常に更新を必要とする可能性がある。

[15] 現在のところ、サイバー保険は主に企業や組織向けに提供されており、個人の最終顧客向けの市場は発展途上にある。

## 3.2 サイバー損害に関するデータの様式化された事実と課題

この段落では、サイバー損害に関するデータおよび関連データの定型化された統計的事実を論じる。第 4 章と重複する部分があることに留意されたい。

### 3.2.1 データの（非）可用性

サイバーリスクは（比較的）新しい分野であり、関連するデータは乏しい。前述したように、以下に述べる数少ない既存のデータベースは、それぞれ我々が関心を持つ現象の一部しかカバーしておらず、ほとんどのデータベースは一般や科学の世界にはアクセスできない。保険会社は過去の実現損害に関するデータをある程度持っていることが多いが、自動車保険のような確立された大衆保険市場に比べると、対象となる損害の数は非常に少ない。多くの保険会社がサイバー市場に参入したばかりであり、そのため最初の保険契約が締結された時点のデータしか収集できていないという事実は、明日の健全な統計分析に必要とされる情報の多くが、現在まだ把握されていないことを示している。
ML/AI による高度な統計手法の利用は、より良いデータベース（より多くの共変量、より多くの保険金請求、...）を提供することによって、大幅に後押しされる可能性がある。

### 3.2.2 技術進歩；データの非定常性

マイクロコンピューターやインターネットの発明以来の技術の進歩、バリューチェーン全体のデジタル化は周知の事実である。ここ数十年、こうした変化は前例のないペースで業界を変革してきたし、現在もそれは続いている。しかし、あらゆる新技術は潜在的なリスクでもある。IT セキュリティのレベルでは、システム（ハードウェア、ソフトウェア、そして最も重要なのは、それらのシステムのユーザー）を常に最新の変化に適応させなければならない。サイバーリスクを分析するアクチュアリーの観点からすると、過去に収集されたデータが明日のサイバーリスクを完全に特徴づけるとは限らないことを意味する。直感的に言えば、新しい技術から生じるリスクは過去のデータには表れない。リスクからの学習のフィードバックループを考慮しなければならない。同時に、サイバーリスクがもたらす金銭的な影響は、長年にわたって増大し続けている。

この定型化された事実を表す統計用語は「非定常性」である。これはサイバーリスクをモデル化する際の重要な課題である。考えられる解決策としては、頻度と重大性の傾向に関する単純な仮定、時間経過に伴う分布の変化を明示的に考慮したモデルの採用、時変パラメータを持つモデル、統計データと専門家の意見の組み合わせ、リスクをモデル化したより一般的なアプローチなどがある。サイバーデータの非定常性を認識し研究することは、古典的な統計モデリングにとっても、ML/AI による新しい方法論にとっても興味深い研究分野である。データのみを用いて）時系列における構造的断絶を特定することは、長い時系列を必要とする困難な作業であるため、専門家の IT 知識をデータと組み合わせることで、純粋な統計分析よりも良い結果が得られる可能性がある。

### 3.2.3 損失の累積

保険の基本原則は「集団における分散」である。多数のリスクを保証し、対応する保険料（予想損失額よりわずかに高い）を得る能力は、古典的な大数の法則や中心極限定理を適用することで形式的に正当化できるビジネスコンセプトである。しかし、保険数理上の重要な結論は、個々のリスクがヘビーテールであったり、リスクが確率的に依存する（あるいはその両方である）場合には、もはや妥当ではない。リスクの確率的依存性は、われわれがサイバースペースで直面する重大な課題である。この観察に関する技術的なケースは、前のセクションですでに述べた（共通の攻撃、インフラ、ネットワークなど）。多くの場合、損失に関する情報は限られており、サイバーインシデントは遅れて観測／報告される可能性があるからである。統計的な観点からは、累積リスクが過小評価されている可能性が高い。理想的には、統計的知識と IT の専門知識を組み合わせた蓄積リスクの適切なモデリングは、興味深い研究分野である。さらに、ML/AI は、異なる企業で発生した事象の背後にある共通の根源を帰属／特定するのに役立つ可能性がある。

保険会社にとって、蓄積リスクは様々な影響を及ぼす。アキュムレーション・リスクはポートフォリオ・リスクをモデル化する際に非常に重要な要素であり、必要な規制資本に大きな影響を与える。同様に、非比例再保険の価格にも影響を与える。運用面でも、蓄積リスクは課題となっている。というのも、多くのインシデントが同時に発生した場合、サイバー問題に即座に対応しようとする IT サービス・プロバイダーに過負荷がかかる可能性があるからである。最後に、多くの統計手法（ML/AI の手法を含む）は、使用されるデータが独立であるという前提に暗黙のうちに依存していることは注目に値する。このような手法の不用意な適用は避けなければならず、相関性の高い入力データを用いた ML/AI 手法の研究が必要である。さらに、従属クレームをモデル化するためのコピュラ法の使用は、統計的観点からは運用可能であり、有望ではあるが、従属性の原因を捕捉するボトムアップモデルを提供するには十分ではない。

### 3.2.4 リスクの多様性

Eling ら（2016）は、サイバーリスクをその起源、結果、主要な特徴に従って分類している。彼らは、「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（*ICT*）の使用から生じるあらゆるリスク」という定義を提案している。*[*サイバーリスクは自然に発生するものと人為的に発生するものがあり、後者は人為的な失敗、サイバー犯罪（恐喝、詐欺など）、サイバー戦争、サイバーテロなどから発生する。

この定義は、サイバーリスクの様々な側面を示しており、マトリックス構造における分類のための骨格として使用することができる。このようなアプローチでは、サイバーインシデントを正しいカテゴリーに分類するために、技術的背景を正しく理解すること（及び具体的なケースに関する十分な情報）が必要となる。これは、保険が適用される（または適用される予定の）分野では特に重要である。ミュンヘン再保険（2021 年）によれば、以下の分野ではすでに保険が適用されている：データ

の損失または盗難、プライバシー侵害保護、サイバー恐喝、物的損害、（偶発的な）事業中断、製造物責任、風評被害、知的財産の損失である。

統計学的観点からは、分類という文脈では相反する目標に直面する。一方では、多数の均質なサブグループがあれば、理論的には各グループのプライシングの精度が高まるが、他方では、実際にはサブグループが多すぎると、各グループのデータポイントが少なすぎて、意味のある統計分析ができなくなる。ML/AI の応用のための潜在的かつ魅力的な視点は、これらの競合する目標の間の良好なトレードオフが達成されるように、損失をサブグループに分類することである。

### 3.2.5 情報の非対称性

情報の非対称性は保険の多くの分野で重要な役割を果たしている。サイバーリスクも例外ではなく、その理由を説明するのは簡単である（しかし、克服するのは非常に難しい）：顧客のサイバーセキュリティのレベルは、リスクの頻度や重大性に強く影響する。企業の真のリスクプロファイルを正確に特定することは、非常に困難で複雑な作業である。保険会社は引受プロセスの一環として、この作業に多大な労力を費やしている。サイバー保険では、情報の非対称性は、付随するサイバー支援によって緩和することができる。

将来のリスク評価は AI によってサポートされる可能性がある。しかし、サイバーアシスタンスサービスが保険に付帯していない場合、IT システムを「外部から」監査・評価するとなると、情報の非対称性から大きな課題が残ることになる。同時に、保険料を下げるためにデータを共有する場合、「良いリスク」と認識されることが顧客の利益になる。もう一つの関連する問題は透明性である。風評被害を避けるために、企業はサイバー事件を一般に報告しないインセンティブを持つかもしれず、明らかなデータ検閲の問題につながる。

## 3.3 ビジョン：異なるソースからのデータのプール

すでに利用可能な情報源とその構造に関する定型化された事実に関する上記の説明から、サイバーリスクとサイバー保険の領域における ML/AI の研究と進歩を妨げる最大の障害の 1 つは、利用可能なデータの不足にあることは明らかである。そこで我々は、保険会社、科学界、規制当局やサイバーセキュリティ・プロバイダーなどのステークホルダーが利用できるサイバーセキュリティとサイバーインシデントに関するデータのパブリック・プールを作るというビジョンを強く支持する。同様の構想は、他の分野ではすでに存在している（オプリスク事例の収集、貸し倒れの回収率など）。

有用なサイバー・データベースのための適切な枠組みを設計することは、サイバー領域の統計的、数理的、技術的な性質に関する知識を必要とするため、独立した研究課題である。サイバーデータベースを作成・維持するグループに資金を提供することは、サイバーセキュリティ機関／情報機関／警察／産業界／研究者にさまざまな形でのアクセスを認めることができる、非常に有用な取り組みとなりうる。この目的のために情報の共有を強制する規制措置も同様に必要である。

# 4. サイバーリスクの種類 / モデリングアプローチ

## 4.1 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

サイバー保険の分野で大きな課題となっているのは、データの不足やその非定常性だけでなく、リスクの特殊性である。もともと他のリスク用に設計された既知のモデルを、サイバーリスクを表現できるように適切に改良し、適応させる必要がある。サイバー保険の文脈では、以下の 3 つのリスク・カテゴリーを区別することができる：

非特異的リスクとは、個々の事業体レベルにおける独立した変動／損失を指す。均質なプールにおいては、これらは保険分野における古典的なリスクである。古典的な保険数理原則が適用できる。

システマティックリスクとは、サイバーリスクが、セキュリティや攻撃技術のランダムな発展や情報の流れのような、基礎となるランダムなプロセスに機能的に依存していることを指す。同様のエクスポージャーは、同じソフトウェア、サーバー、コンピューターシステムを使用したり、同じ産業部門や地域に属することから生じることが多い。この種のリスクは、金融市場の文脈ですでに詳細に分析されており、よく理解されている。

これらは、複製技法とリスク中立評価によるプライシングを含む。

システミック・リスクとは、局所的・大局的なフィードバック効果や相互作用効果のことであり、特異的な変動や外生的プロセスの個々の主体への影響だけでは説明できない。メカニズム的な連関のほかに、戦略的な相互作用も重要な役割を果たす。システミックリスクの中心は、外的要因がモデル化されたとしても、個々のサイバー契約を単独で分析することは不可能であり、むしろシステム全体を俯瞰することが不可欠であるということである。ワーム型マルウェアやサプライヤー攻撃がその例である。2007/08 年以降の金融危機の文脈でも、システミックリスクの調査は重要な意味を持っている。

## 4.2 古典的な保険数理アプローチ

サイバーリスクの価格設定とリスク管理には、特定の用途に適合した健全な保険数理モデルが必要である。特に、ランダムなサイバー事象の頻度とその結果生じる損害額を適切に表現する必要がある。古典的なアプローチは頻度-安全性モデルであり、Zeller and Scherer (2022)はこれをサイバーリスクに適合させている。モデルを校正し、適合度を検証するためのサイバーデータの不足が特に大きな課題である。データが入手可能であれば、モデルの静的分析のための技法を適用することができる。例えば、一般化加法モデル（Zeller and Scherer (2022)のように）、最尤法、限界尤法、ベイズ法を用いた頻度モデリングや、最尤法、閾値超過ピークを用いた重大度モデリングについては、Maillart and Sornette (2010)、Edwards et al (2016)、McNeil et al (2015)、Embrechts et al.

(2013)、de Zea Bermudez and Kotz (2010a)、de Zea Bermudez and Kotz (2010b)がある。

原則として、頻度-激甚度モデルはサイバーリスクのモデル化には限定的な適合性しか持たない。技術やサイバー脅威の急速な発展は、非定常的な発展をもたらす。同時に、リスク間の依存関係も統合しなければならない。古典的なモデルでは、特異リスクとシステマティック・リスクを捉えることができる。しかし、システマティックなリスクには新しいアイデアと具体的なアプローチが必要であり、研究において考案する必要がある。

## 4.3 伝染モデル

システムリスクは、エンティティ間の結合や相互作用から生じる。これらのリスクは、リスクが伝播する可能性のあるネットワーク化されたサイバーシステムの文脈において、高い関連性を持つ。同時に、行為者の行動、例えばサイバーセキュリティへの投資は、他の行為者のサイバーリスクを決定する。この点で、機械論的相互作用と戦略的相互作用を区別することができ、これには異なるモデリングアプローチが必要となる。

メカニズム的な局所的・大域的相互作用は、例えば伝染病や金融市場の分野でモデル化されてきた。頻度-深刻度モデルの文脈では、サイバー事象の発生に対する外生的要因の影響を捕捉するコックス過程は、システマティックなリスクを表現するために使用することができる。しかし、ワーム型マルウェアの拡散のようなシステマティックな現象では、フィードバックループがダイナミクスの重要なドライバーとなる。これらは、例えばホークス過程のような自己励起過程によって定量的に記述することができる。サイバーリスクとサイバー保険の文脈では、Bessy-Roland ら（2021）や Baldwin ら（2017）によってすでに適用されている。ホークス過程はその構造上、頻度・深刻度モデルに容易に統合することができる。金融データの文脈では、これらの過程は既に使用されており、また統計的に較正されている。例えば、Embrechts et al.(2011)、Daley and Vere-Jones(2003)、Giesecke(2008)、Erais et al.(2010)、AitSahalia et al.(2015)を参照。

ホークス過程は大域的なレベルでのフィードバック効果を捉えるのに適したツールではあるが、例えばコンピューターウイルスやトロイの木馬、ランサムウェアの拡散のように、エンティティ間の相互作用を詳細に表現することはできない。一方、伝染病ネットワークモデルは、ネットワークにおける動的な相互作用や増幅を記述し、分析することができる。モデルの複雑さが増すにつれ、統計的分析における課題も当然大きくなるが、反事実的なケーススタディにおいて、少なくとも定性的には重要なメカニズムを解明することができる。

Fahrenwaldt et al. (2018)では、サイバーリスクの動的伝播を研究し、ボトムアップアプローチで保険契約を評価するために、相互作用マルコフ連鎖が採用されている。特に、ネットワーク構造がサイバーリスクに重要な影響を与えることが示されている。Hillairet と Lopez(2021)は、トップダウン・アプローチに代わる興味深いアプローチを提案している。このアプローチでは、相互作用はローカル・レベルでは記述されず、母集団レベルでグローバルに記述される。具体的には、Kermack

and McKendrick (1927)の母集団ベースの SIR モデルを使用し、IT 機器のグローバルな母集団内の感受性個体、感染個体、回復個体の総数の決定論的ダイナミクスを記述する。このような実用的なアプローチでは、複数の詳細が無視されるが、モデルの管理性が大幅に向上する。拡張モデルの応用は、Hillairet et al.

## 4.4 戦略的相互作用

ネットワークにおける伝染効果に加えて、戦略的相互作用もサイバーリスクの重要な側面を構成している。第一に、サイバー脅威の領域では、攻撃とそれに対する防御は、関与する主体によって行われる戦略的ゲームである。第二に、サイバーセキュリティへの投資は、他の主体のセキュリティも高めるという外部性を持つ。第三に、規制当局、保険会社、被保険者の行動は、すべての関係者のペイオフと効用を共同で決定する。ゲーム理論は、こうした効果を研究するための適切な概念的枠組みを提供する。サイバーリスクとサイバー保険のゲーム理論的側面に関する文献は、Böhme and Schwartz (2010)、Reik and Böhme (2018)、Marotta et al. (2017)の調査で詳しく論じられている。

既存のゲーム理論モデルはこれまでのところ単純化されすぎているため、実際のデータに適用できる範囲は非常に限られていると言える。また、サイバー保険がサイバーセキュリティに与える影響など、文献にある定性的な意味合いは曖昧であり、具体的な提言を導くことはできない。

特に、サイバーリスクのゲーム理論モデルは、これまでのところほとんどが静的なものであり、非常に限られた範囲の相互作用メカニズムを持つ非常に単純なサイバーネットワークしか想定していない。したがって、今後の研究の目的の一つは、ダイナミックな設定におけるエンティティのより複雑な機械的相互作用と戦略的相互作用を組み合わせることでなければならない。

## 4.5 主要なモデル化の課題とプライシング手法

すでに述べたように、重要な課題は、十分な質と粒度の適切なデータを収集することであるが、モデルの開発と改良も今後の研究の重要な課題である。特に、システミック・リスクを適切に取り込み、同時に扱いやすいモデルを構築する必要がある。さらに、伝染に関する現実的なネットワークモデルを含む動的な戦略的相互作用モデルの設計と研究も必要である。第 6 章では、未解決の問題や今後の研究の展望について論じる。

サイバーリスクの算定には、特異リスク、システマティックリスク、システミックリスクを統合する統一的なアプローチが必要である。同時に、戦略的相互作用も考慮しなければならない。今後の研究では、この目的のために保険数理と金融数理からのアプローチをさらに発展させ、融合させる必要がある。これらの側面に関する最初の議論は、Föllmer and Schied (2002)、Wüthrich et al.(2010)、Knispel et al.(2011)、Föllmer and Schied (2016)のアプローチに基づく Awiszus et al.(2022)に見出すことができる。重要なリサーチクエスチョンのより詳細な説明は第 6 章にある。

# 5. 統計的手法、機械学習、AI

リスクと保険金請求の確率論的モデリングは、入手可能で収集されたデータの統計的分析とともに、アクチュアリーの中核的な仕事の一つである。主な用途は、リスクのプライシング、ポートフォリオ・リスクの計測（規制資本の計算を含む）、準備金の計算である。サイバーリスクの分野では、サイバーアシスタンスなどの付加サービスが中核的な重要性を持つ。すべての応用分野は相互に関連しているが、場合によっては、モデルが特定の応用分野に合わせて実用的に調整されることが多いため、若干異種にモデル化されている。

保険業界のいくつかのタスクに使用するモデル／アルゴリズムの選択は、適用される規制の枠組みの制約によっても決定される。内部プロセスは ML/AI によって顕著な制約なしに改善することができるが、プライシング、リザーブ、SCR 計算のような保険数理アプリケーションに関してはそうではない。現在、ほとんどの規制当局は、「解釈可能なモデル」の使用と、「十分に長い」データ履歴（[16]）がモデルの推定に使用されていることの証拠を要求している。今日現在、欧州の保険規制の枠組みでは、ソルベンシーⅡの第一の柱と第二の柱に関連する申請は、ほとんど「古典的な」統計的手法に基づいている。ML/AI 手法の使用に関するこの慎重な見解の詳細な理由は、コンサルテーション・ペーパーBaFin (2021)に記載されている。

この段落では、ML/AI を保険数理に応用する際に考慮すべきいくつかの問題について簡単に触れる。AI 手法の特徴として、「古典的な」統計モデルと比較して、モデル化の過程で（先験的に）仮定される規則性や構造が少ないことが多い。その仮説空間は一般的に大きくなり、因果関係はデータから発見された依存関係の同定に置き換えられる。[17]モデルはしばしばブラックボックス的な性格を示し、学習データにほとんど登場しない、あるいは全く登場しない事象への外挿は制御が難しい。データのパターンが再現されるようなモデルの一見良いパフォーマンスも、方法論のメカニズムが十分に理解されていなければ、誤解を招きかねない。このような困難は、特に定量的なリスク管理や保険の分野、つまりサイバーセキュリティのようなデリケートな分野では避けなければならない。しかし、ML/AI のツールは、GLM のような「古典的な」保険数理モデルの開発を支援するために、あるいはモデル間の競争において挑戦するために活用することができる。ソルベンシー2 の包括的な目的のひとつは、保険会社が 1 年間のデフォルト確率を「200 年に 1 度のイベント」よりも小さくするのに十分な資金を保有しているかどうかをチェックすることである。しかし、このような確率論的言明に

---

[16] この要件は、サイバー保険の分野でもこれまでの課題であった。というのも、高品質のデータがまだ十分な量入手できないからである。

[17] データに偽相関が潜んでいて、因果関係が相関関係に置き換えられているとすれば、これは深刻な問題である。 例えば、[18] 生命保険や医療保険において、平均余命や医療費が男女で異なるという明らかな統計的証拠があるにもかかわらず、なぜ男女一律の料金体系が提供されているのかを説明することができる。

は、確率モデルと、言明が適切に定義される確率空間が必要である。ML/AI モデルは多くの場合、これを提供しない。欧州法で明示されているもうひとつの包括的な目的は、差別の回避である [18] 。これを価格設定モデル内の要件に置き換えると、（性別のような）特定の変数が「古典的な」統計モデルに入らないことを「証明」するのは、ML/AI が（おそらく偏った）入力データからバイアスを推論／学習しないことを実証するのに比べ、はるかに容易であることは明らかである。これらの問題を研究機会として解釈すると、解釈可能で、説明可能な結果（依存性対因果性）を提供し、テールへの外挿の際に安定し、（保険数理上の）応用において公正／不偏であることが示される AI／ML に向けたさらなる研究を求めることが適切である。

## 5.1 サイバー で使われている確率的手法の現状

概観を提供するために、本章ではサイバー保険の分野で既に使用されている重要な確率統計モデルを抜粋して説明する。この説明は、様々なモデルの多様性を反映し、様々な可能性のあるアプローチを分類することを意図しているが、決して網羅的であることを主張するものではない。

**静的モデル：**多くの保険用途では、固定された時間軸を考慮すれば十分であり、より複雑で動的な視点は、実際的な理由から省くことができる。視野に入れる時間間隔は、多くの場合、契約期間、例えば 1 年に相当する。この目的のために、例えば、いつクレームが発生したかを正確にモニタリングしたりモデル化したりすることなく、この期間中のクレーム件数とその深刻度を調査する。最も単純には、このような考え方は、計数変数のモデル（頻度モデル）と損害分布のモデル（重大度モデル）につながる。損害の重大度に関する古典的なモデルは、ポアソン法、二項法、負の二項法、幾何級数法である。特に、損失数に対するポアソン法則は、しばしば GLM の枠組みに組み込まれ、ポアソン分布の強度パラメータ λ は、不均一なリスクを考慮するために線形モデルに適用されるリンク関数を通じてモデル化される。サイバー損害の重大度分布については、文献上いくつかの提案がある。極値理論に従い、著者によっては、損失分布の尾部（極端なサイバー損失）を一般化されたパレート分布としてモデル化することを提案している。損失分布の主要部分については、切り捨て対数正規分布が使用される可能性がある。損失を直接記述することを目的としたモデルに加えて、データ侵害で失われたレコード数を金銭的影響に結びつけるアプローチもある。これには Jacobs（2014）や Farkas ら（2021）の回帰に基づく研究がある。この文脈で関連する他の文献としては、データ漏洩をモデル化した Edwards ら（2016）がある。彼らは、暴露されたレコード数には対数正規分布を、一日の頻度には負の二項分布を使用している。Eling and Loperdo (2017)は、重大度について対数正規分布を提案している。重尾行分布に対処するための最近の論文として、Dacorogna et al.（2022）がある。

**確率過程に基づくモデル**多くの場合、ランダムな量の時間発展を明示的に考慮することが重要である。一変量または多変量変数の時間発展が注目される場合、例えばサイバー損失や攻撃の場合、確率過程はそのための適切なフレームワークである。Peng ら（2018）は、コピュラ GARCH モデルによ

ってサイバー攻撃データをモデル化している。Peng ら（2017）は、極端なサイバー攻撃率を表現するためにマークされた点過程を検討している。特異リスクやシステマティック・リスクを研究するだけでなく、システマティック・リスクを考える際には、フィードバック・メカニズムや相互作用効果が中心となる。Baldwin et al. (2017)では、サイバーセキュリティ攻撃における伝染を表現するために、自己励起過程と相互励起過程が適用されている。

**ネットワークモデルと感染拡大**ネットワーク化された IT インフラや、そのようなシステムにおけるマルウェア／ワームの広がりは、集団内での病気の広がりを記述する際に数理生物学でよく使用されるネットワークモデルの適用を動機付ける。Fahrenwaldt ら（2018）は、サイバー攻撃の文脈における脆弱性の感染拡大をモデル化し、サイバー再保険の価格を決定するための（マルコフ）SIS プロセスを検討している。Xu and Hua (2019)は、マルコフ型と非マルコフ型の伝染伝播過程を用いて、サイバー保険をモデル化し評価している。

**教師あり学習からの手法：**Farkas ら(2021)は回帰木を用いてサイバー犯罪のクレームを分析している。今後、この方向での研究が増えることが期待される。

## 5.2 ML 法と AI 法の概要

既存の ML/AI 手法の完全なレビューは本レポートの範囲を超えている。より包括的な調査や詳細については、Trevor et al. (2009)や Shalev-Shwartz and Ben-David (2014)などのモノグラフを参照されたい。ここでは、サイバーリスクの分析に ML/AI をどのように利用できるかという研究の発展機会について議論するために、重要なツールの選択に焦点を当てる。本発表では、[18] というカテゴリーを使用する：

**教師あり学習**：この分野のモデルやアルゴリズムは、入力変数（特性、共変量、予測変数とも呼ばれる）と関心のある出力の両方を含む、十分に大規模なデータセットが事前に利用可能な関数関係の分析を指す。このような状況は保険数理学では一般的である。例えば、個々の保険契約に関する履歴情報である。例えば、各保険契約、各年について、関心のある出力変数（モデル化したい）は保険金請求件数であり、入力は被保険者または保険会社に関する情報である。

**教師なし学習**：このカテゴリーは、与えられた構造がまだ課せられていない入力としての生データの分析に関するものである。むしろ、適切なアルゴリズムを適用することによって、データ内の関連構造を決定することが目的である。保険業界における例としては、与えられたリスク記述に基づくリスクのグループ化（k-means など）や、ソルベンシー II の文脈で金利シナリオに適用される主成分分析などがある。

[18] この分類は補足や改良が可能であるが、本レポートの文脈では、研究の視点を詳しく説明するのに十分であると我々は考えている。

**強化学習**：保険業界で使用される強化学習のアルゴリズムは、通常、経済問題／状況を記述する与えられた損失関数を最小化しようとする。多くの場合、これはマルコフ決定過程の枠組みで適用される。

## 5.3 保険業界で使われている ML/AI の方法

以下では、保険業界における ML/AI の既存のアプリケーションについて簡単にコメントする。

ここでは、数理的でないアプリケーションと数理的なアプリケーションの場合を区別する。

ML/AI の非数値計算への応用：

- 現在のところ、ほとんどの保険会社は ML/AI を使って、契約書、顧客との書面や口頭でのやりとり、電子メール、その他のオンライン・コミュニケーションなどのテキストや自然言語を効率的に**処理することに成功している。**
- **クレーム管理の自動**化 ML/AI によるクレーム管理はほとんどの保険会社で実施されているが、クレーム管理プロセスの自動化のレベルは異なる。
- **不正行為の検知**：保険会社にとって、不正行為の特定は重要である。クラスタリング・アルゴリズムや NN のような ML のツールは、（ある領域で）類似したクレームが不審な金額で発生していることを特定するために使用することができる。多くの場合、ML ツールは統計的テストやルールに基づく識別によって脇を固める。具体的な例は Óskarsdóttir 他（2021）に示されている。
- 主に単純な）保険商品の**引き受けを自動化する：**一部の保険会社は、旅行保険のような単純な商品を最終顧客に販売するロボ・アドバイザーの導入に成功している。
- 例えば、（ロジスティック回帰、ランダムツリー、ニューラルネットワークなどによる）解約率のモデル化や、契約解除の可能性を高める要因の特定など、**消費者の行動を理解する。**
- 他の用途としては、医療報告書のような**大きなテキスト断片の自動分析が**ある。

ML/AI の保険数理への応用：

次に、保険数理への応用について述べる。具体的な例を挙げる前に、一般的な注意を 2 つ述べておこう：

- 多くの保険数理アプリケーションやモデルは、回帰の枠組みに組み込むことができる。このことは、Richman（2018)で強調されており、GLM（頻度と重大度に対するポアソン回帰とガンマ回帰）によるリスクのプライシング、リザーブのためのチェーン・レター・アプローチの回帰コンテキストへの組み込み、リザーブのためのより高度な IBNR モデル、ライフタイムのモデリングからの例、ソルベンシーⅡ／スイス・ソルベンシー・テストのための入れ子の確率的シミュレーションなど、長い例のリストを提供している Hejazi and Jackson (2017)を参照されたい。このように回帰モデルが遍在していることを認識することは重要である。なぜなら、ML 技法はしば

しば回帰状況を出発点とし、最終的にそれを強化したり置き換えたりするために使用することができるからである。

- 数理アプリケーションで使用されている古典的な統計学の手法の多くは、技術的な観点か ら、ML の手法（ニューラルネットワークなど）に容易に置き換えることができる。このような技術シフトを阻む主な障害は、ブラックボックス・アルゴリズムが保険数理 のアプリケーションでは許されないという規制当局の懸念である。例えば、誤ったリスク評 価を除外するため、あるいは違法な差別を防止するためなどである[19] 。たとえ古典的な統計モデルがプライシングやリスク評価において依然として好まれているとしても（その解釈のしやすさを評価して）、ML/AI による新しいツールは、既存のアプローチをベンチマークし、それに挑戦するために使うことができる。

数理アプリケーションにおける ML/AI の使用に関するサーベイ論文はいくつかあり、例えば前述の Richman（2018）によるものがある。保険数理における ML/AI の利用例としては、以下のようなものがある：

- クラスタリング法によるリスク識別非均質なリスク集団が存在する場合、均質な部分集団を識別し、それらのリスク度を正しく評価することは、アクチュアリーにとって極めて重要な課題である。構造化データおよび非構造化データを用いて、様々なクラスタリング手法がこのタスクに利用できる。情報としては、テキストデータ（クレーム処理担当者のメモなど）、経済データベース、ソーシャルメディアからのデータなどがある。
- 例えば、ニューラルネットワーク、回帰フォレストなどを使って、損害の頻度と重大性をモデル化する。個々のリスクのプライシングにおいて中心的な役割を果たすこのタスクは、古典的な統計的手法（回帰、GLM、静的モデルなど）や ML のツールを用いて実行することができる。Dugas ら(2003)は、これらのツールを用いた価格決定に関する入門書を提供している。プライシングとリザーブに関する 100 以上の学術論文は、Blier-Wong ら（2020）で調査されている。
- 特徴エンジニアリング：大きな説明力を持つ新しいモデルを作成したり、既存のモデルを改良したりするには、関連する共変量／特徴を特定し、探索する必要がある。20このプロセスは、アクチュアリーの専門的判断によって実行される場合、非常に時間がかかる。さらに、統計的には無関係であるにもかかわらず、アクチュアリーにとっては妥当であるかのように見えるため、誤った特徴をモデルに組み込んでしまう可能性もある。説明可能なAIの手法に基づき、有用な特徴、さらには特徴の相互作用の可能性を自動的に特定する成功したアプローチが存在する。

---

[19] 例えば、ヨーロッパでは保険料設定に性別を共変数として使用することは認められていない。しかし、テレマティクスのデータのように、明らかに性別とリンクしていないデータからでも、高い確率で性別を予測することができる。AI による意図しない差別の問題は、ML/AI のコミュニティでは「アルゴリズムの公正さ」という用語で知られている。

[20] このトピックに関する古典的な入門書は、Bengio et al.

- 準備金を予測する：保険会社は、発生したがまだ（完全に）決済されていない保険金について、バランスシートに準備金を積み立てる必要がある。未決済の支払いを予測する作業は、通常、標準的な統計ツールによって行われる。いわゆる「チェーンレターアプローチ」は最も有名なものの一つである。Wüthrich (2018)は、MLmethods が代替案としてどのように個別クレームの支払備蓄に使用できるかを示している。この分野におけるさらなる貢献は Blier-Wong et al.
- 保険におけるリモートセンシング画像認識／画像解析ツールの興味深い応用例として、衛星画像などによるリモートセンシングがある。この応用は、例を挙げるのが一番わかりやすい：例えば、悪天候、洪水、干ばつなどによる農業の損失を考えてみよう。このような状況において、各圃場の損失を物理的な検査によって測定するのは非常に時間がかかり、コストがかかる。AI による衛星画像の解析は魅力的な代替手段であり、調査については De Leeuw et al.

我々は、保険業界における古典的なタスクの多くは、ML/AI の利用によってサポート（改善）できると結論付けている。第三者賠償責任保険などの分野では、すでに多くの研究と実務経験が存在する。今日のところ、サイバー保険については特に議論されていないが、これはおそらくこの分野が比較的新しく、短いデータ履歴しかないためであろう。とはいえ、ML/AI はサイバー保険においても興味深いユースケースを提供すると考える。しかし、サイバー保険の文脈では、特に注意しなければならないことがある：

- 学術研究者にとってデータへのアクセスは困難であり、一般的にデータが乏しい。
- サイバーデータ特有の様式化された事実（蓄積リスク、非線形依存性、非定常性など）は、ML/AI 手法の異なる採用を必要とするかもしれない。
- 保険数理、法的見解、IT 知識などを組み合わせる必要があるため、学際的なアプローチ（21 ）が必要である。

[21]これはダコローニャとクラッツ（2022 年） でも強調され、実現されている。

# 6. 将来の研究ビジョン

本章では、サイバーリスクとサイバー保険という広範な分野において、近い将来に取り組むべき研究課題をいくつか提示する。これらの問題の中には、統計モデリング、データサイエンス、AI の活用といった側面が含まれる。また、システミック・リスクや統合的なプライシング技術を組み込んだ高度なモデルの開発という重要な課題に関するものもある。

以下の一連の研究課題は、サイバー保険市場における様々な利害関係者（保険の売り手と買い手、規制当局、社会など）のニーズを考慮しつつ、既存の研究や入手可能なデータの総合的な分析、および我々自身の専門知識に基づいている。個々の研究課題は以下のように構成した：

- それぞれの**リサーチ・クエスチョン／タスク／トピックには、**それぞれのサブセクションの見出しが付けられている。
- 研究の目的は次の段落に明記する。
- その上で、この学際的研究に**誰が関わるべきか（主体）を提案している。例えば、**アクチュアリー、サイバーセキュリティ・アナリスト、心理学者、統計学者、技術者などである。一般的には、学界や規制当局から独立した研究者が、産業界の専門家と協力しながら、主にこれらの問題に取り組むべきである。
- どのような成果を求めるかを簡潔に明記した研究範囲を提案する。
- 次に、学術論文、アルゴリズム、データベース、ソフトウェアなど、**成果物の**種類を特定する。
- 最後に、**技術革新の機会について**詳しく説明する。

すべての研究活動とその成果の**受益者は**、保険会社とその顧客、規制当局、そして社会一般である。なぜなら、リスクはよりよく理解され、より適切に管理、規制、軽減されるからである。多くの場合、方法論は、複雑なサプライチェーンを持つ企業の定量的リスク管理など、他の分野にも応用される可能性がある。

## 研究テーマ 1：

## サイバーリスク評価のプロセスを改善する

目的：これまで未解決であった問題は、サイバー脅威にさらされている企業の個々のリスク状況を、サイバー損害とその財務的影響という観点から、例えば保険会社や規制当局がどのように評価すべきかという問題である。現在のところ、（サイバー）保険契約を引き受ける際には、リスク質問書を使用することが標準的な慣行となっている。

このようなアンケートには通常、IT 関連の質問、たとえばバックアップの頻度や保存データの機密性についての質問が含まれる[22] 。このようなアンケートには、驚くほど少数の質問しか含まれていないことが非常に多い。その理由のひとつは、保険市場における競争と、企業が多くの質問に答えたがらない、あるいは答えられないことである。当然の帰結として、収集される情報は非常に限られたものとなり、その結果、最も重要な質問のみを行うことが要求される。

今後の重要な研究課題は、サイバーリスク評価情報の収集プロセスをどのように大幅に改善できるかである。この質問に対する回答には、IT の知識（何が IT システムのリスク性に影響を与えるのか）、統計的な経験（どのように確率に変換できるのか）、保険数理的な視点（どのような共変量が統計モデルに入るのか）、保険市場からの洞察（どのような数や種類の質問が市場で受け入れられるのか）、心理学（これらの質問に答えることにモラルハザードはあるのか）を含む学際的な視点が必要である。リスク評価を改善するプロセスは、より優れた統計モデルから特定の IT ランドスケープにおける脆弱性の自動検出まで、様々な方法でデータサイエンス／AI によってサポートすることができる。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者

スコープ：特定の企業のリスクを分析する今日の実務を改善する。これには、IT 脆弱性の（おそらく自動的な）分析、リスク軽減のための提案、アクチュアリーや規制当局が使用する確率論的モデルへのマッピングが含まれる。

期待される成果と成果物：研究論文、確率モデル、ソフトウェア、アンケートの設計基準、リスク分析のマニュアル。

---

[22]また、多くの組織にとって、サイバーリスクはまだビジネスリスクとして考慮されておらず、主に IT/エンタープライズリスクとして考慮されているという事実も重要な点である。評価は技術的／技術的な観点から行われ、ビジネスの観点からは行われない。

イノベーションの機会：

- 技術（自動化）を利用して、顧客の内部または外部のリスク評価を行う。
- 自社のリスクプロファイルを（再）評価するためのソフトウェアを開発する。
- IT システムの脆弱性を自動検出する。
- 特定された不確実性に対処するための従業員研修
- サイバー領域における高度な統計モデルの開発
- サイバー分野のリスク分析において、どの質問が本当に重要かを理解する。

22 また、多くの組織にとって、サイバーリスクはまだビジネスリスクとして考慮されておらず、主に IT/企業リスクとして考慮されているという事実も重要な点である。評価は技術的／技術的な観点から行われ、ビジネスの観点からは行われない。

## 研究テーマ 2：

## 関連する共同変数を特定する／個々の価格設定を改善する

目的：関連する共変量を特定する作業は、リサーチ・トピック#1 で議論し始めたアンダーライティング・プロセスに関連しているが、このトピックは統計的モデリングにより深く踏み込んだものである。アクチュアリーは、どの共変量が組織の個別リスクを評価する上で重要であるかをより深く理解する必要がある。現在までのところ、このテーマに関する数少ない学術論文のほとんどは、企業の産業セグメントや企業規模といった間接的な情報を用いている。直感的には、例えば IT ランドスケープや、当該企業で働く従業員のサイバーリスクに関する教育など、より直接的な情報を含めることが望ましいと思われる。

統計学的な観点からは、この作業は重要な問題に集約される：

- 関連する共変量（引受プロセスの一環として現実的に測定可能なもの）を特定する。
- これらの共変量を発生確率と重大度分布に変換する数学的モデルは、最終的に（異質な）リスクに対する保険料を意味する。

関連する共変量の同定には、ニューラルネットワークのような教師あり学習法や、説明可能なアル／説明可能な ML の分野のツールを用いることができる。適切なモデルの特徴づけと効率的な手法やアルゴリズムの開発は重要な研究テーマである。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者

スコープ：個々のリスクを説明するための関連する共変数を特定し、サイバー保険のプライシングモデルに使用する。十分なデータが得られたら、これらの共変数の統計的有意性についてバックテストを実施する。

期待される成果と成果物：研究論文、確率モデル、ソフトウェア。

イノベーションの機会：

- IT の専門知識と数理モデリングを組み合わせる。
- 関連する共変数を特定するために、説明可能な AI のツールを使用する。
- サイバーリスクに関する革新的な統計モデルを作成する。
- 高度なモデル選択ツールを使う

## 研究テーマ 3：

## 損失頻度と重大性のモデル化と推定

目的：もう一つの重要な課題は、利用可能なデータと将来収集される可能性のあるデータに基づき、価格設定とリスク管理に使用できる適合した統計的手法と組み合わせて、頻度／重大度モデルを開発することである。可能な限り均質な料金クラスを生成するためには、企業や契約を分類するサイバーリスクモジュールを適切に定義する必要がある。頻度／重大度モデルは、基礎となる過程（非均質なポアソン過程、コックス過程、ホークス過程など）や重大度分布の選択に自由度を認めるものでもある。モデルの選択と統計的適用の手順を開発しなければならないが、これは AI 法を用いて自動化することもできる。クレーム管理のプロセスは、モデリングとプライシングの視点に合わせるべきである。[23]

エンティティ：アクチュアリー、IT 専門家、確率論者、統計学者

スコープ：損失頻度と重大度に関する革新的な数理モデルを開発し、部分的に専門家の知識に基づく可能性のあるデータに対する推定方法、バックテスト戦略を含む。

期待される成果と成果物：研究論文、数理モデル、ソフトウェア

イノベーションの機会：

- サイバーリスクに関する革新的な確率モデルを開発する。
- ML/AI を使用して変数選択を自動化する。既存のアプローチを使用するか、新しいアイデアを開発する。
- モデル推定プロセスにおいて、データと専門家の意見を組み合わせる。
- サイバーリスクと関連データの非定常性に対処する。

23

## 研究テーマ 4：

## ネットワーク・モデルにおけるシステミック・リスクのモデル化

目的：サイバーリスクの特徴は、特に複雑なシステムにおいて伝染効果が主要な要因となりうることである。したがって、これらのプロセスを適切に記述するネットワーク上の伝染病サイバーリスクモデルを開発することが、引き続き研究の重要な課題である。そのためには、高い粒度における複雑さと、扱いやすさを向上させるための実際的な単純化とのバランスをとる必要がある。そのためには、集約的なレベルでのエンティティの相互作用を捉えるトップダウンモデルの構築と分析が必要になるかもしれない。同時に、大規模モデルの評価を可能にする効率的な数値計算手法、例えばモンテカルロ・シミュレーション法を考案しなければならない。

エンティティ：アクチュアリー、数理生物学者、IT 専門家、リスクマネージャー、確率学者、統計学者。

スコープ：IT ネットワークにおけるシステミック・リスクの現実的なモデルを開発する。基礎となる高次元の数値問題を解く。統計的手法を考案する。

期待される成果と成果物：研究論文、確率ネットワークモデル、ソフトウェア。

イノベーションの機会：

- 革新的な伝染モデルを開発する。
- 革新的な数値的・統計的手法を考案する。
- 今回の文脈で開発されたモデルは、例えば複雑なサプライチェーンを持つ企業のリスク管理など、他の活動／産業／セクターにも利用できるだろう。

## 研究テーマ 5：

## ダイナミックな戦略的相互作用のモデル化

目的：サイバーリスク分野におけるアクターの戦略的相互作用のモデル化は、これまで主に静的モデルに限られてきた。このような関係者の相互作用は、サイバー・エコシステムにおけるサイバー保険の役割の評価にも強く関連している。伝染プロセスは本来ダイナミックなものであるため、プロセスの時間的次元を無視した単純化では不十分な可能性がある。したがって、学術研究は、複雑なネットワークにおける伝染プロセスも考慮した、動的なゲーム理論的サイバーモデルを開発すべきである。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバーリスクの分野における関係者の動的な戦略的相互作用のモデル、サイバーリスクを促進する主要要因の特定。

期待される成果と成果物：研究論文、洗練されたゲーム理論モデル。

イノベーションの機会：

- 動的なゲーム理論的サイバーモデルを開発する。
- 特定された相互作用は、リスクプロファイルを作成する際の共変量として考慮される可能性があり、したがって引受プロセスで使用される可能性がある。

## 研究テーマ 6：

## 多層ネットワークを理解する

目的：生産プロセス、ロジスティクス、金融市場はすべて、今日ではデジタル技術を統合したネットワークを構成しており、それゆえサイバーリスクにさらされている。このように、リスクは多層ネットワークに内在しており、サイバーネットワークはその重要な構成要素の一つである。潜在的な損失をモデル化するためには、相互接続されたネットワークを包括的にモデル化することが望まれる。その知見は、保険ソリューションの開発にも、規制政策上の問題の評価にも利用できる。多層ネットワークは、今後の研究にとってエキサイティングな課題である。

エンティティ：アクチュアリー、IT 専門家、ERM 専門家、リスク管理者、統計専門家。

スコープ：多層ネットワークのモデル、リスク、保険、規制への影響。

期待される成果と成果物：研究論文、確率モデル、シミュレーションアルゴリズム

イノベーションの機会：

- 相互接続されたネットワークの包括的モデリング。
- そのようなネットワークに適合する実世界のデータを入手し、ネットワークの相互作用における構成要素の重要性を定量化する。
- 結合ネットワークの耐障害性を高める方法を特定する。

## 研究テーマ 7：

## 特異リスク、システマティック・リスク、システミック・リスクのプライシング

目的：数理科学と金融数学は、リスクのプライシングのための手法を提供する。これらの手法は主に、プーリング、複製、残存リスクの評価に基づいている。サイバー事象の文脈では、3 つのリスク・カテゴリー（特有リスク、システマティック・リスク、システミック・リスク）が特に関連しており、すべての要素を統合的に組み込んだ統一的な枠組みの設計が本質的な研究課題である。

特に、システミックリスクのプライシングについては、決定的な解明がなされていない。

最後に、プライシングの方法論は、利用可能なデータを用いてキャリブレーションされた具体的なモデルに基づいて保険実務に適用されるべきである。サイバー保険の分野では、これまで場当たり的な手法が適用されてきた。

エンティティ：アクチュアリー、リスクマネージャー、統計学者

スコープ：保険数理的な観点から、サイバーリスクの異なるカテゴリー（特異リスク、システマティックリスク、システミックリスク）を区別し、全体的な方法でモデル化し、統合的なプライシングの枠組みを開発する。

期待される成果と成果物：研究論文、価格設定アルゴリズム、ソフトウェア

イノベーションの機会：

- サイバーリスクのあらゆる側面のプライシングのための包括的モデルを開発する。
- 規制の観点から、標準化された手法と個別のモデルの使い分けについて、関連するいくつかのリスクカテゴリーと照らし合わせながら議論する。

## 研究テーマ 8：

## システミック・サイバーリスクに関するデータ

目的：サイバーリスクとサイバー保険の分野では、データはまだ十分には利用できない。システミック・リスクに直面した場合、デジタル・ネットワークにおける損失蓄積を特徴づけるデータがさらに重要となる。疫病ネットワークモデルの文脈では、接続性情報が中心的な重要性を持つ。関連する研究課題は、i）システミックリスク、その根底にあるグラフ構造、および拡散プロセスを特徴づけるためには、どのような種類のデータ（および情報源）が不可欠か、ii）利用可能なデータ量に応じて、モデルの較正のためにどのような統計手法が利用可能か、または開発する必要があるか、である。同時に、公的研究に利用可能な適切なデータベースを構築するための戦略を考案する必要がある。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：システミック・リスク、特にスプレッド・プロセスに関連するデータを特定する。

期待される成果と成果物：研究論文、サイバーリスクに関する想定データベースの仕様、データベース。

イノベーションの機会：

- データを特徴付け、システミックリスクに関連する統計的手法を開発する。
- 実データからシステミックなサイバーリスク、特に相互作用プロセスやネットワーク構造を推定する。
- 異なる情報源からのサイバーデータをプールし、統計的推論の確かな基礎を提供する。
- 保険数理／サイバーセキュリティの学術研究者と規制当局が協力する。

## 研究テーマ 9：

## 既存の ML メソッドをサイバー犯罪特有の様式化された事実に適応させる。

目的：どのような統計モデルや ML/AI 手法の適切性も、選択されたモデルの枠組みに関する基礎的な仮定に大きく依存する。例えば、入力データが独立かつ同一分布であることが要求される場合がある。サイバーの文脈では、入力データが非定常（これは同一分布に違反する）、従属（これは独立に違反する）、重尾行（すなわち、モーメント条件に違反する可能性がある）であると信じるに足る説得力のある理由がある。必要な仮定の正式な検証なしに統計的手法を適用することは可能である（純粋に実用的な観点からはある程度うまくいくことが多い、つまり何らかの結果が得られる）が、有害な結果をもたらす欠陥のある推論が発生する可能性があるため、推奨はできない。特にサイバーリスクの特性を考慮すると、既存の統計的手法、データサイエンスの手法、AI のツールの前提を緩和して数学的研究を行う必要がある。

エンティティ：アクチュアリー、数学者、確率学者、統計学者。

スコープ：ML/AI/古典統計学の既存の手法を、その基礎となる仮定とそれを緩和する可能性の観点から分析する。サイバーアプリケーションに適した拡張を開発する。

期待される成果と成果物：研究論文、アルゴリズム、ソフトウェア

技術革新の機会:

- 非定常データ、依存データ、ヘビーテールデータのための ML 手法。
- アルにおける概念的革新
- サイバーリスクに適した ML 技術。

## 研究テーマ 10：

## サイバーリスクに関するモデルの推定（統計的推定と専門家の意見の組合わせ等）

目的：これまで、実現したサイバー損害（または関連情報）に関するデータは限られていた。しかし、根本的なリスクについては技術的な理解があり、その経済的な結果については経済的な理解がある。限られたデータに対処するための明白なアプローチは、経験的データと専門家の意見を組み合わせてモデルを開発し、結論を導き出すことである。データの不足は、根本的な問題の構造的な理解によって緩和される可能性がある。このような異質な情報源を組み合わせることは、さまざまな方法と数学的ツールを用いて達成することができる。重要な研究課題は、このような方法論のための有効で頑健な戦略をどのように考案するかということである。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：データと専門家の意見を数学的に正しい方法で組み合わせ、サイバーリスクの有効かつ強固な推定戦略を考案する。

期待される成果と成果物：研究論文、アルゴリズム、ソフトウェア

イノベーションの機会：

- データとモデルに関する構造的知識を組み合わせるための新しい統計的方法論（ベイズの枠組みなど）を開発する。
- より多くのデータや専門家の意見が入手可能になった場合、推定値を一貫して更新する方法を検討する。

# 研究テーマ 11：

# サイバーアシスタンス

目的：サイバー保険は多くの場合、純粋なリスク移転だけでなく、サイバーアシスタンスと組み合わされている。サイバーアシスタンスとは、サイバーセキュリティを積極的に向上させるサービスや、サイバーインシデントが発生した場合の被害への対処をサポートするサービスである。サイバーアシスタンスは保険会社のビジネスモデルを拡張し、多くの場合、有能な IT 専門家をパートナーとして従事させるが、情報の非対称性を低減し、リスクを軽減することも可能にする。サイバーアシスタンスは多くの興味深い問題を提起しており、そのすべてがさらなる研究の可能性を秘めている：

(a) 市場ではどのようなサイバー支援が求められているのか？

(b) このようなサービスは、個人のリスクを軽減するためにどのように設計されるのだろうか？

(c) サイバー・サービスはシステミック／システム上のリスクも軽減できるのか？

(d) サイバーサービスのコストは保険会社と被保険者の間でどのように分担すべきか？

エンティティ：アクチュアリー、IT 専門家、プロダクト・デザイナー、リスク・マネージャー、統計学者。

スコープ：商品設計、リスク分布への影響などを含め、サイバー保険におけるサイバー支援の可能性について全体的な理解を得る。

期待される成果と成果物：学術論文、保険商品のドラフト。

イノベーションの機会：

- 革新的な支援サービスを開発し、価格を設定する。
- リスク移転とリスク軽減を組み合わせる。
- 効率的な IT 支援を導入することでリスクを軽減する。
- 適切な警告システムを導入することで、IT インフラ全体を安定させる。

## 研究テーマ 12：

## 累積リスクのヘッジ

目的：リスクマネジャーやアクチュアリーの観点から、少なくとも 2 つの定型化された統計的事実はサイバー保険において非常に重要である：

(a) 大規模な個別損害（極端なサイバー事件）；

(b) 多くの損失が同時に発生する事象（累積リスク）。

カテゴリー(a)は、保険契約における適切なカバー限度額によって削減することができるが、2 つ目のカテゴリー(b)は、価格設定、保険設計、リスク管理において積極的に検討する必要がある課題である。特別な再保険契約、金融市場における保険リンク証券の発行、あるいは政府の介入を通じて、蓄積リスクにいかに有意義に対処できるかを探ることは興味深く、また重要である。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：特別な再保険契約、金融市場における保険リンク証券の発行、または政府の介入を通じて、蓄積リスクにどのように対処できるかを調査する。

期待される成果と成果物：研究論文、契約設計、規制介入のためのガイドライン。

イノベーションの機会：

- ILS や政府の介入は、蓄財のためだけでなく、他の状況においても検討すべき興味深い選択肢である。
- このテーマは政策研究者にとってもチャンスである。

## 研究テーマ 13：

## 資産クラスとしてのサイバーリスク

目的：自然災害のリスクを資本市場に移転するために、いわゆる CAT ボンドが長年利用されてきた NatCat になぞらえれば、サイバー関連の変数に依存するクーポンを持つ同様のボンドを立ち上げることはもっともらしいと思われる。このような保険リンク証券をどのように設計し、モデル化し、価格設定することができるのか、また、それが市場に受け入れられるのかどうかは、依然として未解決の研究課題である。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバー関連保険リンク証券が、サイバーリスクを金融市場に移転することを可能にする資産クラスとなり得るかどうか、またどのようになり得るかを分析する。

期待される成果と成果物：研究論文、サイバー関連保険リンク証券の青写真。

イノベーションの機会：

- 再保険、金融市場、ポートフォリオ最適化の研究者や専門家を巻き込み、革新的な商品を構築する。
- 幅広いリソースを活用し、サイバーリスクを金銭的にヘッジする。

## 研究テーマ 14：

## サイバー保険ギャップを埋める

目的：現在、サイバー保険の需要と供給のミスマッチ、いわゆるサイバー保険ギャップが頻繁に報告されている。保険会社がなぜこの分野の保険契約を増やしたがらないのかを詳しく調べることは興味深いだけでなく、このギャップを埋める革新的な方法を見つけることは業界にとっても有益であろう。需要と供給の相互作用の中で、顧客のニーズ（例えば、無制限の保険カバー）とリスク管理上の考慮事項（例えば、極端なポートフォリオ・ロスの削減）のバランスをどのように取るかを理解することが重要である。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバー分野における現在の保険格差の原因を分析し、それを克服する方法を提案する。

期待される成果と成果物：研究論文、サイバー・カバレッジを高めるための戦略

イノベーションの機会：

- サイバー保険格差の理由を理解する（経済、行動、リスク管理の観点から）。
- 顧客のニーズに対する洞察力を高め、これらのニーズを保険会社が提供する商品に対応させる。

# 研究テーマ 15：

# 最適な契約設計

目的：保険契約の設計には、複数の側面から詳細なバランスをとる必要がある：

(a) 十分な保険需要を保証するためには、顧客のニーズに適切に対応しなければならない。

(b) 契約上および法律上の観点から、どの事象がカバーされ、どの事象が除外されるかを明確に規定しなければならない。

(c) 契約は（生の保険金請求に適用される計算式として）保険会社がカバーする保険金請求部分の配分を変更する。顧客と保険会社の両方の観点から、契約設計は損害発生時に提供される補償額を反映したものでなければならない。

(d) サイバー・アシスタンス・サービスは、純粋なリスク移転に加えて含まれなければならないもう一つの要素である。

(e) 理想的には、契約設計は潜在的な損害の保険数理上の評価と一致しており、クレーム部門は発生した損害に関する情報を一貫した方法で収集し、記録している。

これらの要件のバランスをとるのは、一般的に容易なことではない。さらに、目的関数が複雑であるため、「最適な契約」の基準を定義することさえ困難な作業である。サイバー保険の文脈でこの多次元問題をより深く調査することは、依然として重要な研究課題である。

エンティティ：アクチュアリー、IT 専門家、確率論者、リスクマネージャー、統計学者。

スコープ：最適なサイバー保険契約の様々な側面を理解し、その知識を最適な設計に活用する。

期待される成果と成果物：研究論文、適切かつ革新的なサイバー保険契約を規定するガイドライン。

イノベーションの機会：

- サイバーエクスポージャーに関する学際的な洞察を組み合わせ、優れた製品を提供する。
- 契約設計が提供する機会を活用し、ポートフォリオの損失分配を最適な形で形成する。

# 研究テーマ 16：

# 行動上の課題

目的：サイバーリスクの分野では、コンピューターなどのデジタル技術の利用者の行動も重要な意味を持つ。例えば、ソーシャル・エンジニアリングは、機密情報の漏洩の引き金となり、ハッカーに他の保護されたシステムへのアクセスを提供する可能性がある。保険リスクと潜在的な損失を評価するためには、サイバーアシスタンスサービスの文脈でも同様に、リスクの範囲、保護手段、発生した損失、インシデントへの対処戦略に関するデータを収集し、適切なモデルを開発する必要がある。この研究課題には、保険数理科学、コンピュータ科学、社会科学、心理学の各分野の専門家による学際的な協力が必要である。

エンティティ：IT 専門家、心理学者、リスクマネージャー

スコープ：：行動特性によるサイバーリスクの範囲、保護対策、発生した損失に関するデータを収集する。インシデント管理戦略を調査、考案し、適切なモデルを開発する。

期待される成果と成果物：研究論文、トレーニングチュートリアルの開発

イノベーションの機会：

- ソーシャル・エンジニアリングのさまざまな形態を、リスク、技術、社会通念、心理的側面などの観点から分類する。
- これらの脆弱性を軽減するために、どのような手段が効果的かを理解する。

## 研究テーマ 17：

## 個人顧客向けサイバー保険

目的：現在、サイバー保険市場の発展の焦点は、主に企業や大規模な機関を対象とした補償に置かれている。その背景には、複雑で非定常的なサイバーリスクは、エクスポージャーを評価する際に不完全な情報に直面し、かなり注意深く監視しなければならないことがある。サイバーアシスタンスはサイバー保険の重要な柱であり、保険のビジネスモデルを拡大すると同時に、このような環境下でのリスク移転を促進する。複雑で個別的なサービスを個人顧客向けに確立するのは困難である。そのようなソリューションは標準化され、スケーラブルでなければならない。個人顧客にとってのもう一つの重要な課題は、サイバー・イベントの発生確率がユーザーの行動に大きく影響されることである。しかし、これは直接観測できるものではない。企業とのもう一つの違いは、個人家庭におけるサイバー事件は、しばしば金銭以外の損失（失われた個人データ、評判へのダメージなど）につながることであり、これらは通常、保険の対象には含まれない。

したがって、重要な研究課題は、個人顧客向けの費用対効果の高いサイバー保険商品の開発である。情報の非対称性から、ボーナス・マルスのシステムや、セキュリティ・ソフトウェアや標準化されたサイバーアシスタンスとの組み合わせは、有望なアプローチかもしれない。また、個人顧客セグメントにおけるこのような商品が、一般的にどの程度サイバーセキュリティを向上させることができるのか、また、どの程度福祉を向上させることができるのかを調査する必要がある。

主体：アクチュアリー、IT 専門家、製品デザイナー。

スコープ：個人顧客向けに標準化されたサイバー保険ソリューションを開発する。

期待される成果と成果物：研究論文、製品イノベーションの提案

イノベーションの機会：

- 個人顧客セグメントにおけるサイバー保険ソリューションを標準化した。
- 適切なボーナス・マルスのシステム、セキュリティ・ソフトウェアやサイバー支援との結合。
- 福祉への影響を分析する。

# 研究テーマ 18：

# システムの回復力

目的：サイバー損害の程度は、システムの設計によって形成される可能性がある。サイバーシステムは一元的に管理されることなく、ダイナミックかつインタラクティブに進化するが、その発展は規制の介入によって影響を受ける可能性がある。リスク移転としてサイバー保険を提供し、連携サービスとしてサイバーアシスタンスを提供する保険業者の専門知識は、規制政策を設計する際に含まれるかもしれない。同時に、保険契約の条項が代理店にインセンティブを与え、サイバーセキュリティの体系的な向上につながるかもしれない。重要な研究課題は、保険業界と規制当局がどのように連携してデジタル・ネットワークの回復力を高めることができるかということである。これは、レジリエントな欧州を構築するための重要な要素である。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：保険業界と規制当局が連携してデジタル・ネットワークの回復力を高めるための指針を提供する。

期待される成果と成果物：研究論文、政策提言

イノベーションの機会：

- サイバー保険会社やサイバーセキュリティ・プロバイダーの学際的な専門知識を活用し、レジリエントなデジタルシステムがどのように構成されているかを学ぶ。
- 学際的な研究は、デジタル技術の回復力を高めるための効率的な戦略を生み出すことができる。

# 研究テーマ 19：

# モデルの堅牢性

目的：データとモデルはサイバーリスクと潜在的なサイバー損害の評価を可能にし、それによってリスクの軽減とヘッジに貢献する有用な情報を提供する。しかし、モデルに絶対的な信頼性と正しさを求めるナイーブな見方は適切ではない。モデルの仕様が誤っていたり、確率の推定が間違っていたり、あるいは単に起こりうるシナリオを無視していたりする可能性がある。モデルの堅牢な仕様と堅牢なソリューションの設計は、サイバーリスクの分野におけるもう一つの重要な研究課題であり、ナイティアンの不確実性に関する保険数理や金融の文献と密接に関連している。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバーリスク領域におけるモデルの堅牢な仕様を開発する方法と、堅牢なソリューションを特徴付ける方法を調査する。

期待される成果と成果物：研究論文、実務への応用に関する提言

イノベーションの機会：

- ナイト派の不確実性の中で十分に機能する戦略を提供する。これにより、実際のセキュリティとリスク管理が大幅に改善される。
- 学術的には、ナイト派の不確実性と最適な意思決定に関する最新の結果を、サイバーセキュリティと保険の分野に移転する道が開かれる。

# 研究テーマ 20：

# データ収集

目的：本報告書の各所で強調されているように、十分に質の高いデータの欠如は、科学研究にとって大きな問題であると同時に、保険分野におけるリスク移転の解決策にも支障をきたしている。データ保護だけでなく、経済主体レベルのインセンティブが、重要な情報を研究者と共有することを妨げている。他方、犯罪集団は、ルールに従うことなくデータへのアクセスを獲得し、それを不正な目的のために利用する。この非対称性は、サイバー・システム・セキュリティの発展において深刻な問題を引き起こす可能性がある。だからこそ、研究においては、サイバーシステムのセキュリティを損なうことなく、科学者がデータにアクセスできるような戦略を立てるべきなのである。

一方で、サイバーセキュリティ分野の企業は、標準化され匿名化された方法で研究目的のためにデータを提供できるようにしなければならない。他方で、一般的に企業は研究目的で情報を広く利用できるようにする経済的インセンティブを持たないため、欧州の研究者のために適切なデータベースの開発を強制する規制要件を設けるべきである。他のほとんどの大陸では、データの流れや保存に関する規制が緩く、民間の技術者グループがデータベースを構築し利用することができるため、これは、国際競争の観点からも、欧州の成功に不可欠である。特に研究目的のデータは、犯罪集団に競争上の優位性を与え続けるのではなく、サイバーセキュリティを強化するための AI の開発を促進することができる。最低限の目標は、公平な競争の場を作ることである。研究用データベースの開発と、それに付随する必要な規制措置の設計は、重要な研究テーマである。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバーシステムの安全性を損なうことなく、科学者のデータアクセスを可能にする戦略を策定する。これには、調整された法的枠組みと規制介入が必要である。

期待される成果と成果物：データベース、学術論文、サイバーセキュリティの向上。

イノベーションの機会：

- 適切なデータベースを通じて、サイバー脅威との闘いにおいて、欧州が他の地域と比較して公平な競争条件を構築する。
- 欧州における学際的な専門知識を拡大することにより、サイバーセキュリティ分野における革新的な開発を促進する。

- サイバーセキュリティと保険における現実的な評価と成功戦略を達成するために、実際のデータに基づいてモデルを構築、校正、検証する。

# 研究テーマ 21：

# 福祉と規制への影響

目的：サイバーセキュリティの向上とサイバー保険による金銭的な保護は、コストがかからないわけではないが、技術プロセスや経済全体の回復力を高めることができる。規制要件は、適切な対策を実施し、有害な行動を抑制するインセンティブを創出しなければならない。適切な仕組みを構築するためには、仕組みと規制の厚生への影響を理解する必要がある。この作業は非常に複雑であり、社会への影響だけでなく、他のシステムと結合したサイバーネットワークの優れたモデルを必要とする。

そのためには、アクチュアリーや数理経済学者、IT の専門家が参加する学際的な研究が必要だ。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバーセキュリティ、サイバー保険、規制が福祉に与える影響を調査し、効率的な投資と規制措置の提言を決定する。

期待される成果と成果物：研究論文、規制政策への提言

イノベーションの機会：

- 社会福祉の一般的な文脈におけるサイバーセキュリティと保険の分析。
- リスクと対策を、社会にとっての利益という観点から評価する。
- 対策と規制の根拠

## 研究テーマ 22：

## サイバーリスクに対する説明可能な ai

目的：多くの中核的な保険アプリケーション、特に保険数理において、機械学習ツールは、一般的に十分な説明ができず、場合によっては不透明であるため、規制当局から直接利用することは認められていない。このような理由から、ML は保険会社において、プロセスを合理化する手段として、あるいは保険数理モデリングに取って代わることなく、古典的な保険数理モデリングを支援／強化する手段として適用されることがほとんどである。このことは、いくつかの問題を提起している：サイバー保険の文脈における ML 手法は、保険のプライシングとリザーブに関する現行の規制要件にどのように適合させることができるのか？規制上の要件を満たすために、ML 手法はどのように古典的な保険数理手法と組み合わせることができるか？説明可能な保険数理において、さらなるテスト手続きに必要な追加コストは何か？説明可能な AI、すなわち AI の妥当性をテストすることは、AI の上に別のモデル層を導入することになる：これは、どの程度モデルの不確実性を増大させるのか？

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：サイバーリスクに対する説明可能な AI の方法を考案する。AI の費用便益分析のレシピを提供する。

期待される成果と成果物：研究論文、モデル選択のガイドライン、アルゴリズム。

イノベーションの機会：

- サイバーリスクの説明可能なアル
- 人工知能分野における能力を大幅に強化する。

## 研究テーマ 23：

## ビジョン：自律的なサイバーリスク管理

目的：多くの分野で、部分的なタスクの自動化が可能である。例えば保険業界では、クレームの自動管理や引き受けの自動化、リスク分類、プライシング、リザーブリングに ML を活用することなどが将来的に考えられる。サイバーリスクとサイバー保険の分野では、この種の応用はまだ検討されていない。人工知能はこれまでのところ、大量のデータの評価を自動化・高速化する手段として成功を収めている。しかし、実質的な認知能力を必要とする複雑な評価にはまだ手が届いていない。

したがって、サイバーリスクの包括的な自動リスク管理のための青写真を作成することが先見的な課題であり、あらゆるレベルで自律的に分析を実施し、理解しやすい方法で行動を提案し、その実行を決定する。このようなアプローチは、まず、シミュレートされたデータに基づいて作成された簡略化された人工環境において、プロトタイプとして実験的に実装することができる。さらなるステップでは、この方法論の拡張性と頑健性がテストされるだろう。長期的な最終結果は、現実世界における自律的なリスク管理を前向きに構想することであるが、中期的な焦点は、サイバーリスクとリスク管理の交差点における人工知能の応用に関する実質的な専門知識を欧州で開発することにある。

エンティティ：アクチュアリー、IT 専門家、リスクマネージャー、統計学者。

スコープ：人工環境における自律的なサイバーリスク管理を設計し、サイバーリスクとリスク管理の交差点における人工知能に関する実質的な専門知識を開発する。

期待される成果と成果物：研究論文、シミュレーションアルゴリズム、人工データ、ソフトウェア。

イノベーションの機会：

- サイバーリスク分野におけるリスク管理の自動化。
- 人工知能分野における能力を大幅に強化する。
- リスク管理、IT、人工知能の分野における学際的な相乗効果

# 7. 結論

サイバーリスクは複雑な特徴を示している。それらは非定常であり、相互作用する技術的・社会的システムの中で時間とともに進化する。相互作用と重い尾引きがサイバーリスクの特徴である。本報告書では、サイバーリスクとサイバー保険に関する今後の研究の主要課題を明らかにした。第 6 章で詳細にまとめた疑問点を調査するには、専門家間の学際的な協力が必要であり、それには保険数理や IT セキュリティの分野の科学者、規制当局や企業の関係者が関与すべきである。

**データ：**データ：データの収集とその利用可能性は、今後大幅に改善されなければならない。現在までのところ、研究に利用できるデータは限られており、その質も向上させなければならない。我々は、欧州がサイバーセキュリティにおいて競争力を持つことができるデータベースを実現するために、政府のインセンティブと規制介入を提唱する。これはまた、レジリエントな欧州を構築する上で不可欠な前提条件でもある。

**モデル：**サイバーリスクのモデルは、保険数理分析やリスク管理ソリューションの実行可能性の基礎でもあるが、さらに開発されなければならない。これは、実務でプロキシとして使用できる実用的なモデルと、サイバーリスクの主な分類（特異リスク、システマティックリスク、システミックリスク）を捉えるモデルの両方に関するものである。

**統計的手法：**同時に、データを分析し、統計的手法をさらに開発または適応させなければならない。これには ML/AI 分野の手法も含まれる。

**保険商品と市場：**サイバー保険とサイバーアシスタンスの組み合わせや最適な契約設計は、サイバー保険のギャップを埋める戦略と同様に重要なテーマである。個人顧客セグメント向けに標準化されたサイバー保険をどのようにうまく設計するかも重要な問題である。

**社会的・規制的影響：**サイバー保険と関連商品は福祉にプラスの影響を与えるだろう。これについては、より詳細に検討する必要がある。政府関係者は、サイバーネットワークの機能性とセキュリティの両方を強化するような形で関係者のガードレールを選択し、それによって欧州における全体的なレジリエントな構造を確立すべきである。

# 8.保険用語集

| | | |
|---|---|---|
| **Accumulation risk(s)** | **累積リスク** | 同じ基礎的要因または結合プロセスによって引き起こされるリスク／損失の累積 |
| **Actuary** | **アクチュアリー** | 保険数理科学の専門家であり、通常は保険業界または学界で働く数学者である。 |
| **Adverse selection** | **不利な選択** | 逆選択とは、情報の非対称性に直面した行為者の意思決定行動がパレート最適でないことを指す。保険の文脈では、この用語は主に契約締結前の意思決定を指す。リスク選択が不十分な場合、結果として悪いリスクだけが保険対象となり、良いリスクに対する保険料は高すぎる。 |
| **Aggregate losses** | **総合損失** | 保険ポートフォリオや保険会社のレベルなど、集合的なレベルでの損失 |
| **Calibration** | **キャリブレーション** | 主に利用可能なデータに基づいて、特定のモデル・パラメータを持つ具体的なモデルを選択すること。金融市場の文脈では、通常、モデル価格が市場価格と一致するようにモデル・パラメータを指定することを意味する。 |
| **Central limit theorem** | **中心極限定理** | 極限定理は、独立・同定分布するリスクの和がほぼ正規分布することを説明する。 |
| **Claim** | **クレーム** | 契約上カバーされている損害による保険契約者の請求 |
| **Collective models** | **集団モデル** | 保険集団をロス・プロデューサーとして解釈する保険数理モデルの一種。これにより、非均質プールの場合でも、独立同次分布確率変数によって損失を記述することができる。 |
| **Consequential damage** | **結果的損害** | ある事象の結果として発生する損失。保険契約においては、どの事象とどの損失が契約の対象となるかが重要である。 |
| **Contingency plans** | **緊急時対応計画** | コンティンジェンシープランは、万が一の事態に備え、的を射た方法で対応できるようにするために、事前に取るべき行動を記述するものである（ピアソンの）相関は、2 つの確率変数の間の一対（線形）依存性の尺度である。最もよく知られた依存性の尺度であるため、確率的依存性の同義語として口語で使われることが多い。 |
| **Correlation** | **相関性** | 2 つの確率変数の相関は、共分散と標準偏差の積の商として得られるパラメータである。多変量ガウス確率変数の文脈では、相関は依存構造を記述する。しかし一般に、相関は周辺分布の関数でもあ |

| | | |
|---|---|---|
| | | り、依存関係を適切に特徴付けることはできない。代わりにコピュラのような他の概念が必要である。 |
| **Copula** | **コピュラ** | ランダムベクトル内の依存構造に関する全情報を含む関数。ランダムベクトルを一変量の周辺則とそれらの間の関連を捕捉するコピュラに分離することができる。 |
| **Covariates** | **共変量** | 出力が機能的に依存する外生的な入力は、共変量と呼ばれる。 |
| **Dependencies** | **依存関係** | 確率論では、2 つの確率変数が独立であるとは、一方の確率変数の分布が他方の確率変数の無条件分布と同じである場合をいう。独立の概念はシグマ代数の族に一般化できる。独立性がない場合は依存性となる。有限次元における依存性はコピュラで表現できる |
| **Derivatives** | **デリバティブ** | デリバティブは、偶発債権とも呼ばれ、現時点ではその発生が未確定な将来の状況に応じて、将来の資源の交換を指定する契約である。 |
| **Distribution** | **分布** | 分布は、（確率）法則、または確率尺度とも呼ばれ、さまざまな可能性のある事象の発生確率を特定する。 |
| **Extreme value theory** | **極値理論** | 数理統計学の一分野で、確率変数列の極大・極小に関する極限定理を扱う。この分野の結果は、分布の尾部の統計的記述、順位統計のモデル化、高い閾値を超える超過のモデル化などの応用に非常に有用である。 |
| **Feedback effects** | **フィードバック効果** | システムにおけるフィードバックと増幅による現象 |
| **Game theory** | **ゲーム理論** | プレイヤーの戦略的相互作用の数学的理論であり、その共同行動がシステムの進化を決定する。 |
| **GLM** | **GLM** | GLM は一般化線形モデルの略称で、一般化線形回帰のモデルクラスである。 |
| **Heavy tails** | **重いテール** | より正確には、指数モーメントが有限ではない分布である。 |
| **Idiosyncratic risk** | **特異リスク** | 共通の基礎的要因やシステミックなフィードバック効果に左右されず、すべての事業体にわたって独立している個別リスク |
| **Insolvency** | **債務超過** | 義務の履行が不可能になった状態 |
| **Insurance coverage** | **保険** | 契約上指定された条件下で、通常は特定の稀な事象が発生した場合に、補償金を支払う義務または補償金を受け取る権利が生じること。 |

| | | |
|---|---|---|
| **Insurance-linked securities** | **保険リンク証券** | キャッシュ・フローが損失イベントまたは保険金支払いの関数として定義される金融市場商品 |
| **Interaction, local vs. global** | **交流、ローカル対グローバル** | 統計力学では、これを形式化するために静的平衡概念も存在する。 |
| **Knightian uncertainty** | **ナイトの不確実性** | リスクとは対照的に、起こりうるシナリオに具体的な確率を割り当てることはできないが、シナリオごとに異なる確率が考えられる。 |
| **Law of large numbers** | **大数の法則** | 独立同値分布する確率変数の平均値が期待値に収束することを表す。 |
| **Losses** | **損失** | 保険事故における損害の財務仕様 |
| **Loss frequency** | **損失頻度** | 損害発生のタイミングを確率的に記述し、モデル化または測定する。 |
| **Loss severity** | **損害の重大性** | 確率的記述とモデル化、あるいは損失規模の測定 |
| **Model risk** | **モデル・リスク** | 使用したモデルの枠組みや具体的に特定したモデルが適切でないリスク |
| **Monetary risk measures** | **金融リスク対策** | バリュー・アット・リスク、アベレージ・バリュー・アット・リスク、ユーティリティ・ベースのショートフォール・リスク、エクスペクテンタイルズなどがその例であり、ソルベンシー資本要件、パフォーマンス測定、リミット・システムなどに適用できる。 |
| **Monetary protection** | **金銭的保護** | 保険は現実の損害を防ぐことはできないが、金銭的な補償金の支払いを約束し、それによって金銭的な保護を提供することはできる。 |
| **Moral hazard** | **モラルハザード** | 情報が不完全な場合、保険加入後のモニタリングがなければ、リスクに物理的に備えるインセンティブが欠如する可能性がある。 |
| **Pooling of risks** | **リスクのプール** | 小さな確率でしか発生しないリスクの大きな集合体が形成される。個々の損害が大きくなる可能性があっても、リスクごとの保険料は控えめで十分である。 |
| **Portfolio management** | **ポートフォリオ管理** | 利益の最大化、リスクの最小化、有用性の最大化、規制要件の遵守など、定義された目的を達成するために投資ポジションを選択・調整する。 |
| **Premium** | **プレミアム** | 保険契約の価格。リスク・プレミアムとコスト負担金から構成される。 |
| **Premium principles** | **プレミアム原則** | 保険料の計算方法は、期待価値に加えリスク調整額を含むのが一般的である。 |

| | | |
|---|---|---|
| **Pricing** | **価格** | 保険、金融商品、その他の商品の価値を決定する方法 |
| **Risk transfer (financial)** | **リスク移転 (金融)** | 保険および/または金融契約による損失に対する財政的保護 |
| **Regulatory capital** | **規制資本** | 銀行や保険会社は契約上、将来の支払いを約束している。不確実性に直面してもこうした義務を果たすためには、最低限の資金を維持する必要があり、その規模は規制資本によって決定される。 |
| **Reinsurance** | **再保険** | 元受保険者の保険ポートフォリオは、その流通構造と販売市場によって大きく左右される。異なる保険者のポートフォリオを組み合わせることで、リスクを適切にプールすることができる。このサービスは、適切な保険料の支払いと引き換えに再保険者が提供する。 |
| **Reserving** | **予約** | 将来の保険金請求に対応するためには、保険会社は十分な経営資源を有していなければならない。この目的のために、引当金は貸借対照表の負債側に計上されなければならない。引当金の計上プロセスには、適切な保険数理計算が含まれる。 |
| **Robustness** | **堅牢性** | 保険数理における堅牢ネスとは、モデルの不確実性が存在する中で、不利なケースであっても十分 受け入れられる解を導き出す手順を開発することである。堅牢性とは、モデルの不確実性が存在する場合に、不利なケースであっても十分に許容できる解を導く手順を開発することである。 |
| **Resilience** | **レジリエンス** | 構造物や事業体の財産は、危機発生時に損害の範囲を限定し、その機能を迅速に回復させるためのものである。 |
| **Scenario analysis** | **シナリオ分析** | 特定の定義されたシナリオに対するプロセスと影響の分析 |
| **Spread mechanisms** | **普及メカニズム** | ネットワーク化されたシステムにおいて、ローカルまたはグローバルな相互作用プロセス、例えば病気やコンピューターウイルスが伝播するメカニズム |
| **Stationarity** | **定常性** | 確率過程の確率的性質が、対象とする時間窓の特定の位置から独立であること。言い換えれば、確率的メカニズムの本質的性質は、時間が経過しても変化しない。 |
| **Statistics** | **統計** | 現実の多くの場面では、現象を確率論的に記述することが適切である：起こりうる出来事には確率が割り当てられる。しかし、真の確率はわからない。この不確実性は、統計モデルによって表現される。統計モデルは、枠組みとして確率論的メカニズム群を先験的に規定する。統計学は、データから確率への推論を系統的に導くとい |

| | | |
|---|---|---|
| | | う逆問題に取り組む。これは統計的推論と呼ばれる。複数の手法が存在する。 |
| **Stochastic models** | **確率モデル** | 不確実性とは、実際に起こるシナリオについての知識がないことを表す。このような状況に対するモデルは確率論で開発される。より具体的には、シナリオに特定の確率を割り当てるモデルを確率論的モデルと呼ぶ。確率論はその性質を研究し、方法を開発する。一方、統計学は、データから真の確率測度を推論するという逆問題に焦点を当てている。確率論的モデルと統計学的モデルをまとめて確率モデルと呼ぶ。 |
| **Strategic interaction** | **戦略的相互作用** | 結果が多くのアクターの行動によって左右される場合、個々のアクターは、自分の目的を追求する際に他のアクターがとりうる行動について説明し、観察し、そしてしばしば予測を立てなければならない。このような状況は戦略的相互作用と呼ばれる。数学的には、これはゲーム理論で研究されている。 |
| **Structural break** | **構造破壊** | 以前はデータを適切に記述できたモデルのパラメータが突然変更されること。特に統計学のある種のモデル群では、正しい仕様をテストしたり、モデルの枠組みを調整したりするために重要である。 |
| **Surcharge for costs** | **追加費用** | 保険会社には、管理費やインフラ整備費など、リスク保険料とは別に請求しなければならないコストが発生する。 |
| **Systematic risks** | **システマティック・リスク** | 一般的な外生的要因プロセスによって駆動される確率的変動であり、典型的な例は通常の金融市場リスクである。 |
| **Systemic risks** | **システミック・リスク** | システムにおけるフィードバックと相互作用に基づくリスク。システム全体を考慮せずに、個々のポジションを単独で評価することは不可能である。 |
| **Time series** | **時系列** | a) 離散時間のランダムデータ b) 離散時間の確率過程のモデル、通常は標準的な方法が開発されている限定されたモデル族に属する。 |
| **Underwriting** | **アンダーライティング** | アンダーライターとは、保険会社、再保険会社、ブローカーの従業員のことで、顧客に保険ソリューションを提案し、申込書を検討し、リスクを評価し、契約を締結する。このプロセスはアンダーライティングと呼ばれる。 |
| **Validation** | **バリデーション** | 統計モデルの枠組みが適切かどうかをデータに基づいて検証すること。対照的に、キャリブレーションとは、与えられたモデルの枠組みの中でモデルを選択することを指す。 |

# 9.参考文献

Aït-Sahalia, Y., Cacho-Diaz, J., and Laeven, R. J. (2015).相互励起ジャンプ過程を用いた金融伝染のモデル化。Journal of Financial Economics, 117(3), 585-606.

アリアンツ (2022).アリアンツ・リスク・バロメーター。技術担当者。Allianz Global Corporate & Specialty.

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß A., and Weber, S. (2022).サイバー保険のモデリングとプライシング-調査。Working Paper, Leibniz Universität Hannover.

Bundesanstalt für Finanzdienstleistungsaufsicht & Deutsche Bundesbank (2021).リスクモデルにおける機械学習 - 特徴と監督上の優先事項：Consultation paper, available at https://www.bundesbank.de/en/homepage/machine-learning-in-risk-models-characteristicsand-supervisory-priorities-793670.

Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., and Williams, J. (2017).サイバーセキュリティ攻撃における伝染。Journal of Operational Research Society, 68(7):780-791.

Bengio, Y., Courville, A., and Vincent, P. (2013).表現学習：表現学習：レビューと新たな展望。IEEE transactions on pattern analysis and machine intelligence, 35(8), 17981828.

Bessy-Roland, Y., Boumezoued, A., and Hillairet, C. (2021).サイバー保険のための多変量ホークス過程。アクチュアリー科学年報, 15(1), 14-39.

Blier-Wong, C., Cossette, H., Lamontagne, L., and Marceau, E. (2020).損害保険における機械学習：損害保険における機械学習：プライシングとリザービングのためのレビュー。Risks, 9(1), 4.

Böhme, R., and Schwartz, G. (2010).サイバー保険のモデル化：統一的枠組みに向けて。WEIS.

CSIS（2020 年）。サイバー犯罪の隠れたコスト技術報告書。戦略国際問題研究所(CSIS)はマカフィーと提携している。

Dacorogna, M., Debbabi, N., and Kratz, M. (2022).サイバー・レジリエンスを強化する

ヘビーテールデータをモデル化する新しいアルゴリズムによってサイバーリスクを把握する。ESSEC ワーキング

論文 2210。https://arxiv.org/abs/2209.02845

Dacorogna, M., and Kratz, M. (2020).不確実性からリスクへの移行：サイバーリスクの事例。Cybersecurity in Humanities and Social Sciences.A Research Methods Approach".H. Loiseau, D.Ventre, H. Aden 編。WILEY - ISTE.

ダコローニャ、M.、クラッツ、M.（2022）。特集号。「サイバーリスクとセキュリティ」。Risks 10: 112.

https://doi.org/10.3390/ risks10060112.

Daley, D. J., and Vere-Jones, D. (2003).点プロセスの理論入門：

第 1 巻：初歩的な理論と方法。シュプリンガー・ニューヨーク。

Dugas, C., Bengio, Y., Chapados, N., Vincent, P., Denoncourt, G., and Fournier, C. (2003).

統計的学習アルゴリズムを自動車保険料率決定に応用する。CAS フォーラム（Vol.

1, No.1、179-214 頁）。アーリントン：アーリントン：Casualty Actuarial Society.

Edwards B., Hofmeyr S., and Forrest S. (2016).Hype and heavy tails: a closer look at data breaches.J Cybersecur 2(1):3-14.

Eling M., and Loperfido N. (2017).データ侵害：適合度、プライシング、リスク測定。Insur Math Econ 75:126-136.

Eling M., and Jung K. (2018).データ漏洩損失の横断的依存性をモデル化するためのコピュラ・アプローチ。Insur Math Econ 82:167-180.

Eling M., Schnell W., and Sommerrock F. (2016).サイバーリスクとサイバーリスク保険に関する 10 の重要な質問。ジュネーブ協会。

Eling M., and Wirfs J.H. (2019).サイバーリスクイベントの実際のコストはどの程度か？Eur J Oper Res 272(3):1109-1119.

Embrechts, P., Klüppelberg, C., and Mikosch, T. (2013).極端事象のモデル化：保険と金融のために（第 33 巻）。Springer Science & Business Media.

Embrechts, P., Liniger, T., and Lin, L. (2011).多変量ホークス過程：金融データへの応用。応用確率学会誌, 48(A), 367-378.

ENISA（2023 年）。EU におけるサイバー保険の需要サイド.ISBN 978-92-9204-586-9, doi：

10.2824/94949, カタログ番号 TP-04-22-095-EN-N

Errais, E., Giesecke, K., and Goldberg, L. R. (2010).アフィン点過程とポートフォリオの信用リスク。SIAM Journal on Financial Mathematics, 1(1), 642-665.

Fahrenwaldt, M., Weber, S., and Weske, K. (2018).ネットワークモデルにおけるサイバー保険契約のプライシング。ASTIN Bulletin, 48(3):1175-1218.

Farkas, S., Lopez, O., and Thomas, M. (2021).一般化されたパレート回帰木によるサイバークレーム分析と保険プライシングおよびリザーブへの応用。保険：

数学と経済 98: 92-105.

Föllmer, H., and Schied, A. (2002).リスクと取引制約の凸尺度。Finance and stochastics, 6(4), 429-447.

Föllmer, H., and Schied, A. (2016).確率論的金融。

Giesecke, K. (2008).ポートフォリオの信用リスク：トップダウン・アプローチとボトムアップ・アプローチ。In：Frontiers in Quantitative Finance：Volatility and Credit Risk Modelling.R. Cont.Wiley.第 10 章。

Hejazi, S. A., and Jackson, K. R. (2017).ニューラルネットワークアプローチによる SCR の効率的な評価。Journal of Computational and Applied Mathematics, 313, 427-439.

Hillairet, C., and Lopez, O. (2021).保険ポートフォリオにおけるサイバーインシデントの伝播：コンパートメント疫学モデルと組み合わせた計数過程。In：Scandinavian Actuarial Journal, pp.

Hillairet, C., Lopez, O., d'Oultremont, L. and Spoorenberg, B. (2021).サイバー伝染：ネットワーク構造が保険ポートフォリオの損失に与える影響。Hal-03388840.

ジェイコブス・J. (2014).ポネモンのデータ漏洩コストを分析する。

Kermack, W. O., and McKendrick, A. G. (1927).伝染病の数学的理論への貢献。(1927)：伝染病の数学的理論への貢献。シリーズ A, 数学的・物理学的性格の論文を含む, 115(772), 700-721.

Knispel, T., Stahl, G., and Weber, S. (2011).等価原理から市場整合的評価へ。Jahresbericht der Deutschen Mathematiker-Vereinigung, 113(3), 139-172.

De Leeuw, J., Vrieling, A., Shee, A., Atzberger, C., Hadgu, K. M., Biradar, C. M., ... and Turvey, C. (2014).保険におけるリモートセンシングの可能性と導入：A review.リモートセンシング, 6(11), 10888-10912.

Maillart, T., and Sornette, D. (2010).サイバーリスクの重税分布。The European Physical Journal B, 75(3), 357-364.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017).サイバー保険調査。In：Computer Science Review.

McNeil, A. J., Frey, R., and Embrechts, P. (2015).Quantitative Risk Management: concepts, techniques and tools-revised edition.プリンストン大学出版局。

Óskarsdóttir, M., Ahmed, W., Antonio, K., Baesens, B., Dendievel, R., Donas, T., and Reynkens, T. (2021).保険における監視された詐欺検出のためのソーシャルネットワーク分析。リスク分析。

Peng, C., Xu, M., Xu, S., and Hu, T. (2018).多変量サイバーセキュリティリスクのモデル化。Journal of Applied Statistics, 45(15):2718-2740.

Reinhart, J. (2021).サイバー保険-まだ子供か、それとも大人か？DGVFM Weiterbildungstag にて講演。

Richman, R. (2018).AI in actuarial science.SSRN 3218082 で入手可能。

Riek, M., and Böhme, R. (2018).消費者向けサイバー犯罪のコスト：測定の問題点と推定値の実証的探求。Journal of Cybersecurity, 4(1).

ロマノスキー S. (2016).サイバー事件のコストと原因を検証する。J Cybersecur 2(2):121-135.

Ponemon Institute LLC (2016).データ漏えいのコスト調査：グローバル分析。

Shalev-Shwartz, S., and Ben-David, S. (2014).機械学習を理解する：理論からアルゴリズムまで。ケンブリッジ大学出版局。

Trevor, H., Robert, T., and Jerome, F. (2009).統計的学習の要素：データマイニング、推論、予測。

Wüthrich, M. V. (2018).個人保険金支払い予約における機械学習。Scandinavian Actuarial Journal, 2018(6), 465-480.

Wüthrich, M. V., Bühlmann, H., and Furrer, H. (2010).市場整合的保険数理評価（第 2 巻）.ベルリン：Springer.

Xu, M., and Hua, L. (2019).サイバーセキュリティ保険：モデリングとプライシング。North American Actuarial Journal, 23(2):220-249.

de Zea Bermudez, P., and Kotz, S. (2010a).一般化パレート分布のパラメータ推定-パート I. Journal of Statistical Planning and Inference, 140(6), 1353-1373.

de Zea Bermudez, P., and Kotz, S. (2010b).一般化パレート分布のパラメータ推定-パート II.統計計画と推論, 140(6), 1374-1388.

Zeller, G. and M. Scherer (2022).マークされた点プロセスに基づくサイバーリスクの包括的モデルとその保険への応用。European Actuarial Journal, 12, 33-85.

TP-04-23-347-EN-N

## ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

**ENISA**
European Union Agency for Cybersecurity

**Athens Office**
Agamemnonos 14
Chalandri 15231, Attiki, Greece

**Heraklion Office**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

**Brussels Office**
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-628-6
doi: 10.2824/773850