保険・年金フォーカス

サイバーリスクの変容と保険対応

サイバー保険はランサムウェアの進化にどう対応してきたか?

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

近年、サイバーリスクが増大している。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。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。他にも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、多様なサイバー攻撃にさらされている。

ここ数年、特に深刻化しているのが企業等へのランサムウェアによる攻撃だ。攻撃者は、まず、ウイルス感染により、端末の一部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する。そして、それらを使用可能とするための、身代金を要求する。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。

損保会社は、サイバー保険の開発や引き受けを通じて、ランサムウェアによる攻撃を含めて、サイバーリスクへの補償を行っている。米国のアクチュアリー会は、サイバー保険を通じたこのリスクへの対応について継続的に議論を行っている。日本でも、ランサムウェアによる被害事案が増加しており、対策が求められる。本稿では、その議論や対策など、サイバーリスクの動向を見ることとしたい。

2――日本でのサイバーリスクの顕在化

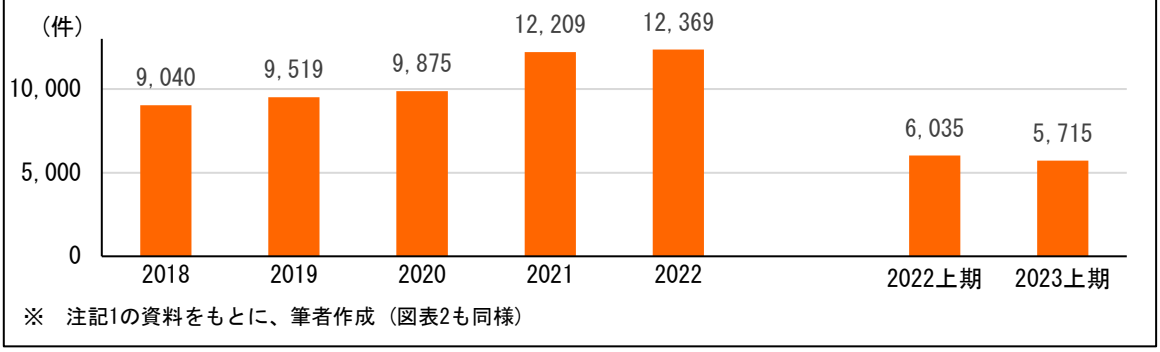
まず、日本で、警察庁が今年公表したサイバー事案に関する資料[1]から見ていく。

1｜被害業種は製造業とサービス業で過半を占め、規模では中小企業に多い

2022年に検挙されたサイバー犯罪の件数は、12,369件で、前年よりも160件増加した。2023年上期は5,715件で、前年同期に比べてやや減少した。しかし、長期的な観点からは、増加傾向が続いており、サイバー犯罪の拡大が見てとれる。注意したいのは、この件数には、検挙に至っていないケースは含まれていない点だ。ここにあらわれている件数は、氷山の一角、という可能性もある。

[1] 「令和4年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁，令和5年3月16日）および「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁，令和5年9月21日）

図表1. サイバー犯罪の検挙件数[推移]

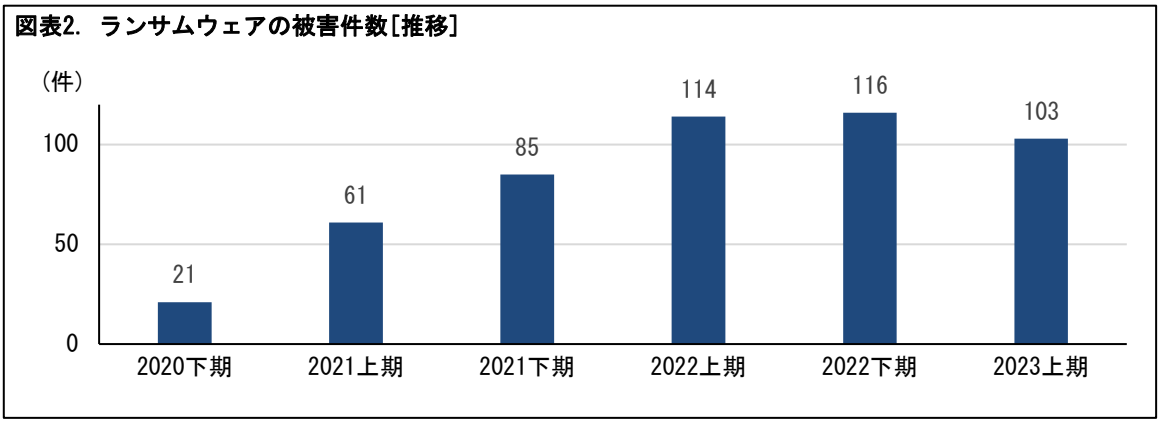


※ 注記1の資料をもとに、筆者作成（図表2も同様）

2｜ランサムウェアの被害件数は急増

つづいて、ランサムウェアによる被害を見てみる。警察庁への報告件数は、2022 年に 230 件、2023 年上期に 103 件で、近年、急増している。特徴として、身代金の要求と、保存データ公開の脅迫という二重恐喝(ダブルエクストーション)による被害が多くを占めること(2022 年に手口が確認できた 182 件のうち 119 件(65%))。暗号資産による対価の要求が多くを占めること(2022 年に直接的な対価の要求が確認できた 54 件のうち 50 件(93%))の 2 点が挙げられている。

図表2. ランサムウェアの被害件数[推移]



3――サイバーリスクの分類

次に、アメリカのアクチュアリー会(SOA)でのサイバーリスク管理に関する議論の様子を、同会の研究所のペーパー(以下「ペーパー」と呼称)[2]をもとに見ていく。アメリカでも、サイバーリスクが高まっており、サイバー保険の開発やその価格設定を含めて、リスク管理の議論が続いている。

1｜一般社会と保険業界では、「壊滅的なサイバーリスク」の定義がやや異なっている

一般に、サイバー攻撃には、時間の経過とともに被害が拡大していくものが多い。特に、ランサムウェアのようなマルウェアへの感染を伴う攻撃では、感染したネットワーク内で被害が拡大していくケースがよく見られる。ペーパーでは、危機的なリスクを管理するうえで、被害が極大となる「壊滅的なサイバーリスク」とはどういう状態か、についての議論が示されている。

[2] “Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion” (SOA Research Institute, Jan. 2023)

(1) 一般社会にとっての「壊滅的なサイバーリスク」

一般社会にとっての壊滅的なサイバーリスクには、様々な定義が考えられる。例えば、経済的影響、ネットワーク効果、深刻度の3つの尺度で判断するという考え方がある。ここで、経済的影響は、ネットワークやデータが利用できないことによるビジネス上の損失。サイバー問題の理解、制御等に必要となる労働力の急増に伴う支出増加。売上の減少をもたらす、ビジネスまたは評判への影響。供給側と需要側の連鎖的な影響の合計とされている。また、ネットワーク効果は、ソフトウェアの大規模再利用、オペレーティングシステムの標準化、ネットワーク構成の類似性であり、ビジネスや業界全体の高レベルの接続性と組み合わされて捉えられる。深刻度は、文字通り、発生する事象の深刻さの度合いだ。これらの尺度のどのレベルより上を「壊滅的」とするかについては、議論が分かれる。

この他に、攻撃対象による定義もある。攻撃の主な対象が単一の組織ではなく、ネットワークを介して伝播し、他の企業に影響を与える攻撃であれば、壊滅的なサイバーリスクとするというものだ。これも、人によって細部の見方が異なるため、定義は一様ではない。ただ、多くの人に共通する定義として、エネルギー、交通、医療などの社会の重要インフラへの大規模な攻撃が行われれば、壊滅的なサイバーリスクとみなされるとしている。

(2) 保険業界にとっての「壊滅的なサイバーリスク」

保険業界にとっての壊滅的なサイバーリスクは上記のものとやや異なる。一般に、保険会社にとっては、保険金支払いの件数や金額の増加につながるシステムの脆弱性が、壊滅的なサイバーリスクと捉えられる。ただし、その具体的な測定方法については議論が定まっていない。

特に、サイレントサイバーリスクについては、保険業界独自のリスクとして注目されている。サイバーリスク保険以外の一般の保険契約(自動車保険、火災保険など)では、契約規定のなかにサイバーリスクが明示的に含まれていない場合や、明確に免責とされていない場合がある。こうした場合、サイバー事件による損害保険の補償(損害賠償補償など)の範囲があいまいになる。保険会社側からみると、補償を提供する意図がなかった保険契約からも、サイバー攻撃によって、保険金請求が発生する恐れがある。これが、(サイバー保険以外の)従来の損害保険に潜在する、サイレントサイバーリスクとなる。[3]

2｜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

サイバーリスクのモデリングに関するペーパー(以下「モデリングペーパー」と呼称)[4]によると、ひとくちにサイバーリスクといっても、被害の内容や規模に応じて、次表の通り、3つのタイプ(特異的、システマティック、システミック)に分類されるという。壊滅的なサイバーリスクは、システミックタイプのリスクが極大化したものと見ることができるだろう。

ランサムウェアによる攻撃のリスクも、これをもとに分類することができる。

---

[3] 詳しくは、「サイレントサイバーリスクの増大ーサイバーリスクの引き受けは、サイバー保険にとどまらない!?」篠原拓也(保険・年金フォーカス, ニッセイ基礎研究所, 2022年10月11日)をご参照いただきたい。

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

図表 3. サイバーリスクの分類

	特異的		システマティック		システミック	
	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―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によりデータベースが侵害	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
※ 注記 4 のペーパーをもとに、筆者作成

3｜ランサムウェア攻撃の進化により、保険業界の変化が促された

近年、サイバーリスクの高まりを受けて、アメリカでは、サイバー保険の補償内容の見直しや料率の引上げが行われている。これは特に、ランサムウェアの進化に対応する意味合いが強いとされる。ランサムウェアの進化に伴って、保険業界が変化した点として、次のものが挙げられている。

・保険会社は、これまで以上に多額のサイバー保険金支払いを行っている。
・保険会社の多くは、引き受け時に保険の適格性を見るために、長期のサイバーリスク評価を実施している。
・サイバー保険の引き受けの焦点は、サードパーティの責任の評価から、事象が発生した被保険者の被害対応費用の評価に移行した。
・保険会社は、様々な安全策(多要素認証、オフラインでのバックアップ、特権管理者のアクセス、特権の昇格付与等)と、多くのサイバーリスク技術管理を要求することにより、引受ガイドラインを見直すことで対応した。
・ビジネスメール詐欺が出現していることで、ランサムウェアに関する議論がさらに進んでいる。ただし、被害者が形式上「進んで」金銭を提供してしまった事象は保険の支払い対象とはなっていなかった。ソーシャルエンジニアリング詐欺(情報通信技術を使用せずに、電話で聞き出す、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方法で、パスワードなどを盗み出す方法)の保障も、ビジネスメール詐欺の出現後に、始まっている。

4――サイバーリスクに関する知識ギャップ

サイバーリスクは、保険を提供するために必要な情報がまだ不十分と見られている。保険事業を通じて経験データを蓄積したり、リスク管理やセキュリティに関する経済学等の関連分野の研究から補強したりすることにより、知見を高めていくことが必要とされる。モデリングペーパーでは、サイバー保険のモデリングに関する先行文献にもとづいて、知識ギャップを、次ページ表のように列挙している。サイバーリスクに関しては、まだ数多くの研究課題が残されていることがうかがえる。

図表 4. サイバーリスクに関する知識ギャップ

（サイバー保険の設計、価格設定）

・サイバーリスクとコストを評価するために最も有用な指標は何か。
・保険数理部門は、サイバー保険の管理と価格設定のために広く受け入れられているデータにどのように到達できるか。
・企業は、保険に加入したり、保険料を安くしたりするために、どのような情報を保険会社に提供する意思があるか。
・サイバーリスク保険はどのように規制されるのか。サイバーリスクには新たな規制モデルが必要なのか。どうすれば、保険契約者が望むような少ない制限や除外のもとで、保険契約におけるリスクを減らし、完全な保障を提供できるのか。
・認可保険会社と非認可保険会社（エクセス＆サープラス（認可保険会社では引き受けが難しく、高度な専門性が必要なリスクを、規制が緩やかな監督の下で引き受ける会社））のモデルの違いは何か。
・保険会社はどうすればサイバーリスクをオペレーショナル・リスクと見なし、引き受けに結びつけることができるか。
・壊滅的なサイバーリスク事象が、サイバー保険市場に与える影響はどのようなものか。
・利用可能なサードパーティのリスク評価の信頼性はどの程度か。
・サイバーリスクの再保険の課題は何か。
・伝統的なサイバー再保険の資本市場代替案（すなわち、CAT 債、パラメトリック保険、カタストロフィック・リスク・エクスチェンジ、保険リンク証券）は存在するか。もし存在するのであれば、これらの代替案をサイバーリスク移転にどのように利用できるのか。
・サイバー保険は収益性の高いビジネスなのか。
・異なる価格戦略は、サイバーセキュリティ市場の発展にどのような影響を与えるのか。
・サイバーリスクを評価するために、ベイズ確率を使用してリスクスコアをどのように開発できるのか。

（サイバーデータ）

・公的または民間の情報共有基盤は、サイバーリスクデータの可用性と品質を支援するために、どのように設計されるのか。
・サイバーデータの欠如に対処するための代替手段として、シナリオをどのように利用することができるか。
・測定データの収集と分析の方法を改善して、測定コストを削減し、信頼性を高めるにはどうすればよいか。
・変化のリスクは、サイバーリスクデータにどのような影響を与えるか。行動経済学は、攻撃の動機を判断するのに役立つだろうか。
・内外の環境の変化を考慮して、サイバーデータの収集をどのように改善することができるだろうか。サイバー関連の強靭性の構築に向けて、どのようにサイバーリスクを効果的に管理することができるだろうか。

（サイバーリスク管理）

・サイバー保険は組織のセキュリティにプラスとマイナスの両面でどのような影響を与えるのか。
・組織はどのようにサイバー保険の購入（または非購入）を決定するのか。
・企業は、単にサイバー保険だけに頼るのではなく、より安い保険料を得るためにセキュリティの改善を実施するのか。保険会社はモラルハザードを減らすためにどのように行動できるのか。
・技術的なデータソリューションだけでなく、社会経済的なリスク要因、プロセス、サイバーセキュリティの人々に対する理解を深めるために、サイバーセキュリティの提供とデータをどのように拡大できるのか。
・全体的なサイバー意思決定アプローチとコーポレート・ガバナンスのために、サイバーリスクとそれに対応する意思決定を上層部間でどのように推進できるのか。
・サイバーリスクの用語とフレームワークの違いは何か。これらの違いをよりよく理解することは、サイバーリスク管理にどのように役立つのか。
・極端なサイバーリスクに対して、リスク移転はどのように機能するのか。
・サイバー保険や引受において、システミックなサイバーリスクまたは壊滅的なサイバーリスクを説明するために、グローバルな対話をどのように構築することができるのか。
・サイバーセキュリティ侵害の可能性を決める要因として他に何があるのか。
・サイバー攻撃は企業価値以外のビジネス運営にどのような影響を与えるか。
・回復戦略の策定に関する保障と効率性のトレードオフは、サイバー脆弱性をどのように防ぐのか。
・サイバー攻撃は米国外の地理的地域にどのような影響を与えるか。他の地域でサイバーリスク分析を行うことで、文化の違いや法的起源が市場参加者のサイバー攻撃への対応に及ぼす潜在的な影響をどのように浮き彫りにできるか。
・サイバーリスクと他の種類のリスク（例：地政学的リスク、世界的な健康危機）の間に相関関係は存在するか。
・学際的な研究を実施することは、サイバーリスク管理とサイバー保険の実務を理解するのに役立つか。
・回復力を促進するために、サイバーリスクと移転戦略をどのように開発し、実施することができるか。サイバー関連の強靭な管理フレームワークを作成することは、組織や政府がサイバー環境の変化に適応するのにどのように役立つか。

※ 図表４は、注記４のペーパーと以下の文献をもとに、筆者作成
“Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective” Tøndel, I.A., Seehusen, F., Gjære, E.A., Moe, M.E.G. (2016). In: Buccafurri, F., Holzinger, A., Kieseberg, P., Tjoa, A., Weippl, E. (eds) (Availability, Reliability, and Security in Information Systems. CD-ARES 2016. Lecture Notes in Computer Science, vol 9817. Springer, Cham.)
“Cyber risk management: History and future research directions” Eling, M., McShane, M., & Nguyen, T. (Risk Management & Insurance Review, 24(1), 93-125., Mar. 2021)

5――おわりに（私見）

本稿では、サイバーリスクの変容の動向を、ランサムウェアを中心に紹介した。そして、それに合わせて、保険がどのように対応しようとしているのか、議論や対策を見ていった。

第３章までのとおり、ランサムウェアの二重恐喝や、二重、三重の被害など、サイバーリスクの被害の深刻化は進んでいる。システミックサイバーリスクや、壊滅的なサイバーリスクといった広範囲に渡るリスク発現の恐れも高まっている。

サイバー保険を含めて、これらのリスクを管理するためのフレームワークづくりが急務であると言えるだろう。今後も、サイバーリスクに関する保険業界の動向をウォッチしていくこととしたい。

（参考文献）

「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁，令和５年３月 16 日）

“Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion”（SOA Research Institute, Jan. 2023）

「サイレントサイバーリスクの増大－サイバーリスクの引き受けは、サイバー保険にとどまらない!?」篠原拓也（保険・年金フォーカス，ニッセイ基礎研究所，2022 年 10 月 11 日）

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

“Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective” Tøndel, I.A., Seehusen, F., Gjære, E.A., Moe, M.E.G. (2016). In: Buccafurri, F., Holzinger, A., Kieseberg, P., Tjoa, A., Weippl, E. (eds) (Availability, Reliability, and Security in Information Systems. CD-ARES 2016. Lecture Notes in Computer Science, vol 9817. Springer, Cham.)
https://doi.org/10.1007/978-3-319-45507-5_12

“Cyber risk management: History and future research directions” Eling, M., McShane, M., & Nguyen, T. (Risk Management & Insurance Review, 24(1), 93-125., Mar. 2021)
https://doi.org/10.1111/rmir.12169

