基礎研レター

サイバーリスクへの保険会社の対応（欧州）

EIOPA のレポートの公表

保険研究部 主任研究員　安井　義浩
(03)3512-1833　yyasui@nli-research.co.jp

1――ストレステスト 4 つめの方法論

2023 年 7 月 11 日、欧州保険・企業年金監督機構（EIOPA）は、サイバーリスクの保険ストレステストの原則的な方法論について報告書[1]を公表した。これまでに「保険のストレステスト一般の方法論（2020.3）」「流動性ショックへの対応（2021.1）」「気候変動リスクへの対応（2022.1）」の 3 つが公表されているが、今回の「サイバーリスクへの対応」は 4 つめである。

この報告書をもとに、保険会社のサイバーリスクの特徴などを要約する形で紹介する。

2――保険会社に対するサイバー攻撃の特徴

1｜サイバー攻撃に至る動機

・金銭を得る目的

不正行為、詐欺行為、機密データの販売、会社の評判やシステム環境を背景とした脅迫

・スパイ活動

機密データへの侵入、将来の破壊活動に使えるような情報の入手

・妨害工作

機密データの削除や変更、極端な場合はその産業全体に及ぶ影響もありうる。一般に保険会社のような金融機関は、サイバー攻撃の「よい目標」である。保険会社は多くの取引記録、顧客データ等を保有しており、その中には個人の健康などのセンシティブ情報も含まれている。悪意ある攻撃者にとってはいい「カネヅル」である。

2｜加害者は誰か？

---

[1] Methodological Principles of Insurance Stress Testing　（EIOPA 2023.7.11）
https://www.eiopa.europa.eu/system/files/2023-07/Methodological%20principles%20of%20insurance%20stress%20testing%20-%20Cyber%20component.pdf
（報告書の翻訳や内容の説明は、筆者の解釈や理解に基づいている。）

そうした悪意を持つ攻撃者は誰かというと、以下のような者が考えられる。

・犯罪組織

通常は金銭目的であり、サイバー攻撃の大部分の目的はこれであろう。この種の組織は今や国際化し、技術的能力も専門分野ごとに分業化するなど、高度化してきている。

・国家

諜報機関によるスパイ活動やサイバー攻撃に注力する国家もありうる。

・ハッカー

特定のイデオロギーに基づいて組織を破壊しようとする者もあるが、そうした目的であれば、保険会社を標的にすることは少ない。

・内部関係者

これについては、金銭的な要求、何らかの復讐のための妨害工作、など様々な動機がありうる。内部関係者は既になんらかのアクセス特権を持っている者が多く、通常はこうした者によるダメージは大きい傾向がある。

3｜サイバー攻撃にはどんな種類があるか

これについては、欧州ネットワーク・情報セキュリティ機関（European Union Agency for Cybersecurity :ENISA）の年次報告書（ENISA Threat Landscape 2021）に従って、以下のようなものが想定されている。

・ランサムウェア

ファイルを暗号化することで利用不可能とし、もとに戻すことと引き換えに金銭を要求する。

・マルウェア

プログラムの改ざん、問題ない文書のふりをして内部に侵入し、個人情報等を収集する。

・クリプトジャッキング

標的のパソコンを使用して、仮想通貨による不正なマイニング（取引、採掘とも呼ばれる）を行う。データの損傷・被害はないが、大きな電力の使用、メモリや CPU などに多大な負荷をかけることになる。

・電子メール関連の脅威

・データ侵害

・可用性と統合性に反する脅威（Denial of Services : DoS）

大量のデータを送り付けること等により、正常な業務運営を妨害すること

・ディスインフォメーション

ニセ情報の流布により判断を誤らせること

・悪意のない脅威

ヒューマンエラーやシステム設定のミスを誘発すること

・サプライチェーン攻撃

4｜サイバー攻撃により、どんな影響があるか

・直接的な経済的損失

IT 機器の損傷、盗難。身代金の支払いなど

・可用性の喪失による経済的損失

事業の損失　労働時間の損失　システムが利用できなくなることによる損失

・復旧作業の手間・コスト

追加の労働時間　対処するための外部サポートの取り入れ

・法的な影響

顧客データ流出等、管理責任を問われることによる罰金など

・風評リスクの現実化

3――保険を引受けていることによる、隠れたサイバーリスク

無理もないことではあるが、保険会社は、従来、例えば「サイバー攻撃による損害の場合には保険金支払いを行わない」などの除外条件を設定していなかった。従ってサイバー攻撃の場合でも、保険金支払を行わざるを得ず、そうした保険金支払いが増加することで損失が増加するケースが多いとされる。これを通常の明示的な(原文では affirmative)サイバーリスクと区別して、サイレント(silent)サイバーリスクと呼んでいる。

サイバー攻撃による損失のなかでは、現時点ではむしろこちらの方の規模が大きく、サイバーリスクによる損失全体の 8 割を占めているという調査結果もある。

これらは非常に幅広い事象であるので、すべての保険に当てはまるが、代表的には以下のような保険種目において、影響が大きいとされる。

・損害賠償保険、火災・不動産保険、事業中断保険、信用保険

・誘拐と身代金のための保険

・海上・航空・運輸保険

・自動車保険のうち第三者損害賠償

・労災補償

・生命保険における医療保険や死亡保険の支払い

4――ストレステストに用いるシナリオの選択

さて、サイバー攻撃そのものの特徴を挙げてきたが、このあと EIOPA においては、ストレステストの一つとして、何らかのサイバー攻撃を仮定して、どのような損失が発生するかのシミュレーションを行い、それに基づいて、どのような防御策や対応策があるかを、保険監督者や各保険会社があらかじめ把握するようにしていく方針である。

具体的なシナリオを描くことは難しいが、例えば、クラウドの停止、ランサムウェア、サービス妨害、データ侵害、停電などを想定した具体的なストレステストにより、脆弱性や対応の方向性を検討しようとしている。引き続き、検討状況をみていきたい。