研究要旨

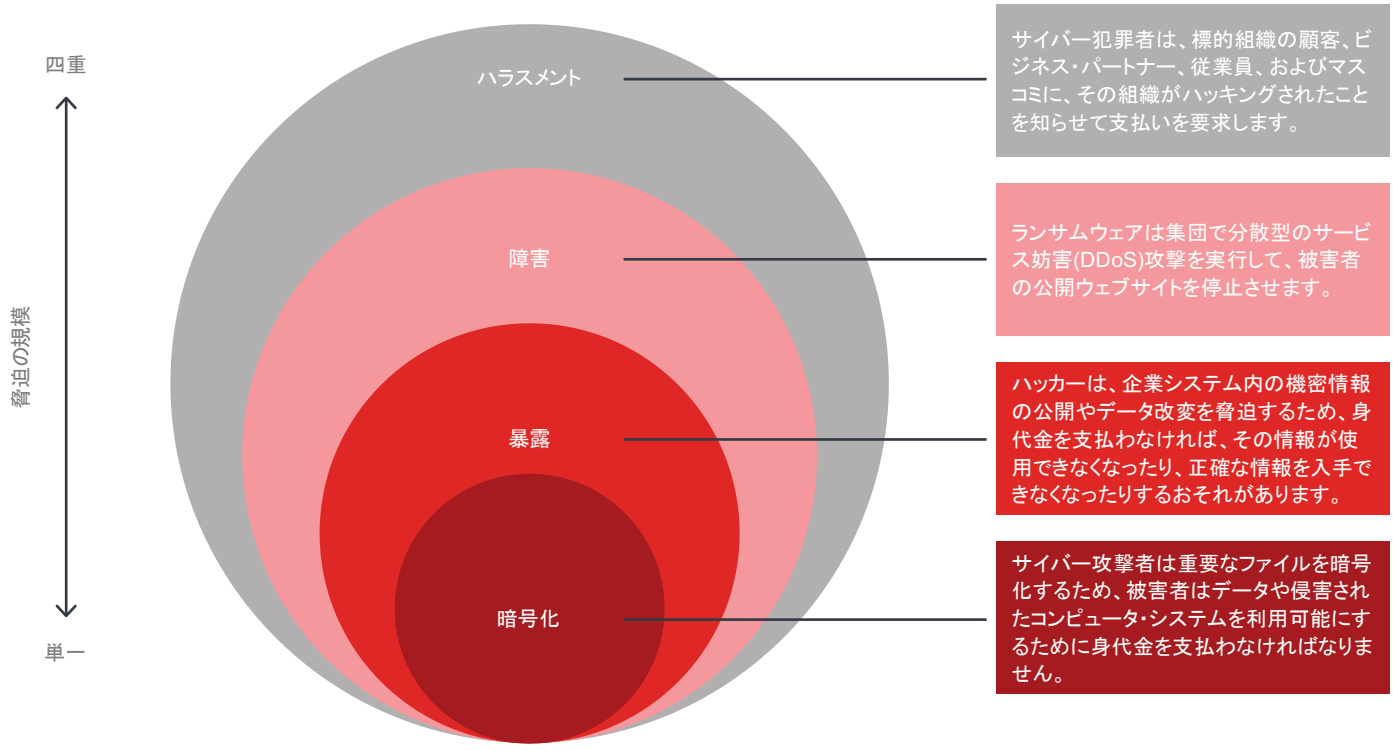
ランサムウェア:保険市場の観点

THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

ジュネーブ協会 Cyber & Evolving Liabilityディレクター、**Darren Pain**
ジュネーブ協会 Public Policy & Regulationディレクター、**Dennis Noordhoek**

ランサムウェア - ファイルやシステムへアクセスし、被害者が解読キーと引き換えに身代金を支払うまでユーザーのアクセスをブロックする悪意のあるソフトウェアの一種 - やその他関連するサイバー空間での脅迫が、最近深刻な問題となっています。企てられた侵入や成功した攻撃の数、および身代金要求の金額は、近年急激に増加する傾向にあります。またサイバー犯罪者は、被害者を脅迫するために巧妙な手法を展開しています。ランサムウェアの攻撃者は、単にデータやファイルを暗号化して身代金を要求するだけでなく、さらなる脅迫手法を採用する傾向が強まっています。これらには、身代金を支払わないと機密情報の公開をすると脅迫したり、企業のウェブサイトを停止させたりすることなどが含まれます(図1)。

図1:ランサムウェア犯罪者のさまざまな脅迫方法



出典:ジュネーブ協会

ハッカーが既製のランサムウェア・ツールやサービスを利用できるようにする、サービスとしてのランサムウェア(RaaS)というビジネスモデルの発展は、この種のサイバー犯罪に大きな影響を与え、技術的なITスキルが限られていても、攻撃者が高度な破壊的攻撃を仕掛けることを可能にしています。RaaSエコシステムが出現し、サイバー犯罪者が専門的な役割を担うようになったことで、そのほとんどの役割は実際の攻撃とは何の関わりもないかもしれません。これらには、未知の脆弱性の特定、初期侵入、マルウェア開発、支払われた身代金の処理、さらには交渉の役割などが含まれます。

保険分野への影響

サイバーリスクを明示的に担保する保険契約は、通常、サイバー攻撃に関連する外部費用(例:フォレンジック調査、データやシステムの復元、および危機管理費用)、事業中断費用、攻撃の影響を受けた第三者への負債、および支払われた身代金を補償します。ランサムウェアは、過去2年間にサイバー保険会社の引受実績が著しく悪化した重要な要因となっています。米国のサイバー保険の損害率は、全体で2019年の44.6%から2020年には66.9%に上昇しており、信用格付け機関であるAM Best社によると、保険金請求の4分の3をランサムウェアが占めています。[1]

最近の指標においても、ランサムウェアが依然として主な要因であり、保険金請求の状況に大きな改善は見られないことが示されています。保険金請求が継続的に増加していることから、昨年はサイバー保険料が大幅に上昇したにもかかわらず、2021年もサイバー保険会社の損害率は高い結果となりました。

進行中の政策論争

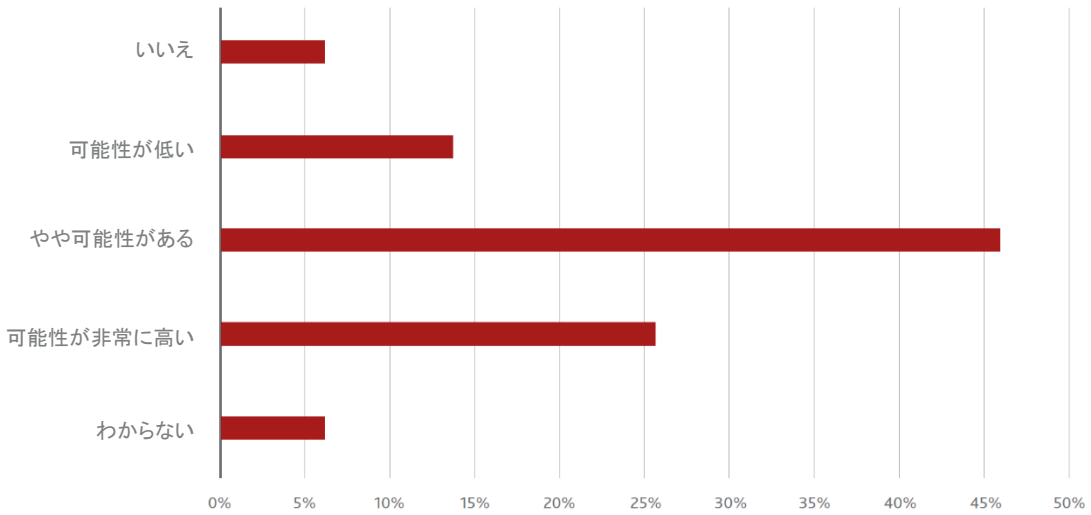
企業は身代金を支払うことでランサムウェア犯罪者に動機を与える可能性もあり、それにより、その企業や他社に対する攻撃リスクが増大します。ランサムウェア攻撃の被害者が保険に加入しているかどうかにかかわらず、このような経済的外部性は存在しますが、一部の外部評論家は、保険加入により標的型ランサムウェア攻撃が助長され状況を悪化させる可能性があるという懸念を表明しています。たとえば、2021年に実施されたある調査によると、調査対象となった英国のITセキュリティ専門家の70%が、ランサムウェアの身代金要求に応じた企業への保険金支払いが問題を悪化させ、攻撃が増えると考えています。[2]政府も、身代金要求額がサイバー保険の保険金額に合わせて要求されていることがよくあることを強調し、保険が意図せずにランサムウェアによる脅迫に影響を与えていることを示唆しています。

このことは、身代金に関連する経済的外部性を緩和するために、政府がどこまで介入すべきかについての政策論争を再燃させました。つまり、身代金を支払うことがランサムウェアをさらに助長し、将来の脅迫要求を増大させる可能性があることを、法律、規制、および税金を用いて被害企業に認識させるということです。

身代金の支払いを全面的に禁止することについて、多くの国で政策協議が行われています。その理由は、身代金の支払いまたは身代金を保険金でのてん補を禁止した場合、ランサムウェアの被害者がサイバー犯罪者に支払う可能性は低くなるからです。また、ランサムウェアの標的企業が支払いをしなかったり、支払い金額を減額しようとしたりすると(潜在的な資金源としての保険金がないため)、身代金を要求するハッカーの動機も低下します。[3]

図2:身代金支払い禁止に関する保険会社および再保険会社の見解

(企業や保険会社による) 身代金支払いを違法とすることで、ランサムウェア攻撃を阻止できますか。[(a)]



(a) 世界のサイバー保険市場で事業を行う15の保険会社および再保険会社のサンプルに基づく

出典:ジュネーブ協会

1 AM Best 2021.
2 Talion 2021.
3 Logue and Shniderman 2021.

真の解決策とならない身代金支払いの禁止

実際には、ランサムウェアに対する簡単な解決策はありません。意図しない結果が生じる可能性もあり、対策には重大なトレードオフが伴うこともよくあります。

たとえば、身代金の支払いを完全に禁止すると、そのような取引が見えないところで行われたり、あるいはランサムウェアの攻撃者が、要求が満たされない場合に資産を破壊したり人身傷害を引き起こしたりするなど、新たな形の脅迫を助長する可能性があります。

ジュネーブ協会がサイバー保険会社や再保険業者を対象に実施した調査によると、身代金支払いの禁止や関連する保険金支払いの禁止は、ランサムウェア攻撃をいくらか抑制する可能性が高いとほとんどの人が感じていますが(図2)、国際的に一貫して禁止しない限り、そのような単刀直入な政策は常に望ましい効果をもたらすとは限らないことが明らかになりました。保険会社の支払いのみを禁止することは特に効果がなく、他の形でリスクファイナンスを構築することが難しい場合は、被害者から重要な保護手段を奪うことになります。身代金支払いを補償するサイバー保険なしでは、被保険者に不利益を与えるだけでなく、ランサムウェア攻撃を助長してきたRaaSの成長に対処することにもなりません。

1990年代にイタリアで起きた誘拐事件の経験は、身代金禁止の課題を浮き彫りにしています。イタリア政府が1991年に身代金の支払いを違法としたことは、その後の誘拐率の平坦化に大きく貢献したと考えられています。しかし、誘拐されたイタリア市民の家族が単に当局への犯罪報告をやめただけで、この脅威が完全になくなったわけではありません。ランサムウェアの身代金支払いが禁止された場合、被害企業は攻撃を隠蔽し、発覚を避けるために非公式の方法で身代金支払いをする可能性があります。これは、新しいランサムウェアの傾向を捉えることが難しくなるということです。

解決策の一環としてのサイバー保険

身代金の支払額が注目を集めがちですが、ランサムウェア攻撃による被害総額は、脅迫による要求額をはるかに超えます。保険は、ランサムウェアによって多様な第一次および第三次被害に直面する企業を支援する重要な役割を果たします。サイバー保険は、攻撃を受けたあとに、弁護士やコンピュータ・フォレンジック・アナリストなど適切な専門家チームを招集して事案を評価し、タイムリーな対応を助言する仕組みです。これらの専門家は、暗号化解除キーの実行や復元作業が可能かなど脅迫の信用性を評価できる立場であるため、大抵の場合、実際に支払う身代金額の引き下げなど貴重な交渉に役立ちます。

表1:ランサムウェアに対する政策に関わる保険会社および再保険会社の提案

目的	政策提言
抑止	• ランサムウェア攻撃を行うサイバー犯罪者に対する罰則の強化 • 禁止された組織との取引を禁じる国際的な制裁制度の促進、および新種のランサムウェアに関する情報の共有
阻害	• 暗号通貨取引所やピアツーピア(P2P)・プラットフォームを、追加の顧客情報およびトレーサビリティ要件も含めて、アカウントの作成および取引の監視に関するデュー・デリジェンスの基準に準拠 • 無認可の取引所や仮想通貨交換サービスの違法行為を追跡、起訴、および公表
準備	• 最低限のサイバー・セキュリティ規範やベスト・プラクティス(たとえば、特に中小企業を支援するための最低限のセキュリティ・ガイドラインや事案対応支援といった公的なレジリエンス規範)を奨励する仕組みの促進 • ランサムウェア事案の情報開示体制の強化(可能であれば脅迫を悪化させないような期限で、特定のセクターの当局への事案報告の義務付けを含む)、および、企業がサイバー防御を強化し、攻撃者の新しいTTPに対する認識を高め、情報共有を促進するのに役立つ、より多くの脅威インテリジェンスの公開(例:暗号化解除キー) • クラウド・プロバイダーなどの主要なネットワーク・インフラストラクチャに対する責任の強化による、全体的なデジタル資産のレジリエンスの向上
対処	• ランサムウェア攻撃の実行者を追跡・訴追し身代金を回収するための強力な攻撃力の構築、および、法執行機関における調整や法的措置の一貫性の向上 • 政府が後援する機関の設立による、主にサイバー犯罪の被害を受けた小規模企業の支援 • サイバー犯罪対策のための公的機関および法執行機関の技術的知識と技術の向上

出典:ジュネーブ協会

サイバー保険は、ランサムウェアの被害組織ができるだけ早く復旧するために必要な運用上および財政上の支援を提供するだけでなく、サイバーリスク管理全体に大きく貢献します。保険は、ランサムウェアやその他のサイバー犯罪へのエクスポージャーに関する意識を高め、リスク管理に関する専門知識を共有し、またリスク防止や軽減への投資を奨励することによって、サイバー・セキュリティ規範やベストプラクティスに良い影響を及ぼすことができます。たとえば、通信事業者は(直接または専門のサイバー・セキュリティ会社と協力して)脅威となる環境を継続的に監視し、保険契約者が知らなかった企業のネットワークやシステムの脆弱性および弱点を浮き彫りにすることがよくあります。同様に、利用可能な保険の契約条件によって、保険会社または再保険会社は適切なサイバー衛生への投資を奨励することができます。これにより、ランサムウェアやその他のサイバー攻撃を受ける可能性が大幅に低下します。これらの保険の主要な利点は、ランサムウェア攻撃を実行するサイバー犯罪者に対する不注意な逆インセンティブ効果と比較検討する必要があります。

政府と規制当局によるランサムウェア攻撃の対策強化の必要性

ランサムウェアに対する特効薬はありません。根本的な原因を減らし、影響を抑え、ビジネスのレジリエンスを確保するためには、多角的な取組みが必要です。政府は規制機関や監督機関とともに、サイバー空間の安全性を向上させ、正当な企業がサイバー攻撃者に対して優位に立つことを支援する重要な役割を担っています。表1は、ランサムウェア攻撃の抑止、サイバー犯罪者のビジネスモデルの阻害、侵入に対する組織の備えの強化、および攻撃に対するさらに効果的な対処を目的とした政策について、保険会社および再保険会社からの提言を示しています。

これらの提言の多くは、最近のランサムウェアの流行を受けて、サイバー・セキュリティを強化するために各国政府によってすでに発表されている対策に反映されています。特に、ランサムウェアの種類に関する情報を追跡、監視、および共有するための仕組みを改善することは有益です。政府が支援するセキュリティ機関によって収集された脅威についてのインテリジェンスは、サイバー犯罪者の特定と追跡に使用される可能性があります。また、マルウェアの拡散を阻止するための効果的な対策や暗号化解除ツールについて、被害を受ける組織に事前の警告や助言を提供することもできます。

不正取引の特定と根絶に役立つ暗号通貨規制の強化、暗号通貨追跡の強化、盗まれた資金を回収するためのフォレンジックやその他のブロックチェーン・インテリジェンス・ツールも必要になります。特に、匿名性の高いコインの採用や、オンライン犯罪の調査や制裁の実施を困難にする分散型取引所の使用など、新たな傾向に対処するために必要です。[4]世間の注目を集める押収とともに、これは抑止力として機能します。法執行機関が暗号通貨を押収できるとサイバー犯罪者が知れば、将来的に暗号通貨を使用する動機が低下する可能性があります。

政策は、ランサムウェア攻撃に対する企業のレジリエンスを高めることにもつながります。サイバー保険単体の保険料総額は、世界の損害保険市場の1%未満ですが、この種の保険を購入している小規模企業は約3分の1にすぎないという報告があります。サイバー・エクスポージャーは増加の一途をたどっているため、まだ規模が小さく黎明期のサイバー保険の市場を育成するための政策措置は、サイバー空間の社会的利益を実現するのに役立つでしょう。

参考資料

AM Best.2021.Best's Market Segment Report (Bestの市場セグメント報告書):Ransomware and aggregation issues call for new approaches to cyber risk.(ランサムウェアや集積の問題解決に必要とされる、サイバーリスクに対する新たなアプローチ)
https://news.ambest.com/presscontent.aspx?refnum=30762&altsrc=9

Clark, R., S. Kreps, and A. Rao.2022.Shifting Crypto Landscape Threatens Crime Investigations and Sanctions. (変化する暗号通貨の様相は犯罪捜査と制裁措置を脅かす)Brookings TechStream.3月7日
https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/

K. Logue and A. Shniderman.2021.The Case for Banning (and Mandating) Ransomware Insurance. (ランサムウェア保険の禁止および義務化の事例)
https://repository.law.umich.edu/law_econ_current/207/

Talion.2021.Ransomware Perceptions Report (ランサムウェアの知見に関する報告書)、2021.
https://talion.net/wp-content/uploads/2021/08/Talion-Report_final.pdf

4 たとえば、Moneroは、IPアドレス隠蔽などのプライバシー強化技術を利用して、取引に関与する人々の身元を難読化し、トークンの互換性を向上させています。Clark et al.2022.