国立大学法人
岩手大学
IWATE UNIVERSITY

サイバーリスクと保険に関する諸問題の検討

–ランサムウェアによる身代金の支払いに保険金は支払われるべきか？–

岩手大学
深澤　泰弘

1　はじめに：問題提起

・サイバーリスクの脅威は年々増加。

⇒高度な技術を悪用したサイバー攻撃やインターネット空間を悪用した犯罪などによる被害が多数発生しており、件数も被害額も相当数に及ぶ。

・ランサムウェアの被害：令和6年上半期のランサムウェアの被害報告件数は114件（令和5年上半期：103件、下半期：94件）

1　はじめに：問題提起

- **ランサムウェア**（ransomware）：コンピュータシステムのバックアップ機能を停止させ、ユーザーのファイルを暗号化し、解除キーと引き換えに身代金を要求する悪意のあるソフトウェア（マルウェア）の一種。

⇒いったんコンピュータやネットワークが感染すると、ユーザーはシステムの再構築か身代金の支払のいずれかを選択しなければならなくなる。

1　はじめに：問題提起

◎ランサムウェアによる損害

①身代金の支払

②データの暗号化やパソコンのロックによる営業停止に伴う喪失利益の発生や、調査・復旧に伴う費用などによる損失

③データの不正使用による顧客情報の漏洩や、データ価値の減少

1　はじめに：問題提起

- 日本：身代金の支払については保険でカバーされない。
- 米国：ランサムウェアの加害者から要求された身代金の支払についてもカバーする保険が販売されている。

⇒肯定説と否定説で、議論が対立している。

- 本報告の目的：米国の議論の状況を整理して、日米で取り扱いの異なるランサムウェアに基づく身代金の支払いに対する保険適用の是非について若干の検討

2　身代金の支払は法的に問題があるか？

◎一部の場合、身代金の支払といえども資金を提供することが違法・不当な行為に当たる可能性がある。

- 外為法違反？
- 会社法違反？
- 反社会的勢力への資金提供や関与？

2　身代金の支払は法的に問題があるか？

- 身代金の支払自体は、基本的には違法ではない。
- 罰金（やわが国にはない民事的制裁）を保険でカバーしてよいか？といった議論とは異なる。
- 身代金を支払う者はあくまで被害者である（身代金を支払っても仕方がないとは通常言えない）。

3　米国の議論の状況

- 米国においても、身代金の支払は基本的には違法ではない。

⇔我が国の外為法のように、米国政府による制裁対象者に支払を実行する米国人や米国事業者に対しては、高額な罰金を科す権限を認める連邦法はある（OFAC）。

３　米国の議論の状況

・ランサムウェアの被害にあった企業のうち、身代金を支払った被害者は２０％以上に上る（2020年）。

・身代金を支払っているのは民間企業だけではない。

⇒フロリダ州リビエラビーチ：約60万ドル

⇒フロリダ州レイクシティ：約50万ドル

⇔マサチューセッツ州ニューベッドフォードは、身代金の支払を拒否（バックアップからシステムを復元する。）

3　米国の議論の状況

- 身代金の支払は通常暗号通貨（多くはビットコイン）。

⇒迅速で信頼性が高く、疑似匿名の支払いを行うことができる。

- さらに暗号通貨取引を追跡困難にするために、「ミキシングサービス」なども使っている。

3　米国の議論の状況

- 米国のサイバー保険は、ファーストパーティー型とサードパーティー型がある（もちろん混合もある）。

⇒前者は、被保険者に生じた幅広い費用が補償の対象

⇒後者は、被保険者のネットワークセキュリティの不備や機密情報の保護の不備の結果として生じる第三者の財産的損失に起因する請求などの法的責任が補償の対象。

3　米国の議論の状況

・ファーストパーティー型

⇒サイバーインシデントの管理と緩和を支援する通知、広報、その他のサービスにかかる費用、事象の原因を特定するためのフォレンジック調査の実施、バックアップから電子データの復元、事業中断、身代金の支払等が補償対象

・身代金の支払は、ファーストパーティー型の補償内容。

3　米国の議論の状況

・サイバー保険では、金銭的な補償のほかに、攻撃以前のサービスと攻撃以後のサービスも提供されている。

⇒攻撃以前のサービスは、サイバー攻撃を防ぐためのサービスが提供され、攻撃以後のサービスは、攻撃による被害を最小限に抑えるためのサービスが提供される。

3　米国の議論の状況

- 攻撃以前のサービス：パスワード管理ソフトウェアのアクセス、綿密なジオブロッキング、オンラインまたは対面式のサイバーセキュリティトレーニング等。包括的なサイバー健康診断のようなものを提供するところもあり。

3　米国の議論の状況

・攻撃以後のサービスは多くの場合「インシデント対応チーム」により行われる。

⇒チームは関連する様々な分野の専門知識を持つ個人グループにより構成され、保険会社または保険会社と関係のある第三者プロバイダーによって雇用される。

⇒チームには、フォレンジック、危機管理、広報、IT専門知識、信用調査を行う者と、それらの指揮を執る「攻撃対処担当（breach coach）」がいる。

3　米国の議論の状況

○身代金の支払という損害を保険でカバーすることに肯定的な立場

❶保険契約者側がランサムウェアによる身代金の支払といった損害を保険金により填補してもらうことができる。保険契約者側のリスク移転・リスク分散が可能になる。

⇒ランサムウェアの被害件数も被害額も年々拡大しており、大企業に限らず中小企業も含めて、いつこのような被害にあうか、わからない。このようなリスクを保険によってヘッジすることができるのは保険契約者側にとって大きなメリットがある。

3　米国の議論の状況

❷身代金の支払をコントロールすることができる。

⇒保険金を支払う際に一定の条件（例えば、保険契約者側に身代金を支払う前に被害の通知義務を課すとか、身代金を支払う前に保険者の同意を得る必要があるとか）を付けておけば、身代金を支払うよりも低い金額でコンピューターを復旧させたり、要求額よりも低い額に身代金を抑えられる可能性がある。

3　米国の議論の状況

- 身代金の支払のほうが、操業停止に伴う損失やコンピュータの復旧費用よりも安く済むことがあり（多くの場合はそう）、身代金が保険で賄われるのならば、保険契約者側は身代金の支払を選択するが、そうではない場合、操業停止に伴う損失やコンピュータの復旧費用を填補する額の保険金を保険会社は支払わなければならなくなる。

⇒身代金の支払に保険金が支払われるのならば、その分の保険金の支払額で済む方が、それ以外の損害に対する保険金の支払額よりも安く済ませることができる。

3　米国の議論の状況

- 身代金の支払をコントロールするために、保険会社が行っている最も一般的なことは、身代金の支払に際し、保険会社から書面による同意を得るようにさせていること

⇒保険金の支払にこのような条件を加えておくことで、保険契約者側が勝手に身代金を支払ってしまうのを防ぐことができる。

⇔ただし、このような同意要件を加えると、保険会社に同意についての裁量権があるのか、あるとしてどこまで許されるか、裁量権を濫用しないかという問題が生じうる。

3　米国の議論の状況

- どの程度の裁量権があるかは状況に応じて判断するしかない。明らかに不合理な身代金の額に対して、保険会社が同意しないというのは不当ではないが、同意するのが合理的な場合に、保険会社が保険金を支払いたくないなどの理由により同意しないというのであれば、これは同意の裁量権の濫用となりそう。

⇒このような問題に対しては、合理性の基準とか、契約における公正取引義務のようなもので対応できる。

3　米国の議論の状況

- 保険会社が身代金を支払うことやその額が妥当ではないと合理的に考えるときは、同意をしないという選択肢をとることになるし、それが適切であるということになる。

⇔ただ、保険会社は基本的に同意を認めないということはしないようで、その理由としては、①不誠実訴訟を起こされたくない、②身代金の支払の妨げになるという評判を避けたい、③攻撃対処担当が攻撃後の処理に関係している場合にその判断を尊重している等である。

- むしろ身代金の支払を拒絶するのは保険会社よりも保険契約者側という意見もある。

3　米国の議論の状況

❸身代金の支払を保険金でカバーできないとなると、保険会社の規制当局の役割を失うことになる。

⇒保険会社は被保険者が身代金を支払うことで、保険金を支払わなければならないから、被保険者が身代金を支払わないように、被保険者を導く。

⇒具体的にはセキュリティ対策を支援したり、攻撃以後の処理を適切に行ったりする。これによりランサムウェア攻撃を減らすことになる。

⇒保険会社の規制当局的な役割を期待できる。

3　米国の議論の状況

・身代金の支払に保険が掛けられないとなると、保険会社は身代金の支払には興味・関心がなくなるから、それらを減らそうとするインセンティブがなくなる。保険会社の規制当局的な役割を期待できなくなる。

⇔身代金の支払以外のランサムウェアの被害にも保険会社が保険でカバーするのであれば（現にそうしているわけであるが）、身代金の支払以外の損害については保険会社に利害関係があるから、それらの損害がなくなったり減るように保険会社は行動するはずである。したがって、身代金の支払を保険でカバーしない場合であっても、それ以外の損害について保険でカバーするのであれば、保険会社の規制当局的な役割は期待できる。

3　米国の議論の状況

○身代金の支払という損害を保険金でカバーすることに否定的な立場

❶身代金を支払うことで、犯罪者集団の資金を潤すことになる。

⇒身代金を保険金で填補することができれば、被害者は身代金を確実に支払うことができるようになるため、犯罪者集団は、身代金を確実に確保する機会が増える。そうすると、犯罪者集団の活動資金は増えることになるし、さらにランサムウェア攻撃を仕掛けることになる。

3　米国の議論の状況

⇒ランサムウェアの被害が増える。
⇒保険金の支払額が増える。
⇒保険料の請求額が増える。
⇒保険会社の利益が増えている。
⇒保険会社がランサムウェア攻撃を
　煽り立てる悪循環に一役買っている。
⇒「恐喝経済(the extortion economy)」

3　米国の議論の状況

❷保険に加入していることで、ランサムウェア攻撃のターゲットになる。

⇒身代金を支払う資力がなさそうでも、それを保険でカバーできる企業や団体であれば、ランサムウェアの加害者としては、攻撃の対象となり得る。

⇒身代金の支払をカバーする保険の存在が、標的を拡大している。

3　米国の議論の状況

❸身代金を支払っても、その他の被害の防止にならないかもしれない。

・合理的な加害者であれば、約束を守る方が良い。

⇒身代金を支払ってもデータの復旧を行わないのなら、身代金を誰も支払わない。これは金銭目的でランサムウェア攻撃を行っている加害者にとっても望ましくない。

⇒理論的には、ランサムウェアによる攻撃が１回限りのものでないのなら、加害者は協力するはずであるから、身代金の支払をしたら、データ復旧のためのキーの提供はするはず。

３　米国の議論の状況

⇔ただし、攻撃者の特定が難しい以上、１回限りの攻撃者か何回も実行する攻撃者か、すなわち、信頼のおける攻撃者か否かを区別するのが難しい。

⇒身代金を支払ってもデータ復旧をしてもらえないのではないか、約束を破るのではないかと思っていた方が合理的。

⇒攻撃者側も自分は信頼のおける攻撃者であることを表明したり、信頼してもらうことが難しい。

3　米国の議論の状況

❹身代金の支払に保険金が支払われることによるモラルハザードの発生

⇒身代金の支払が保険によりカバーできるのであれば、ランサムウェアの被害にあわないように準備する（システムを強化する）などを行わない。被害の全額が保険金で補えるのなら、被害の発生を減少させるためのコストをかけることがばかばかしい（モラール・ハザード）。

⇒ただ、これは免責額を設定するとか、保険料で調整するとかで、一応の対策ができそう。

3　米国の議論の状況

- 保険金詐欺は、通常の身代金目的の誘拐（偽装誘拐）よりも、起こしやすい？起こしにくい？
- 支払先や資金の流れは特定しにくそうではある。
- ランサムウェアの被害等の記録の確認や攻撃者の追跡などはどの程度できるのか？

⇒かなり専門的な知識も必要な気がするとなると、偽装誘拐のように、加害者と被害者が共謀してランサムウェアの被害を作出し、保険金を騙し取るといった心配はさほどしなくてもいい？

4　検討

- ランサムウェアによる身代金の支払を保険でカバーすることで、肯定説のあげる❶や❷のような効果が生じることは、現在のランサムウェアによる損害の対策（解決）として意味のあることかもしれない。

4　検討

- 身代金の支払を保険がカバーすることで、攻撃者は身代金を確実に取得することができ、それによりさらに攻撃を行うインセンティブが生まれたり標的を広げようという気になる。

⇒将来、ランサムウェア攻撃が増加し、さらに被害が拡大することになる。

⇒保険料が高くなるが、ランサムウェアに備えた保険に加入する必要性は高くなるので加入せざるを得ない。

⇒ランサムウェアの攻撃者と保険会社だけが儲かるだけであって、社会全体から見たら望ましくない。

4　検討

- ランサムウェアによる身代金の支払は保険でカバーしない方が良い、という結論が妥当。
- この点に関しては我が国の現状の実務の在り方で良い。

⇒それで問題はないのか（それで身代金の支払に一定の歯止めをかけることができるか）は注意が必要。

4　検討

- ランサムウェアによる被害（操業停止やデータの復旧作業による損害）が全額補償されるわけではなく、補償されない額が身代金の額を上回りそうだという場合、保険契約者側は身代金の支払を選択してしまう。
- 身代金の支払をさせない⇒ランサムウェアの攻撃者に資金を提供しない⇒攻撃者に、ランサムウェアによる攻撃をしても経済的利益は見込めないとわからせる⇒ランサムウェアによる攻撃を減少させる、というサイクルを築くためには、一番初めの「身代金の支払いをさせない」ということが重要になる。

4　検討

- 「身代金の支払をさせない」ということを、立法による解決が見込めない（外為法のような法律で取り締まることができない）のならば、保険の活用により同様の効果を導くことも可能？

⇒身代金を支払わなくても、操業停止による損失やデータ復旧等にかかる費用が保険金で十分にカバーされるのならば、被害者である保険契約者側は身代金を支払わないという選択をとる。

4　検討

・保険による十分な補償が必要。

⇔ただ、それをすべて保険契約者たちの保険料で賄うとなると限界が生じるかもしれない（保険料がとても高くなり、誰も保険に入らなくなる）。

⇒国による補助？

4　検討

- 支払うことができる保険金の額を上げる（十分な補償を行う）という方法だけではなく、支払う保険金の額を下げる（保険金を支払わなければならない事態を減らす）ことができれば、それの方が社会全体にとってプラス。
- ランサムウェアによる被害を受けたとしても、その後の対応（サービス）により被害を最小限に食い止めることができれば、支払わなければならない保険金の額を減らすことができる。

4　検討

- これを保険契約者に押し付けるのは難しいので、多くの案件を処理している（経験や知識といった被害を最小に食い止める術を持っている）保険会社に任せることができると良い。
- また、そもそもランサムウェアによる被害をなくすことにも、保険契約が影響をおよぼすことができるとよい。セキュリティの程度によって保険料を増減したり、引き受けを拒んだりしたらよい。