

## 王の身代金保険: ランサムウェアのリスクマネジメントにおけるサイバー保険の役割

アーロン・D・クームス、デイヴィッド・F・クライン

- 今日の企業は、常にハッカーによる身代金要求目当てのランサムウェア攻撃を受けるリスクに晒されています。
- ダークサイドによるサイバー攻撃を受け、身代金を支払ったコロニアル・パイプライン社も、サイバー保険に加入していたと報じられています。
- サイバー保険については賛否両論がありますが、サイバー攻撃によるリスクを管理、軽減する上で、重要な役割を果たしていくでしょう。

あなたのパソコン画面には、赤い画面とロックアイコンが映し出され、ハッカーからはビットコインによる支払い請求が…。

700年ほど前、イングランドはフランス国王の[ジョン2世を捕らえ](#)、400万[エキュ](#)の身代金を要求しました。フランスにこの高額身代金の支払い能力がなく、最終的にジョン2世は、自身の解放を確保しようと[2人の息子を身代わりの人質](#)として差し出しました。

今日、危険に晒されているのは、王と王国の領土ではなく、コンピューターシステムと電子データの王国です。これらのデータは、外国のハッカーにより人質に取られ、ハッカーは、データの暗号化を解除する鍵と引き換えにビットコインで身代金を要求します。しかし、1300年代のフランスとは異なり、今日の多くの企業は、身代金を支払うことができ、実際に支払っています。

ダークサイドとして知られるサイバー犯罪グループが、コロニアル・パイプライン社のコンピューターシステムを人質に取ったとき、[コロニアル社のCEOが、データを取り戻すために75ビットコイン\(440万ドル\)の支払いに応じる](#)まで、1日もかかりませんでした。しかし、米国の東海岸に燃料を提供する要となるパイプラインが再稼働するまでには、数日を要しました。

そして、コロニアル社の440万ドルの支払いは、全国のメディアで大きく取り上げられましたが、2021年3月に保険会社CNAがランサムウェア攻撃に対応するために[支払ったとされる](#)破格の4,000万ドル(公表されている過去に支払われた身代金の中で最高額)と比べて、はるかに低い金額でした。

コロナル社は、ハッカーによる攻撃の影響を緩和するためサイバー保険に加入していたと報道されています。ほとんどのサイバー保険には、ランサムウェア攻撃の調査費用、ハッカーとの交渉及び身代金の支払いにかかる費用をカバーする[恐喝のカバレッジが含まれています](#)。また、[損害保険](#)の中には、ランサムウェア攻撃から生じた他の損失をカバーするものもあります。

ダークサイドの攻撃(及びコロナルの支払い)により、ランサムウェアのエコシステムに対する監視が強化されました。このような[身代金支払いを違法](#)とすることを政府に求める声もあります。いずれの政府もまだ身代金の支払いを全面的には禁止してはいない一方で、米財務省は、米国の経済制裁の対象となっている者に身代金を支払う場合、[民事罰のリスク](#)がありうることを勧告しています。しかし、最近、サイバーセキュリティ及びIT産業の著名な専門家からなるグローバルタスクフォースは、身代金支払いは控えるべきであるが、[全面的禁止は解決策にならないと結論付けています](#)。そのような禁止をすれば、ハッカーは、社会的ニーズが満たされなくなるという脅威に直面したときに身代金要求への抵抗力が最も弱いと思われる病院など、最も脆弱なエリアに攻撃の対象をシフトしたり、ランサムウェア攻撃から回復するためのリソースを他に有しない中小企業に攻撃の対象をシフトしたりする可能性があるからです。

また、保険が支払可能であることを非難する声もあります。少なくともある記者は、保険会社にとってサイバー保険を売ることはビジネスとして儲かるので、これが[ランサムウェア攻撃を助長している](#)と指摘しています。大手保険会社のAXA社は最近、フランス政府からの圧力を受けて、フランスの子会社はランサムウェア支払いをカバーする保険を今後は販売しないことを[発表しました](#)。

しかし、身代金支払いのために保険が存在することが問題ではなく、むしろ解決策の一部になる可能性があります。保険が適用されることで、企業は、コンピューターセキュリティを軽視するようになったという[意見](#)があります。しかし、これは、過失責任をカバーする保険が、危険な行動を助長していると主張するのと変わりません。政策決定者は、罪のない被害者を救済する保険の有用性を認めていました。そして、多くの法域で、重過失ある行為から生じた懲罰的損害賠償であっても、保険をかけることができるとされています。その理由は、[ある州の最高裁](#)が判示したように、保険契約者は、単に懲罰的損害賠償をカバーする保険に加入しているからといって、より重過失ある行為をする可能性が高くなるわけではないからです。

また、保険会社は、保険金支払いの可能性を最小化するために、契約者に対し、サイバーセキュリティのベストプラクティスを積極的に導入するよう促す強い経済的動機を有しています。火災保険会社が昔からガイドラインを定め、物件を検査し、その結果に応じてより有利な保険料を設定することで、産業・商業の安全水準を向上させてきたように、サイバー保険会社は、ハッカーの攻撃を阻止し、損失を防ぐためのベストプラクティスを促進することができます。

さらに、保険会社が、身代金支払いを行わない場合における保険金支払いの損失より安価であるため、身代金支払いを奨励しているとの[意見](#)もあります。しかし、保険の有無にかかわらず、企業は同じような費用対効果の分析を行います。誘拐・身代金保険は[何世紀にもわたり存在し](#)、1960年代から1970年代にかけて、[企業によるその購入](#)がより一般的になりましたが、そのような保険が利用可能になったからといって、身代金支払いの可能性が高まったという証拠はありません。むしろ、ランサムウェア保険の利用により、身代金の支払総額が減少する可能性があります。初めてランサムウェア攻撃を受けた企業と異なり、ランサムウェア保険会社は、身代金を減らす交渉を行う専門知識を蓄積し、交渉を合法的に行うことができる立場にあります。

フランスは、手遅れになる前に王の身代金を支払うことができませんでした。しかし、今日のサイバー犯罪者は、被害者の支払い能力より高い身代金を要求するような真似はしません。身代金の支

払いが合法である限り、保険は、サイバー犯罪者の次の人質になるリスクを軽減するうえで、重要な役割を果たし続けると考えられます。

本稿の原文(英文)につきましては、[Insuring a King's Ransom: The Role of Cyber Insurance in Ransomware Risk](#) をご参照ください。

---

### 本稿の内容に関する連絡先

**奈良 房永** (日本語版監修)  
31 West 52nd Street  
New York, NY 10019  
+1.212.858.1187  
[fusae.nara@pillsburylaw.com](mailto:fusae.nara@pillsburylaw.com)

**Aaron D. Coombs**  
1200 Seventeenth Street, NW  
Washington, DC 20036  
+1.202.663.8071  
[aaron.coombs@pillsburylaw.com](mailto:aaron.coombs@pillsburylaw.com)

**保川 明** (日本語版作成協力)

**David F. Klein**  
1200 Seventeenth Street, NW  
Washington, DC 20036  
+1.202.663.9207  
[david.klein@pillsburylaw.com](mailto:david.klein@pillsburylaw.com)

### Legal Wire 配信に関するお問い合わせ

**田中 里美**  
[satomi.tanaka@pillsburylaw.com](mailto:satomi.tanaka@pillsburylaw.com)

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2021 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.