

「最新クロスボーダー紛争実務戦略シリーズ」 第35回

オリック東京法律事務所・外国法共同事業の訴訟チームにより、国境を超えるプロジェクトにおける紛争解決戦略について毎月開催されているオリックライブラリーセミナーの内容に基づき、実務的な観点から紹介して頂く論稿シリーズで、JCAジャーナル2011年11月号から連載頂いております。

ランサムウェア：進化するサイバー脅威に企業はどう備えるべきか、どのように「証拠」を残すべきか。

I. 序文

ランサムウェアは、もはや企業が遠い世界のリスクとして無視できるような小さな脅威ではなく、さまざまな業界のビジネスに対するサイバー脅威としてかつてないほど進化・成長している。数多くのバリエーションがあるこの形のマルウェアは、一般的に、感染したシステム上にあるデータファイルを暗号化したりロックしたりすることで、復号鍵と引き替えに「身代金」と呼ばれる対価を要求する。研究によれば、全企業のほぼ半数が過去数年で何らかのランサムウェアによる攻撃を受けていると報告されている。2017年に世界中で発生したWannaCryやPetyaランサムウェアの攻撃が示すとおり、このサイバー脅威はあらゆる企業にリスクをもたらしている。たとえば、2017年5月に発生したWannaCryランサムウェアによる攻撃は、150カ国を超える国々で30万台以上のコンピュータシステムに影響を及ぼした。ランサムウェアに感染すると、企業は自社のデータシステムにアクセスできなくなるため、ビジネスの中止という深刻な損失に見舞われる。WannaCryを原因とする損失はおよそ40億ドルに上った。このようなサイバー脅威に直面している企業側としては、複数の側面からそれに対する準備を整え、復旧のための具体的な計画を立てる必要がある。その中でも、適切な保険による補償があることを確認することは重要な要素となる。この記事では、ランサムウェアによる脅威の概要を述べるとともに、そういったランサムウェア攻撃に備えるために企業が何をすればよいかについて説明する。さ

ダレン S. テシマ (Darren S. Teshima)

オリック・ヘリントン・アンド・サトクリフ LLP、サンフランシスコ・オフィス
米国カリフォルニア州弁護士

たかとり よしひろ
高取 芳宏

オリック東京法律事務所・外国法共同事業
弁護士(日本及び米国ニューヨーク州登録)・英国仲裁人協会上級仲裁人(FCIArb.)

や くら しんすけ
矢倉 信介

オリック東京法律事務所・外国法共同事業
弁護士(日本及び米国ニューヨーク州登録)・弁理士

らに、サイバー脅威に対処するために利用可能な保険による補償について議論し、法的な観点から適切な補償を得られるための「証拠」の残し方について提言する。

II. ランサムウェアの概要

ランサムウェアは以前から存在していたが、2015年以降、ビジネスがランサムウェア攻撃のターゲットになってきた。ランサムウェアは進化し続けており、数年前まではマルウェアを含むリンクや添付ファイルがついたスパムメールを介してやってくるのが一般的だったが、今ではスピアフィッシングメールや、ソフトウェア脆弱性を突いたシステムへの侵入もランサムウェアのバリエーションに含まれている。たとえば、2017年に発生したWannaCryとPetyaによる攻撃では、Windowsオペレーティングシステムの脆弱性が悪用された。この脆弱性を突く攻撃の前にMicrosoftからパッチが発行されていたものの、影響を受けた企業の多く

はこのパッチをインストールしていなかった。

一旦システムに入り込むと、ランサムウェアは他の脆弱性も悪用して、特定のファイルパスやユーザーアカウントをさらに深く掌握する。そしてシステム上で自身を実行・インストールして、コマンドサーバーと同期する。その後マルウェアがサーバー上のデータとファイルを暗号化またはロックした上で、システムのロックを解除するための復合鍵と引き替えにランサムウェアが身代金（多くはビットコインやその他の暗号通貨）を要求する。身代金は300～10,000ドル程度であるが、ビットコイン価格の暴騰により、費用はどんどん膨れ上がっている。2017年には、1,000ドル未満だったビットコイン1個の価格が12月初めには17,000ドルを超えた。

身代金の支払いにかかるコストに加え、ランサムウェア攻撃を受けた後の会社のビジネスの遅延に伴う費用が莫大になる場合がある。ランサムウェア攻撃を含む多くのサイバー攻撃が24時間以内に解決されている一方、かなりの数のサイバー攻撃の結果、復旧と通常業務への復帰までに3日以上を要している。会社が身代金の支払いを拒否し、バックアップサーバーでの作業を余儀なくされた場合には、ビジネスの損失はかなりのものになると思われる。

またランサムウェアにより、特に企業が保有しているデータの種類によっては、企業のコンプライアンス面での課題が露呈する可能性がある。たとえば、病院やその他の医療機関は、保護医療情報（PHI）に関して厳しい規制を受けている。そういうデータをランサムウェアが暗号化した場合、一部の規制によってこのことがデータ侵害とみなされ、影響を受けた個人に対してその旨を通知しなくてはならない場合がある。一部の識者は、ランサムウェア攻撃に悪用された既知の脆弱性に企業が正当な理由なくパッチを適用していない場合、米国連邦取引委員会法の違反と見なされる可能性があるとも示唆している。

III. 企業はどのように備えるべきか

ランサムウェア攻撃に備えるために企業が実行できる予防策はたくさんある。脅威に遭遇したときに警戒を続けられるような従業員の訓練、バックアップシステムが設置されていることの確認、インシデント対応策の準備とテスト、利用可能な保険による補償（サイバー保険など）の検討などが含まれる。また、もはやサイバー攻撃からの完全な防御は困難であることを直視し、仮に攻撃を受けた場合、漏洩を引き起こした場合の責任を最小化する方策、「証拠」の残し方を考察したい⁽¹⁾。この分野においては、完全な防御や正しい答えはないが、正しい証拠作りの正しいプロセスはある（There is no perfect protection or right “answer”, but there is right “process” to produce right “evidence”）ことを認識したい。

A. 訓練

従業員は、ランサムウェア攻撃に対する企業の防衛の最前線である。企業は従業員がフィッシングメールを識別したり知らない送信元からの添付ファイルを開いたりしないよう、ランサムウェアに関する従業員の訓練に時間を割く必要がある。頻繁に出張したり離れた場所からノートパソコンで作業したりする社員がいる企業では、社員がインストラクションにしたがって自分のノートパソコンのセキュリティシステムその他のプログラムを更新するように徹底させる必要もある。また、定期的に事前の告知なしでの偽のフィッシングメール演習を実施することも検討する必要がある。それによって従業員が常に目を光らせるだけでなく、有益なデータやベンチマーク評価が従業員から提供され、そのデータを会社がレビューした上でリスク管理面での進歩を評価できるため、偽のメールによる演習は多くの会社にとって有益である。

B. バックアップシステムと事業継続計画

企業の事業継続計画の一環として、バックアップシステムを最新の状態にしておくことは不可欠である。ランサムウェア攻撃が発生した場合、バックアップシステムが物理サーバー上にある場合で

もクラウドプロバイダにある場合でも、バックアップシステムを保護し、影響を受けていないことをテストで確認してから、復元して会社の業務を復旧させる必要がある。バックアップに戻すこととで生産性がいくらか失われることは避けられないが、バックアップが不完全な場合や古い場合よりもはるかに損失は小さくなると考えられる。

C. システムを最新の状態にしておく

WannaCryやPetyaによるランサムウェア攻撃の損害が明らかになったことで、企業がオペレーティングシステムやソフトウェア、ファームウェアを最新の状態にしてパッチを適用しておくことが重要となってきた。

その他のITプロトコルでも、アクセスが必要となるネットワーク内の特定のファイルやディレクトリへのアクセスを制限するなど、ランサムウェア攻撃による損害を抑制することができる。すべてのディレクトリとファイルにアクセスさせる方が特定の権限を設定するよりも管理は楽かもしれないが、そうすると脆弱性が生じ、それをランサムウェアに悪用されて、ロック対象となる重要なファイルを簡単に見つけられてしまう可能性もある。

D. インシデント対応策

企業はインシデント対応策にランサムウェア攻撃のシナリオを組み込んで、攻撃が発生した場合の対応方法を練習するシミュレーションを実施する必要がある。慎重に準備し、訓練することで、復元と復旧における問題を識別できるようになり、復旧にかかる時間を短縮できる。なお、侵入テストその他のシミュレーションは、結果が外部に漏れないよう、法律顧問の指導のもとで実施する必要がある。この点は、外部の弁護士からの法的なアドバイスを求める形をとっておくことが、弁護士・依頼者間秘匿特権 (Attorney Client Privilege) を確保する点からも重要である⁽²⁾。筆者らが所属する法律事務所においても、国境を超えるサイバー攻撃に対処するため、ビデオリンクを駆使して、企業の法務・知的財産・人事・広報・

各事業部・マネージメント等を横断的に召集し、いざ攻撃を受けた場合や漏洩が起きた場合に、どの部署のどの担当者が、どの範囲で情報を共有し、対策を適切・迅速に取れるか、という「インシデント・シミュレーション」を実施している。このようなシミュレーショントレーニングは、どのコミュニケーションチェインや、オペレーションにおいて、その理解に齟齬があるか等、企業におけるリスクの源泉となり得る「曇」を出すことに有益なだけでなく、まさにこのようなトレーニングを実施している事実そのものが、「うちの企業はやれるだけのことはやっていた」という事実を示すための有益な「証拠」となり得るのである。

V. 保険による補償

サイバーリスク管理計画の最後の重要な要素は保険である。近年、この種の保険に加入する企業は増加しているが、まだ比較的新しいタイプの補償であるため、補償の形や規模にはさまざまなものがある。また、企業総合賠償責任保険 (CGL) など他の種類の保険とは異なり、サイバー補償には基準となる形式がない。実際、この種の保険商品はさまざまな異なる名前で売り出されている。サイバー保険の補償は、モジュール形式、すなわち保険契約者がさまざまな種類の補償からプログラムに含めるものを選択する形式になっている。そのような補償モジュールのひとつがサイバー脅迫補償、つまりその名が示唆するとおり、ランサムウェア攻撃をやめさせるための身代金の支払いに対する補償を提供するものである。後述するとおり、サイバー脅迫の補償はランサムウェア攻撃に対応するために利用可能なサイバー補償のひとつに過ぎない。それ以外では特に、ランサムウェア攻撃によってかなりの期間ビジネスがシャットダウンされるに至った場合に被る潜在的な損失からビジネスを守るために事業中断補償モジュールを、サイバー保険に含めることを検討する必要がある。ランサムウェア攻撃が発生した場合、サイバー保険以外の保険証券から、従来の身代金誘拐に対するものを含めた補償が提供される場合もある。

A. サイバー保険による補償の概要

サイバー保険の補償にはさまざまな形式があるが、保険証券では一般的に、ファースト・パーティ・カバーとサード・パーティ・カバーという2種類の主な補償モジュールを提案している。ファースト・パーティ・カバーには、(1) 事業中断、(2) データ復元および(3) サイバー脅迫が含まれる。ファースト・パーティ・カバーでは一般的に、データの侵害や、ランサムウェア攻撃を含めたサイバー攻撃が発生した場合に保険契約者が被る損失に対する精算の補償を提供している。

サード・パーティ・カバーには、(1) プライバシーおよびサイバーセキュリティに対する責任、(2) プライバシー規制に対する責任、(3) 技術的な誤りや抜け (tech E&O)、ならびに (4) マルチメディアに対する責任が含まれる。最初に挙げたサード・パーティ・カバーは特にデータ侵害やサイバー攻撃に該当するものであるが、tech E&Oとマルチメディアに対する責任の補償は本質的にはサイバー保険の補償ではなく、サイバー保険に当てはまらない第三者責任補償をさまざまな形で提供している (tech E&Oの補償は多くのサイバー保険に含まれるため、補償モジュールとして最初に挙げられることが多く、サイバー補償を提供する保険証券のいくつかが「tech E&O」保険と称されることもある。)。プライバシーおよびサイバーセキュリティに関する責任の補償は、一般的に、企業の怠慢により引き起こされたデータ侵害を申し立てる主張 (たとえば個人の特定が可能な情報や健康情報を保護するための適切な注意を企業が怠ったと主張する集団訴訟など) の結果として発生する防衛費用や損害を対象としている。企業がサイバーセキュリティの侵害を防止しなかったために、ランサムウェア攻撃などネットワークへの不正アクセスにつながったと申し立てられる場合もある。たとえば、企業が自社のファイアウォールが不完全であることを知っていた、あるいは既知のリスクに遭遇してもパッチの適用を要求しなかったという主張である。

あらゆるサイバーリスクに対する補償と同様、ランサムウェア攻撃に対する補償も所定の保険証

券に記載された文言の言い回しによって異なる。以下では、ランサムウェア攻撃の結果として生じやすいファースト・パーティ・カバー、すなわちサイバー脅迫、事業中断およびデータの復元に焦点を当てるとしている。

また、有事の際の、サイバー攻撃対処に詳しい法律事務所・弁護士の紹介といった、法的助言の面のケアが含まれている場合もある⁽³⁾。

B. サイバー脅迫の補償

すべてのサイバー保険業者が提供しているわけではないが、今では多くのサイバー保険証券がサイバー脅迫を補償している。このファースト・パーティ・カバーは、一般的に、ネットワークへの攻撃や機密情報の公開をやめさせたり防いだりするための身代金の支払いをカバーするものである。保険金については多くの場合、サイバー脅迫の「脅威」を終わらせるために保険契約者が支払う金額を保険業者が補償することを規定する内容で立案される。それに続き、補償のセクションで、保険契約者のネットワーク上にあるデータを改変または破壊する脅威や、ネットワークを使って第三者にマルウェアをばらまく脅威、個人の特定が可能な情報 (PII)、保護医療情報 (PHI) その他の機密情報にアクセスする脅威などを含めて「脅威」を定義する。また保険証券では多くの場合、サイバー脅迫の脅威の原因と範囲を調査する際にかかる費用の補償も提供している。

サイバー脅迫の補償では、通常、身代金を支払う意思を示す書面を事前に保険業者が提出することが要求される。このことは、補償を維持するためにはランサムウェア攻撃が発生した場合には早急に保険業者に通知することが非常に重要であることを意味する。ランサムウェア攻撃は、より大規模なデータ侵害を隠蔽するために人の気を散らす手段としてよく使われている。ときには、サイバー犯罪者がランサムウェア攻撃を放置しておき、最初の侵害から長い時間が経過した後になって実行に移すことがある。したがって、身代金がごく少額であったとしても、保険業者に通知することが鍵となるのである。

また、一部の保険証券では、保険契約者が法執行機関に対してランサムウェア攻撃を通知し、法執行機関によって身代金の支払いが推奨されていることが要求される。どのような場合でも法執行機関への通知は推奨される行動だが、これはすなわち、法執行機関から身代金を支払うべきでない旨の推奨が存在することは補償の対象外となる可能性があるということでもある。後述するとおり、米国連邦捜査局（FBI）はランサムウェア攻撃の被害者に対して身代金を支払わないように推奨しているが、考慮すべきさまざまな事情があるということはFBIも認識している。

サイバー脅迫の補償では多くの場合、保険契約者が履行する必要のある免責条項や保有額を差し引いてから補償が適用される。この免責条項の金額が、身代金の支払いに対する補償の障壁となる可能性がある。たとえば、保険証券で免責条項が請求1回あたり50,000ドルとなっていて、要求された身代金が25,000ドル相当（多くはビットコインなどの暗号通貨の形）であった場合、身代金要求があってもサイバー脅迫の補償に該当しない。

サイバー脅迫の補償で慎重に確認すべきもうひとつつの項目が、暗号通貨の形での身代金の支払いを除外するように、補償内容を制限するような支払形式の定義がないかどうかである。多くの保険証券では「金銭」などの漠然とした用語を指しているため、ビットコインその他の暗号通貨を含めているはずだが、一部の保険証券では明確な用語を使っており、それによって保険業者がこのような新しい形式の支払は除外されると主張する可能性がある。

すべての補償と同様、サイバー脅迫の補償もいくつかの例外の対象となる。増加し続ける、よく知られたランサムウェアの脅威に対する主な例外事項としては、ソフトウェアを最新の状態にしておかなかったことに関するものがある。このような「パッチ未適用」の例外事項では、通常、既知のソフトウェアの脆弱性に対するソフトウェアパッチや更新プログラムを保険契約者がインストールまたは実装していない場合には、保険業者は損失に対する保険金を支払わないと規定されて

いる。たとえば、前述のWannaCryによる攻撃に関しては、保険業者が補償を拒否するべくこの例外事項を引き合いに出す可能性がある。

C. 事業中断やネットワーク中断の補償

ランサムウェア攻撃を働くサイバー犯罪者にとってこの攻撃が利益を生み出す主な理由のひとつは、今日のビジネス環境において企業にはシステムをシャットダウンしている余裕がないため、シャットダウンを一刻も早く終了させようと身代金を支払ってしまうことである。分単位で（数日や数週間は言うまでもなく）収入が失われる場合もある状況では、企業を自社のネットワークからロックアウトするランサムウェア攻撃は非常にコストのかかるものである。よって、そのような事業中断を対象とするサイバー保険の補償が、企業のリスク管理計画の重要な要素となる。

ファースト・パーティ・カバーは、一般的に、あらかじめ定義された待ち時間（サイバー攻撃後12時間など）の後に、攻撃がなかった場合に得られたと思われる事業収入の損失のほか、給与を含めた通常の営業費用を補償する。この補償では、事業収入の損失を減らす、あるいは回避するために負った通常の営業費用に加え、保険契約者が負った追加費用も補償される。したがって、このサイバー補償は企業総合賠償責任保険の中の事業中断に対するファースト・パーティ・カバーに類似した運用だが、営業のシャットダウンの原因がサイバー攻撃であるという点が例外である。

一部の保険証券では、事業中断の補償を、データが改変されたり破壊されたりする状況に限定している。ランサムウェア攻撃は必ずしもデータを破壊したり改変したりするわけではなく、データを暗号化したりアクセスを拒否したりするため、保険契約者としては、自分が加入している（加入しようとする）保険のサイバー事業中断補償の具体的な内容を慎重に精査し、データへの不正アクセスでも補償が発動するかどうかを確認する必要がある。また、情報の盗難や紛失、不正アクセスがなされたことが「十分に疑わしい」ということにとどまらず、盗難や紛失、不正アクセスの事実が「実

際に発生したこと」が補償に要求されるかどうかを確認する必要がある。同様に、一部の保険証券では、正当な理由によるPIIやPHIなどのデータの侵害の疑いではなく、そういうデータが本当に侵害されたという事実が要求される場合がある。

D. データ復元の補償

ランサムウェア攻撃との関係で影響する可能性のあるもうひとつのサイバー関連ファースト・パーティ・カバーが、データ復元の補償である。この補償は通常、サイバーセキュリティ侵害（多くはDoS攻撃やマルウェア攻撃を含めたネットワークへの不正アクセスや改変と定義される）の結果として失われたデータの復旧、再現および再収集の費用をカバーするものである。この補償には、そのような損害を受けた、あるいは破壊されたデータの置き換えまたは再現が可能かどうかを判断するための費用も含まれる。ランサムウェア攻撃は、身代金を支払わなければデータを破壊するという単純な脅しのほか、データの破壊や改変を含めた企業のネットワークに対するより大きなサイバー攻撃の一部であるため、この補償も含まれている可能性がある。前述のとおり、より大きなサイバー攻撃の一部として被った関連の損失に対して補償が利用可能であることを確認するためには、ランサムウェア攻撃が発生したら早急に保険業者へ通知することが必要不可欠である。

E. サイバー攻撃に関連しない保険証券

ランサムウェア攻撃はサイバー脅威だが、従来の保険証券に適用できそうな補償があるかどうかを企業は確認する必要がある。たとえば、誘拐・身代金の保険証券でそういう補償を提供している可能性がある。現在、サイバー攻撃以外の多くの保険証券にはデータ侵害やサイバー攻撃に関連する損失を除外する条項が含まれているが、そういう保険証券でも慎重に読み直して確認する価値はあるものと思われる。

企業総合賠償責任保険（CGL）による事業中断の補償も利用できる可能性もあるが、そのような保険証券の多くには、データ侵害やサイバー攻撃

に関連する請求を除外する条項が含まれている場合がある。一部の保険証券では、データは有形の資産ではないことが明確に記述されているため、保険業者側もデータ侵害は物理的な損失の定義に合致しない旨をすでに主張している。

V. ランサムウェア攻撃への対処法

企業が全力を尽くしてランサムウェア攻撃を防止しようとしても、ハッカーはその企業のシステムに侵入しようと思う限りそのための道を見つける。前述のとおり、全企業の40%以上がランサムウェア攻撃のターゲットになっているという試算が出ている。企業がランサムウェア攻撃に遭った場合には、感染したコンピュータを早急にネットワークから取り外して隔離するなどのインシデント対応計画を即座に実行に移す必要がある。感染したコンピュータをネットワークから取り除くことによって、ネットワークの他の部分をランサムウェアが攻撃することを防止することは可能だが、その攻撃が検知されるまでの間に手遅れになっている可能性がある。バックアップシステムを保護し、そのシステムが感染していないことを確認してから、バックアップを復元する必要がある。バックアップなしで作業した結果、一部の作業内容が失われてビジネスの混乱が生じるとはいえ、損失は最小限に抑えられるものと思われる。

また、企業は、サイバー犯罪者が自分たちの要求を尊重して復号鍵を渡してくれることを期待すべく身代金を支払うかどうかを判断しなければならない。前述のとおり、実際に犯罪者が復号鍵をくれるかどうかは確実なことではない。身代金が比較的少額であることから、それ以上の事業の停止や損害を防止するために身代金を払ってしまうと考える企業も多いだろう。しかし、前述したとおり、法執行機関は企業に対し、身代金を払わず、代わりにその要求を法執行機関に報告するように促している。たとえば、FBIは身代金の支払いを推奨していない。FBIが注意しているのはとりわけ、身代金を支払っても暗号化されたデータへのアクセスが保証されるわけではない、あるいは少なくとも最初に要求された金額では保証され

ないということ、また身代金を支払うことで、このような犯罪ビジネスモデルの成長を助けてしまうということである。

前述のとおり、企業はランサムウェア攻撃に遭ったら、サイバー保険業者を含めた保険業者にそれを通知することも考慮する必要がある。身代金の金額が保険証券の保有額を超えていて、企業が身代金を支払う前に保険業者が同意していれば、身代金を支払ってもそれは保険業者によって補償される。また、身代金の金額が保険証券の保有額を超えていないためにサイバー脅迫の補償が発動しなくても、そのインシデントを保険業者に通知しておくことは、事業中断の補償など、該当する可能性のある他の種類の補償を保持するためにも役立つ。

VII. 結論

ランサムウェア攻撃はとどまることのない脅威であり、すべての企業が適応する必要のある新たなリスクの分野となる。企業側では、ソフトウェアのパッチを最新にしておくなど、さまざまな技術的予防策を補完するエンドユーザー向け啓発トレーニングを通じて、リスク緩和のための企業文化を醸成する必要がある。また、リスク管理計画の一環として、保険による補償が、この新たなサイバーリスクに対する防御において重要な役割を果たすものと思われる。また、上記に述べたような各種対策が、いざ攻撃を受けた場合ないしは保険金請求をする場合に、適切な補償を得られるための重要な「証拠」となりうることを認識し、各法的措置を適切に講じていくことが重要である。そのためには、企業の経営陣がセキュリティの「当事者」あるいは「責任者」として直接指示すべき分野であることを認識し、適切な将来への「投資」として位置づけることが重要であろう。



[注]

- (1) 高取芳宏共同編著・矢倉信介共著「訴訟・コンプライアンスのためのサイバーセキュリティ戦略」(NTT出版 2015年) 7頁等。
- (2) 高取芳宏著「企業間紛争解決の鉄則20」(2012年 中央経済社) 鉄則6 49頁等。

- (3) 例えば、筆者らの事務所は、東京海上日動火災保険によるサイバーセキュリティ保険において、有事の際に、紹介すべき法律事務所として掲載されている。