Legal Wire

pillsbury

Japan Practice

Vol. 34 / June 2017

最近の身代金ウイルスなどのサイバー攻撃、サイバー保険の重要性を再認識させる契機に

奈良房永（日本語版監修）

ジェームス・ボボテック、ペリ・マハリー

要点

- 身代金ウイルスによる大規模なサイバー攻撃は、しっかりしたサイバー保険の重要性を明確にしました。
- サイバー保険の補償範囲にサイバー恐喝を含めることは、今日のビジネス社会におけるリスクマネジメントのベストプラクティスとして広まりつつあります。
- 加入しているサイバープライバシー保険の内容を確認し、見直すことが今求められています。

5 月 12 日、大量の身代金ウイルスによるサイバー攻撃が発生し、150 を超える国の 10 万台以上のコンピューターがこれに感染する結果となりました。このウイルスは、「WannaCry」や、「WanaCryptor」、「Wcry」などとして知られるトロイの木馬型プログラムの一つで、ファイルを暗号化してアクセス不能にした上で、被害者に身代金を求め、支払がなかった場合にはデータを破壊すると脅迫するものです。5 月 14 日現在、WannaCry の被害は少なくとも 10 万を超える組織・団体の 20 万人のユーザーに及んでおり、その中には、英国の国民健康保険、グローバル運送業者である FedEx,中国の各大学機関、ロシア内務省、テレフォニカ、ガスナトゥラル、イベルドローラ、ルノーなどが含まれています。このサイバー攻撃は拡散を続けていますが、サイバー保険に加入する必要性を再認識させるとともに、身代金ウイルスによる攻撃から生じる様々な損害までカバーする保険に加入しておくべきことを再認識させるものとなりました。

WannaCry とはどのようなものか

WannaCry は、Windows XP や Windows 7 を含む旧バージョンの Windows の脆弱性を利用するものです。米国国家安全保障局が後に WannaCry によって利用されることになる「EternalBlue」問題を発見した後、マイクロソフトは、本年 3 月に、WannaCry や他のウイルスが Windows 7 を利用しているコンピューターやネットワークに侵入することを防ぐための更新プログラムをセキュリティ情報として発表していました。しかしながら、多数のマイクロソフトユーザーがセキュリティパッチをダウンロードしていませんでした。マイクロソフトが Windows XP のサポートを既に終了していたにも関わらず多くの人々がいまだにこれを利用していたことも、ハッカーを助長させることにつながりました。また、アジアの一部などにおいて Windows の海賊版が横行しているので、そのようなユーザーは海賊版使用が発覚することを恐れてプロ

グラムの更新を行うことに消極的でした。これらの結果として、一部の地域では、様々なバージョンの Windows がセキュリティパッチなしで利用されている状況が一般的となり、WannaCry の容易な侵入を許すこととなりました。

WannaCry に感染すると、ビットコインによる身代金の支払いを求められます。最初に要求される金額は 300US ドルですが、その際、3 日以内に支払わなかった場合、要求額を 600US ドルに引き上げるとの脅迫を受けます。さらに、ハッカーは、7 日以内に支払いがなされなかった場合、暗号化されたファイルは削除され、他の場所にバックアップをしていなかった場合、そのファイルは永久に失われるとも脅迫してきます。

WannaCry は無差別に攻撃を行い、特定の標的や対象業種といったものを特に有していません。さらに悪質な点として、適切な防衛策を施していないシステムの隅々へ広がっていくように設計されている点が挙げられます。また、何らユーザーによる操作を要することなく拡散可能ということは見逃すことのできない点と言えます。

身代金ウイルスとは何か

身代金ウイルスは、コンピューターシステムやネットワークに侵入し、暗号化機能などのツールを利用して、ユーザーによるシステムへのアクセスを妨害したりデータの利用を不能にした上で、身代金の支払いを要求するものです。なお、このような身代金の支払いについては、しばしばビットコインによることが求められます。身代金ウイルスによる攻撃は、電子メールに含まれる添付ファイルなどを通じて行われることが多く、その中には、実行ファイルや、アーカイブ、画像などが含まれます。添付ファイル等が開かれると、ウイルスがユーザーのシステムの中に入り込みます。身代金ウイルスの中には、(個々のパソコンやサーバに対し)暗号化を行うもの、画面をロックするもの、モバイル端末(主にアンドロイド端末)を狙ったものなどがあります。

ユーザーは、直ぐには身代金ウイルスへの感染に気づきません。暗号化メカニズムの構築が終了するまで、ウイルスはひっそりとバックグラウンドで実行されます。その後、不意に脅迫画面が表示され、ユーザーにデータがロックされたことを通知するとともに、ロックを解除するためには身代金を支払うよう要求します。その時点では、セキュリティ対策を講じてデータの保存を行おうとしても遅すぎるということになります。

現在、身代金ウイルスによる攻撃が増加しています。このようなウイルスの数は 50 種類を超えています。加えて、身代金ウイルスは急速に進化を遂げています。変種が出現する都度、より優れた暗号化機能や新たな特性が備えられています。このような事態は決して見過ごすことができません。決定的な解決方法を見出すことが困難な理由の一つには、暗号化機能それ自体は悪意のあるものではないということです。実際のところ、有用なプログラムの多くが暗号化機能を利用しています。

捨てる神あれば救う神あり－身代金ウイルスによる損害を広く補償範囲に含む保険商品

何らかのサイバー保険に加入する必要性については、今日疑問の余地のないものとなっています。さらには、そのようなサイバー保険を頼りにすることが必要な時代を迎えているとも言うことができます。サイバー保険の多くは、支払事由について様々な種類のものを選択的に提供しており、これらをニーズに応じて選ぶことが可能とされています。その中には、「サイバー恐喝」や「身代金ウイルス」についての補償などと一般的に言われているものがあります。このような場合、(i)身代金として支払った金額、(ii)恐喝者との交渉のために雇ったコンサルタントや専門家に費やした費用、(iii)身代金ウイルスの除去や、予防措置などに要した専門家費用などに対して保険金が支払われるという補償選択肢が一般的です。他には、「事業妨害(Business Interruption)」や「時間要素(Time Element)」の補償などと言われるものも一般的になっており、このような補償が含まれる場合、サイバー攻撃を受けたために失われた事業収益まで補償されることもあり得ます。

身代金ウイルスの攻撃により被害を受けた場合、どのような対応をすべきか

- **保険会社への早急な連絡**

  サイバー保険の中には、被保険者が保険会社に連絡した後に生じた費用のみ補償すると定めているものもあります。また、被保険者が適切な法執行機関へ報告することや、身代金の支払いの前に保険会社の同意を得ることを要求している保険もあります。危機的な状況に対し、至急対応しなければとの衝動に駆られることは理解できるところです。しかしながら、保険からの補償を受ける権利を保全するため、まずは保険契約における通知条項の内容を理解し、これに従った対応を取ることが推奨されます。

- **身代金の要求に応じるかの検討**

  身代金を支払ってしまうという誘惑はあるでしょう。しかしながら、たとえ支払いに応じたとしても、ファイルの暗号化が解除されるという保証はありません。加えて、身代金を支払うということは、犯人のビジネスに寄与するということを意味するものです。より多くの人々が身代金ウイルスに感染する事態を招くことにつき、その責任の一端を担うことにもなってしまいます。

- **損失の記録**

  損失についての適切・正確な記録を残すことが必要不可欠です。本来不要だったはずの費用、専門家費用、損害緩和措置のために要した費用、身代金ウイルスによる攻撃に関連して生じたその他の費用などの損失を把握することが可能となるよう、新たに別の勘定項目を開設してください。また、サイバー攻撃への対応の全てを記録し、保管するとともに、追加費用に関する領収証や他の記録も全て保存するようにしてください。

- **専門家の利用**

  一般的に、フォレンジック会計を専門とする会計士のような、クレーム専門のコンサルタントを利用することが賢明な対応と言えます。業務が妨害され、事業に毀損が生じたような場合には尚更です。また、被保険者の事業の財務上の特有性を明確にするために、他の専門家を追加することが必要となる場合もあるでしょう。このような専門家に費やした費用や損害緩和のために要したその他の費用は、多くの場合、一定の限度額の範囲内においてサイバー／プライバシー保険の補償範囲に含まれます。ただし、保険会社の事前承認を要することが一般的です。また、保険のカバレッジを専門とし、その経験を重ねている弁護士を利用することも検討すべきです。弁護士の利用は、権利主張を行う場面のみに限られるものではありません。本来秘匿特権の対象とされるはずのコミュニケーションがその性質を失わないようにするため、あるいは、保険金を請求する際に、注意不足の結果困難な状況に陥るといった事態を招かないようにするため、弁護士を利用することが考えられます。保険会社に対してその存在を知らせることなく、後方から支援させる形で弁護士を利用することも可能です。実際のところ、保険会社も通常同様の対応をしています。保険会社の損害査定人とは協力すべきですが、彼らが保険会社のために業務を行う立場にあり、被保険者のために働いているのではないことは念頭に入れておく必要があります。自らの立場を主張する必要があるのなら、そのための代弁者を雇わなければなりません。

身代金ウイルスによる攻撃に対する予防策にはどのようなものがあるか

- **コンピューターやネットワークの全てが現行バージョンであること、セキュリティが最新のものに更新されていることの確認**

  Windows ユーザーは、最新のセキュリティに更新されていることを確認する必要があります。また、フルサポートを受けることが可能なソフトウェアのみを利用することも重要です。このような対応を怠った場合、保険による補償範囲に大きな影響が出る可能性があります。

- **優良アプリケーションの一覧表の策定**

  一般的で自らのセキュリティ・ポリシーにおいて許可されたプログラムのみが実行可能となるような対応を行ってください。

- **バックアップの確保**

  現在使用されているネットワーク（ライブネットワーク）と接続されておらず、また、マッピングが不可能な媒体に、データのバックアップを保管する体制を確固たるものとしてください。

- **危機対応計画の策定**

  身代金ウイルスによる攻撃事例について検討し、そのような事態に対応することを想定した演習を実施することが求められます。

「泣きっ面に蜂」とならないように

事業運営上のリスクマネジメントの一環として、日々の警戒活動や、ライブネットワーク非接続・非関連媒体によるバックアップデータの保管、マクロの無効化、頻繁なセキュリティ更新やセキュリティパッチのインストールなどが行われるべきです。また、このような対応とは別に、サイバー保険による補償範囲にサイバー恐喝を含めることは、単に推薦されるという次元のものではなく、今日のビジネス社会におけるリスクマネジメントのベストプラクティスとして広まりつつあります。今日の状況の中、そのような対応を採らなかったとすると、まさに「泣きたくなる」（Wanna Cry）結果をもたらすこととなりかねません。

本稿の原文（英文）につきましては、Do Recent Events Make You “Wanna Cry”? をご参照ください。

本稿の内容に関する連絡先

奈良房永
1540 Broadway
New York, NY 10036-4039
212.858.1187
fusae.nara@pillsburylaw.com

James P. Bobotek
1200 Seventeenth Street, NW
Washington, DC 20036
202.663.8930
james.bobotek@pillsburylaw.com

Peri N. Mahaley
1200 Seventeenth Street, NW
Washington, DC 20036
202.663.9209
peri.mahaley@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

園谷吉基
Japan Practice Program Administrator
yoshimoto.tsumuraya@pillsburylaw.com