AIG

数字の裏側を読む：
サイバー保険における保険金請求の主要因

CLAIMS INTELLIGENCE SERIES

AIG損保

著者について

Kathy Avery：AIG Europe Limited の経営保険に関する損害サービス担当者。英国および国際的な業務過誤賠償責任保険とサイバー保険を専門としています。

José Martínez： AIG EMEA（欧州、中東およびアフリカ地域）における経営保険に関する損害サービス部門の VP。

調査分析対象

2016 年 10 月、AIG Europe Limited は同社のサイバー保険において、2013 年 9 月～2016 年 9 月に通知された 221 件の保険金請求事案を分析しました。本資料はその分析結果を元にして作成されています。

問い合わせ

AIG はサイバー保険の引受と損害サービス提供をヨーロッパ全土に展開しており、経験豊かなチームが毎年様々な保険金請求事案を扱っています。このレポートは、ロンドンに拠点を構える AIG Europe Limited が作成・発行したホワイトペーパー「Behind the numbers: Key drivers of cyber insurance claims」 を日本語に翻訳したものです。本文中に記載された内容、データ、参考資料料等に関するお問い合わせにつきましては、AIG Europe Limited までお願い致します。

AIG Europe Limited is registered in England: company number 1486260.
Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB.

AIG EMEA（欧州、中東およびアフリカ地域）のサイバー保険における保険金請求の統計は、サイバー恐喝およびランサムウェアが、大小さまざまな組織にとって、最も増えつつあるサイバー損害（サイバー犯罪による損害）であることを明らかにしています。重大性の観点から言えば、事業中断やデータ漏洩は、現在および将来的な損失を引き起こす重要なものの一つになるでしょう。

メディアにおいては、大規模な情報漏洩や、最近では「IoT」を食い物にする大胆な分散型サービス妨害攻撃（以下 DDoS 攻撃）といったサイバーインシデントが多く取り上げられています。しかし、2013 年から 2016 年 9 月までの AIG EMEA の統計によれば、サイバー恐喝およびランサムウェアこそが、最も急成長しているサイバー犯罪であることがわかります。

この期間における保険金請求の 16%は、暗号化ランサムウェアによる脅迫事案に対するものであり、それに加えて 4%は、その他のサイバー恐喝に関するものでした。特に、2016 年においては、サイバー恐喝の劇的な増加が顕著となりました。経営保険部損害サービス担当者の Kathy Avery は、「今年最初の 9 カ月間、我が社は多くの事業社からランサムウェア等の攻撃の被害にあったとの通知を受けましたが、そのほとんどにサイバー脅迫による要因がありました。比較的小規模なビジネスまで影響を受けたのです」と語りました。

AIG EMEA が受けたサイバー保険における保険金請求（2013-2016）– 種類別

16%	暗号化ランサムウェアによる恐喝
14%	ハッカーによるデータ漏洩
10%	その他のセキュリティエラー・不正アクセス
10%	その他のウイルス・マルウェアの感染
8%	従業員の過誤（例えば間違ったデータを送るなど）によるデータ漏洩
7%	なりすまし詐欺
6%	サービス妨害攻撃（DoS 攻撃）
6%	情報資産の盗難または物的損害（例えばラップトップ PC の紛失など）
4%	その他のサイバー恐喝
4%	情報保護関連法令違反に基づく法的手続き
4%	システムエラーまたはシステム停止
4%	事業中断
9%	その他

注：数値は四捨五入の関係で 100%にならないことがあります。

Avery は、ランサムウェアがシステムに入り込み、ファイルを暗号化してしまったオンラインのガーデニング事業者の実例を挙げました。中小企業はビジネスに悪影響を及ぼすような大量の極秘データは保有していないとしても、その企業は顧客にコンタクトしたり、請求書類等にアクセスすることができなくなりました。そのため、ファイルを開くために身代金を支払うことにし、AIG 社のフォレンジック担当パートナーのサポートにより、解読キーのアプリケーションを手に入れました。

サイバー恐喝と、DoS 攻撃、および DDoS 攻撃には、"脅迫"の要素があるという点において、重複するものがあります。過去 3 年間、AIG EMEA のサイバー保険における保険金請求の 6%は、DoS 攻撃のカテゴリーに分類されます。Avery は、「DoS 攻撃は、"脅迫"グループに分類されます。SQL インジェクションを使用してデータを持ち出し、身代金を支払わなければデータを公開すると脅迫するのです」と語りました。

サイバー保険における保険金請求が増加するにつれ、サイバー恐喝の通知も増加しており、実際には報告されていない、より多くの数のランサムウェアによる損害があるのではないかと推測されています。Avery は、「ランサムウェアの場合、通常はビットコインにより身代金を支払いますが、もし対応の経験が豊富でない場合、ファイルを解読している途中に他の攻撃を受けてしまう脆弱性があります。また、その身代金の要求の小ささに驚くこともあります」と語っています。

しかし、そういった攻撃を高頻度で繰り返すことにより、恐喝による収益は大きくなり、サイバー犯罪者にとって、"あぶく銭"に簡単にたどり着ける方法でもあります。Cyber Threat Alliance（CTA）の調べによると、悪意のある犯行をする者（サイバー犯罪者）は、過去 3 年で CryptoWall コードにより 3 億 2,500 万ドル、そして 2015 年に簡素なランサムウェアを使用した Cryptolocker は 3,000 万ドル以上の収益を上げたとされています。

McAfee Lab 社は、2016 年度の脅威予想のトップにランサムウェアを置いており、金融サービスや地方自治体を含めた産業部門が新たなターゲットになると予測しています。病院や医師の手術もターゲットとなっています。「医療においては、暗号化ランサムウェアによって患者のケアができなくなる、信頼性を損なうといった直接的な強い影響を与える潜在性を持っています。影響を受けやすい分野でもあります」と KPMG 社技術責任者の David Ferbrache 氏は語りました。

同氏は、「1 月か 2 月くらいに変化がありましたが、それは全く異なったタイプのランサムウェアによる脅迫であり、異質な系統で異質なツールが使用されていたのです。つまり、このことが示唆することは、すべてが『サービスとしてのサイバー犯罪』モデルとなってしまったということなのです。すべてのサイバー犯罪が商品化されてしまったのです。そして、ランサムウェア攻撃を指揮するグループも、知識が豊富になってきていると睨んでいます」と続けました。

サイバー恐喝の場合、保険金請求の重大性は、業種（種類）別による構成や、引き起こされる事業中断の程度、フォレンジックおよびシステム復旧の必要性により左右されます。ランサムウェアによる要求は、通常極めて少額ですが、一方で、DoS 攻撃および DDoS 攻撃においては、ウェブページの削除に関連する費用は後述のインターネット・ショッピング業の事例が示すようにとりわけ高額となります。

Ferbrache 氏は、「DoS 攻撃も、非常に多くが商品化されています。サイバー犯罪者は、公式サイトを襲いアクセスを集中させる DoS 攻撃を一時間 5 ドルから 10 ドルで購入するのです」と説明します。

同氏は、「誰もが心配しているのは、DDoS 攻撃でしょう。現在、人々は、デジタルビデオレコーダー、CCTV カメラやホームルーターといった、モノのインターネット（IoT）のボットネットを目にして

いますが、これこそが、非常に大量のアクセスによる混乱を招く要因になります」と続けます。

サイバー犯罪者がこの 3 年間で CryptoWall コードで稼いだ額、3 億 2,500 万ドル

2016 年 10 月、DNS（Domain Name System）サービスを提供する Dyn 社が、大規模な DDoS 攻撃を受け、広範囲にわたる混乱を招くことになりました。この DDoS 攻撃では、接続された何千万もの監視カメラ、ウェブカメラ、スマートサーモスタット、そして赤ちゃん監視用のカメラまでもがボットネットとして、デバイスマルウェア「Mirai」により乗っ取られました。Akamai Technologies 社の最新インターネットセキュリティレポートによると、大規模な DDoS 攻撃は、年間 138%の割合で成長しているとされています。

ランサムウェアや DoS 攻撃に影響を受けた場合、事業中断のコストはピークの取引期間には特に高額になります。最近公開されたある調査によると、回答の半数は、ピークの取引期間には、1 時間で 10 万ドル以上を損失したと回答しています。CMS Cameron McKenna 社の共同経営者である Stephen Tester 氏は、「ある事例では、脅迫金の要求はたったの 262 ポンドでしたが、事業中断による損害額は 7 ケタ台になりました。週末をかけてウェブサイトを削除したのです」とコメントしました。

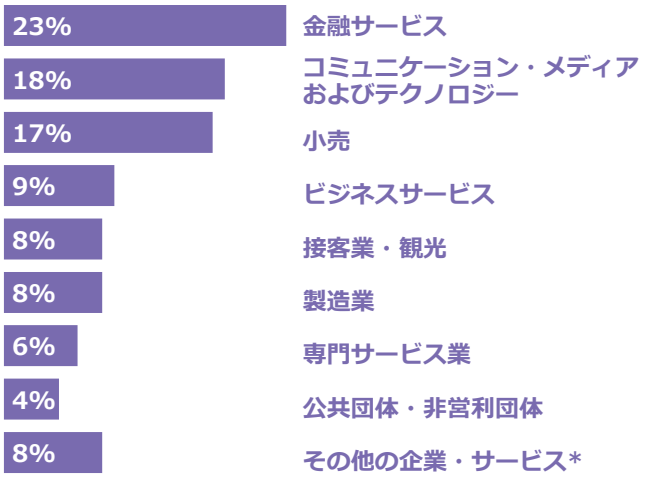
AIG EMEA への最近の保険金請求においては、事業中断に関する保険金請求はサイバー保険における保険金請求の 4%にすぎませんが（それに加えて 4%は、システム機能障害および停止によるもの）、この種の保険金請求は、将来的に頻度とその重大性の観点においてより増加すると予想されています。早急な初動対応こそが潜在的な影響を軽減させることに繋がります。

情報漏洩による保険金請求を加速させる法令

AIG EMEA における情報漏洩による損害は、ハッカーにより引き起こされたものと、従業員の過誤によるものの 2 つのカテゴリーに分類されます。この 2 つの合計で、過去 3 年に受けたサイバー保険における保険金請求の 5 分の 1（22%に相当）に相当します（3 ページ目参照）。風評被害による影響や、被害者への通知に対する要求の増加により、情報漏洩によるコストは増加しており、今後の保険金請求の頻度およびその重大性に大きく影響すると思われます。

予想される通り、ここ最近のサイバー保険における保険金請求事案は、機微情報が干渉を受けた場合に被害者への通知が求められる産業において発生しています。過去 3 年に AIG EMEA が受領した保険金請求のほぼ 4 分の 1 が金融サービス事業者からであり、それに通信業を含むコミュニケーション・メディアおよびテクノロジー事業者（18%）が続きます。

AIG EMEA が受けたサイバー保険における保険金請求(2013-2016) – 業種別



*建設業、飲食業、情報産業、輸送業、農業・漁業、エネルギー産業、不動産

注：数値は四捨五入の関係で 100%にならないことがあります。

General Data Protection Regulation（GDPR）において、EU に拠点を置く企業、および EU 外に拠点を置きながらも EU 市民のデータを取り扱う企業は、可能な限り情報漏洩発生から 72 時間以内に監督官庁に報告することが求められています。また、適切に情報を保護できなかった企業には、厳しい罰金が科せられることになります。法令に則した情報管理を行わなかったり、情報漏洩について監督官庁への報告を怠ったり、被害状況把握のための調査を実施しなかった場合に、当該企業の全世界での年間総売上高の 2%相当額までの罰金が課されることもあります。より重大な違反に至っては、罰金が 4%に達することもあります。

AIG EMEA が受けたサイバー保険における保険金請求(2013-2016) – 件数別

新たな情報保護規則や、ニュースの見出しを賑わす情報漏洩事案の発生は、サイバー保険への需要を高め、それがサイバー保険における保険金請求の頻度を高める一つの要素となることは想定内ではあります。経営保険部損害サービス担当 VP の José Martínez は、「AIG EMEA で、単独証券（stand-alone policies）ベースのサイバー保険における年間の保険金請求件数を確認したところ、2013 年で 2 件だったものが、2016 年 9 月の時点で 121 件、年間予測で 170 件に達していました」と述べました。

Ponemon 社および IBM 社の調査によると、情報漏洩によって生じる総コストの平均は、世界水準で 2013 年より 29%も上昇して 400 万ドルに達しているとされています。しかし、総コストが上昇しているにも関わらず、保険金請求の事案の重大性（被害額）は、専門家による迅速な対応により軽減していると Avery は説明します。「サイバー保険を活用することで、多くの事案について、発生から 48 時間以内に沈静化することができます」。

情報漏洩による総コストの平均は、2013 年より 29%も上昇して 400 万ドルに

さらに、Avery 氏は「導入間近の欧州の情報保護規則に準じて、会社が適切なシステムを導入し、それにより情報漏洩事案にうまく対応できたことが証明できれば、罰金を少なく抑えることもできるでしょう」と付け加えます。

サイバー保険における保険金請求には、従業員の過誤や会社に不満を持つ元従業員による犯行といった人的要因によるものもあります。従業員がフィッシング詐欺にあったり、間違った情報を送ってしまったりすることは、会社におけるトレーニングや、適切な管理およびシステムにより、減らすことができます。ノートパソコン、USB ドライブ、およびハードディスクドライブの紛失や窃盗を原因とする事案は AIG EMEA が 2013 年から 2016 年の間にサイバー保険において受領した保険金請求の 6%を占めました。

主に法律事務所にターゲットをしぼり、サイバー攻撃を金曜日の午後に行い、不正行為が次の月曜日まで発覚しないようにするといった、いわゆる「Friday Afternoon Fraud」でも悪用されたように、人的ミスや内部情報は、誰もに共通する脆弱性です。本物と見せかける為に正規の取引の詳細を用いて、機密情報を手放すように事務所を丸め込んでいることからもわかる通り、犯罪者たちは以前にも増してより洗練されてきています。

このような方法では E メールが企業への詐欺行為に使用されているのが一般的ですが、特になりすましメールが不特定多数にばらまかれていたような場合、このような事案が、はたしてサイバー保険ないし業務過誤賠償責任保険の補償対象になるのかどうかについては疑問が残ります。「補償対象か否かの瀬戸際にある保険金請求事案がかなり多くあります。その多くは実際には情報セキュリティへの干渉を伴わない、電子的になされた従来型の詐欺です」と Tester 氏は語ります。

社長へのなりすまし（Fake President Fraud）もまた別の問題です。多くの場合、犯人は従業員（一般的には会計部門の従業員）に主に電話や E メールで連絡を取り、より高い役職につく人を装って緊急の支払いを指示します。米国で「Business Email Compromise」と総称される詐欺による損害は、2016 年 5 月には 3 億 1 千万ドルにのぼり、FBI の Internet Crime Complaint Center によれば、その驚愕の伸び率は 1,300%にも達するとされています。

KPMG 社の Ferbrache 氏は、「この数字は米国および一部の国からの報告によるものだけですから、氷山の一角にすぎません。これは極めて大きな問題です。時に、これらの不正行為はまず法律事務所や会計士を巻き込んで、ターゲットとなる組織を騙したり、フィッシングしたりする E メールを作るための経路にす

るのです」と語りました。また、同氏は、「CEO になりすました不正行為の平均被害額は、16 万ドルにのぼります。欧州で報告を受けた最高額のケースでは、被害額は 4 千万ドルでした。しかし、これらがサイバー犯罪とすべきなのかもしくは巧妙に構成された信用詐欺とすべきなのかはわかりません」と付け加えました。

サイバー保険の保険金請求事例を掘り下げる

以下に記載する AIG 社における実際の保険金請求事例は、様々な種類の損害が同社の CyberEdge（サイバー保険）の対象になったことを示しています。同時に、中小企業から大企業まで広範囲にわたってサイバーインシデントの影響を受けたことがわかります。

オンライン刺繍会社に対するランサムウェア攻撃

2015 年のクリスマスの直前、英国のあるオンライン刺繍会社はランサムウェア攻撃を受けました。攻撃者は 2 つのユーザーアカウントを作成、暗号化し、注文、在庫、そして会計に関する顧客の詳細や情報を消去するよう試みました。また、攻撃者は特定のメールアドレスに連絡を取るよう記載された脅迫メモを残していきました。

攻撃者は、データの暗号化には失敗しましたが、多数のファイルを削除したり、データを移動させることに成功しました。データが再配置されたため、被保険者はその正確さを信頼することができず、システムを介した業務の遂行ができなくなりました。最後のデータバックアップは攻撃の 4 日前であった為、その前週の情報についても失われてしまいました。

被保険者は、この攻撃に関する法律上および IT に関するアドバイスを受けました。第三者のデータは影響を受けていなかったため、被保険者は情報保護機関への報告については免れました。

被保険者の IT コンサルタントは、影響をいかに軽減し、将来的なインシデント発生の可能性を最小化するための予防策についてアドバイスを提供しました。被保険者は特に、攻撃がどのように発生したかを調査し、有事のリカバリープランを検討するために、被害を受けたサーバーのデータを保全することを助言されました。

保険仲介業者の内部ネットワークドライブに保存されたファイルの暗号化

ある被保険者のコンピューターが、被保険者のコンピューターと社内ネットワークドライブに保存されていた特定のファイルを暗号化する CryptoWall マルウェアに感染しました。

ファイル名は、「help_your_files.png」に変更されており、ファイルへのアクセスを回復するために脅迫金が要求されました。

英国に拠点を置く当該被保険者は、暗号化されたファイルには、名前や住所などの顧客情報は含まれるものの、それ以外の個人情報や財務に関する情報については含まれていないと考えました。被保険者の IT システムのルーティンのバックアップには、暗号化されたファイルがアクセスされたり、エクスポートされたりもしくはデータが消失したりしたという決定的な証拠がありませんでした。

そこで、被保険者は Lloyd's や FCA(Financial Conduct Authority)への通知義務に関する法的な助言を受けました。また、外部 IT コンサルタントは被保険者に対し、当該インシデントに対する応急処置（ユーザー間のファイル共有の制限など）を実施、将来的のインシデントを予防するための防衛策を講じるよう助言しました。

オンラインショップ（小売業）に対する DDoS 攻撃

ある被保険者のウェブサイトが、DDoS 攻撃の対象となり、その結果ウェブサイトにアクセスできなかったり、パフォーマンスが著しく低下したりしました。攻撃に先立ち、被保険者は同社のウェブサイトにおけるプロテクションが極めて低いことを警告し、3,000 ポンドを支払わなければオフライン化するというオンラインメッセージを受け取りました。攻撃中にはさらに 500 ポンドの脅迫金が要求されました。

ウェブサイトの中断の結果、被保険者の売り上げは減少しました。その被害額ははかりしれません。被保険者によれば、いかなるデータに対しても（不正な）アクセスや、抽出は見られませんでした。被保険者はまた、この攻撃に起因する法的な通知についても必要はないとの助言を受けました。

しかし、IT や PR において、検討が必要な様々な問題が発生しました。外部の IT コンサルタントに加え、被保険者は PR コンサルタントにより、一時的に中断されている被保険者のウェブサイトへのフォローについての助言を受けました。

債権回収会社における不正な郵送

ある被保険者は、第三者のソフトウェアプラットフォームのエラーによって誤発送を引き起こしてしまいました。被害を受けた第三者は、この結果、不履行となった業務について被保険者に 11,275 ポンドを損害賠償請求しました。被保険者はこの金額をプラットフォームプロバイダーから回収しようとしていましたが、この金額を支払わざる負えなくなるリスクは実際に存在していました。

このインシデントは様々な問題に波及し、プラットフォームプロバイダーとの契約の範囲や、また被保険者のプロバイダーから請求された金額の支払い能力に関しての法的なアドバイスがなされました。このインシデントの結果、個人情報漏洩やデータの消失等はありませんでしたが、被保険者に対しては情報保護に関する助言も同時になされました。

外部 IT コンサルタントは、被保険者にこの事故は被保険者のシステムや従業員の問題によるものでもないことを証明しました。また、最終的に、多くの人が苦情の手紙を受け取ることになったため、被保険者は社内外の PR アドバイザーに相談して、PR の回答が適切かどうかを検討するように勧められました。

サイバー保険の保険会社に確認すべき事項

1. その保険会社には保険金請求事案の対応および支払い実績がありますか？

2. その保険会社は日々変化するサイバーリスクに先立って、被保険者の助けとなる新しい手法を持続的に模索していますか？

3. その保険会社は世界規模でしっかりした補償を提供することができますか？

4. その保険会社はフォレンジック、IT、法律または PR 等の分野におけるトップレベルの専門家のパネルを持っていますか？

5. その保険会社はリスクを最小化するための事前サービスや、事故対応の専門性を活用することで、保険引受業務および損害サービスにおいて全体的（包括的）なアプローチをすることができますか？

6. その保険会社はコミュニケーションや保険金請求事案を外部弁護士に任せっぱなしにしていますか？それとも保険引受部門と損害サービス部門の間で継続的な話し合いができる専門性の高い内部のチームを有していますか？

AIG損害保険株式会社
〒105-8602 東京都港区虎ノ門4-3-20

S042538