Claims Intelligence Series

サイバー保険における保険金請求：ランサムウェアによる業務妨害

AIG損保

AIG が 2017 年に対応したサイバー保険における保険金請求の統計にはサイバー関連事業の成熟が進んでいる事実と、最近数か月に見られた WannaCry や NotPetya を含む、一連の高度で体系的なマルウェアやランサムウェア攻撃を特徴とする脅威環境を反映しています。欧州の多くの企業・団体で、業務やネットワークの中断が重大な問題になりましたが、ほとんどの場合、そうした損失には十分な保険が掛けられていませんでした。

昨年初めに AIG のサイバー・エキスパートが予想していたように、2017 年にはランサムウェア攻撃やサイバー事業中断が頻繁に発生しました。AIG の保険金請求の統計を見ると、2017 年のサイバー保険における保険金請求のうち、ランサムウェアを主な損失原因とするものが 4 分の 1 以上（26%）を占めています。2013 年～ 2016 年までこの割合は 16% であり、大幅に増加しています。

EMEA（欧州・中東・アフリカ地域）のサイバー保険担当責任者の Mark Camillo によれば、「米国国家安全保障局（NSA）から流出したツールと、国家の支援を受けたグループが結びついたことで、組織的な事案が発生しました。」「Wannacry の拡散により、世界中で数十万台のコンピューターが影響を受けましたが、もし英国の研究者がこのランサムウェアを早期に発見し、キルスイッチを起動していなければ、事態はより深刻なものになっていたでしょう。」

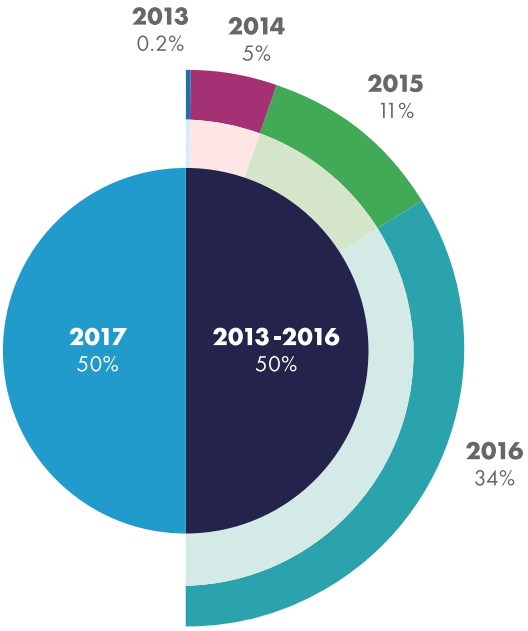
ランサムウェアに次いで多い主な侵害のタイプとしては、ハッカーによるデータ漏洩、その他のセキュリティエラー・不正アクセス、なりすまし詐欺が続いています。従業員の過誤を原因とする保険金請求は、2017 年は 7% とわずかに減少したものの、依然としてヒューマンエラーが、サイバー保険における保険金請求の大半において重大な要因になっています。

ポイント

- 2017 年の保険金請求の通知は過去 4 年間の合計に匹敵し、1 営業日あたりの請求件数は 1 件に上ります。
- サイバー保険における保険金請求の原因として最も多いのは、依然としてランサムウェアであり（主な影響は事業中断）、ランサムウェア攻撃の世界的増加を反映しています。
- サイバー保険における保険金請求の多い業種は、専門サービス、金融サービス、小売業ですが、事案の発生は幅広い業種に拡大しており、いかなる業種もサイバー攻撃と無縁ではないことが分かります。

AIG EMEA が受けたサイバー保険における保険金請求（2017）– インシデント別

AIG EMEA が受けたサイバー保険における
保険金請求（2013－2017）－ 件数別



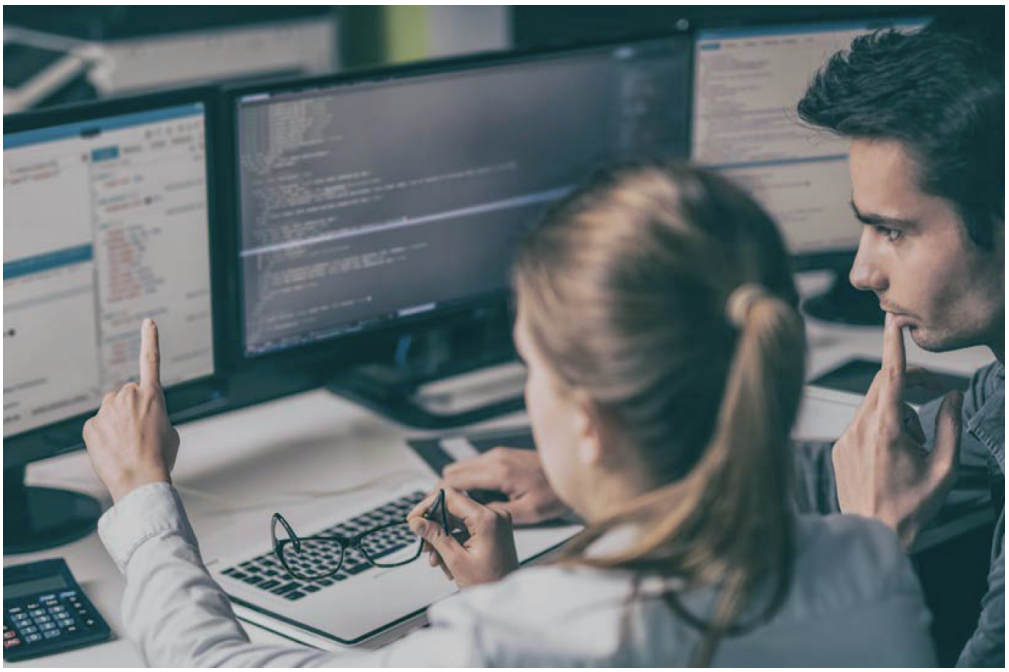
保険金請求の頻度は、昨年から引き続き増加しています。2017年に AIG のサイバー保険専門の損害サービススタッフが対応した請求件数は、1 営業日あたり 1 件に相当します。請求頻度の上昇は、サイバー被害の拡大という大きな傾向を反映しています。

サイバー保険が多くの企業・団体に普及するにつれ、保険加入者にとって、よりなじみ深い商品になっています。補償の範囲や、保険会社に通知できる／すべき事象についても、理解が深まっています。

ランサムウェアや分散型サービス妨害（以下 DDoS 攻撃）による一連の組織的な攻撃の波を受け、サイバー保険への加入が大幅に増加しました。このことからも、保険金の請求頻度が今後も上昇すると思われます。Camillo によれば、「従来サイバー保険に加入してこなかった企業・団体の間で保険への関心が高まっており、保険料の増加だけを見ても、請求件数は前年比で増加が見込まれます。」

Wannacry の拡散により、世界中で数十万台のコンピューターが影響を受けましたが、事態はより深刻なものになっていた可能性もあります。

Mark Camillo



全業種に共通の脅威

AIG の保険金請求の統計には、サイバー攻撃に無縁な業種はないという事実が表われています。2017年は、それまで AIG のサイバーにおける保険金請求の統計に全く表われたことのなかった 8 業種の保険加入者から、サイバー保険金請求がありました。保険金請求の行われる業種が、従来からサイバー攻撃の対象となってきた業種だけでなく、エネルギー関連業や運送業などにも拡大するとともに、請求件数も毎年増加する傾向が続いています。

金融サービスは依然として保険金請求件数が多いものの、2017 年の業種別割合（18%）は低下しています（2013 年～2016 年は 23%）。銀行業や保険業は膨大なデータを収集・保存し、厳格な規制の対象となっている（それゆえ多額の課徴金を課せられる可能性がある）という性質から、金融機関は常に強固なサイバーリスク対策を必要としてきました。

ただし、金融機関による保険金請求の割合が低下しているのは、単に、AIG EMEA のサイバー保険の引受件数が拡大し充実した結果、他の業種からの請求が着実に増加していることの表れと言えるでしょう。Camillo によれば、「従来、当社では常に金融業が主要な引受業種の 1 つでしたが、昨年来、その他の業種からの保険加入が多くなっています。この傾向は、夏に起きた事件・事案のために特に顕著になっています。」

更に、「最近のランサムウェア攻撃は、多くの場合、攻撃対象業種が無差別でした。」「攻撃対象となったソフトウェアのユーザーに特定の脆弱性がある場合、2017 年に多発したような無差別攻撃の被害を受けることになります。しかし 2018 年は、特に国家主導の活動が活発化している現在の政治環境において、より明確な対象を狙った攻撃が行われるかが気になるところです。」

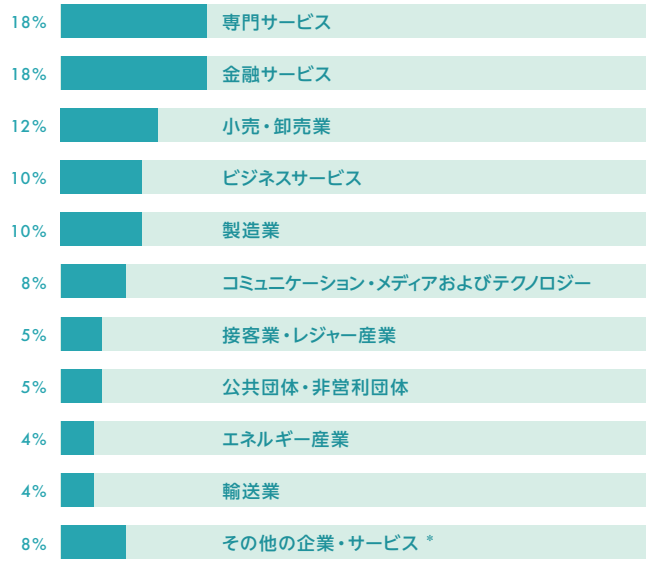
専門サービスは、サイバー保険における保険金請求全体に占める割合が大きく上昇したのに対して（2013 年～2016 年の 6% から 18% に）、従来それよりも請求件数の多かった他の業種は、割合が低下しています。AIG の経営保険部損害サービス担当者 Kathy Avery によれば、「専門サービスはデータを狙った攻撃の対象になるケースが増えています。」「大きな顧客データベースを持つ弁護士事務所や会計事務所は、データの質の高さから、サイバー犯罪者にとって間違いなく魅力的であり、通常の金融取引を狙うサイバー犯罪の被害を受けやすくなっています。」

「企業経営者の間には依然として、『うちではありえない』、『我が社に特別なデータはないから、狙われるはずがない』と考えるような態度が見られます。 しかし、会社に特別なデータがない場合でも、ランサムウェアによる恐喝の被害者になる可能性があり、ファイルを暗号化されてしまえば、業務が立ちゆかなくなります。」

弁護士や会計士などの専門サービスは、データを狙った攻撃の対象になるケースが増えています。

Kathy Avery

AIG EMEA が受けたサイバー保険における保険金請求（2017）– 業種別



＊ 飲食業、建設業、不動産、農業・漁業、情報産業
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。

ランサムウェアのコモディティ化

昨年は、欧州各国の企業・団体に被害を与える大規模な組織的事案が発生しました。WannaCry は Windows の脆弱性を利用して、150 か国以上で数十万台のコンピューターにマルウェアを拡散しました。被害を受けた企業は、医療、金融サービス、物流、教育、製造業など多くの業種に及びました。

過去 2 年間でランサムウェアのコモディティ化が更に進み、最近の変種の製作者は、「アフィリエイト・パートナー」に収益分配契約を持ちかけています。現在は脅迫金を支払った場合でも、データを回復できる保証はありません。初期のランサムウェアにあった「プロ意識」（被害者が脅迫金を支払いデータを回復するために、Bitcoin にアクセスさせるコールセンターが用意されていました）は、もはや過去のものになりました。

しかし「サービスとしてのランサムウェア」（RaaS）は、依然として企業・団体の脅威になっています。企業は自社のデータに重要性がない、あるいは不正アクセスはありそうもないと考えている場合がありますが、2017 年の保険金請求を見ると、ランサムウェア攻撃はほぼ無差別であり、あらゆる業種・規模の企業・団体で被害を受ける可能性のあることが分かります。当社は、ランサムウェアの自動化とコモディティ化の傾向が今後も続き、企業や個人に対する攻撃が増えると予想しています。

また、クリプトジャッキング（cryptojacking）、別名クリプトマイニング（cryptomining）[1] が増えることも予想されます。仮想通貨の市場規模は、2017 年に 1,200% 以上拡大しました。[2] 電子通貨の価格上昇はサイバー犯罪者の関心を呼び、仮想通貨を採掘するためにネットワークを乗っ取り、マルウェアを利用する事案が増えています。

今後、従来型の脅迫で問題になるのはデータ漏洩であり、またより明確な対象を狙ったものになると予想されます。これは現在のところ米国市場に見られる傾向ですが、欧州企業でも、特に米国で事業を行う企業に、損失が発生しています。EU の「一般データ保護規則」（GDPR）は、恐喝者の新たな交渉手段になる可能性があります。GDPR の下では、企業・組織が脅迫金を支払わず、データが破壊された場合、より重大な結果を招くことになり、それを知った上で脅迫してくるでしょう。

ネットワークの中断：重大な損失

保険金請求の統計によれば、2017 年には多くの欧州企業・団体にとって事業中断が重大な問題になっていたにもかかわらず、事業中断（サイバービジネス中断を表す際には「ネットワーク中断」と記載される）が損失の主な原因であるものは、2013 年～ 2016 年に比べると減少しています。かなりの件数の保険金請求で、ネットワーク中断が複数ある損失原因の 1 つになっていますが、必ずしも主たる原因に挙げられているわけではなく、その結果、保険金請求統計に占める割合は低下しています。

EMEA 地域サイバースペシャリストの Martin Overton によれば、「保険契約者は最初の通報時点で、何が問題なのか理解していない場合が非常に多いのです。」「単にウィルスであるとか、誰かが恐喝しようとしているとしか考えていません。フォレンジック調査チームが派遣され、詳しい調査が行われて初めて、自社のデータにアクセスできない、あるいはシステムが切断されているために、業務に支障が出ると気付くのです。」

[1] https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#48b90c4d5ae8

[2] https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#53e14c226eed

多くの企業では、ネットワーク中断の損害を補償するサイバー保険に加入していない状況が続いています。例えば、昨年のランサムウェア攻撃によって生じた財務的な損害の多くは、バランスシートの毀損です（コラム参照）。

2017 年の保険金請求を見ると、ネットワーク中断による損失の大きさは、中断の期間や企業規模、業種によって大きく異なることが明らかです。AIG Europe の場合、2017 年のネットワーク中断による損失の補償額は、3,250 ドルから 520 万ドルまでの幅があります。

EMEA 地域経営保険部損害サービス担当バイスプレジデントの José Martinez によれば、保険契約者が強固なサイバーセキュリティ対策を整備していない、あるいはデータのバックアップがない場合に、ランサムウェア攻撃によるネットワーク中断の被害が最も発生しやすい傾向があります。「これは特に中小企業にとって問題です。というのは、システムがあまり堅固でない場合が多く、またバックアップも一定期間毎にしか取っていない場合があるからです。」

「一般的に会社にバックアップがある場合、ほぼ全てのケースで、会社が脅迫金を払おうとすることはありませんでした。」「しかし昨年は、これが現実の問題になった事案も数件あり、バックアップが不十分であったために、実際に要求をのまざるをえなかったところも数社ありました。データを回復するために、脅迫金の支払いを検討せざるを得なかったのです。」

更に「こうした事例では、期間が長引くほど財務上の損害も大きくなります。」「実際 2017 年は、前年をはるかに上回る件数で、保険契約者から当社のフォレンジック調査パートナーであるKPMGに対して、ランサムウェア処理や、データの暗号解除、バックアップを使った復旧への支援依頼がありました。更にこうした保険契約者の一部からは、フォレンジック調査支援に加えて、システムやデータへのアクセス不能や、スタッフを帰宅させなければならなかったことなどによる損失に対しても、保険請求がありました。」

事業中断に備えた保険契約はまだ極めて不十分

データを暗号化するランサムウェアなど、2017 年にシステムを閉鎖に追い込んだ攻撃では、それによって引き起こされた事業中断の多くに、保険が掛けられていませんでした。新聞の見出しを飾ったランサムウェア攻撃も、その動機は必ずしも経済的な利益とは限らず、国家を後ろ盾とする組織が、混乱の誘発を望んでいる場合もあります。

実際にこうした混乱が大規模に発生しており、WannaCry が阻止されていなければ、はるかに深刻な事態になっていた可能性もあります。脅迫金の支払いは 15 万ドル弱に過ぎませんが、WannaCry 関連被害の総額は推計で 80 億ドル[3] に上り、そのうち 5 億ドルは直接的な費用と間接的な業務の混乱[4] によるものと考えられます。

マルウェアやランサムウェアが高度化するのにともない、事業中断による損失も拡大すると予想されます。ネットワーク中断が企業・団体に与える脅威は重大であるにもかかわらず、正当な注意が払われていません。

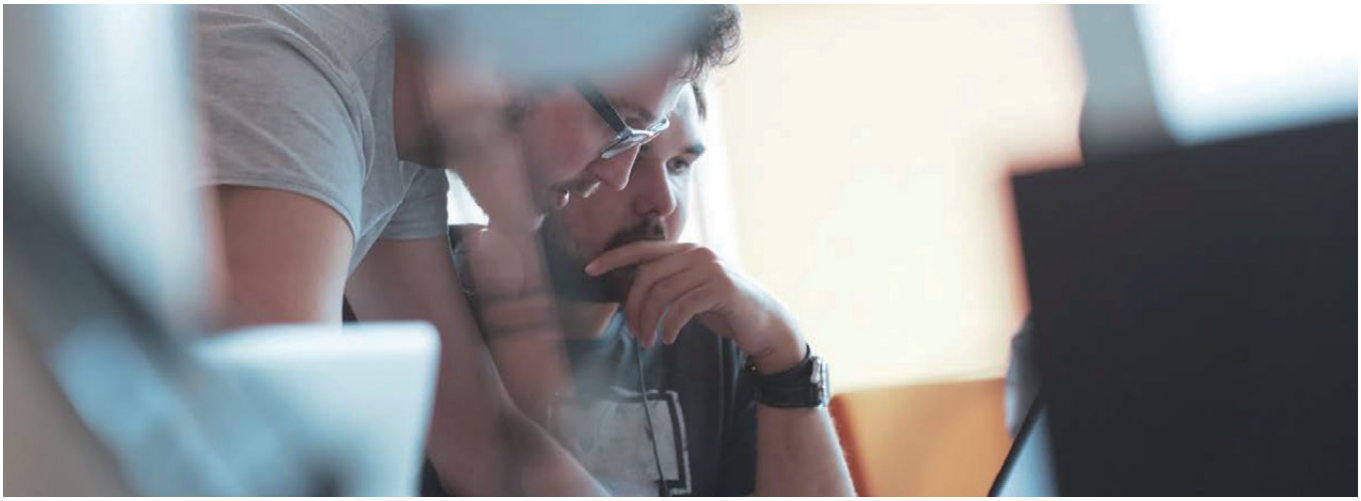
「アンダーライターやブローカーとお客様を訪問してお話しする場合、事業中断にあまり関心を示されないことが非常に多いのですが、これこそが現在、多くの企業に取って最大の問題であることを考えれば、奇妙なことです」（EMEA 地域サイバースペシャリストの Martin Overton）。

しかし昨年は、バックアップが不十分であったために、実際に要求をのまざるをえなかった会社もありました。

José Martinez

[3] https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH

[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf



GDPR がデータ漏洩トレンドのトップに

2018 年 5 月 25 日の GDPR 施行以降、データ漏洩などのセキュリティエラーによる保険請求が急増すると予想されます。企業がこれまでより積極的にデータ漏洩を報告するようになり、米国各州でデータ漏洩通知法が施行された際に見られたのと同じように、サイバー保険における保険金請求にも影響が出るでしょう。

Avery 氏によれば、「小規模な保険契約者の多くは、データ漏洩通知を行うよう勧められていますが、現行法上、その義務はありません。」「しかし 5 月に GDPR が施行されると、小規模保険契約者も選択の余地はありません。施行後はデータ漏洩通知が増えることが確実に予想されます。」

更に Avery 氏によれば、Cambridge Analytica と Facebook の個人情報スキャンダル発覚以降、個人情報に対する態度に変化が見られ、2018 年の保険金請求の種類にも影響がでることが予想されます。これは個人情報漏洩に対する消費者の許容度が、過去に比べて大幅に低下しているためです。

「最近ある大学で、データ漏洩に伴う保険金請求事案を扱いました。」「その大学は、GDPR が既に施行されているかのようにデータ漏洩通知を行っています。これは極めてコストのかかる仕事になり、また大学の評判の面からも対応が難しいものでした。通知相手が 10 万人になれば、大変な大事業になります。データ漏洩通知を受け取った人は、それが注意を呼びかけるためのものであったとしても、衝撃を受ける可能性があります。」

英国の大手スーパーマーケット Morrisons に対して従業員が起こした集団訴訟の結果は、裁判所がデータ漏洩に対する補償をどのように扱うかについて、重要なテストケースになるでしょう。従業員は、2014 年に 10 万人近い社員の個人データが盗まれたことで生じた、「衝撃と心労」に対する補償を求めています。[5)]

GDPR の導入により、今後、会社や取締役に対する株主代表訴訟が増えるという予想も、一部にあります。米国ではかなり以前から厳格な通知要件が導入されており、有名なデータ流出事件のほとんど全てで、少なくとも 1 件の集団訴訟が起きています。

欧州には、これと同じレベルの訴訟環境や集団的救済の仕組みがまだありませんが、Morrisons 事件の判決を契機に、今後同様の訴訟が提起される可能性があるでしょう。Camillo によれば、「Morrisons の事案でデータ流出による心労を根拠とする裁定や補償が認められれば、それは重要なものになる可能性があり、興味深い前例になるでしょう。」「個人情報漏洩について一般市民に通知した場合、企業・団体に対するこの種の訴訟が増える可能性があります。」

[5] https://www.independent.co.uk/news/business/news/morrisons-data-leak-staff-payout-details-sensitive-data-personal-online-hack-a8086521.html

更に「会社役員賠償責任保険(D&O 保険)のほとんどは、データ漏洩に対する株主代表訴訟の免責条項がないため、こうしたタイプの保険金請求に応じて、今後対応していくことになります。」「GDPR に関しては、制裁金という要素もあるため、現在のところ不確実なところが多くあります。こうした不確実な部分については、今年ようやくその一端が明らかになると思われますが、これは規制当局が GDPR をどの程度積極的に運用しようとするのかによって変わってくるでしょう。」

GDPR には、企業が第三者のデータ保護に必要なシステムやセキュリティの整備を怠った場合に課される制裁金が、2 種類あります。1 つ目は、1,000 万ユーロもしくは前年の全世界年間売上高の 2% のうちいずれか高い方の額、2 つ目は、2,000 万ユーロもしくは前年の全世界年間売上高の 4% のうちいずれか高い方の額です。

Camillo によれば、「2018 年後半になれば、制裁金が実際に保険対象になるか、徐々に明確になっていくでしょう。」「欧州の一部の国では、保険の適用が禁止されることが分かっていますが、英国を含めまだ正確に分からない国もあります。英国政府からは、保険の対象となるのはより行政的罰金だろうとの発言も出ています。」

DDoS 対策を怠った企業

Mirai ボットネットによって DNS プロバイダの Dyn が機能停止に追い込まれてから 2 年後の現在も、DDoS に対する脆弱性は依然として脅威であり、企業がこうした攻撃からネットワークを守るための十分な対策をとっているとは、言えません。

Reaper ボットネットは最新の変種です。Mirai 同様、ホームルーターや IP カメラ、ベビーモニターなどモノのインターネット(IoT)を構成するセキュリティの甘い多数の家庭用機器が感染しています。

Overton 氏によれば、「Reaper ボットネットを構成している IoT 機器は、1.6Tbit ／秒の送信能力を持ち、…これは膨大なデータ量です。」「現在、膨大な数のボットネットが拡散し、退潮の兆しが全く見られないことが分かっていますが、多くの企業で必要な対策が進められていません。」

現在市場では、攻撃を受けている最中でもシステム運用の継続を保証するソリューションが多数入手可能であるにもかかわらず、企業の DDoS 対策導入が十分進んでいるとは言えず、中小企業は関連費用が原因で対策が手つかずになりがちです

現在、膨大な数のボットネットが拡散し、退潮の兆しが全く見られないことが分かっています。
Martin Overton

結論：
サイバー健康診断の時期？

AIG では、事業中断／ネットワーク中断による重大な経済的影響は 2018 年を通して続き、それにより保険需要が拡大するとともに、欧州全体でサイバー保険市場の成長が続くと予想しています。事業の拡大にともない、当然、保険金請求の頻度と、またおそらく請求額の大きさも、拡大が続くと予想されます。

今後 1 年間の保険金請求のトレンドに引き続き影響を与える要因としては、ランサムウェアのコモディティ化や、GDPR の影響で今年後半に予想されるデータ漏洩による損害の急増、脆弱性と政治的不確実性の高まりを背景とした国家主導組織による影響の継続があります。従来型のサイバー脅迫やなりすまし詐欺も、注視すべきトレンドであることは間違いなく、こうした攻撃に対する防衛の最前線に立つのは、やはり社員です。

業種や企業規模にかかわらず、相互接続と一層のデジタル化が進む世界で事業を営む企業・団体にとって、攻撃や、攻撃によって生じる経済的影響の可能性に対する脆弱性が、これまでになく高まっています。AIG では、2017 年に見られたランサムウェア攻撃の組織的な性質も氷山の一角に過ぎず、今後一層困難な課題になると予想しています。

事後の対策より予防が大切であるのは常に正しいとしても、システムやネットワークがいつか侵入を許してしまうことは不可避であり、企業・団体はそれに備える必要があります。サイバーレジリエンスの高い企業・団体とは、こうした備えを怠らず、対策を実践し、更には強固なサイバーリスク戦略を実行するとともに、ネットワーク中断を含む全ての範囲のサイバー被害に対して補償を受けられるよう確保している企業・団体です。

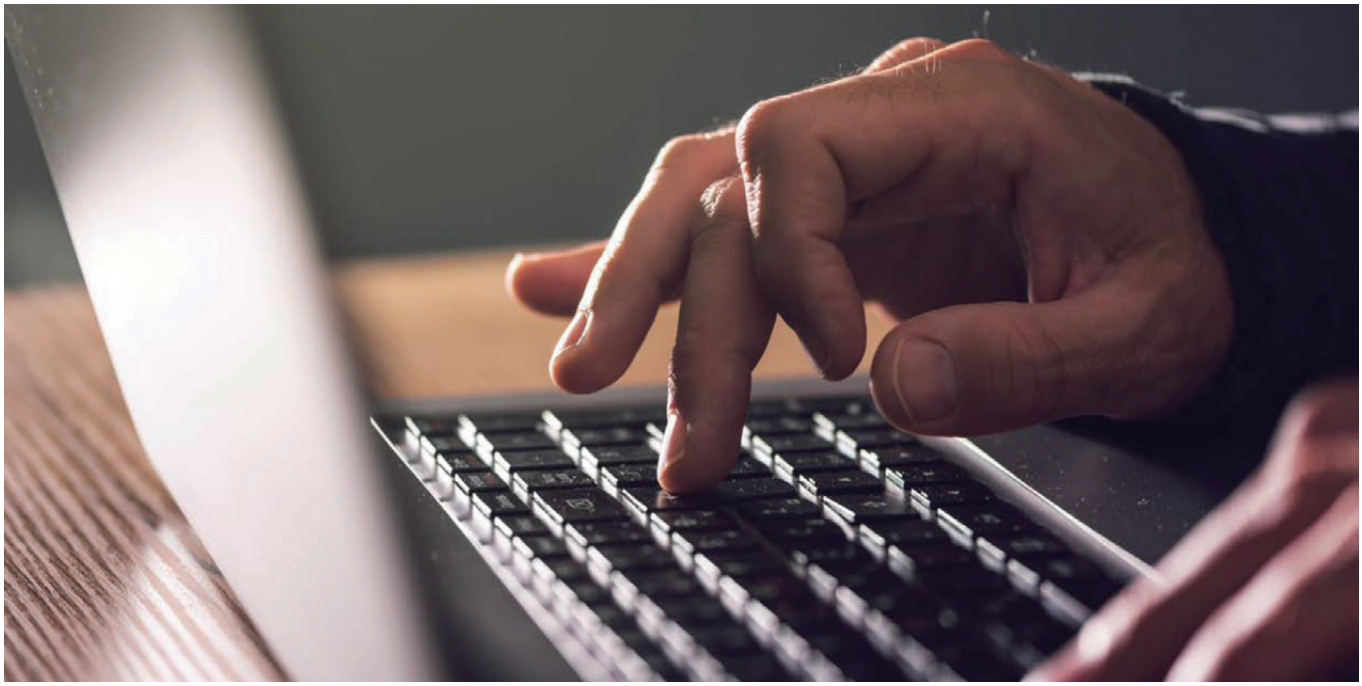
企業で特に重大な
サイバーセキュリティ・リスク

AIG に対する保険金請求実績から分かる、企業で特に重大なセキュリティエラー関連のリスクは、次のとおりです。

- リモートアクセスが可能でパスワードが脆弱な外部サーバ。これはマルウェアやランサムウェアの侵入を許す可能性があります。リモートアクセスは慎重に管理すべきです。

- パスワードのフィッシングでハッキングを許してしまうユーザーの意識不足。ユーザーがフィッシング・メールのコンテンツを開いてしまうと、偽のログインページが表示され、そこから認証情報を吸い出されて、被害者のアカウントにハッカーが侵入できるようになってしまいます。ユーザーは「このメールは信用できるか?」と考える必要があります。 ログイン情報を要求された場合は、警戒すべきです。

- 脆弱なログイン手順。フィッシングのリスクは、アカウントのログインに 2 つのコードを要求する 2 段階認証を導入すれば排除できます。少なくとも役員とパートナーシップ組織のパートナー、支払業務担当の社員には採用すべきです。費用が原因で対策が手つかずになりがちです。



保険金請求に係わる ケーススタディー

ランサムウェア攻撃により事業中断の被害を受けた製造業企業

保険契約者は、クレーン、掘削機、大型起重機や特殊起重機の設計・製造を行っています。

保険契約者は 12 月 1 日に、ランサムウェア攻撃を受けていることに気付きました。フォルダーや文書のうち 85% あまりが暗号化されています。AIG CyberEdge のホットラインに電話をかけ、IT フォレンジック調査会社の事件対応サービスを受けました。その助言に従い、バックアップからのデータ復旧を決定しました。この作業は 12 月 3 日に完了しました。

IT システムがダウンした結果、サーバにアクセスできないため、様々な部署の従業員が 12 月 1 日と 2 日の間、業務を行うことができませんでした。保険契約者の従業員は、製造要員や技術者が約 300 名います。会社の主な事業はターンキー・プロジェクトやエンジニアリング・プロジェクトであり、業務の実施には IT 機器の使用が不可欠です。

エンジニアリング・チームは、情報を会社のサーバに保存して、従業員間で共有します。エンジニアリング・スタッフの人件費請求の対象となる業務時間は、プロジェクトに直接計上されます。エンジニアはこの 2 日間業務が不可能になったため、会社が人件費を請求できる時間数に直接影響が出ました。この時間を後から回復することは難しく、それは複数のプロジェクトの工期を守る必要があるからです。仮に工期に間に合わなかった場合、顧客から違約条項を発動されることになります。

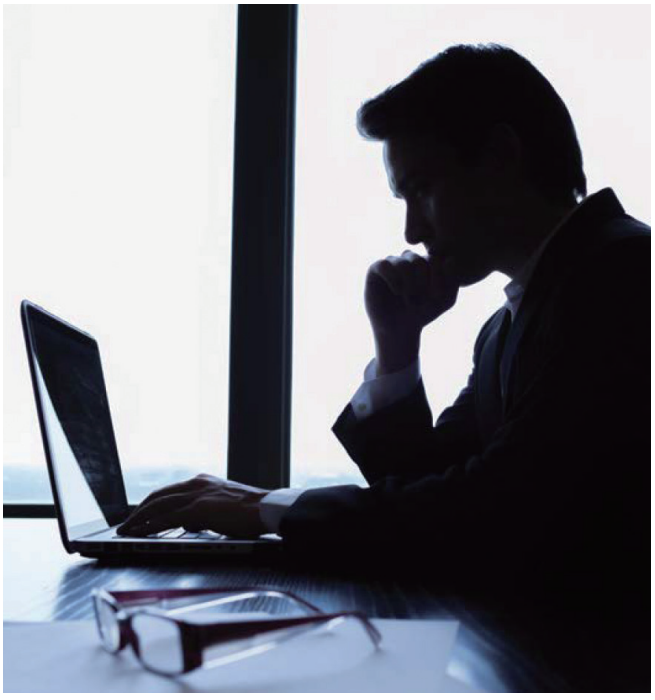
業務の継続と期日内のプロジェクト完了を確保するために必要なエンジニアリング・スタッフの追加人件費が、補償の対象になりました。

金融機関に対する DDoS 攻撃と恐喝の脅威

保険契約者である金融機関は脅迫金を要求する電子メールを受け取りました。その内容は、DDoS 攻撃を受けたくなければ 1 ビットコインを支払うよう求めるものでした。脅迫金を支払わない場合、要求を 10 ビットコインに引き上げるとも脅されました。

この金融機関は AIG の支援を受け、攻撃の影響を緩和する DDoS 防御サービスを導入するとともに、ISP に攻撃の可能性があることを連絡しました。ファイヤーウォールなどの不十分なリソースによって、自社で対応することは回避しました。

事件の調査から、犯人グループはラトビアを拠点としている可能性が出てきました。犯人グループは『XMR Squad』と名乗っています。このグループは先週来、数社に DDoS 攻撃を仕掛けており、脅威の信憑性が高いように思われました。しかしイングランド銀行からの情報によれば、今回のメールは本物の XMR Squad ではなく、模倣犯からのものと思われることが分かりました。



犯人がこの保険契約者の管理する個人情報にアクセスできる可能性は、見当たりません。最終的に脅威は現実のものとはならず、保険契約者が持つデータ資産の秘密性、完全性、利用性にはなんの悪影響もありませんでした。

保険契約者のウェブサイトとデジタルプラットフォームは、いずれもネットワーク接続と運用が維持されました。ただし、モニタリングとトラフィック分析を強化・継続しました。契約者に重大な経済的被害は発生しませんでしたが、今回の事案に関して外部から法務その他の危機管理アドバイスを受けるための経費が発生した上、調査と問題解決のために経営陣は相当な時間を費やしました。事案対応に要した経費は AIG が補償しました。

ラグジュアリー・グッズ企業を狙ったフィッシング攻撃

保険契約者はフィッシング・メールによる詐欺の被害を受けたようです。まずは従業員が狙われ、次に顧客が狙われました。

予備調査によれば、保険契約者が問題に気付く 9 か月前に、ある従業員がフィッシング・メールに記載されたリンクをクリックしてしまい、その結果、犯行グループが受信トレイにアクセスできる状態になっていました。他に少なくとも 2 名の従業員が同様のフィッシング・メールのリンクをクリックし、受信トレイへのアクセスを許してしまいました。犯行グループはこの 3 つの受信トレイにアクセスすることで、顧客の連絡先情報を取得した可能性があります。

その結果 12 か月にわたり、保険契約者からの送信を装う（実際には犯行グループが送った）「なりすまし」のフィッシング・メールを受け取った顧客から、問い合わせを受けることになり、しかも問い合わせ件数が次第に増えていきました。こうしたメールは、もともと従業員

3 名が受信したメール同様、顧客に偽のリンクをクリックするよう求めるもので、実際にクリックすると、ログインの認証情報やクレジット情報、その他保険契約者による「顧客確認」分析の支援に利用される個人情報を、入力するよう求められます。

このフィッシング・メールを受信したと連絡のあった顧客の中には、従業員の 1 人の受信トレイにあったスプレッドシートに掲載されている方も見つかりました。このスプレッドシートは顧客元帳で、約 2 万 1,000 件のメールアドレスが記載されていました。

AIG の助言で採用されたフォレンジック IT スペシャリストが、疑わしい URL へのアクセスを遮断した上で、感染した受信トレイに対象を絞って調査を行い、アクセスされたデータを確認しました。データを詳しく分析した結果、不正アクセスを受けたデータレコードは 1,000 件未満に絞り込まれました。そのため保険契約者は、被害を受けた顧客に対して、状況に応じた個別の対応を取ることが可能になりました。被害を受けた顧客の多くは富裕層や有名人でした。

調査分析対象

2018 年 3 月、AIG Europe Limited は同社のサイバー保険において、
2013 ～ 2017 年 12 月に通知された 600 件の保険金請求事案を分析しました。

www.aig.com

Mark Camillo
Head of Cyber,
EMEA
Tel: T +44 (0)20 7651 6304
mark.camillo@aig.com

Kathy Avery
Financial Lines
Major Loss Adjuster
Tel +44 (0)20 7063 5423
kathy.avery@aig.com

Martin Overton
Cyber Specialist,
EMEA
Tel: +44 (0)20 7954 7129
martin.overton@aig.com

José Martinez
VP, Financial Lines
Major Loss Claims, EMEA
Tel: +34 91 5677 431
jose.martinez@aig.com

AIG損保

このレポートは、AIG Europe Limited が作成・発行したホワイトペーパー「Cyber insurance claims: Ransomware disrupts business」を日本語に翻訳したものです。

AIG損害保険株式会社
〒105-8602 東京都港区虎ノ門 4-3-20

S043098