サイバーを理解する

ランサムウェアの傾向：リスクと回復力

Allianz Global Corporate & Specialty

AGCS について

Allianz Global Corporate & Specialty（AGCS）は、世界有数の企業保険会社であり、Allianz Group の重要な事業部門の一つです。当社では、10 の専門分野にわたり幅広い商業的リスク、企業リスク、特殊リスクに対するリスクコンサルティングサービス、損害保険ソリューション、代替的リスク移転サービスを提供します。

当社のお客様は、Fortune Global 500 企業から小企業や個人事業主に至るまで、きわめて多様です。その中には、世界最大の消費者ブランド、テクノロジー企業、世界規模の航空産業や海運業だけでなく、衛星事業者、さらにはハリウッドの映画制作会社なども含まれます。ダイナミックで多国籍化するビジネス環境において、AGCS では規模、複雑さともに最重要のリスクに対する賢明な解決策、そして傑出したクレーム体験をお届けするという信頼を顧客から寄せていただいています。

AGCS は、自社のチームで世界 30 以上の国々、またアリアンツグループのネットワークやパートナーを介して 200 を超える国や地域で業務を行っており、従業員数は約 4,400 人を数えます。アリアンツグループの最大の損害保険ユニットの 1 つとして、当社は堅固かつ安定した財務格付けに支えられており、AGCS の 2020 年の世界総保険料収益は 93 億ユーロに上ります。

www.agcs.allianz.com

はじめに

Accenture 社[1]によれば、2021 年上半期、全世界のサイバー侵入事件は前年比で 125%増加しており、この 3 桁増をもたらした上位 2 つの要因はランサムウェアと脅迫となっています。ランサムウェア攻撃が減少傾向にあることを示す証拠はほとんどありません。脆弱なサイバーセキュリティ、法執行機関が現在置かれる厳しい状況、そして暗号通貨の存在は、起訴リスクがほとんどない状態で大きな収益を得ようとする犯罪者にとって肥沃な土壌を生み出しています。

攻撃の頻度と重大度は、過去 2 年間で高まってきています。米国の連邦捜査局（FBI）[2]によれば、2020 年通年の米国でのインシデント件数は 20%、ランサムウェア攻撃は 225%増加していて、その後 2021 年の最初の 6 か月間でランサムウェア・インシデントは 62%も増加しています。2021 年通年のランサムウェア攻撃による世界各国企業のコスト負担は約 200 億ドルに上ると Cybersecurity Ventures 社[3]では推定しており、2031 年までに合計 2,650 億ドルに達すると予測しています。

ランサムウェアは、あらゆるセクターの企業にとって真の脅威となっており、簡単な救済策が見えない中、サイバーセキュリティに投資し、サイバー犯罪を実行しにくくする責任は個々の企業にあるのです。攻撃を防いで影響を軽減する措置を講じる企業は、ランサムウェアの犠牲になる可能性がはるかに低くなります。

「今の状況が改善する前に、ランサムウェア攻撃の件数が増え続けるという可能性さえあります。管理体制をさらに強化する必要があることを企業に理解してもらうために、保険会社としては保険契約とサービスの両方を改善することを通じて顧客と共に取り組む必要があります」と **Scott Sayce（Global Head of Cyber at AGCS 兼 Global Head of the Cyber Center of Competence for AGCS and the Allianz Group）**は話します。「ランサムウェア攻撃は必ずしもすべてが標的型というわけではありません。脆弱性に対処していなかったり、それを理解していない企業を『下手な鉄砲も数撃ちゃ当たる』式に狙ってくる犯罪者もいます」。

「急速に進化する今日のサイバー保険市場では、各種サイバー攻撃に備えた緊急対応サービスと金銭的補償を提供する保険適用がもはや標準となってきています。サイバー保険市場では、経済的損失の補償に加えて『デジタル SWAT チーム（特別部隊）』を提供しているといえます」。

> ランサムウェア攻撃が減少傾向にあることを示す証拠はほとんどありません。

1 Accenture 社：「2021 年上半期、世界のサイバー侵入活動は 2 倍以上に増加 — Accenture's Cyber Incident Response Update より」（Global Cyber Intrusion Activity More than Doubled in First Half of 2021, According to Accenture's Cyber Incident Response Update）2021 年 8 月 4 日
2 FBI：「休日と週末のためのランサムウェア認識」（Ransomware Awareness for Holidays and Weekends）2021 年 8 月 31 日
3 Cybersecurity Ventures 社：「全世界のランサムウェアによるコスト負担は 2031 年までに 2,650 億ドルを超えると予測される」（Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031）2021 年 6 月 3 日

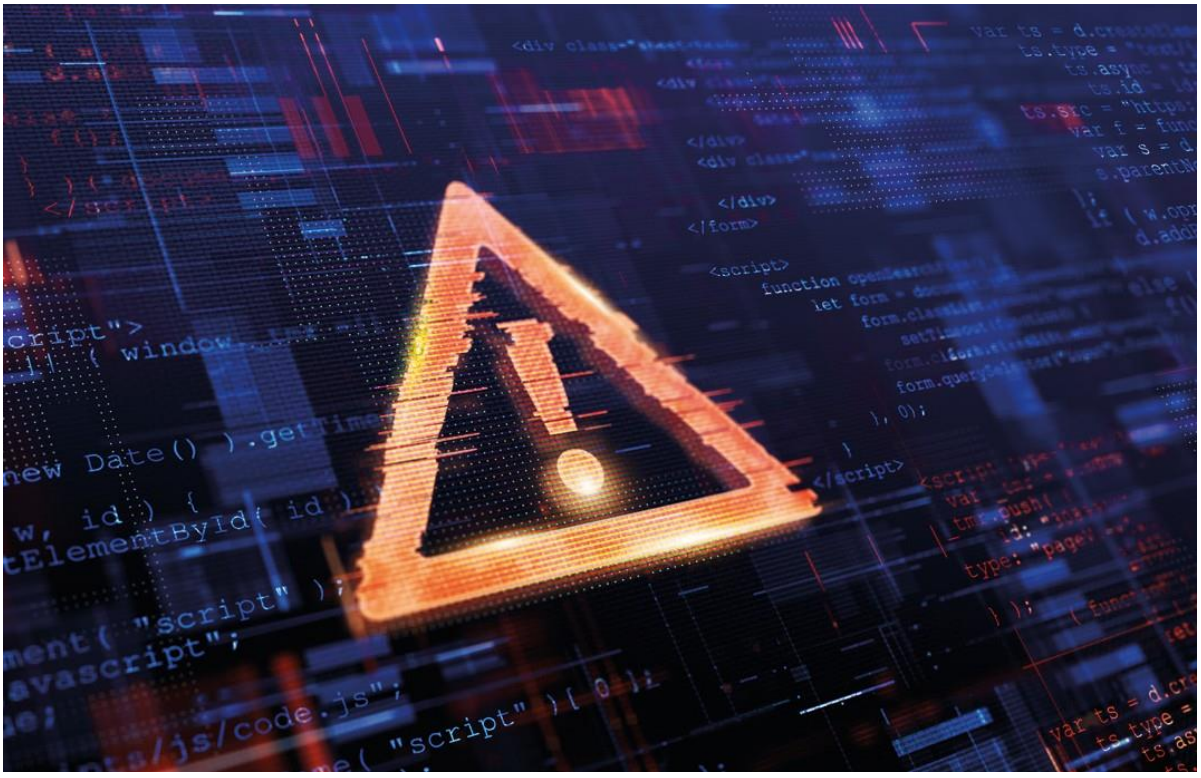
月額 40 ドルのサブスクリプションから — ビジネスとしてのランサムウェア

サイバー脅迫、特にランサムウェアは大きな事業に成長してきています。犯罪者が組織的になり、戦術とビジネスモデルが高度化するにつれて攻撃も増加してきています。たとえば、**「サービスとしてのランサムウェア」（RaaS）**の開発により、犯罪者は攻撃を実行しやすくなってきています。商業ビジネスのように運営される REvil や Darkside などの RaaS グループでは、ハッキングツールを販売またはレンタルし、これらを使って購入者などが攻撃を実行して被害者を脅迫するのです。これらのグループではまた、ヘルプ窓口やランサムウェア交渉サービスなど、さまざまなサポートサービスも提供しています。

RaaS により参入障壁が低くなり、犯罪者は活動を拡大して攻撃を強化できるようになってきています。技術的な知識があまりない人でも、RaaS を使えばランサムウェア攻撃を仕掛けることができます。月額わずか 40 ドルのサブスクリプションでも、攻撃が成功すれば身代金で数千ドルの収入になることもあります。REvil では 2021 年の最初の 6 か月で 1 億ドル近くの身代金を集めた可能性があると推定されています[4]。

ランサムウェア犯罪者集団は基本的に、効率や収益性といった商業的動機で動くものだと説明するのは Michael Daum（Senior Cyber Underwriter, AGCS）です。「ランサムウェア攻撃はビジネスのように運営されています。『二重脅迫』攻撃を展開する集団の大幅な増加、そしてサプライチェーンインシデントの急増（さらには『三重脅迫』の出現、9 ページを参照）などのトレンドはいずれも、投資リターンと効率を高めて成果を最大化するために、犯罪者が攻撃の最適化を図る目的で用いている手段の表れに過ぎないのです」。

4 Coveware 社：「ランサムウェアが国家安全保障の優先事項となる中、第 2 四半期の身代金支払い額が減少」（Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority）2021 年 7 月 23 日



増える脅威主体、増える攻撃、増えるクレーム

低リスクなうえに高収益が得られるという特徴を備えたランサムウェア攻撃。少なくとも当面の間はなくなることはないと **Marek Stanislawski**（**Global Cyber Underwriting Lead, AGCS**）は話します。

「攻撃を実行するための知識のハードルは比較的低く、ランサムウェアツールも簡単にアクセスすることができます。暗号通貨（右枠内を参照）の存在、そして犯罪者が発見と起訴を比較的容易に回避できるということから、ランサムウェアは犯罪者が簡単に成功できる分野となっています」。

ITの脆弱性が深刻化し、犯罪者が悪用できるアクセスポイントは今や無数に存在しますが、デジタル化への依存度の高まり、コロナによるリモートワークの急増、そして IT 予算の緊縮などは、このように脆弱な状態に至った理由の一部に過ぎません。初回攻撃は通常自動化されていますが、攻撃のフォローアップに必要な人的能力の不足が、これまで多くのサイバー犯罪集団にとってネックとなっていました。ところが、犯罪者集団は新たにリソースへの投資を行い、それによって能力も高まってきているとStanislawskiは話します。

「今では悪意のある脅威主体の数がさらに増え、犯罪者はこれまで以上に攻撃的な戦術を駆使して金銭をゆすり取ろうとしています」とStanislawskiはいいます。「これがランサムウェア攻撃とクレームの頻度と重大度を近年高めている要因の一つとなっています」。

AGCSが過去6年間に分析したサイバークレームの価値の大部分（81%）は、分散型サービス拒否（DDoS）攻撃やランサムウェア活動など、外部インシデントに起因する損失で占められています。ランサムウェアの件数は特に過去 2 年間で増加しており、2020 年にはクレーム件数が前年比で50%増加しています（90件）。2021年前半に寄せられたランサムウェア関連クレームの合計件数（60 件）は、2019 年通年で報告された件数とすでに同数となっています。ただし、これは全クレーム中に占める割合としては依然として比較的小さいものとなっています。

暗号通貨ファクター

暗号通貨はランサムウェアのビジネスモデルの重要な要素であり、この違法市場の成長の背景にある推進力の1つとなっています。ビットコインのような暗号通貨（ランサムウェアの身代金の約 98%がビットコインで支払われていると推定される[5]）は比較的簡単に取得して使用できる一方で、支払いは検証可能です。また、取引は匿名で実行することができるので、加害者は自分の身元を秘匿することができます。

「暗号通貨はランサムウェア攻撃の高まりの重要なファクターの一つで、これがランサムウェア攻撃を手間のかからないものにしています。犯罪者が従来の金融機関を迂回して、テクノロジーに組み込まれた匿名性の裏に隠れられるという点でウィークポイントとなっています。その一方で『know-your-customer（顧客身元確認）』およびマネーロンダリング防止法のより厳格な執行、そしてコンプライアンスの履行が、ランサムウェアのビジネスモデルを混乱させるのに役立つ可能性があります」と **Thomas Kang**（**Head of Cyber, Tech and Media, North America, AGCS**）はいいます。

5 Coveware 社：Ryuk の増加に伴い、第 1 四半期の身代金要求額は 90%増加（Ransom amounts rise 90% in Q1 as Ryuk increases）2019 年 4 月 16 日

戦術の変化

> ランサムウェア攻撃の大半は標的型でも、技術的に高度なものでもありません。

サイバー犯罪者は近年、データの最初の暗号化に加えて、機密データや個人データを公開するという第二の脅迫を組み合わせた**「二重脅迫」**戦術を用いるケースが増加しています。また、ハッカーがバックアップの暗号化や削除を試みた場合、復元と復旧がより困難、または不可能になります。最近懸念される傾向としては、攻撃者が従業員に嫌がらせをしてシステムにアクセスしたり、会社の上級管理職に直接接触して身代金を要求するといったケースがあります。

高度な標的型サイバー攻撃は、高度なリソースを備えた（そして多くの場合、国家の支援を受けた）少人数からなるハッキング集団や、外国の諜報機関によるものであることが一般的です。

このような攻撃では「ゼロデイ」攻撃（それまで知られていなかったソフトウェアのバグ）を使用してシステムに侵入し、発見されることなくデータを盗みだすという手口が一般的です。これとは対照的に、**Thomas Kang（Head of Cyber, Tech and Media, North America, AGCS）**によれば、ランサムウェア攻撃の大半は圧倒的に金銭目的の犯罪組織によるものです。

「メディアでは、注目を集める高度な攻撃の話題をよく耳にしますが、全体として、ランサムウェア攻撃の大部分は標的型ではなく、技術的に高度なものでもありません」と Kang はいいます。「ほとんどの場合、サイバー犯罪者は最も脆弱な企業を探しだし、最小限の労力で身代金が受け取れる可能性が最も高い場所に注力します」。

サイバーリスクモデリング会社の Kovrr 社[6]では、1年間に数十のアクティブな「二重脅迫」ランサムウェア攻撃活動の調査を行っています。調査対象のうち、75%でソーシャル・エンジニアリング（フィッシングメール）が伝播に使われ、25%でリモートアクセスソフトウェアの脆弱性が悪用されていました。

6 Kovrr 社：「2020 年ランサムウェア増加の主な要因」（Key Drivers of Rise of Ransomware in 2020）2021 年 2 月

ランサムウェアによるコスト負担
― 二重脅迫で書き換わるルール、コストは倍に

「従来型」のランサムウェア攻撃
（攻撃対象企業のデータを漏洩せずに暗号化するもの）による潜在的なコスト

データ漏洩イベントに発展するランサムウェア攻撃
（データを盗んで公開するもの）による潜在的な追加コスト

コスト内容：

一回の脅迫

身代金：犯罪者からの支払い要求。

収入の喪失（事業中断）：システムへのアクセスが制約される期間が長いほど損失は大きくなります。

復旧費用：データを復元し、システムを確実に復旧するための費用。

科学捜査費用：セキュリティの脆弱性の原因を調査するために必要な費用。

二重脅迫

通知コスト：顧客、規制当局、およびその他必要な当局へのデータ漏洩発生の通知。

監視コスト：データが盗まれた個人に提供する個人情報盗難／詐欺の監視サービス。

規制上の罰金と訴訟費用：個人データが盗まれたサードパーティーの請求によるもの。

データの回復と PR の修復：ネガティブな風評の影響を抑えるためのコンサルタント、危機管理会社または法律事務所の費用。

出典：Bitsight 社と Kovrr 社　図：Allianz Global Corporate & Specialty。

サプライチェーンへの攻撃は増加する見込み

過去 1 年に注目を集めたランサムウェア攻撃は、これまでにはなかった傾向が現れてきていること、特にサプライチェーンへの攻撃が増えてきていることを示しています。

これには主に 2 つのタイプがあります：ソフトウェア／IT サービスプロバイダーを標的にしてマルウェアの拡散に利用するタイプ、そして重要なインフラなどの物理的なサプライチェーンを標的とするタイプです。

たとえば、米国の石油インフラを標的とした過去最大のサイバー攻撃となった[コロニアル・パイプライン社](#)へのランサムウェア攻撃[7]では、2021 年 5 月、米国東海岸で 1 週間にわたって燃料の供給に混乱が生じました。コロニアル社は、システムを復元するために 440 万ドルの身代金をビットコインで支払い、そのうち約 200 万ドルは後に回収されました。[FBI](#)[8]によれば、サイバー犯罪者は、より高額の身代金がより高い確率で稼げることを期待して、収益性の高い大企業や重要サービスのプロバイダーを標的とするケースがますます増えてきています。

7 Bloomberg 誌：「不正入手したパスワードを使用してハッカーがコロニアルパイプラインに侵入」（Hackers Breached Colonial Pipeline Using Compromised Password）2021 年 6 月 4 日

8 FBI：「休日と週末のためのランサムウェア認識」（Ransomware Awareness for Holidays and Weekends）2021 年 8 月 31 日

三重脅迫とは？

二重脅迫が、コロナパンデミックの初期段階からサイバー攻撃の一形態として成功している状況から、ランサムウェアの脅威が進化を続けている様子を見て取ることができます。次に克服しなければならない課題は？三重脅迫・・・

ソフトウェアテクノロジー企業である Check Point Research 社[9] によれば、2021 年上半期のランサムウェア攻撃は、三重脅迫と呼ばれる新手の攻撃手法の革新に後押しされるかたちで、2020 年比で世界的に 100%以上急増しています。

三重脅迫ランサムウェアの場合、ハッカーは DDoS、ファイル暗号化、データ盗難という 3 つの形態の攻撃を組み合わせ、しかも複数の企業を標的にします。

注目すべき最初のケースは、2020 年 10 月に起きた Vastaamo クリニックへの攻撃[10] でした。40,000 人の患者を持つフィンランドのこの心理療法クリニックでは漏洩が 1 年間続き、その結果として広範な患者データの盗難とランサムウェア攻撃が発生しました。クリニックに身代金要求が送られる一方で、個別の患者にも少額の身代金要求が電子メールで送られてきました。攻撃者は、身代金を支払わなければセラピストとのセッションノートを公開すると脅迫したのです。

また、ハッカーがランサムウェア攻撃を行うのにデジタルサプライチェーンを利用するケースがますます増えてきています。今年の初め、REvil がソフトウェアプロバイダーの Kaseya 社のシステムに侵入し、同社のマネージドサービスプロバイダー（MSP）のクライアントに送信されたアップデートにランサムウェアを埋め込み、クライアントが無意識のうちに顧客情報を公開してしまうという事件が起きました。この攻撃は、これまでで最大かつ最も珍しい身代金要求事件の 1 つで、REvil は、7,000 万ドルの 1 回限りの支払いと引き換えに、影響を受けた全企業のデータとシステムのロックを解除するユニバーサルな復号化キーを提供するとしました。Kaseya 社[11] では身代金は支払っていないと話しています。

この攻撃に先だって、米国のテクノロジー企業である SolarWinds 社が同様の事件に見舞われ、このときはハッカーが SolarWinds 社のソフトウェアを悪用し、同社製品を利用する何千もの企業や政府機関へのアクセスを行いました。

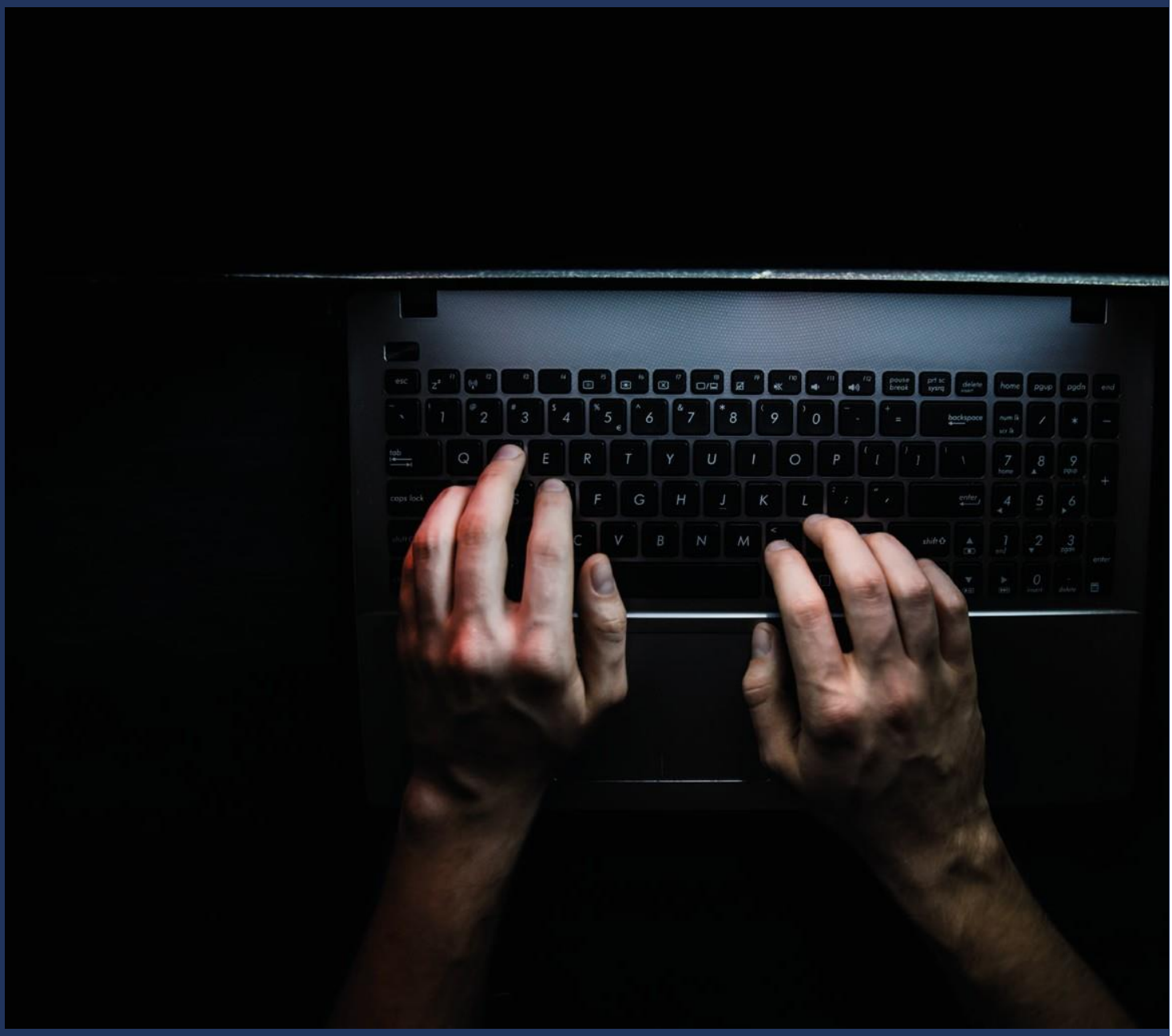
同様に、Microsoft Exchange Server[12] ソフトウェアの「ゼロデイ」脆弱性が 2021 年 3 月に、当初は国家ハッカーと疑われる集団に悪用され、その後は複数の集団が、パッチが適用されていないサーバーの脆弱性を利用してランサムウェア攻撃を行いました。

「サプライチェーン攻撃は、ランサムウェア関連の次の大きな問題になる可能性があります」と Stanislawski はいいます。「Kaseya 社に対して行われたような攻撃が増えるのではないかと思っています。Kaseya 社のように何千もの企業にサービスなどを提供する会社で、大きな損害を引き起こせば犯罪者がより高額の身代金を受け取れる可能性のある企業は数多く存在し、彼らのうってつけの標的となるのです」。

実際、欧州ネットワーク・情報セキュリティ機関（ENISA[13]）では、サプライチェーン攻撃は 2021 年末までに前年比の 4 倍に増加すると予測しています。

米国の石油インフラを標的とした過去最大のサイバー攻撃となったコロニアルパイプラインに対するランサムウェア攻撃では、2021 年 5 月、米国東海岸で 1 週間にわたって燃料の供給に混乱が生じました。

9 Checkpoint Software Technologies 社：「ランサムウェアの新たな脅威：三重脅迫」（The New Ransomware Threat: Triple Extortion）
10 Wired 誌：「死を間近に迎えた男性、セラピスト、そして世界を震撼させた身代金攻撃」（A dying man, a therapist and the ransom raid that shook the world）2020 年 12 月 9 日
11 Bloomberg 誌：「ハッカーに身代金は払っていないと Kaseya は表明」（Kaseya Says It Didn't Pay a Ransom To Hackers）2021 年 7 月 26 日
12 CSO 社：「Microsoft Exchange Server のハッキング：時系列経緯」（The Microsoft Exchange Server hack: A timeline）2021 年 5 月 6 日
13 ENISA：「サプライチェーン攻撃の脅威の状況」（Threat Landscape for Supply Chain Attacks）2021 年 7 月 29 日



$5.3mn

2021 年上半期の身代金平均要求額

$570,000

2021 年上半期の身代金平均支払額

身代金の力学

身代金の要求額は過去 18 か月で急激に増加しています。サイバーセキュリティ会社の Palo Alto Networks 社によれば[14]、2021 年上半期の脅迫の身代金平均要求額は 530 万ドルで、2020 年の平均額の 518%増しとなっています。同社によれば、最高要求額は昨年の 3,000 万ドルから 5,000 万ドルに増えている一方で、ハッカーに支払われる金額はそれよりもはるかに少ないことがよくあるということです。上半期の平均支払額は 2020 年から 82%増えて 57 万ドルでした。

法執行機関は通常、身代金要求には応えないようにとの助言をしていますが、この背景には身代金を支払うことで問題を助長し、将来的に更なる攻撃を引き起こす可能性があるからです。また、身代金を支払ったからといって、企業が迅速にファイルを回収でき、システムを復旧できることが保証されるわけではありません。多くの場合、身代金支払いの時点ですでに被害は発生しており、大半の組織では収入を失い、ファイルやシステムの復元のための費用負担も発生しています。

「会社が身代金を支払ったとしても、ファイルを復元してシステムを稼働状態に復旧するためには多大な労力が必要となります。復号化キーを持っていても、これは非常に大きな仕事となります」と Stanislawski はいいます。

コロニアル・パイプライン社が標的となったような攻撃は、ランサムウェア犯罪集団に対する政治圧力を高める動きに一役買っています。その結果として、身代金の支払いを禁止する、または少なくとも身代金支払いを報告することを企業に義務化することを求める声があがっています。ただしその一方で、これらの施策は適用法や規制の対象となり、生命の危険を伴う可能性がある場合には問題はさらに複雑になります。いずれにせよ、攻撃の影響を受けた企業は、警察や国家調査当局に通知を行い、協力する必要があります。

14 Palo Alto Networks 社：「ランサムウェアの危機が激化するなか、身代金支払額が過去最高に」（Extortion Payments Hit New Records as Ransomware Crisis Intensifies）2021 年 8 月 9 日

ランサムウェアによる損失の主な要因は事業中断と復旧費用

AGCS のクレーム分析によれば、ランサムウェアによる損失の最大要因は、サイバーインシデントによる大半の損失と同様に、事業中断による損失と復旧に要するコストとなっています（枠内を参照）。

State of Ransomware（ランサムウェアの状況）レポート[15] によれば、ランサムウェア攻撃からの復旧にかかるコスト、そして業務停止によって生じるコストの総平均は、2020 年には 761,106 ドルであったものが 2021 年には 185 万ドルと、過去 1 年間で 2 倍以上に膨らんでいます。ランサムウェア攻撃後の業務停止期間は平均 23 日となっています[16]。

「サイバーによる事業中断の場合、タイミングがすべてです。身代金を支払うのに 1 週間かかった場合、その時点で損失はすでに顕在化しており、復旧のためのコストもすでに動いています。たとえば、科学捜査の専門家と対応策コンサルタントにかかるコストは 1 日あたり 2,500 ドルに上ることもあり、短期間のうちに 7 桁（億円単位）に達する可能性もあります」と **Rishi Baviskar（Global Cyber Experts Leader, Risk Consulting, AGCS）**は話します。

15 Sophos 社：「ランサムウェアの状況 2021 年」（State of Ransomware 2021）2021 年 4 月 27 日
16 Coveware 社：「ランサムウェアが国家安全保障の優先事項となる中、第 2 四半期の身代金支払い額が減少」（Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority）2021 年 7 月 23 日

サイバークレームが着実に増加

世界のサイバー保険市場の成長もあって、AGCSに寄せられるサイバー保険のクレーム件数は、ランサムウェア攻撃発生の通知をはじめ、近年着実に増加してきています。サイバーがまだ比較的新しい保険分野であった2016年にAGCSに寄せられたサイバー関連クレームの件数が約80件であったのに対して、2020年には合計1,000件を超えるクレームが寄せられています。この傾向は2021年も続いており、今年上半期には500件を超えるサイバー関連クレームが寄せられています。

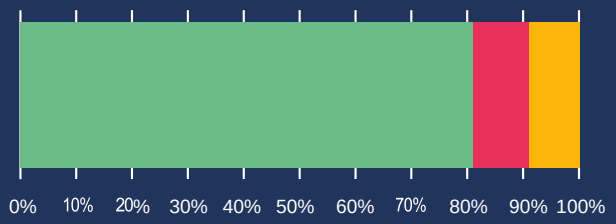
過去6年間に分析したサイバー関連クレームの価値の大部分（81%）を占めるのは、DDoS攻撃やランサムウェア活動など、外部インシデントに起因する損失です。ランサムウェアの件数は過去2年間で急増しており、2020年にはクレーム件数が前年比で50%増加しています（90件）。
2021年前半に報告を受けた合計件数（60件）は、2019年通年で報告された件数とすでに同数となっています。これは全クレームに占める割合としては依然として比較的小さいものです。

とはいえ、病院／ヘルスケア、小売、化粧品、テクノロジーと通信、流通とロジスティクス、建設、クラウドコンピューティング・サービスプロバイダーなど、多くの業界とセクターに影響が及んでいます。

サイバー損失の主たるコスト要因は事業中断で、このコストは保険業界の3,000件近くのサイバー関連クレームの価値（約7億5,000万ユーロ［8億8,500万ドル］）の50%を優に超えます。

「クレーム環境とサイバー脅威環境は、数年前よりもかなり悪化しています」と**Scott Sayce**（**Global Head of Cyber, AGCS**）は説明します。「そのため保険各社は、クライアントと協力して、導入が必要で許容可能な管理体制について、強力な基準ラインを導き出すことなしに、この市場で事業を継続することはできません」。

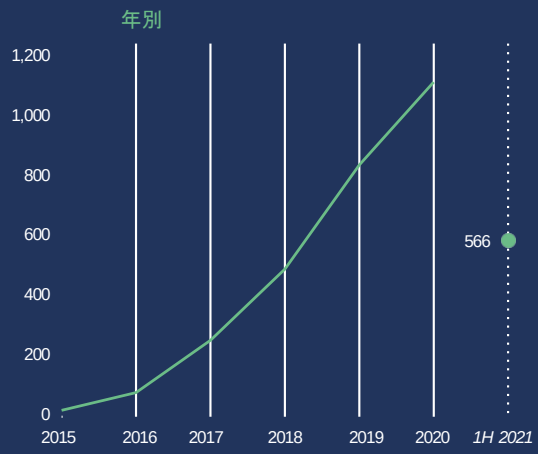
クレーム額別の損失の原因



- **外部からのシステム操作** 81%
  （例：インターネットからの直接攻撃、またはランサムウェア／マルウェアなどの悪意のあるコンテンツ）
- **悪意のある内部の行動** 10%
  （例：不正な従業員による行動）
- **偶発的な内部原因** 9%
  （例：人為的ミス、技術／システムの障害や停止）

2015年から2021年6月30日にかけて報告された7億5,100万ユーロ（8億8,500万米ドル）に相当する2,916件のクレームの分析に基づくものです。合計はランサムウェア・インシデントだけでなく、サイバー関連のすべてのクレームの合計です。合計金額にはAGCSの他にクレームに関わった他の保険会社の負担分も含まれます。
出典：Allianz Global Corporate & Specialty

サイバー関連のクレーム件数



* AGCSはサイバー保険の提供を2013年に開始したばかりであることから、クレーム件数は限られています。合計はランサムウェア・インシデントだけでなく、サイバー関連のすべてのクレームの合計です。
出典：Allianz Global Corporate & Specialty


command
option
alt
PASSWORD
1234**

変化を迎える保険市場

> 保険各社は
> サイバーセキュリティの
> ベストプラクティスを特
> 定すべく企業と協力して
> います。

過去数年のランサムウェアパンデミックは、保険会社と被保険者が攻撃の頻度と重大度の高まりを軽減し、それに伴うサイバー保険金クレームの低減に努める（13 ページを参照）など、サイバー保険市場に大きな変化をもたらしました。

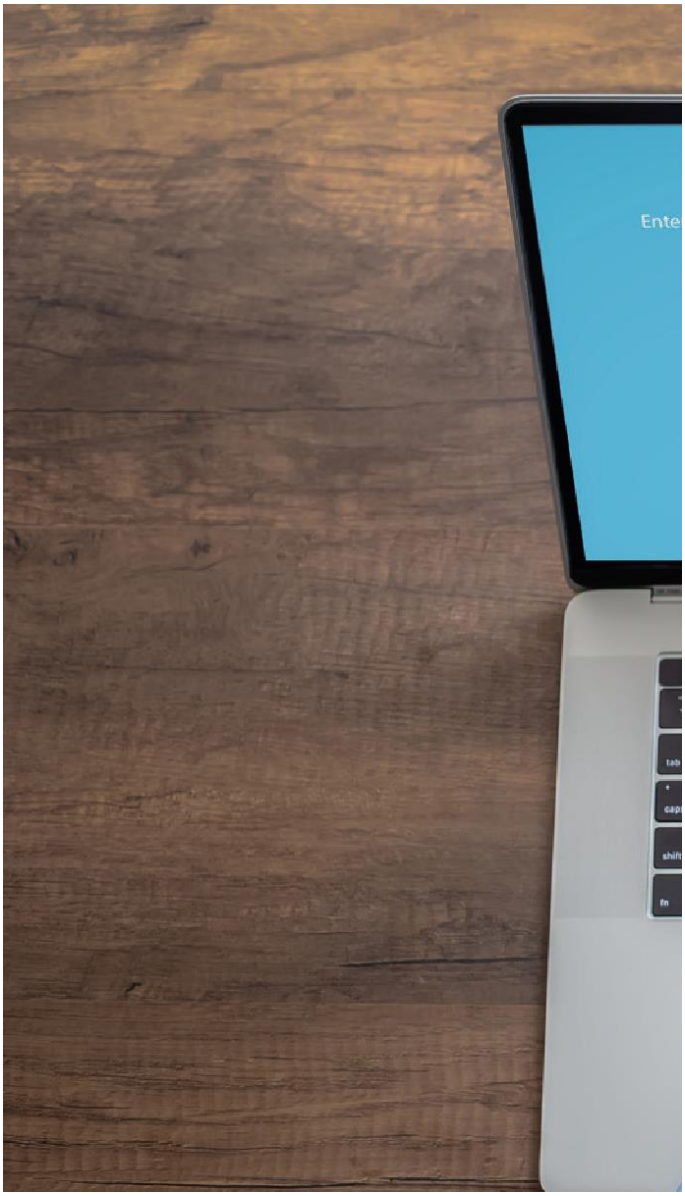
また、サイバー保険料率が上昇する一方で（ブローカーの Marsh 社[17]によれば、米国の保険料率は 2021 年の第 2 四半期だけで 50%超上昇）、キャパシティは引き締められています。アンダーライターは、各組織が導入するサイバーセキュリティ管理の精査を強化するとともに、それに応じたリスクの価格設定を行っています。

今も昔も、保険の役割は優れたリスクマネジメントと損失防止を促進するというものですが、そのルーツは数百年前、初期の工場や蒸気ボイラーにかけられた保険の時代にまで遡ることができます。ランサムウェアは現在も進化を続けるリスクですが、保険会社は企業と協力して、セキュリティ体制を改善するためのベストプラクティスと基準の特定に取り組んでいます。

保険各社はまた、リスク選好の判断に役立つ特定のサイバー引受基準を確立しています。「それによってサイバーリスクマネジメントとセキュリティへの期待を明確に伝えることができます。商業顧客が基準を満たすことができれば、ランサムウェア攻撃と保険確保の面で、立場がより有利になります」と Baviskar は話します。

4 社に 3 社は AGCS のサイバーセキュリティ関連の要件を満たしていませんが、多くのお客様が AGCS との協力の下、基準を満たし、リスクを低減することに取り組んでいます。「このアプローチは、企業のサイバーセキュリティへの投資を促進するとともに、最高情報セキュリティ責任者（CISO）にとっては取締役会との話し合いの際の説得材料となるはずです」と Baviskar は話します。

17 Marsh 社：「グローバル保険市場指数 - 2021 年 Q2」（Global Insurance Market Index - 2021 Q2）



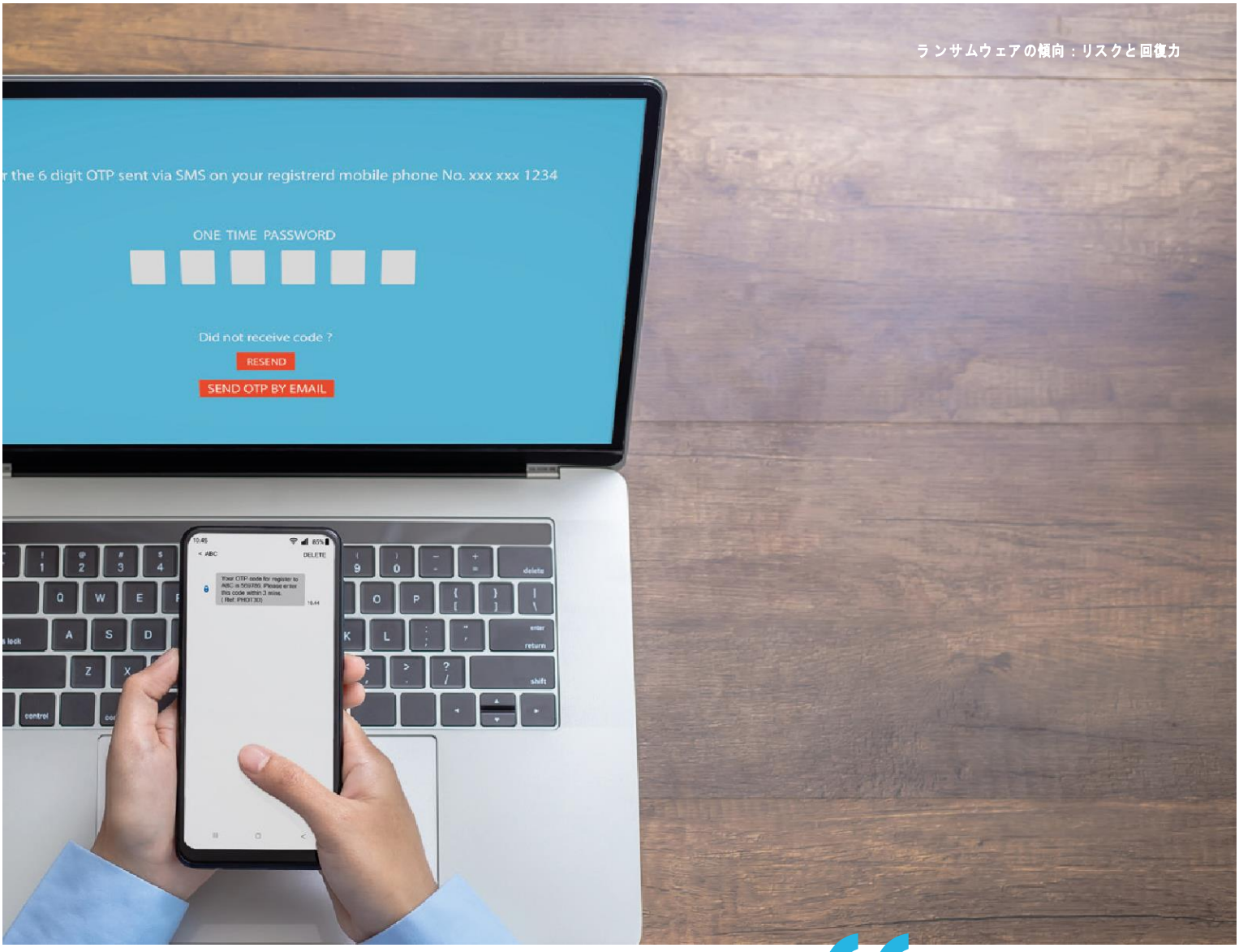
優れたサイバー衛生 – リスクマネジメントは報われる

ランサムウェア攻撃の大部分はサイバーセキュリティを強化することで防ぐことができますが、それでも攻撃者の侵入が起きた場合、堅牢な事業継続計画とインシデント対応計画を立てておくことで、インシデントの影響を大幅に抑えることができます。

ヨーロッパで実施された大規模ランサムウェアクレームの分析では、攻撃の大部分は回避できることを示唆しています。「組織がベストプラクティスに従っていれば、約 80%のランサムウェア・インシデントで損失が回避できたはずです。多くの場合、損失の主な要因は多要素認証がなかったこと（リモートアクセス、特権的 IT アカウント、リモートメンテナンスなどで）または教育が不十分だったことであることが分かっています」と Daum は説明します。

ランサムウェア攻撃を回避するためには、定期的なパッチの適用と 2 要素認証、および情報セキュリティと意識教育、さらには良好なサイバー衛生が不可欠となります。エンドポイント検知と対応（EDR）サービス、ランサムウェア対策ツールキットやサービスなどのサイバーセキュリティツールも、攻撃の防止、脅威の検知、インシデント対応の迅速化に役立つと Baviskar はいいます。

事前のプランニングと対応のスピードによって天と地ほどの違いが出かねないランサムウェア攻撃の場合、その影響を軽減する鍵となるのはインシデント対応と事業継続計画です。対応計画は各種のランサムウェアシナリオに則して定期的にテストする必要があり、さらには役割、責任、情報伝達系統を明確に定義しておく必要があります。また、攻撃の影響を軽減し、復旧と事業継続をスピードアップするためには、重要なシステムやデータのバックアップをはじめ、頻繁なバックアップを行うことも重要です。



ランサムウェアなどのサイバー脅迫イベントが発生した場合、企業はインシデント対応計画[18]に従い、特に上級管理職と法務部門に通知する必要があります。法務部門が最初から関与することで、データ漏洩の結果として起こされる可能性のある集団訴訟やその他の法的請求にさらされるリスクを減らすことができます。また、該当するサイバー保険契約の対象となるかどうかを判断するために、攻撃発生時に保険会社に通知をすることが推奨されています。

最終的な補償範囲の確認とは関係なく、サイバー保険契約者は通常、クレーム後の最初の 48 時間または 72 時間の間、緊急インシデント対応サービスを 24 時間年中無休で利用できるというメリットがあります。これらのサービスに通常含まれるものとしては、専門の危機管理者、IT 科学捜査サポート、および法律顧問などがあります。この他のサービスとしては、従業員向けのオンライン IT セキュリティ教育や、サイバー危機管理計画の作成支援などがあります。

「多くの企業の場合、サイバーセキュリティ、管理体制、および手順を改善すれば、十分な防護を実現することができ、ランサムウェア攻撃の影響を受ける可能性を大幅に減らすことができます。通常、ハッカーがまず攻撃するのは防御力が弱い企業です」と Daum は話します。

> 通常、ハッカーがまず攻撃するのは防御力が弱い企業です。

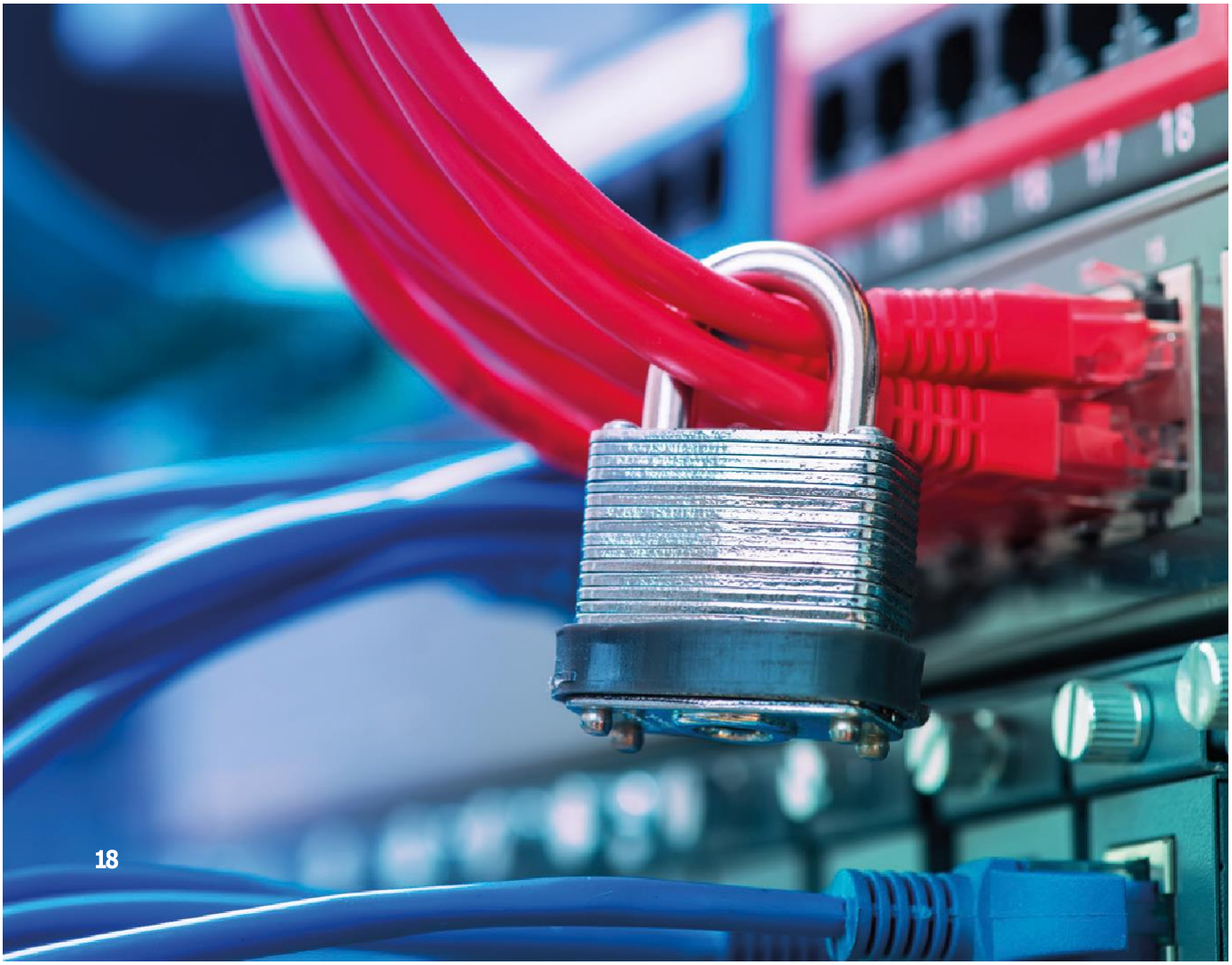
18 Harvard Business Review 誌：「サイバー攻撃は避けられない。あなたの会社の備えは？」（Cyberattacks Are Inevitable. Is Your Company Prepared?）2021 年 3 月 9 日

持続可能な保険市場の創出

犯罪者はサイバーセキュリティと管理体制が弱い組織に注力するので、ベストプラクティスの推奨事項と引受基準を順守していれば、ランサムウェア攻撃の発生を減らすことができます。また、依然として遅れをとっている部分も数多くあるので、企業が IT セキュリティの改善に継続的に投資することも重要となります。セキュリティの欠陥は多くの場合、簡単な対策で解消することができます。保険会社は、クライアントと協力してサイバー攻撃のリスクを低減することで、サイバー市場の長期的な持続可能性を確保することができると Stanislawski は説明します。

「大多数の企業にとって、ランサムウェアは一朝一夕になくなる問題ではありません。とはいえ、これは私たちのクライアントにとって解決できる問題である可能性は高いのです。ドアの開いている家は、鍵のかかった家よりも強盗に遭う可能性ははるかに高くなります。私たちはクライアントとの継続的な協力の下、ランサムウェア防衛のベストプラクティスを特定し、推進しています」と Stanislawski は話します。

ランサムウェアが政府や企業レベルでも注目されていることを考え合わせると、楽観視する理由も十分にあると Kang はいいます。「ランサムウェアによる損失は保険会社や企業にとって痛手となっており、これがリスク軽減とサイバーセキュリティへの企業の投資を後押ししています。持続可能な保険商品を作り上げるには、全員で力を合わせる必要があります」。



ランサムウェア防衛 — 優れたITセキュリティとはどのようなものか？

ランサムウェアの特定：
- ランサムウェア対策ツールセットを組織全体に展開しているか？
- ランサムウェアの脅威を特定するために、どのような積極的措置を講じているか？
- ランサムウェアの脅威に対処するために、ポリシー、手順、アクセス管理体制、情報伝達系統は頻繁に更新されているか？
- ランサムウェアの種類を特定するための社内機能や外部手配は整っているか？

事業継続計画／インシデント対応計画：
- ランサムウェアに特化したインシデント対応プロセスは導入しているか？
- 過去にランサムウェア・インシデントに遭ったことはあるか？ある場合、どのような教訓が得られたか？
- 事前契約のIT科学捜査会社やランサムウェア対策サービスプロバイダーの手配は整っているか？

フィッシング対策の演習と利用者の意識向上教育：
- 情報セキュリティ、フィッシング、電話詐欺、なりすまし電話、ソーシャル・エンジニアリング攻撃に関して、定期的な利用者教育と意識向上教育を実施しているか？
- ソーシャル・エンジニアリングやフィッシングのシミュレーション演習は継続的に実施しているか？

バックアップ：
- 業務中断の影響を最小限に抑えるために、重要システムの頻繁なバックアップをはじめ、定期的なバックアップを行っているか？オフラインのバックアップも行っているか？
- バックアップは暗号化されているか？バックアップは複製を作成し、複数のオフサイトの場所に保存されているか？
- 目標復旧時間（RTO）内に主要資産の復元と復旧を完了するためのプロセスを導入しているか？
- バックアップの整合性を確保するために、定期的にデータを取り出して元データと照合しているか？

エンドポイント：
- 組織全体のモバイルデバイス、タブレット、ノートパソコン、デスクトップパソコンなどで、エンドポイント保護プラットフォーム（EPP）製品とエンドポイント検知と対応（EDR）ソリューションを活用しているか？
- エンドポイントにローカル管理者パスワードソリューション（LAPS）を実装しているか？

電子メール、Web、オフィス文書のセキュリティ：
- センダー・ポリシー・フレームワークを厳密に実施しているか？
- 電子メールゲートウェイは、潜在的に悪意のあるリンクやプログラムを探知するように構成されているか？
- ソーシャルメディア・プラットフォームへのアクセス制限を伴った、Webコンテンツフィルタリングを実施しているか？

セグメンテーション：
- クラウド環境をはじめ、ネットワーク内で物理的、論理的な分離が維持されているか？
- 全体的な攻撃対象域を減らすために、マイクロ・セグメンテーションとゼロ・トラスト・フレームワークを導入しているか？

パッチ適用と脆弱性管理ポリシーの監視：
- 脆弱性を検出するための自動スキャンは実行しているか？サードパーティーによる侵入テストは定期的に行っているか？
- 適切なアクセスポリシーを確実に実施し、重要なデータアクセス、リモートネットワーク接続、および特権的ユーザーアクセスに対して多要素認証を確実に行っているか？
- 不審なアカウント挙動、新規のドメインアカウントおよびアカウント特権の昇格（管理者レベル）、新規サービスの追加、短期間のうちに実行される不審なコマンドチェーンを検出するための継続的な監視を実施しているか？

M&A：
- M&Aに先だって、どのようなデュー・デリジェンス（due diligence ＝ 当然に実施すべき注意義務および努力）とリスク管理を行っているか？
- セキュリティ管理体制の評価を確実に行うために、新たに統合された組織に対して定期的なセキュリティ監査を実施しているか？

これらの推奨事項はすべて、リスク管理の観点から見た技術的な性格のアドバイスであり、業務によっては適用されない場合もあります。推奨事項は注意深く確認し、実装する前に、どうすれば特定ニーズに最適に適用できるかを判断して下さい。保険の補償内容に関する質問については、アンダーライター、代理人、ブローカーの現地連絡先にお問い合わせ下さい。

連絡先

詳しくは、お近くのAllianz Global Corporate & Specialtyのコミュニケーション・チームにお問い合わせください。

Asia Pacific
Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

Central and Eastern Europe
Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

Ibero/LatAm
Camila Corsini
camila.corsini@allianz.com
+55 11 3527 0235

Mediterranean/Africa
Florence Claret
florence.claret@allianz.com
+33 158 858863

North America
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 212 553 1287

Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

UK, Middle East, Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

Global
Hugo Kidston
hugo.kidston@allianz.com
+44 203 451 3891

Heidi Polke-Markmann
heidi.polke@allianz.com
+49 89 3800 14303

詳しくは下記にお問い合わせください：agcs.communication@allianz.com

Allianz Global Corporate & Specialtyは下記にてフォローいただけます：

Twitter @AGCS_Insurance #cyberrisktrends

LinkedIn

www.agcs.allianz.com

Allianz Global Corporate & Specialty SE
Dieselstr.8, 85774 Unterfoehring, Munich, Germany
画像：Adobe Stock
通貨表記は特に記載のないかぎり米ドル表記としました。
2021年10月