アリアンツ・コマーシャル

サイバーセキュリティの動向 2023

最新の脅威とリスク軽減のための最適解

―ハッキング前、ハッキング中、ハッキング後

目次

3ページ
はじめに

5ページ
脅威の状況：
復活したランサムウェアの標的はデータとサプライチェーン

14ページ
今後の脅威：
AI、IoT、スキル不足が 将来のサイバー攻撃を助長

18ページ
保険金請求：
安定化傾向は集団攻撃とデータ漏洩によって脅かされている

24ページ
軽減策：
新たなサイバー脅威と戦うには早期発見が鍵

はじめに

サイバーセキュリティへの投資は実を結んでいますが、脅威となる状況は進化しており、早期発見と対応能力に一層注力する必要があります。

サイバーセキュリティと事業継続性の向上により、暗号化ベースのランサムウェア攻撃への対策が進んでいますが、サイバー脅威の状況は絶えず進化しています。2023年には、ランサムウェアと恐喝の請求が再び増加し、その結果、高額なインシデントが増加しました。これは、対策は進んでいるものの、ランサムウェアによる脅威が弱まる兆しがほとんどないことを示しています。

報告書によると、ランサムウェアの被害者数は2023年第1四半期に世界全体で143%も急増し、1月と2月にはハッキングと情報漏洩の件数が過去3年間で最多となりました。ランサムウェア単独でもその被害額は、2031年までに年間約2,650億ドルに上ると予測されています。

ハッカーがITや物理的なサプライチェーンを標的にし、大規模なサイバー攻撃を仕掛け、企業の規模を問わず金銭を脅し取る新たな方法を見つけることが増えています。現在、ほとんどのランサムウェア攻撃は、恐喝を目的として個人データや機密性の高い商用データを盗取するため、コストと複雑性がさらに増し、風評被害や第三者への賠償責任が発生する可能性も高まっています。アリアンツが保険業界の大規模なサイバー損害について分析したところ、データが流出したケースの割合は年々増加しており、2019年には事件全体の40%でしたが、2022年にはその割合が約77%に達し、2023年には昨年の合計を上回る勢いです。

侵入者から組織を守ることは『いたちごっこ』であり、サイバー犯罪者は依然として優位に立っているのです。脅威の主体は現在、人工知能（AI）を使用して攻撃を自動化し、加速する方法を模索しており、より効果的なAIを搭載したマルウェアやフィッシングを作成しています。接続されたモバイル機器や5G対応のIoT（モノのインターネット）の爆発的な増加と相まって、サイバー攻撃の手口は今後数年間で増加する可能性があります。

143%

2023年第1四半期のランサムウェア被害者数は世界的に増加

ハッキングと情報漏洩の件数が過去3年間で最多

$2,650億

2031年までにランサムウェアが被害者にもたらす年間コストの概算額

サイバー攻撃を防ぐことはますます難しくなり、その掛け金も高くなっています。その結果、早期の検知と対応能力がますます重要になっています。アリアンツの分析によると、侵入は急速に拡大し、いったんデータが暗号化されたり盗まれたりすると、その影響とコストは雪だるま式に増大します。そのコストは、インシデントを早期に検出して封じ込めなかった場合と比べて1,000倍、あるいはそれ以上になる可能性があることを分析は示しています。

最終的には、早期発見と効果的な対応能力が、サイバー攻撃の影響を軽減し、今後も持続可能な保険市場を確保するための鍵となります。

脅威の状況：復活したランサムウェアの標的はデータとサプライチェーン

ランサムウェアは依然としてサイバー脅威のトップであり、サイバー保険金請求における唯一最大の原因となっています。ランサムウェアの攻撃頻度は、2022年の一時的な中断を経て、2023年に再び増加しています。これは、脅威行為者がデータ流出やサプライチェーン攻撃を利用して最大限の影響力を行使しているためです。

ランサムウェア犯罪者にとって、この12か月間は様々な意味でいつも通りの日々でした。サイバーセキュリティの変化に対応し、企業や公的機関から金銭を脅し取る新しい方法を見つけながら、彼らは戦術やビジネスモデルを進化させ続けています。

サイバー脅威インテリジェンス企業 Black Kite[1]の調査によると、ランサムウェア攻撃は2023年初頭に急増し、3月の被害者数は昨年4月の約2倍、2022年のピーク時の1.6倍に達しました。アカマイテクノロジーズによると、2023年第1四半期[2]にランサムウェアの被害者数は世界全体で143%急増しました。一方、NCCグループによると、2023年1月と2月は、ランサムウェアによるハッキングと情報漏洩の件数が過去３年間で最多となり、ランサムウェアの活動も2023年５月時点[3]で前年同期比約50%増となっています。今後、ランサムウェアだけで2031年までに年間約2,650億ドルの被害が発生するとサイバーセキュリティ・ベンチャーズは予測しています[4]。

2023年にはLockBitやClopなどのデータ流出攻撃が急増し、攻撃件数が新たなレベルに達しています。Chinalysis社によると、ランサムウェアの被害者数は今年上半期に4億4,910万ドル[5]を支払い、すでに昨年の合計5億ドル迫る勢いです。現在のペースでは、2023年はランサムウェアの収益が2021年に次いで2番目に大きい年となる可能性があります。

重要な変化

- ランサムウェアグループは、サイバーセキュリティの変化に応じて戦術とビジネスモデルを適応させ続けています。
- Ransomware-as-a-Service (RaaS＝サービスとして提供されるランサムウェア）は、依然として攻撃頻度を増加させる重要な要因となっています。
- 二重、三重の恐喝攻撃は新しいものではなく、現在ではより一般的になり、潜在的に影響を受ける可能性があります。企業にとってはコストもかかります。
- サプライチェーンを利用したランサムウェア攻撃は、今やランサムウェア戦略の一部として確立されています。
- 大規模なランサムウェア攻撃が増加していることから、保険会社は企業間やデジタル・サプライチェーン内に存在する相互接続性や依存関係をより深く理解する必要があります。

今年は、ソフトウェアやITサプライチェーンの脆弱性を悪用し、複数の企業を標的とした大規模なランサムウェア攻撃が発生しました。同時に、ランサムウェア集団は、より多くの攻撃をより迅速に実行するために、ビジネスモデルの微調整を続けています。IBM X-Force[6]の調査によると、ランサムウェア攻撃の実行にかかる平均日数は、2019年の60日以上から2021年には4日未満に短縮されています。

6月、ランサムウェア集団Clopは、数千の企業に影響を与え、数百万人の個人と企業のデータを危険にさらしたと考えられる大規模なサイバー攻撃を成功させました。Clopは、ファイル転送ソフトウェアMOVEitの「ゼロデイ」の脆弱性を悪用し、企業や公的機関からデータを盗み出し、身代金を支払わなければデータを公開すると脅迫しました。

この攻撃は、エネルギー大手Shell, British Airways, BBC, DHL, 保険会社Genworth Financial,米国の保険福祉省とエネルギー省など、多くの大企業や省庁に影響を与えました[7]。Genworth Financialだけでも、約250万人から270万人の顧客の個人情報が流出したと報告されています[8]。Clopは現在、被害者数で2番目に大きいランサムウェアグループです。

Rishi Baviskar (Global Head of Cyber Risk Consulting, Allianz Commercial) は、次のように述べています。「企業がネットワーク・セキュリティやバックアップ戦略を強化し、規制が企業に対し身代金の支払いを思いとどまらせる中、暗号化ランサムウェア攻撃が成功する可能性は低くなっており、脅威の主体は戦略を変えつつあります。最近のMOVEitサプライチェーン攻撃は、犯罪組織が集団攻撃やデータ流出にますます頼るようになっていることを示す良い例です」。

事件の大半はRaaSグループが原因

Ransomware-as-a-Service (RaaS) は、依然として攻撃頻度の主な要因となっています。RaaSキットとサービスにアクセスできるため、独自のマルウェアを開発するスキルを持たない犯罪者でも、迅速かつ安価にランサムウェア攻撃を仕掛けることができます。RaaSキットの価格は月額40ドルからで、サイバー犯罪者はわずかな金融投資で恐喝によって数百万ドルを稼ぐことができます。

Michael Daum (Global Head of Cyber Claims at Allianz Commercial) は、「この問題は決してなくなるものではありません。私たちはしばしば同じ攻撃グループを相手にしています。彼らは姿を消し、再編成され、名前を変えて再び現れます。しかし、優れた手口を持つグループは最も大きな利益を上げ、そのツールや専門知識を他者に再販し始めるのです。彼らは成功した企業のように活動しているのです」と言います。

大企業に対するランサムウェア攻撃は通常、比較的少数のグループから発生します。例えば、アリアンツは、Black Basta, Clop, およびLockBitに起因する複数の保険金請求を処理しました。米国 Cybersecurity and Infrastructure Security Agency[9]によると、LockBitは2022年以降、米国だけで1,700件以上の攻撃があり、約9,100万ドルの身代金が支払われました。

「サイバー犯罪者の手口は進化し続けています。ランサムウェアといえば、攻撃者が金銭を脅し取るために様々なテクニックを駆使することを意味します。以前は暗号化が行われていましたが、現在では、攻撃者がデータを盗んだり、身代金を要求するために暗号化を適用しなかったり、また暗号化と組み合わせてデータを盗んだり、分散型サービス拒否(DDoS)攻撃を実行したりすることが見られます」と、Daumは続けます。

RaaSキットを使用すると、サイバー犯罪者は恐喝要求により数百万ドルを稼ぐことができます。価格の例は以下のとおり

月額40ドル

LockBitは、2022年に世界中で最も導入されたランサムウェアの亜種であり、その数は以下のとおり

1,700+

2022年以降に米国で発生した攻撃

9,100万ドル

身代金の概算額

データ流出の常態化

二重、三重の恐喝（暗号化、データ流出、分散型サービス拒否（DDoS）攻撃を組み合わせて金銭を脅し取ること）は目新しいものではありませんが、現在ではより一般的になっており、被害を受けた企業にとってより大きな影響をもたらし、コスト負担になる可能性があります。

アリアンツが2019年から2023年上半期末までの間に保険業界で発生した大規模なサイバー損害（100万ユーロ超）を分析したところ、データが流出した事案の割合は年々増加しており、2019年には40%だったものが、2022年には約77%に達し、2023年には2022年の合計を上回る勢いです。

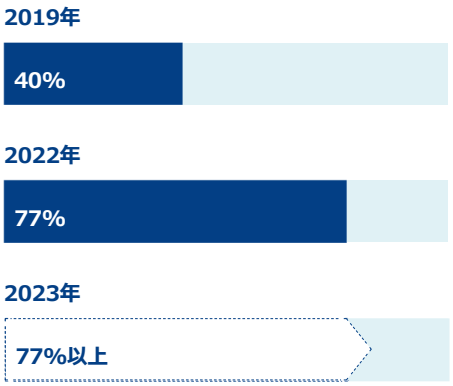
いったん脅威者が システムに侵入すると、データを盗むことよりも暗号化する方がはるかに難しいと、**Michael Daum (Global Head of Cyber Claims, Allianz Commercial)** は説明します。「攻撃者は暗号化を試みる前に、100%データを抜き取ろうとします。その方が、被害者の環境を完全に暗号化するよりも速く、簡単だからです。恐喝を目的とした侵入のほとんどすべてにおいて、データは抜き取られます」。

いくつかの要因が組み合わさることで、脅威行為者にとってデータの流出はより魅力的なものとなっています。収集される個人情報の範囲と量は増加する一方、プライバシーとデータ侵害に関する規制は世界的に強化されています。同時に、アウトソーシングやリモートアクセスの傾向により、脅威者が悪用できるインターフェースが増加しています。

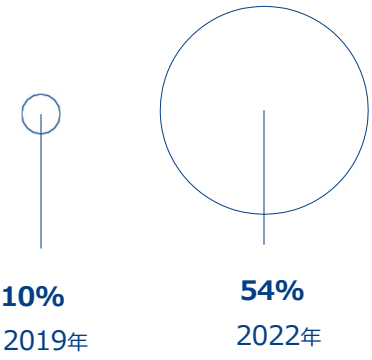
データが盗まれた場合、金銭的にも風評的にも大きな損害を被る可能性があり、企業は身代金の支払いをより強く迫られる可能性があります。2019年から2023年上半期末までの間に保険業界で発生した大規模なサイバー被害（100万ユーロ超）の数々をアリアンツが分析したところ、身代金を支払う企業の割合も年々増加しており、2019年にはわずか10%だったのが、2022年には54%に達しています。

一方、暗号化に加え、データが流出した事案では、身代金を支払う可能性が2.5倍高くなることも分析されています（データが流出した場合に身代金を支払う企業の割合は56%であるのに対し、データが流出しなかった場合に身代金を支払う企業の割合はわずか21%）。しかし、最近の大量ハッキングでは、支払いを拒否する企業も少なくありません。

データが流出する事件の割合は年々増加



身代金を支払う企業の割合は年々増加



比較すると

2.5倍

データが流出した場合、企業は暗号化に加えて身代金を支払う可能性が2.5倍高くなります

ランサムウェアのコスト – 二重恐喝により ルールが変更され、コストが倍増する

『従来型』ランサムウェア攻撃による潜在的コスト
（攻撃された企業のデータを流出させることなく暗号化）

ランサムウェア攻撃がもたらすデータ流出（データを盗み出し、公開すること）による
潜在的な追加コスト

費用の詳細：

単一記号（暗号化）

恐喝金：犯罪者による要求

逸失利益（事業の中断）：システムへのアクセスが制限される期間が長ければ長いほど、損失は大きくなります。

復旧費用： データを復元し、システムを完全に復旧させるための費用

情報解析費用：セキュリティ脆弱性の原因を調査するために発生する費用

二重の恐喝（暗号化と流出）

告知費用： 顧客、規制当局、その他の必要な関係者にデータ侵害を通知します。

監視費用： データを盗まれた個人に提供しなければならない個人情報盗難/詐欺の監視サービス

規制上の罰金と訴訟費用：個人情報が盗まれた第三者からの請求によるもの

データ復旧とPR修復： 悪評の影響を抑えるためのコンサルタント、危機管理会社、法律事務所の費用

出典: Bitsight and Kovrr. 図表: アリアンツ・コマーシャル

「しかし、流出したデータに対して身代金を支払ったからといって、必ずしも問題が解決するわけではありません。特に米国では、企業はデータ流出に対する第三者からの訴訟に直面する可能性があります。企業がデータ流出の身代金を支払ったところで、それが詐欺に使われたり、闇サイトで売られたりしないという保証はどこにもありません」と、Daumは言います。

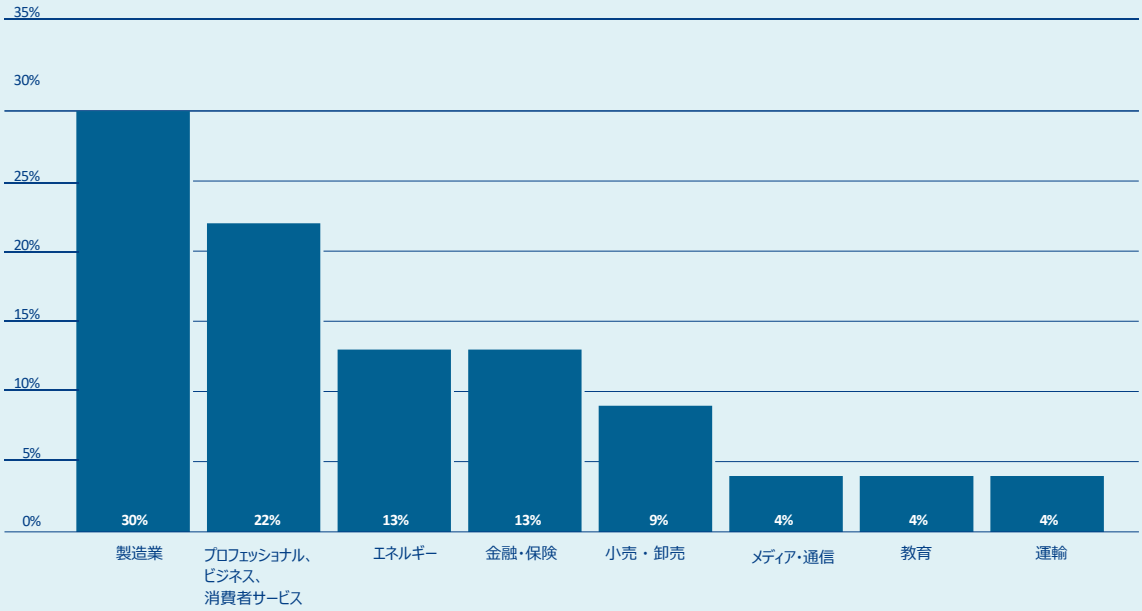
実際、システムまたはデータに再アクセスできるようにするためには、身代金を支払う以外に解決策がないと企業が考えるケースはほとんどありません。被害を受けた企業は、常に警察または国の捜査当局に情報提供し、協力する必要があります。

これまでは、個人情報やクレジットカード情報を保有する企業が情報漏洩の標的となっていましたが、エコシステムを共有する産業・製造業がデータ流出攻撃の被害に遭うケースが増えています。IBM Securityの2023X-Force-Threat Intelligence Index[10]によると、製造業はランサムウェアによるサイバー攻撃の標的となる可能性が極めて高い業界であり、2022年に最も恐喝された業界でもありました。

「データ漏洩を利用すると、さまざまな顧客を持つ標準的な製造会社を攻撃できます。これらの取引先のデータも入手できれば、犯罪者は彼らにも金銭を要求することができ、それは現在いくつかの保険金請求で見られることです」と、**Jens Krickhahn(a Regional Practice Leader, Cyber Insurance, Allianz Commercial)** は言います。

標的とされた主要産業

2022年のインシデント対応業務で観察された恐喝事件の業種別割合



数値は四捨五入のため合計が100%にはなりません。

出典: IBM Securityの 2023年X-Force脅威インテリジェンス指数
(IBM Security's 2023Threat Intelligence Index)

脅迫行為者はサプライチェーンの弱点を狙っています。

サプライチェーンを利用したランサムウェア攻撃は新しいものではなく、今やランサムウェアの常套手段となっています。脅迫の当事者は、ITサプライチェーン内の企業や、物理的なサプライチェーンで機密データを保持する企業を標的とし、複数の企業から恐喝して金銭を要求するケースが増えています。

サプライチェーン攻撃は2019年に初めて話題になりました。
これは、システム管理会社Solar Windsへの侵入であり、史上最大規模のソフトウェア・サプライチェーン攻撃の始まりとなりました。2021年には、IT管理企業のKaseyaが、同社のリモート管理ソフトウェアのゼロデイ脆弱性を悪用してランサムウェア攻撃を行い、約1500の企業に影響を与えたと考えられ[11]、7,000万ドルの身代金が要求されました。

メディア報道によると、2023年6月、北朝鮮のハッキンググループ[12]が仮想通貨企業を標的にするため、SaaSプロバイダーのJumpCloudに侵入しました。ブロックチェーン分析会社Chainalysisは昨年、北朝鮮に関連するグループが複数のハッキングを通じて推定17億ドル相当のデジタルキャッシュを盗んだと発表しました。

「多くの顧客を有するITサプライヤーを攻撃することで、恐喝力はさらに大きくなります。一度に一社だけでなく、多くの企業を攻撃することになります」と、**Michael Daum（Global Head of Cyber Claims, Allianz Commercial）**は言います。

サプライチェーンのサイバー攻撃は通常、高度な国家ハッカーグループによるものと考えられていましたが、RaaSグループが大規模なランサムウェア攻撃を仕掛けるために利用されることが増えています。 最近のMOVEitによる恐喝と同様に、ランサムウェア犯罪者集団は現在、デジタルおよび物理的なサプライチェーンの相互接続性を悪用する機会を虎視眈々と狙っており、より堅牢なサイバーセキュリティを回避してサプライチェーンの他の企業に侵入するために、サイバーセキュリティが脆弱な組織を標的にします。

「ITプロバイダーは高度なサイバーセキュリティを備えていると思われがちですが、必ずしもそうとは限りません。不備があったインシデントの数が増えています。大規模な攻撃者グループは洗練されており、非常に知識が豊富で、興味深いデータを保持しているターゲットや、他の企業へのアクセスを許可するターゲットに惹かれ、それによって恐喝の支払いを要求したり、将来の攻撃を開始したりすることができます」と、Daumは言います。

大量攻撃で高まる危機感

2023年には、RaaSグループがソフトウェアの脆弱性やデジタル・サプライチェーンの相互接続性を悪用してデータを流出させ、何百もの企業に身代金を要求する、大規模なランサムウェアによる恐喝攻撃が複数発生しています。

Clopランサムウェアグループが、広く使用されているファイル転送ソフトウェアのゼロデイ脆弱性を悪用した最近のMOVEit攻撃に加え、2023年にはRaaSグループが同様の攻撃を開始しています。Clopは今年初めにも、ファイル転送ソフトウェアGoAnywhereのゼロデイ脆弱性を悪用して、130社以上からデータを盗み出しました[13]。また別の攻撃では、脅威行為者がパッチの適用されていないVMware ESXiサーバーの既知の脆弱性を悪用し、全世界で3,800台のサーバーを危険にさらしました[14]。

Jens Krickhahn (a Regional Practice Leader, Cyber Insurance, Allianz Commercial) によると、ランサムウェアによる大規模な攻撃は、複数の保険金請求を同時に引き起こすため、保険業界にとって「ゲームチェンジャー」となる可能性があるとのことです。

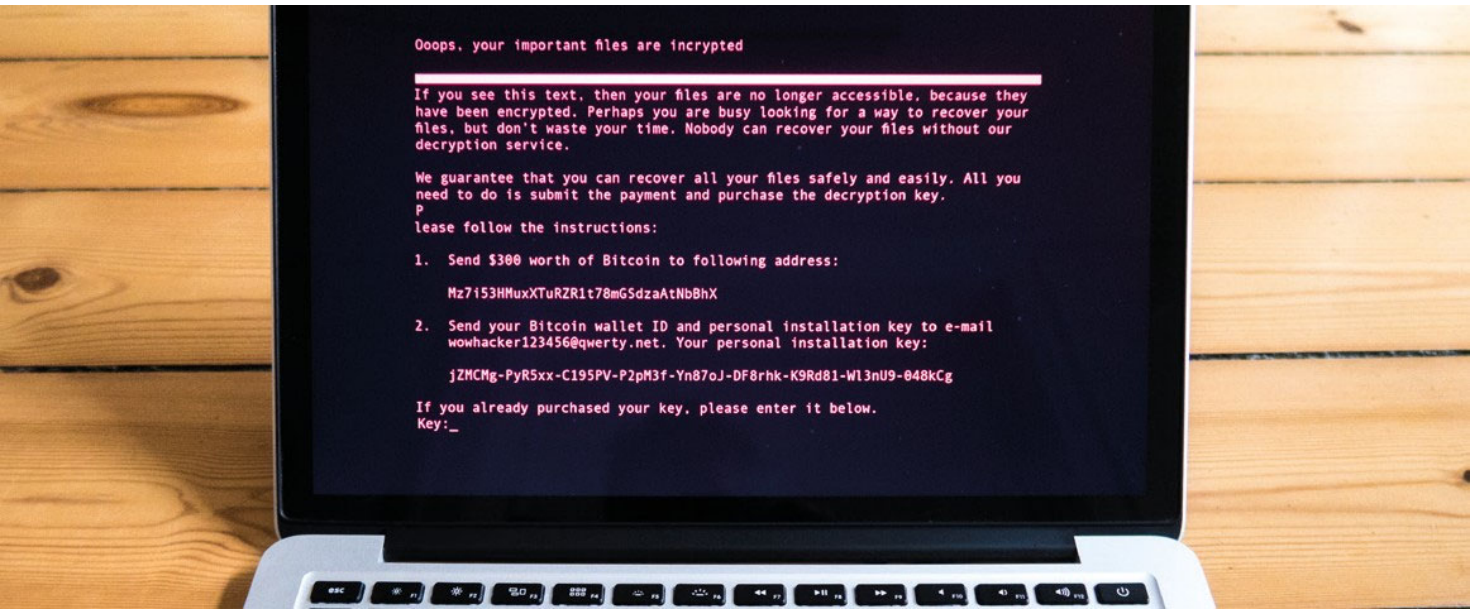
「今年、私たちは40の保険契約で同時にインシデントが発生するという状況を初めて経験しました。保険金請求の管理側では、複数の被保険者と同時に、同じテーマで、異なるサービス・プロバイダーやベンダーに対応しなくてはならないという新しい状況が生まれます。かつては理論上とされていた積みあがるリスクは、今や現実のものとなっています」と、Krickhahnは言います。

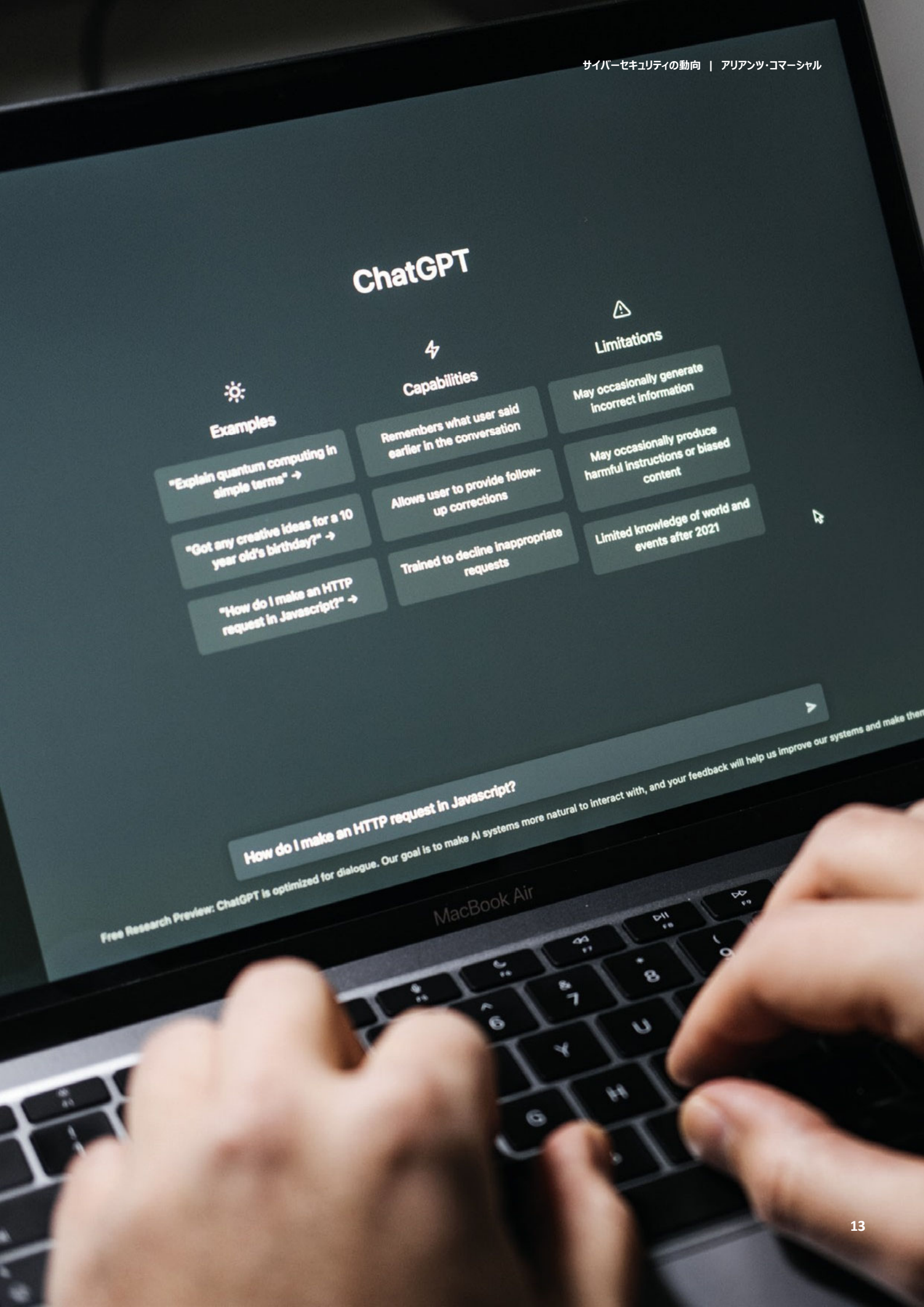
「大規模なITベンダーやデータセンター・プロバイダーに対する同様の攻撃が成功した場合、世界的な影響を及ぼし、保険業界に大きな影響を与える可能性があります」

「今日の知識を踏まえると、多くの保険会社がさまざまな業界やセクターに対するエクスポージャーをより慎重に検討し、補償だけでなくキャパシティ管理についても検討する必要があることは間違いありません。多くの企業が単一のベンダーに依存していることを知れば、保険会社はエクスポージャーを管理するために、集約条項などのソリューションを検討する必要があるかもしれません。

保険会社は、企業間およびデジタルサプライチェーン内に存在する相互接続性と依存関係をより深く理解したいと考えています」と、**Tresa Stephens (a Regional Head of Cyber, Allianz Commercial)** は付け加えます。

「被保険者とそのベンダーとの間の相互依存関係を見極めて追跡することが非常に難しいため、サイバーリスクの蓄積をモデル化することは困難です。被保険者だけでなく、私たちも多くのリスクを引き受けているようなものです。私たちはすべてのベンダーとサプライヤーを見ており、当社のポートフォリオにおける相互依存関係を理解する必要があります」。




ChatGPT
Examples
"Explain quantum computing in simple terms" →
"Got any creative ideas for a 10 year old's birthday?" →
"How do I make an HTTP request in Javascript?" →
Capabilities
Remembers what user said earlier in the conversation
Allows user to provide follow-up corrections
Trained to decline inappropriate requests
Limitations
May occasionally generate incorrect information
May occasionally produce harmful instructions or biased content
Limited knowledge of world and events after 2021
How do I make an HTTP request in Javascript?
Free Research Preview: ChatGPT is optimized for dialogue. Our goal is to make AI systems more natural to interact with, and your feedback will help us improve our systems and make ther
MacBook Air

今後の脅威: AI、IoT、スキル不足が将来のサイバー攻撃を助長

人工知能（AI）は、自動化された攻撃プロセス、より説得力のあるフィッシング、より迅速なマルウェア開発など、将来のランサムウェア攻撃を後押しすると広く推測されています。しかし、より効果的で迅速な検知と脅威インテリジェンスにより、サイバーセキュリティを強化することも可能なのです。

脅威行為者はすでに、ChatGPTのようなAIを搭載した言語モデルを使用してコードを作成しています。生成AIは、技術的に習熟していない脅威行為者が独自のコードを作成したり、既存のランサムウェアの新しい系統やバリエーションを作成したりするのに役立ち、潜在的に彼らが実行できる攻撃の数が増加する可能性があります。

Rishi Baviskar (Global Head of Cyber Risk Consulting, Allianz Commercial) は、次のように述べています。
「今後、悪意ある行為者によるAIの利用は増加し、さらに強力なサイバーセキュリティ対策が必要になることが予想されます。AIは、より自動化された攻撃を行うだけでなく、データを盗み出したり、データを汚染したりする新たなテクニックを開発するためにも利用できます。 AIとモノのインターネット（IoT）の普及や5Gの高速化などを組み合わせる可能性を考えると、深刻な問題が目前に迫っているのかもしれません」。

音声シミュレーションソフトは最近、サイバー犯罪者の武器に加わりました。2019年、英国のエネルギー・プロバイダーのCEOは、その親会社のトップらしき人物から電話を受け、サプライヤーに電信送金をするよう依頼された後、詐欺師に22万ユーロを送金しました。音声はAI[15]を使って生成されたものでした。

2023年8月、Google傘下のサイバーセキュリティ企業Mandiantの研究者は、フィッシング詐欺用に設計・販売されたディープフェイク動画技術の最初の既知の事例を記録しました。現行料金は 1分あたり20ドル、フル動画で250ドル、トレーニングセッションで200ドルでしたが、研究者らはハッカー・フォーラムで確認されたサービスが合法的なものかどうか、またディープフェイクが詐欺に使用されたかどうかを確認することはできませんでした。

重要な変化

- AIを駆使した言語モデルと音声シミュレーションソフトがサイバー犯罪者の武器に最近加わりました。
- アリアンツは、モバイル機器にまつわるサイバーセキュリティの不備によって引き起こされるインシデントが増加していることを目の当たりにしています。
- サイバーセキュリティにおける技術的スキルの危機も、インシデントへの対応コストを増大させています。

Michael Daum (Global Head of Cyber Claims, Allianz Commercial) は、脅威行為者による増大する脅威に対抗するには、企業はAIを活用したサイバーセキュリティに投資する必要があると付け加えます。

「AIは脅威行為者を支援しますが、検知のための強力なツールでもあります。今後、AIを活用したサイバーインシデントが増えるかもしれませんが、AIに裏打ちされた検知への投資によって、より多くのインシデントを早期に発見できるはずです。私たちがAIの発展に歩調を合わせることができれば、企業にとっても攻撃者にとっても有利になることはなく、現在と状況があまり変わらない可能性が常にあります」。

モバイル機器による個人および企業データの漏洩

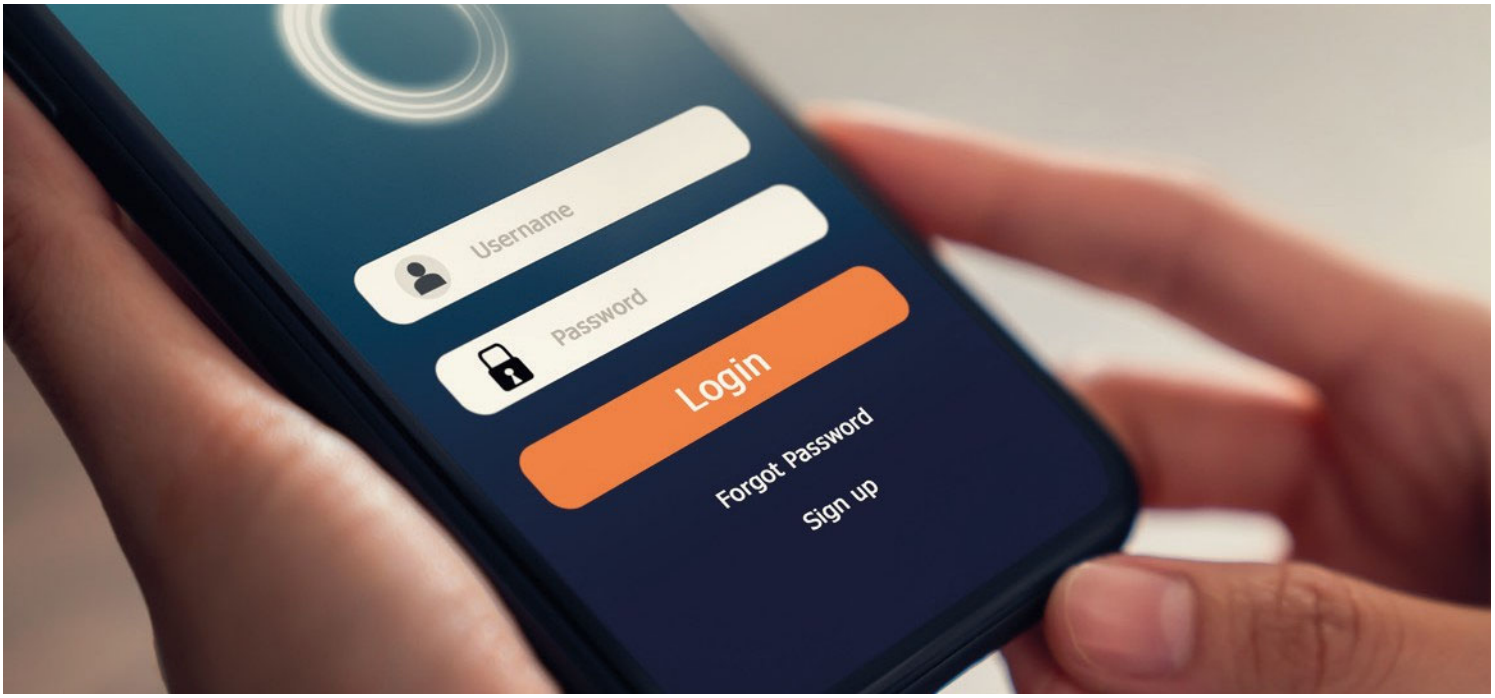
モバイル機器はセキュリティが甘く、個人データと企業データが混在しているため、サイバー犯罪者にとって魅力的な標的となっています。

アリアンツは、モバイルデバイスにまつわるサイバーセキュリティの不備に起因するインシデントが増加していることを目の当たりにしてきました。パンデミック（世界的大流行）の最中、多くの企業では、多要素認証（MFA）を必要とせず、プライベート・デバイスを経由して企業ネットワークにアクセスする新たな方法を可能にしました。その結果、多くのサイバー攻撃が成功し、その結果、多額の損害賠償請求が発生しました。

「**Rishi Baviskar (Global Head of Cyber Risk Consulting, Allianz Commercial)** は、次のように述べています。「サイバー犯罪者は現在、リモートアクセスやログイン認証情報の窃取、ランサムウェアの展開などを目的として、特定のマルウェアを搭載したモバイルデバイスを標的にしています。企業情報と個人情報が同じデバイスに保存されることが増えており、脅威行為者はこれを潜在的な脆弱性と見なしています。特に個人用のデバイスは、セキュリティ対策があまり厳しくない傾向があります。これらのデバイスで公衆Wi-Fiを利用することは、ソーシャルメディア経由のフィッシング攻撃にさらされることを含め、脆弱性を高める可能性があります」。

「5G技術の展開も潜在的な懸念事項です。5Gは、自動運転車やアシスト車、スマートシティなど、より高度なアプリケーションを含む、より多くのコネクテッドデバイスに電力を供給します。しかし、IoTデバイスはサイバーセキュリティに関してはあまり実績がありません」と、Baviskarは続けます。

「多くのIoTデバイスは本質的に安全ではありませんが世界的にこれらのデバイスの数が膨大になり、AIが加わることで、非常に深刻なサイバー脅威が発生する可能性があります。これらのデバイスの多くは容易に発見可能であり、MFAメカニズムを備えていません。現在でも、デフォルトのパスワードがインターネット上で公開されているデバイスを見かけます」と、Baviskarは言います。



サイバーセキュリティのスキル不足がコストと頻度に影響

サイバーセキュリティ専門家の不足が深刻化しているため、サイバーセキュリティへの取り組みはますます複雑になり、将来的に攻撃が成功する可能性が高まる可能性があります。

サイバーセキュリティ専門家のための非営利会員組織であるISC2[16]によると、現在世界のサイバーセキュリティ人材不足は340万人であり、サイバー専門家に対する需要は供給の2倍の速さで増加しています。組織の約70%は、効果を発揮するのに十分なサイバーセキュリティスタッフがいないと回答しています。Gartner社は、2025年までに重大なサイバーインシデントの半分以上の原因は人材の不足または人的ミスになるだろうと予測しています[17]。

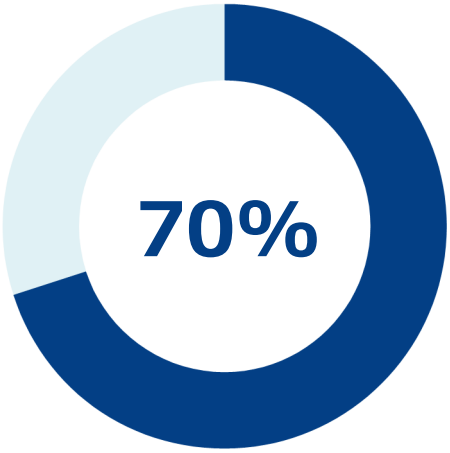
Rishi Baviskar, (Global Head of Cyber Risk Consulting, Allianz Commercial) は、「サイバーセキュリティの技術的スキルに危機が迫っています。テクノロジーの進歩が非常に速いため、脅威に対応できる経験豊富な人材が不足しています。優秀なサイバーセキュリティ技術者を確保するのは非常に難しく、これは企業がサイバー関連被害にあいやすくなることを意味します。熟練したサイバーセキュリティの人材がいなければ、インシデントの予測や防止が難しくなり、将来的に損失が拡大する可能性があります」と述べています。

サイバーセキュリティ専門家の不足も、サイバーインシデントへの対応コストに影響を与えます。IBMの「データ侵害コストレポート2023」によると、セキュリティスキルが高度に不足している組織のデータ侵害コストは平均536万ドル[18]で、平均コストより約20%高くなっています。

「ITスペシャリストは人材が不足しており、ITセキュリティの専門家はさらに不足しています」と、**Michael Daum (Global Head of Cyber Claims, Allianz Commercial)** は述べています。「攻撃やインシデントの量は、組織がITやサイバーセキュリティの専門家を雇用したり訓練したりするよりも速いペースで増加しており、供給が需要を上回ると、インシデント対応や科学捜査の料金がインフレ率よりも高くなります」。

現在、世界のサイバーセキュリティ人材の格差は次のとおり

340万人



効果的なサーバーセキュリティ対策に必要な人材が不足していると回答した組織の割合

保険金請求:
安定化傾向は集団攻撃やデータ漏洩によって脅かされている

過去2年間のサイバーセキュリティの改善により、ファースト・パーティの損害は抑制され、リスク全体の質も向上していますが、サイバー損害の請求件数は2023年上半期に再び増加しました。

2020年と2021年にランサムウェアによる損害が大幅に急増した後、昨年はサイバー保険金の請求件数が安定しました。これは、被保険企業におけるサイバーセキュリティとリスク管理の改善（多要素認証の使用やより効果的なバックアップ戦略など）を反映したもので、暗号化ベースのランサムウェアの効果を低下させ、事業中断の影響を軽減しました。同時に、ランサムウェアの一団を標的とする法執行機関やウクライナ・ロシア紛争が脅威行為者の活動を抑制したと考えられています。

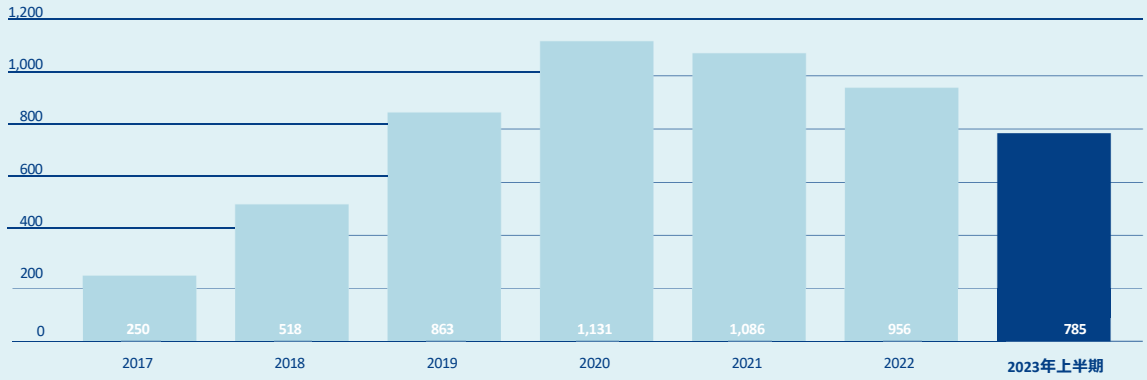
「多くの企業が脆弱性に対処し、M&A（合併・買収）をめぐるガバナンスに顕著な改善が見られました。以前はデューデリジェンスがITセキュリティやデータプライバシーの問題を発見できず、大規模な保険請求を数多く生み出してきたという歴史がありました。現在では、M&Aプロセスにおいて、IT資産やサイバーセキュリティに対する高いレベルでの配慮が見られるようになりました」と、**Tresa Stephens (a Regional Head of Cyber, Allianz Commercial)** は述べています。

しかし、ランサムウェアグループは手口を変え、データの流出や、ITサプライチェーンの弱点を突いた集団サイバー攻撃が増加しています。例えば、今年初めに1,000社を超える企業に影響を与えたMOVEit集団サイバー攻撃は、複数の保険契約者に同時に影響を与え、2023年の保険金請求件数の増加をもたらしました。

重要な変化

- ランサムウェアと恐喝ベースの攻撃は、件数と頻度の点で依然としてサイバー保険請求の最大の原因となっています。
- 米国では、恐喝の申し立てに加え、生体情報に関連するデータプライバシーに関する請求件数も増加しています。
- アリアンツが大規模なサイバー損害について分析したところ、データが流出したケースの件数が大幅に増加し、公表される事件の数も大幅に増加していることが示されています。
- アリアンツの損害賠償請求分析は、早期に発見されずに封じ込められた侵害は、費用が1,000倍も高額になる可能性もあります。

サイバー関連保険請求の年間件数



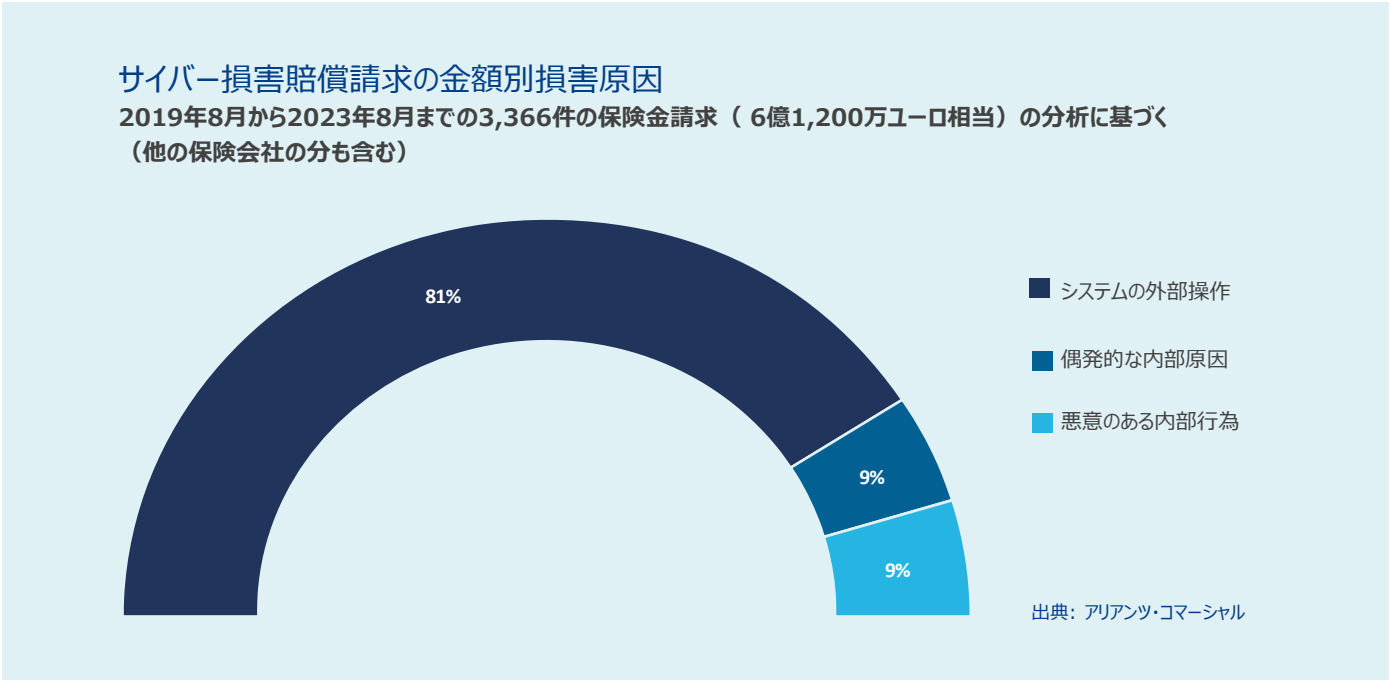
合計には、年間の全てのサイバー関連請求が含まれます。数値は報告内容の更新により今後変更される可能性があります。
出典: アリアンツ・コマーシャル

「昨年の保険金請求頻度の安定に続き、今年も保険金請求頻度がさらに上昇しました。 攻撃者は現在戻ってきており、より強力なツール、強化されたプロセス、攻撃メカニズムを用いて、再び西側経済に焦点を当てています」と、**Michael Daum (Global Head of Cyber Claims, Allianz Commercial)** は述べています。

ランサムウェアと恐喝による攻撃は、件数と頻度の点で依然としてサイバー保険金請求の最大の原因であり、単独のサイバー保険だけでの請求の80%以上を占めています。

「MOVEitはデータ転送ソフトウェア製品のゼロデイ攻撃で、数千の企業を襲い、数百万の個人に影響を与えました。米国では、主にデータ流出の恐喝による損害賠償請求が発生しています」と、**Marisa Anthony (Senior Complex Claims Handler, Cyber, Allianz Commercial)** は述べています。
「MOVEitが沈静化しても、また新たな攻撃が出てくることは十分に予想されます。サイバー攻撃は頻繁に発生することが予想されるため、早期発見・早期対応が重大性を抑制するカギとなります。保険会社として、私たちは企業間やデジタル・サプライチェーン内に存在する相互接続性と依存関係をよりよく理解する必要があります」。

> 攻撃者は現在戻ってきており、より強力なツール、強化されたプロセス、攻撃メカニズムを用いて再び西側経済に焦点を当てています。



注目されるプライバシーと賠償責任リスク

米国では、恐喝請求に加えて、音声や指紋データなどの生体情報に関連するデータプライバシー請求の件数も増加しており、組織がオンラインセキュリティを向上させるためにこれを管理する傾向が強まっています。同時に、多くの企業が、製品やサービス提供の一環として、あるいは販売やマーケティングを支援するために、位置情報、健康状態、行動などの個人情報を追跡しています。

米国にはデータプライバシーをカバーする連邦法はありませんが、カリフォルニア州プライバシー権法やイリノイ州生体認証情報プライバシー法（BIPA）など、多くの州が厳格な法律を導入しています。一方、データプライバシーおよびデータ侵害に関する集団訴訟の数は増加の一途をたどっており、原告らはこれを潜在的に利益が得られ、拡大する訴訟分野であると考えています。

「リスクの質が向上し、被保険者がサイバーセキュリティの強化に努めた結果、第一当事者からのサイバー賠償請求は以前の保険引受年度と比べ、ある程度安定しています。しかし、米国では規制や第三者賠償責任に関する動きも活発化しています。企業による生体認証データの利用はますます増えています。同時に、消費者のプライバシーの権利に対する意識も高まっており、この分野の規制は進化し続けています」と、**Tresa Stephens (a Regional Head of Cyber , Allianz Commercial)** は述べています。

個人情報保護に関する法律、裁判の判決や裁定はまだ進行中であり、企業や保険会社がデータプライバシー賠償責任のエクスポージャーを評価することを困難にしています。これは、より確立された損害賠償限度額よりも予測しにくいものです。

「私たちは、生体認証の関連の保険金請求、地理的追跡、音声と指紋、オンライン追跡の申し立てなど、訴訟の牽引力が高まっていることを目の当たりにしています。ほとんどの場合、これらの請求はすべてプライバシーの問題と、生体認証データがどのように収集され使用されるかを人々に知らせていないことに基づいています。このような請求は新しいものではありませんが、増加傾向にあり、原告側の弁護士がそのような請求を提起することがより容易かつより有益になる新たな有利な法律や判決が見られます」と、**Marisa Anthony (Senior Complex Claims Handler, Cyber, Allianz Commercial)** は述べています。「これらの訴訟を弁護するには、通常の一般賠償請求よりもはるかに費用がかかります。特に最近のインフレを考慮すると、侵害弁護および弁護人の時給は非常に憂慮すべきものになる可能性があります」。

データ流出とインフレが保険金請求コストを押し上げています

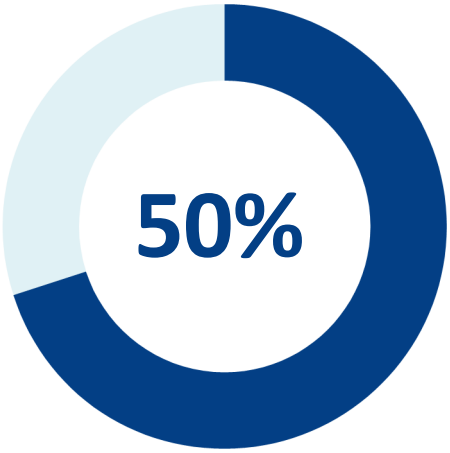
より巧妙な攻撃とインフレが、大規模なサイバー損害のコストを増大させています。組織とそのITインフラの規模や複雑さは、大規模なサイバー損害賠償請求のコストを増加させる重要な要因です。サイバー攻撃が一定以上進行すると第一当事者による復旧費用、事業中断、第三者賠償責任などが重なり、多額の損害が発生しやすくなります。

「事業部門、サプライヤー、世界中の拠点が異なるだけでなく、合併や買収もあるため、大規模な組織全体でサイバーセキュリティを管理することは非常に困難です。99%サイバーセーフであっても、1つでもドアが開いていれば、攻撃者はそれを見つける可能性があります。これは私たちがよく見てきたシナリオであり、一度大規模な組織が攻撃を受けると、多くの場合、多額の損失が発生します」と、**Michael Daum (Global Head of Cyber Claims, Allianz Commercial)** は述べています。

多くの形態のサイバー攻撃と同様、ランサムウェア攻撃の主な損失要因は依然として業務中断です。アリアンツの分析によると、金額ベースでサイバー関連損失全体の50% を占めています。

アリアンツが2019年から2023年上半期末までに保険業界で発生した大規模なサイバー損害（100万ユーロ超）を分析したところ、データが流出したケースの割合は2019年の40%から2022年には77%に増加し、2023年にはこれを上回る勢いであることがわかりました。このようなデータ流出の増加に伴い、第一当事者による復旧・対応費用が増加する一方、通知費用や第三者賠償責任も多額にのぼる可能性があります。IBMの「2023年データ侵害コスト」レポートによると、2023年のデータ漏洩の平均コストは445万ドルで、3年間で15%増加しました[19]。

事業中断による損失



サイバー関連の損害額の割合

データの流出は、サイバー保険金請求のコストを大幅に増加させる可能性があります。**Jens Krickhahn (a Regional Practice Leader, Cyber Insurance, Allianz Commercial)** は次のように述べています。「データの流出は、潜在的な請求額をまったく新しい次元に引き上げる可能性があります。第一当事者からの単なる損害賠償請求であれば、2年以内に解決することも可能ですが、データ流出の場合、解決までに時間がかかるだけでなく、訴訟や規制当局の調査により、データ流出の損害賠償請求の影響額が劇的に上昇する可能性があります。データが盗まれた場合、どのようなデータが流出したかを正確に把握する必要があります。また、顧客に通知しなければならないこともあり、顧客から賠償を請求されたり、訴訟を起こされたりする可能性があります」。

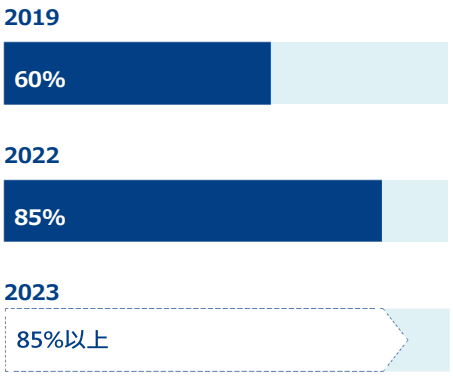
アリアンツが行った保険金請求通知に関する分析によると、早期に発見・対処されず、最終的にデータ流出を引き起こした侵害は、適切な対処を行った場合と比べて 1,000倍以上の費用がかかる可能性があることが示されています。

流出事件は風評リスクが高く、企業や経営陣のリソースを大きく消耗するため、効果的なデータ侵害対応が重要になる、とDaumは説明します。

「以前は、公表される保険金請求の比率はもっと低かったのです。データ流出の場合、ハッカーは盗んだデータを闇サイトで公開すると脅すので、ストレスのレベルははるかに高くなります。世間からの監視や圧力のレベルが上がっているため、これまで以上に準備が重要になっています。法律や広報の専門家が必要な理由もそこにあります。サイバー攻撃は公共の場で行われることが多くなっているため、このようなサポートが必要な保険金請求が増えています」と、Daumは言います。

実際、アリアンツが2019年から2023年上半期末までの間に保険業界で発生した大規模なサイバー損害（100万ユーロ超）を分析したところ、公表される事件の割合が年々増加していることがわかりました。2019年の割合は60%でしたが、2022年には85%に上昇し、2023年にはこれを上回る見込みです。

公表される事件の割合は年々増加しています



軽減策：新たなサイバー脅威と戦うには早期発見が鍵

大半のサイバー攻撃はすぐに収束し、保険に加入していたとしても、多くの場合、保険の免責額の範囲内に収まるか、或いは通知すらされないことがよくあります。アリアンツの分析によると、全体の損害額を押し上げる保険金請求はわずか2%で、ほぼすべてのケースで早期発見が有益となりました。一方、データ流出攻撃の影響を軽減するには、適切なデータ管理が不可欠であり、専門サービスの数も増えています。

Michael Daum (Global Head of Cyber Claims, Allianz Commercial) によれば、「予防策は攻撃頻度を制御し、検知することは重大度を決定します。インシデントの約90%は早期に収束し、ほとんどのケースは保険期間内に収まります。しかし、初期段階で攻撃を阻止できなかった場合、次の段階で攻撃者が捕まることはほとんどありません。攻撃者がデータを抜き取り、暗号化してしまってからでは手遅れで、非常に高くつきます」。

Daumによると、サイバー攻撃による損害を回避し、損失を軽減する鍵は、攻撃を初期段階で検知することです。「アウトソーシングや企業間のデータフローへの依存が高まる中、また、脅威行為者が人工知能を利用する可能性もあるため、組織の周囲を保護するだけではもはや十分ではありません」。

「企業は攻撃を防ぐことはできません。企業ができるのは、ごく初期での防御を超える攻撃の数を減らすことだけです。ITセキュリティにどれだけ投資しても、すべての攻撃を防ぐことはもはや不可能なのです。企業は、こうした攻撃を次の段階に進む前に素早く捉えて、ビジネスを停止させ評判を落とすような最も深刻なインシデントを防ぐ必要があります」と、Daumは続けます。

アリアンツが行った保険金請求通知の分析によると、早期に発見されずに封じ込められなかった侵害は、封じ込められた侵害に比べて1,000倍も、あるいはそれ以上高額になる可能性があります。

重要な変化

- サイバー攻撃の被害を回避し、損失を軽減する鍵は、攻撃を初期段階で検知することです。
- 企業はサイバーセキュリティの追加支出を検知と対応に振り向けるべきです。
  自社のセキュリティチームを通じて侵害を発見した企業は、わずか3分の1にすぎません。
- データを定期的かつ適切に管理し、データが適切に保管され、不要になった場合には削除することを徹底している企業は、リスクを軽減できます。
- 中小企業は、自社の潜在的なリスクを明確に理解し、人材、 IT インフラ、予算などの面でリソースを十分に配分して、それぞれに合ったセキュリティ対策を実施する必要があります。
- 中堅企業は、自社の重要な IT 資産を特定し、サイバーセキュリティ・サービス・パートナーと連携して、ネットワーク境界とエンドポイントに検知・監視 ツールを導入する必要があります。

「早期に発見され、攻撃が食い止められた場合のコストは 2万ユーロです。しかし、侵入が検知されずに拡大した場合、その結果生じるビジネスの中断や侵害のコストは、いとも簡単に2,000万ユーロに達する可能性があります（例を参照）。多要素認証はここ数年、最も効果的な対策の1つでしたが、今後は検知ツール（セキュリティ・オペレーション・センター（SOC））、セキュリティ情報・イベント管理（SIEM）、拡張検知・対応（XDR）、侵入検知（IDS）、侵入防御（IPS）システムなどが、多くの企業にとって当然の次の投資ステップになるでしょう」と、Daumは言います。

大量のアラートを管理するには、人間による監視とトリアージも必要であり、通常はSOCで行われます。

ハッカーがデータを暗号化したり盗んだりした場合、事業の中断や復旧にかかるコストはあっという間に膨れ上がってしまうため、ランサムウェアインシデントの影響を軽減するためには時間が重要だと、**Rishi Baviskar (Global Head of Cyber Risk Consulting, Allianz Commercial**) は説明します。

「目に見えないものは守れません。ネットワークに検出されていない抜け穴がある場合、それは潜在的なアキレス腱になります。また、効果的な早期発見ができなければ、予定外のダウンタイムが長くなり、コストが増加し、顧客、売上、収益性に大きな影響を与える可能性があります。また、早期発見は事後介入よりも費用対効果が高い可能性があります」と、**Baviskar**は付け加えました。

現在、IT セキュリティ予算の大部分は予防に費やされており、検出と対応に振り向けられる予算は全体の約35%です。ただし、検出機能と対応機能の有効性が損失の大きさを左右します。

Baviskarによれば、早期発見技術はすぐに利用でき、効果的です。「検知システムは日進月歩で進歩しており、検知や対応にかかる時間を短縮し、多くの労力を削減することができます。これは、私たちがサイバーリスクの評価とアンダーライティングの際に注目している点です」。

2万ユーロか2,000万ユーロか？早期発見 早期発見と迅速な対応が 全てを変えます

プロフィール: 従業員数2,000人の製造会社

インシデントの結果 1: 1 台以上の従業員のコンピュータが攻撃されます。攻撃は早期に (たとえば、攻撃者が管理者アクセス権を取得できるようになる前に) 検出され、阻止されます。

費用: 鑑識と修復にかかる費用は、合計約2万ユーロです。

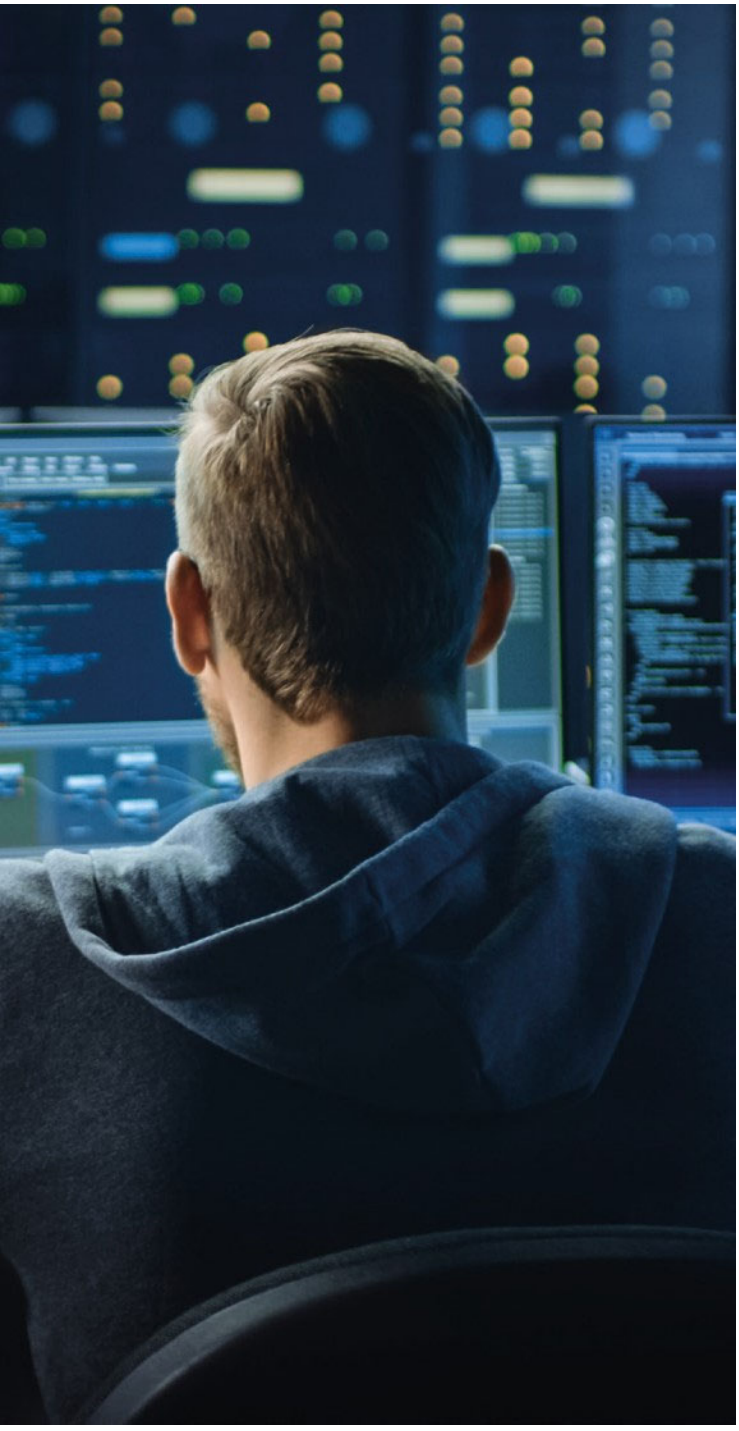
インシデントの結果 2: 同じ状況で、攻撃者は早期に発見されず、封じ込められることもなく、企業のITシステムへの足がかりを得ることに成功し、最終的な攻撃者の目標（ドメイン管理者権限など）を達成することができます。攻撃者は企業を完全に暗号化し、恐喝することができます。

費用: 事業中断（2週間）、身代金、完全な復元、失われた個人データに対する第三者からの請求など、総合的な損失額は約2,000万ユーロ（1,000倍）に達します。

アリアンツが行った保険金請求通知の分析によると、早期に発見されずに封じ込められなかった侵害は発生した侵害と同じか、封じ込められた侵害の

1,000倍以上にもなる

可能性があります



「100%安全ということはあり得ません。攻撃対象の拡大、より巧妙な攻撃、データの流出、大量のランサムウェア攻撃など、サイバー脅威は増大しています。さらに、モノのインターネットや人工知能の普及、規制の強化、侵害コストの上昇、第三者責任の増大などが加わり、早期発見・対応能力への投資がますます必要となっています」と、Baviskarは言います。

企業は、サイバーセキュリティの追加予算を、予防のレイヤーを増やすのではなく、検知と対応に振り向けるべきだとKrickhahnはアドバイスします。「私たちは企業が予防の予算を減らすことを推奨しません。むしろ、ITセキュリティに予算を割き、検出を同じレベルかそれ以上まで強化すべきです。予防から始まり、早期発見と対応に至るまで、エンド・ツー・エンドの自動的な仕組みにすべきです」。

IBM[20]によると、自社のセキュリティチームを通じてデータ侵害を発見した企業はわずか3分の1であり、より優れた脅威検知の必要性が浮き彫りになっています。しかし、攻撃者が情報漏洩を公表した場合、内部で検知する場合と比較して、企業のコストは平均100万ドル近く高くなります。

「多くの企業は、サイバー攻撃に対して積極的ではなく、むしろ消極的になりがちです。より積極的なアプローチの一環として、早期検知に投資すべきです。潜在的な損失に比べれば、検知への投資は非常に小さいものですが、一度検知に投資すれば、自社と重要なシステムを保護する準備が整います」と、Baviskarは言います。

Marisa Anthony (Senior Complex Claims Handler, Cyber, Allianz Commercial) によると、早期の検知と対応は、将来のサイバー攻撃の抑止にもつながります：「優れた検知と対応は脅威行為者を著しく挫折させ、企業を魅力的な標的とはしなくなります。脅威行為者を発見・検知し、即座にシャットダウンする努力を繰り返すことで、脅威行為者は再び動き出します。脅威行為者は、ほとんどの場合、最も簡単な標的を探します」。

最悪の事態への備え

世界的にデータプライバシー規制が強化される中、データ流出攻撃の影響を軽減するには、適切なデータ管理も不可欠です。

「データを日常的かつ適切に保管・管理し、不要になったら削除している企業は、リスクにさらされるデータ量を減らすことができます。私たちは最近、ハードディスクが適切に管理されておらず、攻撃者が10年以上前の情報を悪用したという保険金請求を扱いました。会社がデータを消去していれば、このような高額な賠償請求は起こらなかったでしょう」と、**Marisa Anthony (Senior Complex Claims Handler Cyber, Allianz Commercial)** は述べています。

法律やITの専門家による侵害対応サービスの費用も上昇傾向にあり、料金の上昇や、より複雑な攻撃への対応が課題となっています。例えば、データ流出攻撃では、通常、ベンダーが盗まれたデータを正確に把握するのに時間がかかり、非常に費用のかかるプロセスになる可能性があります。

「外部専門家に依頼する費用が上昇しており、そのため保険金請求額も高額になっています。たとえば、米国では、弁護士は数年前には1時間あたり1,000ユーロを請求していましたが、現在では同様の事件に対して1,500ユーロを請求するでしょう」と、**Marisa Anthony (Senior Complex Claims Handler, Cyber, Allianz Commercial)** は説明します。「また、請求内容の複雑さが増すにつれて、外部の専門家は問題の解決により多くの時間を費やします。そのため、料金が高くなるだけでなく、より多くの人がこれらのより複雑な請求に長時間取り組むようになるのです」。

データ漏洩の専門サービスの需要が高く、データ流出攻撃が増加しているため、企業は事前にベンダーのサービスを確保する必要があります。最近、ある欧州メーカーが米国で受けたサプライチェーン攻撃による損害賠償請求では、恐喝による金銭要求の総額は数千万ドルに達しました。また、このケースでは、被保険者はどのデータが漏洩したのかわからず、非常に高額な電子証拠開示費用が必要となりました。

「教訓の一つとして危機管理計画や訓練、専門ベンダーの起用や契約によって、このような攻撃に対して備えることを強く推奨します。これは非常に重要です。攻撃を受け、急遽プロバイダーを探して交渉しなければならないような事態は避けたいものです」と、Krickhahnは言います。

「このような専門業者のサービスや料金について、事前に合意した料金を設定していない場合、極めて高い料金に直面する可能性が高くなります。しかし、このような攻撃に備えて準備を整え、保険契約に含まれる専門業者のパネルとその料金を利用すれば、より有利な立場に立つことができ、企業にとっての保険金請求の影響とコストを軽減できる可能性が高くなります」と、Anthonyは付け加えます。

ほとんどのサイバー保険に付帯されるベンダー・サービスは、データ流出攻撃を管理し、財務上および規制上の影響を軽減するのに役立ちます。例えば、米国で普及している情報漏洩コーチは、いつ通知するか、誰に通知する必要があるかについて、より多くの情報に基づいた意思決定を行うことで、情報漏洩のコストを軽減するのに役立ちます。データ流出を伴うランサムウェア事件が発生した場合、情報漏洩コーチは、不必要な出費を避け、プライバシー法の不遵守を回避するための専門的な法的アドバイスを提供することができます。

> データを日常的に適切に管理し、適切に保存し、不要になったら削除するようにしている企業は、リスクにさらされるデータ量を減らすことができます。

事案発生前に、企業はサイバー保険の適用範囲とそれに付随するサービスをよく理解しておくべきだと、Anthonyはアドバイスします。「基本的なことのように思えますが、被保険者は保険証券を確認することで多くのことを学ぶことができます。保険契約によって提供されるサポートを利用したり、ベンダーの情報を確認し、ベンダーの重要な連絡先が対応計画に組み込まれていることを確認したり、事前にベンダーと連絡を取り、卓上演習を実施したりすることができます」。

保険契約者は、自分の保険が必要に応じて対応できるよう、保険金請求ワークショップも活用すべきだとDaumは示唆します。「私たちは保険金請求シナリオのワークショップを提供しています。そこではお客様に具体的な事例をお持ちいただき、それを保険の適用範囲や文言と照らし合わせてマッピングします。主要なサイバーリスクシナリオを特定する際には、ブローカーや保険会社と話し合って、原則としてそれらがカバーされるかどうかを確認することをお勧めします」。

Anthonyは被保険者に対し、サイバーインシデントが発生した際には、コストと損失を記録するようアドバイスしています。「私が注目するのは、事故が発生すると、被保険者は保険金請求について数学的に考える必要があり、どのように保険金請求を立証するかの必要もあるということです。例えば、損害の証明が必要ですし、事故に関する詳細な情報をタイムリーに透明性を持って伝える必要があります」。

「サイバーというと、身代金に注目する人が多いのですが、事業の中断は、保険金請求の中でもかなり厄介で、管理が難しい部分です。被害発生から時間が経てば経つほど、詳細がぼやけてきます。ほんの数時間の出来事でも、事業中断という点では甚大であり、立証が非常に難しい場合もあります。このような状況を説明し、損害額を定量化する必要があります」。

アウトソーシングへの依存は中小企業を危険にさらす

中小企業は、マネージドITプロバイダーやサイバーセキュリティプロバイダーなどのサービスをアウトソーシングに依存しているため、サイバー攻撃のリスクがより高まる可能性があります。

大企業がサイバーセキュリティを強化する中、サイバー犯罪者は、予防や対応能力に投資する資金的リソースが少ないことが多い中小企業を標的とする傾向が強まっています。Master Card のRiskRecon[21]によると、2021年中に中小企業で発生したデータ漏洩は世界全体で152%増加しましたが、同時期に大企業で発生したデータ漏洩は75%の増加でした。Vodafone[22]によると、英国では中小企業の半数以上（54%）が2022年に何らかのサイバー攻撃を経験しており、2020年の39%から増加しています。

「中小企業はサイバー攻撃に対して特に脆弱であり、準備やリソースの整った大企業と比較して不釣り合いな影響を受けています。中小企業はサイバーセキュリティのスキルが限られており、クラウドサービスプロバイダを含む第三者に大きく依存しています。また、事業中断の影響を吸収するための財務的支援も少ない傾向にあります」と、**Rishi Baviskar (Global Head of Cyber Risk Consulting, Allianz Commercial)** は述べています。

管理体制が不十分であったり、リスク管理プロセスが不十分な小規模企業が重大なサイバーインシデントに見舞われたりした場合、長期的には存続できない可能性があるというのが現実です。近年、進展が見られ、保険会社、ブローカー、顧客の間で良好な協力体制が築かれていますが、最終的には、サイバーリスクに対する認識とリスク管理に関する教育の強化が依然として必要であり、保険業界には、このプロセスにおいて中小企業を支援する責任があります。

「サイバーセキュリティの課題に効果的に対処するために、中小企業は警戒を怠らず、関連するリスクを明確に理解し、必要なセキュリティ対策を実施するために人員、ITインフラ、予算などのリソースを十分に割り当てる必要があります」と、Baviskarは言います。

「MSSP（マネージド・セキュリティ・サービス・プロバイダー）と話し合いを始めることは、優れた初期段階として機能し、ビジネスの優先事項に合わせたIT予算と戦略の策定を可能にします」。

中規模企業は、まず自社のサイバーセキュリティ戦略で最も重要な情報システム資産を効果的に特定することで、サイバー脅威に積極的に対処できます。 次に、ネットワークアクセスを試みる潜在的な脅威を発見して無効化するために調整された適切な検出ツールと技術の導入を進める必要があります。このような対策には、ネットワーク境界とエンドポイントの両方での検出および監視ソフトウェアの使用が含まれ、多くの場合、サイバーセキュリティサービスパートナーとの協力が必要になります。

企業がサイバー管理を強化すべき脆弱な部分はどこでしょうか。

アリアンツなどの保険会社は、アンダーライティングの観点から、各リスクを個別に評価し、企業のITセキュリティレベルとサイバーセキュリティに強く注目しています。アリアンツのアンダーライティングとリスクエンジニアリングのアンケートによると、多くの企業はIT セキュリティトレーニングの頻度、重要な環境のネットワークセグメンテーション、特にパッチ管理を改善する必要があります。企業のサイバーインシデント対応計画とサイバーセキュリティガバナンスは、最も脆弱な分野の1つです。

良いニュースとしては、保険会社は現在、サイバーリスクの質に関する議論が数年前とは大きく異なっており、サイバー保険市場が成熟するにつれてより良い洞察を得ているということです。多くの顧客がアリアンツと協力してセキュリティレベルの向上に取り組んでいます。

「しかし、サイバー脅威も成熟し続けているため、緩和と対応能力も向上させる必要があります」と、Tresa Stephens (a Regional Head of Cyber, Allianz Commercial) は述べています。

「今後、保険会社は、被保険者がどのようにテクノロジーを利用しているか、また、規制環境がどのように変化するかを予測する上で、被保険者がどの程度先見性を持っているかをより理解したいと考えるでしょう。例えば、被保険者には、人工知能（AI）の活用やAIデータセットのセキュリティといった分野で、アンダーライターからの質問が増えることが予想されます」とStephensは言います。

結局のところ、サイバー保険会社の役割は、純粋なリスク移転にとどまらず、変化するリスク環境に適応し、顧客の保護レベルを高めることにあります。保険会社が顧客とパートナーシップを組めば組むほど、将来的には損害の影響が軽減されることが期待されます。

参考資料

1 Black Kite, Ransomware Threat Landscape Report 2023
2 Akamai Research: Rampant Abuse Of Zero-Day And One-Day Vulnerabilities Leads To 143% Increase In Victims Of Ransomware
3 NCC Group, Cyber Threat Intelligence Report, March 2023 / Howden Predicts Global Cyber Insurance Premiums Could Exceed Usd 50 Billion By 2030, July 5, 2023
4 Cybersecurity Ventures, Global Ransomware Damage Costs To Exceed $265 Billion By 2031, June 4, 2021
5 Wired, Ransomware Attacks Are On The Rise, Again, July 12, 2023
6 IBM Security X-Force Threat Intelligence Index 2023
7 World Economic Forum, Wide-Ranging MOVEit Hack And Other Cybersecurity News To Know This Month, July 17, 2023
8 Reuters, MOVEit Hack Claims Calpers And Genworth As Millions More Victims Impacted, June 24, 2023
9 Cybersecurity & Infrastructure Agency, Understanding Ransomware Threat Actors: LockBit, June 14, 2023
10 IBM Security X-Force Threat Intelligence Index 2023
11 National Counterintelligence And Security Center, Kaseya VSA Supply Chain Ransomware Attack, August 10, 2021
12 Reuters, North Korean Hackers Breached A US Tech Company To Steal Crypto, July 21, 2023
13 Bleepingcomputer, Fortra Shares Findings On GoAnywhere MFT Zero-Day Attacks, April 19, 2023
14 Cybersecurity & Infrastructure Security Agency, ESXiArgs Ransomware Virtual Machine Recovery Guidance, February 8, 2023
15 Bloomberg, The Next Wave Of Scams Will Be Deepfake Video Calls From Your Boss, August 25, 2023
16 ISC2, Revealing New Opportunities For The Cybersecurity Workforce,
17 Gartner, Gartner Predicts Nearly Half Of Cybersecurity Leaders Will Change Jobs By 2025, February 22, 2023
18 IBM Security, Cost Of A Data Breach Report 2023
19 IBM Security, Cost Of A Data Breach Report 2023
20 IBM Security, Cost Of A Data Breach Report 2023
21 RiskRecon By Mastercard, Small Business, Mighty Attack Surface, August 23, 2022
22 Vodafone, Half Of SMEs Experience Surge In Cyber-Attacks – Vodafone Research Reveals, February 15, 2023

Allianz Commercialについて

Allianz Commercial は、中堅企業と大企業、そして専門的なリスク向けに保険を提供するアリアンツ・グループの専門知識とグローバルラインの中心的な存在です。当社のお客様には、世界最大規模の消費者ブランド、金融機関や金融業界の大手企業、世界的な航空・運輸業界、そして経済の屋台骨を支える家族経営企業や中堅企業が名を連ねています。また、洋上風力発電、インフラプロジェクト、ハリウッド映画制作などの特殊なリスクに備える保険も提供しています。

世界No.1の保険ブランド（Interbrandランキングによる）の従業員、財務力、ネットワークを原動力として、私たちは一丸となってお客様が将来に備えるお手伝いをします：伝統的および代替的なリスク移転ソリューション、卓越したリスクコンサルティング、多国籍サービス、シームレスな保険金請求処理など、幅広いサービスを提供することでお客様の信頼を得ています。

Allianz Commercialという商号の下に、Allianz Global Corporate & Specialty（AGCS） の大企業向け保険事業と、中堅企業向けの Allianz Property & Casualty の国内事業体の商業保険事業を統合しました。200を超える国や地域で、自社チームまたはアリアンツ・グループのネットワークやパートナーを通じて事業展開しており、2022年、Allianz Commercial の統合事業では、全世界で190億ユーロを超える総保険料を生み出しています。

連絡先

詳しくは、お近くのアリアンツ・コマーシャル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
Shakun Raj
shakun.raj@allianz.com
+65 6395 3817

Central and Eastern Europe
Andrej Kornienko
andrej.kornienko@allianz.com
+49 171 4787 382

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

Ibero/LatAm
Laura Llauradó
laura.llaurado@allianz.com
+34 660 999 650

North America
Jo-Anne Chasen
jo-anne.chasen@agcs.allianz.com
+1 917 826 2183

UK and Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

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

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

Olivia Smith
olivia.smith@allianz.com
+27 11 214 7928

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

Follow Allianz Commercialは下記にてフォローいただけます

Twitter / X **@Allianz_COMML** and

LinkedIn

www.commercial.allianz.com

Allianz Global Corporate &Specialty SE

Dieselstr. 8, 85774 Unterfoehring, Munich, Germany Images:

Images: Adobe Stock

October 2023