サイバー：変化する脅威のかたち

リスクの傾向、対応、保険の見通し

AGCS について

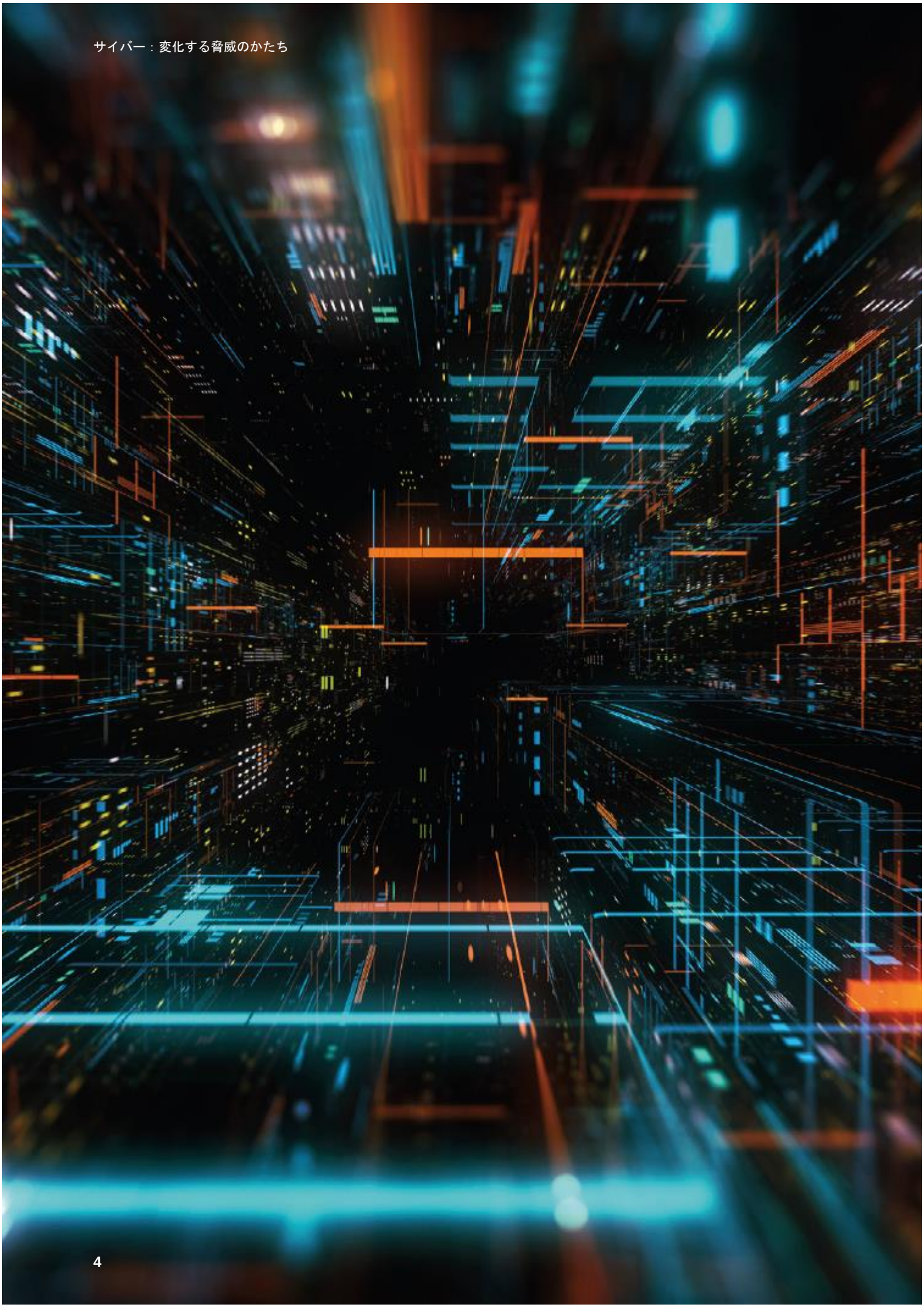
Allianz Global Corporate Specialty AGCS は世界有数の企業保険会社であり、Allianz Group の重要な事業部門の一つです。
当社では 9 の専門分野にわたり幅広い商業的リスク、企業リスク、特殊リスクに対するリスクコンサルティングサービス、損害保険ソリューション、代替的リスク移転サービスを提供します。

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、金融機関、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、水上風力発電所、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 4,250 人を数えます。
アリアンツグループ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 2021 年の世界総保険料収益は 95 億ユーロに上ります。

www.agcs.allianz.com

もくじ



はじめに

サイバー犯罪が世界経済に与える損害は、世界 GDP の約 1%相当の 1 兆ドルを超えると推定されていることから、当社が毎年行っている世界のビジネスリスク上位を特定する調査「**アリアンツ・リスクバロメーター**」で、サイバーリスクがお客様のランキング上位の懸念として必ず挙がることは驚くに及びません（2022 年調査では第 1 位）。実際、AGCS が独自に行った保険業界のクレーム分析によると、当社が過去 5 年間に各国で関わってきた 3,000 件のサイバー関連クレーム総額の 80%以上が外部からの攻撃によるものなのです。

本レポートでは、近年、損害を最も多くもたらしているランサムウェア攻撃関連コストの増加、中小企業の標的化、「ディープフェイク」の時代におけるビジネスメール詐欺の頻度と巧妙さの高まり、さらにはより大きな地政学的緊張の影響など、アンダーライティング、リスクコンサルティング、クレームの視点から主なサイバーリスクのトレンドに着目していきます。

当社の分析によると、当社が参加するサイバー関連クレーム全体の 50%以上で主たるコスト要因となっているのは事業中断ですが、本レポートでは、この他にも企業にとって大きな損害につながる主なリスクをいくつか取り上げていきます。そしてもちろん、サイバーインシデントもその種類にかかわらず、影響を被った顧客やサプライヤー、そしてデータ侵害の被害者による訴訟や賠償請求につながる可能性があります。さらにこれらとは別に、第三者賠償責任リスクが変化し続けていること、そしてサイバーセキュリティが環境、社会、ガバナンス（ESG）の問題としてますます認識されるようになってきていることについても考察していきます。また、サイバーセキュリティの向上の足かせとなっている問題として人材不足があることについても検証していきます。

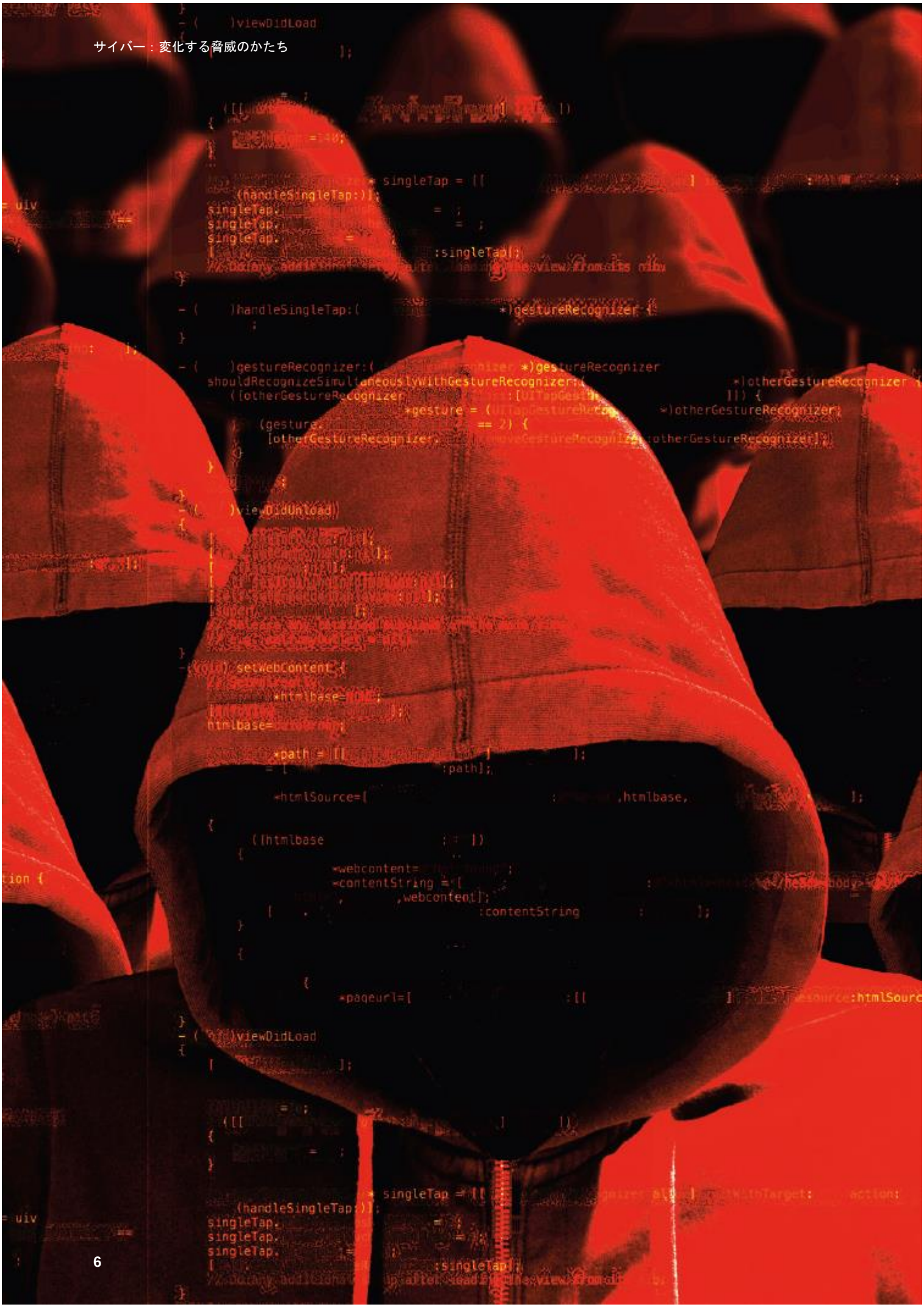
近年の厳しい損害環境に対応するかたちで、保険業界では、企業によるサイバーセキュリティとリスクマネジメント体制の改善を促す目的で、お客様のサイバーリスクプロフィールをより厳密に評価し、補償範囲を明確化するようになってきています。

私たちのこれまでの経験からは、依然として数多くの企業が、IT セキュリティトレーニングの頻度、サイバーインシデント対応計画、そしてサイバーセキュリティガバナンスを改善する必要があることが分かっています。いったん事業中断が起きればクレームのコストは急激に高まっていくので、インシデントへの対応はきわめて重要です。

サイバー成熟度の高い企業や組織のほうが、インシデントへの対応能力が高いことは言うまでもありません。サイバー成熟度やセキュリティの仕組みがしっかりしている企業に対して、高頻度で攻撃が「成功」するということはあまり一般的ではないのです。このような企業の場合は通常、攻撃を受けたとしても損害は比較的小さく済んでいます。

明るい側面としては、サイバーリスクの質に関する議論が数年前とはまったくかたちを変えてきており、サイバー保険市場の成熟にともなって、より良質の知見が得られるようになってきているということがあります。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へのお客様の適応を助け、セキュリティの水準を高めることにあります。このようにお客様とのパートナーシップを深めることで、将来的には損失をより減らすことができると私たちは考えています。

Scott Sayce
Global Head of Cyber and
Group Head of the Cyber
Centre of Competence
AGCS



脅威

サイバー犯罪関連のクレーム活動を今も高めるランサムウェアの脅威

近年、サイバー保険市場の成長に加え、サイバー保険損害の最大の要因の一つであるランサムウェア攻撃の届出などの事案が全体的に増加したこともあり、AGCS ではサイバー保険のクレーム件数が増加傾向にあります。2020 年から 2021 年にかけて、AGCS には全体として年間に 1,000 件以上のサイバー関連クレームが寄せられており、現在はアンダーライティングをより丹念に行うようになったこと、企業とよりよいリスク関連の対話ができるようになったことなどにより、クレーム活動が安定してきてはいるものの、サイバー関連クレームが主に第 3 と第 4 四半期に発生しているというこれまでの歴史もあることから、2022 年もクレーム頻度が高い年となる可能性があります。

法執行機関の努力にもかかわらず、ランサムウェア攻撃の発生頻度は依然として高く、それにともなうクレーム活動も高い水準にあります。ランサムウェア攻撃件数は 2021 年に過去最高の 6 億 2300 万件[1]を記録し、2020 年の 2 倍、2019 年比では 232%の増加となりました。SonicWall 社の Cyber Threat Report[2] によると、2022 年初めにはランサムウェア攻撃の頻度が 23%減少していたものの、2022 年上半期のランサムウェア攻撃件数は世界全体で 2017、2018、2019 各年の通年合計を上回っており、ヨーロッパでは 2022 年上半期のランサムウェア攻撃件数が 63%と急増していることが確認されています。一方、サイバー保護業界の推定によると、各国のさまざまな組織が 2023 年までにランサムウェアにより被るであろう損害は 300 億ドルに上ると予測されており、引き続き企業だけでなく政府にとっても最大のサイバー脅威となります[3]。

サイバー恐喝とランサムウェアがビッグビジネスに成長してきていることは否定できません。ランサムウェアのツールやサポートサービスをサイバー犯罪者に提供する Ransomware-as-a-Service（RaaS）により、犯罪者の参入障壁が下がり、活動規模を拡大して攻撃を強化できるようになりました。2021 年の平均身代金要求額が数百万ドルに上り、RaaS キットの価格が低額のもので月額 40 ドルなので、わずかな投資で、しかも技術的専門知識がそれほどなくてもサイバー犯罪者はランサムウェア攻撃から大きな利益を得ることができるのです。

保険加入企業によるリスクマネジメント措置が効果を発揮し始めているという明るい兆しも見える一方で（サイバーリスク・マネジメント・パートナーシップ、および AGCS ランサムウェア対策チェックリストセクション参照）、全体として AGCS に寄せられるランサムウェアやサイバー恐喝関連クレームの頻度と深刻度は近年著しく高まってきています。

「ランサムウェア攻撃の件数は全体的に高止まりしています」と話すのは **Rishi Baviskar（Global Cyber Experts Leader, Risk Consulting, AGCS）**です。「サイバー攻撃をすべて阻止することは不可能で、防御力の向上が必要な企業もまだ数多く存在します。意識は高まってきており、サイバーセキュリティの改善も進んでいますが、見込み客からの提出資料の半数以上は、依然として私たちが求める管理体制のチェックリストを完全には満たしていません。」

1 SonicWall Threat Intelligence：「2021 年に脅威が倍増。ランサムウェアや悪質なサイバー攻撃の憂慮すべき急増を確認」（Confirms Alarming Surge In Ransomware, Malicious Cyberattacks As Threats Double In 2021）2022 年 2 月 17 日
2 SonicWall Threat Intelligence：「2021 年に脅威が倍増。ランサムウェアや悪質なサイバー攻撃の憂慮すべき急増を確認」（Confirms Alarming Surge In Ransomware, Malicious Cyberattacks As Threats Double In 2021）2022 年 2 月 17 日
3 Acronis：「サイバー脅威中間報告：組織への最大の脅威はランサムウェア攻撃であり、2023 年までに被害額が 300 億ドルを超えると予測」（Mid - Year Cyberthreats Report Finds Ransomware Is The Number - One Threat to Organizations, Projects Damages To Exceed $30 Billion By 2023）2022 年 8 月 24 日

6.23 億件

2021 年のランサムウェア攻撃件数

チェックリスト

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しているか？
- 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、論理的なセグメンテーション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 に先立って、どのようなデュー・デリジェンスとリスクマネジメントを行っているか？
- 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、リスクマネジメント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。

高まる深刻度：二重恐喝が当たり前に

攻撃ツールや脅迫手段の高度化にともない、ランサムウェア攻撃によるクレームの深刻度も年々高まってきています。

全世界のランサムウェア関連クレーム額は2019年以降に大幅に増加してきており、過去2年間にAGCSが他の保険会社と連携して関わった全サイバー関連クレームのコストの 50%を大きく上回り、2022 年に至るまで大きなコスト要因となっています。ランサムウェアイベントによって引き起こされる主な損害要因は、事業中断、復旧費用、専門家の手数料です。

「犯罪者が大企業や重要インフラ、サプライチェーンを標的にするようになり、ランサムウェア攻撃で発生する費用負担は増加しています」と **Rishi Baviskar（Global Cyber Experts Leader, Risk Consulting, AGCS）**は説明します。「また、犯罪者の手口の巧妙化が進み、被害者からより多額の金銭を脅し取る方法が使われるようになってきていることも相まって、費用が増加しています。攻撃によるコストを劇的に増加させてしまう二重・三重の恐喝が、今や当たり前になってきているのです。」

従来型のランサムウェア攻撃では、犯罪者はネットワークに侵入し、マルウェアを使ってデータを暗号化し、その復元と引き換えに身代金を要求してきます。しかし、二重恐喝攻撃では、機密データが盗まれ、それが恐喝の手段として利用されてしまうのです。企業がバックアップからデータを復元できたとしても、データを秘密裏に取り出していれば、身代金を要求することができるのです。

これをさらに一歩進めた三重恐喝は、最初の攻撃対象企業のビジネスパートナー、顧客、サプライヤーなど、盗んだデータによって影響を受ける可能性のある企業などを恐喝するというものです。

二重・三重の恐喝では、ランサムウェア攻撃のコスト負担が高まるだけでなく、第三者賠償責任の要素も加わってきます。CipherTrace 社の調査[4]によると、2021 年には二重恐喝型ランサムウェア攻撃が約 500%近く増加し、身代金支払い額は最初の 6 ヶ月で 42%増の 5 億 9000 万ドルに上ります。

Marek Stanislawski（Global Cyber Underwriting Lead, AGCS）によると、ランサムウェアの深刻度は、犯罪集団の巧妙化と高まるインフレ（IT およびサイバーセキュリティ専門家の手数料の上昇）を要因として、今後も企業にとって重要な脅威となりそうだということです。「近年の身代金要求はオーダーメイドになってきており、犯罪集団は『適切な』金額を判定するために、資力を投じて交渉の専門家を雇い、利益の最大化を図るようになってきています。

「ランサムウェア攻撃者はまた、これまで以上に非情になってきています。サイバーセキュリティの向上により簡単に狙える標的が減ってきているので、攻撃が成功した場合は、より多くの利益を搾り取ろうとします。さまざまな嫌がらせの手段を使って、金銭を脅し取ろうとするのです。」

500%
2021 年、二重恐喝攻撃は約 500%増加

4 CipherTrace 社：「金額に納得できない犯罪者も。増え続けるランサムウェア」（The Price Isn't Always Right. Ransomware is on the Rise）2022 年 4 月 18 日

ランサムウェアによるコスト負担：
二重恐喝で書き換わるルール。コストは倍増。

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。

二重恐喝
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。
データの回復と広報活動：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

身代金支払いに対する措置も

2021 年のコロニアル・パイプライン事件[5]のような破壊的なサイバー攻撃は、ランサムウェアを政治問題化し、法執行機関の努力を倍加させるきっかけとなっています。また、身代金要求の支払いにも注目が集まっており、新たな規則や支払い禁止規則の可能性も出てきています。

身代金要求は増加の一途をたどっており、Paloalto 社[6]の Ransomware Threat Report によると、2021 年の身代金要求は 144%増加し、平均支払額は 78%増加しています。Sophos 社[7]によると、データを復元させるために身代金を支払った企業は約 46%に上ります。特に恐喝を受けやすい製造業と公益事業の身代金支払額平均は 200 万ドルに上りました。

米国財務省は 2020 年に、制裁対象のハッカーへのランサムウェア身代金の支払いを手助けすることは違法となる可能性があるとの声明を発しています[8]。EU 加盟国では、ネットワークおよび情報システム指令（NIS 指令）に基づいて身代金の支払いに罰金を科すことが可能です。Gartner 社[9]では、ランサムウェア身代金の支払い、罰金、交渉を規制する法律を敷く国が 2021 年には 1%未満だったところ、2025 年までに 30%の国が同様の法律を通過させるだろうと予測しています。

米国財務省は昨年、身代金を支払う際に制裁規定に違反することがないよう、企業や組織に警告しています。2022 年 7 月 29 日、ニューヨーク州金融サービス局（NYDFS）では、ランサムウェア事件の報告義務や、恐喝身代金支払いの正当性の立証義務を金融サービス会社に課す新しい規則を発しています[10]。

身代金支払いは、議論の分かれるテーマです。病院や電力会社など、重要サービスの提供者の場合、致命的な混乱を避けるためには身代金要求に従う以外に選択肢がほとんどないことも考えられます。その一方で、恐喝要求に従うことで、さらなるランサムウェア攻撃を助長する恐れがあります。また、制裁規定やテロ規制により、サイバー集団をはじめ、特定の国家、集団、個人への身代金の支払いが禁止されている場合もあります。

「身代金支払いに関する法改正により、ランサムウェアの問題が 100%解決される可能性は低いとはいえ、これが企業の成熟度向上の役に立つ可能性はあります」と **Rishi Baviskar（Global Cyber Experts Leader, Risk Consulting, AGCS）**は話します。長期的には、ランサムウェア攻撃の収益性が低下し、容易な標的を見つけることが難しくなるにつれて、サイバー犯罪者は戦術を統合したり、変更していく可能性があります。

「身代金支払いに関する規制が強化されることで、サイバー犯罪者は、データ窃盗やサプライチェーン攻撃、さらにはより標的を絞った攻撃など、今とは違った形態の攻撃に重点を移す可能性もあります。ランサムウェアの魅力がなくなれば、彼らはサイバー攻撃を収益化する他の方法を探すだけです」と **Baviskar** は話します。

攻撃の影響を受けた企業は、必ず警察や国の調査当局に報告を行い、協力する必要があります。

5 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
6 Paloalto 社：「2022 年 Unit 42 ランサムウェア脅威に関するレポート」（2022 Unit 42 Ransomware Threat Report）
7 Sophos 社：「ランサムウェアの状況 2022 年」（The State Of Ransomware 2022）
8 Cynance 社：「ランサムウェアの身代金要求に応じるのは合法か？」（Is It Legal To Pay Ransomware Demands?）
9 「Gartner 社が 2022-23 年のサイバーセキュリティ予測トップ 8 を発表」（Gartner Unveils The Top Eight Cybersecurity Predictions For 2022 - 23）
10 「ニューヨーク州金融サービス局、サイバーセキュリティ規制の更新を提案」（New York State Department Of Financial Services Proposes Updates To Cybersecurity Regulation）

ハッカーのスイートスポットになりつつある中小企業

>50%

2022 年上半期、中小企業によるサイバー関連クレームの平均コストは 50%以上上昇

現在、あらゆる業種のどのような企業も、例外なくランサムウェア攻撃のリスクにさらされていますが、大企業がサイバーセキュリティを強化する中、中小企業はサイバー犯罪者にとってより魅力的な標的となってきています。

サイバー攻撃は特定のセクターを狙い撃ちするものから、サイバーセキュリティの脆弱性を狙うものに変わってきていると **Scott Sayce（Global Head of Cyber, AGCS）**は説明します。「サイバー犯罪者にとって最も魅力的な標的は、これまでは、相応の努力で金銭的利益を最大化できる大企業でした。大企業がセキュリティに多額の投資を行う中、攻撃の標的は徐々に中小企業へと移りつつあります。現在のスイートスポットは、管理体制、リスクマネジメント、サイバーセキュリティが脆弱な中小企業で、サイバー犯罪者が最も好む標的となっています。」

サイバーセキュリティやリスクマネジメントに投資できるリソースが不足していることが多い中小企業と比較して、大企業は増大する脅威の影響を緩和する備えを整えやすいのです。「中小企業はデジタル化によってリスクが高まっていることを認識はしていますが、サイバーセキュリティと事業価値に結びつけた影響度分析を行っているケースはあまり一般的には見られません」と **Sayce** は話します。

> サイバー攻撃は特定のセクターを狙い撃ちするものから、サイバーセキュリティの脆弱性を狙うものに変わってきている。

最近、アリアンツは主要市場の中小企業向けサイバー事業を拡大することを目的にインシュアテック MGA の Coalition 社と複数年のパートナーシップを結びましたが、その Coalition 社によれば、小規模事業者からのサイバー関連クレームの平均額は 2022 年の上半期だけで 50%以上上昇しています[11]。「さまざまな業界で、インフラストラクチャが脆弱、または対策が不十分な組織が攻撃の標的となるケースが現在も紙面を賑わせていますが、このような状況に拍車を掛けているものとして、今日のリモートワーク文化や企業のサードパーティベンダーへの依存などがあります」と指摘します。これと同様に、ドイツのデジタル協会である Bitkom の調査[12]では、ドイツの中規模企業の IT システムは今年「激しいバーチャル砲火」にさらされてきたと報告しています。一方、非営利団体 Cyber Readiness Institute が中小企業 1,400 社を対象に行った調査[13]によると、サイバー衛生の基本である多要素認証をまだ設定していない企業は世界各国で 55%に上ります。システムのセキュリティをユーザー名とパスワードだけに頼っており、予防可能なサイバー攻撃に対しても脆弱な状態となっているのです。

とはいえ、大企業にも脆弱性や盲点はあります。年間売上が 1 億 5,000 万ユーロを超える企業を含む、AGCS のサイバー保険クレームの約 80%において、最終的な損失を引き起こした原因、もしくはこれに貢献していたのが、被保険企業のセキュリティに見つかった重大な欠陥でした。

「100%セキュアな組織など存在しません。優秀な IT システムを持つ大企業が、攻撃者に侵入口を見つけられてしまい、システムを侵害された事例が最近ヨーロッパでありました。ソフトウェアの脆弱性、従業員のミス、管理体制の甘いサプライヤーなど、高額クレームにつながる端緒はいくつも存在します。規模の大きさや IT の成熟度だけで完全に保護することはできません」と **Jens Krickhahn（Practice Leader Cyber Insurance, Central and Eastern Europe, AGCS）**は話します。

11 Coalition 社：「2022 年サイバー関連クレームレポート中間最新版（2022 Cyber Claims Report: Mid - year Update）を発表」2022 年 9 月 14 日

12 bitkom：「ドイツ企業への攻撃による年間被害額 2030 億ユーロ」（203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen　2022 年 8 月 31 日）

13 Wall Street Journal 紙：「中小企業は多要素認証の導入を急がなければならない」（Smaller Companies Are Urged to Adopt Multifactor Authentication）2022 年 7 月 5 日

「ディープフェイク」時代に増加する BEC 事件

データの入手可能性の高まり、「ディープフェイク」、そしてリモートワークへの移行によって、ビジネスメール詐欺（Business Email Compromise＝BEC）攻撃が容易に行えるようになり、増加の一途をたどっています。

BEC攻撃は、企業の大小を問わず、金銭的な損害や、より深刻なサイバー攻撃へとつながっていく可能性があり、大きな影響を及ぼします。様々な種類が存在する BEC 攻撃ですが、一般的にフィッシングメールやソーシャル・エンジニアリングを用いて、ユーザーの認証情報を盗んだり、従業員を騙して不正な送金をさせるといったものです。犯罪者にとって、BECは比較的少ない時間とリソースの投資で大きな見返りが期待できることから、魅力的な攻撃手法となっています。FBI によると、2016 年 6 月から 2021 年 12 月にかけての世界各国の BEC 詐欺の被害総額は430億ドルに上ります[14]。2019年7月から2021年12月の間だけでも、BEC詐欺が65%も急増しています。

BEC攻撃はますます巧妙さと標的の絞り込みが高度化してきており、今ではバーチャル会議プラットフォームを利用して、被害者に資金の送金や、日常業務に関する情報収集を仕向けるようになっています。これらの攻撃はまた、電話やオンライン会議で、上級管理職になりすました人工知能（AI）による「ディープフェイク」の音声や映像を活用することが多くなってきています。

昨年は、会社役員の声を「ディープフェイク」音声で模して、UAE のある銀行の従業員を騙し、3500 万ドルの不正送金を行わせた事件が発生しています。

430 億ドル
FBI によると、BEC 詐欺の被害総額は全世界で 430 億ドル

また、BEC攻撃の増加を後押ししているものとして、二重恐喝型ランサムウェア攻撃で盗まれたデータが犯罪者によって共有されることがあります。データ漏洩サイトから漏洩したデータには、検索可能なインデックス付きデータもあり、これらにより特定の種類のデータを検索することができるため、サイバー犯罪者はソーシャル・エンジニアリングをさらに高度化することができるのです。Accenture 社[15]では、ランサムウェア攻撃によりデータが漏洩したサイトを分析した結果、被害に遭った 91%がその後にもデータ公開被害を被っていると推定しています。

サイバー犯罪者は、ビジネスメール詐欺の戦略の進化を止めることはないだろうと **Tresa Stephens（Head of Cyber, Tech and Media, North America, AGCS）**は警告します。「米国では、サイバーセキュリティに対する意識、そしてフィッシングに関する従業員教育が高まってきているにもかかわらず、ビジネスメール詐欺によるクレームは現在も見られ、攻撃リスクは高まっていることはあっても、低下していることはありません。オンラインで入手できるデータの量が増大する中、犯罪者がソーシャル・エンジニアリングやフィッシングにますます注目するようになってきているのです。」

14 FBI：「ビジネスメール詐欺：430 億ドルの詐欺」（Business Email Compromise: The $43 Billion Scam）2022 年 5 月 4 日
15 Accenture 社：「流出したランサムウェアデータをサイバー犯罪者が追撃の武器にするやり口」（How Cybercriminals Are Weaponizing Leaked Ransomware Data For Follow - Up Attacks）2022 年 8 月 11 日

地政学的な対立が脅威のかたちを変える

100 億ドル

NotPetya による損害と事業中断の被害額は推定 100 億ドル

ウクライナ紛争、そしてさらに広範な地政学的な緊張により、サイバー脅威のかたちが大きく変わってきています。ロシアとウクライナの戦争は、今のところサイバー保険クレームの顕著な増加にはつながってはいませんが、国家主導のサイバーリスクが高まる可能性を示唆するものではあります。

この紛争では、スパイ活動のリスクが高まっているだけでなく、ロシアやウクライナと関係のある企業、そしてその近隣諸国や同盟国の企業に対する破壊的なサイバー攻撃のリスクも高まっています。戦火がサイバー空間へと波及することにより、西側諸国の重要インフラ、サプライチェーン、企業に対して、物理的な損害や混乱を引き起こすことを狙った標的型の攻撃が行われる可能性もあります。

特に懸念されるのは、ロシアとウクライナのサイバー紛争が起きれば、企業が巻き添えになる可能性があるということです。2017 年には、ロシアが関与した NotPetya と呼ばれる破壊的な「ワイパーウェア」が世界各国の企業に広がり、推定 100 億ドル[16]の被害と事業中断を引き起こしています。また、マルウェア伝染のリスクだけでなく、各国家が戦時に使用するツールや手法が、時間の経過とともにサイバー犯罪者にも広まることが懸念されます。

サイバー脅威のかたちは常に変化していると話すのは Jens Krickhahn（Practice Leader Cyber Insurance, Central and Eastern Europe, AGCS）です。「新たなリスクと脅威が登場してきています。サイバーを活用したハイブリッド戦争を懸念する人は、半年前まではほとんどいませんでしたが、今ではウクライナやロシアの支持者がサイバー攻撃の標的となっており、その間にも世界中の重要インフラへのリスクが高まってきています。悪意ある新形態の攻撃の出現は、常に想定していなくてはなりません。」

16 Financial Times 紙：「保険会社は国家を標的とするサイバー攻撃への対応を見直す必要がある」（Insurers must rethink handling of cyber attacks on states）2022 年 8 月 29 日

サイバー戦争条項で補償内容を明確化

戦争行為は一般的に従来の保険商品からは除外されていますが、ロシアによるウクライナ侵攻を機に、保険市場ではサイバー保険の約款における戦争の問題を取り上げ、お客様に対して補償内容を明確にする取り組みが加速しています。

サイバーリスクは、特に戦争や紛争では、システミックなリスクの集合体を生み出します。国家間のサイバー紛争では、公共事業、通信、決済システムなどの重要インフラが標的となれば、何千もの企業や全市民に想像を絶する損害と混乱が及ぶ可能性があります。

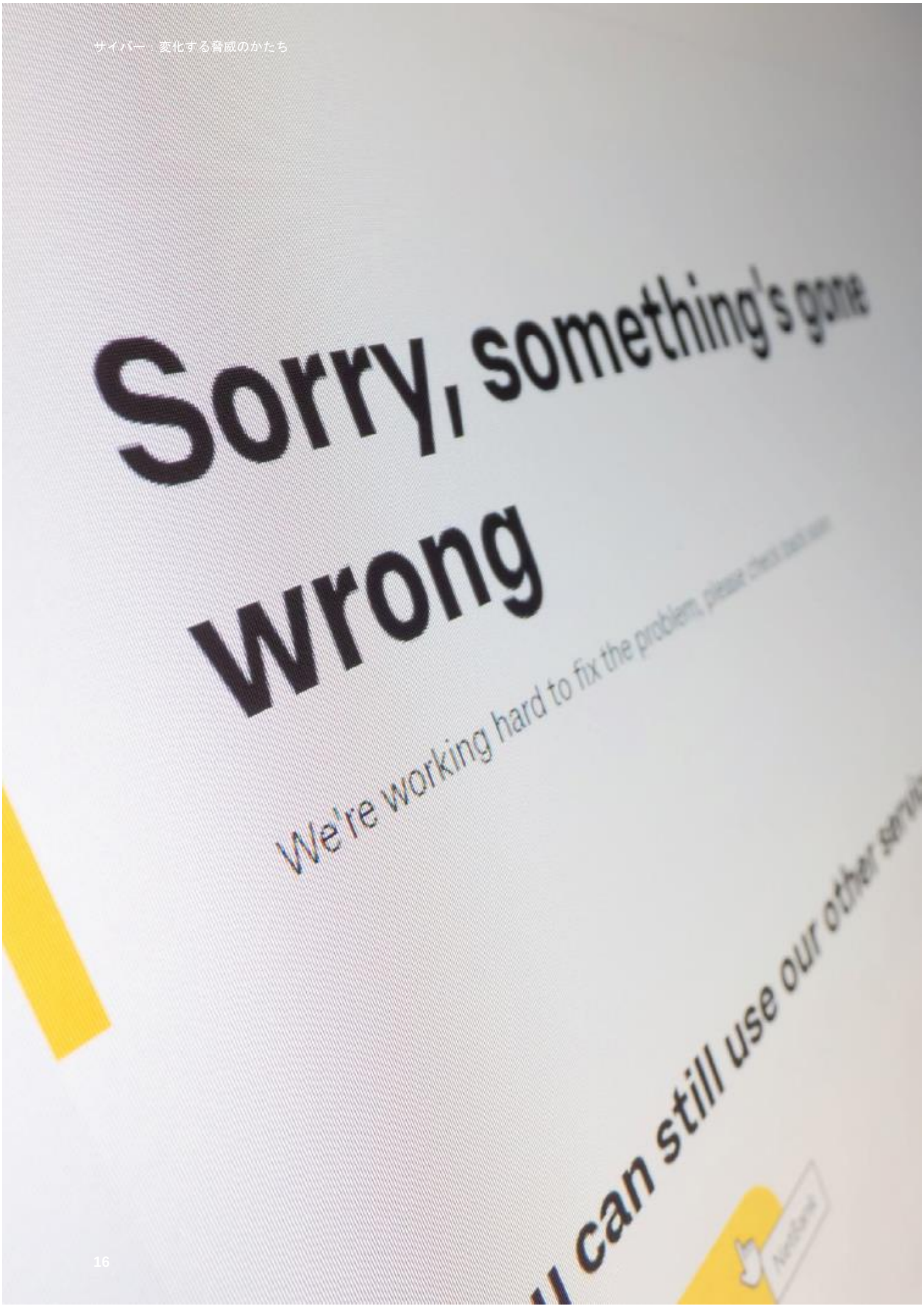
戦争行為とは物理的な損害や人身への傷害の文脈で理解されるものですが、サイバー戦争や紛争は定義が難しく、その帰属の特定も難しくなります。国家、テロリスト集団、サイバー犯罪グループの行動の境界線はますます曖昧になってきており、脅威行為者としての国家とその関係者による秘密裏に行われる敵対行為や、全面戦争には至らない国家支援のサイバー攻撃もあります。

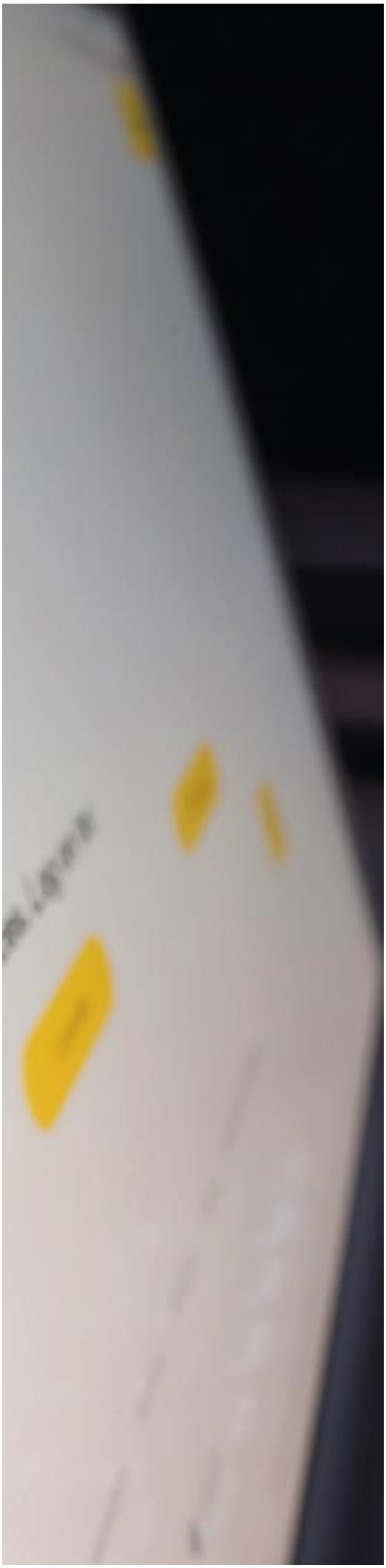
このような出来事に前例がないわけではありません。2017 年には、60 カ国以上の企業や組織に影響を与えた伝染性マルウェア攻撃「NotPetya」が発生していますが、米国と英国のセキュリティ機関では、ロシアに支援されたハッキンググループによるものと考えられています。この他にも、ここ数年の間に紙面を賑わせた民間企業への攻撃で国家主導とされる攻撃としては、ロシアの 2020 年 SolarWinds ハッキング、中国の 2021 年 Microsoft Exchange サーバーへの侵入、イランの 2021 年ボストン小児病院への攻撃がありますが、帰属を証明することは多くの場合非常に難しいのです。

NotPetya 攻撃により、サイバー戦争に関する議論が巻き起こり、これをきっかけに保険会社やブローカーは契約書の文言を改良していきました。クレーム処理と並行して標準的なサイバー戦争免責条項をいくつか設け、補償範囲と、多くの場合、帰属の問題にも対処しています。ロイズ・マーケットは最近、システミックなリスクを抑制し、契約の明確化を促すため、国家によるサイバー攻撃を除外することを発表しています。

サイバー保険の市場と商品の成熟にともなって、保険各社はサイバー戦争条項のあり方について次第に足並みを揃えるようになってきています。

「国家が支援するサイバー攻撃について、より明確化する方向に向かっています」と **Scott Sayce（Global Head of Cyber, AGCS）**は話します。「これまで、大半の保険における戦争や国家支援の攻撃に対する免責条項は、サイバー製品を想定したものではありませんでした。しかし、保険業界では現在、サイバー戦争免責条項の意図と表現を明確化する過程にあり、これによりクレーム発生時の曖昧さの多くも取り除くことができるでしょう」。


Sorry, something's gone wrong
We're working hard to fix the problem, please
can still use our other



事業中断の影響

事業中断は最大の損害要因

サイバーによる事業中断は、デジタル化リスクのうち、多くの企業が第一に懸念するリスクであり、サイバー保険全体として最大の損害要因となっています。世界各国の2,600 人以上のリスクマネジメントの専門家に、今後 1 年間のビジネスにおける最大の懸念を尋ねたアリアンツ・リスクバロメーター2022 では、サイバーインシデントと事業中断が最上位にランキングされています。

また、事業中断の原因として最も恐れられているのは「サイバー」でしたが、これはランサムウェア攻撃の高まりだけでなく、相互接続が進む今日の世界における脆弱性を反映したものです。AGCS が過去 5 年間に関わったサイバー関連の保険業界クレームの分析によると、事業中断は全世界のクレームの 57%と、最大のコスト要因となっており、クレームの深刻さが近年増してきている大きな要因ともなっています。

「デジタル化は企業の深部にまで浸透し、顧客、サプライヤー、従業員とのインターフェースを構成するようになりました。IT の外部委託やクラウドサービスがより広範に、より綿密に利用されるようになってきています。効率性が向上する一方で、これらのトレンドにより脆弱性が生じ、相互接続性とリスクの集積が高まるなど、脅威のかたちが変わってきているのです」と話すのは **Michael Daum（Global Head of Cyber Claims, AGCS）**。

57%
事業中断は、全世界のクレームの 57%を占める主要なコスト要因

産業用制御システム：製造業のアキレス腱

この 5 年間で、製造業や工業系企業が、小売業、金融機関、医療機関などと並んで、サイバー攻撃の標的となってきています。

IT インフラやサイバーセキュリティがそれほど強固ではない製造業や重要インフラ企業を、ハッカーが積極的に標的とするようになってきています。また、製造業や重要インフラ企業に対するサイバー攻撃は、事業中断からの復旧時間が長くかかり、消費者に直接的な影響が及ぶ場合もあることから、犯罪者にとっては効果的な恐喝の材料となるのです。

産業用制御システムを使用する工業・製造業では、古いシステムがネットワークに接続されている場合は特に、サイバー攻撃にさらされる可能性が高まります。

「産業用制御システムは、製造業や生産業のアキレス腱となります」と説明するのは **Rishi Baviskar（Global Cyber Experts Leader, Risk Consulting, AGCS）**です。「何十年もの間、単独でうまく機能してきたシステムは数多く存在します。ところがパンデミック以降、システムをネットワークに接続して遠隔監視や制御を行う企業が増えてきており、これらのシステムの中には、すでにサポートが終了しているネットワーク部品が組み込まれているものもあります。このようなシステムはセキュアではないので、他のネットワークから分離して十分な保護を施さなければ、ランサムウェアなどのサイバー攻撃にさらされる可能性があります。」

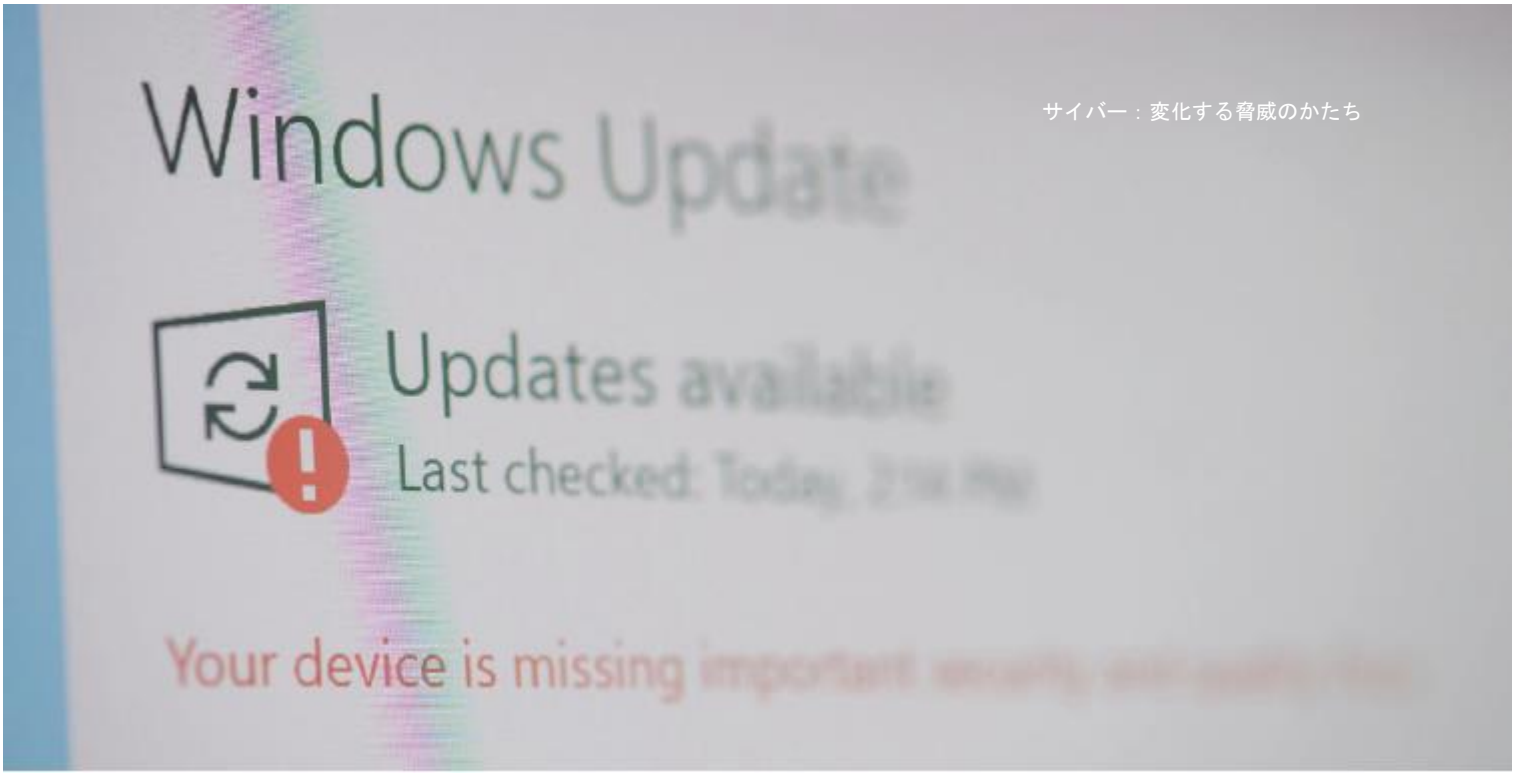
サイバー関連事業中断の誘因は広範に及び、悪意のあるサイバー攻撃、ソフトウェアやハードウェアの不具合、人為的ミス、電力やクラウドの停止といったサードパーティーの IT インフラやサービスの障害などがあります。しかし、近年急増しているランサムウェア攻撃も事業中断が脚光を浴びるようになってきている理由の一つで、ヨーロッパではサイバー保険クレームの最大の損害要因となっています。サイバークレームの約 90%は第一当事者から寄せられたもので、その 80%はランサムウェアによるものです。事業中断による損害は、恐喝要求額の実に 7 倍に上ることもあります。

特筆すべきは、米国では事業中断が、これまで損害の最大要因だった第三者賠償責任に取って代わっていますが、これはランサムウェアインシデントの増加によるものです。これまで米国のサイバー保険市場の最大損害要因はデータ漏洩でした。

これを追認するかたちで **Tresa Stephens（Head of Cyber, Tech and Media, North America, AGCS）**は次のように話します。「サイバーインシデント後に発生する費用のうち、事業中断関連費用がデータ漏洩関連費用を上回る最大の原因となっています。」

ランサムウェア攻撃や IT の停止から迅速に復旧できなければ、事業中断による損害が短時間のうちに膨れあがっていきます。製造業や工業に携わる企業では、小規模な機能停止から生産水準を回復するのに数週間～数ヶ月かかることもあるため、このような事業中断損失のリスクはさらに高まります。また、大手サプライヤーでサイバー関連の事業中断が発生すれば、それがバリューチェーンに波及し、世界中の顧客やサプライヤーが偶発的事業中断（CBI）に陥り、損害を被ることも考えられるのです。

偶発的な事業中断はリスク移転が特に難しい分野だと **Michael Daum（Global Head of Cyber Claims, AGCS）**は言います。「CBI 保険は、特に非 IT プロバイダーにとって大きな問題をはらんでいます。第三者で何が起こったかを確認するためのアクセス権が、被保険者、ひいては保険会社にあるかどうかは明確にはなっていません。最終的には、保険会社ではネットワーク侵入が起きたという証拠が揃ってはじめて、サイバー保険が発動されることになります」と **Daum は言います。**



脆弱なサプライチェーンと M&A を狙うハッカー

最近懸念が高まってきていることの一つに、従来型とデジタル型に関わらず、サプライチェーンが意図的に標的にされていることがあります。このような攻撃は、保険市場にとっては特に懸念されることです。というのも、1 件のサイバー攻撃で、世界各国の何千もの企業に損害が及ぶ可能性があるからです。

近年、ランサムウェア攻撃が巧妙化していることを反映するかたちで、サプライチェーンへの攻撃が重大なリスクとして浮上してきています。パンデミック以来すでに諸々の圧力にさらされているサプライチェーンですが、犯罪者はより効果的な攻撃ができる可能性のあるこのようなサプライチェーンを標的にしています。また、サプライチェーン内の重要な小規模サプライヤーを標的にしたり、合併・買収の過程にあるサプライヤーを標的にして、規模の大きい買収側の企業へのアクセスを狙うのです。

昨年、米国東海岸に燃料油を供給するコロニアル・パイプラインが、ランサムウェア攻撃を受けてパイプライン停止に追い込まれるという事件が発生しています [17]。また、ソフトウェアのサプライチェーンを標的にし、正規のソフトウェアにマルウェアを挿入するといった攻撃も起きています。2021 年に発生したクラウドベースの MSP プラットフォーム Kaseya に対するランサムウェア攻撃 [18] では、ソフトウェアアップデートに挿入されたマルウェアによって約 1,500 社が被害を受けました。

IBM 社 [19] によると、ランサムウェア犯罪者がサプライチェーンの混乱を「人質」に企業に身代金を要求するようになってきており、2021 年は製造業が金融サービスを抜いて最も攻撃の多い業種となりました。製造業への攻撃の約半分（47%）は、脆弱性にパッチが施されていないことよるものでした。

製造業のサプライチェーンは複雑で、何千ものサプライヤーが関わっていることから、サプライチェーンを介したサイバー攻撃に対して特に脆弱な業種であるといえます。大企業の多くはランサムウェア攻撃のリスクを低減するための対策を講じているとはいえ、サプライチェーン全体としてのサイバーセキュリティの成熟度や透明性はまだほとんどなく、中小企業のサイバーリスク管理に至っては遅々として進んでいません。

「企業は、サプライチェーンのサイバーセキュリティに、そしてアウトソーシングをする際にも、サイバーセキュリティに隙間が生じないように注意する必要があります。クラウドサービスを安全に利用するためには明確なセキュリティ知識が必要で、企業はまずこれを確立しなければなりません」と **Michael Daum（Global Head of Cyber Claims, AGCS）**は話します。「アウトソーシングやクラウドのベンダーが全責任を負うというのは、よく見られる誤解です」。

47%

製造業への攻撃の約半分（47%）は、脆弱性にパッチが施されていないことよるものでした。

17 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
18 ロイター通信：「米国の同社 CEO が語る：約 1,500 社がランサムウェア攻撃で被害」（Up To 1,500 Businesses Affected By Ransomware Attack, U.S.）
19 IBM Report：「2021 年、サプライチェーン関連の問題が増大する中、サイバー攻撃の矢面に立たされる製造業」（Manufacturing Felt Brunt Of Cyberattacks In 2021 As Supply Chain Woes Grew）2022 年 2 月 23 日

クラウド・アウトソーシング：将来に向けて蓄積するリスク

セキュリティやリスクの集約に関する懸念が高まっているにもかかわらず、企業は現在もサービスやデータストレージのクラウドへの移行を続けています。

2022 Thales Cloud Security Report[20] によると、企業や組織の 3 分の 2（66%）が機密データの 21%～60%をクラウドに保存しているとのことです。しかし、回答者の 45%がクラウド上のデータやアプリケーションに関わるデータ漏洩を経験した、または監査に不合格なったと回答しており、これは 2021 年に報告された 35%よりも高い割合となっています。世界のクラウドサービス市場の 65%[21] を占めるのは、Amazon、Microsoft、Google の 3 大クラウドプロバイダーです。

少数の IT サービス・プロバイダー、ソフトウェア・ベンダー、そしてプラットフォームにリスクを集中させることは、将来に向けて問題を貯め込むことになりかねないと**警鐘を鳴らすのは Tresa Stephens（Head of Cyber, Tech and Media, North America, AGCS）**です。「サイバーセキュリティやクラウドサービスを少数の事業者に依存することにより、私たちの社会は、単一障害点（1 カ所で障害が発生するとシステム全体が停止してしまう）を中心とする大規模な集合体を作り出しているのです。技術系ソリューションのプロバイダーへのアウトソーシングは有用なことかも知れませんが、アンダーライティングの際にはこうしたリスクの集中を慎重に検討する必要があります」。

サイバー攻撃、機能停止、ソフトウェアのバグなどにより、クラウドサービスやインターネットインフラが数時間から数日間オフラインになり、何千もの企業に事業中断が引き起こされる可能性もあるのです。

「最終的には、どの企業もサイバーセキュリティは自社の責任ですが、特にアウトソーシングやクラウドへの移行の際にはこれを忘れがちになります。企業は、適切な管理体制とプロセスが確実に実施されるようにしなければなりませんが、そうなっていないケースも数多く見受けられます」と話すのは **Marek Stanislawski（Global Cyber Underwriting Lead, AGCS）**です。

20 「クラウドのデータ漏洩とクラウドの複雑さが高まっていると Thales 社が報告」（Cloud Data Breaches and Cloud Complexity on the Rise, Reveals Thales）2022 年 6 月 7 日

21 CRN 社：「クラウド市場のシェアトップ企業：2022 年第 2 四半期は AWS、Microsoft、Google がリード」（Top Cloud Market Share Leaders: AWS, Microsoft, Google Lead Q2 2022）2022 年 8 月 17 日

第三者賠償責任

進化を続けるリスク

サイバー関連の第三者賠償責任リスクは、テクノロジーと規制によって新たなリスクが生み出される中、進化を続けています。

企業や接続機器が人々の健康、行動、生体に関する情報をはじめとする大量の個人データを収集するようになり、テクノロジーの進歩に伴って第三者賠償責任の重要性がさらに高まってきています。同時に、人工知能（AI）と強力なアナリティクスにより、企業や組織は、チャットボットや自動化されたサービスなどを活用して、リアルタイムでデータを処理して意思決定を行ったり、アドバイスを提供できるようになります。

欧州では一般データ保護規則（GDPR）の下で厳しい規則が導入され、カリフォルニア、ブラジル、中国、インドなどの国や地域でもより厳しい規制が導入され、その後もデータ漏洩やプライバシー関連規制は拡大を続けています。さらに、米国の複数の州で生体認証プライバシー法が制定され、EU では AI に関する規制の枠組みが整備されつつあります。2023 年末までには、消費者へのプライバシー権の提供を求める各国政府の規制の適用対象が、世界の GDP の 70%以上に相当する 50 億人に及ぶことになります。Gartner 社によれば、これは 2021 年の約 30 億人から大幅増となります[22]。

サイバーインシデントはその種類にかかわらず、影響を被った顧客やサプライヤー、そしてデータ侵害の被害者による訴訟や賠償請求につながる可能性があることは言うまでもないと話すのは **Tresa Stephens（Head of Cyber, Tech and Media, North America, AGCS）**です。

テクノロジーの進歩に伴って、新技術に内在する欠点が明らかになってから、規制が遅れて適用される傾向があると Stephens は説明します。例えば、技術の進歩やオンラインビジネスモデルへの移行により、企業が消費者データを収集、保存、共有することが容易になっています。ソーシャルメディア各社は、何年にもわたって利用者データの収集を行っており、多くの場合、そのデータが最終的に何に使用されるのか、利用者には知らされないままでした。消費者のプライバシー権に関心が集まるようになると、規制当局もそれに対応するための規制を設けてきました。

また、事業中断や損害賠償費用が損害の大きな部分を占めることが多いランサムウェアのクレームでは、第三者賠償責任による損害が重要になってきています。犯罪者が個人情報を盗んで使用する二重恐喝型ランサムウェア攻撃の高まりによって、データ漏洩関連クレームや訴訟が増える可能性もあります。

「今日のランサムウェアインシデントの多くは情報漏洩を伴うので、個人情報や機密情報を保有する企業にとって大きなリスクとなります。データ保護やプライバシー関連法が進化し、ハッカーが二重恐喝・三重恐喝の手法を用いるようになるにつれ、罰金や罰則だけでなく、第三者賠償責任も今よりも重要になってくると考えられます」と **Michael Daum（Global Head of Cyber Claims, AGCS）**は話します。

70%

2023 年末までには、消費者へのプライバシー権の提供を求める各国政府の規制の適用対象が、世界の GDP の 70%以上に相当する 50 億人に及ぶことになります。

22 「Gartner 社が 2022-23 年のサイバーセキュリティ予測トップ 8 を発表」（Gartner Unveils The Top Eight Cybersecurity Predictions For 2022 - 23）

ESG

ますます環境、社会、ガバナンスの視点で見られるようになったサイバーセキュリティ

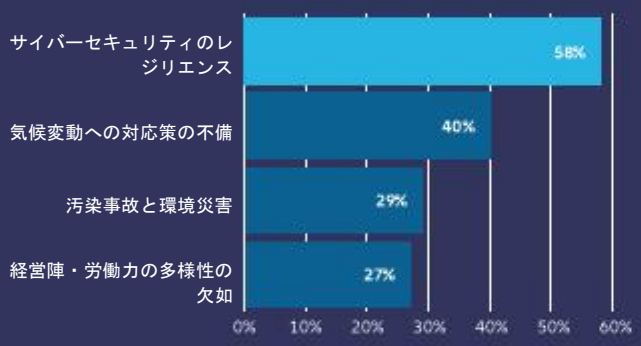
サイバーセキュリティは長い間、IT の問題とみなされてきましたが、今日のデジタル経済の活況をみれば、その見方がもはや正しくないことが分かります。在宅勤務の高まり、デジタル化の加速、かと思えば米国のコロニアル・パイプラインへのランサムウェア攻撃[23]のような事件の影響が広範囲に及んだことなど、サイバーインシデントによって露呈した潜在的・実際的な脆弱性はきわめて明白になってきており、これがひいては、今までよりはるかに幅広い層を — 企業経営陣、各国投資家、顧客の個人情報に触れる可能性のあるステークホルダーなど — サイバーセキュリティの社会的影響にますます関心を向けさせる要因ともなっているのです。

実際、**アリアンツ・リスクバロメーター 2022** の回答者の大半（58%）によると、サイバーセキュリティのレジリエンスは、今や多くの企業にとって最大の ESG リスクテーマとみなされています*（図参照）*。この背景には、サイバー攻撃の拡大と深刻化、さらには個人情報の保護を強化するためのデータセキュリティ規制の導入とその強化などが世界的に進んでいることがあります。
企業が情報やネットワークを適切に保護しなければ、罰金やレピュテーション面での損害を受ける可能性があることから、レジリエンスを構築し、将来の稼働停止などに備えた計画を立てなければ、規制当局や投資家、その他のステークホルダーの審判を受けることになるという認識が広まっています。

23 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

ESG リスクの動向のうち、御社が最も懸念するものは？

回答トップ 4



出典：アリアンツ・リスクバロメーター 2022

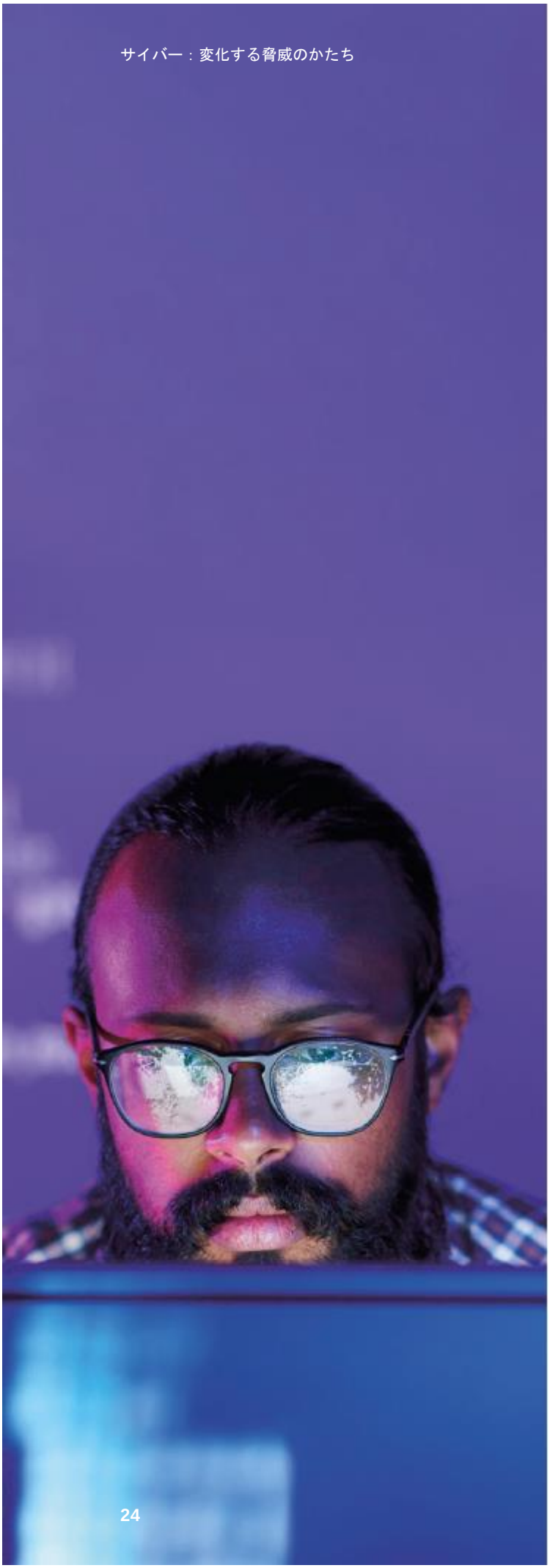
数字は、回答をした全参加者（2,650）の回答のパーセンテージを表したもの。また、リスクは最大で 3 つまで選択可能であることから、数字を合算しても 100%とはなりません。

> サイバーインシデントがもたらす潜在的な脆弱性と実際の脆弱性が明らかになり、これまでよりも幅広い層の人々がサイバーセキュリティの社会的影響に関心を持たざるを得なくなりました。

以前は、サイバーセキュリティの強度を評価されるのはテクノロジー企業が主でしたが、最近では、さまざまな分野の企業がこのような評価の対象になっています。データプロバイダーの ESG 関連リスク分析の枠組みにサイバーセキュリティの検討事項が組み込まれることが増えていますが、これらデータプロバイダーは、企業のデータ保護と情報セキュリティの慣行などを調査し、サイバー犯罪への備えを評価する一方で、投資家は一般的に、データ保護と情報セキュリティの企業方針を調査し、サイバーセキュリティのリスク評価を行います。

企業のサイバーセキュリティのプロセスと方針が取締役会レベルで理解されていて、サイバーリスク監視プロセスが導入されていることはきわめて重要です。投資家の主な不満の 1 つに、透明性に関する不満があります。企業のサイバーリスクを理解するのは難しく、さまざまな理由から企業はこれまで十分な透明性を提供することをためらってきた部分があるからです。しかし、それをためらわない企業は確実にそのメリットを享受しているのです。

サイバーセキュリティを ESG の指標の一つとすることは、まだ比較的新しい考え方ですが、この分野への関心は継続的に拡大していくと考えてよさそうです。こうした変化を認識せず、ESG とサイバーセキュリティの戦略を統合しない企業は、将来、サイバー保険クレーム以上の問題に直面することになるかもしれません。



人材

不足するサイバーセキュリティ専門人材

サイバーセキュリティの専門人材が不足していることが、特にテクノロジー分野以外でのサイバーセキュリティ向上への取り組みを遅らせている可能性があります。

欧米では労働力の供給が制約される中、サイバーセキュリティの専門人材の需要は高まっています。サイバーセキュリティの専門人材を採用したいと考える企業は増えていますが、需要に供給が追いついていないのが現状です。Cybersecurity Ventures 社[24]によると、世界各国で採用者が確保できていないサイバーセキュリティ求人枠の数は、2013 年から 2021 年にかけて 350%増の 350 万に達し、これは大型サッカースタジアム 50 個を満席にできるだけの人数です。

近年、企業経営陣のサイバーに対する意識の高まりによってセキュリティへの投資が加速している一方で、求められるスピードと規模で変更を行うために必要な IT 専門人材の確保に多くの企業が苦戦していると話すのは **Jens Krickhahn（Practice Leader Cyber Insurance, Central and Eastern Europe, AGCS）**です。

「ほんの 2〜3 年前までは、経営トップのサイバーに対する意識は低かったのですが、サプライチェーンへの大規模なサイバー攻撃や、最近ではウクライナ紛争による脅威環境の変化によって、その意識は大きく変わってきています。その結果、経営幹部レベルがサイバーリスク対応にこれまでよりも関与するようになり、投資を強化するようになっています」と **Krickhahn** は言います。

「ところが、今度は人材の問題が出てきました」と **Michael Daum（Global Head of Cyber Claims, AGCS）**が言います。「サイバーセキュリティの専門人材が世界的に不足しており、多くの企業が採用に苦戦していることから、一部の企業ではサイバーセキュリティ改善に向けた取り組みに影響が出ています。」

24 CyberSecurity Ventures 社：「Cybersecurity Jobs Report: 2025 年には 350 万人が不足」（Cybersecurity Jobs Report: 3.5 Million Openings In 2025）2021 年 11 月 9 日

持続可能なサイバー市場

サイバーリスク・マネジメント・パートナーシップ

2020 年と 2021 年のランサムウェアによる損害の増加を受け、保険業界では、企業によるサイバーセキュリティとリスクマネジメント体制の改善を促す目的で、顧客のサイバーリスクプロファイルをより念入りに評価するようになっています。

サイバーセキュリティを強化することで、その企業は攻撃者にとって魅力を失うと **Jens Krickhahn（Practice Leader Cyber Insurance, Central and Eastern Europe, AGCS**）は説明します。「サイバー成熟度やセキュリティの仕組みがしっかりしている顧客企業に対して、高頻度で攻撃が『成功』することはあまり一般的ではありません。攻撃された場合でも、識別や対応の仕組みが確立しているので損害がそれほど大きくならないのが通常です。サイバー成熟度の高い企業や組織のほうが、このようなインシデントへの対応能力が高いことは言うまでもありません」。

いったん事業中断が起きれば、クレームのコストは急激に高まっていくので、インシデントへの対応はきわめて重要だと Krickhahn は話します。「高い防御壁を作っても、それが持ちこたえ続けるという保証はありません。危機管理チームや専門的なサポートパートナーのネットワークなど、インシデントに対応するためのテスト計画と対策も必要です。こうすることで、クレームをできるだけ小さく抑えることができます。これは全員にとって Win-Win となります。企業の IT セキュリティの成熟度が高いほど、損害を被っていたり、過去に損害を受けていたお客様の割合が低くなります。」

ランサムウェア被害は、業界のサイバーリスクへの取り組み方を良い方向に向かわせていて、サイバーリスクの管理と軽減に関する保険会社とお客様の協力も促していると話すのは **Tresa Stephens（Head of Cyber, Tech and Media, North America, AGCS**）です。「私たちは、被保険者のことを詳細に知り、その上でどうすれば会社を守り、サイバーリスクを軽減することができるかに関して、より見識の深い情報を提供して、お客様のお手伝いをしたいと真剣に考えてのことです。3 年前とは雲泥の差です。」と **Stephens** は話します。

「また、サイバーリスクの質に関する議論も、これまでとはまったく形が変わってきました。当社はより良質の知見を得ることができ、保険業界はより多くの価値を提供できるようになっています。例えば、信頼できるパートナーや社内のリスク専門コンサルタントとの連携により、効果的な管理体制とはどのようなものなのかといった有益な情報やアドバイスをお客様に提供したり、リスクマネジメントや対応サービスを提供することができるようになりました。将来的には、当社のお客様に対するサイバー攻撃の成功や、影響の大きいサイバー事象の発生が減っていくはずです。」

保険会社が推奨事項の中で「価値」を置くのはサイバーセキュリティへの投資だと説明するのは **Michael Daum（Global Head of Cyber Claims, AGCS**）です。

「私たちは『デジタルスプリンクラー』の設置を徹底してもらっています。リスク・エンジニアリングとアンダーライティングの推奨事項は、今やサイバー保険に加入するための前提条件となっています。これらの推奨事項は明らかに理に適ったもので、保険がきっかけとなってサイバーセキュリティ対策の実施を 2 年～3 年後にではなく、現段階で実施しようという決定に至るケースも増えてきています。」

AGCS のアンダーライティングおよびリスク・エンジニアリングのアンケートからは、IT セキュリティ教育の頻度、重要環境のネットワークのセグメンテーション、クリーンパッチの管理などを特に改善する必要がある企業が多く存在することが分かります。企業の対応が最も脆弱となっている分野としては、サイバーインシデント対応計画やサイバーセキュリティのガバナンスなどがあります。

Stephens は、保険会社と早い時期から連携して、サイバーセキュリティの隙間に対処するための具体的な計画を立てることを企業に助言します。「私たちは、これをパートナーシップと捉えています。疑問点を事前に的確に把握することで、脆弱性や隙間を特定し、更新前に対処することができます。そのためには、対話を早い段階から、頻繁に行うことが大切です。」

持続可能なサイバー保険商品に向けて

200 億ドル

サイバー保険の保険料は、2025 年までに全世界で総額 200 億ドルを大きく上回る見込み

サイバー保険の需要は引き続き堅調ですが、市場要因や一部セクターにおけるサイバーセキュリティの脆弱性によって成長機会が制限されています。

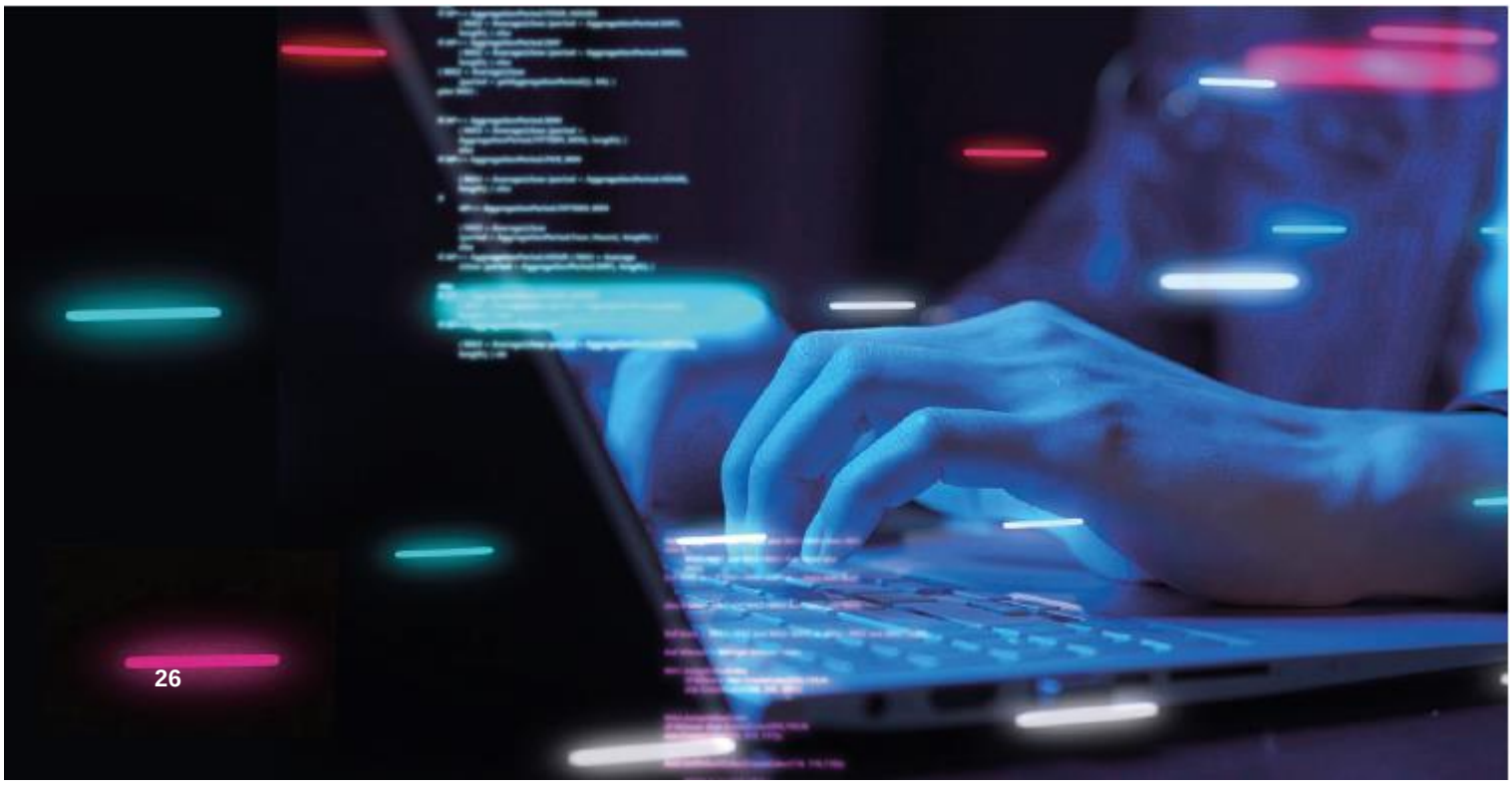
ランサムウェア被害の急増、さらには全体に影響するサイバーリスクや、各種サイバーリスクの集合体に対する認識が高まっていることを受けて、市場の引受キャパシティは制約され、その一方で保険料は上昇しています。また、多くの保険会社がアンダーライティング基準を厳格化し、被保険者に最低レベルのサイバーセキュリティと管理体制を維持することを求めています。

Marek Stanislawski（Global Cyber Underwriting Lead, AGCS）によると、脆弱性があってセキュリティ管理体制が不十分なために、この市場でサイバー保険に加入するのが難しい企業がまだ多く存在するとのことです。「サイバーリスク・プロファイルをしっかり理解しており、適切な管理体制とセキュリティを導入している、管理の行き届いた企業のための引受キャパシティは十分にあります。」

お客様の多くは、第三者賠償責任や事業中断をはじめとする広範なリスク補償を現在も受けていると説明するのは **Tresa Stephens（Head of Cyber, Tech and Media, North America, AGCS）**です。

「サイバー保険市場は修正しましたが、システミックなリスクやリスクの集約など、根深い問題が残っています。また、リスク要因と軽減措置との間には、依然として差異があります。サイバー保険市場が持続可能な状態になる必要があるのです。お客様とパートナーシップ関係を築き、脅威環境への適応のお手伝いをすればするほど、損害が減少することを期待しています。」

サイバーセキュリティの向上において、保険業界は重要な役割を担っていると **Stanislawski** は説明します。「サイバー保険の分野で長期的なパートナーであり続けたいと考えています。サイバー保険は、企業が加入する保険の中でも最も重要なものになる可能性があります。サイバーは現在、大半の企業が直面する最大の脅威であり、今後もそれは変わらないでしょう。」



「企業はサイバーのリスク移転のソリューションを必要としており、私たちがアンダーライティングの調整を続け、お客様と手を携えてサイバーセキュリティの成熟度の向上を目指すのもそのためです」。

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へのお客様の適応を助け、セキュリティの水準を高めることにあると説明するのは **Michael Daum（Global Head of Cyber Claims, AGCS）**です。

「サイバーは保険商品として定着していくでしょう。市場とサイバー商品は成熟しつつあり、成熟度の高いサイバーセキュリティとはどのようなものか、何が保険でカバーでき、何ができないのかについて、次第にコンセンサスが得られるようになってきています。」と Daum は結論付けます。

Munich Re 社によると、全世界の 2022 年初頭のサイバー保険の保険料は 90 億ドルを超えています。2025 年までにこれが 200 億ドルを大きく超えると予想されており [25]、これは AGCS が 2015 年に発表した最初のサイバーリスクレポートで予測した数字でもあります。

25 Munich Re 社：「サイバー保険：リスクとトレンド 2022」（Cyber Insurance: Risks and Trends 2022）

高まるキャプティブとART（代替的リスク移転）への関心

リスク環境の進化とサイバー保険市場の厳しさによって、サイバー保険の加入習慣が変わりつつあります。

ランサムウェアによる損害規模の拡大を受けて、サイバー保険の保険料率は過去 2 年間上昇を続けており、アンダーライティングの基準も厳しくなっています。以前は加入していたリミットやプログラムに加入できない企業や組織も出てきています。その結果、サイバー保険加入希望者の多くが、これまでとは違った、別のサイバー・プログラム構造や別のリスク・ソリューションを検討するようになってきています。

キャプティブは、補償額を増やしたり補償の隙間を埋めたりするための戦術的補完手段としてよく利用されます。近年のランサムウェア攻撃などのサイバー損害を受け、財務上の利益と組織の保護を両立するためにキャプティブの活用を検討する企業が増えてきています。

「保有率は全般的に向上してきており、企業の自己資金の投入も増えてきています。その結果、サイバー保険におけるキャプティブやバーチャル・キャプティブの活用への関心も高まっています。」と **Jens Krickhahn（Practice Leader Cyber Insurance, Central and Eastern Europe, AGCS）**は追認します。

米国でも保有率が大幅に増加しており、リミットの需要にブレーキをかけているのは保険料だと **Stephens** も同意見です。その結果として多くの企業が、サイバー保険の効果を最大化するとともに、高い保有率を実現するためのコスト捻出方法を模索しています。「フロンティング保険やテイラーメイドソリューションなど、サイバー向けの代替的リスク移転ソリューションに関するお客様との会話が増えています。」

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
Shakun Raj
shakun.raj@allianz.com
+65 6395 3817

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

North America
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 973 876 3902

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

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

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

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

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

2022 年 10 月