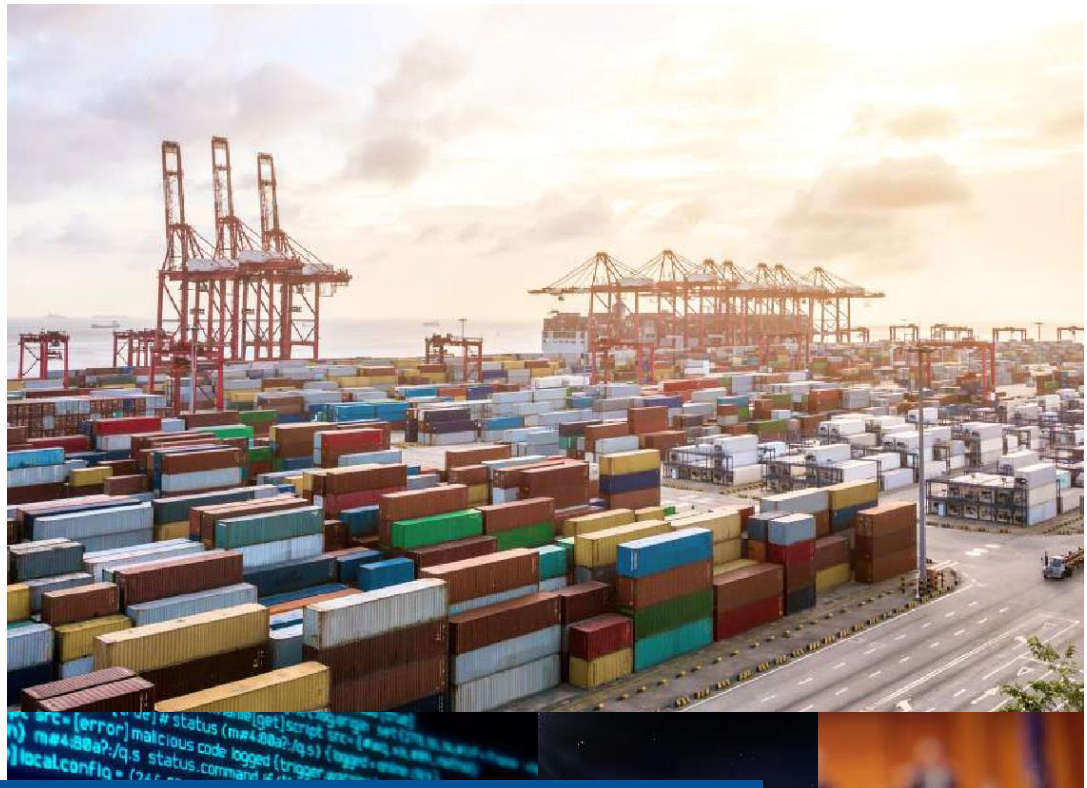
アリアンツ・リスクバロメーター

2019年 トップビジネスリスク

80ヶ国以上、2400人に及ぶリスクマネジメントの専門家が考える企業にとっての2019年の最大の脅威とは

Allianz



ALLIANZ GLOBAL CORPORATE & SPECIALTYについて

Allianz Global Corporate & Specialty (AGCS) は、アリアンツグループにおいて企業保険およびスペシャルティ保険を専門に扱う保険会社です。AGCSでは、あらゆるスペシャルティ分野、代替的リスク移転、ならびに企業分野にわたり保険とリスクコンサルティングサービスを提供します。

保険商品ラインアップ:

- 代替的リスク移転
- 航空（宇宙を含む）
- エネルギー
- エンジニアリング
- エンターテイメント
- フィナンシャルライン（会社役員賠償責任保険［D&O］を含む）
- 賠償責任
- 貨物・船舶
- 中堅企業
- 財物（グローバル保険プログラムを含む）

AGCSは世界34ヶ国に拠点を有し、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210を超える国や地域でサービスを提供しています。また、70ヶ国以上の国籍の約4,700名の従業員が勤務しています。

AGCSは**Fortune Global 500**企業の75%以上に保険ソリューションを提供し、2017年のグロス保険料は74億ユーロに上ります。

AGCS SEは、Standard & Poor's でAA、A.M. Best でA+の格付けを取得しています。

アリアンツ・リスクバロメーターの分析手法

今年で8回目となる**アリアンツ・リスクバロメーター**は、過去最大の86ヶ国、2,415人の回答者の知見が盛り込まれています。この年次企業リスク調査は、アリアンツのお客様（グローバルに事業展開する企業）、ブローカー・代理店、および各種業界団体を対象に行ったもので、さらにAllianz Global Corporate & Specialty（AGCS）をはじめとするアリアンツグループ会社のリスクコンサルタント、アンダーライター、上級マネジャー、およびクレーム専任者も調査に参加しています。

回答者への調査は2018年10月から11月にかけて実施し、大企業をはじめ中小企業も調査対象としています。回答者には特に知見の深い業界を選択していただき、各業種について最大3つの最重要リスクを挙げていただきました。回答者は、最大2業種について回答することができ、そのため回答者2,415人から合計2,882件の回答が寄せられています。

回答の大半は大企業（年間収益5億ユーロ超）に関するもの（1,445件、50%）、中規模企業（年間収益 2.5億～5億ユーロ）については619件（21%）、小規模企業（2.5億ユーロ未満）については818件（28%）の回答となっています。また、22業種のリスク専門家が参加しています。

アリアンツ・リスクバロメーターにおけるランキングの変化は、パーセンテージの前年比ではなく、ランキングの前年比によって決定されています。

通貨表記は特に記載のないかぎり米ドル表記となっています。

↘ **地域、国、業種ごとのすべてのリスクデータはこちら。**

2,415
回答者数

86
国数

2,882
回答数

22
業種

もくじ

03 分析手法

04 2019年 グローバルビジネスリスクトップ10

06 2019年 世界各国のビジネスリスク

08 エクゼクティブサマリー

10 1位 事業中断

12 2位 サイバーインシデント

14 着目テーマ：
サイバー事業中断

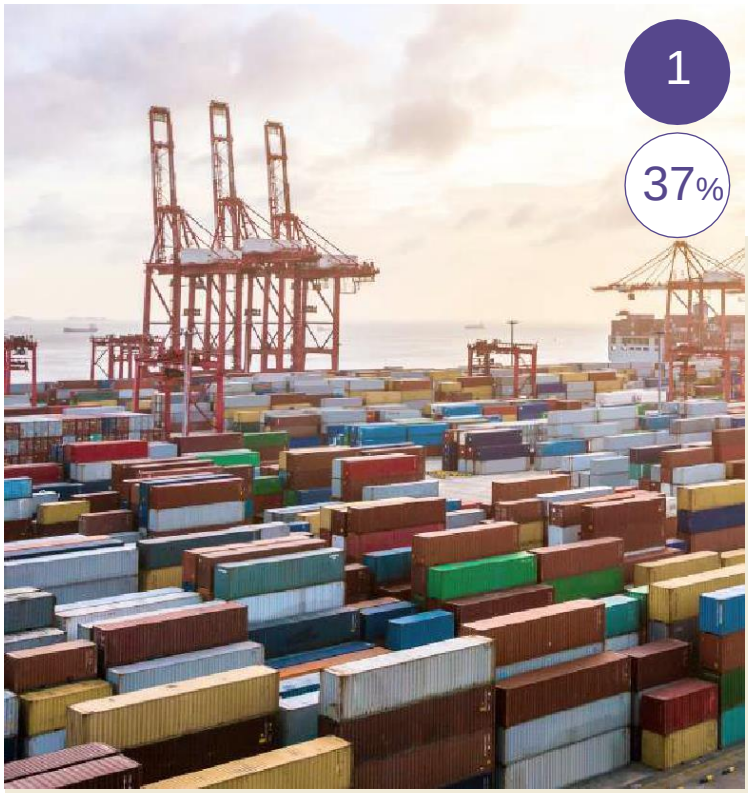
16 3位 自然災害

18 ビジネスリスク：4位～10位

22 中小企業 （SME）のビジネスリスク

24 お問い合わせ先

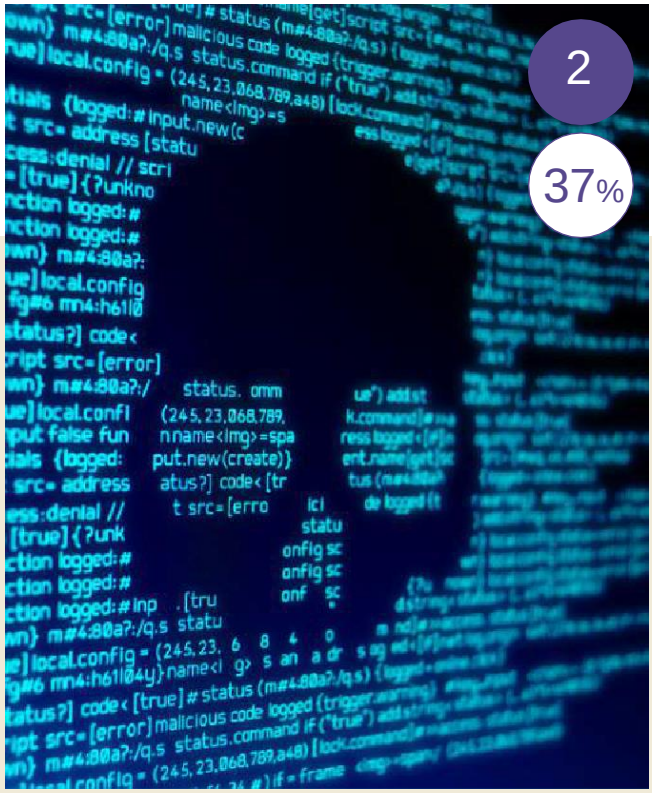
出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、2,415人の回答者から寄せられた全調査回答数（2,882件）の中で回答者が選んだリスクの数をパーセンテージで表したものです。回答者は、最大2業種について回答することができます。また回答者は1業種当たり最大3つまでのリスクを選択することができます。
アリアンツ・リスクバロメーターにおけるランキングの変化は、パーセンテージの前年比ではなく、ランキングの前年比によって決定されています。



=2018:1位（42%）

事業中断（BI）

（サプライチェーンの混乱を含む）



=2018:2位（40%）

サイバーインシデント[1]

（例：サイバー犯罪、IT障害／機能停止、データ漏洩、罰金、処罰）

1 **BIとサイバーインシデントは37%で同順位トップだが、回答数ではBIが上回る。**

2 火災、爆発は、回答数では新技術を上回る。

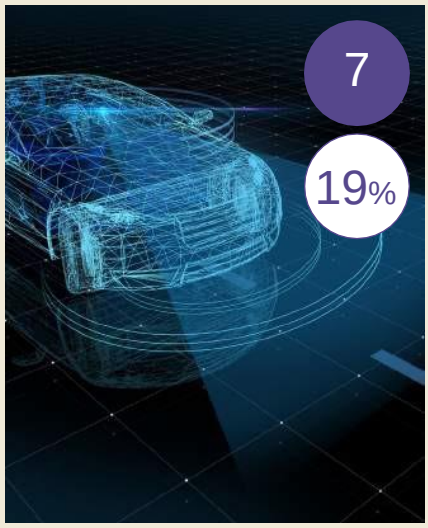
3 気候変動／異常気象の増加は、回答数ではレピュテーション・ブランド価値喪失を上回る。

凡例

- ▲ **2018年よりもリスクが高い**
- ▼ **2018年よりもリスクが低い**
- = **2018年から変化なし**
- 1 **2018年のリスクランキング**

=2018:6位（20%）

火災、爆発



=2018:7位（15%）

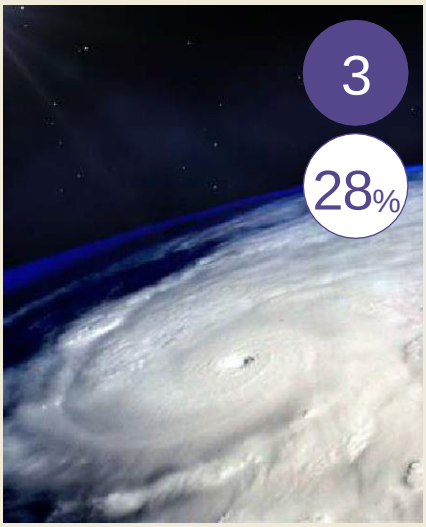
新技術[2]

（例：相互接続の高まり、ナノテクノロジー、人工知能、3Dプリンティング、自律運転車、ブロックチェーンなどによる影響）

アリアンツ・リスクバロメーター

2019年グローバルビジネスリスクトップ10

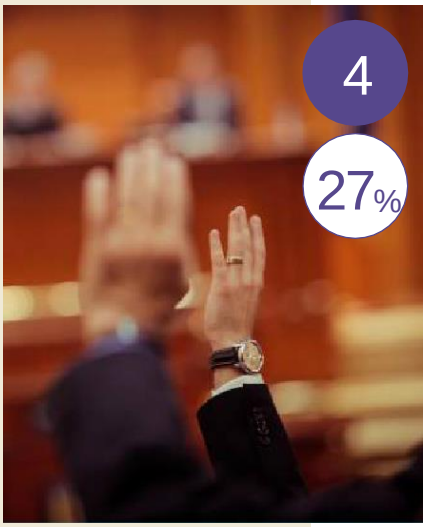
↘リスクバロメーター2019年のすべてのランキングはこちら。



(=) 2018: 3 位 (30%)

自然災害

（例：暴風雨、洪水、地震）



▲ 2018: 5 位 (21%)

法規制変化

（例：貿易戦争や関税、経済制裁、保護主義、Brexit、ユーロゾーン解体）

▼2018: 4 位 (22%)

市場動向

（例：ボラティリティ、競争の激化／新規参入者、M&A、市場停滞、市場変動）

▲ 2018: 10 位 (10%)

気候変動／異常気象の増加

▼2018: 8 位 (13%)

レピュテーション・ブランド価値の喪失[3]

▲ NEW

熟練労働者の不足

スナップショット：2019年 世界各国のトップビジネスリスク

米国
「米国で事業中断（BI）が最上位のビジネスリスクとしてサイバーインシデントを上回ったことが状況をよく表しています。これは従来からのリスクと新たに登場したリスクに対する脆弱性に関して今日のリスクマネジャーが直面する課題の大きさを物語っています。昨年のレポートからこれらの2つのリスクの順位は入れ替わっていますが、どちらのリスクにも依然として大きな注目が集まっており、これらの2つのリスクの繋がりが深まり続けている状況により更に混乱要因となっています」。
BILL SCALDAFERRI, PRESIDENT & CEO, AGCS NORTH AMERICA

ブラジル
「ブラジルでは、多くの企業にとってe-コマースや金融取引のデジタル化のリスクが高まっていることを受けて、サイバーインシデントがトップに挙がっています」。
ANGELO COLOMBO, CEO, AGCS SOUTH AMERICA

英国
「法規制変化がサイバー攻撃と並んで新たに英国で最大のリスクに挙がっていることはさほど驚くことではありません。Brexitに伴う不確実性、さらには規制の重荷やグローバルな貿易戦争の高まりによって自信が揺らいでいることに加え、サイバー攻撃の脅威にも英国企業は引き続きさらされています」。
TRACEY HUNT, DEPUTY CEO, AGCS UK

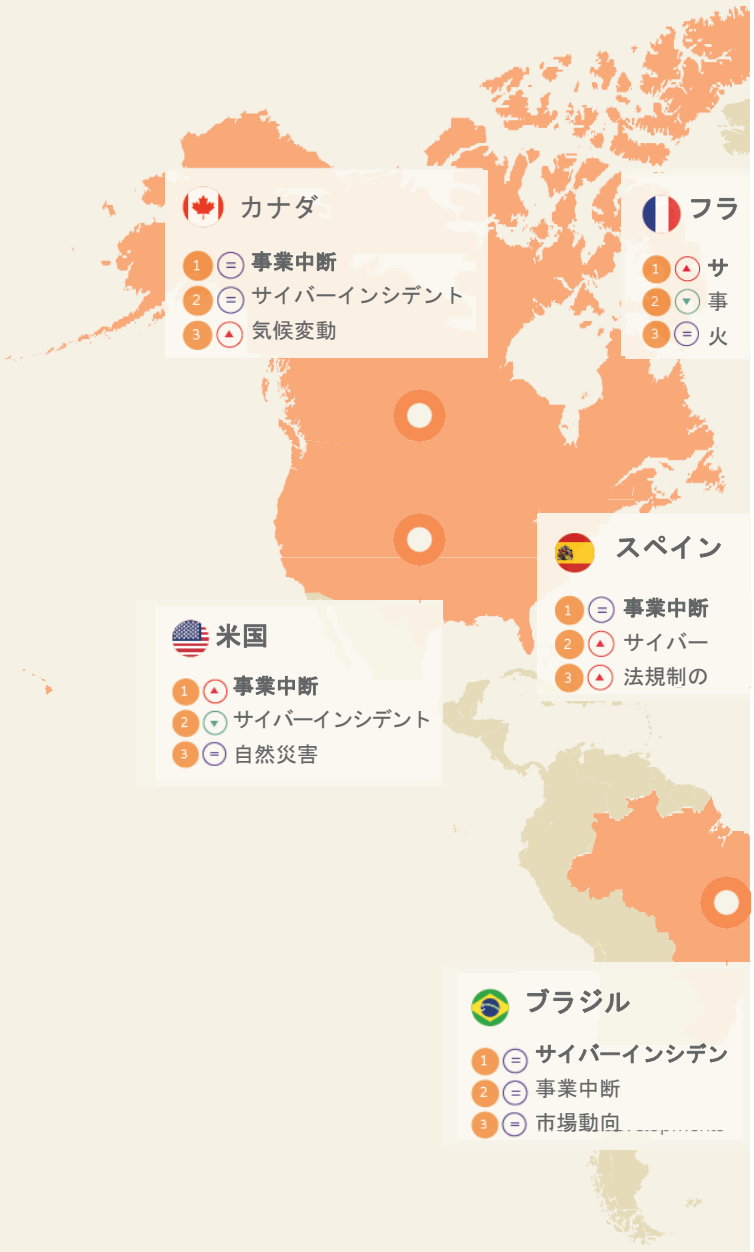
カナダ
「新たに採用された個人情報漏洩報告義務をはじめとする法規制の変化は、カナダのリスク展望に引き続き大きく影響しています。気候変動と自然災害が、環境リスクとともにトップ10に挙がっている状況にも変わりはありません。このようなリスクの中には、自然災害によって引き起こされる汚染リスクで事業中断に至るものも含まれます。どちらのリスクに関しても、構外利益（CBI）をカバーする保険商品を含めた保険ソリューションの需要が高まっています」。
ULRICH KADOW, CEO, AGCS CANADA

ドイツ
「ドイツ企業にとって最大のリスクとなっているのは、サイバーと事業中断です。サイバーインシデントを原因とする事業中断が増えていることから、これら2つのリスクの繋がりがますます深まっています。NotPetyaやWannaCryなどのランサムウェア攻撃により、大規模な混乱とグローバルな大規模損害を被っている企業もあります。ネットワーク化とITインフラの共通化が進むにつれて、サプライチェーンのあらゆる接点がサイバー攻撃の標的となりえます。そのためリスクマネジャーや保険会社にとって、これらの2つの厄難に対して有効な対策を講じることは、単に選択肢の一つなのではなく、義務なのです」。
CHRIS FISCHER HIRS, CEO, AGCS

フランス
「フランスの企業は、サイバーインシデントの発生頻度と影響度が高まっていることにますます不安をつのらせており、それを反映して初めてフランスでサイバーがリスクの最上位にランキングされました」。
CORINNE CIPIÈRE, CEO, AGCS FRANCE

イタリア
「近ごろの食品リコール件数の増加を受けて、食品リコールリスクがイタリアのランキングに新たに挙がってきています（4位）。
NICOLA MANCINO, CEO, AGCS ITALY

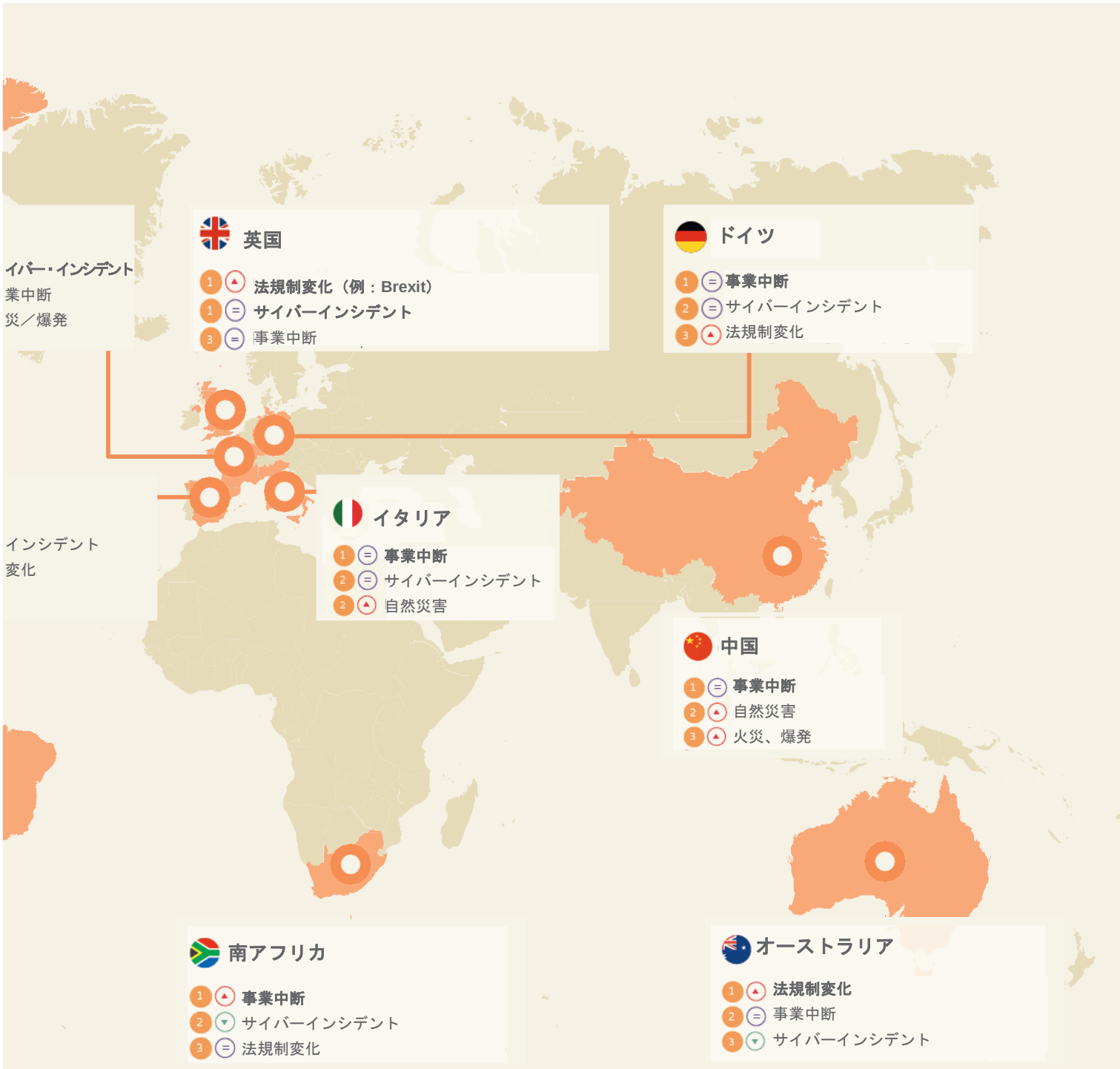
スペイン
「現地の重要機関へのサイバー攻撃が複数件発生していることを反映して、スペインではサイバーインシデントが前年の4位から2位にランキングを上げています」。
JUAN MANUEL NEGRO, CEO, AGCS SPAIN



アジア太平洋
「アジア太平洋地域の多くの企業は、事業中断の影響に大きな懸念を抱いています。現在、財物保険での事業中断事故の平均支払額は300万ユーロを超えています。製造業が東方にシフトしていること、域内で発生する自然災害の頻度が高まっていることなどを反映して、アジア太平洋地域では事業中断による損害のリスクが増大しており、包括的なリスクマネジメントの重要性が高まっています」。
MARK MITCHELL, CEO, AGCS ASIA PACIFIC

このリスクマップでは選定した国におけるビジネスリスクのトップ3を表示しました。
出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ

↘ 地域、国、業種ごとのすべてのリスクデータはこちら。



アフリカ

「アフリカでは、政情不安や政策の不確実性が問題となっており、これが企業や投資家の信頼を損なう大きなリスク要因となっています。アフリカがグローバルな競争力を獲得するためには、技術発展の最先端を行く必要がありますが、新技術によりサイバーインシデントが引き起こされる可能性にも留意が必要です。アフリカの企業にとっては、近代的なリスクマネジメント手法と、信頼できる保険ソリューションを取り入れることで、これらのリスクを軽減していくことがきわめて重要です」。
THUSANG MAHLANGU, CEO, AGCS AFRICA

凡例
▲ 2018年よりもリスクが高い
▼ 2018年よりもリスクが低い
= 2018年から変化なし

エクゼクティブサマリー

テクノロジーは、これまでになかった脅威を引き起こすばかりでなく、新たなビジネスモデルを生み出すものでもあります。自然災害のような従来からのリスクも引き続き大きな問題ではあるものの、**アリアンツ・リスクバロメーター**に今回初めて事業中断（BI）とともに僅差でトップにランキングされたサイバーリスク、さらにはレピュテーションへのリスク、無形財産へのリスク、企業環境のボラティリティや統合に関わるリスクも日々進化を続けています。

事業中断（BI）は、アリアンツ・リスクバロメーターの上位に挙がる多くのリスクの結果として生じることもあり、7年連続で企業にとって最大の脅威としてランキングされています（回答の37%）。AGCSの調査によれば、財物保険での事業中断クレームの平均支払額は300万ユーロ（340万ドル）を超えて、現在は310万ユーロに達しています。この額はその対象ロスの財物損害の平均支払額（220万ユーロ）を39%も上回り、総額は5年前よりも大幅に膨らんでいます。また、大規模事案による損害額は数億ユーロ、またはそれを超えることもあります。企業はさまざまな場面で事業中断のリスクにさらされており、物的な被害はなくても損害額が大きくなる場合もあります。事業を停止状態に追い込んでしまうような事案としては、中核ITシステムの機能停止、製品リコール、品質関連事案、テロ、政治暴力や暴動、環境汚染などがあり、それにより製品やサービスが提供できなくなったり、利用者が遠のくなどして、収益に破滅的な影響が及ぶこともあります。例えば、2018年末の4週にわたって毎週末に行われたフランスのデモの際には、小売業は約10億ユーロ（11億ドル）の損害を被っています[1]。今日の不確実な政治状況では、法規制の変化 — 例えばサプライチェーンへの混乱が予想される2019年予定のBrexitなど — も潜在的な事業中断リスクとなってきます。↘ 10ページ

今回は、これまで事業中断が占めていた最上位のランキングに**サイバーインシデント**（37%）[2]が初めて加わっています。AGCSの分析によると、サイバーインシデントによる保険での平均支払額でさえ、現在は火災／爆発事案の150万ユーロ弱を超えて200万ユーロ（230万ドル）[3]を上回る水準にあり、大規模事案による損害額は数億ユーロ、またはそれを超えることもあります。また、サイバーインシデント自体が事業中断損害を引き起こす例も増えています。企業の主要な資産がデータやサービス基盤であったり、顧客やサプライヤーの集団である場合も多い状況を反映して、回答者がサイバーを最も恐れる事業中断要因として挙げています。

海運、物流、製造業に混乱をもたらした2017年の**WannaCry**と**NotPetya**によるマルウェア攻撃の目立った特徴として事業中断損害がありました。サイバーインシデントが引き金となった事業中断損害の件数は増えてきており、業界全体のロスは1億ドルを超えています。

多くの事案は、悪意のある行為ではなく、技術的な異常やヒューマンエラーによるものです。英国の金融サービス規制当局の分析によれば、ITシステムの機能停止は1年で138%増加しているものの、報告された事案のうちサイバー攻撃に起因するものは18%にとどまっています[4]。

ITシステムの機能停止は大きなリスクをはらんでいます。電力サージやITプラットフォーム移行の失敗などは数億ユーロ単位の損害を招くことがあります。クラウドサービス、オンライン予約プラットフォーム、サプライチェーンシステムなど、ITサービスプロバイダーへの依存度が高まることは、構外利益（CBI）リスクを伴います。2018年には、ネットワーク機器を提供するエリクソン社でのソフトウェアの異常により、ヨーロッパと日本で何百万人もの携帯電話利用者のサービスに障害が発生しました[5]。また2017年には、アマゾン社のAWSクラウドコンピューティング部門の機能が4時間停止したことにより、インターネットサービスやウェブサイトをはじめとする多くの企業が影響を受け、その結果としてこれらの企業は約1.5億ドルの損害を被っています[6]。機能停止の時間がこれよりもさらに長くなった場合、損害額が10億ドル近くに達することも考えられます。↘ 14ページ

1 BBCニュース：黄色ベストデモはフランスにとって「経済的な大惨事」（Yellow vest protests 'economic catastrophe' for France）2018年12月9日

2 事業中断とサイバーインシデントは37%で同順位。回答数では事業中断が1,078件で、サイバーインシデントの1,052件を上回る。

3 2013～2018年にかけて保険業界に寄せられた115件のサイバークレームの平均支払額は2,007,653ユーロ。

4 金融行為監督機構：英国の金融サービス業のサイバーとテクノロジーに対する回復力（Cyber and technology resilience in UK financial services））2018年11月27日

5 ロイター：英国と日本でモバイル業務に障害をもたらしたソフトウェア異常についてエリクソン社が謝罪（Ericsson sorry for software glitch that hits mobile services in Britain and Japan）2018年12月6日

昨年が大きな転機となり、サイバーインシデントに対する懸念が高まっています。サイバー犯罪に関わるコストは2014年に4,450億ドルだったものが、現在は6,000億ドルに上るものと推定されています[7]。これは自然災害による経済的損失額の10年平均、2,000億ドルという数字の3倍に上る水準です。また、国家による重要データや企業秘密の盗難の脅威も高まっており、企業への影響も懸念されます。

大規模なデータ漏洩やプライバシーに関わるスキャンダルをはじめ、プライバシー関連規制の強化のきっかけとなり、他地域においても罰金額の高額化を招く恐れのあるヨーロッパの一般データ保護規則（General Data Protection Regulation＝GDPR）による影響も、企業の懸念材料となっています。また、サイバーインシデントが有価証券関連訴訟や集団訴訟など、訴訟に発展する可能性も高まっています。↘ 12ページ

すべての企業は、事業規模、事業内容、リスクプロファイルに応じたITセキュリティー対策を講じる必要があり、技術セキュリティー対策、適切なバックアップ体制、そして社員教育への投資が求められます。サイバー脅威の高まりと、それによるレピュテーション喪失の懸念が高まる中にあって、社員教育は中小企業においても同じく重要な課題となります。 ↘ 22ページ

自然災害（28%で3位）の分野では、記録的な損害額に達した2017年に引き続き、2018年には北アメリカのハリケーン・マイケルとフローレンス、日本の台風ジェビ（21号）、カリフォルニア州の山火事などにより、およそ1,460億ドルの経済的損害が生じています[8]。回答者は、近年の事象が経済的損失や混乱がさらに増加する前触れかも知れないと懸念しており、そのため**気候変動**（13%で8位）が過去最高位のランキングに入ってきています。気候変動はまた、財物への損害や混乱ばかりでなく、規制や賠償責任の面でも大きく影響してくることが考えられ、排出ガス目標はすでに航空や海運などの産業のあり方を方向付ける要素となっています。また、報告義務や情報開示要件の強化により、企業、そしてその取締役や役員のリスクも高まることになります。↘ 16ページ、20ページ

貿易戦争、関税、**Brexit**により不確実な状況が続く中で、**法規制変化**（27%で4位）に対する企業の懸念が12ヶ月前よりも高まっており、サプライチェーンの回復力に関する懸念も高まっています。また**市場動向**（23%で5位）についても、2018年がボラティリティ、ダイバージェンス、そして不測の出来事の発生が記録的な水準に達した年となり、2019年もこの傾向が続くものと予想されることから、引き続き上位5位以内にランキングされています。**火災／爆発**事故（19%で6位）による影響は長年の懸念材料で、AGCSの分析によれば、過去5年間の火災（山火事を除く）による保険支払額は140億ユーロ（159億ドル）を超え、企業損失の最大の要因となっています。

新技術（19%で7位）は、これまでになかったリスクマネジメントの手法を実現するなど、企業にとっては大きなチャンスをもたらします[9]。その一方で、ネットワーク接続された機器が増えるにしたがって、セキュリティー、データ保護、事業継続、第三者賠償責任、さらには危機的なインフラ破綻などに関する課題もはらんでいます。ドローンの飛行により英国のガトウィック空港で1,000便あまりが欠航となった2018年12月の事案など、不測の事態が現在も発生しています。また近年、航空会社、自動車メーカー、銀行、チャリティー団体などが、製品リコール、サイバーインシデント、企業幹部の行為などによりレピュテーション被害を受けており、ソーシャルメディアを介して危機が短時間のうちに拡大する時代にあって、**レピュテーション・ブランド価値の喪失**（13%で9位）への対策が急務となっています。また、人口動態の変化やBrexitなどにより、**熟練労働者の不足**（9%で10位）が初めてグローバルリスクのトップ10に入っています。
↘ 18ページ

このように数多くの、しかも多様な脅威が存在する中にあって、潜在的な影響をマネージし軽減するためには、これまでになかったリスクマネジメントソリューションをはじめ、ツールやパートナーシップが必要となってきます。保険は、無形のリスクに対してますます有形の支援を提供するものとなっています。サイバー保険では、サイバーインシデントに備え、対抗するための専門的なコンサルタントサービスを活用することができることから、事案への対応の重要な一要素となってきています。サイバー事業中断保険では、ハッキング、技術的障害、従業員のミスなどによってデータやシステムが利用できなくなってしまった場合に、収益の喪失やコスト負担から企業を守ることができます。ノンダメージ事業中断保険では、デモや暴動などの混乱から生じる企業収益の喪失を補償します。レピュテーションリスク保険では、危機が発生した際には助言サービスや対応にかかるコストを提供します。

また、新技術はリスク分析にも寄与しています。今やAGCSなどの保険会社では、サプライチェーンのリスクをよりよく理解するために意味解析を、また、災害後の損害規模を迅速に把握するためにドローンを活用し、インシュアテックとの提携を通じて次世代の訴訟リスクの特定も進めています。ネットワーク化がますます進む世界では、各種端末、工場、サプライチェーンからのデータ、およびさまざまな予測指標を活用してより正確なリスク評価ができるようになり、最終的にはより柔軟でカスタマイズされた、タイムリーなソリューションを提供することにより、損害を未然に防ぐことを目的にリスクをより短時間のうちに把握、管理することができるようになります。

6 Guidewire Cyence Risk Analytics：MMCサイバーハンドブック2018、サイバーリスクの進化とシステムリスクの定量化（MMC Cyber Handbook 2018, Evolution of Cyber Risks Quantifying Systemic Exposures）

7 Center for Strategic and International Studies：サイバー犯罪の経済的影響 — 減少する気配なし（Economic Impact of Cybercrime – No Slowing Down）

8 Swiss Re社、2018年12月18日

9 火災、爆発と新技術が 19%で同順位。回答数では火災、爆発が上回る。

(=) 2019: 1 (37%)

1 重要リスクに着目：事業中断

世界各国で事業中断がトップのリスクに挙がっていますが、これは製品リコールや暴動、さらには環境事案やBrexitに至るまで、リスクの特性が進化を続け、サイバー関連事案も増えてきている状況を反映したものです。

過去5年のリスクランキング（回答数の割合とランキング）
2018: 1 (42%)
2017: 1 (37%)
2016: 1 (38%)
2015: 1 (46%)

リスクのトップとなった国：
- カナダ
- 中国
- ドイツ
- イタリア
- オランダ
- ポーランド
- ポルトガル
- ロシア
- シンガポール
- 南アフリカ
- 韓国
- スペイン
- スイス
- 米国

リスクのトップとなった業種：
- 化学
- 消費財
- 食品／飲料
- 重工業
- ホスピタリティ、レジャー、観光
- 製造（自動車を含む）
- 鉱業
- 石油／ガス
- 電力／ユーティリティ
- 再生可能エネルギー
- 小売業、卸業

アリアンツ・リスクバロメーターによれば、**事業中断（サプライチェーンの混乱を含む）**の影響は回答の37%を占め、7年連続で企業にとって最大のリスクとなっています。そして現状を適格に反映するかたちで、今年初めて**サイバーインシデント（例：サイバー犯罪、IT障害／機能停止、データ漏洩、罰金、処罰）**が同じくトップに並んでいます（37%）[1]。サイバーインシデントはまた、ますますそれ自体が重大な事業中断（BI）損害をもたらす要因となっています（14ページ参照）。

*「サイバーインシデントは、企業の業務を麻痺させ、サービスを提供する能力に重大な障害をもたらすものですが、それでも企業の事業中断を引き起こす数々のトリガーの一つに過ぎません。今回のアリアンツ・リスクバロメーターに挙がる上位リスクの多くが事業中断の原因となる可能性をはらんでいるのです」*と話すのはVolker Muench（Global Practice Leader, Utilities & Services, IT Communication, AGCS）です。

事業中断は、製造工場での火災や自然災害によって生産業務に支障を来すといった従来からのリスクをはじめ、サプライヤーや顧客の施設で発生した財物損害によるサプライチェーンの中断（構外利益［CBI］と呼ばれることが多い）、さらには暴動や内乱など、その原因が何であれ、しかも何千マイルも離れた場所で発生したものだったとしても、企業の収益に甚大な影響を与える可能性があります。そして、その影響はリスクとしてきわめて計量化が難しいものでもあります。

AGCSのクレーム分析ではまた、相互接続が日々進む今日のグローバルな事業環境の中で、財物保険での損害の結果として生じる事業中断の重要性が高まってきている点にも着目しています。現在、財物保険の大規模損害にはほとんどの場合事業中断の要素が関わっており、これまでは50：50程度の比率だったものが、事業中断が損害の大部分を占めることが一般的になっています。現在、財物保険の事業中断損害の平均支払額は310万ユーロと、300万ユーロ（340万ドル）を超え、これに紐付く直接的な財物損害による平均支払額（220万ユーロ）を約39%上回っています[2]。この両方の合計額は5年前と比較して大幅に高額になっています。

事業中断（BI）の原因として、企業が最も恐れるものは？

1. サイバーインシデント
2. 火災／爆発
3. 自然災害
4. サプライヤーの不履行、リーンプロセス
5. 機械故障 [1]

出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、回答をした全参加者（947人）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%とはならない。

1 サプライヤーの不履行は、回答数では機械故障を上回る。

事業中断の原因として企業に最も恐れられているのがサイバーインシデントです。WannaCryやPetyaをはじめとするランサムウェア攻撃などの事案により、企業が大きな混乱に陥り、大規模な経済的損失を被る例が増えています。とはいえ、技術的な障害や従業員のミスによるサイバー事業中断も高い頻度で見られます（*14ページ参照*）。

特に自動車、エレクトロニクス、製薬産業では、サプライチェーンの合理化が進み、企業がより少数のサプライヤーに依存するようになるにつれて、事業中断による損害や構外利益（CBI）にかかわる損害がより大規模に、かつ複雑になる傾向にあります。小規模火災のような事案でも、これらの産業では大きな損害の原因となることがあります。

「例えば自動車産業では、小規模サプライヤーでの一件の火災事故により部品の供給が不足し、サプライチェーンに大きな障害が発生することがあります」と話すのはVolker Muench（Global Practice Leader, Utilities & Services, IT Communication, AGCS）です。「このような事案で保険業界として10億ユーロ（11億ドル）を超える損害が発生した事例もあります。たった一件の火災で工場が閉鎖を余儀なくされ、製造が停止することによりサプライチェーンに損害が発生します。機械故障でも同様の影響が出る場合があります」。

進化を続ける事業中断の脅威

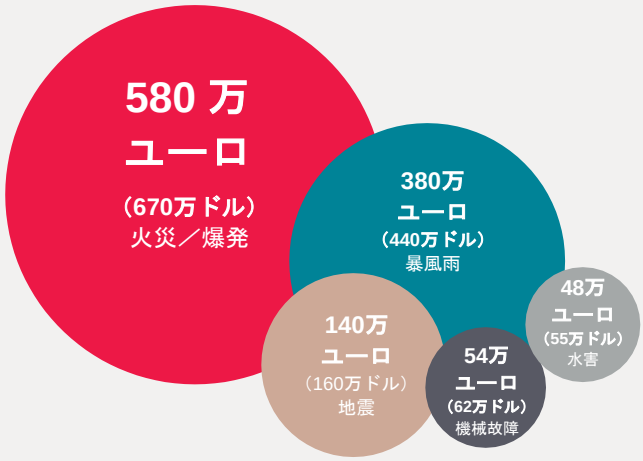
また、ネットワーク化された現在の社会においてリスクの特性が進化を続けるにつれて、企業はますます多くの混乱を招く事業中断シナリオに直面するようになっています。これらのシナリオの中には、物的な損害がないにも関わらず、多額の経済的な損失を招くものも数多くあります。中核ITシステムの機能停止（*14ページ参照*）、製品リコールや品質関連の事案、テロや政治暴力や暴動、環境や汚染に関わる事案、さらには規制の変化などにより、事業が一時的に、または長期にわたり中断し、収益に甚大な損害をもたらす事態にもなりかねません。
製品リコールと品質関連事案は事業中断の脅威として高まってきているとMuenchは話します。「*この種の問題は増えています。サプライチェーン上流のある一つの製品が仕様通りでない場合、プロセス全体、さらには最終製品にまで影響が及ぶことになります。同様の事例は、例えば自動車産業では頻繁に起こっています*」。

Muenchによれば、政治リスク、暴力行為、騒擾などの事案も過去と比較して高い頻度で発生するようになっており、このような事案の間接的な影響により事業中断が発生し、生産停止を余儀なくされたり、影響を受けた地域で利用者の足が遠のくなどによって収益が損なわれたりします。2018年11月から12月にかけてのフランスの暴動やデモのような事案から派生する損害は高額になることと予想されています。例えば、フランス小売業連盟はロイターの取材に対して、デモが始まった11月17日以降の小売業の損害は約10億ユーロ（11億ドル）に上ると回答しています[3]。
また、製造現場や住宅用不動産での汚染、さらにはパイプライン漏れによる汚染のような環境面の問題に企業が見舞われ、それにより事業中断に至るということもあります。これはまた、事業中断リスクの中で見過ごされがちなリスクでもあります。修復や復元作業の長期化や遅延により、出費やサプライチェーンの混乱は短期間のうちに増幅することがあり、その間、企業が業務を行えなくなったり、製品やサービスの供給ができなくなる場合もあります。

さらに、現在の政治状況や事業環境の不確実性の高まり、さらには2019年3月末に予定されているBrexitなどの規制や法の変化も重大な事業中断リスクの要因となります。

*「国境の閉鎖がサプライチェーンの混乱を招くことも考えられます」*とMuenchは話します。*「メーカーが英国産の部品などを必要とする場面、または英国企業が他国製の部品などを必要とする場面では、調達プロセスがこれまでよりも長時間かかることも考えられます」*。

事業中断による出費は？



損害原因別の BI クレーム平均額（一部選択）。
出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ

例えば、英国では合意なき離脱への警戒感が高まる中、小売業やメーカーが倉庫備蓄を急いで進めており、これにより食料品用の倉庫スペースがすでに不足しているとの報告もあります[4]。予定されているBrexit後にはサプライチェーンに障害が生じる可能性があるとの警戒感から、冷凍／冷蔵食品用倉庫は今後6ヶ月間予約で一杯となっており、新たな依頼には対応できない状況となっています。

事業中断対策

事業中断リスクは物的な場合、バーチャルな場合、レピュテーションに関わる場合などがありますが、いずれの場合も経済的な影響は必至です。そのため、十分な計画を立てておく必要があります。企業は、事業復旧がいかに複雑な作業であるかを過小評価してしまうことが多々ありますが、リスクを軽減することはできるのです。確実な事業継続計画を策定し、それを有効なものとするために机上演習で検証を行う必要があります。机上演習は十分な時間的な余裕をもって策定し、各現場特有の脆弱性が検証できるものであることが理想です。

AGCSなどの保険会社は、このような混乱から生じる企業収益の喪失を補償するサイバー事業中断保険やノンダメージ事業中断保険など、これまでになかった保険ソリューションを通じて、企業にこれまで以上の支援を提供しています。AGCSではまた、サプライチェーンのリスクをよりよく理解するために意味解析を活用しています。これによりサプライヤーの関係性を4次サプライヤーまでマッピングすることが可能となり、各リスクや集積リスクに関する問題の特定に役立てることができます。

1 事業中断とサイバーインシデントは37%で同順位トップだが、回答数では事業中断が1,078件で、サイバーインシデントの1,052件を上回る。

2 財物損害と事業中断の両要素が含まれる企業保険損害1,175件の分析による。

3 BBCニュース：黄色ベストデモはフランスにとって「経済的な大惨事」（Yellow vest protests 'economic catastrophe' for France）2018年12月9日

4 Guardian 紙：合意なき EU 離脱への警戒感が高まる中、英国では食料品用の倉庫スペースが不足（UK running out of food warehouse space as no deal Brexit fears rise）2018年 11 月 18 日

(=) 2019: 2 (37%)

2 重要リスクに着目：サイバーインシデント

重大なシステム停止、大規模なデータ漏洩、さらにはこれまでにはなかった対立から派生する脅威の登場に企業が苦悩する中、サイバーリスクがトップに躍り出ています。

過去5年のリスクランキング（回答数の割合とランキング）
2018: 2 (40%)
2017: 3 (30%)
2016: 3 (28%)
2015: 5 (17%)

リスクのトップとなった国
- オーストラリア
- ベルギー
- ブラジル
- フランス
- 香港
- インド
- ニュージーランド
- 英国

リスクのトップとなった業種：
- 航空
- エンターテイメント／メディア
- 金融サービス
- 政府／公益事業
- 専門職サービス
- テクノロジー
- 電気通信

今回初めて、アリアンツ・リスクバロメーターのトップのランキングで**サイバーインシデント**が**事業中断（BI）**と肩を並べました。テクノロジーへの依存度、そして国家や犯罪者による悪意ある活動の高まりから生じる脅威の大きさを反映するかたちで、これらのリスクのつながりがますます深まっています。

サイバー犯罪、個人情報の漏洩、事業中断（BI）（ランサムウェアや分散型サービス妨害［DDoS］攻撃）による損害は高額になることがあります。サイバー犯罪は報道では大きく取り上げられますが、企業でのシステム停止やデータ喪失は、それよりもありふれた技術的障害、ITの異常、ヒューマンエラーが原因であることが多く、これにより多額の損失が生じることもあります。過去5年間の保険業界での保険事故についてAGCSが行った分析によれば、サイバーインシデントによる保険金支払額の平均でさえ、現在は火災／爆発事案による平均支払額の150万ユーロ弱を超えて200万ユーロ（230万ドル）を上回る水準にあり[1]、大規模事案による支払額は数億ユーロ、またはそれを超えることもあります。

昨年が大きな転機となり、サイバーインシデントに対する懸念が高まっています。世界的に大きな混乱をもたらしたWannaCryとNotPetyaのマルウェア攻撃に続いて、2018年は大規模なIT停止、きわめて大規模なデータ漏洩、さらにはプライバシー関連のスキャンダルが発生しており、それに加えて画期的なデータ保護規則が盛り込まれたEUの一般データ保護規則（General Data Protection Regulation＝GDPR）が発効されています。

「*ITが支援的な機能から中核的でビジネスに必須の資産へと移行してから、特にここ数年はサイバーリスクが重要なリスクとして挙がるようになっています*」と話すのはMarek Stanislawski（Deputy Global Head of Cyber and Tech PI, AGCS）。「*顧客にとっては、サイバーがこれまでの『伝統的な』重要リスクと同等の懸念材料となるところまでいよいよ来ており、このことが意味するのは、もはやすべての業種や事業区分の企業がこのリスクを明確に意識しているということです*」。

大規模なデータ漏洩と攻撃が急増

組織が保有する個人データがますます増えるにしたがって、漏洩の規模とそれに伴うコストも膨らんできています。最近の大規模なデータ漏洩としてはEquifax社（1.43億人）、Facebook社（5,000万人）、そしてUber社（5,700万人）の事案がありますが、過去最大級のデータ漏洩としては、2018年末の3.8億人の顧客に影響を与えたMarriott Hotels社の事案があります[2]。

全世界のサイバー攻撃件数は2017年には16万件に膨れあがっていますが、過少報告の風潮も存在することから、Online Trust Alliance社では実際には35万件に上る可能性があるとしています[3]。同時に、Ponemon Institute社とAccenture社では、サイバー攻撃から派生するコストは過去5年間で62%増加しているとしています[4]。Ponemon社によれば、一般的なデータ漏洩のコストは現在では400万ドルである一方で、大規模な漏洩の場合は億ドル単位に上ります。AIR Worldwide社では、Marriott社のデータ漏洩事案のコストは2億～6億ドルに上るものと推定しています[5]。

規制強化と訴訟の高まり

データ漏洩のコストを高めている重要な要素として規制と訴訟があります。2018年5月にはGDPRが発効し、これにより消費者のプライバシー権が拡大されるとともに、規制当局による取締権限が強化され、違反者には高額な罰金が科されます。これ以降、カリフォルニア州、ブラジル、インドなどでこのGDPRを参考に強化されたプライバシー法を導入する計画を発表しています。カナダとオーストラリアでも、GDPRやそれに類似する米国の法令に沿ったかたちで漏洩通知の義務化制度が導入されています。

「*GDPRやそれに相当する規制は『ニューノーマル』なのであり、この中でどのように業務を遂行するかを私たちは考えなければなりません*」とStanislawskiは話します。また、サイバーインシデントが有価証券関連訴訟や集団訴訟など、訴訟に発展する可能性も高まっています。データ漏洩、IT停止、サイバーセキュリティーなどの事案では、問題を起こした企業、または場合によってはその取締役を相手取って、データの対象者、株主、サプライチェーンの取引相手企業などが損害の補償を求めるなど、第三者賠償責任が発生することも考えられます。

米国ではすでにデータ漏洩事案に付きものとなっている集団訴訟はヨーロッパにも広がってきており、精神的苦痛などの非金銭的な損害について消費者が訴えを起こせるようになっています。British Airways社でのデータ漏洩など、GDPRの下で最近発生したいくつかのデータ漏洩事案では英国でも集団訴訟が起こされており、小売企業のMorrison社を相手取った訴訟では、同社の代位責任が認められて、英国におけるデータ漏洩集団訴訟で初めて原告が勝訴しています[6]。

進化する脅威

データ盗難、詐欺、または恐喝などの手法がますます高度化し、サイバー犯罪がまん延してきています。Center for Strategic and International Studies（CSIS）では、サイバー犯罪による全世界の年間損害額は、2014年には4,450億ドルだったものが、およそ6,000億ドルにまで上昇していると推定しています[7]。これは自然災害による経済損失額の過去10年の平均、2,080億ドル[8]の約3倍の水準です。

また、国家が競争や対立の実力行使にテクノロジーを活用する事例が増え、これがビジネスにも影響することから国家による脅威が高まった年でもありました。貴重なデータや企業秘密を盗む目的で、大学や公共セクター機関をはじめ、基幹インフラ企業のネットワークや産業用制御システム（industrial control systems ［ICS］）が、国家やそれに属するハッカー集団の標的となった事例もあります。NotPetyaはウクライナを標的にロシアを後ろ盾とするハッカー集団によって作り出されたものだとされ、中東ではエネルギー企業が破壊的なマルウェア攻撃に見舞われています。

IoTと新技術

技術の進歩によって新たなサイバーの脅威や脆弱性が生み出されています。ますます高まる相互接続性の影響をはじめ、オートメーションや人工知能といった技術の影響について、あらゆる組織が懸念を抱くようになっています。

ネットワーク接続機器の増加、モノのインターネット（IoT）、産業4.0、そしてサプライチェーンのデジタル化により、犯罪者や国家が攻撃に利用できる新たな対象物が生まれ、脆弱性が高まっています。

サイバーセキュリティー企業のKaspersky社では、同社調査対象企業の3/4以上はICS領域でサイバーセキュリティー攻撃の標的になり得ると予想しており[9]、さらにICSに関する最低限のサイバーセキュリティーや規制に従っている企業はわずか23%にとどまっているとしています。2016年に起きたインターネット企業Dyn社に対するDDoS攻撃では、感染したIoT装置で構成されるボットネットの集団が使われており、2018年12月には世界各国5万台のネットワークプリンターがハッカーにコントロールされてしまい、PewDiePieというビデオブロガーを応援するポスターを印刷させられました[10]。

「サイレントサイバー」が静かではなくなる

マルウェアなどのサイバーインシデントによって高まるリスクは事業中断リスク（14ページ参照）だけではなく、物的な損害のリスクも高まることをWannaCryやNotPetyaなどのマルウェア攻撃が知らしめました。また、このことからサイバー保険に関する議論、特に明示的担保の必要性に関する議論に拍車がかかっています。

Property Claims Services社では、NotPetya攻撃による保険会社の支払額は約30億ドルに上ると予想しており、この総額の約90%はいわゆる「サイレントサイバー」リスクに属し、明示的担保による支払いは10%にとどまるとしています。約款上明示されていない補償とは、伝統的な損害保険（P&C保険）に、アンダーライターがそれを意図していなくても、サイバーインシデントが補償されている可能性のあるものをいいます。

「サイレントな」あるいは約款上明示されていないサイバー保険は、どの当事者にとっても確実性と透明性が十分ではなく、企業を十分に守ることができないことも考えられます。アリアンツではグループ全体のプロジェクトとして商業、企業、そしてスペシャルティの保険分野でのP&C保険におけるサイバーリスクについて検証し、「サイレントサイバー」リスクに対応するための新たな引受戦略を構築しました。

*「従来の保険でサイバーリスクがどのようにカバーされるのかを明確に示すとともに、専用のサイバー保険ソリューションが必要となるシナリオも明確にしていきます」*と話すのはEmy Donavan（Global Head of Cyber and Tech PI, AGCS）です。

Stanislawskiは次のように付け加えます。*「リスク移転はサイバーリスク管理の重要な要素ですが、今日のサイバー保険はさらにその先を行くものです。専門家やコンサルタントとの繋がりを確保できることで、その力を借りて事案に対処することができ、さらには事案発生前により周到な備えを整えることができるなど、事案への対応の重要な一要素となることが考えられます」。「すべての企業は、事業規模、事業内容、リスクプロファイルに応じたITセキュリティー対策を講じる必要があり、技術セキュリティー対策、適切なバックアップ体制、そして社員教育への投資が求められます。このうち社員教育は最も見過ごされがちなものかも知れませんが、中小企業にとっても同じく重要な課題です」。「企業は、全社員をサイバーセキュリティーチームの一員と見なし、適切な教育を通じて自信を与えることで、社員を『最も弱い鎖の輪』から『防御の最前線』へと変革する必要があります」。*

1 Allianz Global Corporate & Specialty：サイバーが損害の原因だった 115 件のロスにおけるサイバー損害の平均支払額。火災、爆発による平均損害額 — グローバル・クレーム・レビュー、企業保険損害の上位の要因

2 ロイター：Marriott 社は大きな損害をもたらした Starwood ハッキング事案の規模推定を下方修正（Marriott cuts estimate on size of massive Starwood hack）2019 年 1 月 4 日

3 Online Trust Alliance：サイバーインシデントトレンドレポート（Cyber Incidents Trends Report）2018 年 1 月

4 Accenture 社：サイバー犯罪のコストに関する 2017 年調査（2017 Cost of Cyber Crime Study）

5 AIR Worldwide 社：Marriott 社のデータ漏洩による損害が 2～6 億ドルになると AIR Worldwide 社が推定（AIR estimates losses for the Marriott breach will be between USD 200 million and USD 600 million）

6 BBC News：Morrisons 社はデータ漏洩の難題に敗北（Morrisons loses data leak challenge）2018 年 10 月 22 日

7 Center for Strategic and International Studies：サイバー犯罪の経済的影響 — 減少する気配なし（Economic Impact of Cybercrime – No Slowing Down）

8 Swiss Re 社：2018 年暫定シグマ推定（Preliminary sigma estimates for 2018）2018 年 12 月 18 日

9 Kaspersky：2018 年 産業界のサイバーセキュリティーの現状（The State of Industrial Cybersecurity 2018）

10 BBC News：PewDiePie プリンターハッカーの再来（PewDiePie printer hackers strike again）2018 年 12 月 16 日

着目テーマ：

サイバー事業中断

原因がサイバー攻撃であれ、それよりも高頻度で発生するシステム停止や故障であれ、ネットワーク化が進み、データやサービス基盤、さらには顧客やサプライヤーの集団が企業の主要な資産を成すことも多い今日の企業にとって、サイバーインシデントは今や事業中断（BI）の大きな原因となっています。

サイバーインシデント後の事業中断（BI）は企業にとって重要なリスクの一つとして浮かび上がってきており、混乱に至るシナリオも増え続けています。アリアンツ・リスクバロメーターの回答者が今回初めて、サイバーインシデントについて事業中断（BI）リスクと同程度の懸念を抱いていることがわかりました。事業中断リスクは、過去7年間でトップの脅威で、サイバーとも密接な関係にあります。

多くの企業にとってリスクが最も大きいのはこの領域です。きわめて高度なサプライチェーンを持ち、毎日、または毎月何百万ドルもの収益を稼ぎ出すオペレーションを運営する巨大な組織を考えてみてください。サイバーインシデントによる技術的な問題でそれが機能停止した場合には、組織の規模によっては大きな損害を招くおそれがあります。

*「すべての企業がデジタル化されたビジネスモデルを導入しているので、成功のかなりの部分は、技術によって事業をいかに促進するかにかかっています」*と話すのはGeorgi Pachov（Global Practice Leader, Cyber, AGCS）です。*「技術的な異常によって収益源が断たれてしまうということは想像に難くありません。業務を行ううえでの技術やデータへの依存が非常に高まっていることから、事業中断に至るようなサイバーインシデントの発生頻度は今後ますます高まっていきます。IoT時代において、2台の製造装置が相互に通信できず、データも交換できなくなってしまうような状況となれば、事業中断は避けられません」*。

サイバーインシデント後の経済的損失の主要な要因は？

出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、回答をした全参加者（968 人）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%とはならない。

1. 事業中断、デジタル化されたサプライチェーンへの影響（収益の喪失）
2. レピュテーションの喪失
3. データ漏洩後の賠償責任クレーム（例：他の企業や個人から）
4. 回復／データ復旧コスト
5. 罰金、処罰

*「連日あらゆるサイバーインシデントが発生し、報道でも取り上げられますが、その多様性とすべての企業の経営議題である『デジタル戦略』とを考え合わせたときにはっきりといえることは、企業が事業を継続し続け、競争力を保つためには、革新と技術的な進歩が必要であり、それに伴ってサイバー脅威のリスクも高まることになるということです」*と Georgi Pachov（Global Practice Leader, Cyber, AGCS）は話します。*「事業成長のための技術革新を進めることと、それに関わるデジタルリスク管理のバランスをとることがきわめて重要となってきます。サイバー事業中断保険はこれを可能にする重要な要素の一つとなりえます」*。

損害状況

海運、物流、製造業に大きな損害をもたらした2017年のWannaCryとNotPetyaによるマルウェア攻撃の目立った特徴として事業中断による損害がありました。Maersk社とFedEx社はいずれも3億ドルという記録的な損害を被り、消費財メーカーのReckitt Benckiser社では1億ポンド（1.3億ドル）の収益減に見舞われています。

マルウェア攻撃は現在も企業を悩ませており、一例として半導体メーカーでアップル社の重要サプライヤーでもあるTaiwan Semiconductor Manufacturing Company社が、台湾工場内の機器へのウィルス感染により1日以上生産が中断した2018年8月の攻撃があります。このウィルスは、WannaCryの別種でした。また、2018年9月に発生したバルセロナ市とサンディエゴ市へのランサムウェア攻撃では、サーバーや事務システムに影響が出ています。7月には船会社COSCOの米国内のITシステムが機能不全となっています。保険業界によると、サイバーインシデントを原因とする事業中断のクレーム件数は増えてきており、ロスの中には1億ドルを超えるものもあります[1]。

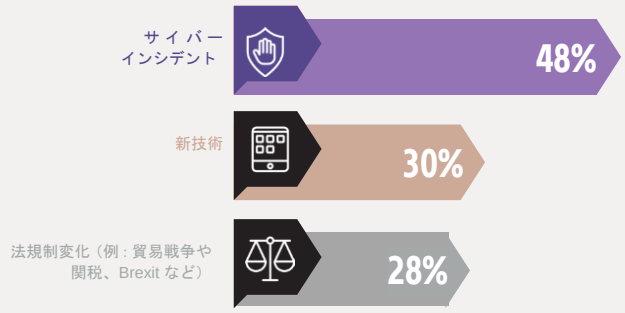
頻発するヒューマンエラーと技術的異常

アリアンツ・リスクバロメーターの回答者によれば、サイバーインシデントは企業が事業中断の原因として最もおそれるものであり、事業中断はまた、サイバーインシデント後の経済的損失のもっとも大きな原因となっています。収益の減少や業務コストの増加などは、悪意ある行為から生じることもありますが、それよりも技術的な異常やヒューマンエラーが原因であることのほうが多いのです。英国の金融行為監督機構（FCA）によれば、同機構に報告されたサイバーインシデントのうちサイバー攻撃は18%に過ぎず[2]、残りの82%は技術的な問題に原因がありました。一方で、Kroll社によるデータ漏洩事案の分析からは、漏洩の88%はヒューマンエラーによるもので、サイバー攻撃によるものは12%に過ぎません[3]。

機能停止やCBIリスクの高まり

企業の日常業務での技術への依存が高まるにつれて、IT機能停止は大きなリスクとして浮上しています。航空輸送産業では技術関連での機能停止事案がいくつか発生しており、2017年の英国航空社システムの一件では、再接続の際の電圧サージによりシステムが休暇期間中に機能停止となり、当初の推定では75,000人もの旅客に影響が出て、コストは8,000万ポンドに及んでいます[4]。また、2018年には英国のTSB銀行がITプラットフォームの移行作業に失敗し、何ヶ月もの間顧客に支障が出ました。この一件で銀行が被ったコストは3億ポンドを超えています[5]。FCAではまた、銀行での機能停止は過去1年間で138%も増えていると報告しています[6]。

今後 3〜5 年に新たに登場してくるビジネスリスクの上位は？



出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、回答をした全参加者（2415 人）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%とはならない。

クラウドサービス、オンライン予約プラットフォーム、サプライチェーンのシステムなど、ITやテクノロジーサービスプロバイダーへの依存度の高まりは、構外利益（CBI）リスクを伴うことになります。2018年には、ネットワーク機器を提供するエリクソン社でのソフトウェア異常により、ヨーロッパと日本の何百万人もの携帯電話利用者へのサービス障害が発生しています[7]。2018年のVisa社の機能停止では、ヨーロッパ全域の銀行や小売業者が利用する支払いカードサービスに影響が出ました。また2017年には、アマゾン社のAWSクラウドコンピューティング部門の機能が4時間停止しことにより、インターネットサービスやウェブサイトをはじめとする多くの企業が影響を受けていますが、この機能停止はヒューマンエラーが原因だったと報告されています。この際、アマゾン社のサービスに依存するS&P 500企業の損害総額は1.5億ドルにのぼったとGuidewire Cyence Risk Analytics社では推定しています[8]。

また、クラウドサービスプロバイダーで12時間以上の機能停止が発生し、北米とヨーロッパでそれぞれ3業種（金融、ヘルスケア、小売）、5万社の企業が影響を受けたという想定を考えた場合、損害総額は北米では8.5億ドル、ヨーロッパでは7億ドルに上るとも推定されています[9]。

*「たった一つの故障箇所が、サプライヤーから最終顧客までのバリューチェーン全体にわたって連鎖反応を起こし、重大な事業中断、そして保険会社には大きな損害を与える可能性があります。また、同じ事案によりレピュテーションの喪失が伴うこともあるのです」*とPachovは話します。

1 Allianz Global Corporate & Specialty：グローバル・クレーム・レビュー、企業保険損害の上位の要因

2 金融行為監督機構：英国金融サービスにおけるサイバーと技術回復力（Cyber and technology resilience in UK financial services）2018 年 11 月 27 日

3 Kroll 社：情報コミッショナーへのデータ漏洩報告は 75%増加（Data breach reports to Information Commissioner increase by 75%）2018 年 9 月 4 日

4 Financial Times 紙：75,000 人の旅客が立ち往生した IT 故障による英国航空の負担は 8,000 万ポンド（BA faces £80m cost for IT failure that stranded 75,000 passengers）2017 年 6 月 15 日

5 ロイター：TSB 停止コストがあったにも関わらずスペインのサバデルは予想を上回る（Spain's Sabadell exceeds forecasts despite TSB outage costs）2018 年 10 月 26 日

6 金融行為監督機構：英国の金融サービス業のサイバーとテクノロジーに対する回復力（Cyber and technology resilience in UK financial services））2018 年 11 月 27 日

7 ロイター：英国と日本でモバイル業務に障害をもたらしたソフトウェア異常についてエリクソン社が謝罪（Ericsson sorry for software glitch that hits mobile services in Britain and Japan）2018 年 12 月 6 日

8 Guidewire Cyence Risk Analytics：MMC サイバーハンドブック 2018、サイバーリスクの進化とシステムリスクの定量化（MMC Cyber Handbook 2018, Evolution of Cyber Risks Quantifying Systemic Exposures）

9 Guidewire Cyence Risk Analytics、Allianz Global Corporate & Specialty、アリアンツ・リスクバロメーター 2018

2019: 3 (28%)

3 重要リスクに着目：自然災害

自然災害を原因とする経済的損失が増大し、気候変動に関する懸念が高まるにつれて、自然災害リスクを有効なかたちでマネージするためには、企業と保険会社はともに、変化し続ける世界中のリスクに対して先手を取って対応していく必要があります。

過去5年のリスクランキング（回答数の割合とランキング）
2018: 3 (30%)
2017: 4 (24%)
2016: 4 (24%)
2015: 2 (30%)

リスクのトップとなった国：
- アルゼンチン
- チリ
- インドネシア
- 日本
- トルコ

リスクのトップとなった業種：
- エンジニアリング、建設／不動産
- 海上／海運

2018年には自然災害により11,000人を超える人々が死亡、または行方不明となっています。その中でも最も死者／行方不明者が多かったのは9月に起きたインドネシアのスラウェシ島の地震津波災害で、3,500人以上もの人々が死亡、または行方不明となっています。また、Swiss Re社による暫定的な推定によれば、**自然災害（例：暴風雨、洪水、地震）**による2018年の経済的な損失は約1,460億ドルに上ります[1]。

また、同社の**Sigma**調査記録に基づいた推定によれば、自然災害と人為的災害による2018年の保険支払額だけをみても790億ドルに上るとしており、支払額が史上4番目に大きい年となっています。これは過去10年の年平均（710億ドル）を上回りますが、それでもカテゴリー4を超える3つのハリケーンHarvey、Irma、Maria（HIM）に見舞われ、保険支払額としては記録的な年となった2017年（1,500億ドル）と比較すると半減しています。

*「2017年のハリケーン災害に規模的に匹敵する単一の大規模自然災害は2018年にはありませんでしたが、複数の中小規模事案の累積により保険金支払額は多額になっています」*と話すのはCosmin Tanasescu（Head of Catastrophe Risk Research & Development, AGCS）です。*「北大西洋でのハリケーン被害を見た場合、2018年は『2017年の弟の年』と考えることができます」*。

2018年の大口損害のうち700億ドルは自然災害が占めるものと想定され、北米のハリケーン・マイケルとフローレンス、アジアの台風ジェビ（台風21号）とマンクット、カリフォルニアの山火事、インドの洪水、日本、インドネシア、パプアニューギニアの地震などが含まれます。2018年にはHIMの損害に匹敵する災害は発生していないとはいえ、大きな災害は起きています。例えば、カリフォルニア州でカー・ファイアとタブス・ファイア（山火事）が大きな被害を出した2017年に続き、2018年は同州のみで山火事による保険金支払いが100億ドルを超える2度目の年となっています。さらに、日本損害保険協会（GIAJ）によれば台風ジェビ（台風21号）は支払額としては過去最大の台風となっています。この台風は2018年9月に西日本に上陸し、広範囲にわたって氾濫と暴風による被害をもたらし、保険金支払額は5,851億円（52億ドル）に上ると同協会では推定しています。その後再保険会社Munich Reでは、保険支払額は90億ドル程度になると推定しています[2]。

*「過去数10年間、自然災害による損害が増大してきた大きな要因としては、リスクと財物価格の高まり、そして危険度の高い地域への集中をあげることができます」*と話すのはCarina Pfeuffer（Cat Risk Analyst, AGCS）です。

自然災害により高まる気候変動リスクへの懸念

アリアンツ・リスクバロメーターの回答者の多くは、最近の自然災害や異常気象は、経済的損失と混乱が今後さらに増大する前兆であるかもしれない考えており、そのことから**気候変動／異常気象の増加**がグローバルリスクランキングで過去最高位の8位（13%）にまで上昇しています（*20ページ参照*）。

気候変動は世界のどの地域にも見られます。海氷や極地氷冠の融解による海面水位の上昇、永久凍土層の融解をはじめ、一部地域では干ばつや熱波、逆に他の地域では豪雨が起きている状況などは、気候の温暖化の影響によるものであると一般的に理解されており、今後はこれらの影響がさらに激しさを増していくものと一般的に予想されています。

人間は化石燃料の使用、雨林の伐採、そして畜産業などを通じて、自然に存在する温室効果ガスに加え大量の温室効果ガスを大気中に排出しており、これが温室効果、ひいては地球温暖化を促進しています。

*「自然災害による経済的な損失は全世界で増大傾向にあります。自然災害リスクを有効なかたちでマネージするためには、契約者も保険会社も、変化し続ける世界中のリスクに対して先手を取って対応していく必要があります」*とTanasescuはいいます。

異常気象は、その激しさと頻度の両面で変化していくものと考えられています。熱帯性暴風雨では風速が強まり、米国では熱波や干ばつが激しさを増すと予想されています。例えば、2050年には米国西部の山火事発生期間が現在よりも3週間長くなり、そのことから今後は火事被害面積も増大するものと予想されます。大西洋と太平洋北東岸のハリケーンに関しては、雨量と雨の激しさが増すものと予想されています。ヨーロッパでは鉄砲水や多雨期の洪水が今よりも高頻度で発生します。アジアでは降水日が全体として少なくなる一方で雨量全体は増えるものと予想され、洪水などが増える一方で、雨水の浸透による地下水の補充が不足するようになると予想されています。

*「気候変動の影響は、多様で地域ごとにそれぞれ異なり、影響の度合いは高まっています。気候変動による自然災害への影響の評価は、活発な研究が行われている分野であり、危険の種類と地域別に詳細に区別して評価を行うことが求められています」*とTanasescuは話します。

洪水 vs 暴風

2018年と2017年にそれぞれ発生したハリケーン・フローレンスとハーヴィーでは、激しい暴風雨においてリスクが多面的に発生するということが分かりました。いずれのハリケーンの場合も、暴風による損害よりも洪水被害への懸念が高く、このことはハリケーンの被害を本当の意味で効果的に評価し、軽減するためには、自然災害リスクをより包括的なかたちでマネージする必要性があることを改めて強調するものでした。

異常気象のモデリングと予報を今後さらに改善していくことが重要となってくるとTanasescuはいいます。ハリケーン・フローレンスの場合、当初予報では大型ハリケーンとして上陸するとされていましたが、2018年9月にノースカロライナ州ライツビルビーチに上陸する直前にカテゴリー1に格下げされています。地崩れや鉄砲水の原因となる総雨量は予想が難しかった一方で、ハリケーンの進路予想は比較的正確に行うことができました。

企業が自分を守るためにできること

AGCSなどの保険会社では、企業がリスクにさらされる度合いを低減し、自然災害による影響を軽減することを目的に、暴風雨を監視し、自然災害活動を評価するための高度な災害マネジメントツールを活用しています。AGCSの**顧客リスクプロファイル**サービスでは、詳細なハザード情報と高度なモデリング情報を活用して、各企業の所在地ごとに最大の脅威を特定しています。それにより企業は自らの自然災害リスクをよりよく理解することができ、リスクマネジメント戦略を確認し、リスク選好に応じて保険内容を最適化するなど、適切な軽減対策を把握することができるようになるとTanasescuはいいます。

*「災害への備えの中で重要な要素として、サプライチェーンの分析と、多様な要素が多面的に盛り込まれた緊急時のシナリオプランニングがあります」*とTanasescuは話します。*「AGCSがサプライチェーンリスクマネジメント能力を絶えず高めるために各種のアプローチや手法の評価を行っているのはこのためです。企業は将来の進出先の計画を立てる場合、当該進出先に的を絞った自然災害リスクプロファイルを検討の材料とし、さらには気候変動による直接、間接の影響から生じる将来的なリスクレベルを評価するなど、先を見越して考える必要があります」。*

↘暴風への備えに関するチェックリストの詳細はこちら

↘洪水によって生じ得る損害を最小限にとどめるために、洪水発生前、発生時、発生後にとるべき行動のチェックリストはこちら

↘ 地震への備えに関するチェックリストの詳細はこちら

1 Swiss Re社：2018年暫定Sigma推定（Preliminary sigma estimates for 2018）2018年12月18日

2 Munich Re 社：数字で見る2018 年の自然災害（The natural disasters of 2018 in figures）2019 年 1 月 8 日

ビジネスリスク：4〜10位

法規制変化

27% 2018: 5 (21%)

Ludovic Subran（Chief Economist of Euler Hermes and Deputy Chief Economist of Allianz）によれば、2018年は世界貿易にとってターニングポイントの年となりました。米国の関税は3.5%から80年代中期と同水準の5.2%に引き上げられ、洗練された保護主義（関税によってではなく規制による方法など）を優先してきた歴史に決別を遂げました。とはいえ2019年の多国籍企業にとって、年末の中国との休戦は米中対立の高まりを単に先送りしたものに過ぎません。多国籍企業が活力の回復に苦しむ中、ゲームのルールは、その株主、所在地、そしてターゲットとする市場によって異なってきます。

一部に企業買収関連法の強化に乗り出した国があり（米国、フランス、ドイツ）、その一方で今後さらなる制裁の対象となることを懸念する国もあります（ロシア、イラン、キューバ）。サプライチェーンはリスクにさらされており、新たに登場する貿易体制の負の影響を回避すべく、貿易転換の検討を進める企業もあります。一方、例えばEUでは加盟国が新たな自由貿易協定を結び（EUがカナダ、日本と）、中核産業の強化を図ろうとしています。2019年は、緊迫する選挙戦、ユーロ域の成長見通しが低いこと、そして**Brexit疲れ**などから、ヨーロッパではリスクが高まります。Brexitは、投資家や企業が嫌気するような政治的な顛末や規制当局の動きがあれば、現在はソフトランディングになると予想される状況も、ハードランディングとなってしまう可能性もあります。

市場動向

23% 2018: 4 (22%)

2018年はボラティリティ、ダイバージェンス、そして不測の出来事の発生が記録的な水準に達し、2019年もこの傾向が続くものとLudovic Subran（Chief Economist of Euler Hermes and Deputy Chief Economist of Allianz）は考えています。昨年、米国の成長が堅調だったことから、特に新興市場は厳しい金融条件に見舞われました。原油価格も1バレル57〜87ドルの間で推移し、秋以降の状況は原油輸入業者にとっては不意打ちとなりました。

米国が堅調に成長する中でヨーロッパやアジアが減速し、米国と他の諸国との分化は明確に現れていました。金融市場でも、不測のデータ漏洩や、ゾンビ企業（利益に比して多額の債務を抱える会社）に関する好ましくない報道などにより株価の修正が起こるなど、厳しい状況が続きました。さらに、多国籍企業、特に輸出企業は、貿易戦争の中ではマイナスのイメージで見られました。例えば、自動車関連企業は、モビリティーの大変革、貿易戦争、規制関連の打撃などに見舞われ、最悪の状況となっています。2019年は年間を通して、不確実性に関わるコストが広がり、さらには政治的背景の急変や、場合によっては収用や没収の復活なども前面に出てくる可能性があります。影響を受けやすい業種（エネルギー、機械・機器、小売）では現在も市場の統合が進んでいます。

火災、爆発

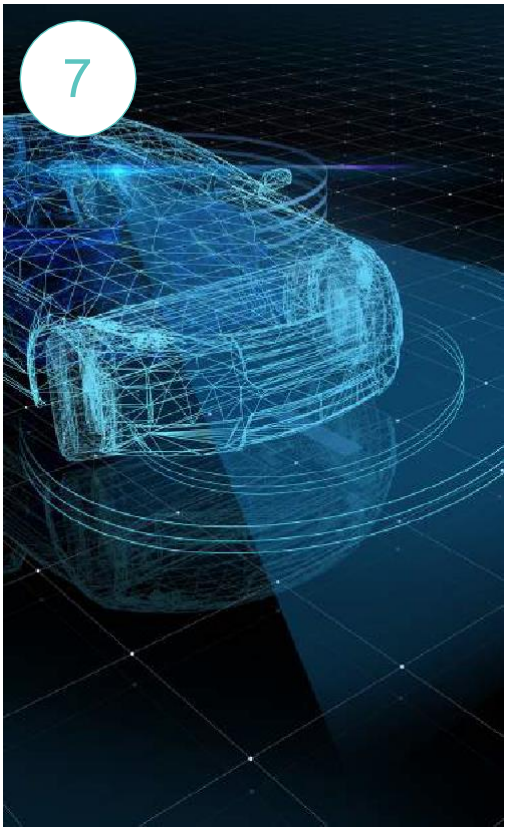
19% (=) 2018: 6 (20%)

AGCSが行った保険業界の損害に関する調査によれば、保険会社と企業の損害額が最も大きいのは火災／爆発事故となっています。火災／爆発事故は、2018年までの5年間について分析した47万件以上の保険業界の企業クレームの24%を占め、それに続く航空衝突／墜落事故の割合は14%となっています[1]。

建物や工場の火災、電気火災、ガス爆発（山火事を除く）などの火災／爆発事故の件数は9,500件に及び、保険金支払額は140億ユーロ（159億ドル）を超え、過去5年間について分析した20件の自然災害以外の大規模災害の半分以上（11件）がこのような火災／爆発によるものです。製造業などの効率化が進むにつれて、リスクにさらされる面積当たりの価額が飛躍的に高まってきており、損害請求や支払いが10年前と比較して大幅に高額になってきています。現在、火災／爆発事故の支払額の平均でさえ147万ユーロで、150万ユーロに迫る勢いです。

新技術

19% (=) 2018: 7 (15%)



新技術は、これまでになかったリスクマネジメントの手法を実現するなど、企業にとっては大きなチャンスをもたらしますが、その一方で、新技術は時として不測の事態を引き起こすリスクもはらんでいます。違法なドローンの飛行により英国のガトウィック空港で1,000便あまりが欠航となった2018年12月の事案などがその一例です。

2025年までに「モノのインターネット（IoT）」を構成するネットワーク接続装置は1千億個を超え、各種センサーが家庭や工場、さらにはサプライチェーンでデータの収集を行うようになっていると予想されています。*「これはつまり、さまざまな予測指標や、より柔軟でカスタマイズされたタイムリーなソリューションを活用することにより、今よりも正確なリスク評価ができるようになるということです」*とMichael Bruch（Global Head of Liability Risk Consulting/ESG, AGCS）は話します。同時に、端末のネットワーク化は、サイバーセキュリティー、データ保護、事業の継続性や賠償責任などに関する課題を突き付けるものであり、重大なインフラ破綻の可能性を高めるものでもあります。

Bruchは続けます。*「新技術の透明性と信頼性の面では、より高度な透明性を実現することが可能となります。保険産業は、技術革新を進める新規のパートナーとともに、リスクベースのサービスの開発を主導することができます。ネットワーク化がますます進む世界では、リスクをより短時間のうちに把握、管理し、損害を未然に防ぐことを目指すべきです」。*

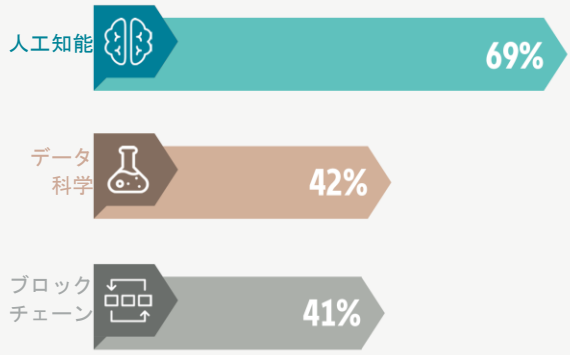
AGCSではすでに複数のインシュアテックの会社と提携しており、次世代の訴訟リスクを特定するために機械学習を活用するなどの取り組みを行っています。

1 Allianz Global Corporate & Specialty：グローバル・クレーム・レビュー、企業保険損害の上位の要因

新技術

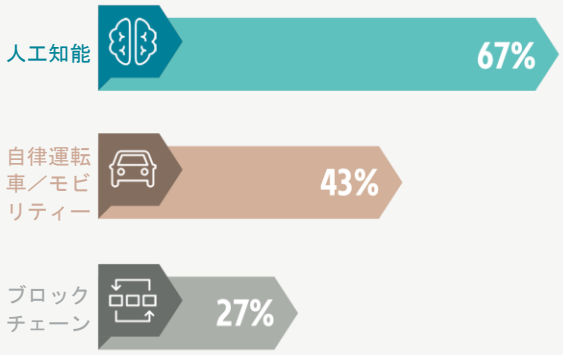
デジタル生態系とプラットフォームが、被害を未然に防止するための各種リスク軽減サービスの基盤となります。同時に、データの利用、正確さ、セキュリティーに関する懸念も高まってきています。

最も有用、または価値のある新技術は？

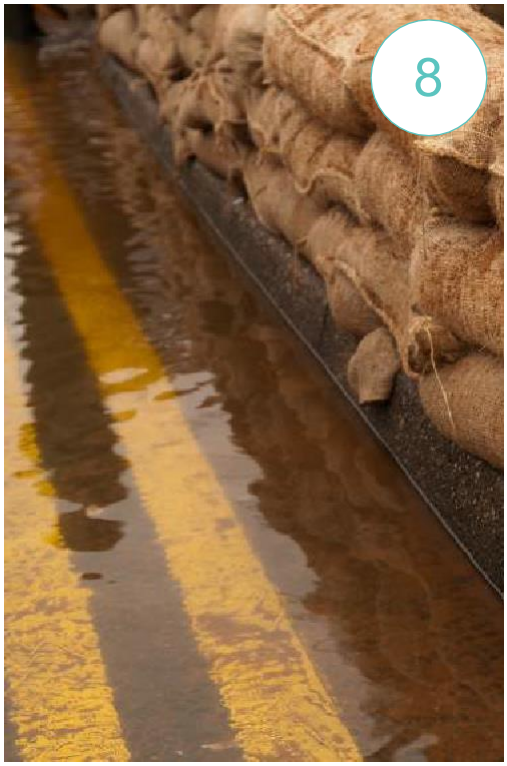


出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、回答をした全参加者（505人）の回答のパーセンテージを表したもの。
また、リスクは最大で3つまで選択可能であることから、数字を合算しても100%とはならない。

潜在リスクが最も大きい新技術は？



出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、回答をした全参加者（505人）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%とはならない。



8

気候変動／異常気象の増加

13% ▲2018: 10 (10%)

2017年と2018年は、ハリケーン、熱帯性サイクロン、および山火事の記録的な年となり、2017年の全世界の自然災害による保険金支払額は過去最高の1,500億ドルとなりました。米国のUS National Climate Assessmentによると、気候変動について対策を講じない場合、暴風雨、洪水、干ばつ、熱波や山火事の激しさが増し、今世紀末にはこれらによる年間の損害額が千億ドル単位になると警告しています。気候変動によるコストはすでに目に見えて高まっています。分析からは、天候に関連した洪水被害の件数は1980年の3〜4倍に増えていることが分かります[2]。

何も対策を講じない場合、気候変動は経済、政治、社会に大きな影響を与えることになり、食料と水の安全保証、健康、人の移動や対立などにも影響が及ぶことが考えられます。間接的な影響としては文化や行動様式の変化なども考えられます（例えば、プラスチックに関する消費者意識や、化石燃料に対する投資家意識の急速な変化など）。気候変動はまた、規制と賠償責任の面でも大きな影響があります。排ガス規制や削減目標は、すでに航空や海運などの産業のあり方を方向付ける要素となっており、気候変動に関する報告義務や情報開示要件が強化されるにつれて、これらの企業の取締役や役員のリスクも高まることになります。

2 Munich Re：気象関連災害の傾向 — 保険会社と社会への影響（Trends in weather-related disasters - consequences for insurers and society）2016年3月

レピュテーション・ブランド価値喪失

13% 2018: 8 (13%)

企業にとって、レピュテーションは最も貴重な資産です。近頃では、製品リコール、サイバーインシデント、業界内の対立、経営陣の行為などにより、航空、自動車製造、銀行など、企業のレピュテーションが損なわれる事案が多発しています。Facebook社では、プライバシースキャンダルや大規模なデータ漏洩などが起こって2018年は混乱の多い年となり、株価は40%近くも下落しています[3]。

ソーシャルメディアの時代にあって、レピュテーションとブランドを守ることは切迫した課題となっています。ソーシャルメディア利用者は全世界で30億人と推定されています。Facebook MessengerとWhatsAppでは一日600億件のメッセージを取り扱っており、レピュテーション関連事案が瞬く間に拡大してもおかしくない状況にありますが、その一方でソーシャルメディアは顧客をモニターしたり、顧客と有意味な関係を築くための一助ともなります。過去10年間に起きた125件のレピュテーション関連事案に関するPentland Analytics社とAon社の調査によれば、ソーシャルメディアの登場以来、レピュテーション関連事案の株価への影響は2倍に高まっています[4]。また、効果的なプランニングと危機管理が必須となっています。レピュテーション関連リスクに対する企業の備え、さらには危機発生直後の管理対応の仕方によっては、企業価値が最大で20%高まる場合もあれば、逆に最大30%損なわれることもあると推定されています。保険では、無形のリスクに対して助言料や危機対応にかかるコストの負担などの支援を提供することができます。

熟練労働者の不足

9% 2018: 15 (6%)

今回、熟練労働者の不足が初めてグローバルリスクのトップ10に入ってきており、このことには人口動態の変化、デジタル経済の中での人材の層の薄さ、さらにはBrexitによる不確実性など、多くの要因が関わっています。

*「熟練労働者ばかりでなく、人的資本全般が、デジタル経済の中で稀少な資源となってきています」*と話すのはLudovic Subran（Chief Economist of Euler Hermes and Deputy Chief Economist of Allianz）です。*「人工知能、データ科学、『フロンティアリスクマネジメント』（サイバーリスクやレピュテーション関連リスクのマネジメント）などの分野は10年前にはほとんど存在しなかったため、これらの分野の能力を持った社員の獲得競争は激化しています。必要なスキルセットを持った人材の層には限界があり、即戦力化が求められる中でOJTは可能ではないことから、魅力的な報酬でさえ人材を引きつけるには十分ではありません」*。

規制の変化もマイナスの影響となることがあります。英国内のある調査では、10社中9社が有能なスタッフを確保することに苦労しており、Brexitによりこの状況はさらに悪化するとしています[5]。新たな人材の雇用は迅速に行わなければならない状況となっています。Scott Steinmetz（Global Head of MidCorp Risk Consulting, AGCS）はこういいます。*「経営陣は若い従業員の技術的な鋭敏さを進んで活用しなければなりません。また、既存の枠組みを打ち壊すテクノロジーや考え方は、利益を生む技術革新に結びつくことがあるので注力する必要があります。労働者の減少を機械学習やオートメーションで埋め合わせることも可能ですが、その場合は大規模投資が必要となります」*。

3 CNBC：2018年のFacebook社株価下落に繋がったスキャンダルやその他の事案（Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018）2018年11月20日

4 Pentland AnalyticsとAon：サイバー時代のレピュテーションリスク ― 株主価値への影響（Reputation Risk In The Cyber Age - The Impact On Shareholder Value）2018年8月

5 Independent紙：調査によれば英国企業の10社中9社が有能なスタッフの確保に苦労。Brexitにより人材不足はさらに悪化（Nine in 10 UK employers struggling to find skilled workers with Brexit set to make shortage worse, survey finds）2018年6月12日

中小企業（SME）のビジネスリスク

グローバルに事業を展開する中小企業にとっては、サイバーの脅威の増大に関する意識の高まりと、サイバーとレピュテーション毀損との関連性、天候被害、および貿易協定の変更が最大の懸念となっています。

アリアンツ・リスクバロメーターへの回答の約半数は中小企業（SME）事業に関与している方々が占めています（回答数2,882件のうち1,437件）。中規模企業（年間収益 2.5億以上、5億ユーロ未満）の最上位リスクは事業中断（BI）となっており、昨年トップのサイバーインシデントに取って代わっています。小規模企業（年間収益2.5億ユーロ未満）の場合は、2018年のトップリスクであった事業中断に代わってサイバーインシデントが最上位に挙がっています。

サイバーに関する意識の高まり

中小企業ではサイバーリスクへの認識が向上してきており、十分な保険を確保する傾向が高まっているとRajiv Iyer（Global Head of MidCorp Package, Small Business and Casualty, AGCS）はいいます。

「*これはクラウドコンピューティングやソーシャルメディアの進歩により小規模企業がさらされるリスクが高まってきていること、ならびにEquifax社の大規模データ漏洩をはじめとするサイバーセキュリティー関連の問題が多発していることから、顧客データの保護をより強化する必要性が出てきたことによります。中小企業では、データ漏洩などの事案が発生した場合の防衛を高めるためには十分なサイバー補償が必要であることを認識しているのです*」。

事業中断リスクも引き続き重要

2019年のランキングでは、小規模企業ではサイバーインシデントが順位を上げ、事業中断がトップから5位に下がっています。その一方、中規模企業で懸念される最上位のリスクは事業中断となっています。中小企業にとって事業中断のロスが発生した場合、金額的には損害は少ないとはいえ、引き続き問題であるとIyerは考えています。重大な事業中断の事故が発生した場合、収入と収益への影響が大きいことから、規模の小さい企業にとっては死活的な問題となることもあります。中小企業を見た場合、自然災害、サイバーリスク、法規制変化を要因とする大きな事業中断リスクが存在するとIyerは考えています（23ページ参照）。

小規模企業（年間収益2.5億ユーロ未満）**のリスク トップ5**

ランキング		割合（%）	2018年ランキング	傾向
1	**サイバーインシデント（例：サイバー犯罪、IT障害／機能停止、データ漏洩、罰金、処罰）**	**32%**	2(30%)	▲
2	法規制変化（例：貿易戦争や関税、経済制裁、保護主義、Brexit、ユーロゾーン解体）	**30%**	5(22%)	▲
3	自然災害（例：暴風、洪水、地震）	**27%**	3(28%)	=
4	市場動向（例：ボラティリティ、競争の激化／新規参入者、M&A、市場停滞、市場変動）	**27%**	4(27%)	=
5	事業中断（サプライチェーンの混乱を含む）	**26%**	1(33%)	▼

出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、その企業規模に関する全回答に対してそのリスクが選択された頻度をパーセンテージとして表したもの。回答数：818。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%とはならない。

サイバーインシデントのリスクは、小規模企業では昨年の2位（回答の30%）からトップ（32%）に上昇しており、中規模企業では2位のリスクとなっています。

「*中小企業の場合、社内体制が大企業ほど整備されていないこともあることから、サイバー攻撃やデータ漏洩に関する懸念が高くなっています*」と話すのは**Volker Muench（Global Practice Leader, Utilities & Services, IT Communication, AGCS）**です。「*データセキュリティー上の問題に見舞われたことのある中小企業は多いものの、契約の取り消しなど、レピュテーション被害を恐れてこれらの問題を報告していない場合もあることが、さまざまな調査から分かっています。中小企業の場合は特に、サイバーインシデントとレピュテーションの喪失の間に明確な関係があることが分かっています*」。

↘ 大企業、および中小企業のすべてのリスクランキングはこちら

↘ 22 業種のすべてのリスクランキングはこちら

天候被害

この他に中小企業にとって大きな懸念となるのは、自然災害と異常気象です。自然災害は、中小両規模の企業共に昨年に引き続き3位のリスクとなっており、気候変動／異常気象の高まりも中小両規模の企業でトップ10に入っています。

「*近年、暴風雨、山火事、ハリケーンが大幅に増えてきていることから、収入の喪失を補償する十分な財物保険と事業中断（BI）保険のニーズが高まってきています*」とIyerは話します。

さらに、米国がパリ協定から脱退し、石炭に重点を置いて環境規制を緩和することを決定したことにより、地球温暖化の影響が悪化する可能性もあるとIyerは考えています。

「*ここ数年の自然災害を表す言葉として『過去に例のない』という言葉が使われており、これらの活動が周期的なものであったとしても、現在のところは現実の問題であり、弱まる兆しは見られません*」とIyerは話します。

貿易への影響

中小両規模の企業で重要性が高まってきている懸念としては法規制変化があり、これは小規模企業では昨年の5位から2位に、中規模企業では6位から4位に順位を上げています。多くの国でのポピュリズムの再燃、貿易協定の変更、事実上の貿易戦争の勃発などが、グローバルに事業を展開する中小企業に影響を与えています。

*「関税の拡大や保護主義の強化などによる物品コストの変動は、アリアンツの顧客や企業にとって引き続き変動性の高い要素となっており、これらがひいては収入や販売製品のコストの変動を招くことになります」*とIyerは話します。

中小企業の展望

世界経済が減速する中にあって、その余波として2019年の中小企業全般の生産が減速することも考えられます。関税の引き上げが、純利益ばかりでなく、設備の保守や維持に使われる営業キャッシュフローに波及的に影響をもたらすことも考えられます。多角的なポートフォリオを持つ中小企業ではこのような減速を乗り切ることも可能でしょう。また、サイバーリスクは中小企業にとって現在も大きな脅威であり、データセキュリティー関連の政府規制が変化する中にあって、中小企業に保険を提供する保険会社は、それぞれの中小企業のリスクニーズに特化してカスタマイズされた保険を提供する必要があります。

中規模企業（年間収益2.5億ユーロ～5億ユーロ）**のリスク トップ5**

ランキング		割合（%）	2018年ランキング	傾向
1	**事業中断（サプライチェーンの混乱を含む）**	**38%**	2(37%)	▲
2	サイバーインシデント（例：サイバー犯罪、IT障害／機能停止、データ漏洩、罰金、処罰）	**32%**	1(39%)	▼
3	自然災害（例：暴風、洪水、地震）	**29%**	3(32%)	=
4	法規制変化（例：貿易戦争や関税、経済制裁、保護主義、Brexit、ユーロゾーン解体）	**24%**	6(18%)	▲
5	市場動向（例：ボラティリティ、競争の激化／新規参入者、M&A、市場停滞、市場変動）	**23%**	5(21%)	=

出典：アリアンツ・グローバル・コーポレート・アンド・スペシャルティ
数字は、その企業規模に関する全回答に対してそのリスクが選択された頻度をパーセンテージとして表したもの。回答数：818。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%とはならない。

中規模企業では、事業中断（BI）リスクが昨年の2位（回答の37%）からトップ（38%）に上昇しています。また、法規制変化も中小企業のリスクとして上昇しています。

お問い合わせ

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。

ブラジル
Camila Corsini
camila.corsini@allianz.com
+55 11 3527 0235

フランス
Florence Claret
florence.claret@allianz.com
+33 158 858863

ドイツ
Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

シンガポール
Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

南アフリカ
Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

英国
Michael Burns
michael.burns@allianz.com
+44 203 451 3549

米国
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

グローバル
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：
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 #ARB2019**

LinkedIn

www.agcs.allianz.com

クレジット

寄稿者：
Alejandra Larumbe Milla, Heidi Polke-Markmann, Patrik Vanheyden

出版物／コンテンツ・スペシャリスト：
Joel Whitehead (joel.whitehead@agcs.allianz.com)

デザイン：
Kapusniak Design

画像：
Adobe Stock/iStockPhoto

編集者：
Greg Dobie (greg.dobie@allianz.com)

Allianz Global Corporate & Specialty SE Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany
商業登録：Munich HRB 208312
2019年1月