



アリアンツ・リスクバロメーター

2020年トップビジネスリスク

102ヶ国・地域の2,700人を超えるリスクマネジメントの専門家が考える2020年の企業にとっての最大の脅威とは





Allianz Global Corporate & Specialtyについて

Allianz Global Corporate & Specialty (AGCS) は、グローバルに展開する企業向け損害保険会社であり、Allianz Groupの重要な事業部門の一つです。当社では、12の商品部門が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ています。

当社の顧客は、Fortune Global 500企業から小規模の事業に至るまで、きわめて多様で、その中には世界最大の消費者ブランド、テクノロジー企業、世界規模の航空産業や海運業だけでなく、ワイナリー、衛星事業者、さらにはハリウッドの映画制作会社なども含まれます。ダイナミックで多国籍化するビジネス環境において、AGCSでは大規模かつ複雑なリスクに対する有効な解決策のご提案や事故発生時のプロフェッショナルな対応を通して、お客さまから信頼をいただいております。

AGCSは従業員4,400名以上が勤務、世界33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200を超える国や地域でサービスを提供しています。アリアンツグループの最大の損害保険会社のひとつとして堅固かつ安定した財務格付けに支えられており、AGCSの2018年のグロス保険料は82億ユーロに上ります。

www.agcs.allianz.com/about-us/about-agcs.html

分析方法

第9回となる今回のアリアンツ・リスクバロメーターは、102ヶ国・地域の2,718人という過去最多の回答者の知見を取りまとめたレポートです。この年次企業リスク調査は、アリアンツのお客さま（グローバルに事業展開する企業）、ブローカー、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2019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。

回答は大企業（年間収益5億ユーロ超）に関するものが大半で（1,348件、50%）、中規模企業（年間収益 2.5億～5億ユーロ）については521件（19%）、小規模企業（2.5億ユーロ未満）については849件（31%）の回答が寄せられています。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としました。

[▼ 地域、国、業種ごとのすべてのリスクデータはこちら](#)



回答者数：2,718



国数：102



業種：22

もくじ

- 03 分析方法
- 04 グローバルビジネスリスクトップ10
- 06 世界各国のビジネスリスク
- 08 エクゼクティブサマリー
- 11 1位 サイバーインシデント
- 14 2位 事業中断
- 17 3位 法規制変化
- 18 4位-6位のビジネスリスク
- 19 重要テーマ：7位 気候変動
- 22 8位-10位のビジネスリスク
- 24 お問い合わせ



▼[リスクバロメーター2020年の全ランキングはこちら](#)



2019: 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、罰則)

2019: 37% (1)

事業中断

(サプライチェーンの混乱を含む)

凡例

- ▲ 2019年よりもリスクが高い
- ▼ 2019年よりもリスクが低い
- 2019年から変化なし
- (1) 2019年リスクランキング

出典：

Allianz Global Corporate & Specialty
数字は、2,718人の回答者から寄せられた全調査回答数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。

また、回答者は業種ごとにリスクを最大で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。

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。

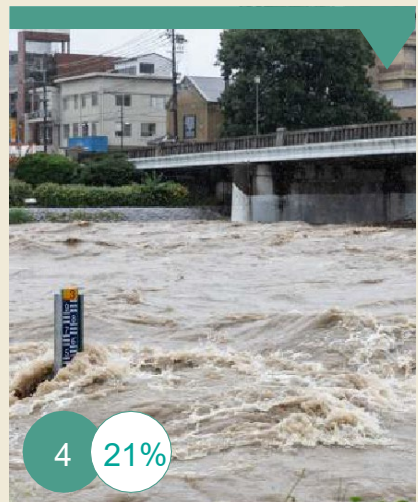
1 自然災害は、回答数では市場動向を上回る。



2019: 27% (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)

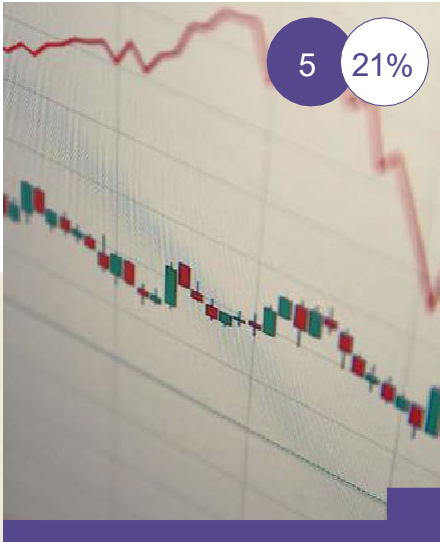


2019: 28% (3)

自然災害¹

(例：暴風雨、洪水、地震)

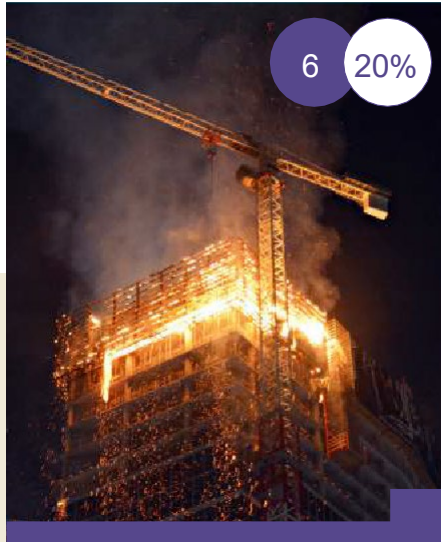
グローバル ビジネスリスクトップ10



2019: 23% (5)

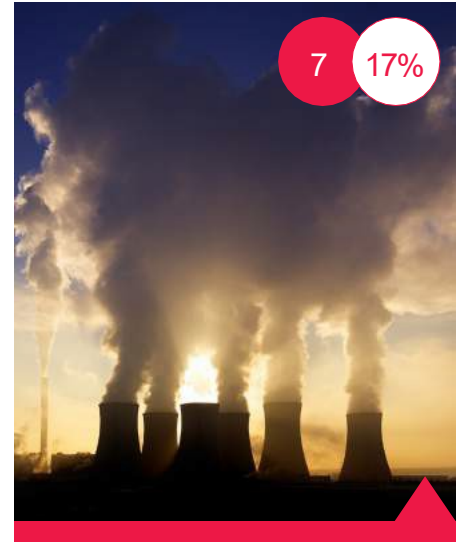
市場動向

(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)



2019: 19% (6)

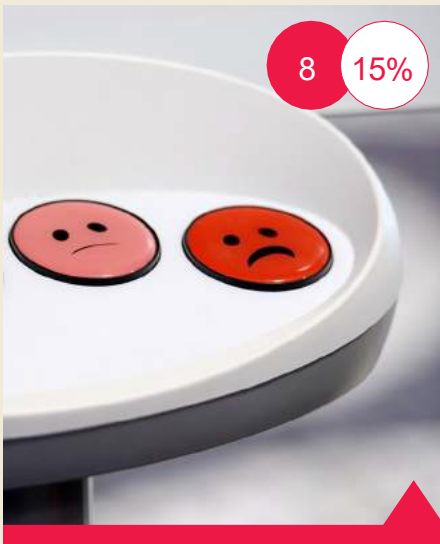
火災/爆発



2019: 13% (8)

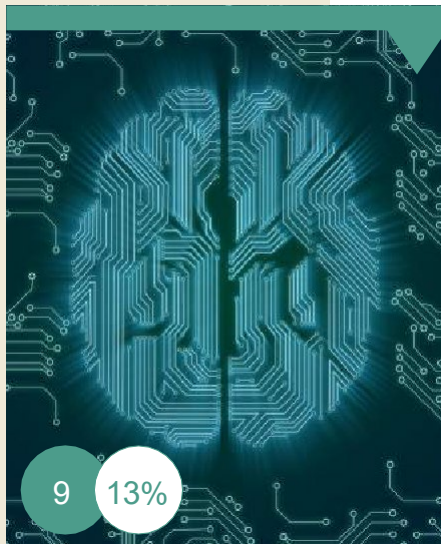
気候変動

／天候の不安定化



2019: 13% (9)

レピュテーション・ブランド 価値の喪失



2019: 19% (7)

新技術

(例: 人工知能、自律運転車、3D プリンティング、IoT、ナノテクノロジー、ブロックチェーンなどの影響)



NEW

マクロ経済の動向

(例: 金融政策、緊縮財政、商品価格の上昇、デフレ、インフレ)

アリアンツ・リスクバロメーター 2020 : 世界各国のビジネスリスク



オーストラリア

- 1 法規制変化 ■
- 2 サイバーインシデント ▲
- 3 気候変動 ▲

「前例のない数の大規模森林火災がオーストラリアの複数の州で発生しており、大きなニュースとなっています。気候変動の一部起因するとされる気温上昇と極度の乾燥で拍車がかかったこれらの火災は、財物損害を引き起こしているだけでなく、煙によって空気の質が有害なレベルにまで達し、それにより事業中断が引き起こされる可能性もあります。人々の意識の高まりと、マイナス影響を直接体験していることを考えると、オーストラリアで気候変動が今回初めてトップ3に挙がっていることは不思議なことではありません」。

JAMES STACK (CEO, AGCS AUSTRALIA)



ブラジル

- 1 事業中断 ▲
- 2 サイバーインシデント ▼
- 3 火災／爆発 ▲

「今年は事業中断がサイバーインシデントを上回っているという事実は、ブラジル企業が緊急時対応計画と復旧計画の策定に取り組み、リスクも低減する必要が依然としてあることを反映しています。事業中断クレームは他のクレームの引き金となることもあり、損害が飛躍的に増えることも考えられます」。

GLAUCIA SMITHSON (CEO, AGCS SOUTH AMERICA)



カナダ

- 1 事業中断 ■
- 2 サイバーインシデント ■
- 3 法規制変化 ▲

「予想通り、BIとサイバーインシデントは、今年もカナダの企業にとって大きなリスクとなっています。法規制変化は、回答者の3分の1近くがトップリスクとしたことで、第3位と大幅に順位を上げています。貿易戦争、関税、経済制裁、保護主義的な動きが繰り広げられる中、企業は市場が今後不安定化するのではないかと懸念を強めています。今日のリスクとエクスポージャーを理解し、この不確実性のマネジメントに役立つ相応のソリューションを見つけていくためには、アンダーライターが適切な質問を行い、判断ができるようにする必要があります」。

LINDA REGNER DYKEMAN (CHIEF AGENT, AGCS CANADA)



中国

- 1 事業中断 ■
- 2 自然災害 ■
- 3 サイバーインシデント ▲

「中国は早期の完全解決の見通しのつかない米国との貿易戦争に突入しています。中国のリスクマネジャーは、関税に関する発表が予測不可能であり、そのため今後に向けた正確な計画作りが難しくなっていることから、今年も最上位のリスクとして事業中断を挙げています。注目すべき点として、非従来のリスクの重大性に対する認識を企業が高めるなか、サイバーが初めてトップ3に入っています」。

PATRICK ZENG (CEO, AGCS HONG KONG AND GREATER CHINA)



フランス

- 1 サイバーインシデント ■
- 2 事業中断 ■
- 3 火災／爆発 ■

「フランスの企業にとって大きな懸念事項となっているのは、今年もサイバーインシデント、事業中断、そして火災／爆発です。一方で、政治リスク／暴力にも注目が集まり、リスクトップ10に新たに加わっていますが、「黄色いベスト」運動や最近のストライキなどによりフランスの経済や企業に影響が及んでいることを考えれば、これも不思議なことではありません」。

CORINNE CAPIÈRE (CEO, AGCS FRANCE)



ドイツ

- 1 事業中断 ■
- 2 サイバーインシデント ■
- 3 法規制変化 ■

「事業中断の原因はますます多様化しており、火災やサイバーインシデントにとどまらず、一部の国では政情不安による事業中断も発生しています。とりわけ、ドイツの自動車産業など、サプライヤーへの依存度の高い企業では、グローバルな繋がりがや依存関係の影響を受けるようになってきました。だからこそ、今日はすべての企業が、事業中断を防止する最善の対策を見つけるだけでなく、発生した場合の影響を減らす最善の方策も見つける必要があります」。

HANS-JÖRG MAUTHE (CEO, AGCS CENTRAL AND EASTERN EUROPE)

これらの画像は、一部選択した国におけるビジネスリスクトップ3を示したものです。

出典：Allianz Global Corporate & Specialty

👉 国、地域、および業種別の全リスクデータはこちら



- 🇮🇹 イタリア**
- 1 事業中断 ■
 - 2 サイバーインシデント ■
 - 3 レピュテーション・ブランド価値の喪失 ▲

「レピュテーション・ブランド価値の喪失は重大な懸念事項になっており、イタリアのリスクトップ3に初めて挙がりました。とはいえ、イタリア企業が引き続き注目する最大の脅威は、事業中断とサイバーインシデントとなっています」。

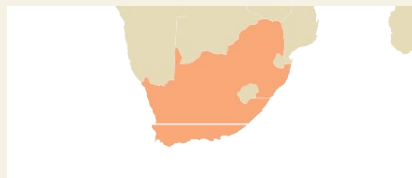
NICOLA MANCINO (CEO, AGCS ITALY)



- 🇸🇬 シンガポール**
- 1 事業中断 ■
 - 2 サイバーインシデント ■
 - 3 法規制変化 ▲

「シンガポールでは、企業が米中間などで貿易紛争が続く不安定な経済環境下での運営を余儀なくされていること、そしてBrexitの最終的な形態を巡る不確実性などから信頼が揺らいでいることを反映して、シンガポール企業にとってのビジネスリスクトップ3に法規制変化が初めて挙がっています。毎年上位に挙がっている事業中断とサイバーインシデントは、現地のリスクマネジャーを現在も悩ませており、昨年発生したサプライチェーンの大規模混乱や重大なデータ漏洩事案を受けて、シンガポール企業にとってのリスクの1位と2位の位置を今年も保っています」。

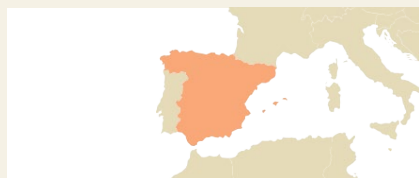
MARK MITCHELL (CEO, AGCS ASIA-PACIFIC)



- 🇿🇦 南アフリカ**
- 1 サイバーインシデント ▲
 - 2 事業中断 ▼
 - 3 法規制変化 ■

「サイバーインシデントが地域のリスクとしては2位に、南アフリカでは最上位に順位を上げる一方で、各企業は法規制変化への懸念も強めており、このリスクが今年も3位に挙がっています。南アフリカの上位リスクは、グローバルなリスクのトップ3と一致しており、アフリカ企業が世界各国の企業と同様の懸念を抱いていることを示しています。アフリカ大陸のリスクとして2019年には5位に挙がっていた事業中断が、今年は最上位に挙がってきていることから、アフリカ全体の企業も事業中断にますます懸念を抱くようになってきていることが分かります。事業中断リスクはまた、タンザニア（1位）、ナイジェリア（3位）、南アフリカ（2位）、カメルーン（2位）の各国でリスクのトップ3に挙がっています」。

THUSANG MAHLANGU (CEO, AGCS AFRICA)



- 🇪🇸 スペイン**
- 1 サイバーインシデント ▲
 - 2 事業中断 ▼
 - 3 自然災害 ■

「世界各国で発生する大規模サイバー攻撃の件数、そしてスペイン企業に影響を与えているランサムウェア事件が増加してきていることにより、スペインではサイバーインシデントに対する意識が高まり、調査開始以来初めてリスクの最上位に挙がっています。2019年はまた、スペインが厳しい熱波や洪水被害に見回れた年でもあり、自然災害に対するスペイン企業の懸念がさらに高まり、今年もリスクのトップ3に挙がっています」。

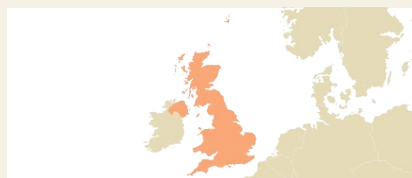
JUAN MANUEL NEGRO (CEO, AGCS SPAIN)



- 🇺🇸 米国**
- 1 サイバーインシデント ▲
 - 2 事業中断 ▼
 - 3 自然災害 ■

「米国ではサイバーインシデントがリスクのトップに挙げられており、これは特段驚くことではありません。ここ何年もの間、接続性の向上と攻撃の高度化によりインシデントの頻度と重大度が高まっています。サイバー保険契約の大半が米国で契約されていることを考えると、このリスクは保険業界全体の方向性を今後左右するとともに、サイレントサイバーリスクに関するポートフォリオの再検証を促すこととなります」。

BILL SCALDAFERRI (CEO, AGCS NORTH AMERICA)



- 🇬🇧 英国**
- 1 サイバーインシデント ■
 - 2 法規制変化 ▼
 - 3 事業中断 ■

「サイバーインシデントは増加しており、英国での調査ではこの状況を正確に反映して最上位のリスクとなっています。Brexitなどの法改正に関する不確実性は現在も続いており、多くの企業経営陣のトップアジェンダとなっていますが、AGCSではお客さまが直面するこれ以外の多くのビジネスリスクを軽減することを目指し、新たな革新的な方策についての検討を進めています」。

TRACEY HUNT (DEPUTY CEO, AGCS UK)

エクゼクティブ サマリー

リスクマネジメント専門家が挙げるトップ10リスク



サイバーインシデントは、100を超える国・地域で、これまでで最大となる2,700人超のリスクマネジメント専門家の回答の39%を占め、世界各国企業の最大の脅威としてアリアンツ・リスクバロメーターでランキングされました。7年前、サイバーリスクという回答はわずか6%にとどまり、順位も15位でした。企業がデータやITシステムへの依存度を高め、世間を騒がす事案が複数発生していることを背景に、サイバーリスクに対する認識は近年急速に高まっています。

企業は、より大規模でコスト負担の大きいデータ漏洩、ランサムウェアやビジネスメール詐欺（なりすまし）事案の増加、さらには事案発生後の訴訟の可能性の高まりなど、ますます多くのサイバー関連の課題に直面するようになっています。また、国家間の政治的闘争がサイバースペースでの争いに発展してリスクの複雑さが増し、その一方で企業合併の分野では、M&Aが成功裏に執り行われた場合でもシステム上の問題が後日発生する可能性があります。 [▶11ページ](#)

アリアンツ・リスクバロメーターの回答者によると、サイバーインシデントの主な原因はデータ漏洩となっています。そして、企業がこれまで以上に大量の個人データを集めて利用するようになっていくことから、データ漏洩事案はますます大規模化し、コスト負担も増大してきています。大規模漏洩（100万件以上のデータが関わるもの）への対処にかかる平均コストは現在、前年比8%増の4,200万ドル¹ となっており、5,000万件を超える漏洩の場合の平均コストは、11%増の3億8,800万ドルとなっています。また、データ保護法とプライバシー規制、および事案発生後の罰則の範囲や地理的な管轄範囲も拡大しています。英国では、規制当局が1億ポンド（1億3,000万ドル）の罰金を課した事案が2019年7月だけで2件も発生しています。2018年にヨーロッパで施行された一般データ保護規則（GDPR = General Data Protection Regulation）により、2020年にはさらなる罰金の波が押し寄せる可能性が高いと考えられます。同規則施行後の最初の9か月間で20万件を超える事案がすでに報告されています。

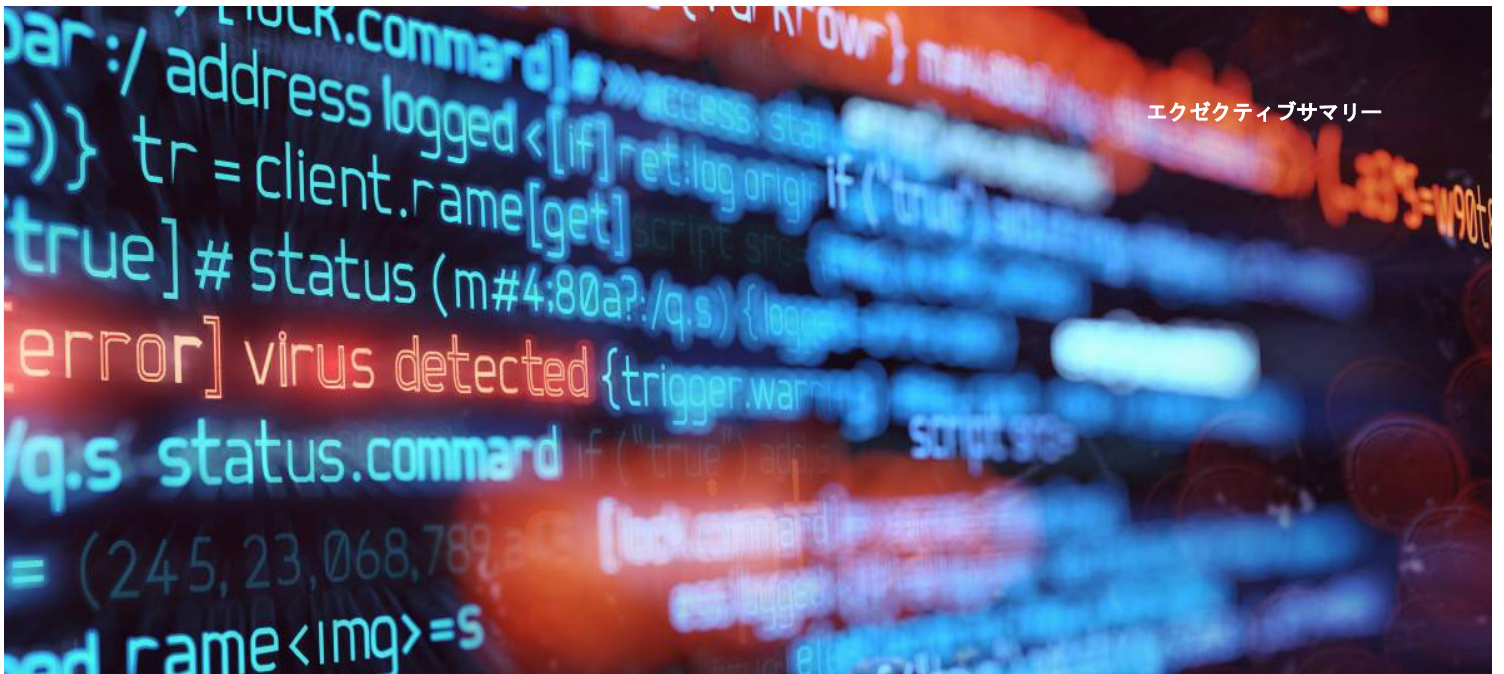
一方、訴訟によるコストへの影響も出始めており、消費者や投資家による集団訴訟の引き金となった大規模侵害事案がいくつか発生しています。たとえば、2017年に起きたEquifax社の大規模漏洩では、2019年7月に7億ドルで和解に至っています。

ランサムウェア攻撃はさらに深刻化してきており、多くの大企業が高度化した攻撃の標的となって多額の身代金を要求されるようになっています。身代金は5年前であれば数万ドル程度が一般的でしたが、今では数百万ドル単位にまで上がっています。工業や製造企業が標的とされるケースも増えてきていますが、損害額では、ITシステムやデータを生命線とする法律事務所、コンサルタント業、建築業が上位を占めています。なりすまし攻撃の頻度も高まっています。企業の従業員を騙してログイン認証情報を入力したり、不正な取引を行わせるなどのソーシャル・エンジニアリングやフィッシング・メールを使ったこのような事件では、FBIによると2016年から現在に至るまで、全世界で260億ドルもの損害が発生しています。 [▶12ページ](#)

サイバーリスクはまた、いくつかの大規模データ漏洩事件を受けて、M&Aの分野でも重要なテーマとなっています。ホテルチェーンのMarriott社で2018年に発生した漏洩事件は、2016年に同社が買収したStarwoodホテルグループでの2014年の侵入事件に端を発したものでした。高度な保護対策を導入している企業であっても、以前から脆弱性のある企業を買収すればリスクにさらされることになり、買収をした企業が合併以前の事件について賠償責任を問われることも考えられます。M&Aを行う企業は、潜在的なサイバー脆弱性やリスクに関する検証を、今よりも高い優先事項として位置づける必要があります。 [▶13ページ](#)

国家のサイバー攻撃への関与も企業のリスクを増大させることとなります。それは企業の知的財産目当て、または混乱や物理的損害を引き起こすことを目的とする集団の標的となる可能性があるからです。中東での緊張の高まりを背景に、国際海運業者がペルシャ湾で攻撃を受けています。石油やガス施設にも影響が出ています。

¹ IBM Security、Ponemon：「データ漏洩のコスト2019年レポート」（Cost Of A Data Breach Report 2019）



サイバーリスクを軽減するうえで最も効果的な対策は準備と教育であり、これにより攻撃の影響を大幅に減らすことができます。事案の多くはヒューマンエラーが原因であり、特にフィッシングやなりすましといった一般的な攻撃形態の場合、教育によって軽減することが可能です。教育はランサムウェア攻撃の軽減にも役立ちますが、安全なバックアップをとっておくことで損害を抑えることができます。事業回復力と継続性を確保するための計画も重要ですが、事案対応計画をテストし、定期的に再検証する必要もあります。

7年にわたりトップにランキングされてきた**事業中断 (BI)** ですが、今回の**アリアンツ・リスクバロメーター**では2位に順位を下げています(回答の37%)。とはいえ、火災や自然災害といった従来の原因(火災による事業中断クレームの平均保険支払額は580万ユーロ[670万ドル]で、火災に付随する財物損害のそれより45%上回っている²⁾)に加え、デジタル・サプライチェーンやデジタル・プラットフォームにおける技術的な問題、さらには社会不安など、新たな原因による事業中断の大規模化と複雑化の傾向には衰えは見られません。

[▶14ページ](#)

顧客やサプライヤーで発生した事案により企業が損害を被るサプライチェーンの中断(CBI)は、10年前はおろか、5年前よりもはるかに大規模化し、範囲も広がってきており、複数の企業や国家に影響を与えるケースも出ています。自動車や医薬品といった産業では、高度に効率化されたサプライチェーンを世界規模で展開していますが、これにより大規模なBIやCBI事案に対する脆弱性も高まる結果となっています。さらに、他の産業もこのようなサプライチェーンを模したものを構築し始めています。

企業はまた、暴動や社会不安、テロ攻撃などの政治的リスクによる直接的・間接的な影響にもますますさらされるようになっており、大きな混乱を招きかねない状況となっています。過去

1年の間に、香港、チリ、フランス、ボリビア、コロンビアなどで社会不安が拡大し、多くの企業で財物損害、事業中断、そして収益の損失などの損害が出ています。2019年10月に始まったチリの抗議デモでは、何百軒ものスーパーマーケットで略奪や放火が起っています。損害額は現在のところ約30億ドルに上っており、依然多くの事業者が何ヶ月にもわたって事業が再開できない状況にあります。香港では、長引く社会不安により観光客が前年比で40%減少しています。この他にもこのような事案による影響として、安全上の理由から従業員が職場に出勤することができず、多くの業種で生産停止に追い込まれてしまう可能性があります。保険業界では、こうした混乱の影響を軽減することを目的とした政治的暴力や暴動のリスクを担保する専用保険への加入が増えています。

[▶15ページ](#)

また今後は、異常気象により水道や電力といったリソースが使えなくなるなどの混乱に企業が見舞われるリスクも高まっていくものと考えられます。2018年にはライン川の一部で水位が下がって航行が不能となったことで、メーカー数社が生産の中断に追い込まれています。事業中断が軽減策によって引き起こされることもあります。たとえば、2019年のカリフォルニア州の干ばつの際には、森林火災のリスクを軽減するために電力会社が計画停電を実施しています。また、一部の業種では、最新の食品サプライチェーンでの主要原料の供給の継続性について懸念が高まっています。食品/飲料セクターでは、2018年夏の需要ピーク時に二酸化炭素ガスが不足して混乱が生じました。近年の干ばつ、熱波、洪水などでは、野菜、小麦、牛乳の収量に影響が出て、これにより食品メーカーや小売業者への供給に影響が出ました。大企業は、増加する事業中断シナリオから収益を守るために、よりカスタマイズされた保険ソリューションをますます求めるようになっていきます。 [▶16ページ](#)

2 Allianz Global Corporate & Specialty、2013年7月から2018年7月にかけて、財物損害と事業中断の両方の要素が関わる1,175件の企業保険クレームの分析に基づくと。

法規制変化（第3位、27%）について、企業は昨年よりも懸念を強めており、初めてトップ3に登場しています。2019年だけでも約1,300の新たな貿易障壁が設けられるなか、回答者は関税、制裁、Brexit、保護主義を重要な懸念材料として挙げています。2020年にはヨーロッパで「情勢を一変させる」EUの持続可能性関連規制が導入されるなど、企業はいろいろな大きい課題に直面することになります。企業や投資家は、ビジネスパートナーを選ぶ際に持続可能性の認定などをますます検討するようになっています。 [▶17ページ](#)

2019年の大見出しとなった災害としては、アジアの壊滅的な台風やオーストラリアの記録的な森林火災などがありました。とはいえ、**自然災害**による経済損失は実際には前年比20%減の約1,300億ドルにまで減少しており、これによりこの脅威が初めて世界のリスクトップ3から漏れる結果となっています（第4位、21%）。一方、**気候変動**（第7位、17%）は、**アリアンツ・リスクパロメーター**史上最高位にまで上昇しています。地球温暖化は世界各国で激しい災害を引き起こし、市民や企業を脅かしています。海水面の上昇、これまで以上に乾燥した干ばつ、激しさを増す暴風雨、大規模な洪水などは、工場などの資産をはじめ、サプライチェーンを結び付ける輸送やエネルギーなどの繋がりを脅かし、企業にとっては物理的な脅威となります。回答者によれば、企業が最も恐れるリスクは物理的損害の増大であり、コストの高まりはすでに顕著になっています。気象関連の洪水被害事案の件数は1980年の3倍から4倍にまで増えています。Climate Transparencyの推定では、G20国だけをとっても異常気象関連による死者数は毎年16,000人に上り、経済的影響は1,420億ドルに達しています³。 [▶18ページ](#)

業務面で気候変動に適切に対処しない場合、批判、レピュテーションの低下、規制や法的措置などを招く場面が増えることになると企業は気付き始めています。気候変動関連の新たな法律が世界各国で毎年約1,500ほど施行されていると推定されますが、企業が圧力を受けるのは政府や規制当局からだけではありません。企業に対する気候変動関連の市民活動は、特にヨーロッパで高まってきており、企業経営陣は投資家やその他のステークホルダーからますます説明を求められるようになっています。

気候変動リスクの開示を怠ったことが訴訟の対象となることが今後さらに増えていきます。現在までに世界の30ヶ国以上で気候変動関連の訴訟がすでに起こされており、その7割以上は米国で起こされたものです。訴訟の多くは、化石燃料の積極的な生産者である「カーボンメジャー」を標的としたものですが、アグリビジネス、製造業、輸送など、炭素排出量の多い他の産業にも拡大していくものと考えられます。

気候変動に対処するには、是正措置と投資が必要ですが、一方で再生可能エネルギー、レアアース採掘、バッテリー生産などの新たなビジネスモデルや市場といったビジネスチャンスをもたらすものもあります。 [▶19ページ](#)

市場動向（第5位、21%）と**火災／爆発**（第6位、20%）のランキングは2019年から変わっていません。 [▶18ページ](#)

そんな中、**レピュテーション・ブランド価値の喪失**も、**アリアンツ・リスクパロメーター**での順位を前年から上げています（第8位、15%）。レピュテーションが関連する企業不祥事の原因となるシナリオは増え続けています。ソーシャルメディアの登場後、レピュテーション事案の株価への影響は2倍に高まっていると考えられています。依然として多くの企業では、レピュテーションの危機から身を守るための対策が不十分です。効果的な計画が必須となってきたおり、専門家による対応があるかないかで事態が違ってくともあります。保険もまた、純営業利益への打撃から会社を守り、ブランド価値回復に向けたコンサル費用などの負担、そして365日24時間体制のレピュテーション危機対応などのソリューションを提供することで、無形のリスクに対して具体的な支援を提供することができます。 [▶22ページ](#)

人工知能（AI）などの**新技術**（第9位、13%）は企業に大きなビジネスチャンスをもたらします。保険業界では、AIの利用により取引のプロセスを改善することができ、すでに多くの利点が見られます。お客さまのニーズをより正確に特定することができ、保険証券の発行やクレーム処理をより迅速に、低コストで行え、事業中断、サイバーセキュリティリスク、マクロ経済危機など、重大な企業リスクの予測をより正確に行うことができます。しかし、新技術にはリスクも伴います。**アリアンツ・リスクパロメーター**の回答者によれば、AIとデジタル・プラットフォームの利用率の増加は、将来的には最もリスクの可能性をはらむイノベーションでもあるのです。AIの場合、透明性や人間の監視が欠如することから、予測不可能な結果が生じ、複雑な責任問題に発展する可能性があります。デジタル・プラットフォームの場合は、技術的な不具合やサイバー事故などによりプラットフォームが利用できなくなり、それに依存する企業がサービスや製品を提供できなくなった場合、複数の企業で数億ドル以上の損害が発生する可能性もあります。 [▶22ページ](#)

マクロ経済の動向は、2020年に新たにトップ10に登場したリスクで（第10位、11%）、その背景には民間部門において世界的な景気後退と債務の蓄積が—特に米国と中国で—起きていることに対する企業の懸念があります。 [▶23ページ](#)

³ Climate Transparency: 「ブラウンからグリーンへ—G20諸国の純ゼロ排出経済への移行2019」(Brown To Green, The G20 Transition Towards A Net-Zero Emissions Economy 2019)



39%▲2019:2位 (37%)

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、罰則)

規模も損害額も拡大を続けるデータ漏洩、ランサムウェア攻撃の増加、そして事案発生後の訴訟の可能性の高まりなど、企業が多く課題に直面するなか、サイバーリスクが初めてアリアンツ・リスクバロメーターの最上位にランキングされました。また、国家間の政治的な問題がサイバー空間での争いに発展すればこのリスクは高まります。さらに企業合併の分野では、M&Aが成功裏に執り行われた場合でも予期せぬ問題が後に発生することがあります。

これまでのランキング (回答の割合とランキング位置)：

- 2018年 2位 (40%)
- 2017年 3位 (30%)
- 2016年 3位 (28%)
- 2015年 5位 (17%)

次の国で最上位リスク：

- 🇦🇹 オーストリア
- 🇧🇪 ベルギー
- 🇫🇷 フランス
- 🇮🇳 インド
- 🇲🇾 マレーシア
- 🇳🇦 南アフリカ
- 🇰🇷 韓国
- 🇪🇸 スペイン
- 🇸🇪 スウェーデン
- 🇸🇰 スイス
- 🇬🇧 英国
- 🇺🇸 米国

次のセクターで最上位リスク：

- 航空
- 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

2020年のアリアンツ・リスクバロメーターでは、サイバーインシデントが最重要のビジネスリスクとしてランキングされました(回答の**39%**)。2013年にはこのリスクが順位としては15位、回答の6%にとどまっていたことを見れば、企業がデータやITシステムへの依存度を高めてきたことを背景にサイバーリスクに対する認識が急速に高まってきていることは明確です。サイバーリスクは進化を続けています。ランサムウェア攻撃が大幅に増えてきていることも手伝って、企業が損害に見舞われる頻度が高まっています。全体として、サイバー攻撃が高度化し、標的も絞り込まれているうえに、攻撃側の身代金要求も百万ドル単位にまで上昇しています。

「サイバーインシデントのコストは全体的に上昇していますが、これは複雑さの高まり、規制の強化、データや基幹システムの喪失で企業が受ける被害によるものです」と話すのはMarek Stanislawski (Deputy Global Head of Cyber, AGCS) です。「データ保護やプライバシー関連の規制範囲と地理的な管轄範囲が拡大し、集団訴訟への対応コストにより、特に大規模データ漏洩に伴うコスト負担は増え続けています。更に漏洩事案が大規模な事業中断を伴う場合損害額も一般的に大きくなります」。(14ページ参照)

最近の傾向

データ漏洩は大規模化、損害額も増大

企業がこれまで以上に大量の個人データを集めて利用するようになってきていることから、データ漏洩事案はますます大規模化し、コスト負担も増大しています。特に、いわゆる大規模データ漏洩(100万件以上のレコードが関わるもの)の頻度が増し、損害額も増大しています。2019年7月、銀行セクターで過去最大規模の漏洩に見舞われたCapital One社では、およそ1億人の顧客に影響が出たことを公表しています。しかし、この漏洩も近年としては決して最大規模のものではありません。

2018年のホテルグループMarriott社と、2017年の信用スコア機関Equifax社でのデータ漏洩は、それぞれ3億人超と1億4000万人超の顧客の個人データが関わっていたと報告されています。両社とも、複数の司法管轄区で多数の訴訟と規制措置への対応を迫られ、英国のデータ保護規制当局は、Marriott社にこの漏洩に関して1億ユーロ(1億3000万ドル)の罰金を科す方針であり、これはEUの新しいプライバシー法施行後の最大の罰金の一つになります。

サイバーインシデントの主な原因は？



1 データやセキュリティの侵害（例：個人情報/機密情報へのアクセスや削除）



2 スパイ行為、ハッカー攻撃、ランサムウェア、サービス妨害



3 従業員による間違いやミス

「機密データの入ったノートパソコンの電車内への置き忘れから、顧客リストの紛失に至るまで、あらゆる行為がデータ漏洩事案に発展する可能性をはらんでいます」と話すのはMarek Stanislawski (Deputy Global Head of Cyber, AGCS) です。「単純なミスから、フィッシングやソーシャル・エンジニアリングの被害者になってしまうケースに至るまで、従業員が原因だったり、従業員が加担する侵害は50~90%に上ると推定されています。十分な教育を受けた、警戒を怠らない従業員を、企業のサイバーセキュリティチームの延長とすることで、企業資産の防護体制をより堅固にする一助とすることができます」。

出典：Allianz Global Corporate & Specialty

数字は、回答をした全参加者（1,071）の回答のパーセンテージを表したものです。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。

なることもあります」とStanislawskiは話します。

特に製品やサービスを提供するうえでデータに依存する組織にとっては、このような攻撃は壊滅的な影響を引き起こす可能性があります。また、身代金要求は全体像の一端に過ぎません。ランサムウェア攻撃で損害が最も大きくなるのは事業中断で、ときとして個人データの窃盗など、真の目的の煙幕としてランサムウェアが利用されるケースもあります。工業や製造企業が標的とされるケースも増えてきていますが、損害額では、ITシステムやデータを生命線とする法律事務所、コンサルタント業、建築業が上位を占めています。

また、Ryukマルウェアなどを利用した事案は、近年のサイバー保険クレーム増加の大きな要因として浮上しています。架空の漫画キャラクターにちなんで名付けられたこのマルウェアは、2018年8月に初めて報告され、世界各国の複数の大企業、病院、地方自治体に対する攻撃に利用されました。

最近の傾向

ビジネスメール詐欺（BEC）攻撃による詐欺損害が数10億ドル規模に

ビジネスメール詐欺（BEC）攻撃、いわゆる「なりすまし」攻撃の頻度も高まっています。米国のFBIによると、BEC事件による全世界での損害額は2016年以降、少なくとも260億ドルに上ります。

これらの攻撃は通常、ソーシャル・エンジニアリングやフィッシング・メールを使って、企業の従業員や上級管理職を騙してログイン認証情報を入手したり、不正な取引を行わせるというものです。

最近の傾向

高まる訴訟の可能性

今日、大規模データ漏洩が規制措置の引き金となるケースが多々ありますが、それに加え、漏洩の影響を受けた消費者、提携企業、投資家から訴訟を起こされることもあります。そうした場合、訴訟費用により大幅にコスト負担が増えることもあります。

米国におけるデータ漏洩訴訟のあり方は現在進行形で変化を続けており、消費者や投資家による集団訴訟の引き金となった大規模漏洩がいくつも発生しています。たとえば、2017年に起きたEquifax社の大規模漏洩では、2019年7月に7億ドルで和解に至っています。米国の司法では「法的地位」（原告に訴訟を起こす権利があるかどうか）の問題が議論されてきましたが、傾向としては原告に有利に推移しているようです。法律や規制の変更によってデータ漏洩に対する補償の円滑化が進む可能性もあります。たとえば、カリフォルニア州の消費者プライバシー法には、米国では初めて消費者が企業を訴えるためのメカニズムが規定されており、データ漏洩に対する法定損害賠償金が定められています。

同月の2019年7月には、British Airways社が50万人の顧客に影響を与えた2018年のデータ漏洩に対して183百万ポンド（240百万ドル）の仮罰金を課されています。

2018年にヨーロッパで施行された一般データ保護規則（GDPR=General Data Protection Regulation）により、2020年にはおそらく罰金処分がさらに増えることとなります。欧州データ保護会議（EDPB）では、GDPR実施後の最初の9ヶ月間に31ヶ国で報告された206,326の案件のうち、各国のデータ保護当局では50%しか解決できていないとする予備報告書¹を公表しています。上記のように、規制当局が未処理案件の処理を進めるにつれて、より多額の罰金がさらに多く記録されるようになっていきます。

Ponemon Instituteによれば、大規模漏洩による平均コスト負担は現在、2018年比で約8%増の4200万ドル²に上ります。データ数が5,000万件を超える漏洩の場合、コストは3億8,800万ドルに上ると推定されます（2018年比11%増）。

最近の傾向

ランサムウェア攻撃による損害が増加

EUの警察機関であるEuropolによると、ランサムウェアはサイバー犯罪のなかでも最大の脅威となっています。

すでに高頻度で発生しているこれらの攻撃は、さらに深刻化しており、多くの大企業が高度化した攻撃の標的となって多額の身代金を要求されるようになってきました。「ランサムウェア攻撃での身代金は5年前であれば数万ドル程度が一般的でしたが、今では数百万ドル単位に

1 欧州データ保護会議：GDPRの実施及び各国監督当局の役割と手段に関する概要第一版（European Data Protection Board：First Overview On The Implementation Of The GDPR And The Roles And Means Of The National Supervisory Authorities）
2 IBM Security, Ponemon：「データ漏洩のコスト2019年レポート」（Cost Of A Data Breach Report 2019）

米国以外でも、多くの国が集団訴訟権の拡大を進めています。たとえばヨーロッパでは、GDPRにより、データやプライバシーを侵害された被害者が法的救済を求めやすくなっています。

さらに、原告の法律事務所や訴訟資金提供者が、ヨーロッパと他地域でのデータ漏洩に対する集団訴訟を起こすことを積極的に検討しています。たとえば、British Airways社での2018年のデータ漏洩について、最近になって英国裁判所が集団訴訟を認めています。また、消費者団体も、GDPRの解釈について異を唱え、争う姿勢をみせています。

最近の傾向 M&Aからサイバー問題が生じる可能性も

いくつかの大規模データ漏洩事件を受けて、合併吸収（M&A）の分野でもサイバーリスクが重要テーマとして浮上しています。たとえば、ホテルチェーンのMarriott社で2018年に発生した漏洩事件は、2016年に同社が買収したStarwoodホテルグループでの2014年の侵入事件に端を発したものでした。

高度な保護対策を導入している企業であっても、サイバーセキュリティーの脆弱な企業や、以前から脆弱性のある企業を買収すればリスクにさらされることとなります。買収をした企業が合併以前の事件で生じた損害の賠償責任を問われることも考えられます。

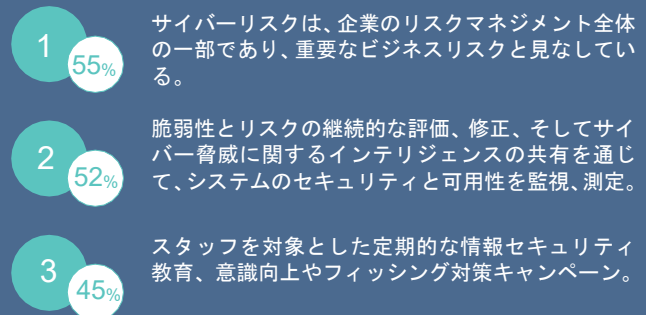
突き詰めれば、M&Aのタイミングでこの分野で相当の注意を払っている企業はそれほど多くはないことから、M&Aを行う企業は潜在的なサイバー脆弱性やリスクに関する検証を、今よりも高い優先事項として位置づける必要があります。それと同時に、多くの企業が新たに取得した会社のシステムの弱点への対処を、M&A完了後、十分迅速に行っていないという状況もあります。

最近の傾向 サイバースペースで展開される政治的ファクター

国家のサイバー攻撃への関与も企業のリスクを増大させています。それは企業が知的財産目当て、または混乱や物理的損害を引き起こすことを目的とする集団の標的となる可能性があるからです。たとえば、中東での緊張の高まりを背景に、国際海運業はペルシャ湾でなりすまし攻撃の標的となっており、石油やガス施設もサイバー攻撃やランサムウェア攻撃を受けています。

さらに、高度な攻撃手法やマルウェアがサイバー犯罪者の手にも徐々に行き渡りようになっていることが考えられ、その一方で国家の関与によりハッカーへの資金提供が増加しています。企業が直接標的にされていない場合でも、国家が支援するサイバー攻撃により付随的な損害が発生することはあり得ます。たとえば、2017年のNotPetyaマルウェア攻撃も主にウクライナを標的としたものでしたが、世界各地に急速に広がっていきました。

サイバーリスクをマネージし、サイバー回復力を高めるための最良のアプローチは？



「サイバー保険への加入を、企業のサイバー回復力を強化する企業計画の仕上げの要素の一つと考える必要があります」と話すのはMarek Stanislawski (Deputy Global Head of Cyber, AGCS) です。「他のあらゆる対策が不十分な状況では、保険が企業の回復を助ける重要な役割を果たしますが、戦略的リスクマネジメントに取って代わるべきものではありません。従業員の意識向上、そしてシステムの更新と継続的な監視に投資を行うことは、間違いなくあらゆる企業のサイバーto-doリストのトップに挙げられるべきです」。

出典：Allianz Global Corporate & Specialty
数字は、回答をした全参加者（1,071）の回答のパーセンテージを表したものです。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。

リスク軽減

サイバーリスクを軽減するうえで最も効果的な対策は準備と教育であり、これによりサイバー事件発生の可能性や発生した場合の影響を大幅に減らすことができます。事案の多くはヒューマンエラーが原因ですが、特にフィッシングやビジネスメール詐欺といった一般的なサイバー攻撃形態の場合は、教育によって軽減することが可能です。

教育はランサムウェア攻撃の軽減にも役立ちますが、安全なバックアップをとっておくことで、このような攻撃で生じる損害を抑えることができます。事業回復力と継続性を確保するための計画もサイバーインシデントの影響を軽減するうえで重要ですが、事案対応計画をテスト、実行し、定期的に再検証する必要もあります。

▶ [サイバーリスクと保険に関する詳細はこちら](#)



37%▼2019:1位 (37%)

2 事業中断

(サプライチェーンの混乱を含む)

火災や自然災害は事業中断による損害の最大の原因であり、事業中断による損害は付随する財物損害より最大で45%も多くなることがあります。その一方で、デジタル・プラットフォームやサプライチェーン、政治リスク、さらには環境的な要因など、これまでは珍しいとされた引き金が企業にとってより大きな意味を持つようになっています。

これまでのランキング
(回答の割合とランキング位置)：
2018年 1位 (42%)
2017年 1位 (37%)
2016年 1位 (38%)
2015年 1位 (46%)

次の国で最上位リスク

- 🇦🇺 オーストリア
- 🇧🇷 ブラジル
- 🇨🇦 カナダ
- 🇨🇳 中国
- 🇨🇴 コロンビア
- 🇩🇪 ドイツ
- 🇮🇩 インドネシア
- 🇮🇹 イタリア
- 🇲🇾 マレーシア
- 🇳🇱 オランダ
- 🇵🇭 フィリピン
- 🇵🇱 ポーランド
- 🇸🇬 シンガポール
- 🇹🇯 タンザニア

次のセクターで最上位リスク：

- 🏭 化学薬品、医薬品、バイオ医薬品
- 🍷 食品／飲料
- 🏭 重工業
- 🚗 製造（自動車を含む）
- 🛢️ 石油／ガス
- ⚡ 電力とユーティリティ
- 🔋 再生可能エネルギー
- 🛒 小売／卸売
- 🚚 輸送業

事業中断（サプライチェーンの混乱を含む）の影響は、これまで7年連続でアリアンツ・リスクバロメーターでは企業の最大のリスクとしてランキングされてきましたが、2020年には、事業中断とも密接な関係にあるサイバーインシデントがトップの座につきました。

事業中断（BI）の脅威は、リスクマネジメント専門家の目から見てもはや単独の脅威としては最大のものではないとはいえ、その脅威が減少しているわけではありません。BI損害が、火災や自然災害などの従来の原因に加え、デジタル・サプライチェーンや社会不安などの新たな原因によりさらに複雑化していく傾向には衰えは見られません。

顧客やサプライヤーで発生した事案により企業が損害を被るサプライチェーンの中断（CBI）は、10年前はおろか、5年前よりもはるかに大規模化し、範囲も広がっています。自然災害、火災、サイバー攻撃はどれをとっても近年、複数国で複数企業に影響を与える大規模CBI損害事案を引き起こしています。自動車や医薬品といった産業では、高度に効率化されたサプライチェーンを世界規模で展開していますが、これによりきわめて大規模なBIやCBI事案に対する脆弱性も高まる結果となっています。たとえば、2018年米国で発生した自動車部品工場火災では、複数の自動車メーカーで供給不足が発生し、業界全体で何億ドルもの損害を引き起こしました。その前年、チェコ共和国の自動車部品メーカーで発生した火災でも同様の影響が出ました。さらに、他の産業もますますこのようなサプライチェーンを構築するようにな

ってきています。

最近の傾向

データの脆弱性とデジタル・サプライチェーンの反応

テクノロジーやデータへの企業の依存度の高まりがBIやCBIのクレームにも現れ始めています。原因はともあれ — 技術的な不具合、サイバー攻撃、火災や浸水のような物理的な原因など — 重要データやテクノロジーが使えなくなってしまうと、企業は大規模な事業中断損害を被ることになります。

データ、あるいは「ビジネスインテリジェンス」の喪失は、損害の重大な原因として浮上しています。企業が長期間にわたってデータへのアクセスができなくなると、たとえば注文を受け付けられないなどの状況に陥り、収益に大きな影響が出る可能性があります。2019年のBIクレームのなかで目立ったものの一つとして、ヨーロッパのあるメディア企業での火災に関連した事案がありました。クレームのかなりの部分が、データが利用できなかったことと、復元コストに関連したものでした。

サービスや商品を送り届けるうえでデジタル・サプライチェーンを活用することには数多くのメリットがあります。共有テクノロジーに基づくプラットフォームでは、当事者間でのデータ交換が可能となり、管理業務と注文を自動化し、オンデマンドで製品を配達できるようになります。デジタル・サプライチェーンは透明性が高く、商品を元まで遡って追跡することも可能です。たとえば、食品と医薬品産業ではサプライチェーンを移動する原料や製品を追跡するためにすでにブロックチェーンを利用していますが、これはたった2つのセクターの例に過ぎません。

しかし、このようなプラットフォームでは連鎖反応が起きる可能性もあり、そうなったらBIがセクター全体に雪崩のように広がることになります。技術的な不具合やサイバーイベントのためにプラットフォームが利用できない場合、同じシステムに依存し共有する複数の企業すべてに大きなBI損害が発生する可能性もあります。2019年6月、一部のGoogleクラウドサービスのシステム停止により壊滅的な障害が発生し、YouTube、Uber、Snapchatなど、数々の大手オンライン・サービスプロバイダーで数時間にわたり混乱が生じています。2017年には北米のAmazon Web Servicesが4時間停止するという事故がありましたが、これによりS&P 500の企業が被った総損害額は1億5,000万ドルに上ると推定されています。

「デジタル・サプライチェーンには効率的で追跡可能だという利点がありますが、データセンターの火災やハッキング攻撃により重大なBIが発生する可能性もあり、システムがいったんダウンしてしまうと手動業務に戻れなくなることもあります」とRaymond Hogendoorn (Global Head of Property and Engineering Claims, AGCS) は話します。「サプライチェーンをデジタル化すると、BIに対する企業の脆弱性も高まります」。

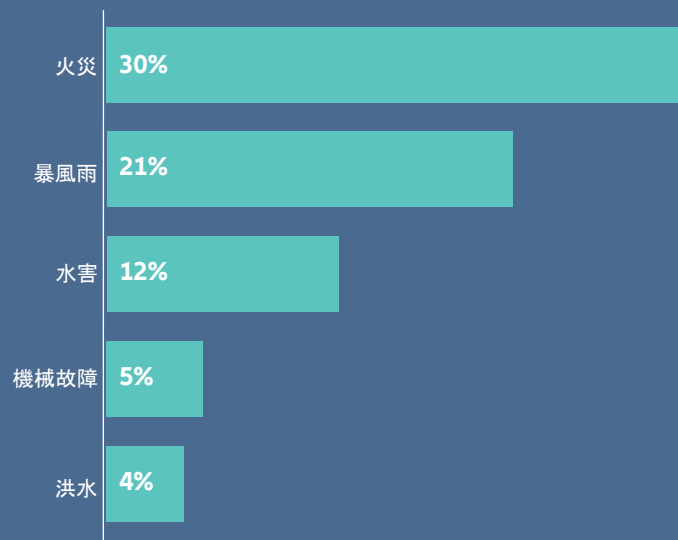
最近の傾向 過小評価される政治的暴力によるBI

今日の不安定な世界では、企業はあらゆる形態の政治リスクにさらされており、暴動や社会不安、ストライキ、そしてもちろんテロ攻撃により大きな混乱に見舞われることがあります。

過去1年の一部の例を見ただけでも、香港、チリ、フランス、ボリビア、コロンビアなどで社会不安が発生し、多くの企業が財物損害、BI、そして収益の損失に見舞われています。

「政治に端を発するBIリスクは過小評価されることがよくあります」とHogendoornは話します。「10年前であれば、たとえばチリのような場所で抗議デモが発生しても、グローバル企業にはほとんど何の影響もないということもありましたが、今日はこのような出来事の影響がはっきりと現れるようになってきています」。

事業中断保険クレームの原因として最も頻度が高いのは？



AGCSの調べでは、事業中断損害の原因として最も高い頻度で見られるのは火災／爆発事故で、件数としては全体の3分の1近く（30%）を占めています。また、火災に伴うBIコストにより最終的な損害額合計が大きく膨らむこともあります。たとえば、火災／爆発事故によるBI損害額の平均は580万ユーロ（670万ドル）に上り、財物の直接的な損害額の平均400万ユーロ（450万ドル）を45%も上回っています¹。

出典：Allianz Global Corporate & Specialty。2013年7月から2018年7月にかけて、財物損害（26億ユーロ）と事業中断（37億ユーロ）の両方の損害があった、企業保険クレーム1,175件、総額63億ユーロ（71億ドル）の分析に基づく。

2019年10月に始まったチリ政府に対する抗議デモでは、数人の死者、数千人の負傷者、財物への重大な損害が発生しています。何百軒ものスーパーマーケットが略奪や放火の被害に遭い、財物と輸送関連の損害は現在のところ30億ドル程度に上ると推定されています。小売業大手のWalmart社も大きな損害を被りました。

「仮に略奪『だけ』だったとしても、スーパーの営業再開までには数ヶ月かかるので、BI損害は莫大になります」とBjoern Reusswig (Head of Global Political Violence and Hostile Environmental Solutions, AGCS) は話します。「今回の事案による損害は、政治的暴力・暴動保険の歴史上最大のものの一つになると予測されています」。

また、政治リスクでは物理的な被害がなくてもBI損害が生じることがあります。香港では、長引く社会不安により観光客が前年比で40%も減少しており、観光産業に大きな影響が出ています。

「お客さまやホテルの宿泊客の足が遠のくだけではありません」とReusswigは続けます。「この他にもこのような事案による影響として、安全上の理由から従業員が職場に出勤することができなくなるという影響もあります。そのため、他の業種でも生産性が低下したり、生産停止に追い込まれる可能性があります」。

¹ 2013年7月から2018年7月にかけて、財物損害（14億ユーロ）と事業中断（21億ユーロ）の両方の損害があった総額35億ユーロ（40億ドル）354件の火災クレームの分析に基づく。

香港では、政治的暴力や暴動を担保する専用保険への加入はあまり一般的ではないために、多くの企業が損害や混乱のコストを自ら負担せざるを得なくなります。一方で、保険会社としては政治リスクから生じるBI損害が世界的に増加しており、その理由の一つとして区域封鎖や主要施設休止に伴う利益喪失をカバーする特約を購入する契約者が増えているということもありますが、企業やサプライチェーンの国際化が進んできているということも理由の一つです。

最近の傾向
迫り来る環境的要因

企業は今後、異常気象や環境的要因による混乱のリスクにますますさらされるようになります。自然災害による損害に占めるBIの割合は、わずか10年～20年の間に大幅に高まってきており、これに一役買っているのがグローバルゼーションとサプライチェーンにおける依存関係です。たとえば日本で発生した暴風雨やチリで起きた地震により、ヨーロッパの製造工場での生産業務に影響が出るといったこともあり得るのです。

異常気象はまた、水や電力などのリソースの可用性にも影響することがあり、これにより予期せぬ影響が出ることもあります。2018年にはライン川の一部で水位が下がって航行が不能となったことで、メーカー数社が生産の中断に追い込まれています。気象事象や気候変動に対する軽減対策でさえBIを引き起こすことがあります。たとえば、2019年のカリフォルニア州の干ばつの際には、電力会社が森林火災のリスクを軽減するために計画停電を実施しています。

さらに、住宅地にあった製造施設や工業施設の操業が認められなくなったり、洪水リスクの高まりなどにより拠点の移転を余儀なくされるといったケースをはじめ、新たなサプライヤーを見つけなければならないような状況が発生することも考えられます。また一部の業種、特に現代の食品サプライチェーンにおいては、主要原料の供給の継続性に関する懸念が高まっています。食品／飲料セクターでは、2018年夏の需要ピーク時に二酸化炭素が不足して混乱が生じました。また、異常気象により特定食品の供給が変動することもあります。近年の干ばつ、熱波、洪水などでは、野菜、小麦、牛乳などの収量に影響が出て、これにより食品メーカーや小売業者への供給に影響が出ています。

「サプライチェーン・リスクへの異常気象の影響、そしてこれらのリスクをどのようにマネージするかということ、をますます多くの企業が考えるようになってきました」と話すのは **Georgi Pachov (Global Property Practice Leader, Cyber, AGCS)** です。「食品／飲料業界の企業からは、製品の主要原料に関わるBI、そしてこれを保険でカバーする方法としてどのようなものがあるかについての問い合わせも寄せられています。保険業界としては、今後目的に合致したBIソリューションの提案が課題になります」。

軽減
カスタマイズされたBI保険への転換

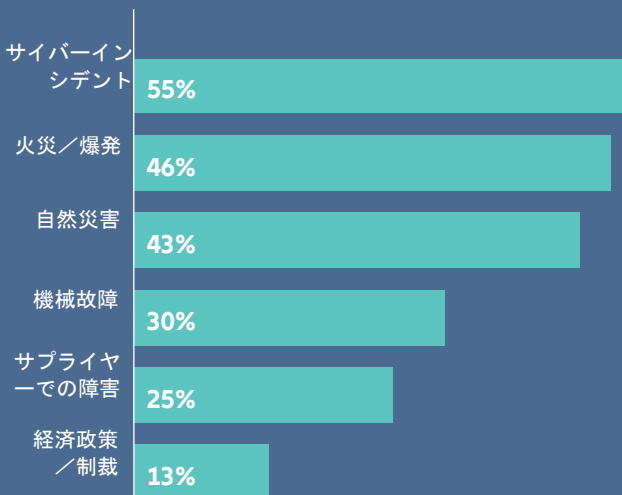
多くの業種やサプライチェーンで事業中断に対する懸念が高まっている中で、株主や顧客もリスク回避志向を強めており、予期せぬ不祥事に対する許容性も低くなってきています。その結果として大企業は収益を守るために、よりカスタマイズされたBIソリューションをますます求めるようになってきました。

「企業収益を守るためのBIソリューションの需要は高まっています」とPachovは話します。「火災や自然災害といった従来のBIの原因ではなく、2年～4年先を見据えたビジネスモデルや戦略へのリスクから身を守るためのものです」。

「5年後のBI保険ソリューションは、現在よりもはるかにカスタマイズされたものになり、ソリューションの開発と位置づけではデータに基づいた考え方が盛り込まれるようになるでしょう」。お客さまの収益をより広範なBIリスクから守ることを目的に、当社ではお客さまとのパートナーシップを構築しています」。

▼ [事業中断保険ソリューションに関する詳細はこちら](#)

業務中断の原因として、あなたが最も脅威と感じるのは？



「今日、多くの企業のサプライチェーンの統合が以前よりもはるかに進んでおり、BIの経済的影響も拡大を続けています」と **Raymond Hogendoorn (Global Head of Property and Engineering Claims, AGCS)** が説明します。「ある企業で発生した火災やサイバー攻撃のような事案がサプライチェーン全体に波及し、複数のメーカーに影響が及ぶこともあります」。

出典：Allianz Global Corporate & Specialty。数字は、回答をした全参加者（1,018）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



27%▲2019:4位(27%)

3 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)

米中貿易紛争の緩和への期待は2019年中には実現することはありませんでした。約1,300の新たな貿易障壁が設けられ、保護主義がニューノーマルとなっています。一方、2020年には「情勢を一変させる」EUの持続可能性関連規制が導入されるなど、企業は大きな課題に直面することになります。

次の国で最上位リスク：

- オーストリア
- ブルガリア
- コロンビア
- クロアチア
- ハンガリー
- ロシア

米国と中国という世界の2大経済大国は、18か月以上にわたって激しい貿易紛争を闘っており、数千億ドル相当の互いの商品に関税を課しています。米中貿易紛争により米国の平均関税率が2017年末の3.5%から8%に増加しており、1970年代以来みられることのなかった水準に近づいています。それと同時に、世界貿易全体で関税が課される物品の割合も高まっています。

欧州連合(EU)では、このような傾向に対抗するという意味合いもあって反対のスタンスをとっており、EU-日本自由貿易協定とEU-シンガポール自由貿易協定が発効し、欧州委員会の委任終了の数か月前にはEU-ベトナムとEU-メルコスール国(アルゼンチン、ブラジル、パラグアイ、ウルグアイ)との協定交渉を最終決着していることから分かるように、より自由で環境に優しい貿易モデルを積極的に推進しています。「貿易政策は、経済外交、地政学的影響力、環境政策など、さまざまな政策目的実現のための単なる政治の道具になりつつあります」とLudovic Subran(Chief Economist of Allianz)は説明します。「このような活動は米国に限定されるものではなく、日本、韓国、インド、そしてEUにも広がっています」。

一方、企業は2020年に大きな規制上の課題に直面することになります。「EUの持続可能性関連規制は『情勢を一変させる規制』に他なりません」とSubranは付け加えます。「企業への影響は、これまでの会計処理やデータ保護関連の新規制の影響と同じぐらい広範囲に及ぶことになります」。

持続可能性をリスクマネジメントとして主流化するという事は、要するに、どの企業も最先端の方法論と手法を用いて、環境、社会、ガバナンス(ESG)関連のリスクと機会を開示することにより、ESGプロファイルを確立しなければならないということを意味します。このプロセスの中心となるのは脱炭素化の推進、つまり2050年までに二酸化炭素排出ゼロを実現するための明確な道筋を定義することです。多くの国がすでにこの目標を法律で定めており、今後数年のうちに、おそらくEUを含むさらに多くの国々がこれに追従することになります。多くの企業にとって、データ収集、ターゲット設定、そして測定を実施するプロセスは手間のかかる作業になりますが、その一方で大きなチャンスをもたらすものともなります。「企業も投資家も、自らに課される規制上の制約も大きな原動力となり、ビジネスパートナーの選択に際しては、ますます持続可能性の認定などに基づいて選択を行うようになっていきます」とSubranは話します。「今後施行される持続可能性関連規制を予め織り込んで行動する企業は、競争面で他社に先んじることになります」。

「持続可能性は生き残りや成功のための最重要課題であり、これはヨーロッパに限ったことではありません。この分野で先頭に立って規制を行っているのはEUですが、他のEU施策と同様に、ヨーロッパの持続可能性規制はかなり急速に世界標準になっていくものと考えられます」。

4 自然災害

(例：暴風雨、洪水、地震)

21% ▼2019:3位(28%)

2019年に大きく報道された災害には、アジアでの壊滅的な台風やオーストラリアの記録的な森林火災などがあります。しかし、再保険会社 Swiss Re社によれば、自然災害による経済損失額は実際には前年比で20%減の約1,330億ドルにまで減少しています¹。北アメリカのハリケーン・ドーリアン(45億ドル)、そして日本の台風15号(70億ドル)と19号(80億ドル)などを含めたうえで、保険金支払額も840億ドルから500億ドルに減少しています。

「2019年も、2017年の大西洋ハリケーン期に匹敵する規模の経済損失(過去最高記録)をもたらす大規模災害が発生することはありませんでした」と話すのはCarina Pfeuffer (Cat Risk Analyst, AGCS) です。

「複数の中小規模の災害により被害が広範囲にわたって発生し、その被害の合計は保険金支払額の総額を大きいものとなりました」。

近年、地震や津波など、気象関連以外の大規模自然災害が少なく、その結果としてアリアンツ・リスクバロメーターではこれらのリスクの重要度が低下しています。「とはいえ、気象学的、地球物理学的、気候学的、水文学的な事象に頻繁に見舞われる世界の多くの地域では自然災害リスクはトップ3に挙がっています(例：米国、中国、日本)」とPfeufferはいいます。「同時に、気候変動/天候の不安定化は、アリアンツ・リスクバロメーターで史上最高位に上がってきています(第7位)」(19ページ参照)。

▼ [暴風雨チェックリストをダウンロード](#)

▼ [洪水チェックリストをダウンロード](#)

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)

21% ■2019:5位(23%)

Ludovic Subran (Chief Economist, Allianz) によれば、2019年は市場のボラティリティが高く、これは2020年も続いていきます。また、貿易紛争と政治リスクに起因する不確実性も、引き続き市場に影響を与えることとなります。金融市場への政治リスクの直接的な波及、そして介入主義的な政策によるマイナスの外部リスクをマネージする必要性が、低成長・低インフレによって覆い隠されることも考えられます。ボラティリティの高まりとともに、グローバル市場の方向性を予測することも難しくなります。歴史的に見れば、サイクルの後期では債権資産が好調になります。

深刻な景気低迷が起きれば、株式市場では二桁台の下方修正が生じることになります。超穏健である中央銀行は、債券利回りを低いレベルに維持するでしょう。「2020年満期の10年ドイツ国債の利回りは-0.4%、米国債の10年利回りは1.7%になると私たちは予想しています」とSubranは続けます。「米中貿易紛争によるボラティリティの高まりにより、ドル高が続き、人民元安はさらに進むはずで、世界の細分化が進むということは、新興市場にとっては商品価格、通貨、資本の流れが不安定化することを意味します」。

6 火災/爆発

20% ■2019:6位(19%)

火災/爆発事故は、アリアンツ・リスクバロメーターの回答者によれば企業への2020年の脅威としては6番目に挙がっていますが、AGCSによる保険金事故分析の結果を見ると、実際には経済的損失の最大の原因となっています。火災/爆発事故は、2018年までの5年間で140億ユーロ(157億ドル)を超える損失が発生しており、これはAGCSが調査した47万件を超える保険金事故の総額のほぼ4分の1(24%)に相当します。これは、損害原因の第2位、航空機の衝突/墜落事故(14%)を大きく上回っています。火災による保険金支払額の平均でさえ、150万ユーロ(165万ドル)に達します。

大企業では防火対策やリスクマネジメントの改善により火災による損害は減少していますが、一部の業種や製造現場では、面積あたりの財物/資産の価値が過去10年間で4倍にまで膨らんでおり、そのため、いったん事故が発生した場合の損害やその後の事業中断(火災は事業中断クレームの原因として最も頻度の高い原因[15ページ参照])によるコスト負担が大幅に高まることとなります。小規模火災であっても、金銭的には大きな影響が出ることもあり、それがセクター全体に波及することもあります。企業が損害のリスクを低減するには、現場の防火対策を定期的に評価し、見直す以外にありません。

¹ Swiss Re: 「大規模災害による世界各国の2019年保険損害額は560億米ドル」(Global catastrophes caused USD 56 billion insured losses in 2019) 2019年12月19日



17%▲2019: 8位(13%)

7 気候変動

／天候の不安定化

企業は、自然災害により大きな財物損害が発生する可能性がありうることに加えて、気候変動関連のリスク — 業務面、レピュテーション面、規制面の影響など — についても全方位的に考える必要があります。気候変動への対処には、是正措置と投資が必要となりますが、それはビジネスチャンスをもたらすものでもあります。

気候変動／天候の不安定化は、2020年のアリアンツ・リスクバロメーターのランキングで史上最高の順位に上昇していますが（回答の17%）、これはその影響が企業と保険会社の両方にとって大規模かつ不測のシナリオを生じさせ、そのため軽減と回復にむけたあらゆる対策の中心とするべきであることを反映したものです。気候変動によるコスト負担の増大はすでに顕在化しています。分析からは、気象関連の洪水被害事案の件数が1980年の3倍から4倍の水準にまで増えていることが分かります。

世界の平均気温上昇を、産業革命以前に比べて2℃より十分低く保ち、1.5℃に抑える努力をすることを目標とした国連の重要なパリ協定から4年が経過した現在、排出量削減に向けたこれまでの進捗と政策が不十分であったことが明らかになっています。

将来のビジネスモデルをより気候に優しいものとするために、多くの産業では変革に伴う大きなリスクと費用負担に直面しています。アリアンツの推定によれば、気候変動による諸々の課題に対処するために、世界各国の企業で今後10年間で2.5兆ドルものコスト負担が生じることも考えられ¹、そのうちエネルギー・セクターをより「グリーン」にするためのコストの支出が最大となります。これ以外で特に影響の大

きいセクターとしては、ざっと挙げただけでも自動車、化学薬品、農業産業などがあります。

リスクとチャンス

「これらのセクターは、体系化された準備と行動を今起こさなければ、規制当局や政府の圧力が高まり、先延ばしにした移行をきわめて短期間のうちに行うことを余儀なくされます」と Thomas Liesch (Climate Integration Lead, Allianz) は話します。政策としては、カーボン・プライシング（炭素の価格付け）、エネルギーや効率化に関する諸条例、モビリティ関連規制、特定業種に特化した課税、罰金、および課徴金が考えられます。

そのため、企業は移行リスクに対応し、ビジネスモデルの脱炭素化を進める必要があります。回復力の鍵は、排出量を削減し、避けることのできない気候変動の激しさに適応することにあります。

¹ アリアンツ：「COP25 ただ乗りなどというものはない」(No Such Thing As A Free Lunch)

「変革には、もちろん投資と費用が伴いますが、これに勝る新たなビジネスチャンスも現れます」と Liesch は話し、新しいビジネスモデル、製品、販売市場などから生まれるチャンス — たとえば再生可能エネルギーの生産技術、蓄電池の生産、レアアースの採掘、さらには余剰の再生可能電力による水素生産のような新技術 — は企業の費用負担の何倍にもなることが考えられると付け加えます。

物理的・人的損害の影響

アリアンツ・リスクバロメーターの回答者によると、企業が気候変動によって最も恐れるリスクは物理的損害の増加で（回答の49%）、それに次いで業務上の影響、そして市場や規制環境の変化による影響となっています（図を参照）。

「経済的には、気温が3°C~ 4°C高まった世界で生じる物理的なリスクとコストは、数倍にもなります」とLieschはいいます。また、アリアンツも加盟する保険業界のプロのリスクマネージャーからなる団体、CRO Forumの報告書「The Heat Is On – Insurability and Resilience In A Changing Climate」の知見を引用し、Lieschは次のように指摘します「熱波と干ばつの大幅な増加、アマゾン熱帯雨林の消失、地中海地域の砂漠化、永久凍土の融解、異常気象の増加と海水面の上昇、リスクにさらされる財産の価値の低下、低海拔沿岸地域の放棄、そしてその適応（例：護岸や排水設備など）や維持にかかるコストの増加などは、今後発生する可能性のある影響のほんの一部に過ぎません」。

地球温暖化は世界各国で激しい災害を引き起こし、企業を脅かしています。海水面の上昇、これまで以上に乾燥した干ばつ、激しさを増す暴風雨、大規模な洪水などは、工場などの資産をはじめ、サプライチェーン全体を結び付ける輸送やエネルギーなどの繋がりを脅かし、企業にとっては物理的な脅威となります。

「気候変動は、将来の問題として提示されることが多く、地球温暖化の道筋も今世紀末を念頭に計算されますが、この視点も急速に変化してきています」と話すのはAmer Ahmed（CEO, Allianz SE Reinsurance）です。「『気候危機』や『気候の緊急事態』に関する公の議論では、私たちの社会が今日すでに支払っている犠牲を強調するようになっていきます」。

Allianz Reでは、気候変動の研究者に年間賞を授与するとともに、その影響を軽減するソリューションの提案も行っています。Ahmedはこう続けます「保険会社は、リスクを引き受ける者として当事者であり、私たちの事業にもすでに気候危機の影響が見られます」。

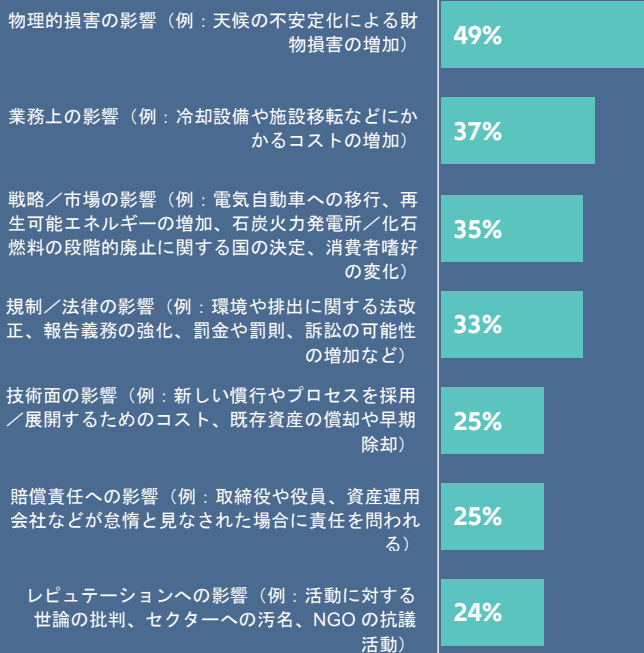
たとえば、2017年は特に重大な大災害が発生した年でした。ヒューストン市では、40年にも満たない間に「500年に1度」といわれる洪水に3度も見舞われ、カリフォルニア州では史上最も破壊的な20の森林火災のうち5つをこの年に経験しています。

さらに、バングラデシュ、インド、ネパールでは4,100万人が洪水やモンスーンの被害を受けています。かと思えば、世界で最も通行量の多い水路であるライン川では、水位が歴史的な低水準にまで低下し、商業交通が立ち往生しました。

このような災害では心痛む人的被害も発生しましたが、これは何も最貧国に限ったことではありません。Climate Transparency の最近の報告では、異常気象による G20 国での死者数は年間 16,000 人に上り、経済的影響は年間 1,420 億ドルに達すると推定しています²。

2 Climate Transparency: 「ブラウンからグリーンへ — G20 諸国の純ゼロ排出経済への移行2019」 (Brown To Green, The G20 Transition Towards A Net-Zero Emissions Economy 2019)

気候変動：その影響による企業への最大のリスクは？



「気候変動が企業に与える影響はさまざまです」と Chris Bonnet (Head of ESG Business Services, AGCS) はいいます。「まず、企業が直面する物理的損害のシナリオが広がります。たとえば、気温が2°C以上上昇すると、暴風雨や洪水のリスクにさらされる地域が拡大します。次に、排出量を削減するための法的・政治的な政策が、自動車、輸送、ユーティリティなどの産業にとって大きな課題となっており、これらの業種はどれも、ビジネスモデルを変革して「脱炭素化」する必要があります」。

出典：Allianz Global Corporate & Specialty。数字は、回答をした全参加者（2,718）の回答のパーセンテージを表したものです。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。

規制、投資家、賠償責任の脅威の高まり

激しさを増す気象事象による損害の大規模化への対応の他にも、企業の対応が求められる気候変動関連の脅威が先進国でも、新興市場でも増加しています。

「ビジネス戦略、業務面、そして製品面でも気候変動に適切に対処しない場合、消費者からの批判、レピュテーションの低下、規制や法的措置などを招く場面が増えることになると企業は気づき始めています」と話すのは**Chris Bonnet (Head of ESG Business Services, AGCS)**です。

気候変動関連の新たな法律が世界各国で毎年約1,500ほど施行されていると推定されますが、地域によって管轄当局の対応はまちまちです。

ヨーロッパでは金融セクターに焦点を当てており、たとえば英国では最近、イングランド銀行が「世界で最も厳しい」とする「気候ストレステスト」の下で数十年に及ぶ3つの異なるシナリオで、銀行（貸出）と保険会社を対象としたストレステストを実施すると発表しています³。オーストラリアでは、気候リスクを健全性規則に統合するために多くの努力が行われています。日本では、金融システムと重工業の密接な関係を踏まえて、統合的なアプローチが必要であるとの認識に達し、194社が気候関連財務情報開示タスクフォースの提言を採用しています。気候変動関連情報の開示に関しては、シンガポールもリーダー国の一つと見なされています。

しかし、気候変動への対応に関連して企業に圧力をかけていけるのは政府や規制当局だけではありません。企業に対する気候変動関連の市民活動は、特にヨーロッパで高まっており、企業経営陣は投資家やその他のステークホルダーからますます説明を求められるようになっていきます。たとえば、アクティビスト（市民活動的）ヘッジファンドのTCIでは最近、二酸化炭素排出量の開示を怠った企業の役員を追求していくとの計画概要を発表し、さらには気候透明性を強く主張しないファンドマネージャーを解職するよう資産所有者に呼びかけています³。

「気候リスクに対する企業の対応に関心を持つステークホルダーは多く、行動を起こさないことによるレピュテーションの低下はステークホルダーの判断に影響を及ぼすこととなります」と話すのは**Karsten Berlage (Regional Head, Americas, AGCSの Alternative Risk Transfer unit)**。「資本投資家が、環境への配慮が足りないと見なされる企業を投資先から除外するといったこともあり得ますし、格付け会社とメディアは、気候災害を回避するために企業がどのような取り組みをしているかを注視しています」。



気候変動リスクの開示を怠ったことが訴訟の対象となることが今後さらに増えていきます。

気候変動リスクの開示を怠ったことに対する訴訟が今後さらに増加していくことに疑いの余地はありません。現在までに世界の30ヶ国以上で気候変動関連の訴訟がすでに起こされており、その7割以上は米国で起こされたものです。米国では、企業が気候状態の変化に合わせてビジネス慣行を調整することを怠ったとする訴訟が増えています。訴訟の多くは、化石燃料の積極的な生産者、いわゆる「炭素メジャー」を標的としたものですが、アグリビジネス、製造業、輸送など、炭素排出量の多い他の産業にも拡大していくものと考えられます。

将来に向けた準備

「環境、社会、ガバナンス (ESG) 関連の課題と気候変動への企業レベルでの取り組みに関して、企業役員が責任を問われることもあることを踏まえると、企業の戦略、ガバナンス、リスクマネジメント、財務報告などを検討する際に、これらの影響も考慮に入れていく必要があります」と**Shanil Williams (Global Head of Financial Lines, AGCS)**は言います。「低炭素の未来に向けて企業のビジネスモデルの準備を整えるという作業は、戦略、ガバナンスと報告、リスクマネジメント、および業務機能に関連した複数部門による取り組みになっていきます」。

「どの企業も、気候変動対応の移行における自らの役割とペースを決め、主要なステークホルダーを巻き込んで対処する明確なスタンスを確立する必要があります」とBonnetは付け加えます。「リスクマネージャーは、ESGと気候変動の重点化を社内でも推進し、意思決定に反映させていく必要があります」。

「現在、多くの企業がリスクマネジメントよりもリスク報告に重点を置いています。気候変動の真の影響を理解するためには、通常の2~5年というスパンを超えて、さまざまな将来シナリオを予測して、それに備える必要があります」。

³ Financial Times 「ヘッジファンドTCIは気候変動問題で企業役員を責任を問うことを宣言」 (Hedge fund TCI vows to punish directors over climate change) 2019年12月

8 レピュテーション・ブランド価値の喪失 15%▼2019:9位(13%)

サイバー侵入からソーシャルメディア、企業の不正行為、そしてサプライヤーの不正行為にいたるまで、レピュテーション関連の企業不祥事の原因となるシナリオは増え続けています。企業のレピュテーションの価値を算出することは困難ですが、その価値が明確になるのは、問題が発生してレピュテーションが損なわれたときです。また、市場価格が驚くほどのスピードで崩れることもあります。レピュテーションの危機の4分の1以上が1時間以内に、3分の2以上が24時間以内に拡散すると推定されています。ソーシャルメディアの登場後、レピュテーション事案の株価への影響は2倍に高まっていると考えられています。

リスクが高まっているにもかかわらず、依然として多くの企業で、レピュテーション危機の影響から身を守るための対策が不十分です。効果的な計画と危機管理が必須となっており、専門家による対応があるかないかで事態が違ってくることもあります。また、レピュテーション危機を有効にマネージした企業の時価総額は、翌年には6%上昇するという調査結果もあります。

保険もまた、レピュテーション事案に関連する純営業利益への打撃から会社を守り、ブランド価値回復に向けたコンサル費用などの負担、そして365日24時間体制のレピュテーション危機対応や戦略的なメディア分析報告などのソリューションを提供し、無形のリスクに対して具体的な支援を提供するものが増えています。

レピュテーションリスク保険に関する詳細はこちら

9 新技術 13%■2019:7位(19%)

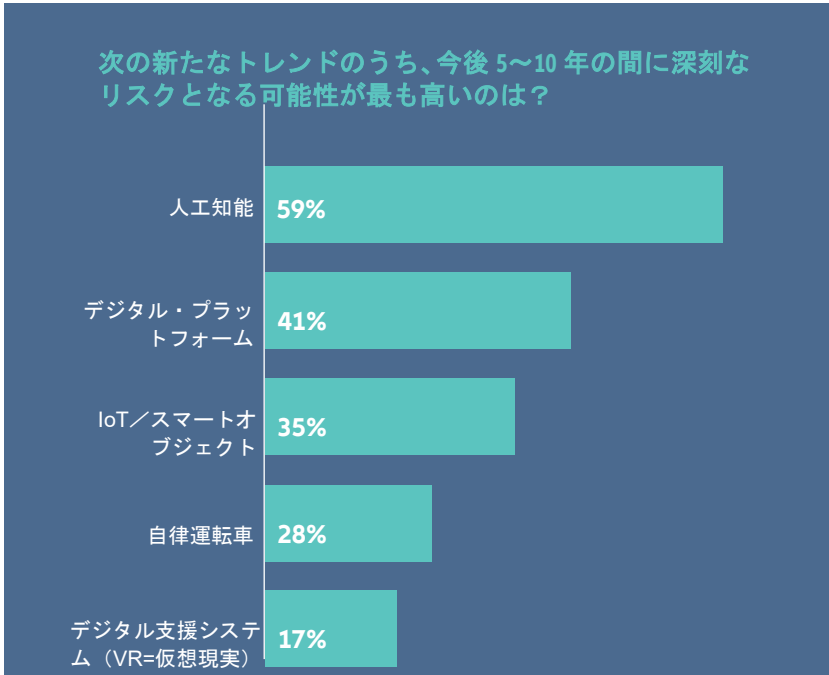
(例：人工知能、自律運転車、3Dプリンティング、IoT、ナノテクノロジー、ブロックチェーンなどの影響)

新技術は企業に大きなビジネスチャンスをもたらします。その一方で、新技術によりリスクが生じ、意図せぬ影響が出ることもあります。アリアンツ・リスクバロメーターの回答者によれば、現在、多くの産業で変革の重要な推進力として利用が増加している人工知能（AI）は、将来的にリスクを生じさせる可能性が最も高い新技術でもあります（左グラフを参照）。

「チャットボットから自律運転車に至るまで、AIの広範な利用により産業や社会に変革が起こっており、効率の向上、新製品、反復作業の削減などのメリットが生まれています」と説明するのは Michael Bruch（Global Head of Liability Risk Consulting/ESG, AGCS）です。

「たとえば保険業界では、AIの利用により取引のプロセスを改善することができ、すでに多くの利点が見られます。お客さまのニーズをより正確に特定することができ、保険証券の発行やクレーム処理をより迅速に、低コストで行え、事業中断、サイバーセキュリティ脅威、マクロ経済危機など、重大な企業リスクの予測をより正確に行うことができます。さらに、チャットボットは365日24時間体制で顧客対応を行うことができます」。

その一方で、AIの進歩に伴い、機械が人間に代わって意思決定をするようになることも考えられます。意思決定が移譲され、透明性や人間の監視が欠如すると、不測のリスクや予測不可能な結果が生じ、複雑な賠償責任問題に発展することも考えられます。それと同時に、AIに関わる倫理的、社会的な懸念も高まっていると Bruchは言います。



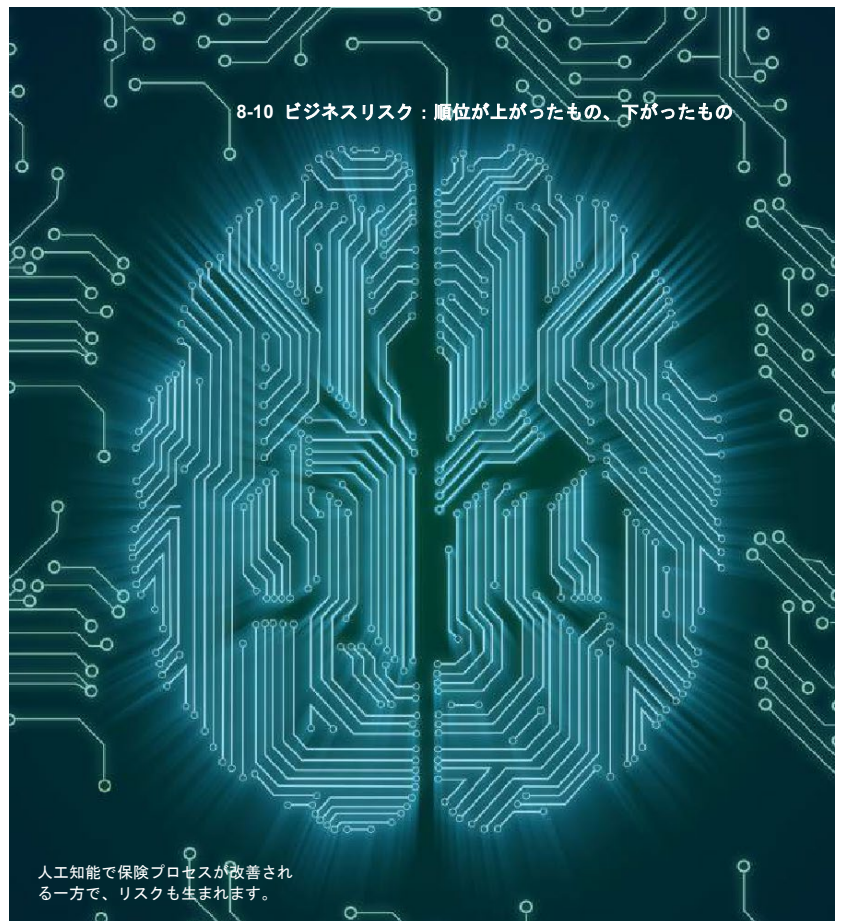
出典：Allianz Global Corporate & Specialty。数字は、回答をした全参加者（2,718）の回答のパーセンテージを表したものです。また、リスクは最大で3つまで選択可能であることから、数字を合算しても100%とはなりません。

デジタル・プラットフォームの支配

今日の企業が直面する複雑な技術的な動向のうち、最も直接的な影響を生じさせるのはデジタル・プラットフォームです。企業がデジタル・プラットフォーム上に中核機能を構築または移行するなか、事業を推進するために企業が利用するクラウドベースのソフトウェアやサービスの集合体が過去10年で発展を遂げてきました。技術、ビジネス、社会経済の分野で今後重要となる動向をとりまとめたレポート、**AGCS Trend Compass**によると、このトレンドは現在、臨界質量に達しています。

これらのプラットフォームでは、2つまたはそれ以上のユーザーサイト間の直接的なデジタル・インタラクションを可能にし、購入者と販売者のコミュニティを結び付けることで、商品、情報、仕事、サービスを自由に提供したり求めることができるようになってきました。これにより巨大な規模の市場が生まれますが、これは世界の時価総額上位企業10社のうち7社がプラットフォーム・ビジネスモデルを基盤としていることから分かります。しかし、デジタル・プラットフォームへの依存度の高まりによりリスクの可能性も高まり、**アリアンツ・リスクバロメーター**の回答者はこの意味でデジタル・プラットフォームをAIに次ぐ第2のリスクに挙げています。

「それぞれの業種でプラットフォームの台頭に直面する大企業はいくつかのリスクにさらされます」と話すのは**Adeline Roupillard**（**Global Practice Head of Digital Transformation, AGCS**）です。「プラットフォームは市場の独占につながる可能性があります。初期のプラットフォームは、市場参加者のインタラクションのあり方を再定義し、それにより市場全体を支配するようになりました。プラットフォームがそれをそれほど早く出現しなかった産業において企業は、競争相手のプラットフォームがスタンダードとなることを許すわけにはいきません。なぜなら、そうってしまったら自分がそのプラットフォームに縛られることになり、事業運営に大きなコスト負担を強いられることになるからです。」



人工知能で保険プロセスが改善される一方で、リスクも生まれます。

「企業として、業界をリードするプラットフォームを持たない場合、顧客への直接的なアクセス、そして顧客関係から得られる貴重なデータを徐々に失ってしまい、その結果としてブランドを損ねてしまうリスクを被ることになります」。そして、デジタル・プラットフォームがどんどん大規模化するにつれて、相互接続性のリスクも増大していきます。技術的な不具合やサイバー事案など、どれかひとつの要素に障害が発生すると、プラットフォームそのものが利用できなくなってセクター全体に連鎖的に事業中断が波及するなど、バリューチェーン全体に影響が及ぶ可能性もあります。システム障害が長引けば、このような事案での損害額は複数の企業にわたって数億から数十億ドル単位に達することも考えられます。

▼人工知能のリスクについて詳しく知る

10

マクロ経済の動向

(例：金融政策、緊縮財政、商品価格の上昇、デフレ、インフレ)

11%▲ [新]

2019年を通して、景気後退のリスクがますます現実味を帯びていきました。**Ludovic Subran**（**Chief Economist, Allianz**）によれば、2019～2020年は超穏健である中央銀行と新たな財政刺激策が（米国、中国、そして度合いは少ないもののヨーロッパでも）世界的な景気後退を回避する助けとなるでしょう。とはいえ、横ばい成長が常態化します。

2019年上半期に貿易や製造業、そして多くの国の経済で見られた局所的な景気後退が、政治リスクの高まりによって（米中のしのぎ合い、Brexit、イタリアの新政府）夏頃悪化しました。

「今後を見通して私たちが描く基準シナリオはソフトランディングで、消費者が回復力に貢献することになります」とSubranは話します。金融刺激策もこれまではうまく機能していましたが、現在の利率では、他の脆弱性を助長しながら効果をますます失っていくこととなります。このような緩和的な金融政策からの撤退を急ぎすぎたり、舵取りを誤ってしまうようなことがあれば、すでに高水準にある債務の蓄積は米国と中国で — 特に民間部門に関連して — 懸念材料となる可能性があります。

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。

Africa

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

Asia Pacific

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

Central and Eastern Europe

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

Mediterranean

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

North America

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

South America

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

UK, Middle East, Nordics

Jonathan Tilburn
jonathan.tilburn@allianz.com
+44 20 3451 3128

Global

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

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

編集チーム : Greg Dobie、Christina Hubmann、Damien Keg、Alejandra
Larumbe、Heidi Polke、Joel Whitehead

デザイン : Kapusniak Design

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 #ARB2020



LinkedIn

www.agcs.allianz.com

[▼ アリアンツ・リスクバロメーター2020の全結果をダウンロード](#)

免責条項及び著作権

Copyright © 2020 Allianz Global Corporate & Specialty SE。無断複写・転載を禁じます。

本書に記載される内容は一般情報を提供することを目的としたものです。記載情報の正確さには万全を期しましたが、情報はその正確性に関する表明や保証を一切伴うことなく提供されたもので、Allianz Global Corporate & Specialty SEは記載の過ちや漏れについて一切の責任を負うものではありません。

Allianz Global Corporate & Specialty SE
Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany

商業登録 : Munch HRB 208312

画像 : Adobe Stock / iStockPhoto

2020年1月