Allianz Global Corporate & Specialty

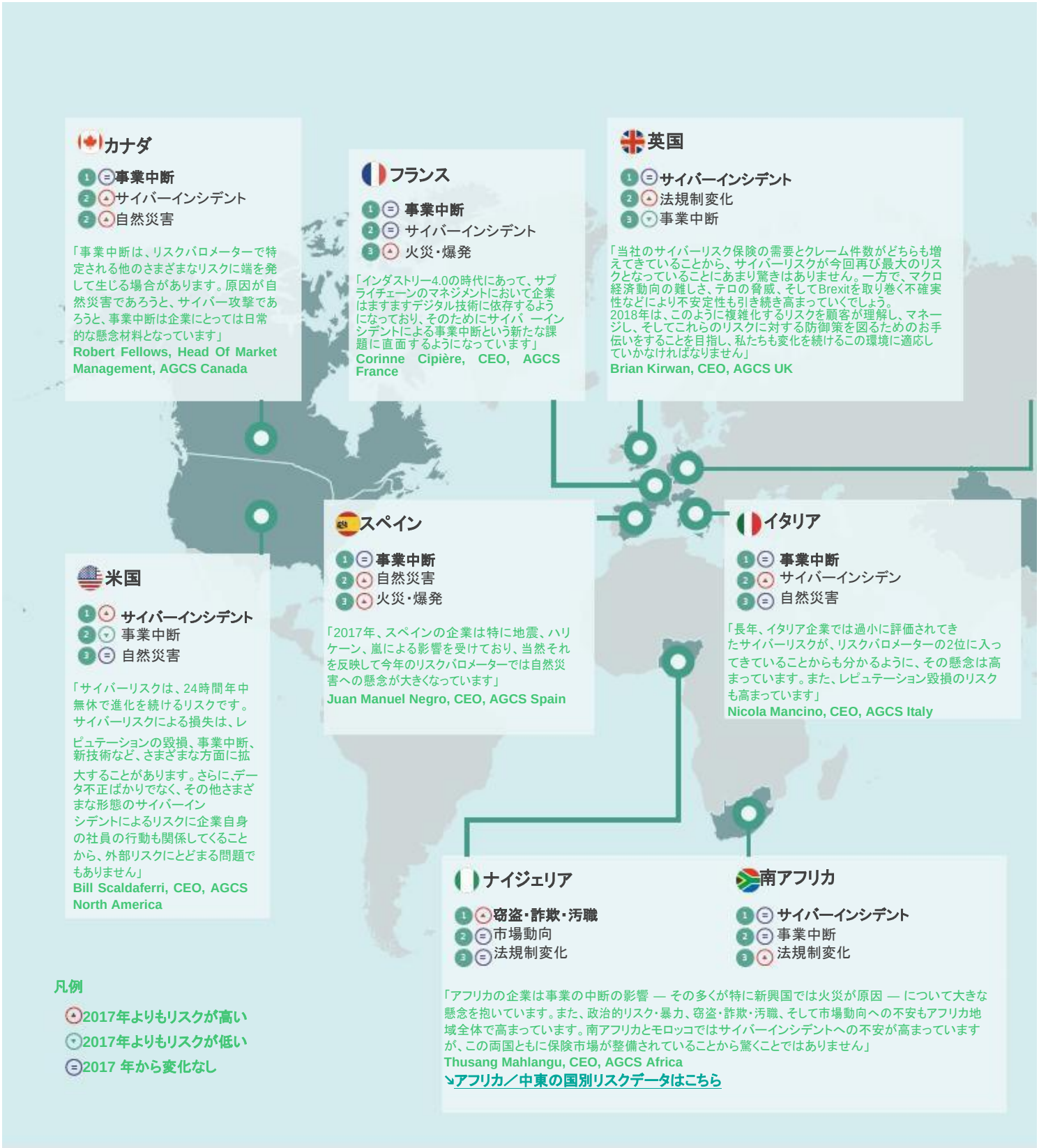
アリアンツ・リスクバロメーター

2018年のトップビジネスリスク

80 ヶ国、1,900人に及ぶコーポレート・リスク・マネジメントの専門家が考える
企業にとっての2018年の最大の脅威とは

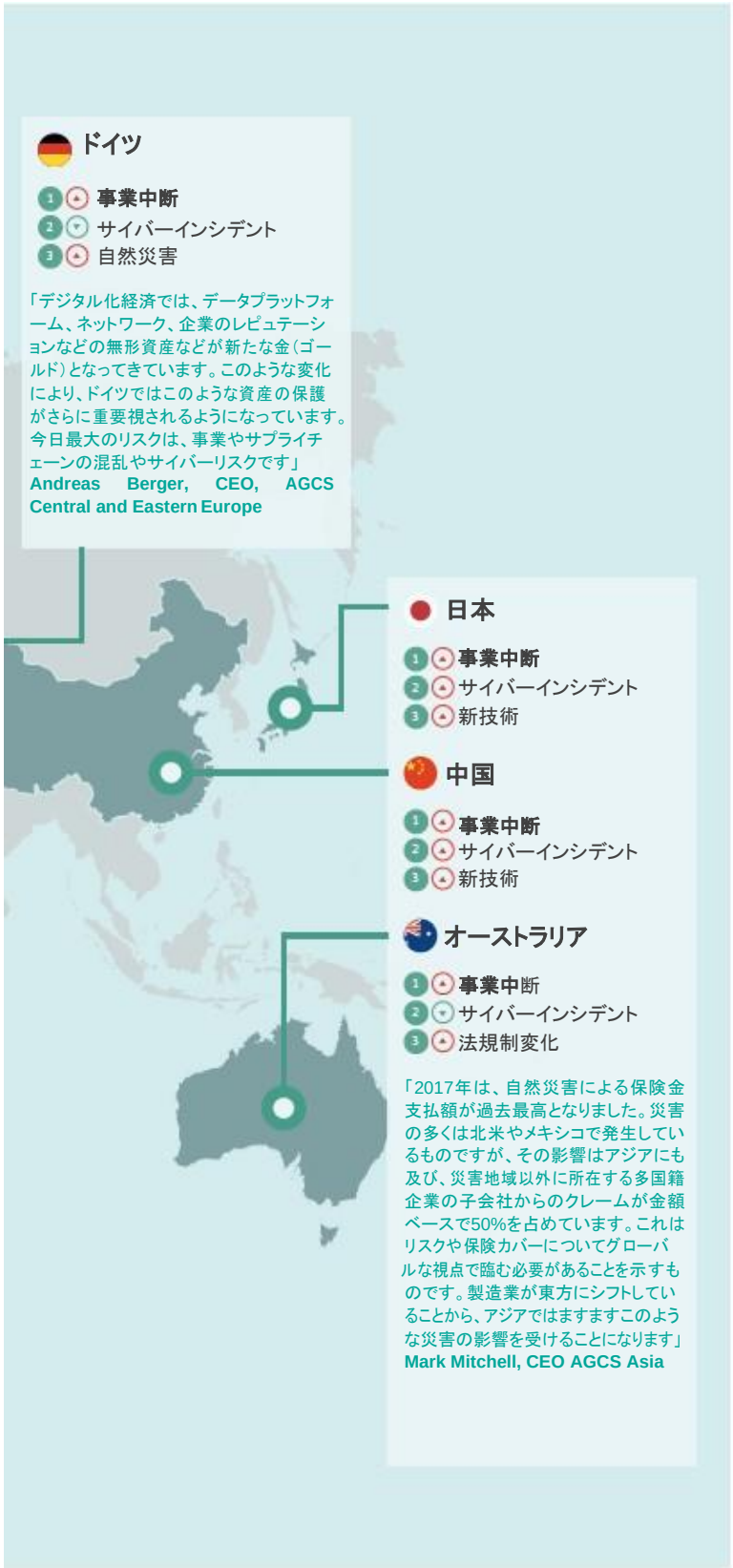
Allianz

スナップショット：2018年 各国最大のビジネスリスク

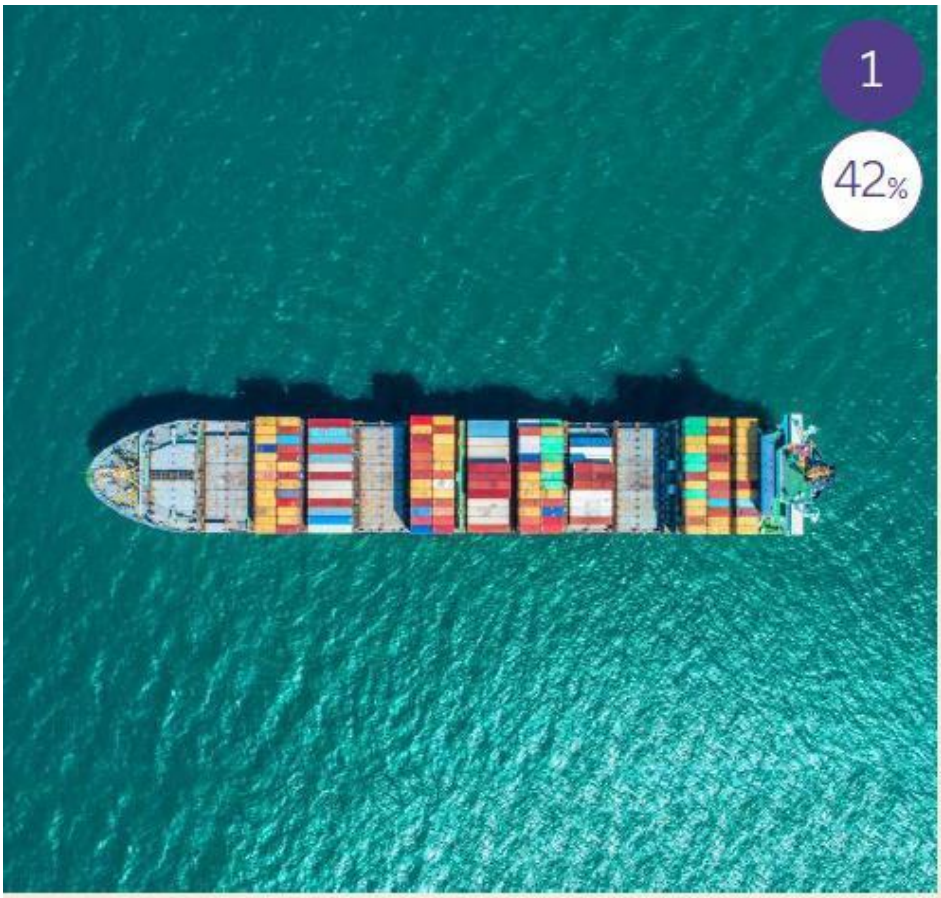


このリスク地図は、各国の3大ビジネスリスクを示しています。
出典：Allianz Global Corporate & Specialty

↘国別、地域別、産業別リスクのデータはこちら



目次



出典：Allianz Global Corporate & Specialty
数字は、回答者が選択したリスクの数が調査の全回答数（2,376件）に占める割合として表したもの。1,911 人の回答者は、最大 2 つの業界について、業界あたり最大 3 つのリスクを回答することができる。

↘リスクバロメーター2018 年ランキングの全容はこちら

(=) 2017: 37% (1)

事業中断
（サプライチェーンの混乱を含む）

(▲) 2017: 30% (3)

サイバーインシデント
（サイバー犯罪、IT 障害、データ侵害等）

凡例
- (▲) 2017年よりもリスクが高い
- (▼) 2017年よりもリスクが低い
- (=) 2017 年から変化なし
- (1) 2017 年のリスクランキング

(▲) 2017: 16% (7)

火災・爆発

(▲) 2017: 12% (10)

新技術
（拡大する相互接続の影響、ナノテクノロジー、人工知能、3D 印刷、ドローン等）

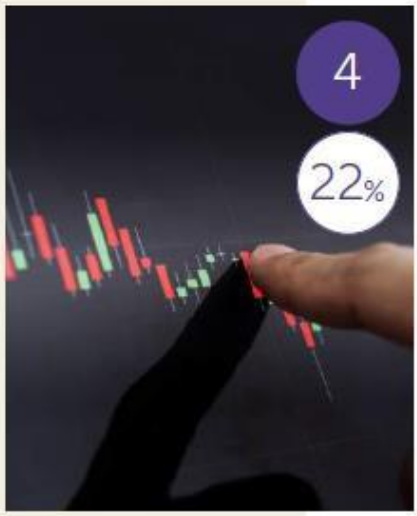
アリアンツ・リスクバロメーター

2018年グローバル・ビジネスリスク トップ10

2017: 24% (4)

自然災害

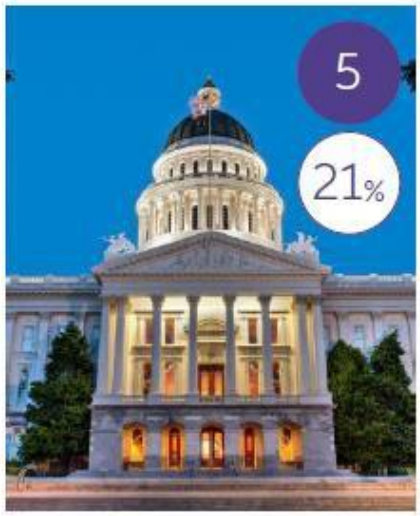
（暴風、洪水、地震等）



2017: 31% (2)

市場動向

（ 不安定性、競争激化／ 新規参入者、M&A、市場停滞、市場変動）



2017: 24% (5)

法規制変化

（政権交代、経済制裁、保護主義、Brexit、ユーロ圏の分裂等）

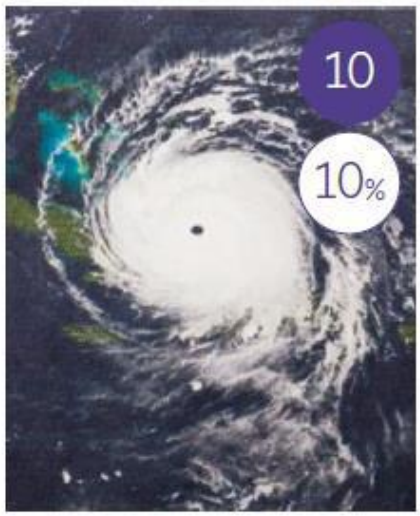
2017: 13% (9)

レピュテーション・ブランド価値喪失

2017: 14% (8)

政治的リスク・暴力

（戦争、テロ、社会的混乱等）



NEW

気候変動／増加する異常気象

エクゼクティブ・サマリー

80ヶ国のリスクマネジメント専門家1,911人の見識に基づくアリアンツ・リスクバロメーター2018によれば、企業にとって2018年以降最大の脅威となるのは事業中断とサイバーインシデントの複合リスクである。

事業中断は、収益に与える影響が甚大であることから、6年連続で最も重視されるグローバルリスクのトップ（回答の42%）にランクされている。自然災害や火災によって施設やサプライチェーンが被る物理的な影響といった従来的なリスクから、物理的な被害をあまり伴うことがないデジタル化や相互接続から派生し、大きな経済的な損失を引き起こすこれまでにないトリガーに至るまで、企業はますます多くのシナリオに直面している。また今回の調査で初めて、サイバーインシデントが最も懸念される事業中断のトリガーとして挙げられている。事業中断はまた、サイバーインシデント後に起こる経済的損失の最大の原因でもある。サイバーに端を発する事業中断インシデントは増加しており、その原因としてはもちろんランサムウェアなどのハッカー攻撃もあるが、それよりも頻度が高いのは技術的障害や従業員の人為的ミスを原因とするケースである。↘8ページ>>

サイバーインシデントは、今年も引き続き上昇傾向が見られ、2番目に重視されるビジネスリスクとなっている（40%）。5年前のサイバーインシデントのランキングは15位であった。自然災害と同様、いったん攻撃を受ければ何百という企業に影響が拡大する可能性をはらんでおり、件数そのものも増加している。ハッカーが、共通の依存関係にあるインターネットを利用して多くの企業に混乱をもたらす、いわゆる「サイバーハリケーン」も増加している。その一方で、ヨーロッパではEU一般データ保護規則（GDPR）が2018年5月に導入されることから、当該規則を遵守しない企業に対する罰則金の種類や金額が増えていく可能性がある。データ不正への企業の対応方法は、最終的なコストに直接的に影響するものであるが、GDPRの下ではこの傾向がさらに強まることになる。サイバーインシデントへの不適切な対応は、レピュテーションの毀損と決定的にリンクしている。↘10ページ>>。また、中小企業（SME）でもサイバーリスクに対する意識が急速に高まってきている。↘16ページ>>。

自然災害による支払保険金は、2017年に1,350億ドルという記録的な水準に達し、自然災害リスクが2018年のビジネスリスクの第3位に上がった（30%で3位）。この動向は、今後さらに**気候変動**の激しさや頻度が増していく前触れではないかと企業は懸念しており、これにより気候変動が新たにトップ10に登場することとなった（10%で10位）。また、沿岸部の急速な都市化により潜在的な損失がさらに大きくなってきている。↘12ページ>>。

1 Munich Re NatCatSERVICE

それに対して、**市場動向**を懸念する企業の割合は12ヶ月前と比較して減ってきている（22%で4位）。また、保護主義的な施策が減ってきているにもかかわらず、**法規制変化**によるリスクの受け取り方に変化はない（21%で5位）。**火災・爆発**に対する懸念は増加しており（20%で6位）、クレーム分析によれば大規模な火災事故による事業中断ロスの総額は 200万ドル（170万ユーロ）に達する。また、数分のうちに危機がグローバルに拡大する危険性のある時代にあって、**レピュテーション・ブランド価値喪失**に対する懸念も増大している（13%で8位）。さらに、テロに対する懸念は高まってはいるものの、**政治的リスク・暴力**への懸念は前年比で少なくなっている（11%で9位）。2018年には、諸々の政治的活動が全般的に高まっていく傾向にあるものと予想されている。↘14ページ>>。

前年比で大きく動いたものに**新技術**に伴うリスクがある（15%で7位）。また長期リスクとしては、密接な関係にあるサイバーインシデントに続いて新技術が2番目に挙がっている。障害や悪意のあるサイバー攻撃に対する機器の脆弱性は今後も高まっていき、基幹インフラに重大な混乱を来す可能性をはらんでいる。また、責任の所在が人から機械に移行する中で、各企業はこれまでになかった損害賠償のシナリオにも備える必要性に迫られる。

↘18ページ>>。

これまでになかった新たなリスクの登場により、潜在的な影響をマネージし、緩和するためには新たなツールが必要となってくる。保険も、中断事象に伴う収益減を補償する新たな保険カバーを提供する — 例えばサイバーインシデントによる事業中断や財物損害を伴わない事業中断（NDBI）の補償 — といったことをはじめ、データ不正や企業のレピュテーションに関わる事案発生時に、危機管理スペシャリストを提供するなど、インシデント進行中にその影響を軽減する助けとなる諸々のサービスを提供するといったことも増えてきており、その役割は日々進化を続けている。このことは、今日のリスクマネジメント環境がかつてないほど流動的にな ってきているという事実、および**アリアンツ・リスクバロメーター**に挙げるさまざまな脅威の相互関連性から来る影響を反映したものといえる。

リスクバロメーターの分析手法

第7回**アリアンツ・リスクバロメーター**は過去最大のものであり、80ヶ国の1,911人という過去最多の回答者の見識を盛り込んだものである。コーポレートリスクに関するこの年次調査は、アリアンツの顧客（世界的規模の企業）およびブローカーを対象に行ったものである。またAllianz Global Corporate & Specialtyおよびその他アリアンツグループの企業保険部門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、クレーム専任者についても対象としている。

調査は2017年10月から11月にかけて実施し、大企業から中小企業を対象としている。最大2つの産業について複数回答を可能とし、2,376の回答、6,472のリスクに関する回答が得られた。回答者には、回答者自身が特に見識の深い業種を選んでもらい、各業種について最大3つの最重要リスクを回答してもらった。

回答の大半［回答数：1,257件、53%］は大企業（年間収益 5億ユーロ超）に関するもので、中規模企業（2.5億～5億ユーロ）に関する回答は516件（22%）、小規模企業（2.5億ユーロ未満）に関する回答は603件（25%）となった。22の業種のリスク専門家が参加した。

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ではなく前年のポジションとの比較で決めている。

特に記載のない限り通貨は米国ドルで表示している。

↘地域別、国別、業種別のリスクデータ全容はこちら

2018 年:42%／2017 年:37% (1)

1 注目の上位リスク:
事業中断

これまでになかった新たな損失トリガーが次々と登場し、サイバーによる事業中断(BI)事案が増える中、「ネットワーク社会」ではBIが最大のリスクとなっている。

過去5年のリスクランキング(回答割合%とランキング)
2017年:37% (1)
2016年:38% (1)
2015年:46% (1)
2014年:43% (1)

最大リスクとした国:
- カナダ
- 中国
- フランス
- ドイツ
- 香港
- インドネシア
- イタリア
- 日本
- モロッコ
- オランダ
- 韓国
- スペイン
- スイス

最大リスクとした業種:
- 航空産業
- 食品飲料業
- 製造業(自動車製造業を含む)
- 電力・ユーティリティ
- 小売・卸業
- 運輸

企業が直面する脅威は変化しているといわれるが、調査結果は以前と変わっていない。アリアンツ・リスクバロメーターでは、6年連続で事業中断(サプライチェーンの混乱を含む)が企業にとっての最大のリスクとなっており、2018年に企業が直面する最重要リスクのトップ3位以内にこのリスクを入れた回答数は前年よりも増えて42%にのぼる。工場火災、輸送コンテナの破壊、サイバーインシデントなど原因は何であれ、事業中断は企業収益に甚大な影響を与えるが、その影響は最も測定が難しいリスクでもある。特に規模の小さい企業にとって、重大な事業中断は企業の存続を脅かす影響を及ぼす。さらに、相互接続性の高まりにより、より大きな損失の可能性も高まっている。事業中断はまた、今回のアリアンツ・リスクバロメーターの上位に挙がる他のリスクに端を発して生じる場合もある。

増え続ける事業中断シナリオ

事業中断は、自然災害による従来的な財物損害をはじめ、サプライヤーや顧客拠点における財物損害によるサプライチェーンの途絶 — 偶発的事業中断(CBI)ともいわれる — などがトリガーとなることがある。

事業中断による損失は、物理的な損害による損害額を大きく上回る場合が多い。財物保険で事業中断を伴う大口クレームの平均額は200万ドルを超えており[1]、これは直接的な財物損害のみの平均を3割以上も上回る(それぞれ240万ドルと175万ドル)。

一方、多くの物的資産を所有する形態から、無形資産やサービスから多くの価値を生み出す形態の企業が増える中で、物理的被害を伴わずに収益の損失が発生する非伝統的なリスクが事業中断のトリガーとなるケース — いわゆる財物損害を伴わない事業中断(NDBI) — も増えてきている。

「ネットワーク社会において事業中断リスクの性格が変化する中で、企業はますます多くの事業中断シナリオに直面するようになっています」と話すのはVolker Muench(Global Practice Group Leader, Property, AGCS)である。「2017年にピークを迎えた自然災害による影響など、伝統的なリスクにもこれまでと同じように対応していく必要があるとともに、データ自体がきわめて重要な資産となっている中で、デジタル化やサプライヤーの相互依存、さらには製品品質にかかわるインシデントに端を発するさまざまなトリガーをはじめ、テロ、政治的動向、ストライキなどによって市民の足が関係地域から遠のくことによる収益の減少など間接的な影響からくるこれまでになかったさまざまなトリガーへの対応も迫られています」。

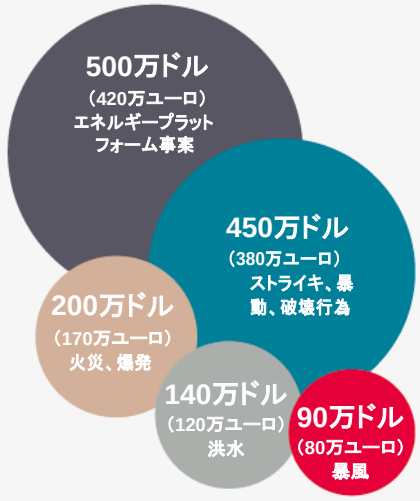
しかも脅威はこれにとどまらない。不確実性の高い今日の政治状況や事業環境においては、ビジネスモデルを揺るがすような突然の規制変更への懸念も高まってきており、規制上の承認や製品免許の取り消しも事業中断のリスクとなりえる。

企業が最も脅威に感じる事業中断の原因は?

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

出典: Allianz Global Corporate & Specialty
数字は、全回答者(845人)の回答のパーセンテージ。リスクは最大で 3 つまで選択することができることから、数字を合算しても100%とはならない。

BI のコストは？



損害の（一部の）原因別に見たBIクレーム額平均。エネルギープラットフォーム、およびストライキ、暴動、破壊行為は発生頻度は低いが損害額が大きくなる事案である。**出典:**Allianz Global Corporate & Specialty

高まるサイバーBIおよびインターネットサプライチェーンのリスク

アリアンツ・リスクバロメーター調査の開始以来はじめて、企業が最も恐れるBIトリガーとしてサイバーインシデントの影響がトップ（回答の42%）にランクされた。BIはサイバーインシデント後の経済的な損失の最大の要因でもある（回答の67%）。これは過去12ヶ月間で回答者のBIリスクの捉え方が大きく変化していることを表しているとともに、サーバーインシデントの規模が拡大している現状を反映している。2017年には**WannaCry**や**Petya**といったランサムウェアによる攻撃（*10ページ参照*）などにより、多くの企業やサービスが大規模な混乱や経済的損失を被っている。また、サイバーリスクの分野でAGCSと提携するアナリティクスとモデリング会社のCyence社によれば、2016年10月に起きたインターネットプロバイダーDyn社に対する大規模なサービス妨害攻撃（*10ページ参照*）も、リスクが相互につながっているという現状、さらには共通のインターネットインフラ、そしてサービスプロバイダやその技術に多くの企業が同じように依存している現状を反映したものだとしている。

ハッカーがファイルを暗号化し、そのロックを解除することと引き換えに金銭を要求するといったランサムウェアインシデントの頻度がこの1年で倍増しており、そのようなインシデントを原因としてサイバーBIが生じることはあるとはいえ、ありふれた技術的障害やヒューマンエラーを原因とするサイバーBIのほうが発生頻度は高い。例えば、2017年2月にはAmazon社のクラウド保存サービスが4時間にわたって停止し、その影響が複数のインターネットサービス、ウェブサイト、その他の事業にまで波及している。その後、この機能停止はヒューマンエラーによるものであったと報告されている[2]。Cyence社では、この結果としてAmazon社のサービスに依存していたS&P 500企業が被った損失は併せて約1.5億ドルに上ると推定している[3]。

BI は、サイバーインシデント後の損失の最大原因の一つであると Cyence 社は指摘する。例えば、クラウドサービスプロバイダーが 12 時間以上機能停止となり、北米とヨーロッパ地域の 3 業種（金融、ヘルスケア、小売）の企業のうち 50,000社がこの停止の影響を受けたとした場合、北米における損失総額は8.5 億ドル、ヨーロッパでは7 億ドルに上る可能性があると同社では推定している。

リスクの軽減、意味解析、および保険の進化

また、今年のリスクバロメーターではBIは2番目に過小評価されたリスクとなっている（11ページ参照）。

「*BI の影響は過小に評価しがちです*」と話すのは**Thomas Varney（Regional Manager Americas, Allianz Risk Consulting, AGCS）**である。「*リスクの中には非常に複雑なものもあります。実際のリスクの把握や損失の計算ばかりでなく、サプライチェーンのどの箇所で実際に混乱が生じたかを把握することすら難しい場合が往々にしてあります*」。

「*企業が『事業復旧』の複雑さを過小評価する場合も多く、特に代替サプライヤーに関係する緊急対応プランには問題があるケースが見られます*」とMuenchは話す。「*その他の良い例としてサイバーリスクがあります。自社ITを復旧するためのサイバー攻撃後のIT継続計画を定めているからといって、これでBIの脅威に適切に対応できているでしょうか？サイバー攻撃の影響で、サプライヤーの一社が製品やサービスを納入できなくなった場合の影響は？*」

それでも、リスクを軽減することはできます。「*これまでになかったBI環境に対応すべく、企業は自社の緊急対応プランを継続的に微調整し、あらゆるシナリオに対応する計画を立案し、リスクを予測検出する仕組みを全部門共通で戦略的に築き上げる必要があります*」とMuenchは話す。

AGCSなどの保険会社では、事案発生を原因とする収益の減少を補償するサイバーBI保険やNDBI保険などの新たな保険ソリューションを通じて、企業にさらなるサポートを提供することができます。AGCSではまた、企業のサプライチェーンリスクをよりよく理解するために、意味解析ツールを活用します。これによりサプライヤー同士の関係を四次サプライヤーまでマッピングすることが可能で、固有のリスクと累積リスク特定がしやすくなります。

「*これまでになかったNDBIトリガーが登場してきていることを理解することが重要です*」とVarneyは話す。「*今日の脅威については理解しているかも知れませんが、明日の脅威はどうでしょうか？事業の進化とともに変化を続ける諸々の影響に遅れをとらないようにするためには継続的な注意が必要です。新たに導入した設備、実施したM&A、そして異なるサプライヤーの起用などといった要素は、事業の成長とともに絶えず変化していくものなので、企業はこれらを理解していなくてはなりません*」。

1 Allianz Global Corporate & Specialty、グローバルクレームレビュー：事業中断に注目
2 「インターネットをまひさせたAmazonの機能停止はタイプミスが原因」The Guardian紙、2017年3月3日
3 サイバーリスクの進化：システムリスクの定量化、Cyence, MMC サイバーハンドブック 2018、George Ng、Philip Rosace

2018 年:40%／2017 年:30% (3)

2 注目の上位リスク:
サイバーインシデント

「サイバーハリケーン」などの新たな脅威、レピュテーショナルリスクの高まり、データ関連規制の強化により企業やリスク専門家の懸念がこれまで以上に高まっている。

過去5年のリスクランキング(回答割合%とランキング)
2017年:30% (3)
2016年:28% (3)
2015年:17% (5)
2014年:12% (8)

最大リスクとした国:
- オーストラリア
- オーストリア
- ベルギー
- ブラジル
- インド
- インドネシア
- オランダ
- シンガポール
- 南アフリカ
- 英国
- 米国

最大リスクとした業種:
- エンタテイメント／メディア
- 金融サービス
- 専門業
- 技術
- 電気通信

重要なワクチンの生産に障害が生じ、薬品不足の懸念が高まる。世界最大規模の「スマート」港が機能停止となり、コンテナが立ち往生。2017年6月に発生した**Petya**ランサムウェア攻撃によって起こった上述の出来事は、絶えず進化を続けるサイバーの脅威、そしてそれが最終損益に与える影響に対して企業があまりにも脆弱であることを露呈したものである。ワクチンの件では支払保険金で2.75億ドル[1]、港湾ターミナルの件による海運会社他の損害額は推定3億ドル[2]となっている。その1ヶ月前に発生した**WannaCry**攻撃による経済的損失は最終的には80億ドルに達する可能性もあると推定するのはCyence Risk Analytics社である。自然災害と同じように、たった一件のサイバー攻撃により数百もの企業が影響を受けることがあり、これにより重大な事業中断が生じたり、顧客や評判の喪失を招くこともある。よって、サイバーインシデントが2018年の時点で**アリアンツ・リスクバロメーター**を6年連続で上昇し続けていることも驚きではない。サイバーリスクは現在11の国でトップのリスクとなっている。

いくつもの脅威が過小評価されている

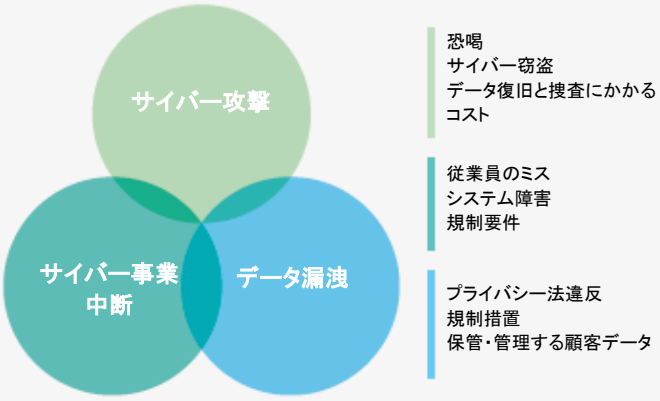
「*どの会社も例外なく、過去にサイバーリスクの影響を受けたことがあるか、今後受けることになります。これは誇張ではありません。どちらかといえば、その脅威があまりよく理解されていないがために過小に評価されているというのが現状です*」と話し、リスクバロメーター回答者の50%以上は、企業が最も過小評価するリスクとしてサイバーリスクを挙げていると指摘するのは **Emy Donavan(Global Head of Cyber at AGCS)**である。「*現在、企業のデジタル領域には複数のサイバーリスクが存在します*」。

個人情報や知的財産の流出の可能性があるばかりでなく、取引先などに破損したファイルを送信すればネットワークにかかわる賠償責任を問われる場合もある。また、サイバー恐喝、特に事業中断(BI)(9ページ)など、これまでになかった脅威に対して回答者はますます懸念を高めている。一方で、2018年1月にはコンピュータチップにセキュリティー上重大な2つの欠陥 — MeltdownとSpectre — が存在することが発見されたことにより、世界中のコンピューターや情報端末からハッカーなどによりデータが盗み取られる可能性があるとの恐れが高まったが、今後もサイバー相互接続性から予期し得なかった脅威が出現する可能性が示された。

2018年にはさらに大規模なインフラ攻撃が

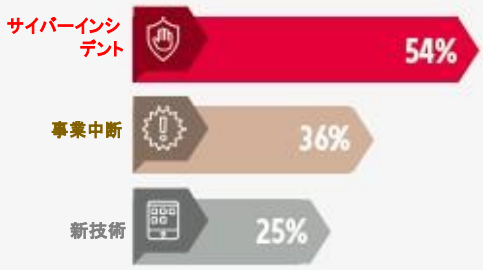
また、企業はサイバー攻撃がさらに高度化していることに懸念を抱いている。各種の重要インフラでインシデントが発生する中で、2017年12月には、初めて工業プラントの安全システムがハッカーによって侵入されたという報告があった[3]。一方、WannaCry やPetyaをはじめ、Twitter、CNN、Netflixに混乱をもたらしたインターネットプロバイダーDynへの**Mirai**による攻撃 — 大規模な分散型サービス妨害(DDoS)攻撃 — などは、より広範な累積事象、つまり「サイバーハリケーン」などの拡大傾向の表れである。さらに、ハッカーがインフラに対する共通の依存関係を利用して、より多くの企業に混乱をもたらすといったことも起こりえる。この傾向は2018年も続いていく可能性が高い。

デジタルの危険性:サイバー攻撃ばかりではない
企業のデジタル領域はいくつもの脅威にさらされている。



出典: Allianz Global Corporate & Specialty

現在最も過小評価されているビジネスリスクは？



出典: Allianz Global Corporate & Specialty
数字は、回答をした全参加者(902)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 つまで選択することができることから、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後の経済的損失の主な原因は？

出典: Allianz Global Corporate & Specialty.
数字は、回答をした全参加者(902)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 つまで選択することができることから、数字を合算しても 100%とはならない。

*「BIのような中核的サイバーリスクの防止を考えるとき、注意を要する脅威は企業の規模や業種によって異なります」*とDonavanは話す。*「小規模企業はランサムウェア攻撃で活動がまひしてしまう可能性が高い一方で、それよりも規模の大きい企業ではDDoSをはじめ、システムを圧倒してしまうようなより広範な脅威にさらされています。サイバー事案を完全に防ぐことは不可能ですが、発生してしまったものに関しては、被害の程度を大幅に軽減するためのアプローチは数多く存在します」*。

ランサムウェアに対する防御として最も有効な手段は、隔離されたバックアップを定期的に、有効かつセキュアなかたちで実施することだとDonavanはいう。ユーザー毎のアクセス権の設定も有効な手段である。DDoS攻撃に対処する場合は、システムの冗長性を確保し、バックアップサーバを構築することが不可欠だ。

レピュテーションが危険にさらされる

サイバーインシデントはハッカーによるものばかりとは限らない。技術的な障害や、従業員の悪意や無知から来る行動が原因であることが多い。原因は何であれ、サイバーインシデントとレピュテーションの毀損は決定的にリンクしている。レピュテーションの解析と調査を専門とするMediaTenor社によれば、サイバー攻撃を受けた企業の75%がレピュテーションへの損害や喪失を被っている。エンタテイメント、銀行、小売業は機密データを取り扱うことから特に被害を受けやすい。さらに、メディアによるネガティブ報道がなくてもレピュテーションに損害が及ぶ場合がある。機密性の高いデータが漏洩すれば、メディアの関与がなくても重要なステークホルダーからの信頼が失われることがある。

サービスとしてのサイバー保険

相互接続が増えてきているということは、企業がサイバーセキュリティーと事後の復元力について検討し、サイバー保険をリスクマネジメントの一環として考えることの重要性がかつてないほど高まっていることを意味する。サイバー脅威の進化に伴って、サイバー保険の提案内容も単にBIや復旧コストを補償するといったものから進化してきている。例えば、企業でデータ漏洩があった場合、専門の弁護士、ITフォレンジック要員、危機管理コンサルタントをただちに動員し、そのインシデントの進行中に影響を軽減していく必要があるが、これらを保険でカバーしていくことができる。

*「見て見ぬふりはできません。対応が早ければ早いほど好ましい結果となります。サイバーインシデントへの対応が不十分な企業は、良い対応をした企業と比較して株価への長期的な影響が大きくなります」*とDonavanはいう。

1 「Merckへのサイバー攻撃による保険会社のコストは2.75億ドルに上るか」Reuters、2017年10月19日
2 「Moller-Maerskがサイバー攻撃のコストを最大3億ドルと試算」Financial Times、2017年8月16日
3 「サイバー攻撃でプラントの操業が停止したことは重大な転機」Reuters、2017年12月14日
4 「企業がレピュテーションを守り、成長させるためのお手伝いをすることでリスクマネジマントを強化」
MediaTenor

GDPR(EU一般データ保護規則):2018年サイバーリスク問題で最大の出来事

2017年の暮れにEquifaxとUberで大規模なデータ漏洩が発生し、2億人以上の情報が流出した可能性が指摘される中、データ保護セキュリティーが再び注目を集めている。2018年5月にヨーロッパで導入される**General Data Protection Regulation (GDPR)**で今以上に監視が強められることになる。GDPRでは、データ漏洩の発生を規制当局とデータ所有者に通知することを義務づけるなど、現在よりも厳格な手順が求められ、EUで事業を行う企業でこれに適合しない者に対する罰則も大幅に強化されることになる。罰則金は最大でグローバル収益の4%にも達し、罰則金の種類と額についても今後さらに増えていくものと予想される。また、これに対して企業がセキュリティーを強化していく中で、サイバー保険の需要も高まるものと予想される。

*「すでに厳格な法律が敷かれる米国と比較して、ヨーロッパ企業のプライバシーリスクに対する意識はさほど高まっていませんでしたが、今後は今まで以上に厳しい賠償責任と報告義務を負うことになります」*と話すのは**Emy Donavan(Global Head of Cyber at AGCS)**。*「自分の会社にも潜在的な脆弱性が存在するという現実に多くの企業が気付き始めていて、いったんGDPRが実施されれば、プライバシー問題は現実としてコストを伴うものだという認識が比較的短期間のうちに高まっていくでしょう。データ漏洩に対して十分に準備をすることは、レピュテーションへの影響を和らげるとともに、事業中断を減らすことにも役立ちます。漏洩に対する企業などの対処方法が、コストに直接影響するということは過去の経験から分かっています。GDPRの下ではこの傾向はさらに強まっていくでしょう」*。

2018 年:30%／2017 年:24% (4)

3 注目の上位リスク:
自然災害

自然災害の増加から生じる疑問:この異常気象が新しく「ニューノーマル」となっていくのか？アリアンツ・リスクバロメーターの回答者は懸念しつつ「そうである」と回答し、そして損害がさらに増大することを懸念。

過去5年のリスクランキング（回答割合%とランキング）
2017年:24% (4)
2016年:24% (4)
2015年:30% (2)
2014年:33% (2)

最大リスクとした業種:

- エンエンジニアリング、建設
- エンタテイメント／メディア
- 海事・海運業
- 石油・ガス
- 再生可能エネルギー

自然災害による総損害額は約3,300億ドルに上る。支払保険金は約1,350億ドルに達し [1]、そのうち少なくとも900億ドルは9月に大災害をもたらしカテゴリー4以上の3つのハリケーン — **Harvey, Irma, Maria（HIM）** — によるものだった。9月のハリケーン活動はそれまでの記録を塗り替え [2]、2017年は損害額として記録的な年となった。同じく9月にはメキシコで地震が発生しており、その損害額は20億ドルを超えている。さらに10月末までの山火事による支払保険金はカリフォルニア州だけで100億ドル近くに達した [3]。2017年は、どこを見ても目を見張るような自然災害関連の数字が容易に見つけられる年となった。しかも、数字はさらに酷くなることも考えられる。ハリケーンHarveyによるヒューストン市の洪水被害から、ハリケーンMariaによるプエルトリコの記録的な停電による事業中断（BI）に至るまで、HIMの影響が実に広範及んだことから最終的な損害額が判明するまでには相当の時間がかかることが考えられる。

このような被害は米州に限ったものではない。バングラデシュ、中国、スリランカ、ペルー、ジンバブエで深刻な洪水被害が発生している。コロンビアやシエラレオンの土砂崩れでは多数の死者が発生し、イベリア半島では激しい山火事が猛威をふるい、地中海全域とアフリカの一部、そしてオーストラリアでは干ばつ状態が何年も続いている。オーストラリアではまた、3月にサイクロンDebbieが襲来し、フィリピンではクリスマスの日に熱帯暴風雨Tembin による洪水や土砂崩れが起きている。自然災害が、少なくとも保険という尺度で見て比較的身を潜めていたともいえるここ数年で企業などが無関心になっていたとしても、2017年は警鐘の年となり、自然災害が2018年リスクバロメーターでは3位の位置にランクインしている。

*「最近の出来事は、自然災害が社会と経済の両面においてきわめて大きな影響をもたらす場合があることを私たちに思い出させるものでした」*と話すのは **Ali Shahkarami（Head of Catastrophe Risk Research, AGCS）**である。*「あらゆる業種でますます合理化が進み、グローバルに繋がるようになってくると、自然災害が、例えば事業中断やシェアの縮小など、あらゆるリスクのトリガーとなったり、それを助長する場合があることがますますはっきりとしてきます。リスクバロメーターで継続的に自然災害に注目が集まっているということは、間違いなく現状を反映していることを示しています」。*

「自然災害の影響は、被災地域の建造物への物理的な被害をはるかに超えるものです。被害を直接受けた地域の通常の社会生活や産業活動に混乱を来し、一見影響を受けていないと思われるようなあらゆる産業にまで影響を及ぼします」。

気候変動と急速な都市化

回答者は、自然災害の年となった2017年はこの先を占う前触れではないかと憂慮しており、気候変動の影響により自然災害の激しさが今後も高まっていくのではないかと考えている。調査によれば、気象関連災害は2000年以降46%増加しており、そのうち797の災害は2016年中に発生し、損害額は1,290億ドルに上る [4]。**気候変動／増加する異常気象**（10位）は2018年の10大リスクに新たに登場したもので（15ページ参照）、多くの研究者が気候や気象パターンによる潜在的な影響は、世界全域に見て主に3通りに分類されるとしている:暴風の激化、豪雨による洪水、そして激しさを増す干ばつである。再保険会社のMunich Reでは、統計的に有意なかたちで関連づけることはできないとしながらも、2017年のハリケーン・シーズンには気候変動の影響があったのではないかとしている [5]。同社ではまた、2017年が「今後の序章」のようにも思えるとし、激しい暴風雨の数が増えるという将来予測が、2004年、2005年、そして昨年のような異常な年が頻度を増していくというかたちで現実のものとなるかもしれないと警鐘を鳴らす。

1 「自然災害レビュー2017」Munich Re NatCatSERVICE
2 「大西洋ハリケーン・シーズン総括:決して忘れることのできない17の瞬間」The Weather Channel、2017年11月28日
3 「10月の山火事クレーム額が州全体で94億ドルを超える」カリフォルニア保険局
4 「健康と気候変動に関するランセット・カウントダウン」
5 「2017 年ハリケーン・シーズン:きわめて激しい嵐のクラスター」Munich Re

被害が大きかった自然災害
1992~2017 年(総損害額と支払保険金)

総損害額(US$)
支払保険金(US$)

出典: Munich Re NatCatService。画像:Allianz Global Corporate & Specialty。
データは 2016 年 3 月時点のもの。ただしハリケーン Harvey、Irma、Maria に関するデータは 2018 年1月4日時点。
損害発生の場所は参考用のみ。

自然災害への準備体制の改善に向けた5つのステップ

自然災害リスクのマネジメントに関する手順がなかったり、レビューが実施されていない場合、損害の規模が大幅に増大することがある:

1. 緊急準備体制プランのテストを実施し、更新する。
2. 洪水、暴風、高潮など、どのような事象に備えるのか。さらに、それによるリスクの度合いを判定する。
3. 事業継続プランのレビューを行い、更新する。
4. 保険契約を理解する。担保内容に抜けがあれば、それを是正する。
5. 事象への影響を最小限に留めるために、サイトなどを予め改善する。

↘暴風チェックリスト
↘洪水チェックリスト
↘地震チェックリスト

将来的な自然災害による潜在的な損害は、急速な都市化、都市化に十分に見合っていないインフラ開発、そして相互接続性の高まりなどを原因とする偶発的事業中断(CBI)により、さらに増幅されることとなる。例えば、米国では過去10年の間に人口増加と商業物件の開発が大幅に増えている。モデラーであるAIR Worldwide社では、米国の沿岸地域でリスクにさらされる住宅や商業物件の保険価額は、3年で15%増の13兆ドル[6]を超えていると推計している。

*「危険にさらされる市民や開発が、特に米国の沿岸地域では増えてきています」*と話すのは**Andrew Higgins(Technical Manager, Americas, Allianz Risk Consulting, AGCS)**である。*「沿岸部地域を守るためには、十分な都市計画法の導入をはじめ、熱帯性降雨が適切に排水されるようにコンクリートを減らして緑地を増やし、抑えの利かない過剰開発を抑制していく必要があります。ハリケーンHarveyを例にとると、記録的豪雨(154cm／60.6インチ)[7]が降ったテキサス州ネダーランドの半分の降雨量しかなかったヒューストン市の一部地域で、重大な洪水被害が発生したという事例があります。その違いは過剰な開発でした」。*

急激に変化するリスクの集中に対応するための新たなツール

急激に変化するリスクの集中に対応するために、AGCSなどの保険会社では多くの新しい大規模自然災害マネジメントツールや、保険ソリューションを活用し、2017年の災害時に暴風の監視、損害の評価を実施している。具体例として、リスクをより素早く、より正確に評価するためのドローン技術 — 屋外での屋根被害の評価、近接不能地区での利用をはじめ、水害を評価するために大規模施設の屋内で活用 — 衛星技術、3D撮像などの技術がある。

*「私たちは現在、重要な意思決定の大きな助けになるものとして、最先端のデータ解析ツールや地理情報システム(GIS)に、衛星撮像、ビッグデータ、機械学習技術を融合した先進的なソリューションを複数用意しています」*とShahkaramiは説明する。*「例えば、これにより山火事の直後に被災地域の空撮画像を見ることができ、施設などの被害の程度を評価したり、暴風雨後の洪水被害の程度や建物屋上部の被害を推定することができるようになります。技術的に見れば非常に刺激的な時代で、お客様のために利用可能なあらゆるツールを活用していくことに私たちは意欲を感じています」。*

1,100 件以上

4 件の事案 — ハリケーン 3 件と山火事 1 件 — で AGCS が 60 日間で取り扱ったクレーム数

6 「リスクにさらされる沿岸部:米国沿岸部物件の推定保険価額2016更新版」AIR Worldwide
7 「ハリケーン Harvey、テキサスで 60 インチの雨を降らし、米国の暴風雨記録を塗り替える」Washington Post 紙、2017 年 9 月 29 日

4 市場動向

22% ▼ 2017年：31% (2)

Ludovic Subran（Global Head of Macroeconomic Research at Allianz）によれば、このリスクに対する企業の懸念は、2017年が「特別な年」であった為12ヶ月前と比較して減少している。政治的、政策的な不確実性が増す中で、三大巨大経済圏（米国、ヨーロッパ、中国）はともに成長し、世界貿易が復活し、市場は金融の好調と安定性が見られた。注意を要する要素がいくつか存在するものの、この構造は今後も続くものと考えられる。好調な企業収支に伴い潤沢な資金が記録的水準に達し、デジタル革命において自社株買いの増加等の有機的な成長の可能性に対して疑問符が付く中、2018年には再びM&Aの波が訪れるものと考えられている。さらに、市場と政治が再び結びつくようになると、不安定性が90年代半ばの水準にまで高まる可能性もある。世界的に見て倒産件数は安定しているとはいうものの、小売、サービス、建設セクターでは増加してきている。まず、最初に混乱が生じるのはエンドユーザーに最も近い業種で、これらの業種ではすでに価格圧力がかかっている。

5 法規制変化

21% = 2017年：24% (5)

Ludovic Subran（Global Head of Macroeconomic Research at Allianz）によれば、世界各国で2017年に新たに実施された保護主義的施策は例年の半数の404件にとどまっているものの、新たな保護施策は主に米国が取り入れたもので、中国に影響を及ぼすものであるという意味で政治的な意図を見て取ることができることから、保護主義は企業の懸念材料の一つとして挙がっている。2018年はまた、世界がきわめて分断された状況が続くこととなる。米国が口火を切った関税戦争、金融や規制に関係する地域間の不均衡、通貨の政治問題化などが資金の流れを脅かし、経済、金融の小分割化が広がる中で、グローバルな貿易協定や多国間の枠組みなどは棚上げにされている。政治的なリスクの最上位に挙がるのは、依然として原油価格の下げ止まりの中での湾岸地域の分断や、経済的不均衡が拡大するヨーロッパで引き続き見られる分離リスク、負債が過去最高水準にまで膨れあがり、財政面の修正が米国と中国で深刻なダメージをもたらいているなど、経済に関係するものである。

7 新技術

15% ▲ 2017年：12% (10)

企業のサイバーリスクの高まりの背景には過去10年の技術の進歩がある。デジタル化の普及や、バリューチェーンのあらゆる段階で行われる膨大な情報のやり取りの影響をまったく受けない業種はない。このような相互接続性は、エンドユーザーに近いほど事業の成長、コストの最適化、ビジネスモデルの柔軟性を可能にする。リアルタイムのモニタリングやデータ解析に根ざした予測的メンテナンスを拡充することで、小規模な損害の頻度を減らすことができる。しかしその一方で、相互接続性は製品やサービスの提供を不可能にしてしまうほどの重大リスクをはらんでおり、さらにはサイバー攻撃やインフラの破綻から来る大規模な損害を伴う場合もある。相互に接続する業種が、これまでになかった賠償責任のシナリオにさらされる場面が今後も増え続けると回答者は見ており、結果としてこのリスクは今後10年にわたって企業がさらされる脅威の中で2位にランクインしている（18ページ参照）。

8 レピュテーション・ブランド価値喪失

13% ▲ 2017年：13% (9)

ソーシャルメディアや相互に接続したサプライチェーンなどにより、危機的状況が瞬時にグローバルに伝播する時代にあって、健康や安全性関連のインシデント、製品リコール、データセキュリティーの侵害をはじめとする、さまざまな原因からのレピュテーション毀損リスクが爆発的に増加している。企業の価値の実に1/4（24%）はそのブランド価値にあると推定されている [1]。またレピュテーションに関係する危機状況に端を発し、1ヶ月の間に企業が株価上の企業価値の20%を失う確率が80%で、それは5年間影響が継続すると推計する調査もある [2]。企業の規模がどれほど小さくても、この影響を免れることはできない。レピュテーションを守るための備えが不十分であることが多いが、保険では、無形のリスクに対して危機管理の専門家へのアクセスや活用のためのコストなど、有形の支援を提供することができる。責任ある対応をとることの効果は大きい。効果的な危機管理を実施した企業の株価は、その翌年には10%以上上昇し、失敗した企業の株価は15%以上低下していることが調査により分かっている。

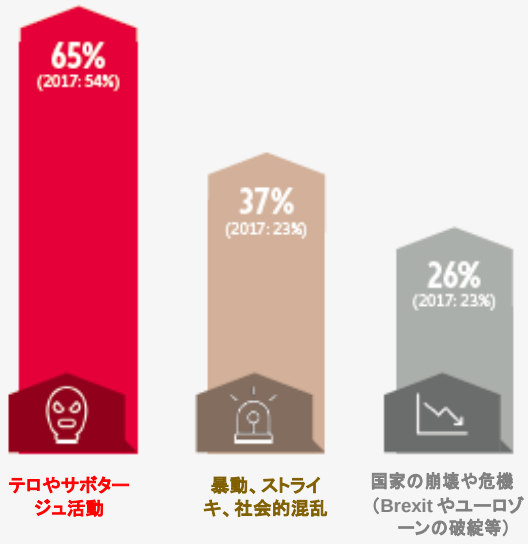
1 Brand Finance Global 500 Report 2012
2、3 Oxford Metrica/Aon Reputation Review 2012

6 火災・爆発

20% 2017年：16% (7)

AGCSが行った11,000件以上の大口保険クレームの分析によれば、全体として火災と爆発は企業が被る損害の第二の原因となっており、物理的な損害よりも事後の操業の混乱への影響のほうが大きくなることもある。過去5年の事業中断保険クレームの最大の原因は火災や爆発であり、大口事案の平均損害額は170万ユーロ（200万ドル）に上る。したがって世界各国の回答者が毎年このリスクに敏感になることは特に不思議なことではない。企業が恐れる事業中断の原因としてもサイバーリスクに続き2番目にランクインしている。リスクバロメーターに今回初めて登場したブルキナファソとトーゴの2ヶ国では、火災と爆発が企業にとっての最大の脅威としてトップに挙がっている。

「政治的リスク・暴力」の中で企業が最も懸念するリスクは？



出典：Allianz Global Corporate & Specialty
数字は、回答をした全参加者（246）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 つまで選択することができることから、数字を合算しても 100%とはならない。

9 政治的リスク・暴力

11% 2017年：14% (8)

政治的リスクと暴力に対する企業の捉え方は前年と比較してあまり変化していないが、回答者のテロへの警戒心は高まっている。また、直接的な被害者ではなくても企業が影響を受けることもある。近隣で攻撃があれば、周囲一帯が閉鎖されるなどして事業運営に支障が出る場合がある。**Christof Bentele（AGCS Global Head of Crisis Management）**は、2018年には西ヨーロッパや北米で攻撃などが増加すると見ている。薬物の使用あるいは小規模の攻撃はあるものの、英国のマンチェスターやベルギーのブリュッセルで最近起こった中東から帰国したIS戦闘員などによる爆弾事件も起こる可能性はある。標的となる可能性が高いのは、小売商業施設をはじめ、主に交通インフラや多くの人が集まる場所である。世界的に見ると、全般的な傾向として政治的活動が高まり、それによりさらなる混乱が起こるものと予想される。

10 気候変動／増加する異常気象

10% 2017年：6% (14)

2017年の自然災害による支払保険金は1,350億ドル[4]に達し、史上最も大きい年となり、保険の尺度で見て比較的損害が少なかった過去数年の傾向に終止符を打つかたちとなった。また、気象事案の発生頻度とその激しさは全体としては高まってきていると考える者も多い。調査によれば[5]、2000年から2016年にかけて気象災害が46%増加し、2016年には「異常な」気象災害が797件記録されている。気候変動と気象災害との間に直接的な相関を見出すことは容易ではない。記録的な損害が生じた背景には急激な都市化など、他の要素も関係しているが、リスクバロメーター回答者の間で気候変動の影響に対する懸念が高まっていることは確かで、調査開始以来、初めて11の国でトップ10にランクインされている。気象災害による企業への損害が重大なものにとどまるのか、それとも壊滅的なものになってしまうかの分かれ目は、十分な準備とリスク軽減策を講じているかどうかにかかってくる場合がある。

4 「自然災害レビュー2017」Munich Re NatCatSERVICE
5 「健康と気候変動に関するランセット・カウントダウン」

中小規模企業のリスク

データ漏洩やフィッシング攻撃による潜在的な影響が実感を持って捉えられる中、中小規模企業におけるサイバーリスクへの認識が急激に高まっている。また、対抗策を講じるには大企業とは異なるさまざまな課題が存在する。

リスクバロメーターの回答のうち、中小規模企業（SME）の専門家からのものが半数近くを占めている（47%）。中規模企業（年間収益2.5～5億ユーロ）では、サイバーインシデントが初めてトップのリスクとなっており（回答の39%）、小規模企業（年間収益2.5億ユーロ未満）では、2番目に重要なビジネスリスクにランクインしている（回答の39%）。

*「サイバーインシデントの昨年順位からのジャンプアップ ― 中規模企業では3位から1位、小規模企業では6位から2位 ― は注目すべき現象で、データ漏洩に対する関心がSME企業とその保険ブローカーの間で高まっていることを反映しています」*と話すのは**Vinko Markovina（Global Head of MidCorp, AGCS）**である。

「リスクバロメーターの結果が示すとおり、意識は高まっていますが、自社がさらされるリスクを過小に評価していたり、インシデントに対する備えをしていない、もしくは対応することができないというSMEは依然として少なくありません。このようなことは致命的な間違いとなることもあります」。

数多くのサイバーインシデントが発生し、それらが報道されることにより、SME企業もその経済的な影響に関するデータを入手できるようになってきている。そしてこのようなインシデントにより壊滅的な打撃が生じることもある。北米のSME のデータ漏洩に起因する平均被害コストは、2017年に11万7千ドルだった[1]とする調査があり、また別の調査によれば小規模企業の50%がハッカー攻撃による漏洩被害を受けている。この両方の数字とも前年比で増えてきている[2]。

↘企業規模別のリスクランキングはこちら

↘16 の業種別のリスクランキングはこちら

小規模企業の 5 大リスク（年間収益2.5 億ユーロ未満）

ランク		パーセント	2017 年のランク	動向
1	**事業中断（サプライチェーンの混乱を含む）**	**33%**	2 (27%)	▲
2	サイバーインシデント（サイバー犯罪、IT 障害、データ侵害等）	**30%**	6 (22%)	▲
3	自然災害（暴風、洪水、地震等）	**28%**	4 (25%)	▲
4	市場動向（不安定性、競争激化／新規参入者、M&A、市場停 滞、市場変動）	**27%**	1 (32%)	▼
5	法規制変化（政権交代、経済制裁、保護主義、Brexit、ユーロ圏の分裂等）	**22%**	3 (26%)	▼

出典: Allianz Global Corporate & Specialty
数字は、各リスクが選択された頻度をその企業規模の全回答数のパーセンテージとして表したもの。回答数:603
リスクは最大で 3 つまで選択することができることから、数字を合算しても 100%とはならない。

事業中断（BI）は、小規模企業では前年の2位（回答の27%）から上昇して最大のリスク（33%）となった。一方、中規模企業ではサイバーインシデントがトップに上がり、事業中断は2位となっている。

*「脅威が増え続け、その影響を過小評価することはできないことから、SME のリスクランキングで BI が上位に挙がっていることは驚くことではありません」*と話すのは **Vinko Markovina（Global Head of MidCorp, AGCS）**である。*「SME に影響する BI リスクのうちサプライチェーンの混乱は一つの要因にしか過ぎません。十分な在庫を手元に持つこと、サプライヤーの地理的集中を避けること、サプライヤー同士の M&A に目を配ること、外注を要するような製品の専門化を避けることなどは、障害に備える軽減戦略としてきわめて重要になってきます。効果的なマネジメントを怠れば、波及的な影響が短時間のうちにエスカレートしてしまう場合もあります」。*

1 Kaspersky Lab
2 2017 **年中小企業サイバーセキュリティーの状況報告、**Ponemon Institute

SMEは、自社にIT部門を持つだけの収益がなかったり、絶え間なく進化を続ける脅威に対する防護策を講じるための知識やリソースを持たないなど、脅威に対して脆弱であることが少なくない。特にメールを介したフィッシング攻撃や、自社のe-コマース店舗での不正行為の被害を受けやすい。

サイバー脅威に対抗するためには、包括的な情報セキュリティー管理システムを導入する能力を持った情報セキュリティー担当責任者（CISO）を採用することが必須とされるが、これは往々にして費用負担が大きいばかりか、長い時間を要し、SMEの経済力では手が届かない場合が多い。そこでAGCSでは、シリコンバレーを拠点とするZeguro社と提携して「**バーチャルCISO**」プラットフォームを保険内容の一環として提供している。これを通じてAGCSではSMEが自社向けにカスタマイズされたセキュリティー推奨事項や従業員教育を活用できるようにし、インシデントによる経済的損失のリスクを全体的に減らす支援をしている。

*「サイバー保険は、SME規模の企業にとっては理解しづらく、比較的高額な保険であった時期も過去にありましたが、この種の保険商品の数が増え、価格が下がり、理解しやすくなるにつれて需要は高まってきています」*とMarkovinaは話す。*「2018年は、SME分野でのサイバー関連の動きが加速することはあっても、減速することはないでしょう」。*

中規模企業の 5 大リスク（年間収益 2.5 億～5 億ユーロ）

ランク		パーセント	2017 年のランク	動向
1	**サイバーインシデント（サイバー犯罪、IT 障害、データ侵害等）**	**39%**	3 (29%)	▲
2	事業中断（サプライチェーンの混乱を含む）	**37%**	1 (35%)	▼
3	自然災害（暴風、洪水、地震等）	**32%**	5 (23%)	▲
4	火災・爆発	**23%**	7 (17%)	▲
5	市場動向（不安定性、競争激化／新規参入者、M&A、市場停滞、市場変動）	**21%**	2 (33%)	▼

出典: Allianz Global Corporate & Specialty
数字は、各リスクが選択された頻度をその企業規模の全回答数のパーセンテージとして表したもの。回答数：516
リスクは最大で 3 つまで選択することができることから、数字を合算しても 100%とはならない。

SME にとっての 4 つの上昇リスク

自然災害
比較的静穏だった過去数年を経て、記録的な損害が生じた2017年は中小規模企業にとって警鐘の年となった。

気候変動
大規模企業（年間収益5 億ユーロ超）ではリスクのトップ10 にランクインしていないこのリスクも、小規模（7 位）と中規模企業（8 位）にとっては相対的に重要な懸念材料となっている。

政治的リスク・暴力
客足の遠退きを招くテロや社会的混乱に対する中規模企業の懸念は高まっている（10 位）。

火災・爆発
このリスクの影響は中規模企業にとって大きな懸念材料であり、リスクランキングの 4 位に挙がっている。在庫製品の破壊、生産の中断、キャッシュフローの滞りなど、その波及的影響は死活問題に発展する場合がある。

明日のリスク

技術の発展によりリスク環境は不可逆的に変化してきており、これは企業にとっては朗報でもあり、難しい問題でもある。技術革新を通じてリスク軽減の新手法が生み出される一方で、それによりこれまでになかった脅威も生み出されることから、リスクバロメーターの回答者の間ではこのことに対する懸念も高まってきている。

7

アリアンツ・リスクバロメーターの2017の10位よりランクアップ

↘自律機械に関する方針説明書はこちら

自律機械、人工知能（AI）、スマート工場、そしてデジタル化されたサプライチェーンなど、新技術の導入が企業にもたらす事業機会は膨大かつ広範である。ビルや工場、そして情報端末などの相互接続性がさらに高まり、データやアナリティクスの利用がさらに改善されるにしたがって、生産性が高まり、より高度にカスタマイズされた製品などを提供できるようになるものと期待されている。作業の自動化により、ヒューマンエラー — 多くの業種で損害の最大要因 — を減らすことができるとともに安全性も高まる。自律機械を鉱山などの危険な労働環境や危険地域、立ち入り不可能な場所で活用することで、労働災害のリスクを低減したり、災害対応や災害支援活動を強化することができる。さらに、継続的な状態監視や「ビッグデータ」解析の活用によりリスクマネジメントを改善し、リスク軽減策や防止策の改善、災害事前計画の強化、さらに事故に至らなかったニアミスからの学習能力なども実現することが可能となる。

新たな脆弱性

一方で、就業機会の喪失、戦争での使用、「**フェイクニュース**」により市民の考えに影響を及ぼす行為といった新技術への依存の高まりに関係する倫理的、社会的に重要な懸念領域以外でも、企業が直面するリスクは増え続けている。

スマート工場やデジタル化されたサプライチェーンなどを活用し、企業価値の大きな部分をデータ、ネットワーク、顧客関係、知財などの無形財産が占める、相互接続の高い産業においては、いったん不具合が生じると失うものも大きい。データプライバシーへのリスクが高まり、事業中断の危険性が積み重なる中で、故意ではないミスや新技術の利用から生じる予想外の作用などであっても、短時間のうちに顧客の信用を失ったり、レピュテーションの毀損を招く原因となることがある。

システム障害、さらにはハッキングをはじめとするサイバー恐喝やスパイ行為などの悪意による行為に対する相互接続システムの脆弱性は今後も高まっていく。ロイズとサイバーリスク解析モデリング会社であるCyence社が最近公表した報告では[1]、クラウドサービスプロバイダーが悪意のハッキングにより機能停止となった場合、推定損失額は極端な場合には500億ドルを超えることもあるとしている。

自動化によりヒューマンエラーを最小限にとどめ、それにより損害の頻度を減らすことは可能である。

1「コストを算出：サイバーリスクを解読」、Lloyd's、Cyence

今後長期的に見た場合（10年以上）、あなたが考える3大リスクは？

出典： Allianz Global Corporate & Specialty
数字は、回答をした全参加者（1,911）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 つまで選択することができることから、数字を合算しても 100%とはならない。

しかし、さらに大きな損失リスクがこれに取って代わることも考えられる。同様なプログラミングエラーやハッカー攻撃が、単一の型の複数の機械で繰り返し発生することは十分にあり得るし、ある一つの機械が誤った動作を何回も繰り返し、それにより予測を超えるかたちで損失が累積したり、明確な原因の特定が困難になってしまうこともある。

*「相互に接続した経済や社会では、重要インフラ(ITネットワーク、電力供給)を制御する自律機械のシステム誤作動により大きな影響が生じることも考えられます」*と話すのは**Michael Bruch (Head of Emerging Trends at AGCS)**である。*「また、ヒューマンエラーははたして本当に減るのでしょうか？それとも、単にヒューマンエラーが、操作要員や運転者などからメーカー側のアルゴリズムプログラマーやデータアナリストにシフトするといった変化にとどまるのでしょうか」？*

新たな賠償責任のシナリオと製品リスクの増大

責任の所在がこのように人から機械へとシフトし、結果としてメーカーやサプライヤーへとシフトしていった場合、企業は新たな賠償責任のシナリオに直面することになり、賠償責任の所在特定や保険補償がさらに難しくなっていく。デジタル製品は複雑な代物である。そのため、賠償責任は3Dプリンティングをはじめとする製品の欠陥から生じる場合もあれば、問題の原因が利用者のミスと特定される場合もある。また、機械同士、機械とセンサー、または機械とインフラとの通信エラーが原因となる場合もある。

サイバーセキュリティーの脆弱性であれ、未検証の人口知能やナノテクノロジー、さらにはバイオテクノロジーであれ、製品リコールの要因としてテクノロジーは今後さらに大きな位置を占めるようになる。

*「すでに自動車やカメラといった分野では、サイバーセキュリティーの脆弱性に起因するリコールが発生しているにもかかわらず、サイバーリスクは現在過小に評価されています」*とBruchは話す。*「新技術が関与するリコールは、今日よりも大規模かつ複雑なものになることも考えられます。運転者のいない自動車を例にとれば、連続して事故が発生するなど、その技術の基盤となる人工知能技術の安全性に疑問が生じれば、数多くのメーカーや国家を巻き込んだ、きわめて大きなリコールを引き起こす可能性すらあります」。*

また、人間と自律機械が相互に作用し合いながら共存する過渡期が今後訪れることになるが、これはリスクが高まる時期ともなるだろう。例えば、完全または部分的に自律接続性を持った自動車と、従来の自動車とが道路に共存する過渡期においては、道路安全性のブレークスルーが実現するまでの間、事故率が増加するものと予想される。


人工知能


スマート工場やデジタル化されたサプライチェーン


モノのインターネット（IoT）


自律機械

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。

ロンドン
Michael Burns
michael.burns@allianz.com
+44 203 451 3549

ニューヨーク
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

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

ミュンヘン
Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

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

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

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

詳しくは下記まで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** and

LinkedIn

www.agcs.allianz.com

Allianz Global Corporate & Specialty SE

Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany

商業登録：Munich HRB 208312

2018 年 1 月