

プレス・リリース：2023 年度 アリアンツ・リスクバロメーター：日本ではサイバーインシデント、自然災害、事業中断の脅威が今回も上位に

- ・第 12 回 アリアンツ年次調査：サイバーインシデントが 1 位に。日本におけるリスクトップ 3 として約半数の回答者が選択。
- ・自然災害（2 位）、事業中断（3 位）、気候変動（4 位）、新技術（5 位）が今回も日本の重要なビジネスリスクとしてランクイン。
- ・世界では、サイバーインシデント、事業中断、マクロ経済の動向が 2023 年のリスクのトップ 3 に。

シンガポール - 2023 年 1 月 17 日 アリアンツ・グループの企業向け保険会社 Allianz Global Corporate & Specialty (AGCS) がまとめたアリアンツ・リスクバロメーターによれば、**サイバーインシデント**（1 位、回答者の 51%が選択）は、3 年連続 1 位。続いて**自然災害**（2 位、35%）、**事業中断**（3 位、33%）、**気候変動**（4 位、30%）、**新技術**（5 位、16%）が今回も日本の重要なビジネスリスクとしてランクインしています。

12 回目となる 2023 年度 アリアンツ・リスクバロメーターでは、94 の国や地域の 2,712 人のリスクマネジメント専門家（CEO、リスク・マネジャー、ブローカー、保険専門家等）の意見を取りまとめました。

本調査では、**サイバーインシデント**および**事業中断**は、世界的に見て、企業にとって最大のリスクとして 2 年連続でランクインしています（いずれも全回答者の 34%）。インフレ、金融市場の乱高下、迫り来る不況など、**マクロ経済の動向**（前年比 10 位から 3 位に上昇）は、新型コロナウイルスとウクライナ戦争による経済的・政治的影響が収束しない中、今年のグローバル・ビジネスリスクのランキングで急上昇しています。

AGCS の CEO、Joachim Mueller は、調査結果について次のようにコメントしています。「2 年連続して、**アリアンツ・リスクバロメーター**は、高まりつつあるサイバー・リスクおよび事業中断が、企業の最大のリスクであることを示しています。同時に、企業は、インフレ、迫り来る不況、エネルギー危機が企業にとって差し迫った脅威であると認識しています。特にヨーロッパおよび米国の企業は、パンデミックの影響と、ウクライナで続く戦争による経済的・政治的影響から生じている、現在の「パーマクライシス」（長期にわたる不安定な状況）を最も心配しています。これは、すべての企業のレジリエンスが試されるストレステストです。」

さらに、「ポジティブな情報としては、保険会社として、このエリアでは多くのクライアントの間で、特に、障害に耐えられるサプライチェーンの構築、事業継続計画の改善、サイバー・コントロールの強化において継続的な改善が見られることです。近年の出来事を考えると、レジリエンス（回復力）とディリスク（リスクを小さくすること）を強化するためのアクションを取ることが、今、企業にとって重要です。」とコメントしています。

アジア太平洋におけるトップ・リスク

事業中断（1位、回答者の35%）が、過去3年間トップに位置した**サイバーインシデント**（2位、32%）を上回り、アジア太平洋のトップ・リスクです。これはあまり驚くことではなく、企業は、サプライチェーンの混乱、不安定な地政学的リスク・経済的リスク・気候リスク、また、デジタル化、脱炭素化といった長期的な変化の中で舵を取らなければなりません。不況の脅威も、2023年に起こりうる混乱の原因であり、サプライヤーの機能不全や倒産を招く可能性があり、重要なサプライヤーが1社または限られている企業にとっては特に懸念されています。[アリアンツ・トレード](#)によれば、世界の企業倒産は、2023年には19%上昇する可能性があるとのことです。

自然災害（3位、27%）、**法規制の変更**（4位、24%）、**気候変動**（5位、22%）がアジア太平洋地域のリスクトップ5にランクインしています。

日本におけるトップ・リスク



Top 10 risks in Japan

Source: Allianz Global Corporate & Specialty

Figures represent how often a risk was selected as a percentage of all responses for that country
Respondents: 57. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2022 rank	Trend
1	Cyber incidents (e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)	51%	1 (63%)	→
2	Natural catastrophes (e.g. storm, flood, earthquake, wildfire, extreme weather events)	35%	2 (46%)	→
3	Business interruption (incl. supply chain disruption)	33%	3 (33%)	→
4	Climate change (e.g. physical, operational and financial risks as a result of global warming)	30%	5 (18%)	↑
5	New technologies (e.g. risk impact of artificial intelligence, connected/autonomous vehicles, electric vehicles, nanotechnology, blockchain, 5G)	16%	7 (11%)	↑
6	Political risks and violence (e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)	12%	9 (8%)	↑
7	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)	9%	8 (10%)	↑
7	Energy crisis (e.g. supply shortage/outage, price fluctuations)	9%	NEW	↑
9	Fire, explosion	7%	NEW	↑
9	Macroeconomic developments (e.g. inflation, deflation, monetary policies, austerity programs)	7%	NEW	↑

日本において、企業は、過去3年間首位だった**サイバーインシデント**について最も懸念しています。2022年の早い時期に、日本の大手自動車メーカーが、あるサプライヤーがサイバー攻撃

を受けた翌日に全国の自社工場をすべて丸1日閉鎖しました。工場の休止は約13,000台の生産に影響を及ぼしました。

半導体の重要な部品を製造する日本の半導体会社も、サイバー攻撃を受けました。

大手各社は適切にサイバーセキュリティ対策をしていますが、政府は下請けの中小企業について懸念しています。

Allianz Cyber Center of Competenceによれば、ランサムウェア攻撃の頻度は、2023年にも上がり続けています。その一方で、データ漏洩1件あたりの平均コストは過去最高の435万ドルで、2023年に500万ドルを上回る見込みです。ウクライナにおける紛争と、さらに広範囲の地政学的緊張が、国家支援型とされる攻撃者による大規模サイバー攻撃のリスクを高めています。さらに、サイバーセキュリティ専門家の不足が深刻化しており、セキュリティの向上に関しても課題をもたらしています。

1875年の記録開始以来、最高気温を記録した日本では、異常気象が依然としてリスクとなっています。3,700万人が住む首都圏の一部で40°C近くの気温が記録され、首都圏の電力は、停電の恐れがある使用量にまで近づきました。

多くの国々の企業にとって、2023年は、**事業中断**（BI）のリスクが高まる年になりそうです。なぜなら、多くのビジネスモデルは、突然の衝撃や変化に弱く、その結果、利益や収益に影響を与えるからです。

事業混乱のリスク源は広範囲にわたります。サイバー攻撃は、企業が最も恐れるBIの原因です（回答者の45%）。2番目に重要な原因はエネルギー危機（35%）で、その次が自然災害（31%）です。日本では、急騰するエネルギーコストと猛暑により、エネルギーを多く消費する産業の中には、エネルギーをより効率的に使用したり、生産拠点を移転させたり、一時的な操業停止も検討しなくてはならないところもあります。

アリアンツ火災海上保険株式会社の元田賢代表取締役社長は、日本の調査結果について次のようにコメントしています。「多くの企業にとって、サイバー空間における脅威はかつてないほど高く、サイバー保険の保険金請求は高い水準にとどまっています。大企業は、今ではサイバー攻撃の標的にされることに慣れて、ほとんどの攻撃を撃退することができます。しかし、中堅・中小企業では、彼らの被害を過少評価しがちなケースが多くなっています。これらの企業は、自社のサイバー・コントロールを強化するために継続的に投資することが必要です。」

「事業中断は、サイバーインシデントや自然災害など、ランキング入りしている他の多くのリスクによって起こる結果であり、世界でも日本でも、企業にとって長い懸念になることでしょう。企業が、将来、リスクのつながりに対処するためのレジリエンスを築く必要が大いにあるでしょう。」とコメントしています。

世界および国別のリスク・ランキングをすべて見る

詳しくは下記にお問い合わせください。

シンガポール : Shakun Raj 電話 : +65 6395 3817 shakun.raj@allianz.com

Allianz Global Corporate & Specialty について

Allianz Global Corporate & Specialty (AGCS) は、世界有数の企業向け保険会社であり、アリアンツ・グループの重要な事業部門の一つです。当社では、9の専門分野と6つの地域拠点で、幅広い商業的リスク、企業リスク、特殊リスクに対するリスクコンサルティングサービス、損害保険ソリューション、代替的リスク移転サービスを提供します。

当社のお客様は Fortune Global 500 企業から中小企業主に至るまで、きわめて多様です。その中には、世界最大の消費者ブランド、金融機関、テクノロジー企業、世界規模の航空産業や海運業だけでなく、水上風力発電所やハリウッド映画製作会社なども含まれます。ダイナミックで多国籍化するビジネス環境において、AGCS では規模、複雑さともに最重要のリスクに対する賢明な解決策とグローバルプログラムを提供し、そして傑出したクレーム体験をお届けするという信頼を顧客から寄せていただいています。AGCS は、自社のチームで世界 30 以上の国々、またアリアンツ・グループのネットワークやパートナーを介して 200 を超える国や地域で業務を行っており、従業員数は約 4,250 人を数えます。アリアンツ・グループの最大の損害保険ユニットの 1 つとして、当社は堅固かつ安定した財務格付けに支えられており、AGCS の 2021 年の世界総保険料収益は 95 億ユーロに上ります。

詳しい情報は、弊社ウェブサイト www.agcs.allianz.com をご覧ください。

将来予想に関する記述についての注意事項

本書には、経営者の現在の見解および想定に基づいた、知られているリスクおよび知られていないリスク、ならびに不確実なことが中心の見通しや見込みといった将来予想に関する記述があります。実際の結果、実績の数字、または出来事は、このような将来予想に関する記述において明示または黙示されたものとは著しく異なる場合があります。以下のような要因における変化により、予想と異なる結果になる場合があります。(i)アリアンツの中核ビジネスおよび中核市場における一般的な経済状態および競争状態、(ii)金融市場の実績（特に市場のボラティリティ、流動性、信用事由）、(iii)一般的に、アリアンツ・グループ、他の有名企業、および金融サービス業界の悪評、規制措置または訴訟、(iv)自然災害等、保険損害事故の頻度および深刻度、ならびに損害調査等費用の動向、(v)死亡率、罹患率の水準および傾向、(vi)継続率、(vii)信用破綻の範囲、(viii)金利水準、(ix)通貨為替レート、特にユーロ/米ドル為替レート、(x)税制等、法規制変化、(xi)組織の統合および再編成を含む、およびそれらに関する買収の影響、(xii)個々のケースにおいて、現地、地域、国内および/または世界の基準で適用される一般的な競争条件。これらの変化の多くは、テロ活動によってさらに大きくなる可能性があります。

更新義務の免除

アリアンツは、法律で開示を求められる情報を除き、本書に記載のいかなる情報も、将来予想に関する記述も、更新する義務を負いません。

プライバシーに関する注意

Allianz SE は、個人情報の保護に取り組んでいます。詳しい情報は、弊社のプライバシー・ステートメントをご覧ください。