pwc

2026年 Cyber IQ調査

――デジタル分断とAIリスクに企業はどう向き合うか

目次

はじめに

米国を中心とした国際秩序、いわゆる「パクスアメリカーナ（米国による平和）」の揺らぎは、サイバー空間にも大きな影響を及ぼしています。自由で相互接続された「開かれたインターネット」はもはや自明ではなく、地政学的対立や保護主義の拡大により、データや技術は国・地域ごとに分断されつつあります。こうした変化は国際協力を弱体化させ、企業のサイバーリスクを複雑化させています。本レポートでは、国際秩序の転換を背景に進むデジタル分断の実態を整理し、日本企業が不確実性の高い環境下で備えるべきCyber IQのあり方を考察します。

世界の動向がサイバーセキュリティに及ぼす影響
地政学が変えるデジタル世界

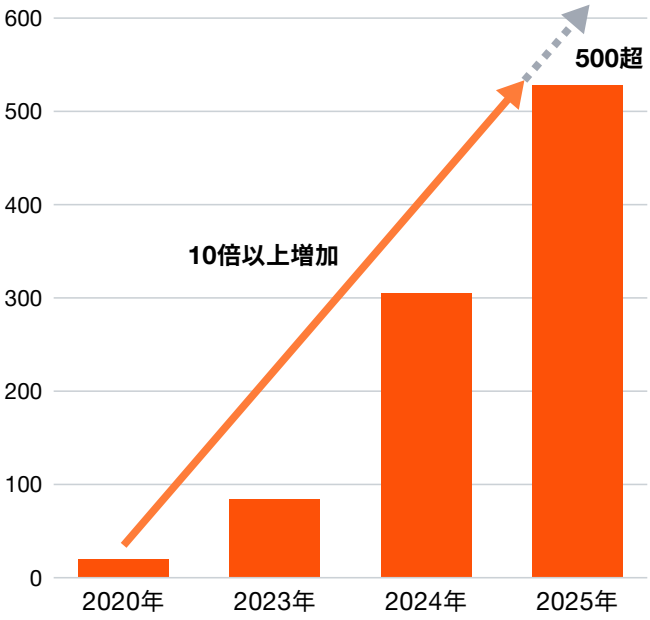
「開かれたインターネット」の終焉

世界のサイバーセキュリティを支えてきた「当たり前」は今、次々と失われつつあります。

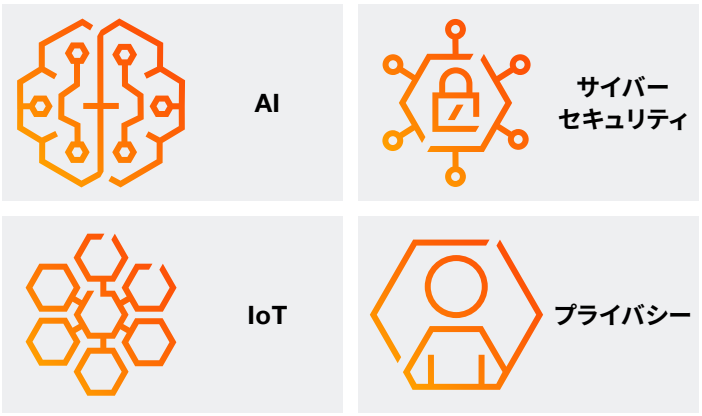
脆弱性情報を共有する国際基盤は停止の危機にひんし、国・地域間の国境を越えるデータ移転には厳しい規制が課されています。さらに、国際的な法執行協力は停滞、あるいは制約が強まり、企業が対応すべき法令・ガイドラインは2020年から2025年にかけて10倍に急増しました（図表1）。こうした変化は、企業の防御体制に重い負担を課しています。攻撃者に有利な環境が広がる中、企業は何を守り、どう備えるべきでしょうか。本章では、日本企業を取り巻く変化の実態を整理します。

図表1：海外展開する日本企業が対応すべきデジタル法規制の動向

海外展開する日本企業が対応すべき法令・ガイドライン数



主要な法令・ガイドラインのカテゴリ



- 昨今では、各国のデジタル分野における法令・ガイドラインは増加し、罰則も強化される傾向にある
- 海外展開する日本企業は準拠すべき法令・ガイドラインをタイムリーに把握・対応することが必要

出所：各国・地域の公的情報を基にPwC作成

変化する国際秩序とデジタル分断

現在、世界各国で保護主義的な政策が強まり、データや技術の流通が国・地域ごとに分断されつつあります。

関税の引き上げ、特定産業への補助金や税制優遇、安全保障を名目とした技術輸出の制限といった現実の政策動向を見れば、その兆候は明らかです。半導体や人工知能（AI）、暗号技術といった軍民両用（デュアルユース）を含む安全保障への影響が大きい領域では規制が急速に強化され、企業の上場や政府調達にも制限が及んでいます。例えば米国は、対中半導体輸出規制の強化に加え、量子コンピューティング、AI、半導体分野への対外投資を制限する規則を2025年に施行しました。EUにおいても、5G通信網からの高リスクベンダー製品の排除や、AI規制法（AI Act）による先端技術の管理強化が進んでいます。中国もまた、データセキュリティ法や反外国制裁法を整備し、半導体材料（ガリウム・ゲルマニウム）の輸出管理を強化するなど、技術・データ両面での統制を強めています。

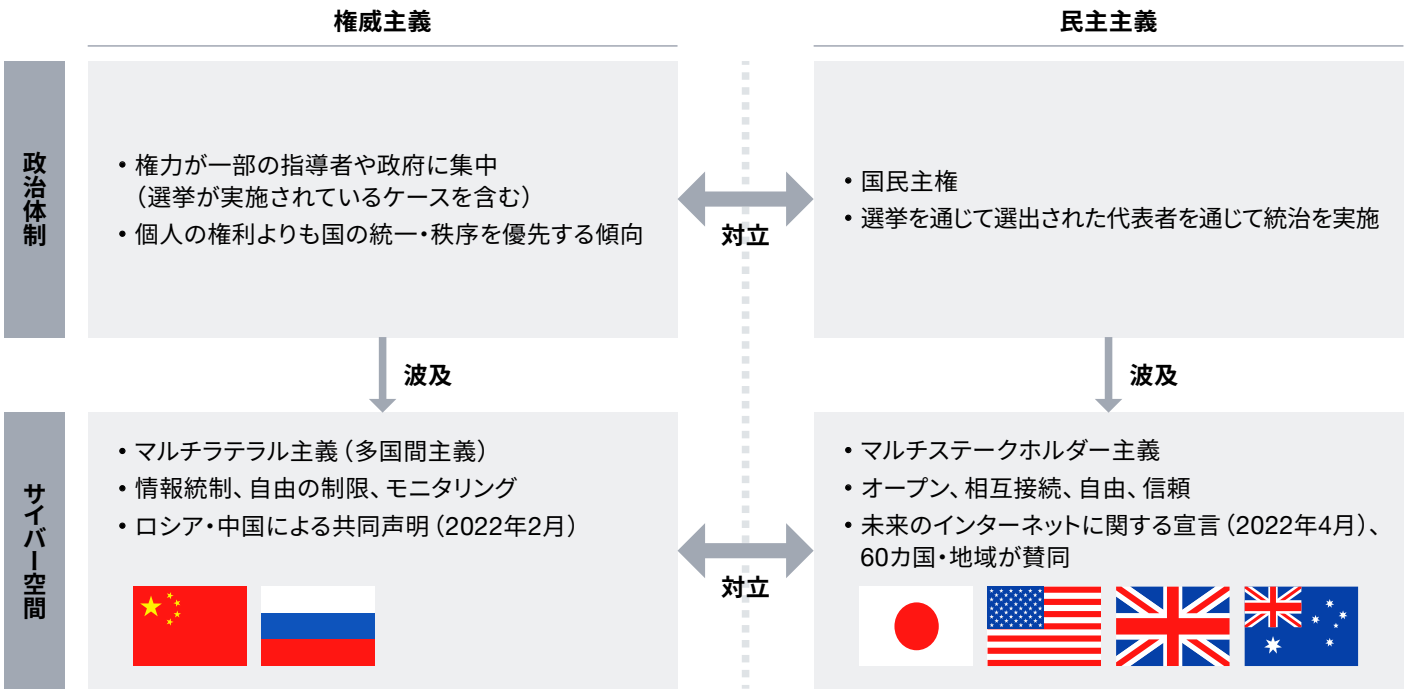
経済や政治の分野で進む保護主義の拡大は、サイバーセキュリティにも深刻な影響を及ぼしています。保護主義の具体例として、関税の引き上げ、輸出入制限、国内産品の優遇や補助金などが挙げられます。対して自由主義は、貿易障壁の撤廃やビザ緩和、人材交流の促進といった、より活発な貿易を促進する政策です。

近年、この構図はデジタル分野にも拡大し、「デジタル保護主義」と呼ばれる潮流が強まっています。データの国外移転を制限するデータローカライゼーションや国産クラウドサービスの利用促進といった取り組みが、その典型例です。

以上のような経済政策の軸に加え、国際秩序を理解する上でもう1つ重要なのが、政治体制をめぐる「民主主義」と「権威主義」の軸です（図表2）。民主主義国家では国民の代表者が選挙で選ばれ、国民の権利を尊重した国家運営が行われます。一方、権威主義国家では権力が一部の指導者や政府に集中し、国の統一や秩序がより優先されると言われます。この体制の違いは、サイバー空間の統治思想にも大きな影響を与えています。伝統的な国際秩序においては、国家が領域内の事柄を排他的に統治する「国家主権」の概念が基礎にありますが、サイバー空間ではその適用範囲をめぐって考え方が分かれています。インターネットはもともと米国の軍事機関の資金で研究された技術から発展し、西側諸国を中心に「自由で相互接続されたオープンな空間」という理念のもと各国政府に限らない産業界・学術界などのコミュニティが議論に参加する「マルチステークホルダー主義」が重視されてきました。

一方で、権威主義国家は「サイバー主権」を掲げています。これは、物理的な国境と同様にサイバー空間にも国家主権が及び、政府が自国内のインターネットを制御・規制できるとする考え方です。この立場からは、国連などの政府間枠組みを通じて、国家を主体とした国際的なルール形成によりインターネットガバナンスを構築しようとする「マルチラテラル主義」が重視される傾向にあります。民主主義国家も国連での議論に参加しています。ただし、サイバー空間における国家主権の考え方や、国際法の適用、統治主体のあり方に関する立場は異なります。

図表2：権威主義と民主主義



出所：公的情報を基にPwC作成

この対立構造は、国際社会でも表面化しています。2022年2月、中国とロシアは北京冬季五輪の開幕に合わせて共同声明を発表し、各国が自らの主権のもとでサイバー空間を管理すべきだとする「サイバー主権」の立場を鮮明にしました。これに対し、同年4月には米国や日本、欧州諸国など約60カ国・地域が「未来のインターネットに関する宣言」に賛同し、インターネットを「自由で開かれ、相互接続され、信頼できるもの」として維持する姿勢を示しました。この宣言では、検閲や遮断への反対とともに、多様な主体が関与するマルチステークホルダー主義への支持が明確に打ち出されています。

ただし、こうした明確な対立軸だけでは、現在の国際環境の複雑さを十分に説明できません。実際の国際情勢は、単純な二項対立で説明できるものではないからです。経済分野の保護主義と自由主義、政治体制の権威主義と民主主義、さらには大国間の米中対立といった複数の軸が複雑に絡み合い、相互に影響し合いながら形成されています。中でも近年顕著なのは、デジタル化を契機として、保護主義・権威主義的な動きが世界的に広がっていることです。こうした傾向は、権威主義国家に限らず見られるようになっています。

さらにデジタル領域では、規制のあり方がより複雑化しています。各国では個人情報保護や越境データ移転の制限、データローカライゼーションの強化が進められています。表向きは国民の権利保護を目的としていても、実際には安全保障のための手段として利用されるケースもあります。こうした動きは、特定の政治体制に限らず各国に広がっており、結果としてデータや技術をめぐる新たな「見えない国境」を生み出しています。

保護主義的政策がサイバーセキュリティに及ぼす影響

保護主義的な動きは、確実にデジタルの領域へと波及しています。

その典型が、「データローカライゼーション」です。EU、米国、中国などの主要経済圏では、プライバシー保護を掲げた法制度が相次いで整備されてきました。その結果、データを域外に移転するには厳格な手続きと審査を要するようになり、かつて自由だった情報流通は例外的な運用に変わりつつあります。データの移転コストが上昇し、国や地域ごとの制度差が企業活動の新たな制約となっているのです。

同時に、情報統制の動きも顕在化しています。日本では、インターネットは誰もが利用できる「開かれた空間」と捉えられがちですが、世界では必ずしもそうではありません。中国では「グレート・ファイアウォール」という国家によるインターネット検閲・遮断システムが存在することが知られており、2025年8月に中国本土で発生した大規模な通信遮断との関連でも注目を集めました。ロシアでも2022年以降、インターネット通信に対する規制の強化が報告されており、接続の不安定さも指摘されています。

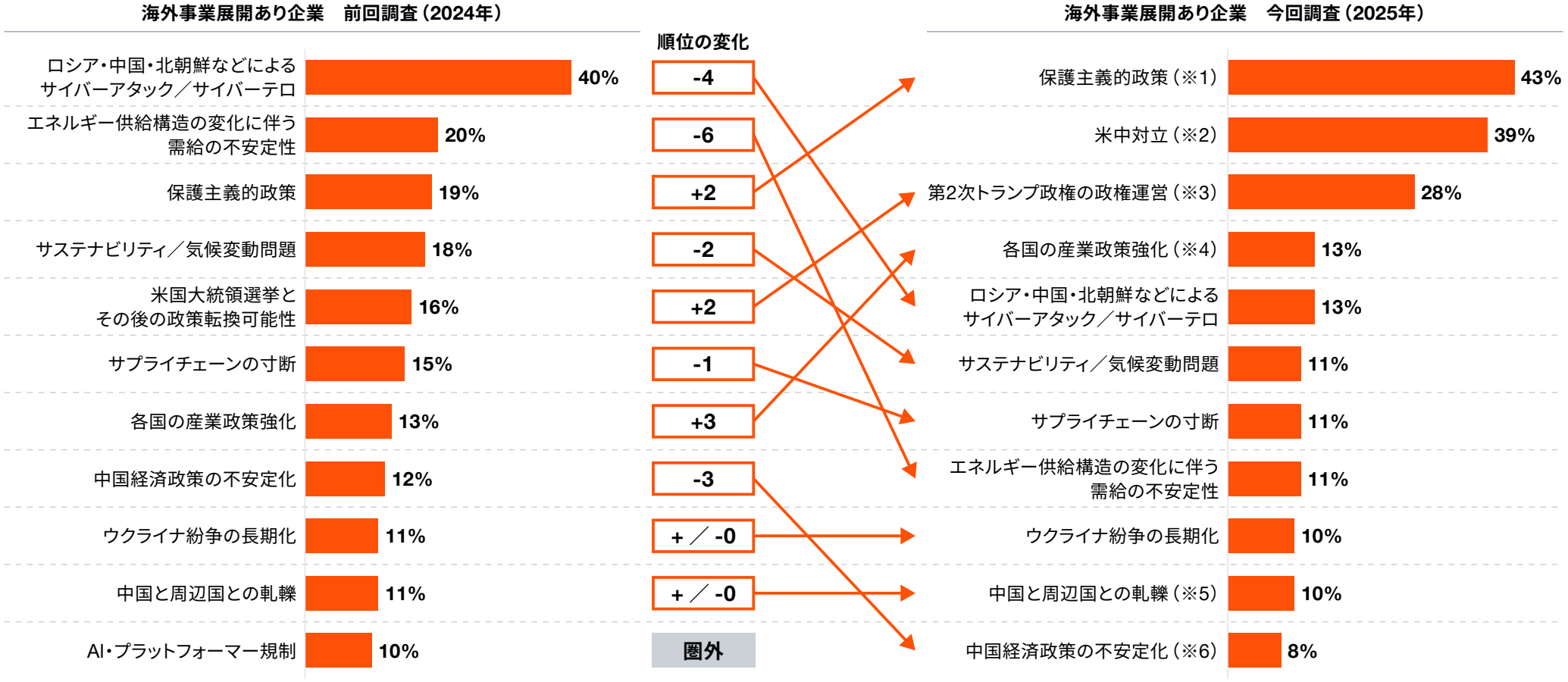
さらにSNSの利用制限は、権威主義国家だけの現象ではありません。先進的な民主主義国家においても、プラットフォーム規制や情報発信の統制をめぐる動きが広がりつつあります。

地政学的な構造変化は、企業のリスク認識を大きく変えています。PwC Japanグループが2025年6月に実施した「企業の地政学リスク対応実態調査 2025」でも、その傾向が明確に示されました（図表3）。

調査では、海外事業を展開する企業に「現在、最も懸念する地政学リスクは何か」を尋ねています。2024年調査では「ロシア・中国・北朝鮮などによるサイバーアタック／サイバーテロ」が首位でしたが、2025年調査では上位から順位を下げました。代わって上位を占めたのは、「保護主義的政策」（43%）、「米中対立」（39%）、「第2次トランプ政権の政権運営」（28%）です。企業の関心は、サイバー攻撃そのものから、国家間の対立や政策の不確実性へと明確にシフトしているのです。

図表3：企業の地政学リスク対応実態調査2025

Q. 今、あなたの会社で最も懸念される地政学リスクは何ですか。(3つまで)



(※1) 米国の各種関税措置、EUの中国EVへの追加関税、資源国による資源輸出制限など
(※2) 貿易摩擦、安保上の対立など
(※3) 前回調査（2024年）の選択肢は「米国大統領選挙とその後の政策転換可能性」
(※4) 米インフレ抑制法（IRA）、EUのネットゼロ産業法、中国の国内企業向け補助金その他の支援など
(※5) 南シナ海、中印国境紛争など
(※6) 不動産産業政策など

出所：PwC Japanグループ 企業の地政学リスク対応実態調査 2025

こうした国際環境の変化は、サイバーセキュリティにも深刻な影響を及ぼしています。

保護主義や権威主義が進行すると、ある傾向が生まれます。それは「サイバー活動によって失われたものを取り戻そうとする誘惑」です。こうした流れを後押ししている要因は3つあります。まず、保護主義政策の強化です。データローカライゼーションや輸出・買収規制の拡大により、技術やデータを合法的に取得することが難しくなりました。その結果、非合法な手段に頼る動きが増えています。

次に挙げられるのが、権威主義国家のサイバー能力の高度化です。国内の監視や検閲を進める過程で、情報操作や他国への影響工作を担う専門機関が発展し、国家レベルの攻撃能力が高まっています。

そして、国際協力の停滞です。先述したとおり法制度や主権の壁が協力を難しくし、結果として攻撃が実行しやすい環境を生んでいるのです。

PwCが世界規模で追跡しているデータでも、この傾向が明確に表れています。2026年8月時点で把握されている脅威アクター（サイバー攻撃グループ）は619に上り、それぞれの拠点や標的となる産業を詳細に分析しています。

国際協力が難しくなる一方で、攻撃者にとってはより行動しやすい環境が広がっています。こうした状況の中で、企業は自らの力で防御を強化しなければなりません。

次章からは、このような環境下、サイバーセキュリティ領域で企業が特に注視すべき事項と企業対応の要諦を多面的に解説します。

巧妙化する攻撃、強まる規制、広がるAI ―変容するサイバーリスクの実像―

2-1.「サイバー脅威」正規アカウント・正規ツールを悪用するサイバー攻撃への対策アプローチ

脅威アクターの動向

昨今では、サイバー攻撃によって基幹システムが停止し、事業継続に大きな影響を受けた日本企業の事例が多く見られます。今後も、ビジネスに多大な影響を及ぼすサイバー攻撃は継続すると予想されるため、日本企業にとっては入念な対策が欠かせません。PwCのサイバー脅威インテリジェンスチームは、今後の動向として、「正規アカウントの悪用（アイデンティティに対する脅威）」「正規ツールの悪用（環境寄生型攻撃：LotL攻撃）」「AIを用いたソーシャルエンジニアリング」に注視する必要があると分析しています。これらは正規の操作を装った攻撃であるため、従来の検知ソリューションでは把握しづらいという特徴があります。脅威アクターが、どのような背景や目的で攻撃手法を変えてきているのか、その動向を見ていきましょう（図表4）。

図表4：主な脅威アクターの動向

ロシアを背景とする脅威アクター	中国を背景とする脅威アクター	北朝鮮を背景とする脅威アクター
• マルウェア依存を減らし、クラウド環境の悪用へ軸足を移す • ICS/OTを狙った破壊活動	• 長期潜伏型攻撃（APT攻撃）、LotL攻撃 • 台湾関連の情報操作	• AIを用いたフィッシングやディープフェイクを多用 • サプライチェーン攻撃能力を強化

出所：PwCサイバー脅威インテリジェンスチーム作成

• ロシアを背景とする脅威アクター

マルウェアへの依存を減らし、クラウド環境の正規アカウントを初期侵入時に悪用する手口に軸足を移しています。また、親ロシア派ハクティビストによる産業制御システム（ICS/OT）を狙った破壊活動は継続的に報告されており、日本企業もサプライチェーンを通じて影響を受けるリスクが常に存在します。

• 中国を背景とする脅威アクター

中国が重視する産業分野（防衛、エネルギー、通信など）と、中国拠点の脅威アクターが標的とする分野には関連性が指摘されており、こうした分野に対する長期潜伏型攻撃（APT攻撃）は今後も継続する可能性があります。また、侵入したネットワーク機器を悪用し、LotL攻撃をすることで、有事の際の破壊活動も視野に入れ、攻撃活動を活発化させる可能性もあります。特に、台湾海峡をめぐる地政学的緊張の高まりが、情報操作やサイバー攻撃の活性化につながる可能性が懸念されています。

• 北朝鮮を背景とする脅威アクター

外貨獲得のための「サイバー金融犯罪」と、国家安全保障に関わる「諜報（ちょうほう）活動」の二軸で攻撃を展開し続けると見られています。また、AIを用いたフィッシングやディープフェイクを多用し、その手口はさらに巧妙になると予測されます。引き続き、金融業界や防衛分野が主要なターゲットとなる可能性があります。

このように、今後のサイバー攻撃は、正規アカウントの悪用（アイデンティティに対する脅威）、APT攻撃やLotL攻撃による潜伏活動、AIを用いた高度なソーシャルエンジニアリングなどの攻撃が多用され、従来のセキュリティ対策では検知が難しい巧妙なサイバー攻撃が増加すると予測されます。この傾向に対して、日本企業は十分な準備ができているでしょうか。PwC Japanグループは、日本企業のサイバーセキュリティの意思決定や企画に携わる300人を対象に調査（以降、本調査）を実施し、各企業の実態を分析しました。

注視すべき3つのサイバー脅威

正規アカウントの悪用（アイデンティティに対する脅威）に対する日本企業の現状

企業を狙ったサイバー攻撃は、メール経由でのスピアフィッシング、VPN製品などのインターネットに露出しているアタックサーフェスに対する脆弱性攻撃が主流でした。こうした傾向は依然として存在するものの、昨今は「アイデンティティ」を狙った攻撃へのシフトが徐々に進行しています。つまり、ユーザーIDやパスワードといった認証情報に加え、デジタルアイデンティティ情報を悪用し、システムへの不正アクセスや個人情報の窃取を狙うサイバー攻撃が増えることが予想されます。

実際のインシデント事例としては、多要素認証を例外的に無効化した委託先社員の正規アカウントや、闇サイトで販売されていた認証情報が悪用され、初期侵入を許したケースがありました。攻撃手法も多様化しており、以下のような巧妙な手口が確認されています（図表5）。

図表5：アイデンティティに対する主な攻撃手法

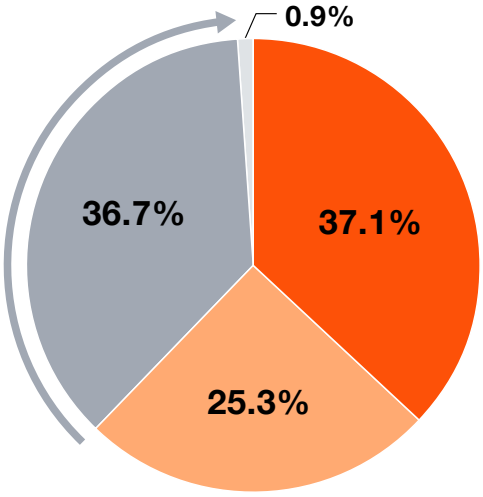
攻撃ベクター	攻撃手法	概要
人間	AiTMフィッシングによるトークン窃取	中間者攻撃により偽のポータルサイトを作成・表示し、ユーザーID・パスワードだけでなく多要素認証コードも窃取することでセッションデータを不正に取得
	MFA疲労攻撃	正規ユーザーに対して、主にモバイルへの多要素認証のプッシュ通知、電話などを繰り返し発生させる。正規ユーザーが疲労し、誤操作・根負けしてログインを許可するように仕向ける
	部外者へのなりすましによる不正オンボーディング	外部委託先などを装ってITヘルプデスクや人事部門にコンタクトして、アカウント登録・権限付与などのオンボーディングプロセスを実施させることで不正ログインを実行
設定	正規アカウントの盗用・悪用	窃取した正規アカウントの認証情報を悪用してクラウド環境にログインし、権限昇格などを実行
	条件付きアクセス、デバイストラストの設定不備	接続元IPアドレス制限や多要素認証の実施例外などの設定不備により、これらのコントロールが適用されないことに乗じて不正ログインを実行
デバイス	インフォスティーラーによるセッション・認証情報の再利用	正規ログイン済みのエンドポイントにインフォスティーラーを感染させ、セッションクッキーやOAuthトークンを窃取して再利用することで、認証を回避して不正ログインを実行
	正規のリモートアクセスツールの悪用	窃取した認証情報およびITヘルプデスクがサポート目的で利用するリモート管理ツールを悪用して不正ログインを実行
トークン	悪意／過剰な権限のOAuthアプリケーション	従業員をだまして悪意のあるOAuthアプリへの権限付与に同意させ、得られたOAuthトークンを悪用して不正操作を実行

出所：公開情報を基にPwC作成

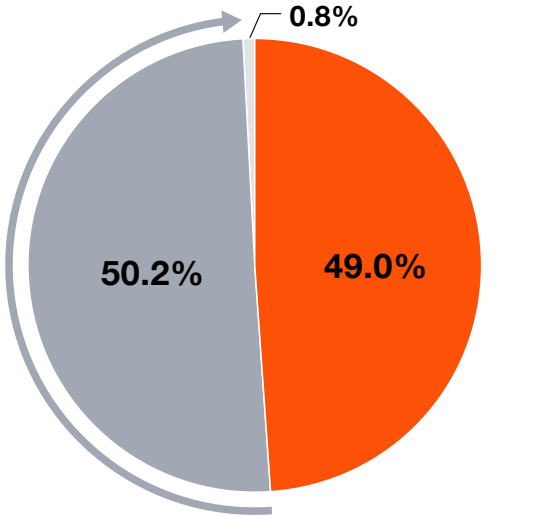
攻撃の矛先が「アイデンティティ」へシフトしているにもかかわらず、本調査では、いまだに多要素認証・多段階認証を導入していない企業が一定数あることが分かりました。多要素認証・多段階認証の導入状況では36.7%が未導入であり（図表6の左側）、組織外ネットワークからのアクセスに対する条件付きアクセスやリスクベース認証の実施状況は50.2%が未実施でした（図表6の右側）。

図表6：認証システムの導入状況

Q. 貴社における多要素認証・多段階認証の導入状況について教えてください。（単一選択、n=300）



Q. 内部システムに対する組織外ネットワークからのアクセスに対する条件付きアクセス、リスクベース認証を実施していますか。（単一選択、n=300）



出所：PwC「2026年 Cyber IQ調査」

正規ツールを悪用するLotL攻撃は重大インシデントの84%で利用

84%

LotL攻撃は、異常な振る舞いを検知することが極めて困難です。標準コマンドなどの企業内に必ず存在する機能を悪用するため、業務の一環として行われた操作なのか、サイバー攻撃なのかを判別することが難しいからです。Bitdefender Labsの2025年の調査によると、重大インシデントの84%でLotL攻撃が行われており、これは脅威アクターが常套手段としてLotL攻撃を用いていることを示しています[1]。

1「Bitdefender 2025 Cybersecurity Assessment Report」、Bitdefender、2025年、https://www.bitdefender.com/en-us/business/campaign/2025-cybersecurity-assessment

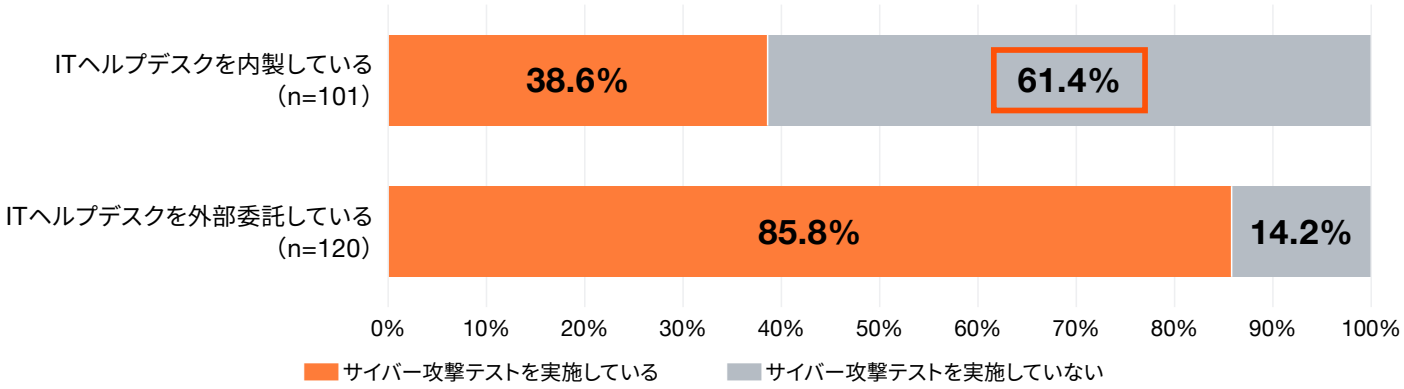
ITヘルプデスクを狙ったサイバー攻撃の懸念

生成AIによって自然な日本語のフィッシングメールや巧妙な偽画像・偽動画が量産される中、従業員やヘルプデスク担当者を標的としたソーシャルエンジニアリングが確認されています。特にITヘルプデスクは、顧客や従業員からの依頼に基づき、パスワードリセットやアカウントのロック解除など、特権的な操作を行う権限を持つため、攻撃者にとって非常に魅力的な標的となります。攻撃者が一度ここを突破すれば、基幹システムへのアクセスも可能になり、ビジネスに甚大な被害をもたらす恐れがあります。

本調査では、ITヘルプデスクを内製している日本企業の61.4%が、サイバー攻撃を想定したテストを「実施していない」と回答しました（図表7）。これは、外部委託している企業（14.2%）と比較して著しく高い水準です。外部委託している企業は、委託先との契約の中でサイバー攻撃テストを含むセキュリティ対策を要件として求めますが、内製化している企業は身内への信頼感から、攻撃を受けるリスクへの感度が低くなっていると考えられます。

図表7：ITヘルプデスクでのサイバー攻撃テスト実施状況

Q. 貴社におけるITヘルプデスク（パスワードリセット等の業務を実施）の体制を教えてください。（単一選択、n=300）
Q. 貴社では、ITヘルプデスクへのサイバー攻撃（ソーシャルエンジニアリングを含む）に関するテストを実施していますか。（単一選択、n=300）



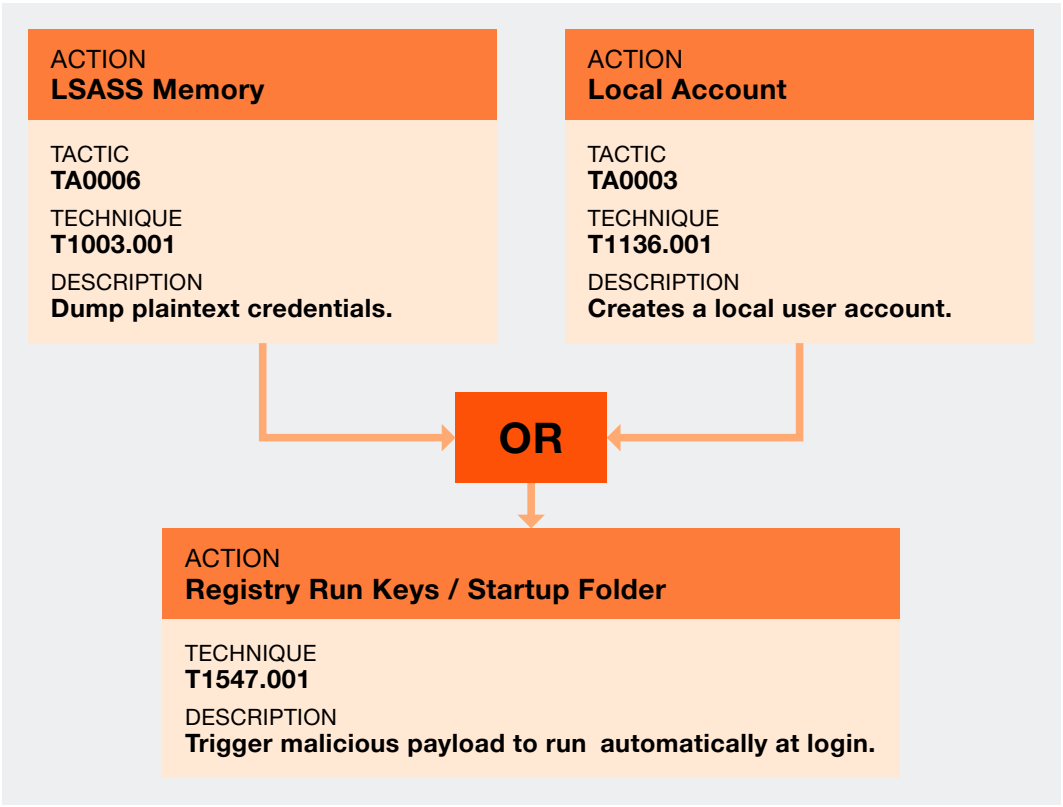
出所：PwC「2026年 Cyber IQ調査」

Attack Flowを用いた文脈に基づく新たなアプローチ

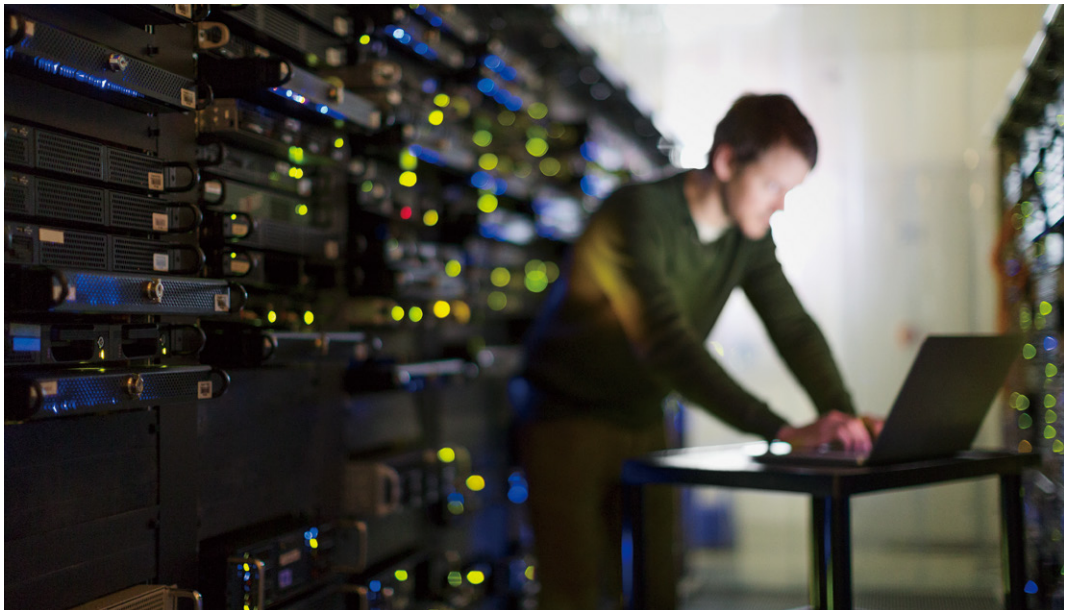
このように、攻撃者が巧妙な攻撃に重点を置くことで、従来のセキュリティ対策では検知が難しいサイバー攻撃がさらに増加すると予測されます。検知困難なサイバー攻撃に対処するための銀の弾丸と言えるセキュリティソリューションは存在しないため、直近で発生したサイバー攻撃の文脈（コンテキスト）を可視化・形式知化することが重要です。つまり、最新の攻撃事例を分析し、攻撃者が「どの局面で何を判断し、なぜその手法を選択したのか」という意思決定プロセスを組織の知識として蓄積・共有し、組織のセキュリティ対策を継続的に進化させることが必要となります。

サイバー攻撃の文脈を可視化・形式知化するための手法の1つに、「Attack Flow」の活用があります。Attack Flowとは、過去に発生した、あるいは今後想定されるサイバー攻撃について、攻撃者がどのような目的を持ち、どのような戦術・技術・手順（TTPs: Tactics, Techniques, and Procedures）を、どのような順番で実行し、攻撃が失敗した際にどのように行動を変えるかをフローチャート形式で描き出すツールです。MITRE ATT&CKは「どのTTPsが使われたか」をカタログやリストで示しますが、攻撃者の思考や判断の流れまでは把握できませんでした。一方、Attack Flowは「攻撃者の意思決定プロセスや攻撃の流れ」を可視化・形式知化することができます（図表8）。

図表8：Attack Flowによる攻撃プロセスの可視化の例



出所：Attack Flow公開情報よりPwC作成



Attack Flowを活用することで、「なぜ攻撃者はこのサーバーに侵入した後、このツールを実行したのか」「次に狙われる可能性が最も高い資産は何か」といった問いに、根拠となる事例をベースに答えることが可能になります。攻撃者の意思を可視化・形式知化することで、攻撃を予測し先手を打つ「プロアクティブ」なサイバーセキュリティへの転換につなげられます（図表9）。

Attack Flowによって可視化された攻撃の文脈は、既存のセキュリティソリューションの能力向上に役立ちます。攻撃文脈を基にしたセキュリティ対策例を3つ挙げます。

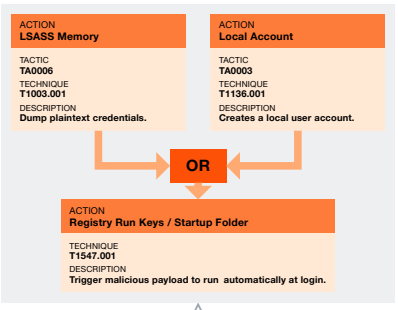
- **SIEM/XDRの高度化**：Attack Flowで示されるTTPsの流れや分岐条件は、SIEMやXDRにおける高度な検知シナリオ（相関ルール）の作成に活用できます。例えば、「VPNでのログイン後、30分以内に特定のコマンドが実行され、かつファイルサーバーへのアクセスが急増した」といった、単体では見過ごされがちな事象の連鎖を1つの攻撃活動として捉えることで、インシデントの検知精度を高められます。

- **Deception（おとり技術）の設置**：Attack Flow上の重要な分岐点、例えば攻撃者が認証情報を窃取した後に必ず試みるであろうディレクトリサービスへのアクセス経路上に、おとり（デコイ）となるファイルやアカウントを意図的に配置します。これにより、攻撃者の行動を誘発し、使用ツールや行動をリアルタイムで把握することが可能になります。

- **脅威ハンティングでの活用**：Attack Flowを「当社には脅威アクターが既に潜伏しているのではないか」という仮説検証に活用します。この仮説に基づき、不審な挙動の痕跡（IoA: Indicator of Attack）を探索する「脅威ハンティング」を実施することで、侵害が深刻化する前に発見・駆除が期待できます。

図表9：Attack Flowを基にしたセキュリティ対策例

Attack Flowによるサイバー攻撃の可視化・形式知化の例



過去のサイバー攻撃事例をフローチャート化し、サイバー攻撃の文脈を可視化・形式知化

MITRE ATT&CKが「どのTTPs（戦術・技術・手順）が使われたか」を示すのに対し、Attack Flowは、

- なぜその行動が行われたのか
- 次に何を狙っているのか
- どの条件分岐で攻撃が変化するのか

といった攻撃者の意思決定プロセスを含めたストーリーを表現可能

攻撃文脈（コンテキスト）を基にしたセキュリティ対策例

SIEM/XDR

Attack Flowの意思決定プロセスや分岐条件を参考に、検知ルールを作成

Deception

Attack Flow上の分岐点や必須行動にデコイを配置し、攻撃者の次の行動を誘発・可視化する設計に活用

脅威ハンティング

Attack Flowを「攻撃の進み方の仮説」として使い、異常アラートがなくても不審な行動を検知するために活用

過去事例を基に文脈を理解して対策に生かす

出所：Attack Flow公開情報よりPwC作成

このように、従来のセキュリティ対策では検知が難しいサイバー攻撃に対処するためには、最新の攻撃事例をAttack Flowを用いて分析し、得られた知見を組織の知識として蓄積・共有した上で、組織のセキュリティ対策を継続的に進化させることが重要です。そのためには、3カ月に一度のペースでレビューを実施し、自組織の対策が最新の攻撃に対して有効か、検知が難しい攻撃に対応できているか、過去に見逃された潜伏がないかを継続的に確認することが求められます。こうした取り組みを通じて、組織としての知見を深め、セキュリティ対策を継続的に高度化していくことが必要となります。

2-2. 中国拠点の脅威アクターによる日本を標的とした攻撃活動の変化

国家の関与が疑われるサイバー攻撃

サイバー空間における脅威アクターによる攻撃活動には、その脅威アクターの拠点が所在するとみられる国家の政治・外交・経済上の課題など、いわゆる地政学的環境との関連性が観測される場合があります。本章では、このような地政学的環境と脅威アクターの活動との関係性に着目した上で、日本と中国を取り巻く昨今の地政学的環境に連動して生じうる中国拠点の脅威アクターの攻撃活動の変化について、機密情報を狙ったサイバースパイ活動、重要インフラに対する長期潜伏や機能停止を企図した活動、世論分断やレピュテーション低下を目的とした影響工作という3つの観点から考察します。

なお、国家の関与が疑われるサイバー攻撃については、各国政府やセキュリティ機関が「パブリックアトリビューション」と呼ばれる形で特定の国家や組織との関連性を公表しており、こうした脅威アクターはしばしばState-Sponsored（国家支援型）アクターとも表現されます。以下の記載は、これらの公表情報やPwCによる分析を基礎としていますが、これらは技術的分析やインテリジェンス評価に基づくものであり、その性質上、一定の不確実性を伴う点、また、脅威アクターの活動と国家の意図を同一視することはできない点にも留意が必要です。

日本と中国を取り巻く地政学的環境

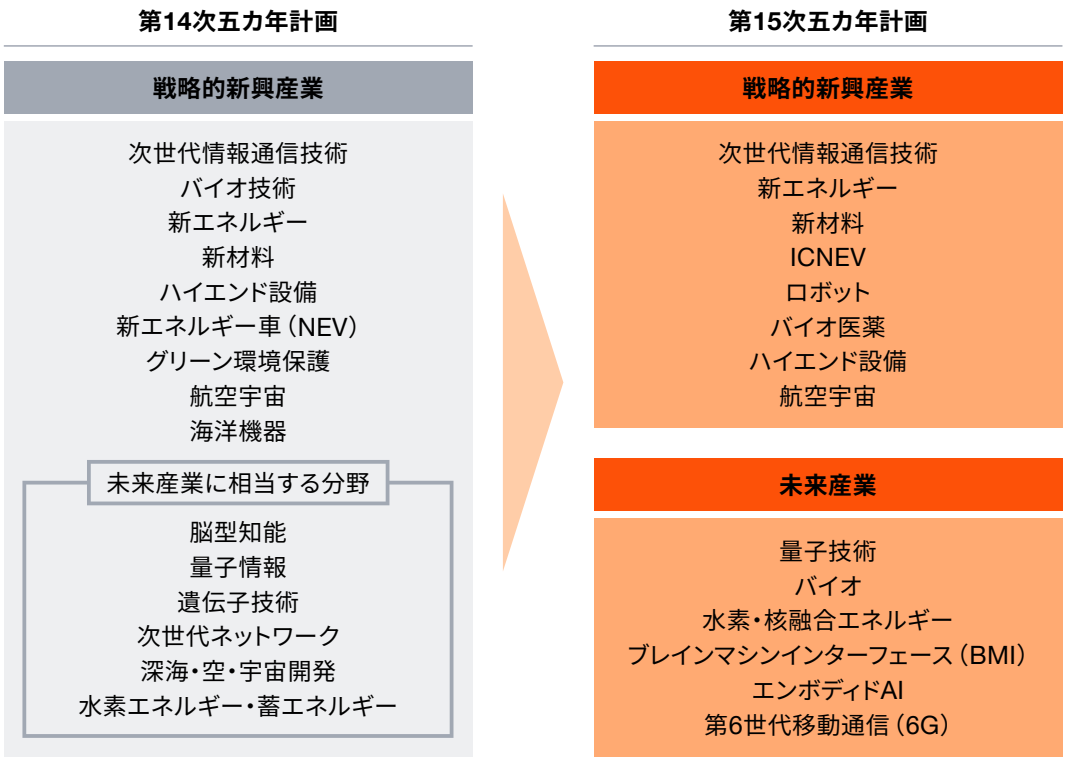
日本を標的とした中国拠点の脅威アクターによる今後の攻撃活動を考察する上では、脅威アクターの地政学的環境の観点において中国の国家戦略および近年の日中関係を理解する必要があります。本章では、前者については2026年から始動した「第15次五カ年計画」の内容を、後者については台湾情勢をめぐる日中関係を、それぞれファクトに基づいて整理します。

中国の国家戦略：第15次五カ年計画

中国共産党は、2026年3月上旬に開催された全国人民代表会で第15次五カ年計画（2026～2030年）を正式に公表しました。ここでは、第14次五カ年計画と比較した際の違いに着目し、中国の国家戦略にどのような変化が見られるかについて確認します（図表10）。

結論から述べると、両者における「新興産業」と「未来産業」の位置付けと扱い方にはっきりとした違いが見られます。まず第14次五カ年計画では、「戦略的新興産業」という1つの大きなカテゴリーが示されており、その中に次世代情報通信技術、バイオ技術、新エネルギー、新素材、ハイエンド設備、新エネルギー車（NEV）、グリーン環境保護、航空宇宙、海洋機器などが含まれています。また、未来産業に相当する分野も例示されていますが、これらはまとめて「戦略的新興産業」として扱われており、「未来産業」として切り出すような二段構えの整理は行われていません。

図表10：第14次五カ年計画と第15次五カ年計画の比較



出所：中華人民共和国国家発展改革委員会（NDRC）の情報を基にPwC作成

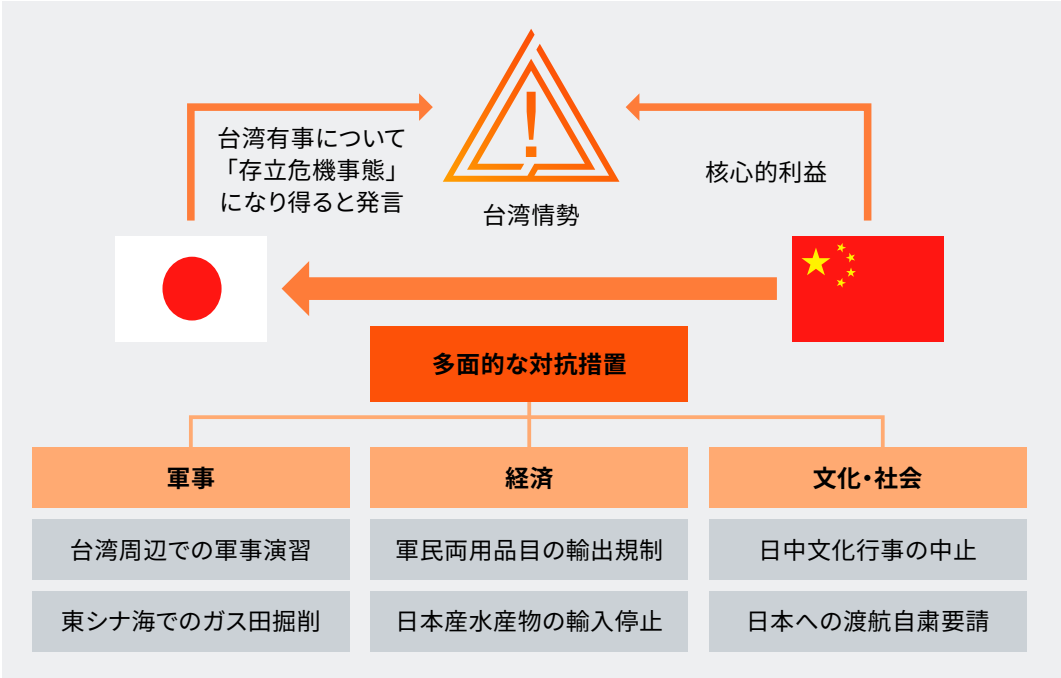
これに対して第15次五カ年計画では、戦略的新興産業を引き続き重視しつつも、第14次五カ年計画では未来産業が新興産業の一部であったのが、新計画ではそこから切り出されて並列に置かれている点が特徴的です。また、未来産業の具体性がより明確化されていることからも、第15次五カ年計画を通じて中国が今後重視する産業も確認することができます。具体的には、量子技術、バイオ、水素・核融合エネルギー、ブレインマシンインターフェイス（BMI）、エンボディドAI（身体性知能）、6G通信が挙げられています。

上記の産業政策に関する変化に加えて特筆すべきは、15次五カ年計画においては、「中国人民解放軍創立100周年の奮闘目標を期限どおりに達成し、国防・軍隊の現代化を質高く推進する」という目標が第15篇で明確に定められていることです。その上で、同篇では、戦略抑止力や無人・智能化（人工知能化）戦力、新領域戦力、先進装備の整備を進めるとともに、軍事理論、人材、組織、統治の近代化を図る方針を示しています。また、軍民融合を通じて民間先端技術や産業基盤を国防に取り込み、重要インフラへの国防要求の反映、国防動員、予備戦力、国境・海空防衛の強化、全民国防教育の推進も盛り込まれています。

台湾情勢をめぐる日中関係の緊迫化

2025年11月、高市首相が台湾有事をめぐって「存立危機事態」に言及したことを契機として、日中関係は短期間で急速に緊迫化しました。この答弁を受け、中国側は「重大な内政干渉」に当たるとする声明を発表し、外交・経済・軍事分野における多面的な対応へと発展しました。中国は日本大使の呼び出しや国連事務総長宛ての書簡送付に加え、台湾周辺での大規模軍事演習「正義使命2025」を実施し、台湾海峡での軍事的プレゼンスを対外的に示しました。さらに、尖閣諸島周辺における中国海警局の船の継続的な航行、東シナ海の中間線付近でのガス田掘削など、東シナ海における緊張を高める活動も確認されています。経済・人的交流の分野でも、日本に対するレアアースの輸出管理の強化や日本産水産物の輸入停止が報じられた他、中国人の対日渡航を控えるよう呼びかける動きや日中交流行事の中止も相次ぎ、日中間の経済活動や人的交流の停滞が一時懸念されました（図表11）。このような事態は、日中間の相互不信が、特定の発言や政策動向を契機として顕在化し得ることを示唆しています。また、中国側の対応は外交・軍事・経済・文化の各分野にわたり、複合的かつ段階的に圧力を強める傾向が鮮明になりました。

図表11：台湾情勢をめぐる日中関係の現状



出所：PwC作成

中国拠点の脅威アクターによる日本を標的とした攻撃活動の変化

前述のとおり、日中関係の緊張は、中国側の外交・軍事・経済にまたがる圧力行使と、日本側の対中依存低減・安全保障見直しを同時に進めています。このことは、中国拠点の脅威アクターにとって「日本からどのような情報・機能・世論を狙うか」という優先順位に変化をもたらし得るとPwCは分析しています。本レポートでは、特に以下の3つの視点（図表12）で、同国が関与する脅威アクターの攻撃活動がどのように展開されるかについて考察しました。

図表12：中国拠点の脅威アクターによる日本を標的とした攻撃活動で想定される変化

1. 日本の官公庁や民間組織の機密情報を標的とするサイバースパイ活動の活発化
2. 日本の重要インフラにおける長期潜伏または機能停止を企図した活動の増加
3. 日本国内の世論分断または日本の国際的信用の低下を目的とした影響工作の増加

出所：PwC作成

日本の官公庁や民間組織の機密情報を標的とするサイバースパイ活動の活発化

サイバースパイ活動の現状

中国を拠点とする複数の脅威アクターが日本の組織に対してサイバースパイ活動を継続的に行っていることが報告されています。例えば、日本の警察庁や外国の政府機関によってパブリックアトリビューションの対象になったグループとして、図表13の4組が挙げられます。

とりわけRed Apollo（APT10）のサブグループとされるMirrorFaceは、2025年初めに日本国内で広く報道されました。警察庁および国家サイバー統括室（NCO）によれば、2019年から2024年にかけて、日本国内の組織、事業者、個人に対して複数の攻撃キャンペーンを展開していました。当該アクターは主に日本の安全保障や先端技術に係る情報窃取を目的としていると分析されています。報告された攻撃キャンペーンでは、日本のシンクタンク、政府、マスコミ、半導体、製造、情報通信、学術、航空宇宙分野の組織や個人が標的となりました。また、過去にはインドや台湾の組織も標的に含まれていました。LODEINFOなどのマルウェアを含むファイルまたはダウンロードリンク付きの標的型メールでは、「日米同盟」「台湾海峡」「ロシア・ウクライナ戦争」「取材のご依頼」などの標題を用いて標的の関心を引く試みが見られます。また、VPN機器におけるリモートコード実行の脆弱性を悪用して標的の環境に侵入した他、コードエディターを悪用してマルウェアを実行した事例も確認されています。

図表13：過去に日本を標的とした中国を拠点とする国家支援型アクター

脅威アクター（PwC追跡名）	公表時期	標的	攻撃事例
1.Red Apollo	2025年1月8日（警察庁／NISC（現NCO））	半導体、製造、情報通信、航空宇宙、シンクタンク、政府関係者（退職者含む）、マスコミ・学術関係の個人・組織	• 2019年ごろから、日本国内の組織、事業者および個人にする主に日本の安全保障や先端技術に関する情報窃取キャンペーンを観測 • 主な手口として、第三者になりすまし、**マルウェアを添付したメール**などを送信して感染させる標的型メール攻撃、**VPN機器などのネットワーク機器の脆弱性を悪用**して侵入する攻撃などが確認されている
2. Red Yuxa	2021年4月22日（国家公安委員会委員長記者会見など）	宇宙航空研究開発機構（JAXA）を含む、約200の国内企業など	• **偽名などを用いて日本のレンタルサーバーを不正契約**として、警視庁公安部が2021年4月に中国共産党員の男を私電磁的記録不正作出罪・同供用罪で検挙 • 捜査の結果、不正契約されたサーバーが国内の宇宙航空分野の研究機関などや約200の国内企業へのサイバー攻撃に悪用されていたことを把握。攻撃主体はRed Yuxa、**背景には中国人民解放軍第61419部隊が関与**している可能性が高いと特定 • 一連のサイバー攻撃は、日本製ソフトウェアの脆弱性が悪用された**ゼロデイ攻撃**であった
3. Red Djinn	2023年9月27日（警察庁／NISC（現NCO））	日本を含む東アジアおよび米国の政府、産業、技術、メディア、エレクトロニクス、電気通信分野	• 2010年ごろから、日本を含む東アジアおよび米国の政府、産業、技術、メディア、エレクトロニクス、電気通信分野を標的に、情報窃取を目的としたサイバー攻撃を実施 • 主な手口は、ネットワーク機器の脆弱性や設定不備を悪用した侵入、**海外子会社のルーターを経由した本社などへの侵入拡大**、改変ファームウェアへの置換によるログ隠蔽と長期潜伏である
4. Red Ladon	2024年7月9日（警察庁／NISC（現NCO））	豪州政府・民間部門、日本国内組織	• 警察庁とNISC（現NCO）は、豪州ACSCが作成したRed Ladonに関する国際アドバイザリーに共同署名、日本企業も過去に当該アクターの攻撃対象となっていたことが確認されている • 上記アドバイザリーでは**Red Ladonは中国国家安全部（MSS）と関係するグループ**と位置付けられており、中国海南省海口市を拠点に活動しているとされる • 脆弱なインターネット接続機器の悪用、**認証情報の窃取、ウェブシェルによる永続化**、侵害済みWebサイトや**SOHO機器のC2・踏み台利用**といった手口が確認されている

出所：警察庁の資料などを基にPwC作成

考察と示唆

過去のRed Apolloの攻撃キャンペーンでは、日米同盟や台湾海峡といったアジア太平洋地域における安全保障問題がおとり文書のテーマとして使用され、半導体や航空宇宙分野を攻撃対象にするなど、日本を取り巻く安全保障環境や中国にとって戦略的に重要な産業がサイバー攻撃の手段または標的選定と密接に関係していることがうかがえます。

このようなサイバースパイ活動は、日中間の外交的対立が先鋭化している現状においては、より活発化していく可能性は十分に想定されます。第15次五カ年計画で言及されている新興産業や新たに設けられた未来産業は日本が強みとする技術とも関連している上、両国が協力と同時に相互の自立や優位確保を志向する局面に入っていることを踏まえると、これら重点分野における技術・知財を狙うサイバースパイ活動は、今後も継続・強化されると見込まれます。さらに、中国側のレアアース輸出規制と日本側の代替調達・技術自立といった「対応策」も、交渉・産業競争力の確保という観点から、中国拠点の脅威アクターによって標的にされる可能性があります。日本の官民組織は、自らが保有する情報のうち、地政学的文脈で価値を持つ部分（安全保障政策、先端技術、対中依存脱却戦略など）を特定し、重点的に保護する必要があります。

日本の重要インフラにおける長期潜伏または機能停止を企図した活動の増加

中国拠点の脅威アクターによる重要インフラへの攻撃事例

2023年、米国CISAなどは、中国拠点の脅威アクターRed Dev 49（別名：Volt Typhoon）が、米中間の重大な危機や軍事衝突の際に米国の重要インフラに破壊的なサイバー攻撃を行うために事前に侵入している（＝Pre-Positioning）と警告しています。Red Dev 49は重要インフラを標的にLotL攻撃を多用することで知られ、侵入後はマニュアル操作で永続的にアクセスを維持し、5年以上にわたって検知されることなく潜伏していた例も見つかっています。攻撃対象は主に通信、エネルギー、交通、上下水道セクターで、OT資産へのアクセスと重要インフラの停止を狙っています。

日本国内では2024年、JPCERTコーディネーションセンターが、日本の組織を狙ってRed Dev 49と多くの共通点がある攻撃キャンペーンOperation Blotlessについて注意喚起を発出しました。

考察と示唆

このような重要インフラを標的とした長期的な潜伏活動は、前章で述べた日中関係の緊張状態に連動して活発化する可能性があることはもとより、潜伏や機密情報の窃取にとどまらず、実際の機能停止にまで踏み込むことも想定されます。

軍事的な側面での重要インフラに対するサイバー攻撃の効果は既に近年の事例で実証されています。ウクライナの電力施設を標的としたサイバー攻撃では、2015年12月にBlackEnergy 3とKillDiskが、2016年12月にIndustroyer（CRASHOVERRIDE）がそれぞれ用いられ、大規模停電が引き起こされました。

こうしたサイバー攻撃と物理的な軍事作戦を組み合わせた手法の効果が、過去の実際の戦争で実証されていることから、地政学的緊張が高まる局面では、関係国の重要インフラに対するサイバー攻撃のリスクも連動して上昇すると評価すべきです。

過去の国際事例を踏まえれば、こうした攻撃が社会・経済の混乱をもたらし得ることを前提に、インフラ事業者は備えを強化する必要があります。日本においても、電力・通信・交通・上下水道などの重要インフラが、地政学的な緊張に伴いサイバー攻撃の標的となるリスクは高まっており、日本のインフラ事業者にはこうしたリスクを想定した長期潜伏型攻撃への監視・検知体制の整備が求められます。

日本国内の世論分断
または日本の国際的信用の低下を目的とした影響工作の増加

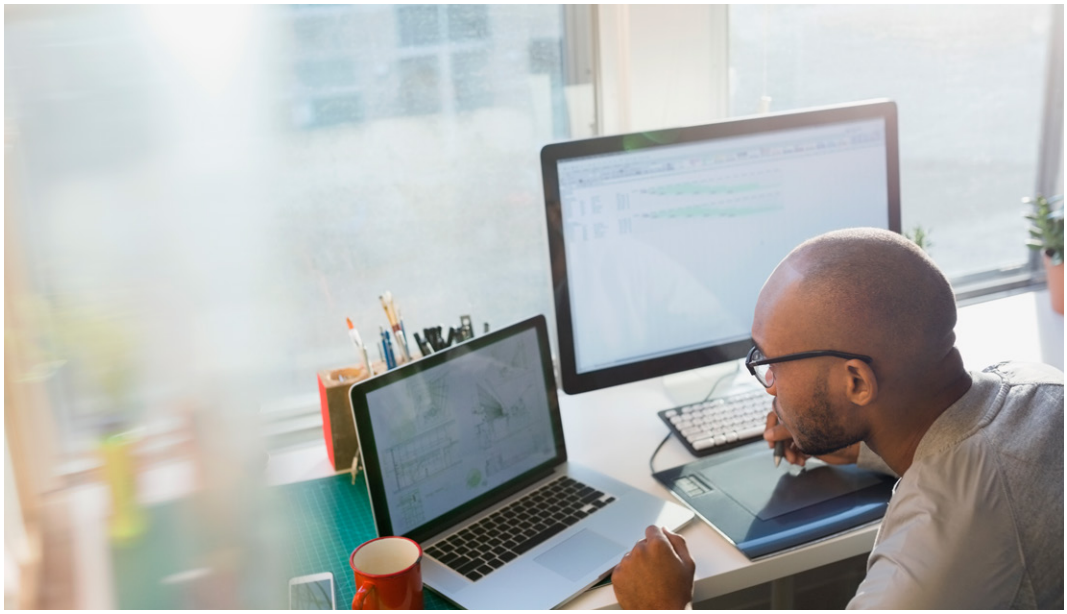
影響工作の実態と日本関連の事例

機密情報の窃取や重要インフラの機能停止を目的としたサイバー攻撃に引き続き警戒すべき一方で、日本国内の世論を分断することや、国際社会において外交的に優位な立場を得るために日本のレピュテーションを低下させることなどを意図した影響工作としての脅威アクターの活動にも注意を払う必要があります。

このような影響工作に関与していると言われる中国拠点の脅威アクターとして、PwCはRed Loke（別名：DRAGONBRIDGE、Spamouflage Dragon、Storm-1376）を追跡しています。同グループは、さまざまなソーシャルメディア上で偽情報を拡散しているとされています。一部の公開調査では、Red Lokeの活動が特定の国家機関と関連している可能性が指摘されていますが、その全容は依然として不明な点が多く残されています。

代表的な例として、2024年の台湾総統選挙では、与党・民主進歩党（DPP）の政治家をおとしめるための情報操作や、虚偽の汚職疑惑を流すことで選挙に影響を及ぼそうとした事案が挙げられます。また、フィリピンのフェルディナンド・マルコス・ジュニア大統領への支持を弱めることを目的に、ディープフェイク動画を拡散した事案も報告されています。さらに、2022年の米国中間選挙では、国内の分断をあおり、有権者の投票意欲をそぐことを狙って活動した他、2024年の米大統領選挙も標的としていたとされています。

Red Lokeは、キャンペーンの実行にあたって多様な手口やツールを用いています。AI生成の画像や動画の活用、正規のソーシャルメディアアカウントになりすます行為、ニュース記事を盗用・改変して虚偽のストーリーとして流す行為などです。SNSプラットフォームが、主な発信・拡散の場となっています。また、現地の一般市民やインフルエンサーを装う架空の人物アカウントを大量に作成し、メッセージにもっともらしさや信頼性があるように見せかけるのも特徴です。具体的な例としては、政治家に対する偽造文書や根拠のない告発を大量に投稿してSNSを埋め尽くしたり、豪州・カナダ・米国のレアアース関連企業を標的にして評判を落とし、市場での立場を弱めようとしたりしているとされています。ただし、こうした広範な活動にもかかわらず、一般ユーザーからの実際の反応は限定的であり、多くのエンゲージメントは同一ネットワーク内の別の偽アカウント同士によるものとみられています。



日本に関連するものとしては、福島での原発処理水放出による環境破壊を非難する記事が2023年後半に生成されています。また、2025年11月下旬、Red Lokeと関係があるとされるブロガーが、高市首相による安全保障・防衛政策、核政策（非核三原則の見直し）を批判する内容を投稿していました。元米海軍関係者を名乗るこのブロガーは、日本の近年の安全保障政策を戦前の軍国主義やファシズムの再来と捉え、表向きは礼儀正しく平和的に見える日本社会の裏に、反米感情や十分に清算されていない戦争意識が潜んでいると主張していました。その上で、高市首相による台湾有事への軍事関与を示唆する発言や、防衛費の増額、非核三原則の見直しをめぐる議論を、東アジアの緊張を高める危険な動きだと批判しています。また、被爆者や一部の政治家がこうした動きに反対していることにも触れ、日本は過去の戦争犯罪を真剣に反省し、再び世界を不安定化させる軍事路線に進むべきではないといった内容を投稿しました。

考察と示唆

今後も日本では、安全保障・核・対中・対台湾政策をめぐる議論が続くと見込まれます。その中で、Red Lokeのようなアクターが特定の政治家や政策を標的にしたナラティブを大量に流し、世論分断や政府不信を増幅させるリスクは高いと考えられます。

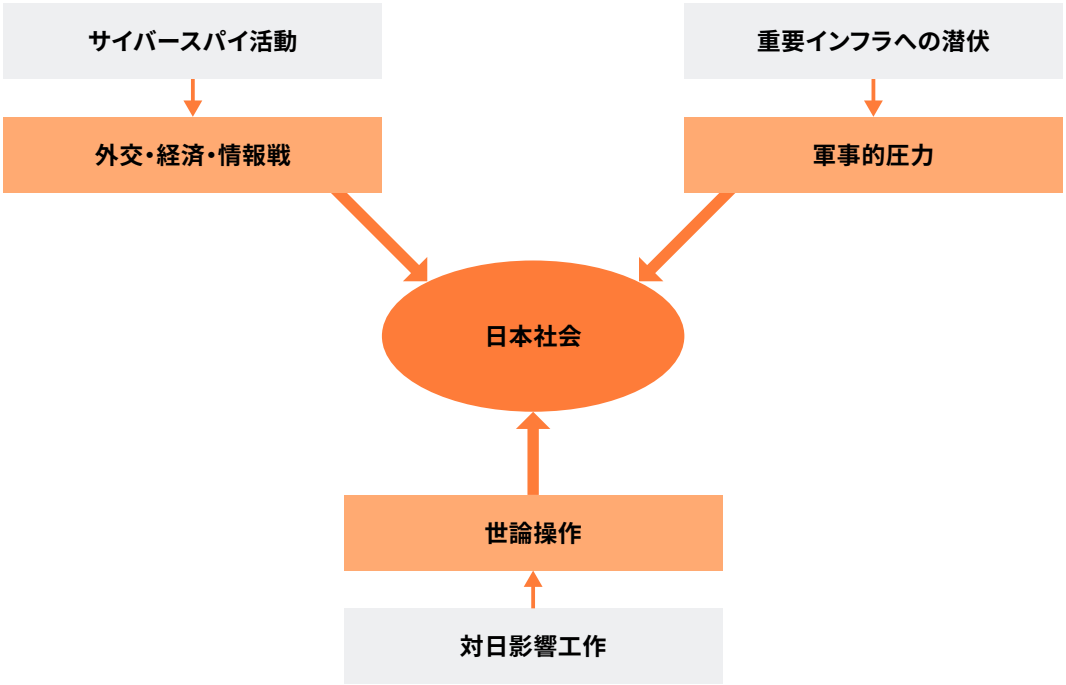
処理水やレアアース企業に対する情報攻撃に見られるように、特定産業・企業を狙ったレピュテーション攻撃は、国際市場における信頼や取引関係にも影響し得ます。AI・ディープフェイクの活用により偽情報の見分けが難しくなる中、政府・企業・メディアには、自国・自組織をめぐるオンラインナラティブの常時モニタリング、偽情報の早期検知とファクトチェック、一貫した説明、SNSプラットフォームとの連携といった体制整備が求められます。

まとめ

中国拠点の脅威アクターによるサイバースパイ活動は、安全保障や先端技術などを重視する傾向を強めており、地政学的な色彩を帯びつつあることから、日本側の制裁対応や代替調達といった政策・戦略情報も今後は攻撃対象になるおそれがあります。さらに、重要インフラへのPre-Positioningは、有事の際に電力・通信・交通などを実際に停止させる攻撃へと発展する可能性も否定できません。影響工作についても、国内世論や国際社会における日本の評判を揺さぶる手段として高度化していくと見込まれます（図表14）。

これらのサイバー上の脅威は、地政学的な緊張と相まって複合的に顕在化する可能性があり、包括的な備えが求められます。日本の官民組織は、個別のサイバー対策にとどまらず、国家レベルの戦略の中で自らの役割と備えを再定義することは、今後の重要な課題となるでしょう。

図表14：中国拠点の脅威アクターによる複合的なサイバー攻撃



出所：PwC作成

2-3.「デジタル規制」先行企業のプロジェクト体制から学ぶデジタル法規制対応

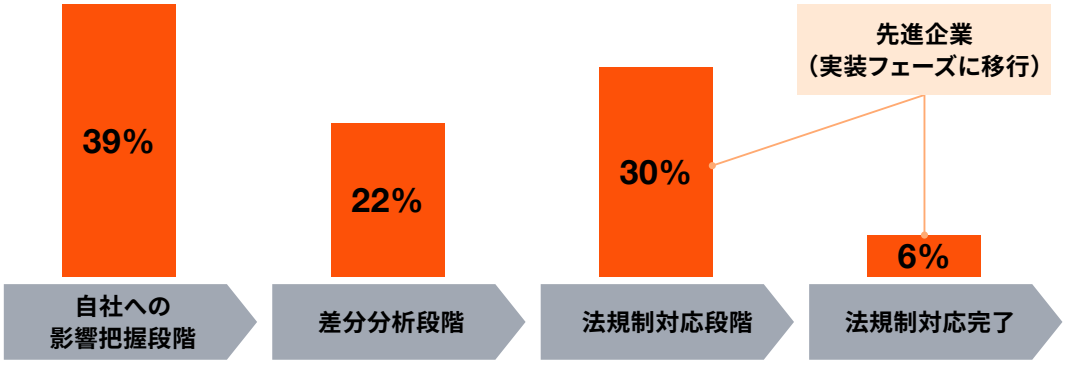
デジタル法規制対応は市場参入の前提条件

前回の「2025年 Cyber IQ調査」では、多くの日本企業がグローバルに拡大するデジタル法規制への対応に乗り出していることを確認しました。しかし、EUのNIS2指令やデータ法、米国のCMMC（サイバーセキュリティ成熟度モデル認証）に代表されるように、デジタル分野の法規制は増加傾向にあり、その内容も詳細化・具体化の一途をたどっています。日本では、経済安全保障分野におけるセキュリティ・クリアランス制度の運用開始に向け、重要経済安保情報保護活用法が2024年5月10日に可決・成立しました。また、能動的サイバー防御に関しては、2025年5月16日にサイバー対処能力強化法および同整備法が成立し、2026年10月1日までに施行予定です。こうした状況下で、単なる情報収集に終始するアプローチはもはや限界に達しています。デジタル法規制対応は、コンプライアンス順守の観点である「守り」から「市場参入の前提条件」へと位置付けが変化しており、規制対応の遅れは市場機会の損失につながるリスクが高まっています。

日本企業の3分の1が実装フェーズに移行

本調査では、デジタル法規制の準備状況やプロジェクト体制について、日本企業においてサイバーセキュリティの意思決定や企画に携わる300人を対象に調査を実施しました。まず、自社が注視しているデジタル法規制について現在どのような準備状況かを調べました（図表15）。多くの企業は、依然として「自社への影響把握段階」（39%）や、要求事項と現状の差を分析する「差分分析段階」（22%）にとどまっています。一方、「法規制対応段階」（30%）や「法規制対応完了」（6%）と回答した先進的な企業も一定数存在しました。つまり、日本企業の3分の1超が、デジタル法規制の実装フェーズに移行していることが分かりました。

図表15：デジタル法規制対応の準備状況

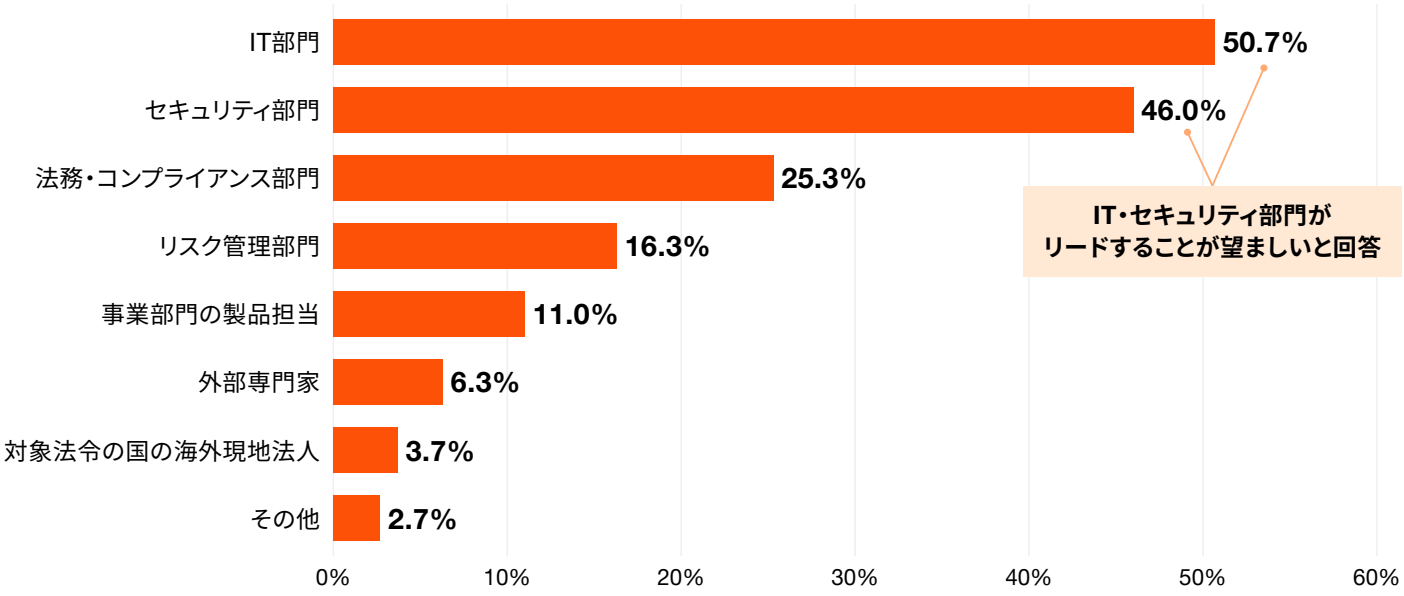


出所：PwC「2026年 Cyber IQ調査」

また、デジタル法規制対応を全社的に推進する主体としてどの部門が望ましいかを尋ねたところ、「IT部門」（50.7%）と「セキュリティ部門」（46.0%）が他を大きく引き離しています（図表16）。これらの部門は、法令対応を専門としている部門ではありませんが、システム対応やセキュリティ対応の必要性から、法令対応を主導せざるを得ない状況であると推測できます。一方、法務・コンプライアンス部門が推進すべきという回答が25.3%しかなかった理由としては、デジタル技術のナレッジや人員の不足が考えられます。

図表16：デジタル法規制対応を推進する主体

Q. デジタル法規制対応を全社的に推進する際、どの部門が主体的に推進するのが望ましいですか。（複数回答、%）



出所：PwC「2026年 Cyber IQ調査」

先進企業の事例

デジタル法規制対応において、実装フェーズに移行している先進企業には、どのような傾向があるのでしょうか。PwCが支援している事例では、共通の傾向があることが分かっています。

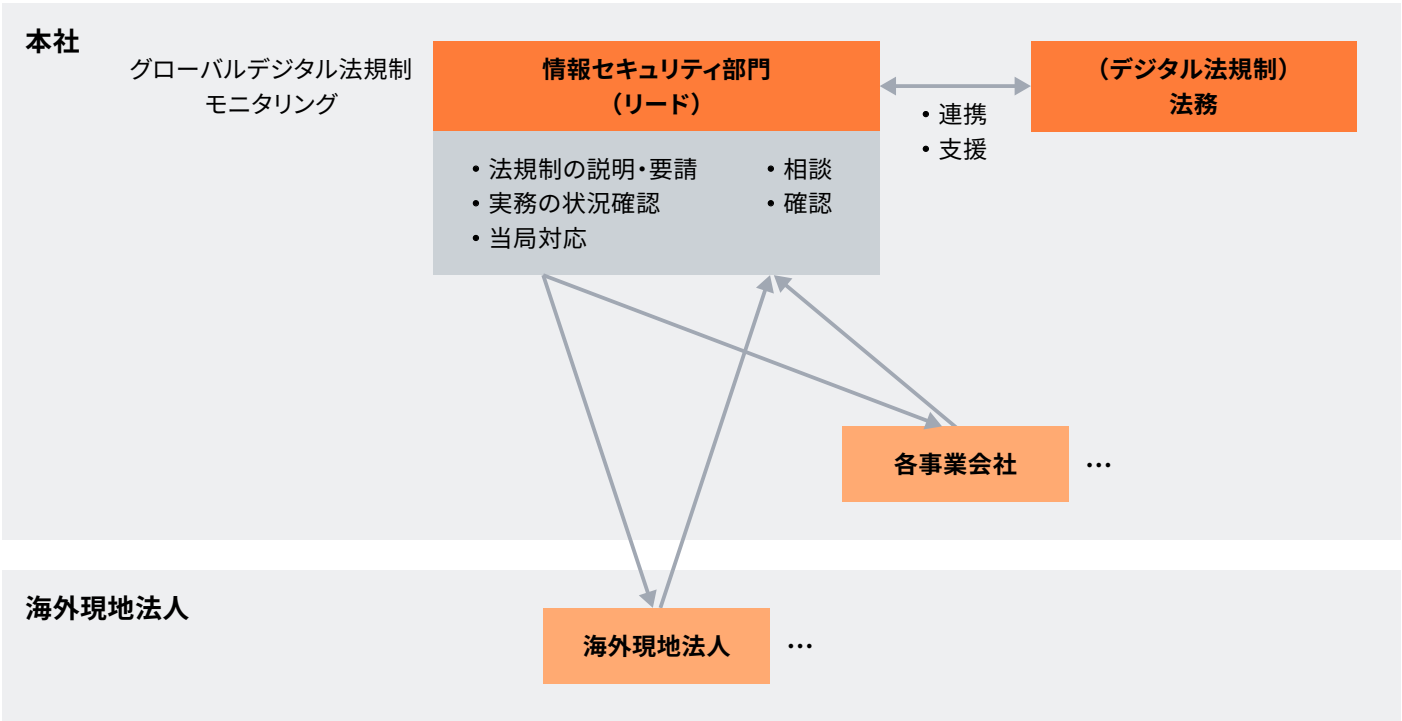
A社の事例：本社の情報セキュリティ部門がリード役となり、法務部門と連携しながら、グローバルに点在する各事業会社や海外現地法人を巻き込むプロジェクト体制を構築しています（図表17）。

B社の事例：本社の品質管理部門が法規制対応をリードし、本社の製品開発・製造部門やOTセキュリティ部門を巻き込みながら法規制対応を実施しています。

C社の事例：本社PSIRTが法規制対応をリードし、本社の製品開発・製造部門や営業部門、顧客対応部門などを巻き込みながら法規制対応を実施しています。

これらの先行事例で共通しているのは、「本社の技術部門」がデジタル法規制対応プロジェクトをリードし、「法務部門」と連携しながら、海外現地法人を含む事業部門を巻き込むプロジェクト体制を構築していることです。具体的な本社部門の役割は、デジタル法規制動向のモニタリングや各拠点に法規制の内容を説明して対応を要請すること、そして法務部門と連携した当局対応です。このように、法規制対応を事業部門や現地任せにせず、IT・セキュリティの知見を持つ本社部門が強力なガバナンスを発揮し、法務や事業部門といった関係者を巻き込みながら全社横断で推進することが、日本企業の好事例と言えるでしょう。

図表17：実装フェーズに移行している先進企業の体制例

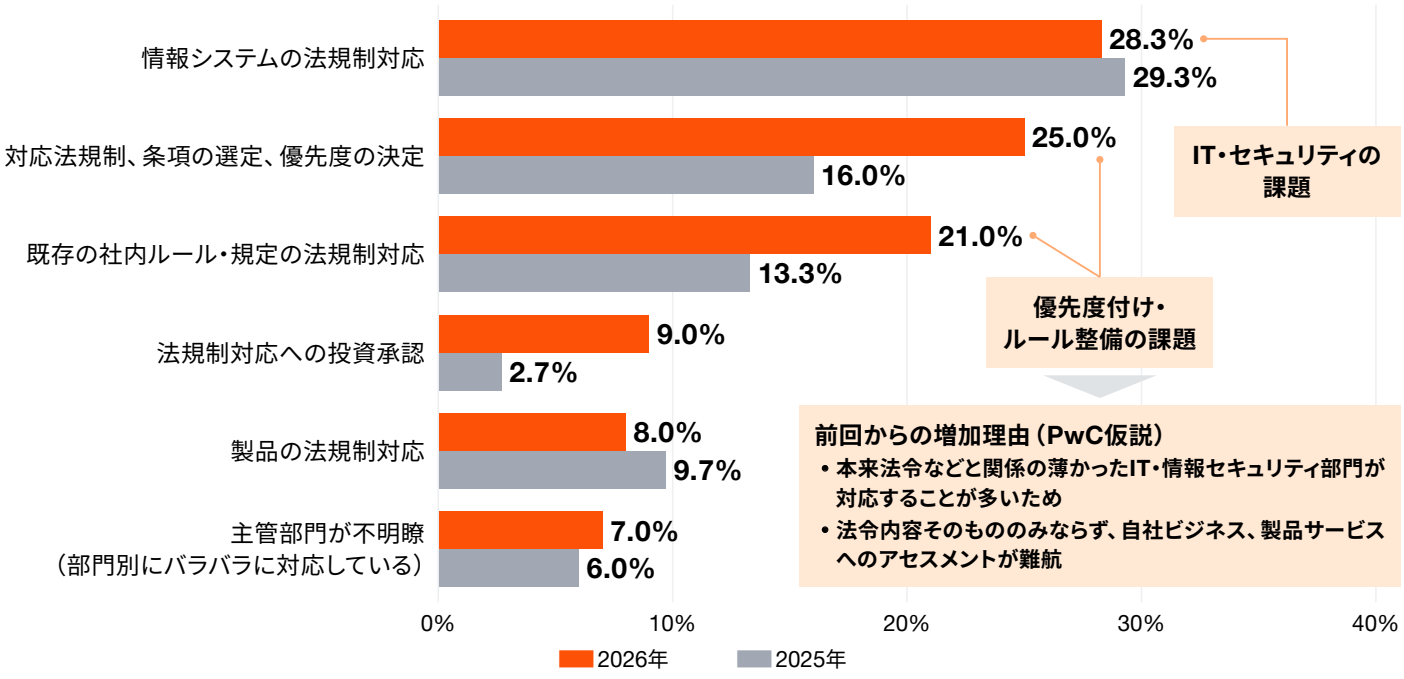


出所：PwC作成

一方、デジタル法規制の適用範囲が広くなり、内容も複雑になっていることから、さまざまな課題が発生しています。具体的には、「情報システムの法規制対応」(28.3%)、「対応法規制、条項の選定、優先度の決定」(25.0%)、「既存の社内ルール・規定の法規制対応」(21.0%)が主な課題となっています(図表18)。2025年との比較では、特に「対応法規制、条項の選定、優先度の決定」と「既存の社内ルール・規定の法規制対応」を課題と考える企業が増えています。これは本来法令などと関係の薄かったIT・情報セキュリティ部門が対応することが多いこと、デジタル法規制の規制カバレッジが広いゆえ自社ビジネスや製品サービスへの影響把握(アセスメント)や組織横断的連携体制の構築が難航していること、社内規定との整合性チェックや社内規定の改定プロセスが煩雑といったことが理由と考えられます。

図表18:デジタル法規制対応における課題

Q. デジタル法規制の対応を行う上での最大の難しさは何ですか。(単一選択、%)



出所:PwC「2026年 Cyber IQ調査」

課題への工夫・乗り越え方

デジタル法規制は、セキュア・バイ・デザイン(Secure by Design)、セキュア・バイ・デフォルト(Secure by Default)、国家安全ないし経済安全保障などの思想に基づき、その規制する範囲が広く、対応に際して企業が直面する課題は多岐にわたります。先進企業は、法対応が主業務に対して急進的な影響を与えないように、横断的な連携体制の構築や、作業効率化のためにテクノロジーの活用など、さまざまな工夫によってこれらを乗り越え、対応を前進させています。その具体的なアプローチは、「組織・プロセス」と「テクノロジー」の2つの側面に大別できます。

「組織・プロセス面での工夫」

実効性のある対応の基盤となるのは、本社主導の強力なガバナンス体制です。先進企業では、まず本社が中心となり、法務、IT、事業部門など、関連する各部門の責任と権限をデジタル法規制の要求に合わせた役割定義書として明確化します。これにより、本社部門の権限など、誰が何に責任を持つのかが明確になり、部門間の連携がスムーズになります。さらに、この体制を形骸化させないために、継続的な勉強会や教育研修を展開することも極めて重要です。これにより、全社的な知識レベルの底上げと意識の統一を図ることができます。こうした変革は一朝一夕には実現しません。ある先進企業では、外部専門家による数年間の伴走支援プログラムを導入し、定期的な進捗確認と助言を受けながら、徐々に全社的な浸透を図ったという事例もあります。

「テクノロジーの活用」

社内規程やプロセスのFit&Gap分析にかかる負荷を軽減するため、生成AIを活用したアセスメントの自動化に取り組む動きも始まっています。生成AIが規制文書と社内規程の関連性を分析・抽出し、社員は最終的な判断に集中することで、分析のスピードを飛躍的に向上させることが期待されています。

また、GRCツールなどを活用し、各国・各地域の法令要件、社内規程、統制項目を一元管理することで、グローバル拠点ごとのコンプライアンス対応状況を可視化し、順守状況の評価や未対応項目の把握を効率的に実施することが可能となります。さらに、法令改正情報や自己点検結果、各種リスク情報を継続的に取り込み、ダッシュボードによるモニタリングやアラート通知を行うことで、従来のスポット型評価から継続的なコンプライアンス管理への転換が期待されています。

まとめ

デジタル法規制対応は、従来のコンプライアンスの観点による「守り」から、グローバル市場にアクセスするための「市場参入の前提条件」（参入規制）へと位置付けが変化しています。対応の遅れは、罰則や行政対応といったリスクにとどまらず、入札・取引からの排除や新市場参入の遅延を招き、市場機会の損失につながりかねません。各国・地域において法規制の詳細化が進む中、日本企業はモニタリング中心の段階から、法規制要求と現業とのギャップを埋める実装フェーズへと、早急に移行する必要があります。

先進企業の事例を見ると、法令対応を個々の事業部門や海外現地法人に委ねるのではなく、本社のIT・セキュリティ部門、品質管理部門、PSIRTなどが社内プロジェクトをリードし、全社的な対応を統括していることが分かります。法令順守を確実に推進するためには、このような本社主導のセキュリティガバナンス体制を構築し、グローバルで一貫した方針と標準コントロールを整備することが不可欠です。

また、優先度付けやルール整備に関する課題に対しては、Fit&Gap分析に基づくアセスメントの実施が有効です。法規制要求と自社の制度・プロセス・システムとの適合状況を体系的に評価することで、自社ビジネスや製品・サービスへの影響範囲を明確化し、限られたリソースをどこに投下すべきかの優先順位付けを行うことができます。このFit&Gap分析にかかる負荷を軽減するため、生成AIを活用したアセスメントの自動化を検討することも今後有効になっていくでしょう。

一方で、欧州を中心に規制の簡素化や見直しの動きも進んでおり、今後1年程度で企業に求められる具体的な対応も変化する可能性があります。このような環境変化に対応するためには、デジタル法規制対応を一過性のプロジェクトとして捉えるのではなく、本社主導の全社的な体制構築と、部門横断的な連携を前提とした継続的なプロセスとして位置付けることが重要です。

2-4.「AIリスク・AIガバナンス」今、必要とされるAIリスクマネジメント ―AIインシデント分析からの考察―

AI利活用に関連するインシデントの傾向分析

生成AIを契機としたAIテクノロジーの進化が急速に進んでおり、ビジネスの前提も大きく変化しています。企業はAIをいかに利活用してビジネスを見直すかの判断を迫られています。こうした状況の中、AI利活用・推進に伴うリスクも増加しており、さまざまなインシデントが発生しています。本章では、実際に確認されているインシデントの傾向を交えて、今後、企業が考慮すべきリスクおよび必要となる取り組みについて考察します。

経済協力開発機構（OECD）は、2020年にOECD.AIと呼ばれるオンラインプラットフォームを立ち上げ、政策立案者、研究者、企業、一般消費者のための世界のAIイニシアチブ、動向、ガバナンスなどに関する包括的な情報を提供しています。この取り組みの一環として、プラットフォーム上では「AIM: AI Incidents and Hazards Monitor」と呼ばれるAI関連のインシデントや危害を記録したデータベースが運営・公開されています。今回、AIMに登録されているデータのうち、2022年1月から2025年9月までの3年9カ月、計9,220件を対象に、世の中で実際に発生しているインシデントの傾向を分析しました。

AI関連のインシデントは、「I. AIを悪用して攻撃が行われたケース」と「II. AIの脆弱性が狙われ攻撃されたケース」に大別されます（図表19）。以降、それぞれの詳細を確認していきましょう。

図表19：インシデント区分と件数

I. AIを悪用して攻撃が行われたケース	II. AIの脆弱性が狙われ攻撃されたケース		
	A. 従来のAI	B. 生成AI	C. AIエージェント
2,543件	38件	125件	17件

出所：OECD.AI「AIM: AI Incidents and Hazards Monitor」を基にPwC作成

I. AIを悪用して攻撃が行われたケース

Iは、サイバー攻撃者がAIを悪用して第三者にサイバー攻撃を実施したケースとなり、その件数は2,543件に上ります。AIのサイバー攻撃への悪用は日々新たなユースケースが報告されており、大きくは以下3つのパターンに区分できます。

1 人間が実施するタスクのサポート、アドバイス

2 マルウェアなどの悪性プログラムによる利用

3 人間が実施するタスクのリプレース

1は、生成AIの台頭当初から確認されているユースケースであり、サイバー攻撃者がAIを悪用して標的組織の調査を実施する、フィッシングメールやマルウェアの試作を行う、サイバー攻撃実行時のアドバイザーとして活用する、といったものです。いずれもAIの活用方法としてはベーシックなものと言え、特にフィッシングメールに関しては、言語の壁が低くなったことにより攻撃が増加しているという報告も確認されています。

2は、2024年後半から確認されており、マルウェアが生成AIを活用する機能を搭載しているケースです。侵入先システムの調査などについて、生成AIを活用することで実際の環境情報を踏まえて動的に動作を判断・生成する、といった機能が確認されています。

3は、「サイバー攻撃者＝人間」が実施していた一連のサイバー攻撃をAIが代替して、自動的に実施するというものです。こうした攻撃・評価を実施するツールの開発がアンダーグラウンドコミュニティ、サイバーセキュリティコミュニティの双方で進んでおり、今後、特に注意が必要と言えます。

上記に共通するのは、「従来、人間が質的に実現できなかったことが達成されているわけではない」という点です。ただし、規模や速度といった観点では、人間の水準を既に凌駕（りょうが）しているため、サイバー攻撃・防衛という攻防のルールが変わっていることを強く認識する必要があります。

II. AIの脆弱性が狙われ攻撃されたケース

IIは、AIのモデルやシステム・サービスに内在している脆弱性を狙い、攻撃を行うケースです。AIの利活用の発展に伴い、AIに関連するインシデントは急激に増加しています。詳細を確認するために、これらのインシデントを、「A. 機械学習などの従来のAI」、「B. 生成AI」、「C. AIエージェント」に区分して整理します。

A. 機械学習などの従来のAI／B. 生成AI

機械学習などの従来のAIに関するインシデントが2023年～2025年の3年間で20件程度であったのに対して、生成AIに関するインシデントは、2023年の単年のみで30件に上ります。これは一過性の状況ではなく、2024年以降もインシデントは増加を続け、わずか2年後の2025年には64件と、初年度の2倍を超える水準に達しました。

これは、従来のAIを利活用する際には一定のリテラシーが求められていたことに対して、生成AIの台頭を機に、AIの民主化が急速に拡大していることを裏付けていることに他なりません。もはや、生成AIを利活用する際に、以前のようなAIリテラシーは必要とされなくなりました。これを、リスクマネジメントの言葉で言い換えると、生成AIの台頭により、AIリスクを閉じ込めていた堅牢（けんろう）な壁が崩壊し、そこからリスクが急拡大したことになります。生成AIはその利便性ゆえにプラスの側面が注目されることが多いですが、利活用に伴うリスクを認識し、利活用とリスクマネジメントの両輪で、安心・安全な利活用を促進していくことが求められているのです。

C. AIエージェント

一方で、AIエージェントに関連するインシデントは20件に満たず、相対的に少ないことが確認できます。これは、生成AIと比較すると、AIエージェントはリスクがないということを意味しているのでしょうか。残念ながらそうではありません。AIエージェントの利活用がまだ発展途上にあり、運用上のユースケースも限られていることから、関連するインシデントが顕在化していないのだと考えられます。逆に言うと、今後、AIエージェントの本格的な利活用フェーズを迎えると、付随するインシデントも急拡大することが想定されます。

AIに関連するインシデント事例

それでは、実際にどのようなインシデントが発生し、それらのインシデントを未然に防ぐためには何が必要だったのかを考察します。

インシデント事例1（B. 生成AIへの攻撃）

AIモデルやシステム、サービスに脆弱性があり、AIモデルが保持している個人情報や機密情報への不正アクセスを許してしまう事例はこれまでも多く発生していました。

具体例としては、チャットボットに共有されたリンクがユーザーの同意なく検索エンジンに自動的に登録され、数十万件という膨大なユーザーの会話が意図せずに公開されてしまった事例が挙げられます。

このようなインシデントを未然に防ぐためには、設計工程において、検索エンジンによるクローリングを想定した上で、共有リンクのデフォルト設定を非公開にするというアクセス制御が必要であったと考えられます。利便性を優先するあまり、プライバシー保護の設計が後回しにされた可能性が指摘されています。また、当該インシデントが外部の検索エンジン起因で発覚していることから、リリース後の内部リスク管理・モニタリングの強化も必要であったと推察されます。

インシデント事例2（B. 生成AIへの攻撃）

生成AIモデルの脆弱性を悪用してセーフガードを回避し、暴力的、もしくは悪意あるコンテンツを生成させる、化学兵器の作り方など犯罪を助長しかねない内容を回答させるなどの事例が非常に多く確認されています。

具体例としては、画像生成AIを利用して、著作権で保護されたコンテンツや学校での銃撃など、攻撃的で潜在的に有害な画像を生成していると、知的財産権や人権保護の観点で指摘を受けた事例が挙げられます。

このようなインシデントを未然に防ぐためには、設計工程において、多層的ガードレールを導入し、プロンプトの適切性を自動的に判断した上で後続処理の分岐を実装する必要があったと考えられます。また、実装工程においては、偽・誤情報の拡散を防ぐという意図においては、生成物にウォーターマーク（電子透かし）を付与し、保存・共有経路での改変検知を実現することも有効です。

インシデント事例3（B. 生成AIへの攻撃）

人間には不可視の内容を画像やテキストに埋め込みプロンプトに命令することで、自らに都合の良い結果となるようにモデルを操る事例が確認されています。

具体例としては、人材採用支援AIの脆弱性を悪用するというケースが挙げられます。求職者が自らの履歴書を作成する際に、履歴書の枠外に極小サイズかつ白文字などを記載して、自らの経歴を詐称するような命令を埋め込むことで、不当に高い評価を得ていたという事例です。

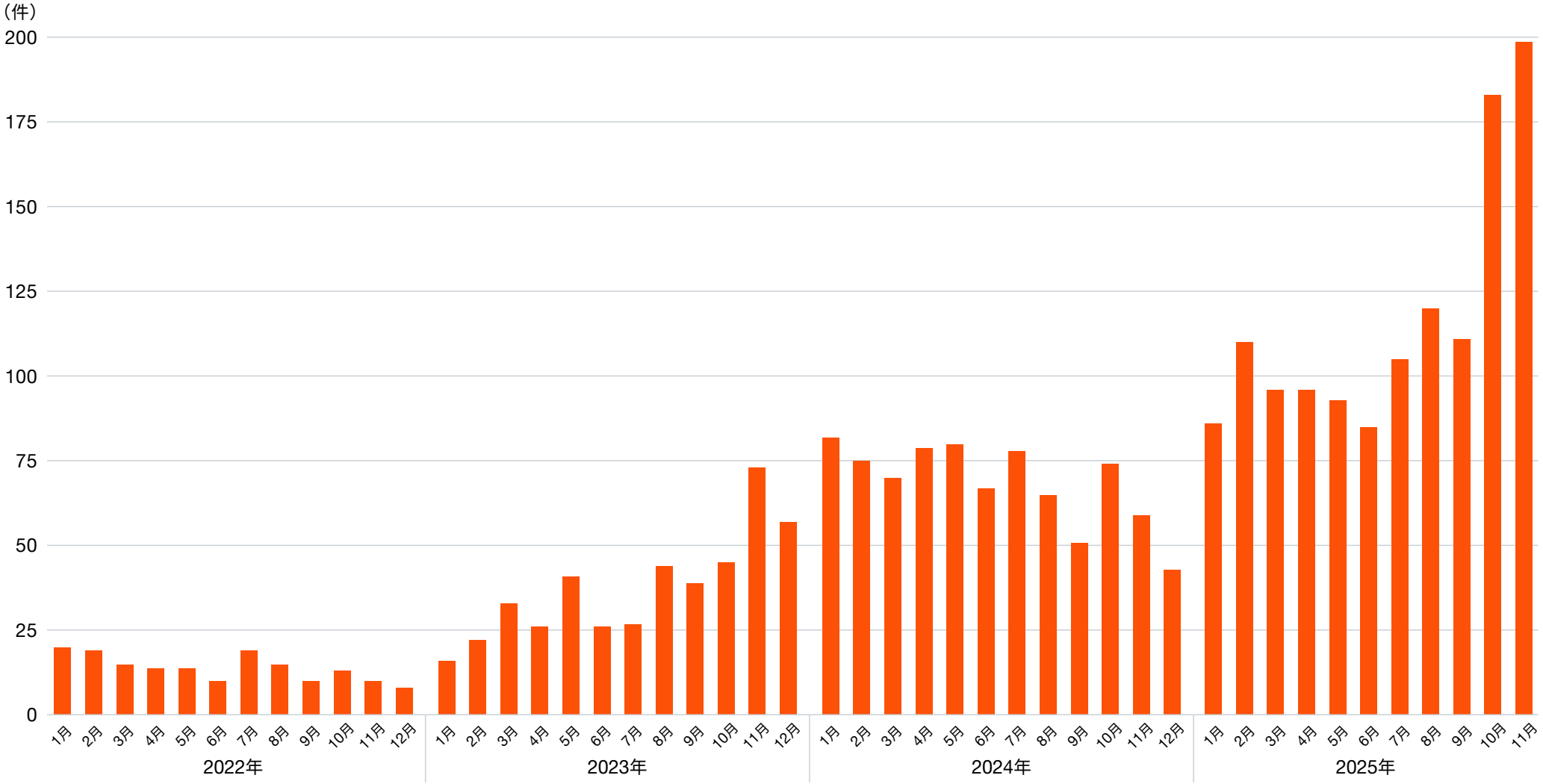
このようなインシデントを未然に防ぐためには、AIの設計工程において、AIが意図的に悪用されるリスクを想定し、履歴書のような非構造化データから悪意のある隠しコマンドを検知・無効化する仕組みを考慮することが必要でした。そして、実装工程においては、履歴書を解析する際に隠されたテキストや特殊な書式によるプロンプト・インジェクション攻撃への対策を実装することが不可欠であったと考えられます。一方で、これらの対策をもって盤石であるとは言えず、運用工程においても、AIによって出力された結果に対する取り扱い方針の策定と当該方針に従った運用プロセスを整備・実施していくことが求められます。

インシデント事例4（AIを悪用した攻撃）

AIを活用し、攻撃手法が高度化する事例も確認され始めています。例えば、AIがディープフェイクや音声クローンを生成し、これを用いることで音声認証システムを迂回（うかい）する事例も出始めています。

攻撃手法が高度化していく中でインシデントを未然に防ぐ難易度も高まっています。インシデント事例1～3のようにAIを開発する事業者のみ、あるいはAIを利活用する事業者のみで対策を講じることに限界があるのかもしれません。AIモデルを開発する事業者の責任、開発されたモデルを安心・安全に利活用・運用する事業者の責任というように、AIライフサイクル全般を通して、各ステークホルダーと連携し、協業していくことで初めて、攻撃手法が高度化していくAI関連インシデントを抑制することが可能となるのです。

図表20：インシデント発生件数推移



出所：OECD.AI「AIM: AI Incidents and Hazards Monitor」を基にPwC作成

AIやエマージングテクノロジーの利活用を促進するリスクマネジメント

前節で確認したとおり、AIの利活用には多くのリスクが内在し、すでにその多くがインシデントとして顕在化しています。しかし、それゆえにAIの利活用にブレーキをかけてしまうこともリスクであるということを忘れてはいけません。現在の、そして今後の経営環境においては、AI利活用はますます必要不可欠となり、AI利活用に躊躇（ちゅうちょ）することは企業の競争力低下やイノベーションを阻害してしまうことになるのです。

それでは、AIリスクをマネジメントしていくためには、どのような取り組みが必要となるのでしょうか。PwC Japanグループは、AIを安心・安全に利活用するために、以下の8項目による取り組みが重要と考えています（図表21）。

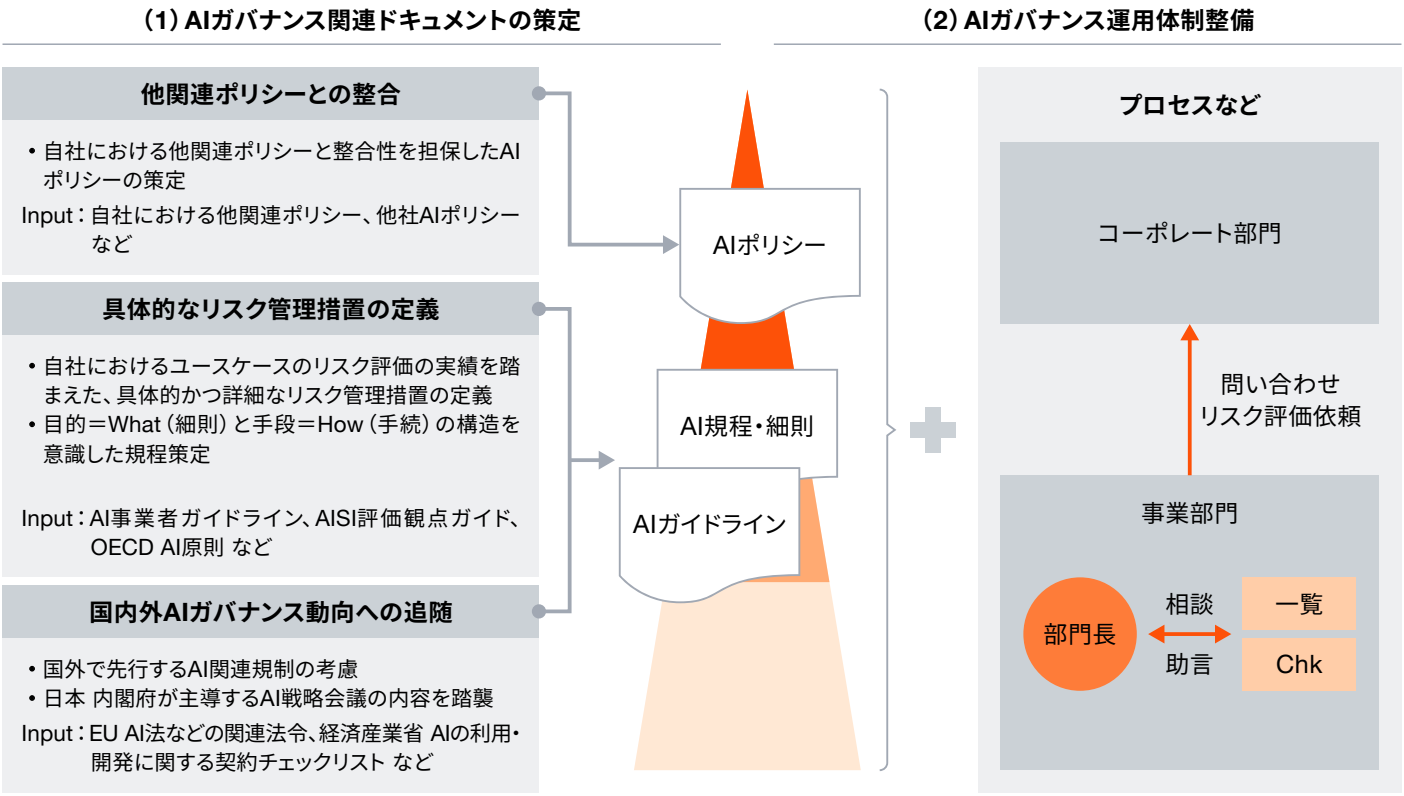
図表21：AIガバナンスを実現する8項目

#	種別	AIリスク対策	実施内容
1	―	現状調査	• AI利活用状況調査 • AIリスク観点とリスクレベル整理 • AIユースケースの類型化とリスク評価
2	人・組織	AIドキュメント策定	• AIポリシー（社外）やAIガイドライン（社内ルール）策定
3		AIガバナンス体制構築	• AIリスク所管部門の整理 • 事業部門やコーポレート部門の役割と責任の整理 • 第三者委員会など、社外有識者を含めた体制検討
4		AI人材育成	• AIガバナンス教育コンテンツの策定 • 全社的な理解促進のための研修実施
5		AIモニタリングプロセス整備	• AIサービスのレビュープロセス整備 • AIリスク観点に関する運用プロセスやチェックシートの策定
6	技術	AIモニタリングツール導入	• AIモニタリングツール導入に向けたPoCの実施 • AIモニタリングツールの導入とモニタリングプロセスの策定
7		AIレッドチームによる診断	• 疑似攻撃によるAIサービス・モデルの脆弱性評価 • 評価結果に基づく是正計画の策定と実行
8	―	継続的改善	• AIリスク対策 #1～#7の定期的見直しと改善 • 継続的改善を実施するプロセス整備

出所：PwC作成

現在、日本における多くの事業者はAIポリシーやガイドラインなどの整備を進めていますが、残念ながら当該ドキュメントの整備をもって盤石なガバナンスを構築することは困難です（#2）。これらのドキュメントを効果的・効率的に運用していくための体制構築（#3）や人材育成（#4）などが必要とされます。特に、AIに関連するリスクは、セキュリティや法務、コンプライアンスなど多岐にわたることに加えて、AI特有の新たなリスクも存在するため、コーポレート部門における役割と責任をどのように定義するかは、非常に難易度が高い課題となります。さらに、コーポレート部門と事業部門、統括会社と国内外グループ会社との責任分界点など、体制構築（#3）においては、整理すべき論点が少なくありません（図表22）。ただし、難易度が高いからと先送りにする猶予はもはや存在せず、AIの安心・安全な利活用を促進していくためには待ったなしの局面を迎えているのです。

図表22：AIガバナンス態勢構築



出所：PwC作成

AI／生成AIで培われたリスクマネジメント手法は、AIエージェントに対しても有効であると考えられます。一方で、AIエージェントの利活用は依然として発展途上にあるため、将来的なユースケースを踏まえて、リスクマネジメント手法もアップデートしていくことが不可欠です。AIエージェント利活用のステージを見極めながら、リスクベースアプローチに従った緩急ある対策を策定し、講じていくことが重要です。加えて、AIエージェントが有する人的作業の代替性という性質を加味し、業務統制的観点の考慮も必要になります（図表23）。「戦略」「組織」「人材」「プロセス」「基盤」の5つの観点から、AIエージェントに対するリスクマネジメントを検討することで、企業の業務効率化や競争力強化に寄与することが可能となるのです。

図表23：AIエージェントに対する業務統制的観点

出所：PwC作成

ただし、AIエージェントは、デジタル処理において人的能力をはるかに凌駕します。今後ますます普及していくであろうAIエージェントネイティブなプロセスを統制するためには、現状のリスクマネジメントの範囲では立ち行かなくなる懸念があり、AIエージェントが他のAIエージェントを管理するといった新たなガバナンス技術の発展が期待を集めています。

AIエージェントにおけるリスクマネジメントはAI／生成AIの延長線上にあり、新たな技術領域に直面した際に、まったく新しいガバナンスモデルを構築することは適切ではありません。似て非なるガバナンスモデルが乱立すると、当該技術を利活用する際の負荷が高まり、技術動向に追随するという競争力の源泉が阻害されてしまいます。また、セキュリティや法務などのコーポレート部門間の連携も複雑さを増し、対策の重複というムダのみならず、対策の抜け漏れなど、思わぬ落とし穴に陥る懸念も伴います。経済産業省は、ガバナンスモデルの乱立を防ぎ、ガバナンス自体をガバナンスするという「ガバナンス・オブ・ガバナンス[2]」を提唱しています。生成AIからAIエージェント、そして、今後、連続的に台頭してくるであろう未知のエマージングテクノロジーの利活用を見据え、日本の事業者は、全体最適が実現されたガバナンスへのトランスフォーメーションに今から着手することが必要とされているのかもしれません。

生成AIがもたらしたAIの民主化、AIエージェントによる自律的な相互連携と意思決定の実現。5年前には考えもしなかった経営環境が、今、現実のものとして形作られようとしています。ここ数年は、技術変化に追随する過程でひずみが生じ、結果として多くのインシデントが発生しています。これらの経験を過去の出来事として終わらせず、未来への学びに変えていく必要があります。そのうえで、生成AI／AIエージェントのさらなる利活用を促進し、一事業者の枠を超えて、国際的な競争力を強化すると同時に、今後発生する技術変化も積極的に受け入れ、安心・安全な利活用をリードしていく、リードしていく。そのようなガバナンスモデルを構築していくことが、今の日本の事業者には期待されているのです。

2「Society5.0における新たなガバナンスモデル検討会」
https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/index.html

おわりに

パクスアメリカーナを前提とした安定した国際秩序は、もはやサイバーセキュリティの前提条件ではありません。国境、政治、価値観の違いは、サイバーリスクの形を変え、攻撃者に新たな機会を与えています。こうした環境において企業に求められるのは、過去の対策をなぞることではなく、変化を前提とした意思決定です。自社の事業と地政学的リスクの関係を理解し、情報を継続的に収集・分析することでCyber IQを高めることが、サイバーリスクの影響を抑え、事業のレジリエンスを維持する鍵となります。

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界137の国と地域に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

発刊年月：2026年7月　　管理番号：I202603-13