地政学的緊張とサイバー脅威：米国関税の潜在的影響

2025年6月

Ilaria Sangalli, Index Research Lead

不確実性を乗り越える：米国の関税が世界貿易とサイバーセキュリティに与える影響

4月2日、米国は主要な貿易相手国に対して関税を課すと発表しました。

この関税措置は、特に中国、カナダ、メキシコ等の国々と米国との貿易戦争が激化する可能性を示唆し、こうした動きから投資家の間では、報復措置によって世界貿易や経済成長がさらに阻害されるのではないかという見方が強まりました。貿易摩擦は国家主体による報復措置を招く可能性もあり、その中にはサイバースパイ活動やサイバー攻撃も含まれます。このような脅威は、政府機関だけでなく民間企業にも深刻な影響を及ぼすことが懸念されます。

また、サイバーリスクの増加に加えて、新たに課された貿易障壁に対応するためにサプライチェーンを適応させる必要が生じることで、企業は、コストの拡大や物流上の課題に直面する可能性があります。

その後、4月9日に発表された90日間の一時停止措置、5月8日の英国との貿易協定、そして5月12日の中国との暫定合意が、市場の回復を後押ししました。とはいえ、最近の通商協定や一時的な関税停止にもかかわらず、企業にとって先行きが不透明な状況は変わっていません。というのも、これらの措置は暫定的なものであるため、その影響を完全に見極めるには時期尚早だからです。そのため、企業はサプライチェーンの大幅な見直しには依然として慎重であり、安定性と予見可能性の改善の兆しを探っています。さらに、サプライチェーンの調整の複雑さと、新たなサイバーセキュリティの脆弱性が生じる可能性が相まって、企業の慎重な姿勢にますます拍車がかかっている状況です。

地政学的緊張や関税紛争に乗じた政治的動機によるサイバー攻撃の増加

地政学的緊張と高度化するサイバー脅威が高まる時代において、世界各国はこれまでにない安全保障上の課題に直面しています。ユーロポール[1]の最新の報告書では、犯罪組織との「シャドーアライアンス（影の同盟）」を通じて活動する、EUを標的とした国家支援型のハイブリッド脅威アクターが増加していることが明らかになりました。これらのアクターは、サイバー攻撃、データ窃取、偽情報の拡散、重要インフラの破壊など、多様な手段で社会の攪乱を図っています。ユーロポールは、現在の地政学的な情勢が、脆弱性を突き、偽情報を広める好機を脅威アクターにもたらしているといいます。

1　ユーロポール（欧州刑事警察機構）はEUの法執行機関です。EU加盟国が国際的かつ組織的な重大犯罪、サイバー犯罪、テロの防止と対策を支援することを使命としています。

この報告書では、ロシアをハイブリッド脅威アクターと明言してはいないものの、「ロシアおよびその影響圏にある国々から、重要インフラや公共機関に対する政治的動機によるサイバー攻撃が増加している」と述べられており、この地域からの活動がハイブリッド脅威の手法と一致していることを示唆しています。[2,3]

これを受けて、欧州委員会は高度なサイバー攻撃に対抗するためのセキュリティプロトコルの強化を計画しており、ユーロポールの人員と予算を倍増させる方針です。この戦略的な取り組みにより、官民両セクターにおけるサイバーセキュリティへの支出が拡大し、サイバーセキュリティ関連の製品やサービス、そして最先端の脅威検知ソリューションへの需要が高まると見込まれています。

地政学的緊張と密接に関連したサイバー作戦の増加も、近年の主要な傾向として、マイクロソフトの「Digital Defense Report 2024」の中で指摘されています。同レポートによると、サイバー犯罪組織は国家主体のグループと連携し、ツールや手法を共有して目的の遂行を狙っています。この協力関係により、ロシアだけでなく、中国、イラン、北朝鮮のアクターも関与する大規模なサイバーインシデントが世界中で発生しています。

また、マイクロソフトは、前回の米大統領選挙戦期間中に、選挙関連のホモグリフドメインの増加も検出しました。これは正規のリンクによく似せて作られた偽のドメインで、ユーザーを欺くことを目的としています。脅威アクターはこれらのドメインを利用してフィッシングやマルウェアを仕掛け、機密情報を盗み取ったり、システムに障害を与えたりすることがあります。マイクロソフトによると、こうした活動の背後には、金銭的利益を狙うサイバー犯罪者と、政治的目的を追求する国家主体のアクターの両方が存在するようです。[4]

米中間の対立を中心とする最近の関税摩擦を受け、サイバー攻撃のリスクが高まることが予想されます。また、貿易戦争や制裁、関税といった経済摩擦は、サイバー空間での対立を助長し、組織にとってのセキュリティリスクを一段と高める恐れがあります。実際にこうした現象は、2018年の米中貿易戦争の際にも確認されており、中国の国家支援を受けた勢力によるサイバースパイ活動が顕著に増加しました。[5]さらに、貿易戦争はサイバーアクティビズムを誘発する可能性もあり、民族主義的なハッカーが敵対勢力と見なす相手に対して独自に攻撃を仕掛けることがあります。

国家が関与するハイブリッド脅威の拡大と、現在の地政学的緊張の高まりは、強固なサイバーセキュリティ対策の重要性がもはや否定できない水準に達していることを明確に示しています。最近の関税紛争に起因する潜在的なサイバーリスクの増加によって、警戒の強化と予防的なサイバーセキュリティ対応の必要性が改めて浮き彫りになりました。

グローバルなサプライチェーンに潜むサイバーセキュリティのリスク

最近の米国による関税措置は、世界中の企業に深刻な先行き不透明感をもたらしています。今回の関税は、将来の事業運営に対して重大な難題を突き付ける恐れがあり、企業はサプライチェーン戦略の抜本的な見直しを迫られかねません。これに関連して行われるいかなる見直しも、企業自身と、そのグローバルなサプライチェーンのサイバーレジリエンスに長期的な影響を及ぼす可能性があります。

もっとも、現時点ではこれらの影響の全容を見通すには早計であり、今後の関税の展開とその波及効果について、なお多くのことを見極める必要があります。

企業は、サプライチェーン構造の見直しという複雑で長期的なプロセスにおいて、新たなサプライヤーの評価、契約の再交渉、物流ネットワークの再構築を慎重に進めていかなくてはなりません。こうした移行期間中には、とりわけ新規の取引先のセキュリティ基

2 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

3 ポーランド内務省事務次官によると、最近の病院に対するサイバー攻撃は国家主体の犯行で、数時間にわたって医療サービスが妨害されました。また、リトアニアの検察当局は、昨年夏にヴィリニュスのイケア店舗で発生した放火事件について、ロシアの軍事情報機関（GRU）が関与していたと非難しています。
https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol#%3A~%3Atext%3DThe%20Europol%20report%20also%20warns%2Cout%20hacking%20and%20cyber%2Dattacks

4 https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/

5 https://www.secureworld.io/industry-news/trade-wars-us-tariffs-cyber-risk

準にばらつきがある場合や、十分な検証を行わずにシステムを統合した場合に、脆弱性が生じる可能性があります。このように一貫性を欠くセキュリティ体制や検証不足のシステム統合が新たな脆弱性を招く恐れがあり、それが脅威アクターによって悪用されることで、サイバー攻撃のリスクを一層高めることになります。

こうした脆弱性への対応の重要性は、最近の調査結果からも明らかになっています。世界経済フォーラムの「WEF Global Cybersecurity Outlook 2025」サーベイで、大企業の54%が、サイバーレジリエンスを実現する上で最大の障壁となっている問題としてサプライチェーンの課題を挙げました。昨今はサプライチェーンがより複雑化し、グローバルなつながりやテクノロジーへの依存が高まっているため、サプライチェーン全体に内在する脆弱性が表面化しています。[6]

今日のサプライチェーンには、サプライヤー、製造業者、流通業者、小売業者など、さまざまなステークホルダーが関わっており、それらが複数の国や地域にまたがって連携しながら機能しています。そのため、一つの脆弱性、例えば接点が一カ所侵害されるだけで、全体のエコシステムに多方面にわたる影響を及ぼす可能性があります。サイバー犯罪者は、ソフトウェアベンダー、オープンソースソフトウェア、クラウドサービス、ハードウェア供給業者といった第三者のベンダーやサービスプロバイダーを標的にすることで、複数の企業に侵入することができます。以下は2024年11月に実際に起こった事例です。サプライチェーン管理ソフトウェアのプロバイダーであるブルー・ヤンダーがランサムウェア攻撃の標的となり、スターバックスUKやスーパーマーケットチェーンのモリソンズ、セインズベリーズなど、多くの顧客が被害を受けました。この攻撃が原因でシステム障害が発生し、これらの企業は手作業での業務や緊急対応策を余儀なくされました。2025年1月期の四半期決算で売上成長率が前四半期の4.9%から2.1%に減速したモリソンズは、その一因として、クリスマス期間中に適正な在庫水準を維持できなかったシステム障害の影響を挙げています。

また、今なお最も深刻なインシデントの一つとされているのがソーラーウィンズへの攻撃です。[7] 2020年12月、ハッカーはソーラーウィンズのソフトウェアアップデートを侵害し、その経路を通じてマルウェアを顧客に送り込み、米国政府機関や有力企業を含む数多くの組織のシステムにアクセスすることに成功しました。この出来事は、サプライチェーンのセキュリティにおける脆弱性と、こうした攻撃がもたらし得る広範な影響を浮き彫りにし、社会に大きなインパクトを与えました。ソーラーウィンズの事案以降、サイバー犯罪者によるサプライチェーン組織への攻撃が一段と活発化しています。サプライヤー1社を侵害するだけで複数の組織にアクセスできる可能性があるため、サプライチェーン攻撃は攻撃者にとって非常に収益性が高く、影響力の大きい手法です。

サイバー犯罪者によるサプライチェーン上の接点への攻撃が増加する中、企業にとっては、自社内のセキュリティ強化にとどまらず、取引先のセキュリティ対策を厳しく評価し、必要な強化策を講じることが不可欠です。とりわけ、最近の関税措置や、潜在的なサプライチェーンの長期的混乱を見据えた対応を取らなければなりません。グローバル化が進む現代においてサイバーレジリエンスを実現するためには、サプライチェーン全体のエコシステムにわたる脆弱性に対応する、包括的なアプローチが求められます。

出所：ナスダック・インデックス・リサーチ、ブルームバーグ、ファクトセット

6 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

7 IT管理ソフトウェアのプロバイダー