新領域安全保障研究所 2024 年
委託研究　要旨

日本企業が直面している影響工作の脅威

～SNS（X）のハッシュタグとボットの株価への影響～

新領域安全保障研究所代表取締役　齋藤孝道

中国国家安全部の関与するサイバー分野における影響工作の研究

株式会社サイント　岩井博樹

日本企業が直面している影響工作の脅威

～SNS（X）のハッシュタグとボットの株価への影響～

《エグゼクティブサマリー》

近年、SNS やメディアを利用した影響工作による世論操作や偽情報の拡散が深刻な問題となっている。特に、悪意の情報拡散が企業の株価を意図的に操作する手段として利用されることが懸念されている。過去の研究では、SNS の投稿内容と株価の変動の間に有意な関連が見られ、ボットによる大量投稿がその原因の一部であることが示されている。

本研究では、「企業に対して意図的な干渉を行う脅威が存在し、その兆候は株価操作を目的とした SNS 上でのボット活動などに現れている可能性がある」という仮説に基づき、下記の検証・提言を行った。

・上記結果から可能性のある影響工作主体についてのアトリビューション
・検知と対策についての提言

1. 8 つの事例について、SNS（X）上における株価とボット、ハッシュタグ利用の関係

その結果、SNS（X）上における株価とボット、ハッシュタグ利用には有意な関係があり、意図的に操作することが可能であることがわかった。そのような操作が行われていた場合、調査対象とした SNS(X)のみでなく、他の SNS やオフラインでの影響工作も含んだハイブリッドな作戦であり、SNS（X）はその兆候と考えられる。

特定の企業に関する SNS（X）上の炎上、8 ケースに注目し、特にハッシュタグの使用状況やボットアカウントの割合、そしてそれらが株価変動にどのような影響を与えているかを分析した。

以下の表に、対象とした 8 ケースにおけるポスト数、ボットの数、ハッシュタグの状況と炎上後の株価の変化について動きの様子を示す。（本報告書では、データセットの欄は具体的な炎上を特定される情報が記載されている。）

	不買運動						その他	
データセット	A	B	C	D	E	F	G	H
ピーク時のポスト数	80,000	1,300	8,000	40,000	800	6,000	350,000	25,000
ボットアカウントの割合	0.351	0.349	0.381	0.26	0.355	0.294	0.255	0.215
1 ポストあたりのハッシュタグ数	1.99	2.04	2.32	1.62	2.93	1.06	0.52	0.22
関係ないハッシュタグ	有	有	無	有	無	-	-	-
値下がりの時系列パターン	ポストの後	ポストの後	ポストの後	ポストの前	ポストの後	-	ポストの前	ポストと同時

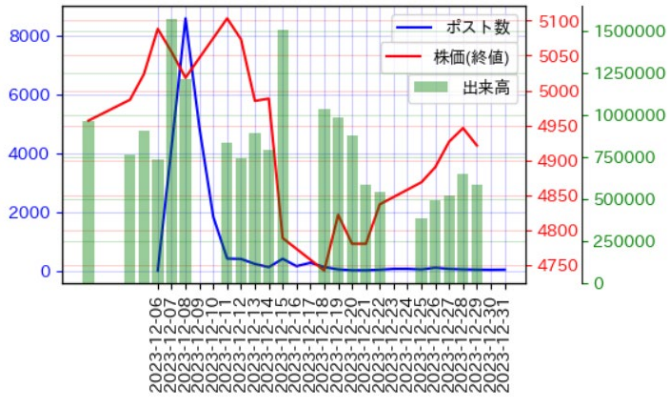
※「ピーク時のポスト数」の数値はおおよその値

その結果、不買運動など、特定企業を標的とした協調的な活動において、**特定のハッシュタグを使った情報拡散や、大量のボットアカウントを利用した意図的な情報操作が確認された**。調査対象のうち半数の**4つのケースでは、影響工作により、企業の評判に悪影響を与え、最終的には株価にも大きな影響を与える可能性があることが示唆**された。

株価操作を狙った影響工作は、週末など閲覧される可能性の高いタイミングを狙って開始され、ボットやハッシュタグを駆使して拡散が試みられる。偶発的なものを除き、炎上を人為的に起こすのにはコストが掛かるので、影響工作を行う者は利害関係者である可能性が高い。また、「ここぞ」の時に炎上を起こされる。よって、それを踏まえた事前の対策が求められる。

影響工作が観測されたケースの例

以下の図は、食品の CM に起用したタレントに関連する炎上の際の株の値動きを示す。閲覧者が増える**週末に一気に関連投稿が増え炎上**した。翌週、**ネガティヴなマインドが株価下落に影響**を与えた可能性がある。



2. 影響工作主体のアトリビューション

SNS の操作には多大なコストと知見が必要である。そのため、**影響工作の主体は、株価の変動から利益を得ることができ、影響工作の知識を持って計画的に実行できる**（もしくはその能力を持った組織に委託できる）ものと推定される。

これらの条件を満たす主体には、たとえば下記が挙げられる。あくまで一例であり、他にも可能性のあるアクターが存在する。

・外資系ファンド　日本国内には影響工作を実施するための知見を持ち、巨額の資金を動かせる主体は限られるが、海外にはそうした主体が日本よりも多く影響工作の委託先も多数存在する。

多くの大手日本企業はすでに SNS リスニングなどのサービスを導入しているものの、総合的な影響工作には脆弱であり、ネット以外のメディアの利用、経営者への個人攻撃など多彩な方法を駆使された場合、対処できない場合も多い。

・我が国に干渉する敵対国　我が国に干渉する敵対国は複数存在し、それらの国の影響工作の能力は我が国より高く、必要があれば充分な資金を投入できる。わが国の特定の企業や産業にダメージを与える。国際的なレピュテーションを下げるなどの目的のためにこうした影響工作を行う可能性が考えられる。

ただし、経営にダメージを与えたり、レピュテーションを下げたりすることは当然ながら多くの注目をあつめるため、日本政府やメディアなどによる調査が行われ、アトリビューションが特定されるリスクが高い。あらかじめ主体が特定されることを想定したうえで攻撃してくるのは、たとえば台湾併合にそなえてゆさぶりをかける場合や、日本のウクライナ支援にゆさぶりをかけるような場合が‘考えられる。KADOKAWA へのサイバー攻撃がロシアからのシグナリングという可能性と同様である。

3. 検知と対策

検知と対策には、定常的な早期警戒システム、リスクマネジメントチームが必要であり、社外の専門機関との連携も不可欠となる。

早期警戒システムには、前項に書いた外資系ファンドや敵対国などの動向を常時把握しておくことも含まれる。いわゆるインテリジェンスに類する情報収集と分析が必要になってくる。

本調査研究は、株式会社新領域安全保障研究所から資金提供を受けて行ったものである。

新領域安全保障研究所　代表取締役
明治大学理工学部情報科学科・教授、博士（工学）
明治大学サイバーセキュリティ研究所・所長
レンジフォース株式会社・代表取締役
齋藤孝道

中国国家安全部の関与するサイバー分野における影響工作の研究

《エグゼクティブサマリー》

本研究では、中国の国家安全部（MSS）が関与するサイバー領域における影響工作について調査した。MSS は対外諜報活動や政治的安全保障に関わる業務で知られているが、以前から政治家などエリート層への影響工作にも従事していることが確認されている。近年では、公安部（MPS）と連携し、デジタルプラットフォームやソーシャルメディアを利用した情報操作が活発化している可能性がある。その手法の進化は IT 技術の発展とともに加速しており、特に偽情報の拡散や影響力のある SNS アカウントの乗っ取りが新たな戦略として採用されている。

1つ目の調査では、情報配信プラットフォームを利用した影響工作について紹介する。韓国NCSCやトロント大学のCitizen Labが報告したPR企業を利用した影響工作キャンペーンと類似性のある、未認知のメディア配信企業を通じた影響工作キャンペーンを発見し、調査分析を行なった。その結果、これらのメディア配信プラットフォームはテンプレート化されたウェブサイトを用いることで、大量のコンテンツが生成されていた。また、日本語のコンテンツには生成AIを利用した偽情報を含む記事が確認され、元首相・鳩山由紀夫氏を題材にするなど実験的な要素も見受けられた。この調査では、安全保障分野の1つであるサイバーセキュリティ分野にも言及している。中国共産党（CCP）に近いインテリジェンス企業は、意図的に中国に有利な脅威情報を積極的に配信することで、西側諸国の脅威データベースに偽情報を組み込むことに成功している。これは、AIが一般に普及しつつある現代において、データ学習が阻害されることを意味しており、新たな脅威となり得る。

2つ目の調査では、中国国内において発生している反体制派のソーシャルメディアアカウントの乗っ取りによる影響工作について調査を行なった。題材として、今年5月頃に話題となっていた中国・反体制派のX（旧Twitter）アカウント「李老师不是你老师」の乗っ取りを目的としたサイバー攻撃を取り上げる。李老师不是你老师は、彼を支援する反体制派らが、中国国内の状況を撮影した写真や動画を海外からXへ投稿していたことで知られる。この活動内容を鑑みると、公安部（MPS）が関与している可能性が想起されるが、サイバー領域においてMSSとMPSが協力関係にあることや、標的ユーザーが海外在住であることを踏まえると、MSSの関与が疑われる事例である。また、この攻撃に悪用された悪性コードを分析したところ、今年2月に情報流出によりMSSやMPSの請負事業者であることが明らかになった安洵信息（I-SOON）の開発したツールが使用されていた可能性が示唆されている。これまでも親中派インフルエンサーを利用して中国に有利な情報を発信する手法はたびたび見られていたが、今回の事例では反体制派の象徴的なアカウントを乗っ取り、標的ユーザーの中国国内の支援者を摘発すると共に、世論操作を行うことが目的であったと推察される。

MSS が仕掛けるサイバー空間における影響工作は、その影響力を拡大し続けている。これらの脅威はサイバーセキュリティ上の重大な問題であり、国家として取り組むべき課題だ。今後、MSS および MPS による影響工作はさらに高度化することが予想されており、我が国はこれに対し、抜本的な対策を講じる必要がある。

本報告書目次

本調査研究は、株式会社新領域安全保障研究所から資金提供を受けて行ったものである。

株式会社サイント
経済産業省情報セキュリティ対策専門官
千葉県警察サイバーセキュリティ対策テクニカルアドバイザー
情報セキュリティ大学院大学客員研究員
岩井博樹