サイバーセキュリティレポート

2024.07

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2024 年 7 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『米国、ロシアがプロパガンダを拡散するために活用した AI 搭載型ボットファームを阻止』

- 7 月 9 日、米司法省はロシアの AI 搭載型ボットファームで使用された X（旧 Twitter）アカウント 968 個と、ボットの登録に使用された 2 件のドメインを差し押さえ、ロシア政府が支援する AI 対応のプロパガンダキャンペーンを中断させたと発表した。
- ロシアは AI 搭載型ボットファーム「Meliorator」を使用して偽の SNS アカウントを大量に作成し、X 上でウクライナのパートナー諸国等の偽情報を流していた。ロシアに有利となるよう世論操作を試みていたと考えられる。
- 昨今の SNS では異なる価値観や意見が見えにくいフィルターバブル等の問題により、情報の真偽の判断が難しくなっている。偽情報の拡散については、欧州連合（EU）が「デジタルサービス法（DSA）」を施行するなど、プラットフォーム企業側の対応を求める法整備が進められている。

第 2 章『JavaScript ライブラリ Polyfill.io 譲渡によるサプライチェーン攻撃の実施』

- 6 月 25 日、オランダのセキュリティ企業 Sansec は、オープンソースの JavaScript ライブラリ Polyfill.io が、同ライブラリを利用している Web サイトに接続するモバイルデバイスに向け、サプライチェーン攻撃を実施していると報告した。
- Polyfill.io は、今年 2 月 24 日に中国系と見られる企業 Funnull に譲渡されていた。それを知った利用者などから、いずれこのようなサプライチェーン攻撃が発生するのではないかと懸念されていたが、それが現実となった。
- JavaScript ライブラリは、組み込まれた Web サイトに接続する Web ブラウザに向けて、任意の JavaScript コードを配信することが可能である。今回は重大な被害は報告されていないが、今後もこのようなライブラリを狙った活動が起こり得るので、注意が必要である。

第 3 章『Meta 社、ブラジル政府から個人データを利用した生成 AI の学習を差し止められる』

- Meta 社は、自社プラットフォームサービスから得た個人データを生成 AI の学習に使用するため、プライバシーポリシーを改訂した。
- 7 月 2 日、ブラジル政府当局は個人データ保護の法律に違反した疑いから、プライバシーポリシーの差し止めおよび生成 AI の学習の中止を命じた。これを受け Meta 社は、ブラジルでの生成 AI ツールの使用停止を決めた。
- AI による個人データの活用と安全の両立を図る動きはまだ始まったばかりであり、本件もその途上で起きた事件の一つと考えられる。

1. 米国、ロシアがプロパガンダを拡散するために活用した AI 搭載型ボットファームを阻止

1.1. 概要

7月9日、米司法省は、米国人のものであるかのように偽装した 1000 近くの SNS アカウントなどを押収し、ロシアによる米国内外でのプロパガンダ拡散の試みを阻止したと発表した。ロシアは、AI 搭載型ボットファーム（AI を使って架空のプロファイル等を生成し、それを使用して SNS 上で偽情報等を拡散するためのシステム）を使って、X（旧 Twitter）上に米国人が発信したように見せかける投稿を大量に流し、ウクライナ侵攻等に関連する世論をロシア側が有利となるような状況に導こうとしていた[1]。

1.2. 米司法省によるアカウント押収

米司法省は今回の活動で、ロシアの AI 搭載型ボットファームで使用された X アカウント 968 個と、ボットの登録に使用された 2 件のドメインを差し押さえ、ロシア政府が支援する AI 対応のプロパガンダキャンペーンを中断させた。

メリック・B・ガーランド米司法長官は、「ロシア政府がウクライナで残忍な戦争を続け、世界中の民主主義を脅かす中、司法省はロシアの侵略に対抗し、米国民を守るために、引き続きあらゆる法的権限を行使していく」と述べた。また、FBI のクリストファー・レイ長官はこの押収について、「本日の行動は、ロシアが支援する AI 搭載型ボットファームを阻止する初の試みだ」としている[2]。

1.3. AI 搭載型ボットファーム「Meliorator」

今回確認されたボットファームには、AI を使ったボットファームの作成と運用が可能なソフトウェア「Meliorator」が使われていた。Meliorator の開発は、2022 年頃からロシアの国営通信社であるロシア・トゥデイ（RT）の副編集長が主導しており、ロシア政府の支援を受けながら、ロシア連邦保安庁（FSB）と共に運用・管理をしていたとみられる。

ロシアの RT 系列組織は、Meliorator を使用して実在の人物を装った偽の SNS アカウントを大量に作成し、X 上で米国・ポーランド・ドイツ・オランダ・スペイン・ウクライナ・イスラエル等の国々に関する偽情報を流していた。これによりロシアは自国の政府にとって有利な状況となるように世論操作を行い、ウウクライナのパートナー諸国を弱体化させようとしたとみられる。

昨今の SNS では偽情報による様々な影響が懸念されている。例えば、個人情報の学習アルゴリズムにより、ユーザーが興味を持ちそうな情報ばかりを届けるようにして、異なる価値観や意見に触れる機会を減少させ、共通の事実認識に至りにくい状態にする「フィルターバブル」の問題がある。ロシア政府は自国に有利となるプロパガンダを大量に放出することで、ロシアに批判的な意見などが見えにくくなるフィルターバブルを意図的に作り出し、自国の主張を強く支持する層を作り出すことを狙っていると考えられている。

---

[1] 出典：U.S. Department of Justice『Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm』
https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners

[2] 出典：U.S. Department of Justice『Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm』
https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners

なお、これまで Meliorator の使用が確認されたのは X のみであるが、他の SNS においても使用できる可能性が高い[3]。

1.4. ロシアのプロパガンダ拡散活動

前述のロシアの工作は、2022 年のウクライナ侵攻以来、侵攻の正当化の主張に世界を共鳴させる目的で執拗に行われてきた。

米司法省のプレスリリースでは、ボットファームで作られた偽アカウントによるプロパガンダの例が以下のように挙げられている。

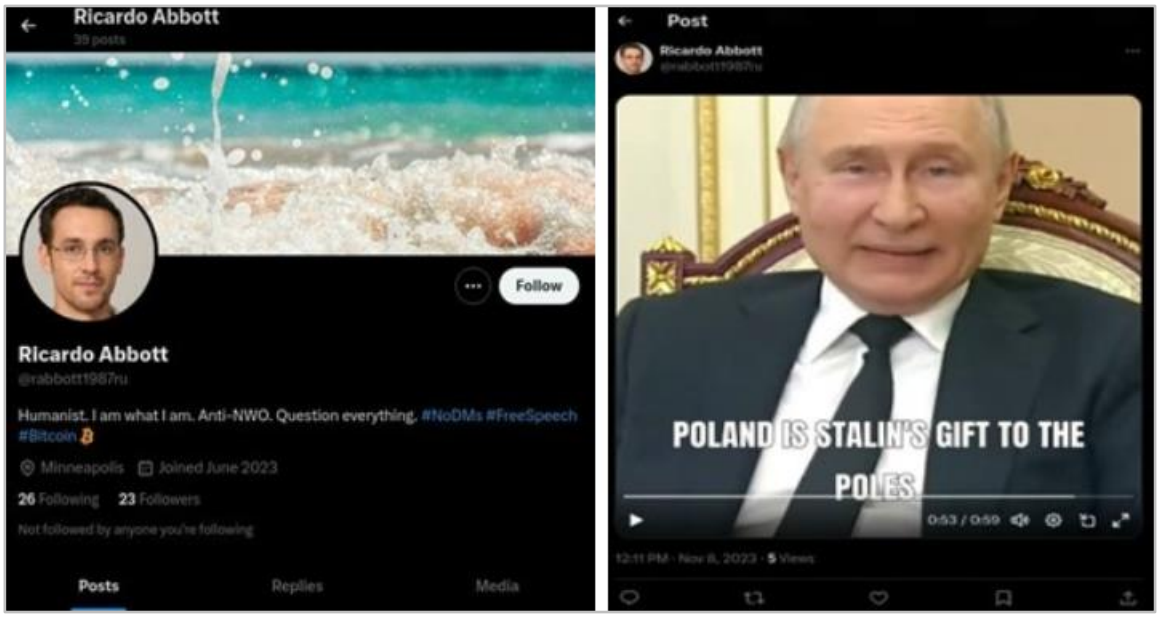

図 1 ボットファームで作られた偽アカウントによるプロパガンダの例①[4]

米国の有権者（左）のものとする偽アカウントが、「ポーランド、ウクライナ、リトアニアなどの地域は第二次世界大戦中にナチスの支配から人々を解放したロシア軍からの『贈り物』だ」とプーチン大統領が語る動画（右）を投稿している。

[3] 出典：BleepingComputer『US disrupts AI-powered bot farm pushing Russian propaganda on X』 https://www.bleepingcomputer.com/news/security/us-disrupts-ai-powered-bot-farm-pushing-russian-propaganda-on-x/

[4] 出典：U.S. Department of Justice『Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm』 https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners

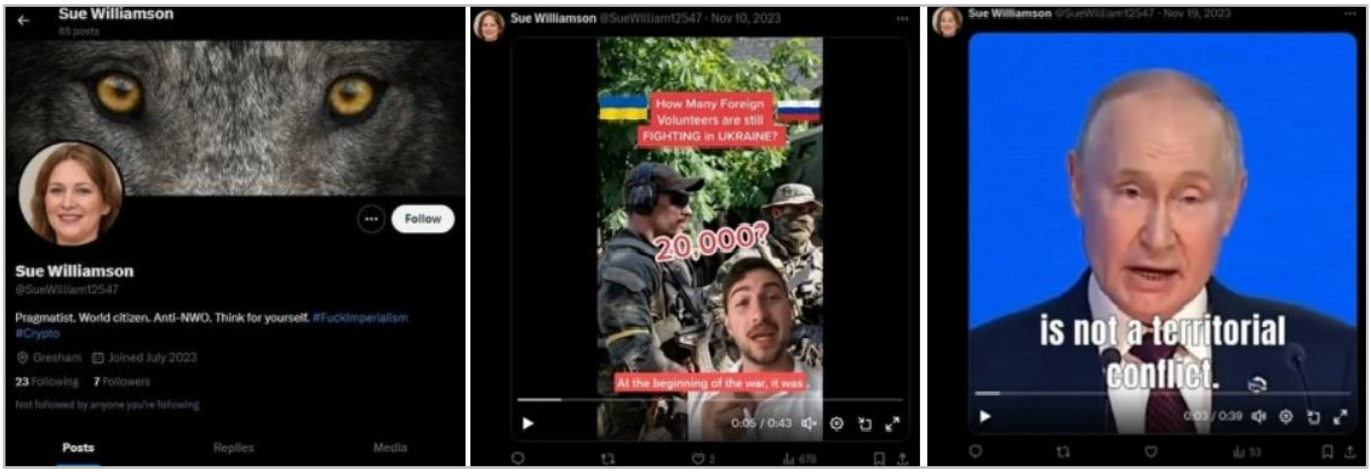

図 2 ボットファームで作られた偽アカウントによるプロパガンダの例②[5]

米国在住者（左）のものとする偽アカウントが、ウクライナ軍の外国人戦闘員の数が推定されているよりも大幅に少ないと主張するビデオ（中）を投稿している。また、同じアカウントより、ウクライナ侵攻は領土問題ではないとプーチン大統領が主張しているビデオ（右）も投稿されている。

1.5. FBI、カナダ、オランダが共同サイバーセキュリティアドバイザリを発表

米司法局による今回のボットファームの阻止に関連し、FBI と米サイバー軍サイバー国家任務部隊（CNMF）はカナダ、オランダ政府と共同でサイバーセキュリティアドバイザリ（JOINT CYBERSECURITY ADVISORY）を発表した。このアドバイザリでは Meliorator の技術について詳しく説明されており、ロシア政府によるこのテクノロジーの悪用を阻止するため、SNS 企業に警告することを目的としたものである[6]。これを受け X は、裁判所が特定し、ボットファームで使用された偽アカウントを自主的に凍結した[7]。

[5] 出典：U.S. Department of Justice『Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm』
https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners

[6] 出典：JOINT CYBERSECURITY ADVISORY『State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity』
https://www.ic3.gov/Media/News/2024/240709.pdf

[7] 出典：U.S. Department of Justice『Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm』
https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners


JOINT
CYBERSECURITY
ADVISORY
TLP:CLEAR
Co-Authored by:
Product ID: AA24-191A
July 9, 2024
POLITIE
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity
Summary
The U.S. Federal Bureau of Investigation (FBI) and Cyber National Mission Force (CNMF), in partnership with the Netherlands General Intelligence and Security Service (AIVD), Netherlands Military Intelligence and Security Service (MIVD), the Netherlands Police (DNP), and the Canadian Centre for Cyber Security (CCCS), (hereinafter referred to as the authoring organizations) are releasing this advisory to warn social media companies that Russian state-sponsored actors have leveraged the covert Meliorator software for foreign malign influence activity benefiting the Russian Government.

図 3 Meliorator についての共同アドバイザリ[8]

発行組織：FBI、米サイバー軍サイバー国家任務部隊（CNMF）、カナダサイバーセキュリティセンター（CCCS）、オランダ総合情報保安局（AIVD）、オランダ軍情報保安局（MIVD）、オランダ警察

1.6. プラットフォーム企業への有害情報対策の義務付け

2023 年 8 月、欧州連合（EU）はその調査報告書の中で、Meta や Google、Amazon、X 等、インターネット上でビジネスを展開する事業者（プラットフォーム）がロシアの偽情報キャンペーンを抑制できなかったことを非難した[9]。EU で以前から問題視されていた、ロシアのプロパガンダ等の拡散は、ウクライナ侵攻後に激化した。特に X においては、イーロン・マスクによる買収以降、ロシアからとみられるヘイトスピーチや誤情報が急速に増加していた[10]。

EU は 2024 年 2 月、こうしたロシアによる巧妙なプロパガンダ操作やヘイトスピーチなどの有害コンテンツの削除や対応策の報告をプラットフォーム企業に義務づける「デジタルサービス法（DSA）」を、7 月の欧州議会選挙を前に全面施行した[11,12]。これにより、従業員が 50 人未満で年間売上高が 1 千万ユーロ（約 16 億円）以下の小規模事業者を除いたすべてのプラットフォーム企業が、偽情報などの有害な投稿の削除や対応策の報告を求められるようになった。

日本においても総務省の「プラットフォームサービスに関する研究会」が、プラットフォーム企業の在り方について 2024 年 2 月

[8] 出典：JOINT CYBERSECURITY ADVISORY『State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity』
https://www.ic3.gov/Media/News/2024/240709.pdf

[9] 出典：Publications Office of the European Union『Digital Services Act』
https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1/language-en

[10] 出典：Forbes JAPAN『ロシアの「プロパガンダ戦略」に無力な SNS 各社、EU が非難』
https://forbesjapan.com/articles/detail/65800

[11] 出典：朝日新聞 DIGITAL『EU のデジタルサービス法、全面施行　小規模事業者除き全企業対象に』
https://www.asahi.com/articles/ASS2K5SDPS2JUHBI02B.html

[12] 出典：Forbes JAPAN『ロシアの「プロパガンダ戦略」に無力な SNS 各社、EU が非難』
https://forbesjapan.com/articles/detail/65800

にとりまとめを公表し、有害情報等の削除について事業者の対応の迅速化や運用指針の透明化を求めた[13, 14]。そして、このとりまとめの方針を基に「プロバイダ責任制限法」を「情報流通プラットフォーム対処法」に改正する法律が成立し、5 月 17 日より施行された。情報流通プラットフォーム対処法では、大規模プラットフォーム企業に対し一定期間内の削除申出への対応や、削除基準の策定・公表を義務付けるなどの規制が新たに設けられた。これにより SNS 上の有害情報削除の迅速化が期待される[15]。このように、偽情報の拡散への対策として、プラットフォーム企業側の対応を求める法整備が進められている。

1.7. まとめ

ロシアは長年に渡り、SNS 上で実在の人物を装い、世界中で様々な偽情報拡散キャンペーンを続けている。西側諸国との関係が悪化する中、ロシアは AI も利用しながら、これらの活動を拡大し、ウクライナの支援を弱体化させ、ロシアに有利となる世論操作を目論んでいる。このような試みに対し、EU では「デジタルサービス法（DSA）」を、また日本でも「情報流通プラットフォーム対処法」を施行し、利用者の保護や有害情報を迅速に削除するなどの対応をプラットフォーム企業に義務づけるよう法整備は進んでいるが、有効性については今後の推移を見守る必要がある。

[13] 出典：総務省『「プラットフォームサービスに関する研究会 第三次とりまとめ」及び 意見募集の結果の公表』
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000220.html

[14] 出典：日経クロステック（xTECH）『プラットフォーマーに有害情報対策を義務付けた EU の「DSA」、日本版への期待も』
https://xtech.nikkei.com/atcl/nxt/keyword/18/00002/020600248/?P=2

[15] 出典：契約ウォッチ（KEIYAKU-WATCH）『【2024 年公布】情報流通プラットフォーム対処法とは？プロバイダ責任制限法からの改正内容を分かりやすく解説！』
https://keiyaku-watch.jp/media/hourei/joho-platform-2024/

2. JavaScript ライブラリ Polyfill.io 譲渡によるサプライチェーン攻撃の実施

2.1. 概要

6 月 25 日、オランダのセキュリティ企業 Sansec は、オープンソースの JavaScript ライブラリ Polyfill.io が、同ライブラリを利用している Web サイトに接続するモバイルデバイスに向けて、悪質な JavaScript コードを配信するサプライチェーン攻撃を実施していると報告した[16]。

Polyfill.io は、今年 2 月に中国系と見られる企業 Funnull に譲渡されていた。これを知った Polyfill.io の利用者などは、いずれこのようなサプライチェーン攻撃が発生するのではないかと懸念していたが[17]、それが実際に発生してしまった。

インターネットに接続されたデバイスの検索エンジンを提供する Censys は、Polyfill.io を利用するインターネット上のホストの数が、7 月 2 日時点で 38 万台を超えることを発表した[18]。

図 4 Funnull の Web サイト

2.2. Polyfill.io について

Polyfill.io は、最新の機能をサポートしていない古い Web ブラウザにおいて、その機能を使えるようにするためのオープンソースの JavaScript ライブラリである[19, 20]。

---

[16] Sansec『Polyfill supply chain attack hits 100K+ sites』
https://sansec.io/research/polyfill-supply-chain-attack

[17] 出典：Internet Archive Wayback Machine『GitHub - Is it true that polyfill.io hosting is going to be owned by a Chinese company?』
https://web.archive.org/web/20240229113710/https://github.com/polyfillpolyfill/polyfill-service/issues/2834

[18] 出典：Censys『July 2: Polyfill.io Supply Chain Attack – Digging into the Web of Compromised Domains』
https://censys.com/july-2-polyfill-io-supply-chain-attack-digging-into-the-web-of-compromised-domains/

[19] 出典：Internet Archive Wayback Machine『Polyfill.io – Polyfill.io』
https://web.archive.org/web/20231012235607/https://cdn.polyfill.io/v3/

[20] 出典：Internet Archive Wayback Machine『GitHub - polyfill-service』
https://web.archive.org/web/20240626194253/https://github.com/polyfillpolyfill/polyfill-service

https://cdn.polyfill.io にて配信されていたこのライブラリを、Web サイトの運営者がそのサイトに組み込むことで、これに接続してくる Web ブラウザごとの機能の差異を補完する JavaScript コード（これを Polyfill という）が動的に生成される。これにより、Web サイトの運営者はこの差異を意識せず Web サイトを提供できる。

Polyfill.io は、2013 年頃からイギリスの経済紙 Financial Times の Web 開発チームが率いるコントリビューター（有志の参加者）のコミュニティによって開発と運用が行われてきた[21]。また、CDN 事業者 Fastly も長年 Polyfill.io を支援してきた。

2023 年 7 月、Financial Times が支援を終了するにあたり、Polyfill.io はそれまで長年にわたり同ライブラリの維持のために中心的な役割を果たしてきた Jake Champion に譲渡された[22]。彼は、2022 年 4 月まで Financial Times に、同年 6 月からは Fastly に勤務している[23]。

図 5 Polyfill.io を利用する Web サイトの HTML ソースコードの例

2.3. Polyfill.io によるサプライチェーン攻撃

【Funnull への Polyfill.io 譲渡】

2024 年 2 月 24 日頃、Funnull いう企業と Champion がそれぞれ、Polyfill.io が 2 月 24 日をもって Funnull に譲渡されることを発表した（現在、Funnull が行った発表［**図 6**］は削除され、Champion が行った発表は非公開となっている）。

Funnull はその Web サイトにおいて、CDN 事業を実施していること、スロベニアに拠点を置き世界中にオフィスがあることを主張している。しかし、そこに記載されているオフィスの住所は存在せず、同社のサイトや Telegram で中国語が使用されてい

[21] 出典：Internet Archive Wayback Machine『Polyfill.io - Polyfill service』
https://web.archive.org/web/20140913204704/https://cdn.polyfill.io/v1

[22] 出典：Internet Archive Wayback Machine『Polyfill.io - New ownership of the polyfill service』
https://web.archive.org/web/20230610084108/http://cdn.polyfill.io/v3/ownership-transfer

[23] 出典：THE ORG『Jake Champion』
https://theorg.com/org/fastly/org-chart/jake-champion

ることから、中国系の企業と見られている[24, 25]。

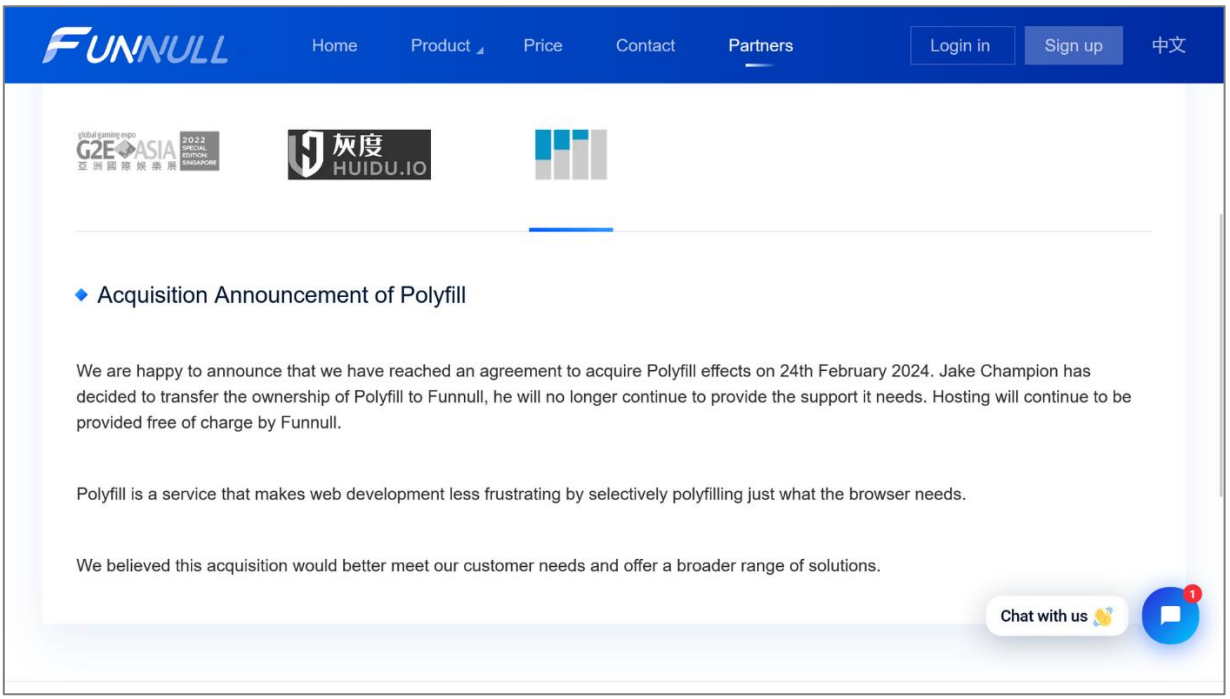

図 6 Funnull が 2 月末に行った Polyfill.io 取得の発表

この譲渡を知った Polyfill.io の利用者などは、同ライブラリによるサプライチェーン攻撃が発生するのではないかと懸念し、Polyfill.io の GitHub リポジトリの掲示板で質問したものの Funnull、Champion からの回答はなく、質問は削除された[17, 26]。

また 2 月 26 日、かつて Financial Times に勤務し、Polyfill.io の開発に関わった Andrew Betts は主要な Web ブラウザでは新しい機能はすぐに実装されるため、もはや Polyfill.io は必要なく、すぐに利用を止めるべきだと主張した[27]（彼も、Champion と同様に、現在は Fastly に勤務している[28]）。

【Polyfill.io が実施したサプライチェーン攻撃の報告】

6 月 25 日、オランダのセキュリティ企業 Sansec は、Polyfill.io が、同ライブラリを利用している Web サイトに接続するモバイルデバイスに向けて、悪質な JavaScript コードを配信するサプライチェーン攻撃を実施していると報告した[16]。同社は、

[24] 出典：The Register『If you're using Polyfill.io code on your site – like 100,000+ are – remove it immediately』 https://www.theregister.com/2024/06/25/polyfillio_china_crisis/

[25] 出典：The Register『Polyfill.io owner punches back at 'malicious defamation' amid domain shutdown』 https://www.theregister.com/2024/06/28/polyfillio_cloudflare_malware/

[26] 出典：Internet Archive Wayback Machine『GitHub - polyfill.io domain owner』 https://web.archive.org/web/20240626181448/https://github.com/polyfillpolyfill/polyfill-service/issues/2873

[27] 出典：x.com『@triblondon』 https://x.com/triblondon/status/1761852117579427975

[28] 出典：Fastly『triblondon』 https://community.fastly.com/u/triblondon

Polyfill.io を利用する Web サイトにモバイルデバイスで接続すると、同ライブラリがスポーツ賭博サイトに転送させるための悪質な JavaScript コードを生成したこと、また Web ブラウザが接続先のサイトに送信する HTTP ヘッダによって Polyfill.io は動的に JavaScript コードを生成するため、この特性を利用した複数の攻撃手法が存在する可能性があることを報告した。

Censys は、7 月 2 日時点でインターネット上の 384,773 台のホストが Polyfill.io を利用していることを検出したと発表した [18]。

図 7 Polyfill.io によるサプライチェーン攻撃についての Sansec の報告

2.4. サプライチェーン攻撃への対応

【ドメイン登録事業者、CDN 事業者の対応】

ドメイン登録事業者 Namecheap は、6 月 27 日、ドメイン「polyfill.io」の停止措置を行った。これにより、https://cdn.polyfill.io から JavaScript ライブラリが取得できなくなったため、サプライチェーン攻撃のリスクは解消した。

この 4 か月前の 2 月 29 日には、CDN 事業者 Cloudflare と Fastly が、いずれサプライチェーン攻撃が起こるリスクを懸念し、Polyfill.io の代替となるサービスを立ち上げ、提供を開始していた[29, 30]。また、Cloudflare は 6 月 26 日、同社の CDN サービスを利用する Web サイトが Polyfill.io を利用している場合、自動的に同社の Polyfill サービスに置き換える機能をリリースした[31]。

【Funnull の主張】

Polyfill.io がサプライチェーン攻撃を行っているという指摘に対して、Funnull 社は、「誰かが悪意を持って私たちの名誉を毀

[29] 出典：Cloudflare『polyfill.io now available on cdnjs: reduce your supply chain risk』
https://blog.cloudflare.com/polyfill-io-now-available-on-cdnjs-reduce-your-supply-chain-risk

[30] 出典：Fastly『New options for Polyfill.io users』
https://community.fastly.com/t/new-options-for-polyfill-io-users/2540

[31] 出典：Cloudflare『Automatically replacing polyfill.io links with Cloudflare's mirror for a safer Internet』
https://blog.cloudflare.com/automatically-replacing-polyfill-io-links-with-cloudflares-mirror-for-a-safer-internet

損している、自身の評判を落とすことになるためそのようなこと（サプライチェーン攻撃）は実施していない」と、X（旧Twitter）で主張した。[32]

同社は、ドメイン「polyfill.io」が停止された後、他ドメイン「polyfill.com」「polyfill.top」などを利用して、サービスの継続を試みたが、いずれのドメインも停止措置に遭っている。

2.5. まとめ

JavaScript ライブラリ Polyfill.io が出所不明な会社に譲渡され、サプライチェーン攻撃が発生してしまった。譲渡先の Funnull は、サプライチェーン攻撃への関与を否定しているが、本件を発表した Sansec は、攻撃で実際に使用された JavaScript コードを公開している。

Web サイトに組み込まれた JavaScript ライブラリは、その Web サイトに接続する Web ブラウザに向けて、任意の JavaScript コードを配信することが可能であり、これを悪用すると今回のようなサプライチェーン攻撃を実施することができる。

今回は重大な被害は報告されていないが、発見や対処が遅れれば広範な被害につながる恐れがあった。今後もこのようなライブラリを狙った活動は起こり得るため、注視したい。

[32] 出典：x.com『@Polyfill_Global』
https://x.com/Polyfill_Global/status/1805923380857897277

3. Meta 社、ブラジル政府から個人データを利用した生成 AI の学習を差し止められる

3.1. 概要

Meta 社が、自社サービスにおいて公開されている個人データを生成 AI の学習に利用しようとし、プライバシーポリシーを改訂した。ブラジル政府当局は個人データ保護の法律に違反した疑いから予防措置として 7 月 2 日、プライバシーポリシーの停止および生成 AI によるデータ処理の中断を Meta 社に命じた。Meta 社はこれを受け 7 月 17 日に、ブラジルでの生成 AI ツールの使用停止を決定した[33]。

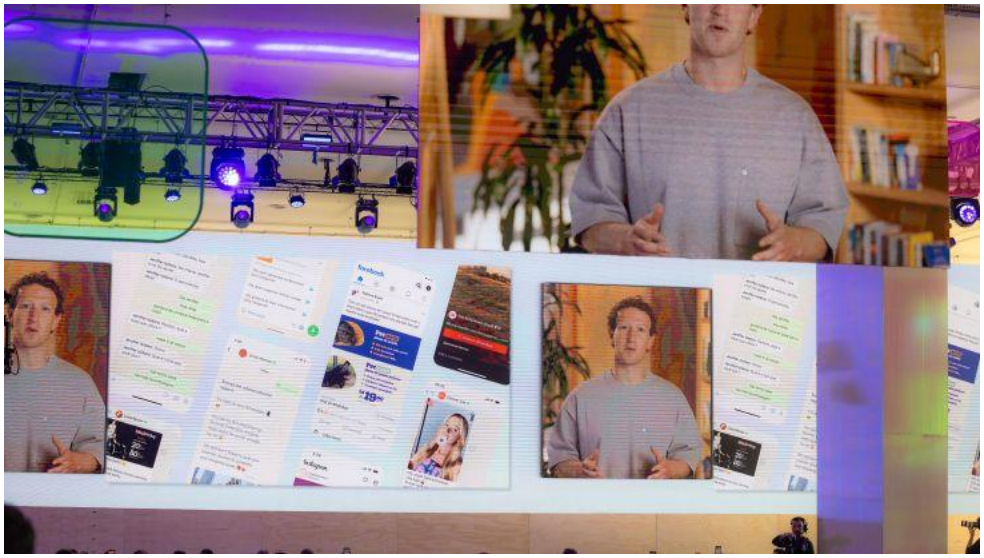

図 8 ブラジルで、生成 AI を活用した新サービスを発表する Meta 社のマーク・ザッカーバーグ CEO [34]

3.2. Meta 社のプライバシーポリシー改訂

6 月 26 日、ブラジルのサンパウロで行われたイベント「Conversations」で、Meta 社のマーク・ザッカーバーグ CEO から、企業向けターゲティング広告の新サービス[35]についてのビデオメッセージが発表された。

この新サービスは、Meta 社のメッセージサービスである WhatsApp、それと SNS サービス（Facebook と Instagram）を利用しているユーザーへのマーケティングを、企業に提供する。まず、ユーザーが公開している SNS サービスでの投稿が、生成 AI の学習に使用される。企業は AI 処理の結果を活用し、広告に最も反応しそうなユーザーにターゲットを絞って、WhatsApp で広告メッセージを送信するというものである[36]。

このサービス提供に伴い同社は、公開投稿に含まれる個人データを AI の学習に使用することなどに対応した、新しいプライ

[33] 出典：Reuters『Meta decides to suspend its generative AI tools in Brazil』
https://www.reuters.com/technology/artificial-intelligence/meta-decides-suspend-its-generative-ai-tools-brazil-2024-07-17/

[34] 出典：CNN Brasil『Brasileiros são os que mais enviam áudios e figurinhas no WhatsApp, diz Mark Zuckerberg』
https://www.cnnbrasil.com.br/tecnologia/brasileiros-sao-os-que-mais-enviam-audios-e-figurinhas-no-whatsapp-diz-mark-zuckerberg/

[35] 出典：Meta『New AI Tools, Meta Verified and More for Businesses on WhatsApp』
https://about.fb.com/news/2024/06/new-ai-tools-meta-verified-and-more-for-businesses-on-whatsapp/

[36] 出典：Reuters『Meta's WhatsApp launches new AI tools for businesses』
https://www.reuters.com/technology/metas-whatsapp-launches-new-ai-tools-businesses-target-messages-chats-2024-06-06/

バシーポリシーを発表した[37]。Meta 社がプライバシーポリシーを改訂したのは今回の新サービスだけではなく、近い将来に主力となるマルチモーダル AI の提供を見据えてと考えられている[38]。マルチモーダル AI は、動画やテキスト等の異なる種類の情報をまとめて扱い、いわばシチュエーションとして理解する生成 AI であり、実用化が進められている。一方で、基となるデータが様々であることから、生成 AI が出力する判断についてその根拠が分かりづらくなるといった面も指摘[39]されており、SNS 等のサービスで利用した場合、個人データの利用について説明責任等を求める法律との整合が難しくなる可能性がある。

3.3. ブラジル政府による Meta 社プライバシーポリシーの停止

【ブラジルの個人データ保護法：LGPD】

ブラジルでは、包括的な個人データ保護法令として「ブラジル一般データ保護法」（Brazilian General Data Protection Law：以下「LGPD」と表記）が施行されている[40]。

LGPD は、厳格なことで知られる EU 圏の一般データ保護規則（GDPR）に倣っている[41]。GDPR と同様に、「識別された、又は識別可能な自然人に関連するあらゆる情報」と広範な個人データを保護の対象としている。また、ブラジル国内の個人データの、国外への越境移転について制限を設けている。個人データを提供する「データ主体」であるユーザーからの事前同意についても厳格である。個人データを処理する者は、その処理について明示し事前に同意を得た上で、取得および処理する必要がある[42]。

LGPD の法制度によって設けられた、個人データ保護を担当する政府機関が、「国家データ保護機関」(Autoridade Nacional de Proteção de Dados：以下「ANPD」と表記)である。

【ANPD の差し止め命令】

ANPD は 7 月 2 日に、Meta 社の新しいプライバシーポリシーについて、LGPD 違反の可能性が有ると判断した[43]。理由として、生成 AI の実用化より前にユーザーから取得した個人データ提供の同意に、生成 AI への提供が含まれているとは考え難いこと、ユーザーが拒否権を行使するには操作が分かりにくいこと等が挙げられている。これにより予防措置として、プライバシーポリシーの有効性を即時停止し、生成 AI の学習のための個人データの処理の中断を命じた。さらに、1 日あたり 5 万レア

---

[37] 出典：The New York Times『Can I Opt Out of Meta's A.I. Scraping on Instagram and Facebook? Sort Of.』』
https://www.nytimes.com/2024/06/07/technology/meta-ai-scraping-policy.html

[38] 出典：AXIOS『Scoop: Meta won't offer future multimodal AI models in EU』
https://www.axios.com/2024/07/17/meta-future-multimodal-ai-models-eu

[39] 出典：産総研マガジン『マルチモーダル AI とは？』
https://www.aist.go.jp/aist_j/magazine/20231129.html

[40] 出典：個人情報保護委員会『外国制度（ブラジル連邦共和国）』
https://www.ppc.go.jp/enforcement/infoprovision/laws/offshore_report_brazil/

[41] 出典：Business & Law（ビジネスアンドロー）『データ越境移転規制の最新動向［第 11 回］ ブラジル』
https://businessandlaw.jp/articles/a20220809-1/

[42] 出典：Progress Software Corporation ブログ『ブラジルの一般データ保護法』
https://www.progress.com/jp/blogs/understanding-brazils-general-data-protection-law

[43] 出典：Autoridade Nacional de Proteção de Dados (ブラジル連邦共和国 国家データ保護機関)『ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta』
https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta

ル（約 8,800 ドル）の罰金を科した[44]。

【Meta 社、ブラジルでの生成 AI ツールの使用停止を決定】

この制裁に対し Meta 社は、プライバシーポリシーは適法であり、ブラジルの人々が生成 AI の恩恵を享受するのをさらに遅らせる処分であると反論した。だが結局、Meta 社は 7 月 17 日にブラジルでの生成 AI ツールの使用停止を発表した[45]。

なお、Meta 社は GDPR のある EU 圏内でも、規制当局の明確な説明が無いことを理由に、適法的にサービスを提供できるめどが立たないことから、次世代生成 AI サービスの提供を中止している[46]。Meta 社以外にも、Apple 社が同様の理由で 6 月に、生成 AI を利用する「Apple Intelligence」機能の EU 圏でのリリースを見送ると発表[47]している。

3.4. まとめ

今回のブラジル当局による対応は、生成 AI の学習の為に個人データを使用することに対し、処罰が下る実例となった。

今回の処罰から Meta 社等の生成 AI サービス提供企業は、GDPR や LGPD といった法規制に対応しようという試みは困難であることを学習したと思われる。一方で、生成 AI の学習への個人データ利用は、規制が厳しくない米国をはじめとする国々で Google や X 等により既成事実化が進んでいる[48]。今後、EU 圏やブラジル等の個人データ規制の強い国に対しては個人データを利用した生成 AI のサービス提供が避けられ、規制の緩い国では最新の生成 AI の提供が進んでいくものと考えられる。

生成 AI により、ユーザーそれぞれの属性や嗜好等の個人データを基にした高精度のサービスが提供されれば、ユーザーは自分に合った提案といった利便を得られる。だが、個人データは濫用されれば、例えばユーザーの属性や嗜好等での格付け処理により社会的に不利益が与えられるソーシャル・スコアリングのように、人権侵害に繋がりかねない。

現在、AI の進化や普及が人権侵害等のリスクをさらに高めることが懸念されている。AI の実用化以前から、個人データの利用については GDPR 等による規制がされてきたが、それだけでは対応しきれなくなってきた。8 月 1 日に発効した EU の「AI 規制法」[49]や 3 月に採択された AI の安全な利用についての国連決議[50]はその対応の先駆けである。AI による個人データの活用と安全の両立を図る動きは始まったばかりであり、今後も様々な衝突を起こしていくものと考えられる。

以上

---

[44] 出典：AP News『Brazil data regulator bans Meta from mining data to train AI models』
https://apnews.com/article/brazil-tech-meta-privacy-data-93e00b2e0e26f7cc98795dd052aea8e1

[45] 出典：Reuters『Meta decides to suspend its generative AI tools in Brazil』
https://www.reuters.com/technology/artificial-intelligence/meta-decides-suspend-its-generative-ai-tools-brazil-2024-07-17/

[46] 出典：AXIOS『Scoop: Meta won't offer future multimodal AI models in EU』
https://www.axios.com/2024/07/17/meta-future-multimodal-ai-models-eu

[47] 出典：The Verge『Apple may delay AI features in the EU because of its big tech law』
https://www.theverge.com/2024/6/21/24183251/apple-eu-delay-ai-screen-mirroring-shareplay-dma

[48] 出典：The New York Times『When the Terms of Service Change to Make Way for A.I. Training』
https://www.nytimes.com/2024/06/26/technology/terms-service-ai-training.html

[49] 出典：European Commission（欧州委員会）『European Artificial Intelligence Act comes into force』
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123

[50] 出典：United Nations（国際連合）『General Assembly adopts landmark resolution on artificial intelligence』
https://news.un.org/en/story/2024/03/1147831

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt