サイバーセキュリティレポート

2024.04

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 4 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『Facebook 等の SNS で有名人を利用したなりすまし広告による被害が拡大』

- SNS 上で有名人がサービスや商品を推薦しているかのように見せかけた広告による消費者被害が拡大している。
- このような「なりすまし広告」は、一見するとニュースサイトの記事のようになっている。広告へのリンクは SNS の広告欄に掲載される。これを見た SNS のユーザーがクリックすると、個人情報を収集するアンケートの入力を求められたり、さらに別の SNS に誘導され投資詐欺に遭ったりする。
- なりすまし広告に用いられるフェイク技術は進化し続けており、見た目だけで判断するのは難しくなっていると専門家は指摘している。今後は、法の整備の他、なりすましを見破る SNS 運営元の技術の向上が期待される。

第 2 章『PAN-OS の GlobalProtect 機能に脆弱性、既に悪用も確認』

- 4 月 12 日、米サイバーセキュリティ会社の Palo Alto Networks が同社の製品にコマンドインジェクションの脆弱性（CVE-2024-3400）があることを公表した。
- 攻撃被害の検証をする中で発覚したゼロデイ脆弱性であり、攻撃可能な設定の疑いのある機器は、全世界で 14 万台以上に上ることが確認されている。
- ネットワーク内への侵入口となる VPN へのゼロデイ攻撃が、本件以外にも相次いでいる。VPN 機器の脆弱性や被害に関する情報収集を強化するとともに、ゼロデイ攻撃を受けることを前提とした多重防御態勢を整える必要がある。

第 3 章『Google が Web ブラウザのプライバシーモードから収集したデータの破棄に合意』

- プライバシーポリシー等の記載内容に反して、IP アドレス情報や閲覧履歴を密かに収集しているとして、Web ブラウザのプライバシーモードを利用するユーザーらが Google（およびその親会社のアルファベット社）に対し、集団訴訟を提起した。
- 本訴訟は和解に至り、裁判所に提出された和解案から、Google がこれまで Web ブラウザのプライバシーモードから収集した 2023 年 12 月以前のデータの破棄に合意したことが明らかとなった。
- Google はプライバシーポリシー等の記載を修正したが、プライバシーモードを利用するユーザーから Web 閲覧履歴やその IP アドレスなどのデータを今後も収集することに変わりはない。Google には、ユーザーのプライバシーを侵害しないよう、集めたデータについて透明性を持って適切に扱うことが求められる。

1. Facebook 等の SNS で有名人を利用したなりすまし広告による被害が拡大

1.1. 概要

SNS 上では、特定のサービスや商品を有名人が推薦しているかのように見せかけた広告が多数みられる。このような広告に騙される被害が拡大していることを受け、4 月 10 日、自民党本部で勉強会が行われた[1]。この会に招かれた実業家の前澤友作氏は、国が対策を行うよう訴えると共に、こうした広告を放置しているとして Facebook や Instagram の運営元である米 Meta 社を提訴する方針を発表した 。前澤氏は以前から、自身に無断でこうした広告が作られていると指摘していた[2]。

近年、Meta 社の上述のサービスや、X 社の X（旧 Twitter）、LINE ヤフー社の LINE 等の大手の SNS は、老若男女から企業までもが利用するプラットフォームとなっており、これらにおいて、広告の掲載料は主な収入源である[3]。SNS は多くの人が目にするため社会的影響が大きいことや、SNS の運営元はその掲載料を得ていることから、運営元に対して責任ある対応を求める声が上がっている。

図 1 自民党で行われた勉強会の様子

1.2. 有名人を利用したなりすまし広告

有名人を使ったなりすまし広告（以下、「なりすまし広告」と記載）は、一見するとニュースサイトの記事のようになっている[4]。例えば、テレビ番組のワンシーンの写真を使い、その出演者をなりすまし広告に登場させたい有名人に差し替える。そしてその有名人が番組内で投資等を宣伝したかのような内容の記事／写真を作成する。こうした記事に、『日本銀行が生放送での

[1] 出典：自民党『[なりすまし広告詐欺]早期の対策へ検討加速を確認』
https://www.jimin.jp/news/information/208023.html

[2] 出典：ITmedia NEWS『前沢友作氏が米 Meta を提訴へ Facebook でなりすまし投資の詐欺広告放置 自民に規制強化要請』
https://www.itmedia.co.jp/news/articles/2404/11/news109.html

[3] 出典：FourWeekMBA『How Does Facebook [Meta] Make Money? Facebook Business Model Analysis 2024』
https://fourweekmba.com/how-does-facebook-make-money/

[4] 出典：NHK『追跡！フェイク SNS 広告の闇 ～なぜだまされる投資詐欺～』
https://www3.nhk.or.jp/news/html/20240424/k10014431421000.html

発言をめぐって〇〇を提訴』（〇〇はなりすましに利用された有名人の名前）のような、目を引くタイトルが付けられている。SNS の広告欄にその見出しが掲載され、SNS のユーザーがこれをクリックしてなりすまし広告へアクセスすると、個人情報を収集するアンケートへの入力を求められたり、さらに別の SNS に誘導され投資詐欺に遭ったりする[5, 6]。

図 2 なりすまし広告の例

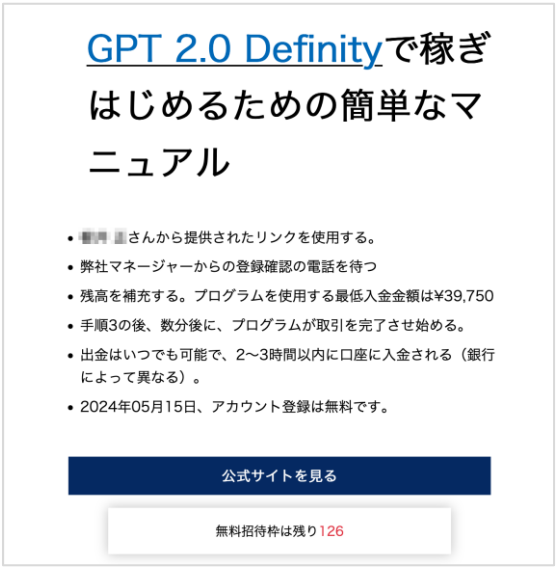

図 3 広告下部に表示される投資詐欺への入り口

有名人や有名企業の名前を騙り、偽物の SNS アカウントで投資詐欺等を行う偽アカウントの問題は以前から存在していたが、なりすまし広告がそれと異なるのは、SNS に掲載される広告を入口として利用している点やニュース記事を装っている点である。前述の前澤氏のみならず、アニメーション映画監督の宮崎駿氏[7]、落語家の笑福亭鶴瓶氏[8]、経済アナリストの森永卓郎氏[9]など、多くの有名人がなりすまし広告に利用され、被害を訴えている。

1.3. 海外の状況

有名人を騙ったなりすまし広告は、日本に限らず、世界中で問題となっている[10]。例えばアメリカでは、俳優のトム・ハンクス氏

[5] 出典：日経 XTECH『有名人になりすまして投資広告を掲載、SNS で接触してみた結果』
https://xtech.nikkei.com/atcl/nxt/column/18/02806/042400012/

[6] 出典：INTERNET Watch『有名人の画像を悪用した広告が氾濫中、LINE で連絡すると投資詐欺に誘導されるケースも』
https://internet.watch.impress.co.jp/docs/column/dlis/1583337.html

[7] 出典：日本ファクトチェックセンター『日銀が宮崎駿監督を提訴」は誤り【ファクトチェック】』
https://www.factcheckcenter.jp/fact-check/economics/boj-sues-director-hayao-miyazaki/

[8] 出典：スポニチアネックス『笑福亭鶴瓶　自身が無断使用された投資話の広告に注意喚起「だまされる人がおったら悪いから」』
https://www.sponichi.co.jp/entertainment/news/2023/10/29/kiji/20231029s00041000592000c.html

[9] 出典：日刊スポーツ『がん闘病の森永卓郎氏、投資詐欺広告で親子の被害額 10 億円「メッタメタにしてやる！」』
https://www.nikkansports.com/entertainment/news/202404230000283.html

[10] 出典：MARKET REALIST『Celebrities Targeted Globally in Rampant Fake Ad Scams; The Battle for Accountability』
https://marketrealist.com/how-do-celebrity-identity-theft-scams-take-place-in-digital-advertising/

やテレビ番組の有名司会者のゲイル・キング氏が、自身の声や画像が同意なく変更され、広告に使われていると訴えている[11]。4 月 24 日、アメリカの連邦取引委員会（Federal Trade Commission）は、消費者への注意喚起として、「有名人は本当にそれを支持した？たぶん違うだろう」と題する記事を投稿した[12]。広告に表示されている有名人やインフルエンサーの名前と「詐欺」や「偽物」という言葉を合わせて検索し情報収集を行うこと等、消費者が広告を見て金銭を支払う前に行うべき具体的なことについて、アドバイスを提供している。

1.4. Meta 社の対応

なりすまし広告に利用された有名人からは、なりすまし広告によって SNS の運営元には広告の掲載料が入っているため、厳しい対策を講じる責任が運営元にあるといった声が上がっている[13]。また、4 月 25 日には、なりすまし広告に騙されて詐欺被害に遭った男女 4 名（神戸市等に在住）が Meta 社の日本法人を提訴。広告が真実かどうか調べる責任を怠ったとして、同社に損害賠償を求めている[14]。

4 月 16 日、Meta 社はなりすまし広告に対する取り組みについての声明を公開した[15]。この声明では、有名人になりすました詐欺的な広告はポリシーで禁止しており、違反している広告を差し止めるための審査を行っていると説明している。一方で、世界中の膨大な数の広告を審査するには課題があることを認めた。問題への対応のために、2016 年以降に 200 億ドル以上投資し、ツールや機能の開発や啓発キャンペーン等を行っているとしている。同声明では具体的な対策については触れられなかったが、Meta 社は NHK の取材に対し、広告の審査チームとして世界に 4 万人を配置し、日本語を含む多数の言語に対応していることや、AI に学習させることにより、なりすまし広告を自動検出できるように取り組んでいること等を明らかにした[14]。

ただ、4 月 19 日、実業家である堀江貴文氏がプロデュースする生成 AI のオンライン研修サービス「ホリエモン AI 学校」を運営するテレワーク・テクノロジーズは、同社の Facebook の公式アカウントや関連アカウントが凍結されたことを報告した[16]。これについて、ホリエモン AI 学校の広告が詐欺と誤認された可能性が指摘されており、Meta 社がなりすまし広告の対策に苦慮している様子が伺える。

1.5. まとめ

なりすまし広告に用いられるフェイク技術は進化し続けており、見た目だけで判断するのは難しくなっていると専門家は指摘し

[11] 出典：USA TODAY『Real products, fake endorsements: Why experts say AI-generated ads will get tougher to spot』
https://www.usatoday.com/story/news/factcheck/2024/02/18/ai-deepfake-ads-tougher-detect/72536444007/

[12] 出典：Federal Trade Commission『Did a celebrity really endorse THAT? Maybe not』
https://consumer.ftc.gov/consumer-alerts/2024/04/did-celebrity-really-endorse-maybe-not

[13] 出典：週プレ NEWS『「SNS 詐欺広告」に画像を無断使用される森永卓郎＆康平親子の地獄』
https://wpb.shueisha.co.jp/news/society/2024/05/02/123083/

[14] 出典：NHK『なりすまし広告 SNS 運営会社「メタ」の日本法人を被害者が提訴』
https://www3.nhk.or.jp/news/html/20240425/k10014432921000.html

[15] 出典：Meta『著名人になりすました詐欺広告に対する取り組みについて』
https://about.fb.com/ja/news/2024/04/our_efforts_to_combat_scams/

[16] 出典：ITmedia NEWS『なりすまし詐欺広告と"誤認"か 「ホリエモン AI 学校」、Meta に広告アカウントを凍結される 運営会社は「ずさん」と苦言』
https://www.itmedia.co.jp/news/articles/2404/19/news125.html

ている[17]。こうした詐欺に騙された場合、金銭的な被害を受けるだけでなく、個人情報の漏洩やフィッシング詐欺等での悪用も懸念される。また、SNS の運営会社も、なりすまし広告の拡散防止に向けた取り組みを強化し、ユーザー保護に努める必要がある。今後は、法の整備の他、なりすましを見破る SNS 運営元の技術の向上が期待される。

[17] 出典：USA TODAY『Real products, fake endorsements: Why experts say AI-generated ads will get tougher to spot』https://www.usatoday.com/story/news/factcheck/2024/02/18/ai-deepfake-ads-tougher-detect/72536444007/

2. PAN-OS の GlobalProtect 機能に脆弱性、既に悪用も確認

2.1. 概要

4 月 12 日、米サイバーセキュリティ会社の Palo Alto Networks は、特定の PAN-OS ソフトウェアがインストールされている次世代ファイアウォールに、コマンドインジェクションの脆弱性（CVE-2024-3400）があることを公表した。PAN-OS は、Palo Alto Networks 社の次世代ファイアウォール上で実行されるオペレーティングシステムである[18]。

この脆弱性が悪用されると、認証されていない遠隔の攻撃者がファイアウォール上の管理者権限で任意のコードを実行できる可能性がある。この攻撃は、日本国内でも既に確認されており、PoC コードも公開されていることから、さらに増加する恐れがある[19, 20]。

図 4 Palo Alto Networks ファイアウォール PA-3400 Series[21]

2.2. ゼロデイ脆弱性の発見

米セキュリティ会社 Volexity は、現地時間 4 月 10 日、同社が監視する顧客のネットワーク環境でファイアウォールからのアラートを検知し、PAN-OS のゼロデイ脆弱性を悪用した攻撃が発生したことを確認した。

調査から、攻撃者が脆弱性を悪用して、ファイアウォールにバックドアのインストールを試みていたことが判明した。攻撃者はさらに、バックドアを利用してファイアウォールの設定変更等を行い、組織のネットワーク内への侵入口を設けようとしていた。

他の複数の顧客においても同様の被害を発見し、今年の 3 月 26 日には既に当脆弱性が悪用されていたことが分かった。この時、攻撃者は脆弱性の悪用の可能性についてテストしていたと思われる。Volexity はこの脅威アクターを「UTA0218」と名付け、特定の国家の支援を受けている可能性が高いと結論付けている[22, 23]。

---

[18] 出典：Palo Alto Networks TECHDOCS『PAN-OS』
https://docs.paloaltonetworks.com/pan-os

[19] 出典：Palo Alto Networks『CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect』
https://security.paloaltonetworks.com/CVE-2024-3400

[20] 出典：独立行政法人 情報処理推進機構（IPA）『Palo Alto Networks 製 PAN-OS の脆弱性対策について(CVE-2024-3400)』
https://www.ipa.go.jp/security/security-alert/2024/alert20240415.html

[21] 出典：Palo Alto Networks『次世代ファイアウォール ハードウェア』
https://www.paloaltonetworks.jp/network-security/next-generation-firewall-hardware

[22] 出典：VOLEXITY『Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)』
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

[23] 出典：Security NEXT『「PAN-OS」脆弱性の詳細や悪用コードが公開済み - 攻撃拡大のおそれ』
https://www.security-next.com/156092

2.3. 脆弱性（CVE-2024-3400）について

この脆弱性は PAN-OS の二つのバグを組み合わせ、二段階の手順を踏むことにより、認証されていない遠隔の攻撃者が脆弱なファイアウォール上でシステム管理者の権限を取得し、任意のコマンドを実行することができる。また侵害時には機密情報の窃取やマルウェアのダウンロードなどが成功する恐れがある[24]。本脆弱性の PoC コード（概念実証コード：脆弱性が悪用可能であることを証明するための検証用プログラムコード）は公開され、実際の攻撃で使用されたコードなども SNS 上に投稿された[25]。

【脆弱性の影響を受ける製品】

今回の脆弱性は、「PAN-OS」のバージョン 10.2、11.0、および 11.1 がインストールされた次世代ファイアウォールにて、GlobalProtect ゲートウェイおよび（または）GlobalProtect ポータルが有効になっている場合に影響を及ぼす[26]。GlobalProtect とは、外部から内部ネットワークへのリモートアクセスを行うための VPN 機能を提供するもので、ユーザーを識別し、証明書の発行やセキュリティ対策などを行う。

インターネット上で公開されている、GlobalProtect 機能を使用したファイアウォール（今回の対象バージョンに限定されない）の数は、4 月 15 日時点で、全世界で 14 万台以上とされる[27]。

2.4. 相次ぐ VPN 機器へのゼロデイ攻撃

本件以外にも 1 月に Ivanti Connect Secure が、中国国家の支援を受けているとされる APT 攻撃グループから[28]、また、4 月には Cisco ASA/FTD が別の APT 攻撃グループ（帰属する国家は不明）からゼロデイ攻撃を受けている[29, 30]。昨年 8 月には AKIRA ランサムウェアグループが Cisco ASA/FTD のゼロデイ脆弱性を長期に渡って悪用していたことが明らかになった[31]。

---

[24] 出典：Palo Alto Networks Blog『More on the PAN-OS CVE-2024-3400』
https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/

[25] 出典：Security NEXT『「PAN-OS」脆弱性の詳細や悪用コードが公開済み - 攻撃拡大のおそれ』
https://www.security-next.com/156092

[26] 出典：Palo Alto Networks『CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect』
https://security.paloaltonetworks.com/CVE-2024-3400

[27] 出典：Censys『April 12, 2024: Palo Alto Networks GlobalProtect PAN-OS command injection vulnerability CVE-2024-3400』
https://censys.com/cve-2024-3400/

[28] 出典：VOLEXITY『Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN』
https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

[29] 出典：CISCO『Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability』
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

[30] 出典：CISCO『Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability』
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

[31] 出典：CISCO『Cisco 適応型セキュリティアプライアンスソフトウェアおよび Firepower Threat Defense ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性』
https://www.cisco.com/c/ja_jp/support/docs/csa/2023/cisco-sa-asaftd-ravpn-auth-8LyfCkeC.html

2.5. まとめ

攻撃者が VPN 機器を研究し、防御側に先んじて内部ネットワークへの侵入を試みている状況は明らかである。

VPN 機器の脆弱性や被害に関する情報収集を強化するとともに、ゼロデイ攻撃を受けることを前提とした多重防御態勢を整える必要がある。

3. Google が Web ブラウザのプライバシーモードから収集したデータの破棄に合意

3.1. 概要

Google が、プライバシーポリシー等の記載内容に反して、Web ブラウザのプライバシーモードを利用するユーザーを追跡し、IP アドレス情報や閲覧履歴を密かに収集していた。これが盗聴に関する法律やユーザーのプライバシーを侵害しているとして、2020 年 6 月、ユーザーらが Google（およびその親会社のアルファベット社）に対し、集団訴訟を提起した[32]。その後、2023 年 12 月、2 社と原告は和解することに同意した。

今年 4 月 1 日に米国連邦地方裁判所に提出された和解案から、Google がプライバシーモードを利用するユーザーから収集した数十億件に上るデータを破棄することに合意したことが明らかとなった[33]。

I. INTRODUCTION

This settlement is an historic step in requiring dominant technology companies to be honest in their representations to users about how the companies collect and employ user data, and to delete and remediate data collected. Plaintiffs secured a groundbreaking settlement that yields substantial benefits for every single class member, including:

Changes to Google's disclosures: Google with this Settlement agrees to rewrite its disclosures to inform users that "Google" collects private browsing data, including by explicitly disclosing that fact in its Privacy Policy and on the Incognito Splash Screen that automatically appears at the beginning of every Incognito session. Plaintiffs obtained a Settlement where Google has already begun implementing these changes, without waiting for final court approval.

Deletion and remediation of private browsing data: While disclosure changes ensure transparency going forward, Plaintiffs also demanded and secured accountability and relief for Google's past conduct. Upon approval of this Settlement, Google must delete and/or remediate *billions* of data records that reflect class members' private browsing activities. This includes data Google collected during the class period from private browsing sessions.

図 5 裁判所に提出された和解案の冒頭文 [33]

3.2. プライバシーモードについて

【プライバシーモードとは】

プライバシーモードは、Chrome、Edge、Firefox、Safari など多くの Web ブラウザが実装するプライバシー保護のための機能である。Web ブラウザをプライバシーモードで起動すると、閲覧した Web サイトの履歴、キャッシュ、Cookie、フォームに入

[32] 出典：ClassAction.org『Case 5:20-cv-03664-SVK Document 1』
https://www.classaction.org/media/brown-et-al-v-google-llc-et-al.pdf

[33] 出典：Ars Technica『Case 4:20-cv-03664-YGR Document 1096』
https://cdn.arstechnica.net/wp-content/uploads/2024/04/Brown-v-Google-Unopposed-Motion-for-Final-Approval-of-Class-Action-Settlement-4-1-2024.pdf

力した情報が、同モード終了時に Web ブラウザから削除されるため、端末を共有する環境において、閲覧した Web サイトや検索キーワードを他のユーザーに知られたくない場合や、アカウントの使い分けを目的として Web サイトのログイン情報をブラウザに残したくない場合等に利用される 。

ただし、これは匿名性を提供する機能ではない。閲覧した Web サイトやそのサイトが利用する Google Analytics などの Web サイト分析サービスでは、IP アドレスや閲覧履歴などが収集される。また、企業などが利用するデバイス管理製品やインターネットサービスプロバイダ等においてもユーザーのプライバシーモードでの Web 閲覧に関するアクティビティを収集するケースも想定される。これらの収集された情報は、分析等によって個人の特定が可能となるおそれがある。

【プライバシーモードに対する誤解】

利用者の多くが、プライバシーモードの動作を誤解しているとする調査結果が報告されている。

2018 年、アメリカの非営利団体 USENIX 協会が発表した調査では、回答者の 75%が、Web ブラウザはプライバシーモードでは Cookie の送信を防ぐと考えていた。また、41%が同モードでのサイト閲覧時に送信元 IP アドレスを隠すことができると答えた[34]。

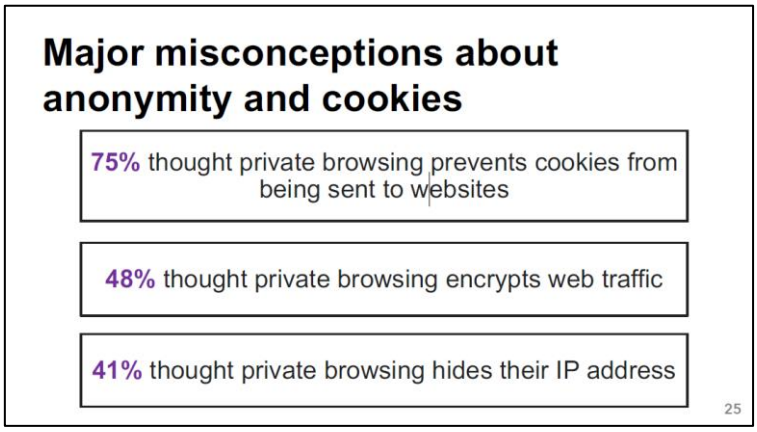

図 6 USENIX 協会の調査結果（プライバシーモードに対する誤解）

3.3. Google に対する裁判

【プライバシーモードでも情報を収集する Google に対する裁判】

2020 年 6 月 2 日、Web ブラウザのプライバシーモードを利用するユーザーを追跡し、密かに IP アドレス情報や閲覧履歴を収集することは、盗聴に関する法律や消費者のプライバシーを侵害しているとして、複数のユーザーが Google（およびその親会社のアルファベット社）に対し、集団訴訟を提起した。

Google が当時公開していたプライバシーポリシーやヘルプページ「Search & Browse Privately（図 7）」では、「Google とどのような情報を共有するかはユーザーが制御できる。プライバシーモードを利用すると、プライベートに Web 閲覧ができる。」と記載されていた。しかし前述のとおり実際には、Google は Google Analytics や広告配信の仕組みを用いて、プライバシーモードのユーザーからも IP アドレス情報や閲覧履歴を収集しており、しかもそのような説明はどこにも書かれていないと、原告は主張した。

[34] 出典：USENIX『Away From Prying Eyes: Analyzing Usage & Understanding of Private Browsing』 https://www.usenix.org/sites/default/files/conference/protected-files/soups18_slides_habib_0.pdf

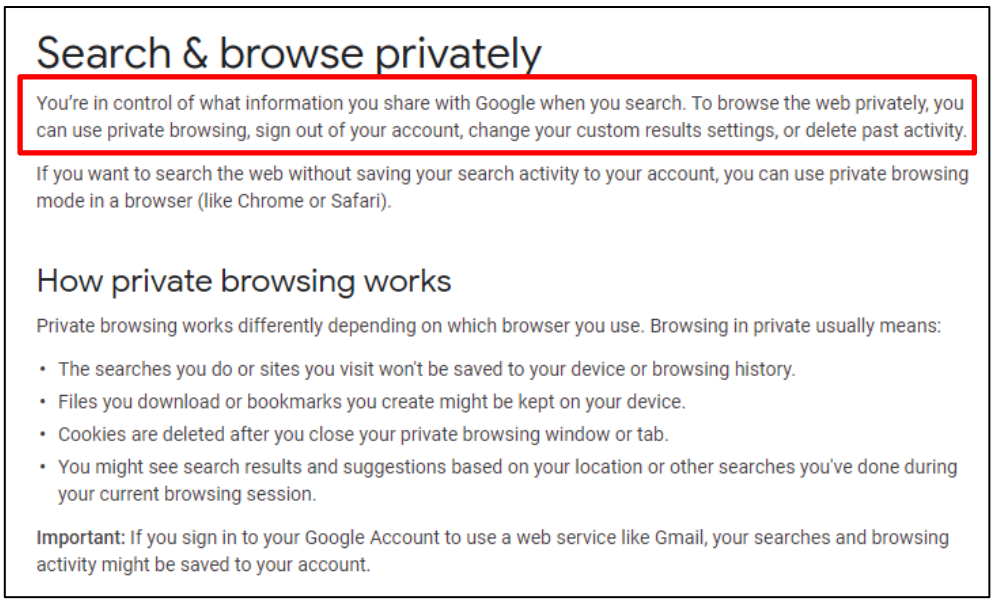

図 7「Search & Browse Privately」の記載（2020 年 5 月 29 日時点）[35]
※赤枠：「Google とどのような情報を共有するかはユーザーが制御できる。
プライバシーモードを利用すると、プライベートに Web 閲覧ができる。」と記載されている。

【和解案の提出】

本裁判で約 3 年半争った後、2023 年 12 月、Google（およびその親会社のアルファベット社）と原告は和解することに同意し、今年 4 月 1 日、米国連邦地方裁判所に和解案が提出された。

和解案では、Google が、プライバシーモードを利用したユーザーからこれまでに収集した数十億件に上るデータを削除することが示された。削除対象となるデータは、米国だけでなく世界中のユーザーから 2023 年 12 月以前に取得されたものとなっている。

和解案では Google が公開するプライバシーポリシー等の修正も求められた。現在は、同ポリシーは修正されており、Google Analytics や広告配信など Google のサービスと統合している Web サイトやアプリでは、Web ブラウザのモードに関わらず、Google と情報が共有されることが同社のサイトに記載されている[36]。また、Chrome のプライバシーモードであるシークレットモードの起動画面には、同モードを利用した場合でも、アクセスした Web サイトとそのサイトが使用するサービス（Google を含む）のデータ収集方法は変わらない旨が記載されている[37]（図 8）。

Google の広報担当は本裁判について、「常々メリットがないと考えていたこの訴訟において和解できたことを嬉しく思います。」「ユーザーがプライバシーモードを利用する際、我々がユーザーとデータを関連付けることは決してありません。」「個人と関連づけたことがなく、個人向けにサービスを最適化させるためにいかなる形式においても使用したことのない古い技術データ

[35] 出典：Internet Archive Wayback Machine『Google Search Help - Search & browse privately』
https://web.archive.org/web/20200529181357/https://support.google.com/websearch/answer/4540094
[36] 出典：Google『ポリシーと規約 - プライバシーポリシー』
https://policies.google.com/privacy?hl=ja
[37] 出典：TECH+『Google Chrome のシークレットモードの注意書きを修正へ』
https://news.mynavi.jp/techplus/article/20240119-2866246/

を、我々は喜んで削除します。」とコメントしている[38]。

和解案では、個人が Google に損害賠償を求めることは制限されておらず、現在も 50 人の個人がそれぞれ Google に対し訴えを起こしている [33]。

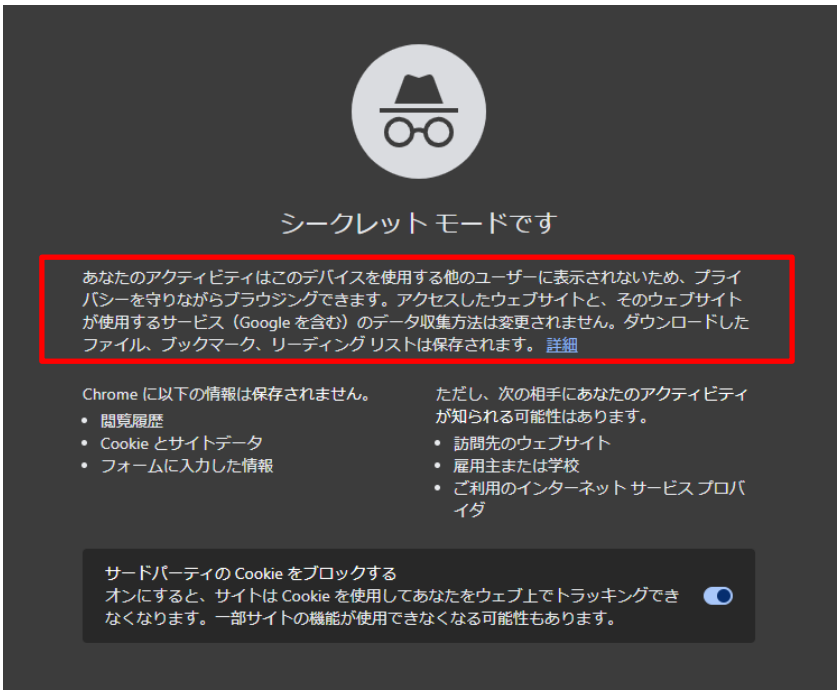

図 8 Chrome のプライバシーモードであるシークレットモードの起動画面（2024 年 5 月 10 日時点）
※赤枠：「アクセスした Web サイトと Web サイトが使用するサービス（Google を含む）の
データ収集方法は変わらない」と記載されている。

3.4. まとめ

今回の訴訟では Google のプライバシーモードについての説明が誤解を招いたことにより提訴され、和解により過去に収集されたデータは削除されることになった。

しかし、プライバシーモードの利用の有無にかかわらず、Web 閲覧履歴やその IP アドレスなどのデータは今後も収集することに変わりはない。Google には、ユーザーのプライバシーを侵害しないよう、集めたデータについて透明性を持って適切に扱うことが求められている。

以上

[38] 出典：BleepingComputer『Google agrees to delete Chrome browsing data of 136 million users』
https://www.bleepingcomputer.com/news/legal/google-agrees-to-delete-chrome-browsing-data-of-136-million-users/

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： WA_Advisorysupport@ntt.com