サイバーセキュリティレポート

2025.02

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部　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 2025 年 2 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『DeepSeek とそのリスク』

- 中国発のオープンソース生成 AI「DeepSeek-R1」が、2025 年 1 月 20 日の発表以来、経済性の高さといった面から人々の関心を集め続けている。
- DeepSeek-R1 の利用は、中国にあるクラウドでの中国政府への情報漏洩、中国政府の検閲を意識したバイアスのある出力といった安全保障上の問題に加え、国際的なコンプライアンス規制や国家間の制裁等による使用規制の可能性といった問題が懸念されている。
- 生成 AI はセキュリティにおいて様々なリスクが有るもので DeepSeek-R1 もその例外では無く、さらに中国発の生成 AI であることによるリスク等についても認識する必要がある。

第 2 章『API への攻撃の急増と AI に潜む API のリスク』

- サイバーセキュリティ企業 Wallarm が公開したレポート「API ThreatStats 2025」によると、2024 年に米 CISA の「悪用が確認された脆弱性(KEV)カタログ」に登録された脆弱性のうち、50%以上が API への攻撃に関連するものとなっており、API が主要な攻撃経路となっている。
- 外部公開された AI に関連した API のうち、89%が強固ではない認証方式を採用しており、ブルートフォース攻撃などの潜在的なリスクを抱えている。
- API への攻撃による被害の規模は大きくなる傾向があり、API セキュリティの強化は最優先に取り組むべき課題である。

第 3 章『放棄された Amazon S3 バケットの悪用リスク』

- 人気のクラウドストレージサービス「Amazon S3」において、ユーザーはデータを「バケット」と呼ばれる場所に保存する。だが、バケットを放棄する場合に適切な処理を行わないと、これを第三者に乗っ取られ、サプライチェーン攻撃等に悪用される恐れがある。
- Amazon S3 のバケット名は削除後、他のユーザーも再度同名で登録することが可能となっている。攻撃者はそのようなバケット名を狙って登録することで、以前と同じようにアクセスしてきた者に対し、攻撃を行うことができる。
- 放棄された S3 バケットの悪用は簡単に実現できるため、現状では使用者側での対策が必要である。

1. DeepSeek とそのリスク

1.1. 概要

大規模言語モデル（LLM）を活用した、中国発の生成 AI「DeepSeek-R1」が人々の関心を集め続けている[1]。2025 年 1 月 20 日に DeepSeek 社によって発表された DeepSeek-R1 は、Google や OpenAI 社等の最新 AI モデルに匹敵する性能を有する一方で、様々な技術を駆使して効率化や軽量化が図られている。これにより DeepSeek-R1 は大量の最新 GPU を必要としないとされ、これまで AI 開発に必要とされた多額のリソースへの投資が抑えられると評価されている。また、PC などのオフラインの端末上でも利用可能な、軽量化がさらに進められた AI モデルも同社からオープンソースで公開されている。

「DeepSeek Shock」と呼ばれる程に世界が関心を寄せる一方で、開発元の DeepSeek 社は中国企業であることから、オンライン利用時のサーバーが中国に有ること等、セキュリティ上の様々な問題が懸念されている。

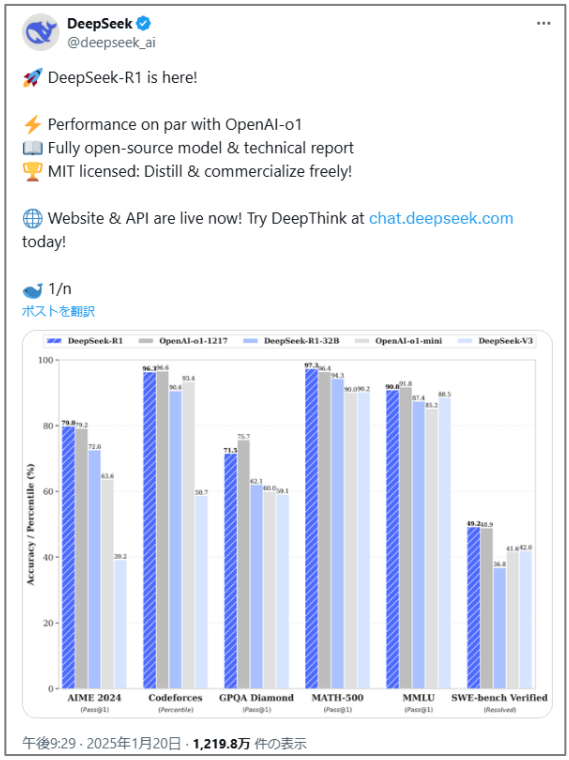

図 1 「DeepSeek-R1」発表に当たり、他社 AI モデルに対する優位を示す Deepseek 社の X のポスト[2]

1.2. DeepSeek-R1 の利用方法

DeepSeek-R1 の動作環境は大きく分けて、オンライン環境（Web 版と API 版）およびオフラインで利用可能なローカル環境の 2 種類がある。

【DeepSeek-R1 のオンライン利用】

オンライン環境では、他の生成 AI サービスと同様に、クラウドサーバーに設置された DeepSeek-R1 に対し、Web アクセス（ブラウザまたはスマホアプリからアクセス）や API リクエストを行うことで処理を実行する。主に、開発元の DeepSeek 社が提供するオンラインサービスを通じた利用が可能である。

[1] 出典：ITmedia AI＋『AI 業界に激震、突如公開の中華 AI「DeepSeek」“驚きポイント”まとめ』
https://www.itmedia.co.jp/aiplus/articles/2501/28/news091.html

[2] 出典：X『@deepseek_ai』
https://x.com/deepseek_ai/status/1881318130334814301

【DeepSeek R1 のローカル環境でのオフライン利用】

DeepSeek-R1 の特徴として、「蒸留」と呼ばれる処理の軽量化が挙げられる。蒸留では、既存の AI モデルを単純化することで必要な作業量を減らしている。DeepSeek 社は、オンライン版よりも蒸留を強めることで、オフラインのパソコン等のローカル環境でも動作する軽量版の「蒸留モデル」も開発した[3]。同社からダウンロード可能で、誰でも利用することができる。

この蒸留モデルは軽量化にあたり、精度をなるべく損なわないように調整されているが、文書能力が落ちるなど精度の低下が存在する。例えば、オンライン版では回答がはぐらかされる天安門事件といった質問に対し、蒸留モデルでは政治的な問題のある問いに対する検知能力等が低下したためか、詳細な回答をするといったことが検証されている[4]。

さらに、この蒸留モデルは無料で商用利用可能なオープンソースであり、同 AI をベースに開発された派生モデルをダウンロードして利用したり、自分で開発したりすることも可能である。一般的なパソコンやスマートフォン単体の環境においても動作するモデルも公開されている[5]。すでに一定の分野に秀でた派生モデルが開発者によって提供されており、日本国内の企業ではサイバーエージェント社が、追加学習により日本語処理を強化した派生モデルを無料公開している[6]。

1.3. DeepSeek-R1 利用のセキュリティ上の問題

【使用回避が進むオンライン利用】

オンライン利用をする際は、中国企業である DeepSeek 社が管理しているクラウドにアクセスする必要があるため、同社での処理における安全性が疑問視されている。中国では、公的機関からサーバーの調査や個人情報へのアクセス等を要求された場合、市民は協力しなければならない。これは、強い権限を有する中国政府が定めた、複数の法律により義務付けられている[7]。このようなことから各国の政府や企業は、組織内で DeepSeek-R1 のオンライン利用を禁止する通達を、相次いで出している[8]。

日本でも、個人情報保護委員会が 2025 年 2 月 3 日に「DeepSeek に関する情報提供」を発表し、日本国内でサービス提供体制が構築されている他のサービスとは異なり、個人情報を含むデータの扱いについて留意すべき点があることが呼びかけられている（**図 2**）。既に、トヨタ自動車や三菱重工業、ソフトバンク等の企業が、アクセスを規制する等、社内での利用を禁止している[9]。

---

[3] 出典：日経クロステック（xTECH）『わずか 1 週間で名をとどろかせた DeepSeek の実力と、登場で NVIDIA 株が急落した理由』
https://xtech.nikkei.com/atcl/nxt/column/18/03084/020500010/

[4] 出典：ITmedia AI＋『話題の中華 LLM「DeepSeek R1」は、天安門事件を説明できるか あれこれ質問した』
https://www.itmedia.co.jp/aiplus/articles/2501/23/news179.html

[5] 出典：ASCII.jp『完全無料！話題の DeepSeek R1 をローカルで動かしてみた。Mac やスマホでも OK！』
https://ascii.jp/elem/000/004/249/4249857/

[6] 出典：X『@CyberAgent_PR』
https://x.com/CyberAgent_PR/status/1883783524836413468

[7] 出典：個人情報保護委員会『外国制度(中華人民共和国)』
https://www.ppc.go.jp/enforcement/infoprovision/laws/offshore_report_china/

[8] 出典：読売新聞『中国ＡＩ「ディープシーク」、個人情報流出の懸念…世界で数百社が使用制限』
https://www.yomiuri.co.jp/economy/20250201-OYT1T50166/

[9] 出典：産経新聞『トヨタや三菱重工が中国 AI ディープシークの利用禁止 情報漏洩を懸念の動き広がる』
https://www.sankei.com/article/20250212-A6B2IDTBG5OCFN7H5FFV2FOW5I/

図 2 個人情報保護委員会発表『DeepSeek に関する情報提供』[10]

他にも、DeepSeek-R1 のアルゴリズムには、中国政府による検閲を意識し、政府に都合の良い回答を出すバイアスが組み込まれている可能性が指摘されている[11]。そのため、特定の政治的意図に沿った情報が提供されるリスクも指摘されている。さらに、入力データは生成 AI の学習に利用される可能性があり、例えば機密データを含んだ情報を学習させた場合、第三者が AI で生成したデータに機密が含まれるといったことが起こる恐れがある。なお、この学習におけるデータ利用の問題は DeepSeek-R1 に限らず、各社の生成 AI の利用においても見られる共通の問題である。

【オフライン利用にも残存する問題】

DeepSeek-R1 のオフライン版では、自前の環境で全ての処理が行われるため、中国政府による規制の問題は無いと考えられている。ただし、中国政府に都合の良いアルゴリズムがオフライン版でも残存する可能性は否定できない。さらに、オフライン版に特に問題がなかったとしても、GDPR といったコンプライアンス規制や[12]、国家間対立による制裁といった米中デカップリング[13]（米国/中国陣営間の分断）がテクノロジーの利用にも影響を与え、DeepSeek-R1 の使用が全面禁止されるリスクも懸念される。実際に、政府機関での中国企業の製品の利用禁止ルールを定める国では、このルールを理由に、オフライン利用でのインストールを含め DeepSeek 社製品を全て利用禁止とする通達が政府組織（オーストラリア政府、米国海軍、NASA

[10] 出典：個人情報保護委員会『DeepSeek に関する情報提供』
https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/

[11] 出典：CNN『DeepSeek is giving the world a window into Chinese censorship and information control』
https://edition.cnn.com/2025/01/29/china/deepseek-ai-china-censorship-moderation-intl-hnk/index.html

[12] 出典：Forbes『The Hidden Risks Of Open Source AI: Why DeepSeek-R1's Transparency Isn't Enough』
https://www.forbes.com/councils/forbestechcouncil/2025/03/06/the-hidden-risks-of-open-source-ai-why-deepseek-r1s-transparency-isnt-enough

[13] 出典：RIETI『中国経済新論：実事求是　関志雄「二期目のトランプ政権における対中政策の展望－懸念される米中デカップリングの加速－」』
https://www.rieti.go.jp/users/china-tr/jp/ssqs/250107ssqs.html

等）で行われている[14] [15]。

また、公開されている派生モデルは気軽にダウンロードして利用できる反面、開発者の信頼性の確認が十分でない場合の危険性もある。ブームに便乗して、派生モデルをインターネット上からダウンロードしようとする利用者を狙ったマルウェアの配布やフィッシングといった攻撃も、既に確認されている[16]。さらに、入手した生成 AI モデルのトレーニングが偏ったものであった場合、利用者がそれと認識することは難しいとも指摘されている[17]。

【OpenAI 社との係争】

DeepSeek 社は蒸留の技術を用いて、OpenAI 社の AI を不正にコピーし DeepSeek-R1 を開発したと疑われている[18]。実際に、特定のプロンプト（指示や質問）に対し DeepSeek-R1 が自身を OpenAI と紹介したとの指摘もされている。OpenAI 社と同社に出資する Microsoft 社は、DeepSeek 社が利用規約に違反し不正に得た出力データを利用して競合モデルを開発した可能性があるとして、調査を進めている[19]。

1.4. まとめ

そもそも生成 AI はセキュリティにおいて様々なリスクが有り、DeepSeek-R1 もその例外ではないことを認識する必要がある。それに加えて、安全保障上のリスクに留意することはもちろん、他社 AI の権利侵害やデカップリング等から、生成物を含め使用が認められなくなるといったことも今後懸念される。

[14] 出典：Cybernews『Australia bans DeepSeek on government devices』
https://cybernews.com/news/deepseek-ban-australia/

[15] 出典：CNBC『NASA becomes latest federal agency to block China's DeepSeek on 'security and privacy concerns'』
https://www.cnbc.com/2025/01/31/nasa-becomes-latest-federal-agency-to-block-chinas-deepseek.html

[16] 出典：日経クロステック（xTECH）『DeepSeek に便乗するサイバー犯罪者、マルウエア配布やフィッシング詐欺相次ぐ』
https://xtech.nikkei.com/atcl/nxt/column/18/03084/021100012/

[17] 出典：Forbes『The Hidden Risks Of Open Source AI: Why DeepSeek-R1's Transparency Isn't Enough』
https://www.forbes.com/councils/forbestechcouncil/2025/03/06/the-hidden-risks-of-open-source-ai-why-deepseek-r1s-transparency-isnt-enough/

[18] 出典：Harvard Law School『DeepSeek, ChatGPT, and the global fight for technological supremacy』
https://hls.harvard.edu/today/deepseek-chatgpt-and-the-global-fight-for-technological-supremacy/

[19] 出典：Bloomberg『DeepSeek がオープンＡＩデータ不正入手か、マイクロソフト調査中』
https://www.bloomberg.co.jp/news/articles/2025-01-29/SQTXNQT0AFB400

2. API への攻撃の急増と AI に潜む API のリスク

2.1. 概要

サイバーセキュリティ企業 Wallarm が公開したレポート「API ThreatStats 2025」[20]により、API (Application Programming Interface) に対する攻撃が増加傾向にあることが明らかになった。また、企業での AI の活用が急速に進む中、AI に関連した API の脆弱性が急増しており、潜在的な攻撃のリスクを抱えていることについても、同レポートは警告している。

2.2. API への攻撃のトレンド

API はシステム間でデータをやり取りするインターフェイスである。自社と他社のサービスを相互に活用し、経済圏を拡大する考え方として「API エコノミー」という言葉が生まれているように、自社サービスの API を積極的に外部公開して価値を高める動きが進んでいる[21]。

このような動きの中、攻撃者は API を主要な攻撃経路として捉えるようになっている。2024 年に米 CISA (サイバーセキュリティ・インフラストラクチャセキュリティ庁)の「悪用が確認された脆弱性(KEV)カタログ」に登録された脆弱性のうち、50%以上が API への攻撃に関連するものであり、2023 年の 20%から急増した [20]。従来は、ブラウザやカーネル、サプライチェーンに関係する脆弱性などが高い割合を占めていたが、API への攻撃に関する脆弱性が史上初めて上回ったことからも、攻撃の主軸がシフトしていることが分かる。

図 3 KEV に占める API への攻撃に関連した脆弱性の割合 [20]

また、API はシステム間でデータをやり取りするという性質上、攻撃に遭った時に被害規模が大きくなる傾向がある。2024 年に発生した API への攻撃による被害事例を以下にピックアップしたが、いずれも漏洩した情報の件数が 1,000 万件を超えている。

[20] 出典：Wallarm『AI Security is API Security』(「Wallarm Annual 2025 API ThreatStats Report」ダウンロードページ) https://www.wallarm.com/reports/2025-api-security-report

[21] 出典：Kong Inc.『API Impact Report 2024: AI Adoption and Innovation Challenges』(ダウンロードページ) https://konghq.com/resources/reports/ai-and-api-adoption-challenges

- 2024 年 1 月、Atlassian 社のタスク管理ツール Trello の API の認証の不備を突かれ、1,500 万件のユーザーアカウント情報が流出した[22]。
- 2024 年 4 月、Dell 社のパートナー向けポータルサイトの API を介して、4,900 万件の顧客情報が流出した[23]。
- 2024 年 6 月、Twilio 社が運営する多要素認証アプリ Authy の API が悪用され、3,300 万件の電話番号が流出した[24]。

2.3. AI に関連した API のセキュリティリスクの増大

AI(人工知能)を利用する上であまり意識することはないかもしれないが、AI のシステムを構成するモデルやユーザーインターフェース間のデータのやり取り、AI を利用したアプリケーションとの外部連携などは、API によって実現されている。

企業での AI の活用が急速に進む[25]一方、2024 年に共通脆弱性識別子 CVE (Common Vulnerabilities and Exposure) が採番された脆弱性のうち、AI に関連した脆弱性も前年比 1,025%増の 439 件と急速に増加しており、これらの脆弱性のうち、98.9%は API にも関連したものだった [20]。

また、AI に関連した API の 57%が外部公開されているが、これらの API のうち、89%が静的な API キーや Basic 認証のような、セキュリティ的に堅牢ではない認証方式を採用している [20]。このような API はブルートフォース攻撃などの潜在的なリスクを抱えた状態で利用されているため、OAuth や JWT のような、より堅牢な認証方式を採用することが推奨されている。

2.4. まとめ

外部公開された API は攻撃者にとって格好の標的となり得るため、API セキュリティの強化は最優先に取り組むべき課題である。組織的な API 利用範囲の統制、インシデント発生時の対応プロセスの確立・見直しも重要である。

特に、企業での AI の活用が進む一方、サイバー攻撃により機密情報の流出や不正データの混入などビジネスに大きなインパクトを及ぼすリスクも高まっており、AI に関連した API のセキュリティ対策は経営課題と言える。

---

[22] 出典：BleepingComputer『Trello API abused to link email addresses to 15 million accounts』 https://www.bleepingcomputer.com/news/security/trello-api-abused-to-link-email-addresses-to-15-million-accounts/

[23] 出典：BleepingComputer『Dell API abused to steal 49 million customer records in data breach』 https://www.bleepingcomputer.com/news/security/dell-api-abused-to-steal-49-million-customer-records-in-data-breach/

[24] 出典：BleepingComputer『Hackers abused API to verify millions of Authy MFA phone numbers』 https://www.bleepingcomputer.com/news/security/hackers-abused-api-to-verify-millions-of-authy-mfa-phone-numbers/

[25] 出典：Gartner『Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026』 https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026

3. 放棄された Amazon S3 バケットの悪用リスク

3.1. 概要

人気のクラウドストレージサービス「Amazon S3」において、ユーザーはデータを「バケット」と呼ばれる場所に保存する。だが、バケットを放棄する場合に適切な処理を行わないと、これを第三者に乗っ取られ、サプライチェーン攻撃等に悪用される恐れがある。脅威インテリジェンスサービスの watchTowr Labs は、放棄された S3 バケットの動向を検証したレポートを発行し、その悪用のリスクについて警告している[26]。

3.2. AWS と S3 バケットについて

AWS（Amazon Web Service）は、世界で最も利用されているクラウドサービスの総称であり、ショッピングサイトで有名な Amazon が 2006 年から同サービスを提供している。世界シェアのランキングで 2 位の Microsoft Azure と、3 位の Google Cloud よりも早くサービスを開始し、低コストで柔軟なサービスの組み合わせが可能なことで人気を集めてきた[27]。

この AWS が提供するサービスのひとつが Amazon S3（S3 は Simple Storage Service の意）で、データの管理やバックアップに利用可能なクラウドストレージを提供する。その、データを保存する場所をバケットと呼ぶ。クラウド上に保存したデータには、URL 経由でアクセスすることができるため、例えば、Web サイトで使う画像などのデータをバケットに保存し、これを任意のページから参照することも可能である。

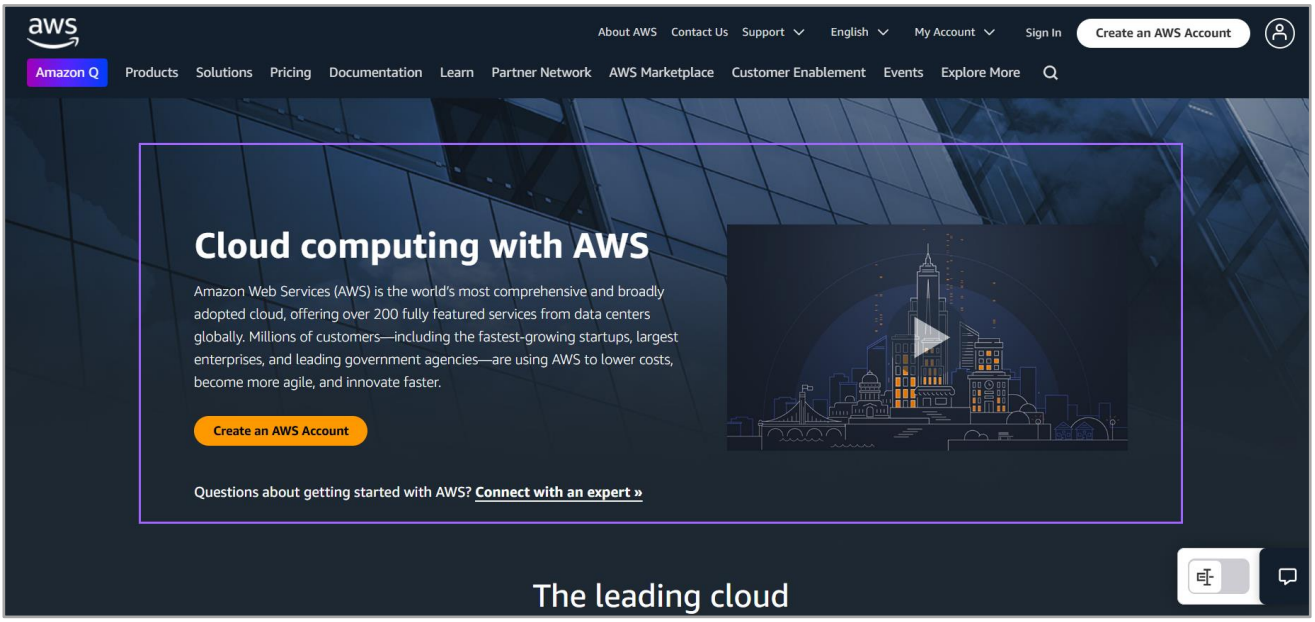

図 4 Amazon の AWS 公式サイト[28]

[26] 出典：watchTowr Labs『8 Million Requests Later, We Made The SolarWinds Supply Chain Attack Look Amateur』
https://labs.watchtowr.com/8-million-requests-later-we-made-the-solarwinds-supply-chain-attack-look-amateur/

[27] 出典：NTT 東日本『Amazon クラウドサービスとは？特徴やメリット・デメリットを紹介』
https://business.ntt-east.co.jp/content/cloudsolution/column-342.html

[28] 出典：Amazon Web Services, Inc. 『What is AWS?-Cloud computing with AWS』
https://aws.amazon.com/what-is-aws/?nc1=h_ls

3.3. 放棄された S3 バケットの悪用リスクについて

【S3 バケットの再利用】

S3 バケットには識別のために S3 バケット名が付与される。このバケット名は、当該 S3 バケットの中のファイルにアクセスする URL 等に使用される（例えば「**amzn-s3-demo-bucket**」というバケット名であれば、URL は「https[://]**amzn-s3-demo-bucket**[.]s3[.]amazonaws[.]com/」）。S3 バケット名はグローバルで一意であるが、S3 バケットを削除した数時間後には他のユーザーでも同じバケット名を登録することが可能になっている。

これが問題となるのは、削除した S3 バケット（放棄バケット）へのリンクが Web サイトやアプリケーション等に残っている時に、他の Amazon S3 ユーザーが同じ名前で S3 バケットを作成した場合である。この新たな S3 バケットには、放棄バケットに割り当てられていた URL がそのまま引き継がれるため、上記の Web サイト等に残るリンクから現在の（新たな）S3 バケットにアクセスできる。

【放棄された S3 バケット（放棄バケット）の悪用】

放棄された S3 バケットは、ブラウザでアクセスすると以下のような状態になっている。

図 5 放棄された S3 バケットにアクセスした時の画面の例[29]

放棄される前、取引先と共用する業務ファイルの置き場所や、ソフトウェアのアップデートファイルのダウンロード先等として利用されていた S3 バケットを攻撃者が見つけると、自らの AWS アカウントを使って、同じ名前の S3 バケットを作成する。そして不正なファイルをこの S3 バケットにアップロードし、放棄バケットと同じ URL に誰かがアクセスするのを待つ。

攻撃者は、持ち主が変わったことを知らずに当該 S3 バケットにアクセスしたユーザーが、アップデートや業務データと勘違いして不正ファイルをダウンロードすることを期待する。もし、そのファイルにアクセスし、ダウンロードした者が自身の PC で実行した場合、マルウェアに感染し、攻撃者のハッキング活動等に繋がる。このような活動の影響が他の組織にも広がればサプライチェーン攻撃が発生することも考えられる。

なお、このような放棄された S3 バケットの悪用事例は、実際に確認されている。演算に関連する bignum というソフトウェアパッケージの配布において S3 バケットが使われていたが、2023 年に、開発者が放棄した S3 バケットを攻撃者が乗っ取り、

[29] 出典：watchTowr Labs『8 Million Requests Later, We Made The SolarWinds Supply Chain Attack Look Amateur』 https://labs.watchtowr.com/8-million-requests-later-we-made-the-solarwinds-supply-chain-attack-look-amateur/

bignum での更新ファイルの代わりに認証情報を盗む不正コードを配布するという事件が発生している[30]。

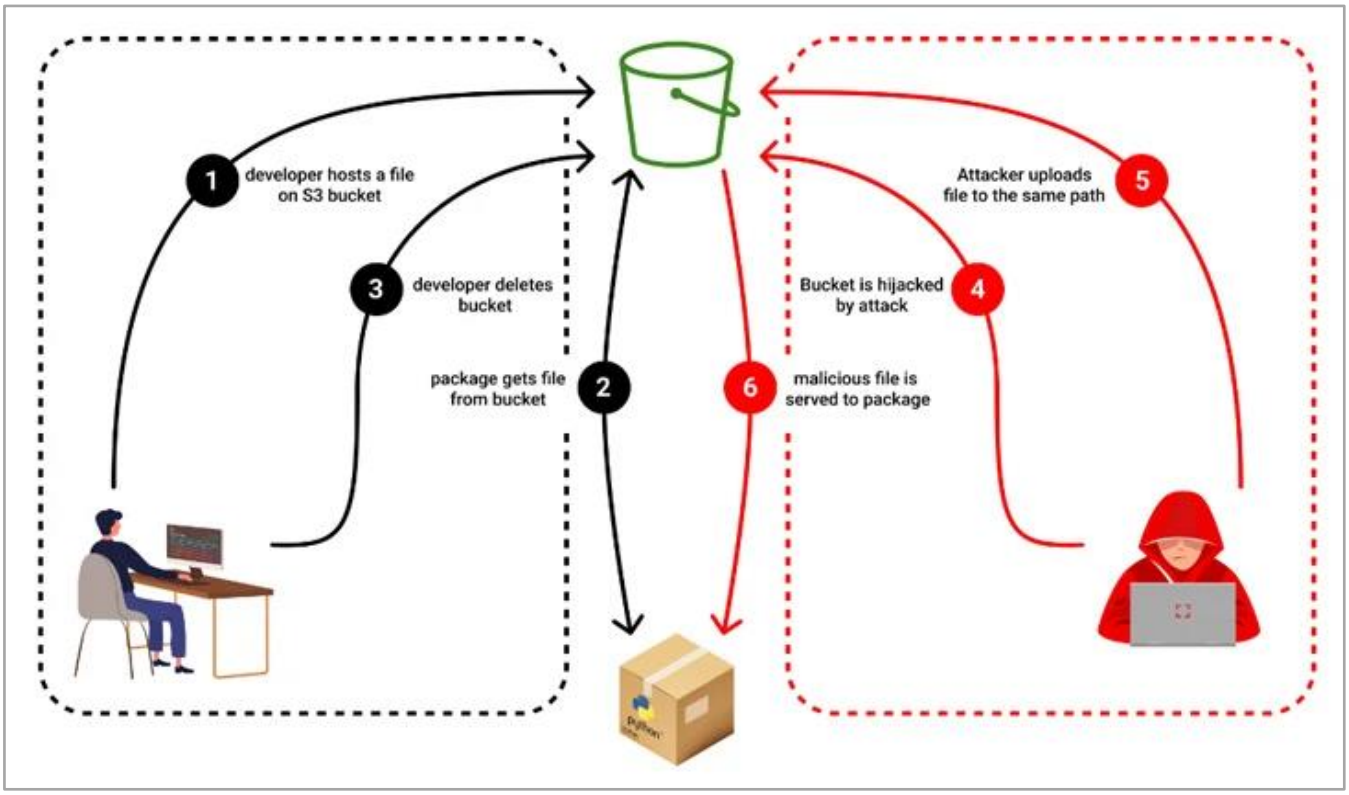

図 6 パッケージソフト（bignum）に関連した放棄バケットの悪用事例[31]

＜図 3 の補足＞

[開発者(左)]

① 開発者は S3 バケットにファイルをアップロードする。

② パッケージ管理ソフトが S3 バケットからファイルを取得する。

③ S3 バケットが不要となり、開発者が削除する。

[攻撃者(右)]

④ 攻撃者が、削除(放棄)された S3 バケットと同名のバケットを作成する（放棄バケットを乗っ取る）。

⑤ 攻撃者が S3 バケット(放棄前と同じ URL)に不正なファイルをアップロードする。

⑥ 不正なファイルがパッケージ管理ソフトに配布される。

【watchTowr Labs の検証】[32]

2 月、脅威インテリジェンスサービス watchTowr Labs は、約 150 個の放棄された S3 バケットを同じ名前で再登録し、それらがどのように使われているかを検証したレポートを発表した。watchTowr Labs が発見したこれらの放棄 S3 バケット

[30] 出典：The Hacker News『New Supply Chain Attack Exploits Abandoned S3 Buckets to Distribute Malicious Binaries』 https://thehackernews.com/2023/06/new-supply-chain-attack-exploits.html

[31] 出典：The Hacker News『New Supply Chain Attack Exploits Abandoned S3 Buckets to Distribute Malicious Binaries』 https://thehackernews.com/2023/06/new-supply-chain-attack-exploits.html

[32] 出典：watchTowr Labs『8 Million Requests Later, We Made The SolarWinds Supply Chain Attack Look Amateur』 https://labs.watchtowr.com/8-million-requests-later-we-made-the-solarwinds-supply-chain-attack-look-amateur/

は、商用およびオープンソースのソフトウェア製品の展開・更新用に使用した後、不要となって削除・放棄されたものであった。S3 バケット自体は削除されていたものの、アプリケーションや Web サイトは、依然としてその S3 バケットに対しアップデートやコードの取得を要求していた。

なお、これらソフトウェア製品の使用者には政府や有名企業も見られた。watchTowr Labs が、検証用に再登録したこれらの S3 バケットを 2 か月間監視したところ、NASA や米国政府のネットワークなどから Windows 等の実行ファイルに関する 800 万以上のリクエストが送られてきたことが分かったという。リクエストの発信元には、軍事ネットワークや有名企業、金融サービス企業、セキュリティ企業、世界中の大学なども含まれていた。この結果から、多種多様の重要な組織で放棄バケットに対する適切な処置が行われていないことが分かる。これらの組織が、Web サイトやアプリケーションに放棄バケットへのリンクが残っていることを認識しないまま利用を継続した場合、悪意を持った個人や国家レベルの攻撃者による放棄バケットの乗っ取りが、甚大な被害に繋がる可能性がある。

3.4. まとめ

放棄された S3 バケットの悪用は、AWS で同じ S3 バケットの名前を再登録するだけで簡単に実現できる。このような手法は AWS だけでなく、他のクラウドプロバイダの類似したサービスでも同様に悪用されるリスクが潜んでいると考えられる。Amazon が S3 バケット名の再利用を禁止しない理由は不明だが、プロバイダとして「AWS のサービスは期待通りに運用されている」との姿勢を示している[33]。そのため、現状では利用者側での対策が重要で、意図しない放棄された S3 バケットの再利用を防ぐため、S3 バケット名を作成するときに偶発的に再利用されにくいユニークな名前を使用すること、また、システムの変更等により S3 バケットの放棄があった後はアプリケーションや Web サイトが放棄予定の S3 バケットを参照していないか確認し、代替となる参照先に修正する等の対応が必要である。

以上

[33] 出典：The Register『Abandoned AWS S3 buckets can be reused in supply-chain attacks that would make SolarWinds look 'insignificant'』
https://www.theregister.com/2025/02/04/abandoned_aws_s3/

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

プロフェッショナルサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt