サイバーセキュリティレポート

2024.01

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 1 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『NIST が AI の攻撃分類に関するレポートを発行』

- NIST（米国国立標準技術研究所）が「敵対的機械学習：攻撃と緩和策の分類と用語」と題するレポートを発行した。
- 敵対的機械学習についての共通理解、および AI を管理するための基準やガイドを作成する際にベースとなる情報を提供することを目的に発行されたもので、予測型 AI に対する攻撃と生成 AI を悪用する攻撃を分類し紹介している。
- AI に関する攻撃情報が体系的にまとめられているため、AI を導入する際のリスク評価に活用できると考えられる。

第 2 章『260 億件に及ぶ漏洩情報「Mother of all Breaches」が発見される』

- 1 月 22 日、サイバーセキュリティメディア「Cybernews」は、260 億件以上の漏洩情報が流通していることを発見し「Mother of all Breaches（MOAB）」と名付けたと発表した。
- 元となったデータは不明だったが、1 月 24 日、セキュリティ企業「Leak - Lookup」は、同社が漏洩情報検索サービス用に蓄積していたデータが元であり、ファイアウォールの設定ミスによりデータを窃取されたことを認めた。
- MOAB のような漏洩情報は以前から流通しており、様々な攻撃で悪用されている。特にクレデンシャルスタッフィング攻撃での悪用が深刻である。多要素認証や FIDO の導入など、セキュリティ対策の強化を検討する必要がある。

第 3 章『Ivanti の VPN 製品にゼロデイ脆弱性、広範囲での悪用を確認』

- 1 月 10 日、Ivanti は VPN 製品「Ivanti Connect Secure」と「Ivanti Policy Secure」にゼロデイ脆弱性があることを明らかにした。悪用された場合、認証メカニズムを回避して任意のコマンドを実行できる可能性がある。その後も 3 つの脆弱性を追加で発表した。
- Ivanti の脆弱性発表後すぐに攻撃手法が広まり、本脆弱性を悪用した侵害が増加した。1 月 16 日の時点で確認された侵害件数は 2,100 台以上であった。
- 相次ぐゼロデイ脆弱性に対処するためには、対応フロー等、組織レベルで準備をしておくことが求められている。

1. NIST が AI の攻撃分類に関するレポートを発行

1.1. 概要

1 月、NIST（米国国立標準技術研究所）が AI の攻撃分類に関するレポートを発行した[1]。本章では、そのレポートで示された AI に対する／AI を利用した攻撃の分類について紹介する。

1.2. NIST が発行したレポートについて

1 月 4 日、NIST は「敵対的機械学習：攻撃と緩和策の分類と用語」と題するレポートを発行した[1]。

機械学習とは AI を実現するための技術の一つである。これにおいて、コンピューターはデータから自動的に学習し、データの背景にあるルールやパターンを発見する[2]。敵対的機械学習とは、機械学習の実施過程や利用において、どのような攻撃が可能なのか、攻撃を防ぐにはどうしたらよいかを明らかにする研究領域である。

この NIST のレポートは、急速に発展する敵対的機械学習に対する共通理解を確立することと、AI システムを評価管理するための基準や実践ガイドを作成する際のベースとなる情報を提供することを目的として作成された。また、このレポートでは、AI を**予測型 AI** と**生成 AI** に分け、AI に関する様々な文献を基に、AI に対する攻撃と AI を利用した攻撃の分類と用語の定義を行っている。

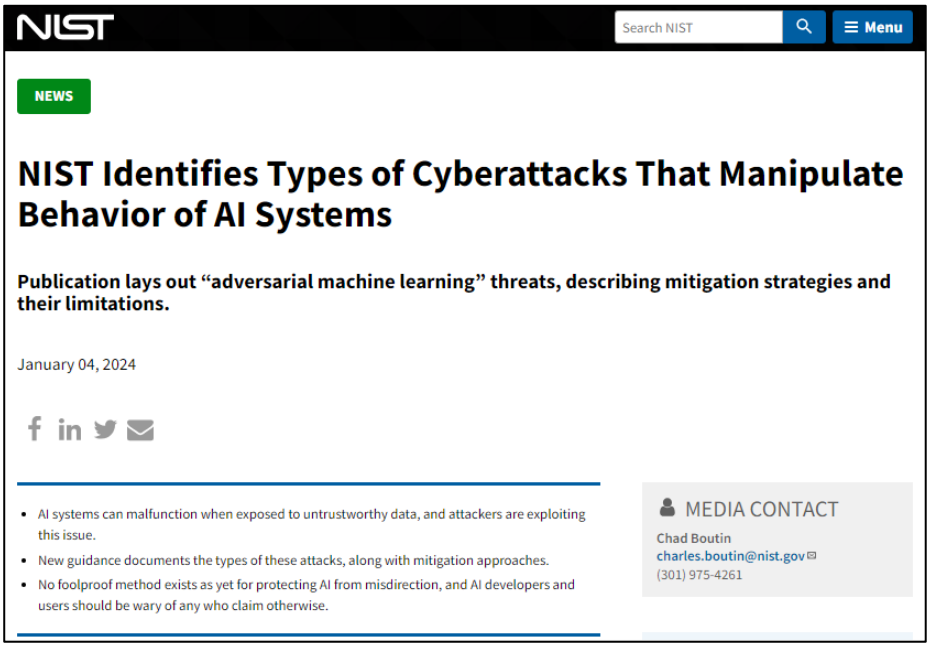

図 1 NIST による本レポートのニュースリリース[3]

[1] 出典：NIST『NIST AI 100-2 E2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations』 https://csrc.nist.gov/pubs/ai/100/2/e2023/final

[2] 出典：野村総合研究所（NRI）『機械学習 | 用語解説』 https://www.nri.com/jp/knowledge/glossary/lst/ka/machine_learning

[3] 出典：NIST『NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems』 https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

1.3. 予測型 AI に対する攻撃の分類

予測型 AI とは、物体の検出や情報の分類といった用途に使用される AI であり、自動運転や画像診断などに使用される。
NIST のレポートでは、予測型 AI に対する攻撃を 3 つのカテゴリに分類している。

【回避攻撃】

回避攻撃とは、AI への入力を変更してシステムの応答を変更しようとする攻撃手法である。
例として、一時停止標識にマークを追加することにより、自動運転車にこれを速度制限標識と誤認させたり、車両を道路から逸脱させるために紛らわしい車線のマークを作成したりすることが挙げられる。

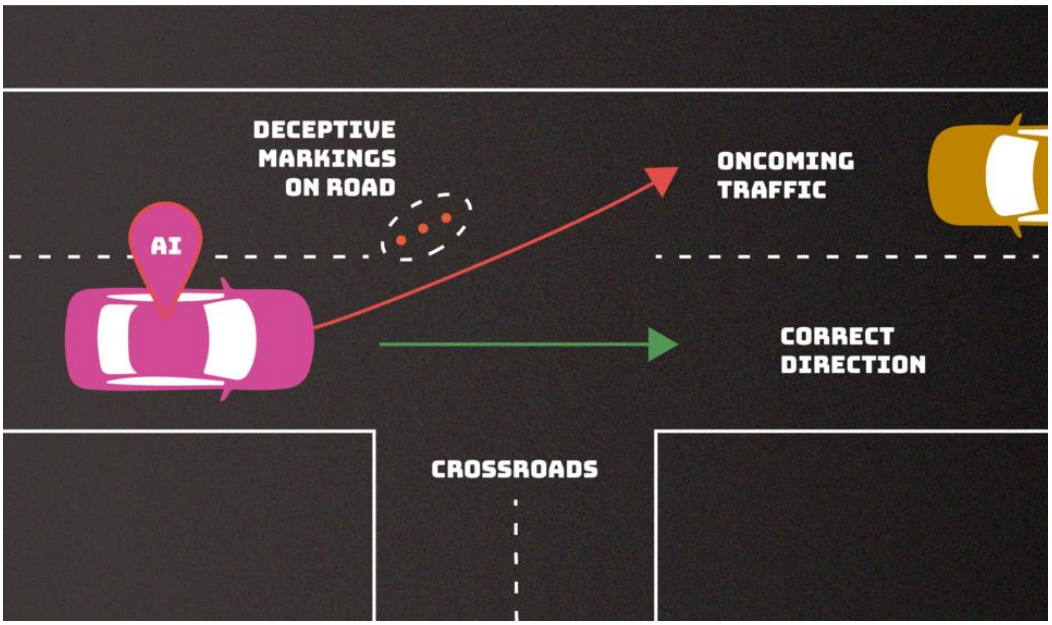

図 2 自動運転車に対する回避攻撃の例 [3]
（攻撃者が設置した偽のマークで自動運転車が対向車線に逸脱する）

【ポイズニング攻撃】

ポイズニング攻撃とは、AI の学習に使用するデータを改ざんし、それを学習した AI を攻撃することである。
チャットボットを作成する際に、AI が学習する会話データに不適切な言葉を多数潜り込ませることで、それらを会話の中で利用して良い一般的な言葉としてチャットボットに解釈させるといったことが、この攻撃に当たる。

【プライバシー攻撃】

プライバシー攻撃とは、AI に関する機密情報を収集したり、AI が学習した情報を抽出し悪用したりする攻撃である。
攻撃者が、AI に多数の正当な質問をし、その回答を使用して AI の内部動作をリバースエンジニアリングし弱点を見つけたり、AI の回答から、AI が学習した内容を攻撃者が推論し悪用したりすることが、この攻撃に当たる。

1.4. 生成 AI を悪用する攻撃の分類

生成 AI とは、学習データと同様の特性を持つ、テキストや画像などのコンテンツを生成できる AI である。
NIST のレポートは、予測型 AI に対する攻撃分類も生成 AI に対して有効であると述べるとともに、生成 AI を悪用する攻撃として 3 つの攻撃分類を紹介している。

【AI サプライチェーン攻撃】

AI サプライチェーン攻撃とは、生成 AI を構成するライブラリやプログラム、データを介して行われる攻撃である。
生成 AI は、様々なライブラリ（機械学習用の TensorFlow や画像処理用の OpenCV 等）やプログラムを基に構成されている。生成 AI が利用するこれらのライブラリやプログラムを予め攻撃者が改ざんし、生成 AI の動作と共に任意のコードを実行させること等が攻撃の例として挙げられる。

【ダイレクトプロンプトインジェクション攻撃】

コンテンツを生成させるために、利用者が生成 AI に出す指示や命令をプロンプトという。
ダイレクトプロンプトインジェクション攻撃とは、攻撃者が生成 AI に悪意のあるプロンプトを直接送信して、AI が本来意図していない動作を実行させることである。攻撃者はこれを利用して、生成 AI が持つ安全対策機能を回避し、生成 AI に対し、マルウェアとして利用可能なソースコードや性的な画像といった有害なコンテンツを生成させたり、生成 AI の学習データに含まれる可能性がある機密情報を回答させたりしようとする。

【インダイレクトプロンプトインジェクト攻撃】

インダイレクトプロンプトインジェクション攻撃とは、攻撃者が、悪意のあるプロンプトを生成 AI に直接送らずに、生成 AI を悪用する攻撃である。例えば、生成 AI の 1 つである LLM（大規模言語モデル）に統合された検索エンジンで、検索クエリにより参照される Web サイトや SMS での投稿にあらかじめ悪意のある内容を配置しておくことで、生成 AI に悪意のある回答や想定外の動作を行わせる。または、攻撃者が利用者を騙して生成 AI に悪意のあるプロンプトを入力させることで、生成 AI から機微な情報を含んだ回答を引き出す[4]。

1.5. まとめ

今回発行された NIST のレポートには、現時点で想定される、AI に対する攻撃および AI を悪用した攻撃が網羅的にまとめられている。
これから AI を導入する組織も多いと考えられる。AI を導入する際はメリットだけでなく、リスクも検討する必要があり、AI を導入することで発生し得る攻撃や悪用事例を想定し対策するにあたり、この NIST のレポートで示された AI の攻撃分類は非常に活用し易い。また、既に AI を導入済みの組織でも、リスクを再度見直すために活用できると考えられる。

[4] 出典：arXiv『Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection』
https://arxiv.org/pdf/2302.12173.pdf

2. 260 億件に及ぶ漏洩情報「Mother of all Breaches」が発見される

2.1. 概要

1 月 22 日、サイバーセキュリティメディア「Cybernews」は、260 億件以上の漏洩情報が流通していることを発見したという記事を公開した[5]。このデータは「Mother of all Breaches」（全ての漏洩情報の母）と名付けられた。漏洩情報としては未曾有の規模であり、多くのセキュリティニュースで取り上げられ、注目を集めた。

2.2. Mother of all Breaches とその出所

【Mother of all Breaches の特徴】

Mother of all Breaches（以下「MOAB」）は、Cybernews がセキュリティ研究者の Bob Dyachenko との共同調査により発見した約 260 億件の漏洩情報である。LinkedIn、Twitter、Weibo、Tencent、といった複数の著名な Web サービスのユーザーデータで構成されており、認証情報も含まれている。これまでに発見された漏洩情報としては最大規模であり、2019 年に発見された漏洩情報ファイル群「Collection#1」（27 億件）[6]の 10 倍近くに及ぶ。12 テラバイトという膨大な容量だが、このデータベースにはインデックスと呼ばれる索引が付けられており、大量のデータでも扱いやすいように加工されている。

BRANDS WITH 100M+ LEAKED RECORDS

BRAND NAME	RECORDS LEAKED
Tencent	1.5B
Weibo	504M
MySpace	360M
Twitter	281M
Wattpad	271M
NetEase	261M
Deezer	258M
LinkedIn	251M
AdultFriendFinder	220M
Zynga	217M
Luxottica	206M
Evite	179M
Zing	164M
Adobe	153M
MyFitnessPal	151M
Canva	143M
JD.com	142M
Badoo	127M
VK	101M
Youku	100M

cybernews

図 3 MOAB に含まれていた漏洩元 Web サービスおよび漏洩件数の内訳(Cybernews より)

[5] 出典：cybernews『Mother of all breaches reveals 26 billion records: what we know so far』
https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/

[6] 出典：INTERNET Watch『国内 800 万件のアカウント情報流出が判明、ダークウェブに出現した約 27 億件の巨大漏えいファイル群「Collection#1」事件』
https://internet.watch.impress.co.jp/docs/news/1171134.html

漏洩情報を収集しているセキュリティ会社「SpyCloud」は、同社が蓄積している漏洩情報と MOAB を比較した分析を行った[7]。それによると、MOAB のうち少なくとも 94%は過去の漏洩事件で流出したもの等、既知のデータであった。残りは、同社にとって未知のものだったが、公の場で配布されたのではなく、非公開で取引されたデータ等ではないかと推測している。

【ハッカー達の反応】

Cybernews の報道後、セキュリティ関係者だけでなくハッカー達の間でも、MOAB はどこから出てきて、どこで入手できるのかと、大きな話題になった。MOAB を発見できなかったハッカー達は、セキュリティ企業が注目を集めるために作成した偽データだろうと疑ったり、過去の侵害データを集めたものにすぎないだろうと推測したりしていた。

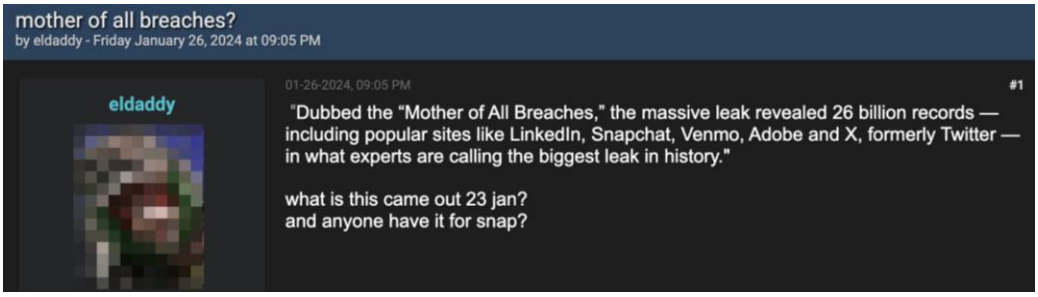

図 4 ハッカーフォーラムでの MOAB についてのスレッド

【MOAB の出所】

そのような中、1 月 24 日、漏洩情報を蓄積し、顧客の漏洩状況をチェックするサービスを提供しているセキュリティ企業「Leak-Lookup」は、X(旧 Twitter)公式アカウントに、Cybernews の投稿を引用する形で、MOAB は自社のデータが元であり、ファイアウォールの設定ミスによって侵入を受けデータを窃取されたことを認める投稿を行った[8]。

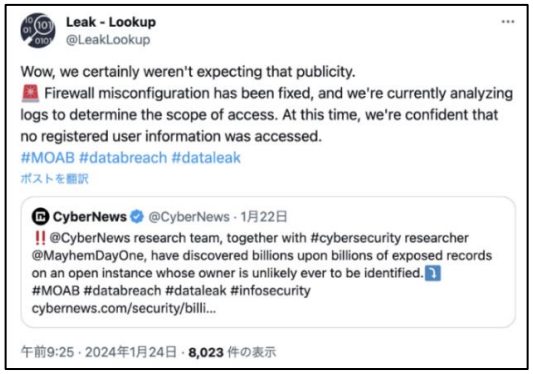

図 5 漏洩を認めた Leak - Lookup の投稿

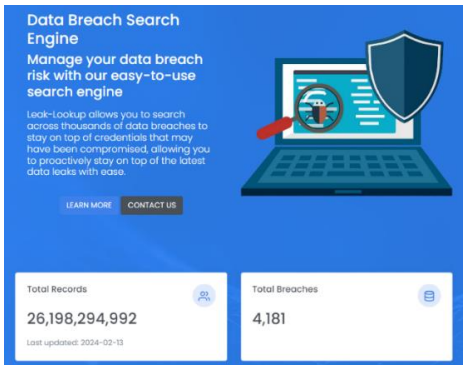

図 6 Leak - Lookup の Web サイト
約 260 億件の漏洩情報の蓄積を誇っている[9]

[7] 出典：SpyCloud『What We Know About the MOAB Data Leak』
https://spycloud.com/blog/moab-data-leak-what-we-know/

[8] 出典：X『@LeakLookup』
https://twitter.com/LeakLookup/status/1749951429693919400

[9] 出典：Leak–Lookup『Leak - Lookup | Data Breach Search Engine』
https://leak-lookup.com/

2.3. 漏洩情報の収集と再配布

過去の漏洩情報を収集し利用しているのはセキュリティ企業に限ったことではない。例えば、世界最大規模のハッカーフォーラム「Breachforums」では、同フォーラムとその前身である RaidForums に投稿された漏洩情報を蓄積し、フォーラムの参加者たちに提供している。現時点でおよそ 150 億件の漏洩情報を取り扱っている。

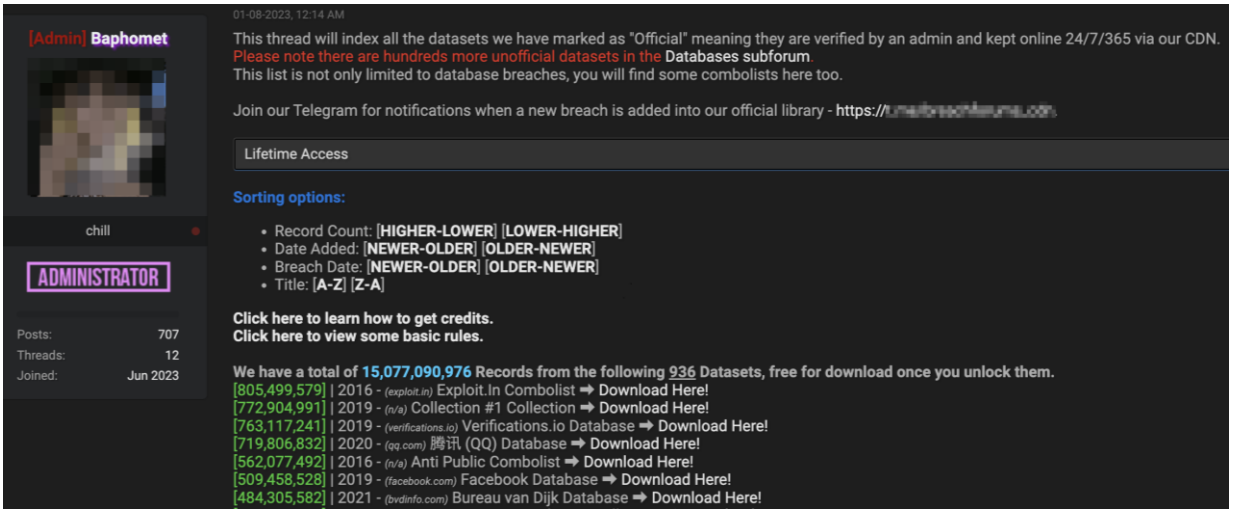

図 7 Breachforums の漏洩情報一覧ページ

また、Telegram においても、過去にランサムウェア攻撃等によって暴露されたとみられる情報を収集し、有償/無償で再配布しているチャンネルが複数存在する。

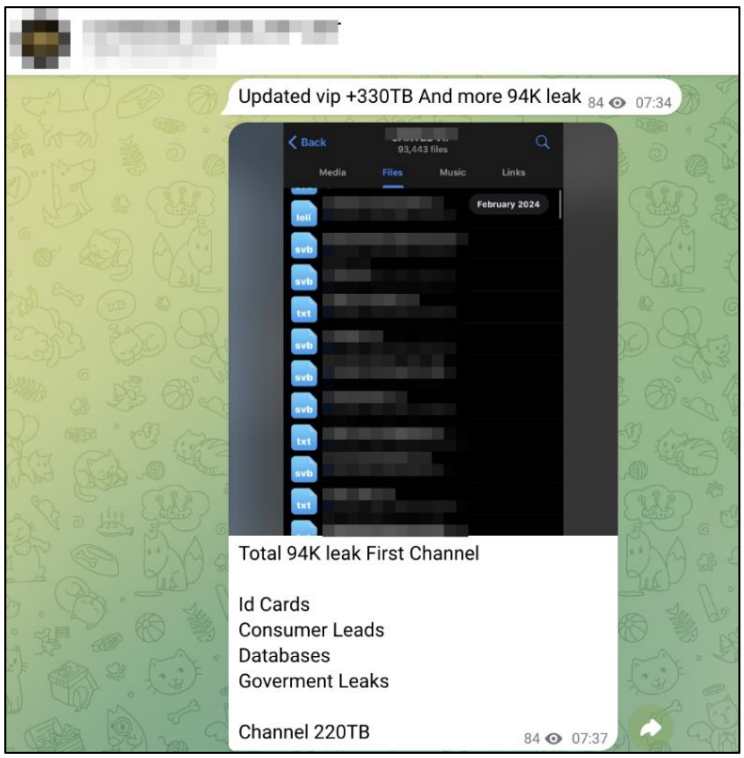

図 8 Telegram で過去の漏洩情報を収集、配布しているチャンネル

2.4. まとめ

過去最大級の漏洩データとして話題になった MOAB だが、実際には以前から、世界人口の数倍にも及ぶ規模の漏洩情報が流通し、様々なサイバー攻撃で悪用されている。

特に、クレデンシャルスタッフィング攻撃（別名「パスワードリスト型攻撃」）への悪用は深刻である。パスワード使い回しが危険であることは繰り返し、様々な形で周知されているにも関わらず、多くのユーザーが SNS やオンラインショッピング等、複数の異なるサービスで、同じメールアドレス／パスワードのペアを認証情報として使用していることが知られている。漏洩情報を入手した攻撃者はその情報を使って、様々なサービスでログインを試みる。パスワードを使い回していると、一カ所から漏洩した情報で攻撃者に様々なサービスへのアクセスを許すことになる。このような状況から、サービス提供者は、ユーザーがパスワードの使い回しを行っており、攻撃者が認証情報を持っている前提に立ち、多要素認証や FIDO などの対策を講じた認証システムを構築する必要がある。

3. Ivanti の VPN 製品にゼロデイ脆弱性、広範囲での悪用を確認

3.1. 概要

2024 年 1 月 10 日、米 IT 管理企業の Ivanti は、同社の VPN 製品「Ivanti Connect Secure」と「Ivanti Policy Secure」に 2 件の脆弱性があることを明らかにした[10]。しかし 2 件とも、発表前に既に中国系 APT とみられるグループによって悪用されていたゼロデイ脆弱性であった。Ivanti の発表直後には PoC が公開されて攻撃手法が広く知られるようになったことから、被害が急増[11]。その後も、侵入に繋がりかねない新たな脆弱性が確認され、1 月 31 日には 2 件（うち 1 件はゼロデイ脆弱性）[12]、2 月 8 日 には 1 件[13]が追加発表された。最初の脆弱性発表時には修正パッチの提供が追い付かず、Ivanti はパッチ未対応のデバイスについて、緩和策の実施を推奨した。修正パッチはその後、順次公開されている。

3.2. Ivanti について

Ivanti は米国に本社を持ち、IT 資産管理をはじめとして、IT セキュリティ管理、IT サービス管理、エンドポイント管理などの機能をひとつのプラットフォームでユーザーに提供している[14, 15]。2020 年 12 月には Pulse Secure LLC を買収した[16]。顧客数は世界中で 4 万社以上に上る[17]。

【脆弱性の影響を受ける製品】

影響を受けるのは以下の 2 製品である。

○**Ivanti Connect Secure**（旧: Pulse Connect Secure）：世界中の多くの企業で利用されている SSL-VPN ソリューション[18]

○**Ivanti Policy Secure**（旧 Pulse Policy Secure）：許可、保護されたデバイスにのみネットワークアクセスを提

[10] 出典：Ivanti『CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways』
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

[11] 出典：VOLEXITY『Ivanti Connect Secure VPN Exploitation: New Observations』
https://www.volexity.com/blog/2024/01/18/ivanti-connect-secure-vpn-exploitation-new-observations/

[12] 出典：Ivanti『CVE-2024-21888 Privilege Escalation for Ivanti Connect Secure and Ivanti Policy Secure』
https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

[13] 出典：Ivanti『CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy Secure』
https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

[14] 出典：Ivanti『Ivanti について』
https://www.ivanti.com/ja/company/about-ivanti

[15] 出典：CYBERNET『Ivanti（旧 LANDESK）とは』
https://www.cybernet.co.jp/ivanti/about/

[16] 出典：Ivanti『Ivanti が MobileIron と Pulse Secure を買収し、あらゆる場所の企業のすべてのデバイスにインテリジェントで安全なエクスペリエンスを提供いたします』
https://www.ivanti.com/ja/company/press-releases/2020/ivanti-acquires-mobileiron-and-pulse-secure

[17] 出典：Palo Alto Networks『脅威に関する情報: Ivanti Connect Secure、Ivanti Policy Secure における脆弱性（CVE-2023-46805、CVE-2024-21887、CVE-2024-21888、CVE-2024-21893）』
https://unit42.paloaltonetworks.jp/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/

[18] 出典：Ivanti『Ivanti Connect Secure リモートアクセス VPN』
https://www.ivanti.com/ja/products/connect-secure-vpn

供するネットワークアクセス制御（NAC）ソリューション[19]

図 9 Ivanti Connect Secure ソフトウェアがインストールされるデバイス（Ivanti Secure Appliance [ISA] 6000）[20]

上記製品のバージョンのうち、脆弱性の影響を受けるのは、Ivanti がサポートしている 22 系や 9 系。サポートが終了しているバージョンについては評価されておらず、サポート対象のバージョンへの移行が推奨されている[21]。

Palo Alto Networks の報告によると、1 月 26 日から 30 日の間に、外部から接続可能であることが観測されたインスタンス数は 145 か国で 28,474 件に上った[22]。

3.3. 本脆弱性を悪用した攻撃について

【脆弱性の発見】[23]

2023 年 12 月半ば、セキュリティ企業の Volexity は、同社が監視している顧客の Web サーバーに、バックドアとして使われる Web シェルが設置されていることを発見した。その後の調査で 12 月 3 日のログにも Ivanti のデバイスに怪しい活動がみられ、Ivanti と密に連携しながら、攻撃者が「CVE-2024-21887」および「CVE-2023-46805」の脆弱性を組み合わせて悪用したことを突き止めた。

【攻撃者について】

今回の Volexity が発見した攻撃は、同社が UTA0178[24]として（Mandiant は UNC5221[25]として）追跡している中国系 APT グループによるものと考えられている。このグループは発覚を避けるため、攻撃の隠蔽を様々に行っていた。Ivanti の当

[19] 出典：Ivanti『Policy Secure Administration Guide』
https://help.ivanti.com/ps/help/en_US/IPS/22.x/ag/ips_intro_pulse_policy_secure.htm

[20] 出典：Ivanti『ISA6000 Hardware Guide』
https://help.ivanti.com/ps/help/en_US/ISA/6000hw/landingpage.htm

[21] 出典：JPCERT/CC『Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起』
https://www.jpcert.or.jp/at/2024/at240002.html

[22] 出典：Palo Alto Networks『脅威に関する情報: Ivanti Connect Secure、Ivanti Policy Secure における脆弱性（CVE-2023-46805、CVE-2024-21887、CVE-2024-21888、CVE-2024-21893)』
https://unit42.paloaltonetworks.jp/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/

[23] 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/

[24] 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/

[25] 出典：MANDIANT『Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation』
https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

該製品にはシステムの改ざんを検知するための整合性チェッカーツールが実装されていたが、APT グループはこのツール自体にも攻撃を行い、攻撃の発覚を困難にしていた。

【ゼロデイ脆弱性発表から侵害拡大へ】

侵害件数は Ivanti の脆弱性の発表後に増大し、16 日に第三者により PoC が公開されると、情報窃取やマルウェアのダウンロードなど様々な攻撃が行われるようになった[26]。被害に遭った組織は世界中に広がっており、その中には様々な規模の民間企業だけでなく、政府機関や軍事部門も含まれている。さらに、Ivanti 社の修正用パッチの発行が予定より遅れたことも被害拡大に拍車をかけた。バックドアとなる Web シェルが存在するデバイスについて、Volexity が 14 日にスキャンしたところ 1,700 台以上が特定され、16 日には 2,100 台以上となった[27, 28]。その後、検出メカニズムを避けるためとみられる、当 Web シェルの亜種の存在も確認されている[29]。

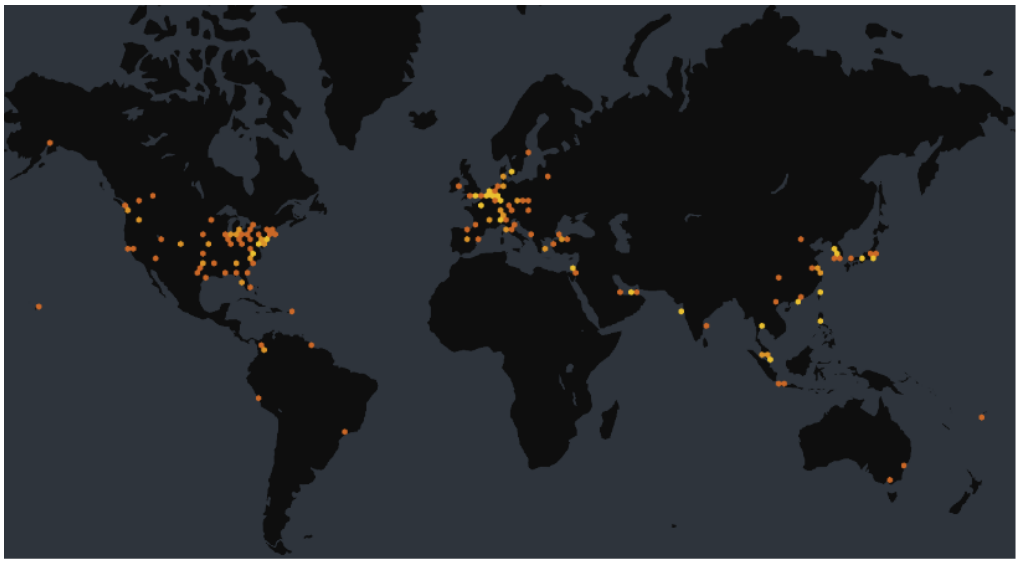

図 10 侵害された Ivanti Connect Secure の分布図[30]

【追加の脆弱性発表】

Ivanti は攻撃を認知した後、自社製品の調査を行った。その結果、上記の脆弱性の他にも認証回避の脆弱性「CVE-2024-21893」および特権昇格の脆弱性「CVE-2024-21888」を発見し、1 月 31 日に公表した。「CVE-2024-

[26] 出典：JPCERT/CC『Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起』
https://www.jpcert.or.jp/at/2024/at240002.html

[27] 出典：VOLEXITY『Ivanti Connect Secure VPN Exploitation Goes Global』
https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

[28] 出典：VOLEXITY『Ivanti Connect Secure VPN Exploitation: New Observations』
https://www.volexity.com/blog/2024/01/18/ivanti-connect-secure-vpn-exploitation-new-observations/

[29] 出典：QUOINTELLIGENCE『UNC5221: Unreported and Undetected WIREFIRE Web Shell Variant』
https://quointelligence.eu/2024/01/unc5221-unreported-and-undetected-wirefire-web-shell-variant/

[30] 出典：Censys『The Mass Exploitation of Ivanti Connect Secure』
https://censys.com/the-mass-exploitation-of-ivanti-connect-secure/

21893」もゼロデイ脆弱性であり、この悪用により新しいバックドアが展開されている[31]。さらに、2 月 8 日にも侵入に繋がる脆弱性「CVE-2024-22024」が発表された。この脆弱性も発表直後に PoC が公表されており、サーバー上のアカウント情報の窃取等に既に使われている可能性が指摘されている[32]。

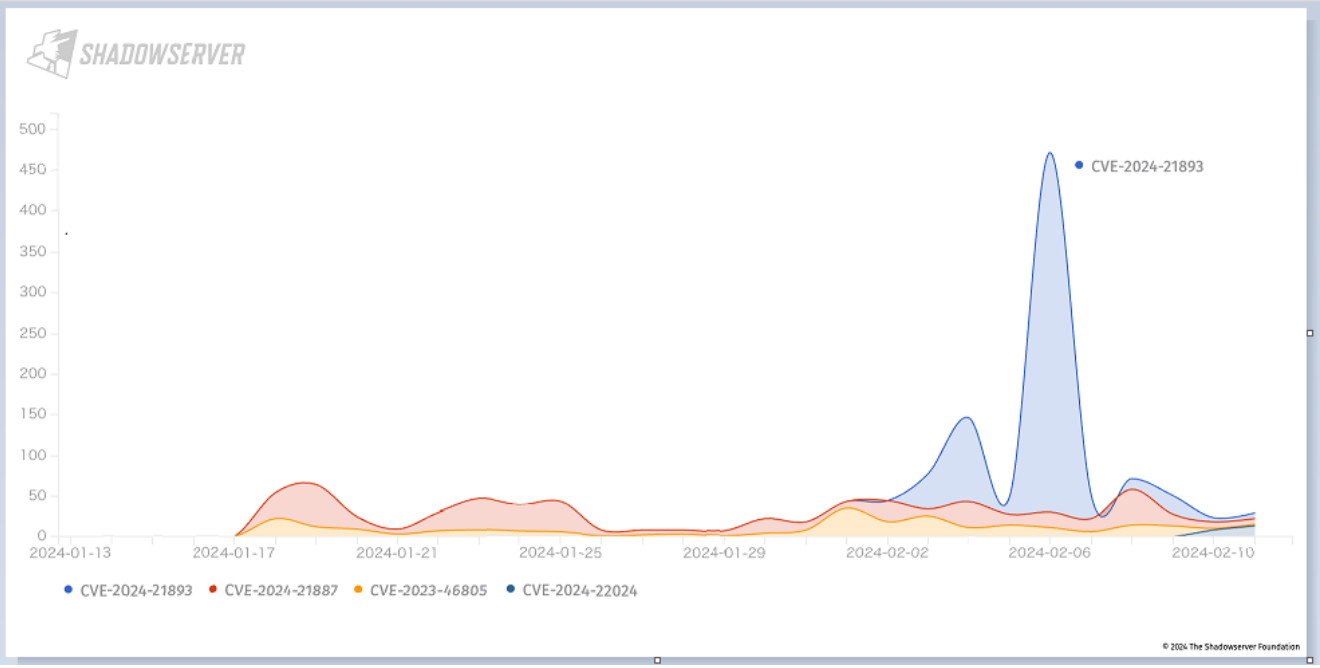

図 11 Ivanti を標的とした攻撃の件数（SHADOWSERVER による検知 [2 月 13 日時点]）[33]

【公的機関による注意喚起】

米政府機関である CISA（米国土安全保障省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）は Ivanti が発表した脆弱性のうち 3 件を、CISA の「既知の悪用された脆弱性一覧」に追加し、注意喚起を行った。また、悪用のリスクが甚大であるため、Ivanti の VPN 製品に対する回避策を実施するよう、19 日に米連邦政府機関に対して緊急指令「ED24-01」を発行した。さらに、1 月末の脆弱性の追加発表の直後には、脆弱な Ivanti 製品をネットワークから切り離すといった踏み込んだ対策を、48 時間以内に実施するよう要請した[34]。日本の JPCERT/CC も Ivanti の発表の直後に注意喚起を発表し、状況の変化があった際には更新を逐次行っている[35]。

---

[31] 出典：BleepingComputer『Hackers exploit Ivanti SSRF flaw to deploy new DSLog backdoor』
https://www.bleepingcomputer.com/news/security/hackers-exploit-ivanti-ssrf-flaw-to-deploy-new-dslog-backdoor/

[32] 出典：SecurityWeek『Exploitation of Another Ivanti VPN Vulnerability Observed』
https://www.securityweek.com/exploitation-of-another-ivanti-vpn-vulnerability-observed/

[33] 出典：SHADOWSERVER『Attack statistics』
https://dashboard.shadowserver.org/statistics/honeypot/time-series/?date_range=30&host_type=src&vendor=ivanti&group_by=vulnerability&style=stacked

[34] 出典：CISA『Supplemental Direction V1: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities』
https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure

[35] 出典：JPCERT/CC『Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起』
https://www.jpcert.or.jp/at/2024/at240002.html

3.4. まとめ

Ivanti はリモートアクセス用の VPN 製品として、大企業や政府機関など世界各地の様々な組織で非常に広く利用されている。侵害を受けたデバイスから LAN 内に侵入される恐れがあり、ハッキングの対象としても狙われやすい。現在もこの脆弱性の悪用は増大しており、対策をしていない組織に対する脅威は高まるばかりである。

最近の VPN 製品の重大な脆弱性は、APT が利用したゼロデイとして発表されることがよく見られる。そして、発表直後から攻撃手法が様々な攻撃者に共有され、未対応のユーザーを襲う展開がたびたび起きている。本件も同様の展開であった上に、Ivanti からの発表は五月雨で、根本的な修正パッチの提供は後手に回った。ゼロデイ攻撃から組織を確実に守るためには、場合によっては、CISA の勧告のように製品をネットワークから切り離す緊急回避も必要となる。組織全体に影響が出る緊急対応を速やかに実行できるよう、ゼロデイ脆弱性が発表された場合の対応フロー等、組織レベルでの準備が求められている。

以上

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