サイバーセキュリティレポート

2025.01

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 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『警察庁が中国系ハッカー集団 MirrorFace のサイバー攻撃について注意喚起』

- 警察庁と内閣サイバーセキュリティセンター（NISC）は、中国の関与が疑われるハッカー集団「MirrorFace」についての注意喚起を行った。この喚起は、標的となり得る日本の組織や個人に対し、中国によるサイバー攻撃への注意と対策を促すために出されたものである。
- 標的型サイバー攻撃を行う MirrorFace のキャンペーンは、日本の安全保障や先端技術に関する情報窃取を目的としており、その標的には、昨年サイバー攻撃による情報漏洩を発表した宇宙航空研究開発機構（JAXA）も含まれている。
- 今回日本が中国を名指しして警告を出したことは注目に値する。日本は中国によるサイバー攻撃を深刻に受け止めており、公に警告を発することで日本が適切な対策を講じる準備があることを中国にアピールし、また国際社会に対して中国の行動を非難する姿勢を示すものとみられる。

第 2 章『ダブルクリックジャッキング攻撃を狙った Web ページの脅威』

- 従来から知られており対策も普及しているクリックジャッキング（Clickjacking）とはアプローチが異なる、「ダブルクリックジャッキング」（DoubleClickjacking）という新たな攻撃手法が最近発見され、話題となった。
- ダブルクリックジャッキングの罠が仕込まれた Web ページへとアクセスしたユーザーに、指定した位置でダブルクリックを促し、1 クリック目の直後に正規サイトのログインページ等にすり替えて、2 クリック目で同じ座標にある重要なボタンをクリックさせるという手法である。
- ダブルクリックジャッキングは、OAuth 等でのアカウントの乗っ取りに悪用可能な手法と検証されている。今後のブラウザや各種 Web ページにおける実装により、ダブルクリックジャッキング対策が進むことが期待される。

第 3 章『暴露型ランサムウェア攻撃 2024 年活動まとめ』

- 2024 年は、前年以前から引き続き、年間を通してランサムウェアグループによる被害組織に関する暴露サイトへの投稿に増加傾向が見られた。
- ブランド力のあるランサムウェアグループが取り締まりを受け衰退したが、代わりに他の RaaS がイニシャルアクセスブローカーやアフィリエイトを取り合うように伸張した。RaaS と組むこれらの側が、ランサムウェア犯罪ビジネスのイニシアティブを取っている状況が改めて明らかになった。
- 国際的な法執行機関による取り締まりが行われても、サイバー犯罪者は別のプラットフォームに移りランサムウェア攻撃を継続する。取り締まり徹底のために、そのような状況を放置する国家への圧力等の動きが、将来の解決策にとって重要と言える。

1. 警察庁が中国系ハッカー集団 MirrorFace のサイバー攻撃について注意喚起

1.1. 概要

1 月 8 日、警察庁と内閣サイバーセキュリティセンター（NISC）は、中国の関与が疑われるハッカー集団「MirrorFace」についての注意喚起を行った。標的型サイバー攻撃を行う MirrorFace のキャンペーンは、日本の安全保障や先端技術に関する情報窃取を目的としており、その標的には宇宙航空研究開発機構（JAXA）も含まれている。この喚起は、他にも標的となり得る日本の組織や個人に対し、中国によるサイバー攻撃への注意と対策実施を促すために出されたものである[1]。

図 1 警察庁のサイトに掲載された注意喚起[2]

1.2. MirrorFace の攻撃キャンペーン

ハッカー集団「MirrorFace」の日本におけるキャンペーンは、2019 年頃から続いており、210 件[3]の攻撃が確認されている。その事例には、複数のサイバー攻撃を受け、2024 年に不正アクセスによる情報漏洩を発表[4]した宇宙航空研究開発機構

[1] 出典：警察庁『MirrorFace によるサイバー攻撃について（注意喚起）』
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html
[2] 出典：警察庁『MirrorFace によるサイバー攻撃について（注意喚起）』
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html
[3] 出典：日本経済新聞『中国系ハッカー、日本を標的　JAXA などに、19 年以降攻撃 210 件』
https://www.nikkei.com/article/DGKKZO85934170Y5A100C2PD0000/
[4] 出典：JAXA『JAXA において発生した不正アクセスによる情報漏洩について』
https://www.jaxa.jp/press/2024/07/20240705-2_j.html

（JAXA）も含まれている。中国は日本の安全保障や先端技術に関する情報窃取を目的としており、宇宙開発において重要な技術情報や研究データを有する JAXA が標的になったとみられる。MirrorFace は日本を主な標的とする一方、昨年秋には EU 内の外交組織への攻撃が[5]、また 2023 年には、ごく少数ではあるが台湾やインドでの攻撃も観測された[6]。

警察庁は今回発表した注意喚起の中で、MirrorFace の攻撃キャンペーンとして下記の 3 つを挙げている。

種類	時期	標的	攻撃事例
キャンペーン A	2019 年～2023 年 (2024 年にも確認)	日本のシンクタンク、政府、政治家、マスコミ等の個人や組織	システムへの侵入方法： ・標的に対してメールを送付。添付されていたファイルを受信者が開くと、バックドア構築型マルウェア（システムへの侵入口を設置するためのマルウェア）である LODEINFO に感染 - 件名は当時の安全保障情勢や国際情勢に関連 - 送信者の詐称も見られた 侵入後の活動： ・Windows Sandbox を悪用したマルウェアの展開
キャンペーン B	2023 年	日本の半導体、製造、情報通信、学術、航空宇宙の分野に関する組織	システムへの侵入方法： ・VPN 機器(Fortinet 等)の脆弱性の悪用 ・SQL インジェクションの実行 侵入後の活動： ・バックドア構築型マルウェアの Cobalt Strike BEACON、LODEINFO、NOOPDOOR の展開 ・Active Directory サーバー、Microsoft 365 へのアクセス等
キャンペーン C	2024 年 6 月頃～	日本の学術、シンクタンク、政治家、メディアに関係する個人や組織	システムへの侵入方法： ・標的型メールを送付し、本文内のリンクをクリックするよう受信者に促す。クリック後に開かれた Web ページで、受信者が zip ファイルをダウンロードして開くと、バックドア構築型マルウェアである ANEL に感染する。 - 件名に使用されていたキーワードは、「取材のご依頼」、「所蔵資料のおすすめ」、「国際情勢と日本外交」等 -送信者の詐称も見られた 侵入後の活動： ・Windows Sandbox を悪用し、さらにマルウェアを展開 ・遠隔操作ツールとして Microsoft の Visual Studio Code (VS Code)を悪用

図 2 MirrorFace のキャンペーンの種類と特徴[7]

[5] 出典：トレンドマイクロ『Spot the Difference: Earth Kasha's New LODEINFO Campaign And The Correlation Analysis With The APT10 Umbrella』
https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html

[6] 出典：トレンドマイクロ『MirrorFace（ミラーフェイス）とは？～警察が注意喚起を行った標的型攻撃グループを解説～』
https://www.trendmicro.com/ja_jp/jp-security/25/a/expertview-20250109-01.html

[7] 出典：警察庁『MirrorFace によるサイバー攻撃について（注意喚起）』
https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf

1.3. 特徴的な攻撃手法

今回の警察庁と NISC の発表で明らかになったのは、端末を LODEINFO 等のバックドア構築型マルウェアに感染させて、攻撃者によるリモートアクセスや指令サーバーとの通信を可能にした後、Windows に搭載された一時的なデスクトップの仮想環境である Windows Sandbox を悪用して、別のマルウェアを活動させるという手法である。 Sandbox は感染端末に直接影響を与えない、隔離された環境である。だが、限定的ではあるものの外部との通信が可能で、Sandbox 内に設置されたマルウェアは、外部ネットワークとの通信や、感染端末内のファイルへのアクセス（共有フォルダを介して行う）が可能となっていた。このような隔離環境を利用した手法は、ウイルス対策ソフトや EDR 等からの検知逃れ、また、端末の遮断時に Sandbox 内の感染した環境が消去されることによる証拠隠滅を狙ったと考えられている。

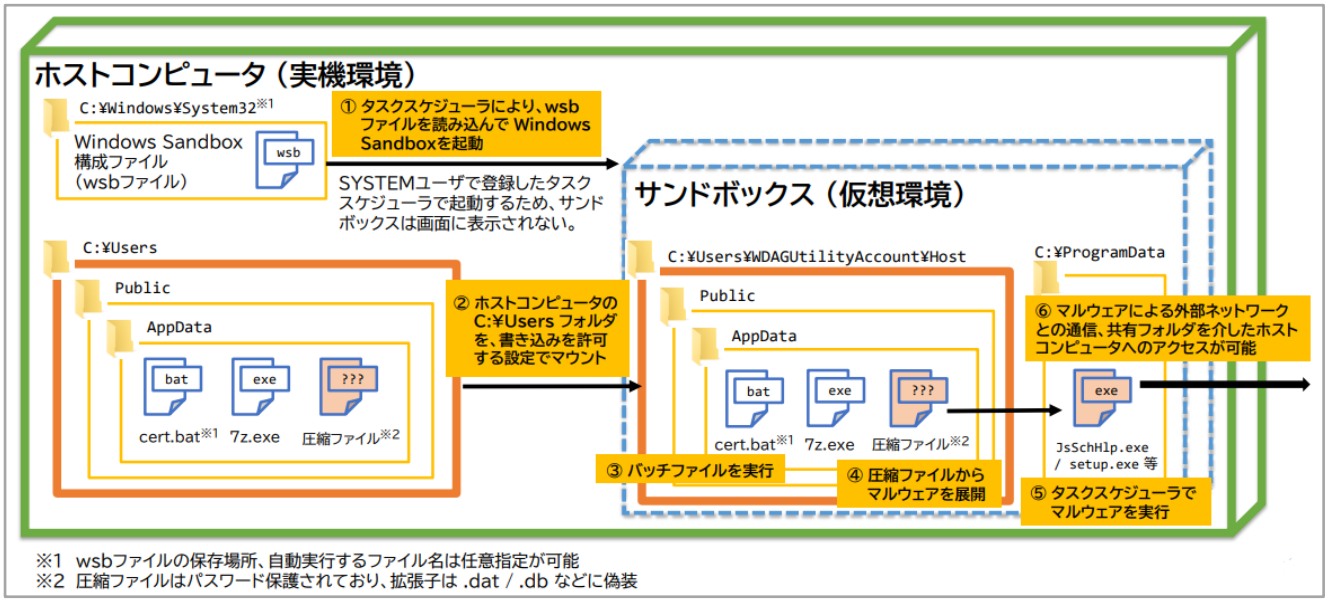

図 3 Windows Sandbox を悪用した攻撃手口（警察庁の資料より）[8]

加えて、感染端末に対する指令等、外部ネットワークとの間の通信をトンネル化して秘匿するために、Microsoft の正規のテキストエディターである Visual Studio Code（VSCode）のリモートトンネル機能を使用するといった事も行われていた[9,10]。

1.4. まとめ

MirrorFace の日本への攻撃は以前より度々報道されていたが、今回日本が中国を名指しして警告を出したことは注目に値する。日本は中国によるサイバー攻撃を深刻に受け止めており、公に警告を発することで日本が適切な対策を講じる準備があることを中国にアピールし、また国際社会に対して中国の行動を非難する姿勢を示すものとみられる。

---

[8] 出典：警察庁『MirrorFace によるサイバー攻撃について（注意喚起） 別添資料「Windows Sandbox を悪用した手口及び痕跡・検知策」』 https://www.npa.go.jp/bureau/cyber/pdf/20250108_windowssandbox.pdf

[9] 出典：警察庁『MirrorFace によるサイバー攻撃について （注意喚起）』 https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf

[10] 出典：警察庁『MirrorFace によるサイバー攻撃について（注意喚起） 別添資料「VS Code を悪用した手口及び痕跡・検知策」』 https://www.npa.go.jp/bureau/cyber/pdf/20250108_vscode.pdf

2. ダブルクリックジャッキング攻撃を狙った Web ページの脅威

2.1. 概要

クリックジャッキングは、Web ページにおける攻撃手法である。誤ってクリックさせたいボタンの有る Web ページを、人間には見えない透明な設定にして別のページにオーバーラップ状態にすることで、意図しないクリックを狙ったものである。2011 年頃に問題となったが、ウェブサイトやブラウザに対策が施されて以降はクリックジャッキングの被害は目立たなくなった。

しかし、最近になって発見されたダブルクリックジャッキングという新たな攻撃手法が、2025 年 1 月に話題となった[11]。この新たなクリックジャッキングはユーザーのダブルクリック動作を悪用し、瞬時にクリック対象を変更することで、意図しない操作を実行させる。従来のクリックジャッキングと発想が異なるため、これまでの対策を回避できてしまう。

2.2. クリックジャッキング（Clickjacking）とは

【クリックジャッキングの手法】

従来から、SNS のページや認証のページを透明化し、これをフレームとして、攻撃者が用意した罠ページに重ねることで、ユーザーに意図しないクリック操作を行わせる攻撃手法である「クリックジャッキング」（図 4）が知られている。

クリックジャッキングは 2011 年頃[12] にはその存在が知られており、攻撃が横行したこともあった[13]。罠ページをクリックしてしまった有名人が意図せずアダルトサイトを薦める投稿を Facebook で公開し、さらに投稿からあらぬ誤解が広まるといった事件も起きた[14]。ユーザーが閲覧している Web ページに、クリックすると Facebook に自動投稿が行われる「Like」ボタンが設置されたページが透明に被せられており、動画再生等のボタンをクリックしたつもりが、見えない「Like」ボタンをクリックしていたとみられる。このように意図しない「Like」をさせられるため、クリックジャッキングは「ライクジャック」とも呼ばれた。

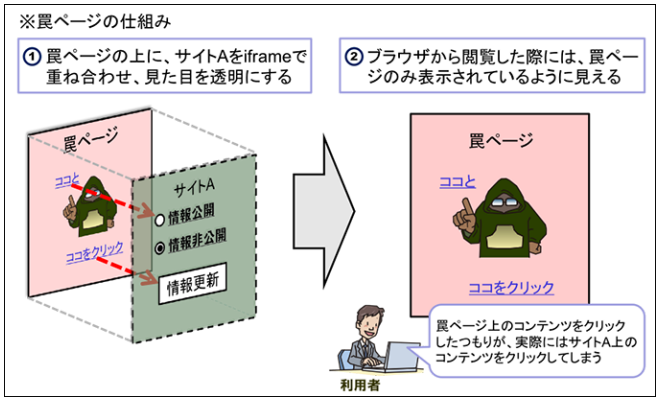

図 4 IPA による従来のクリックジャッキングの図解 [15]

[11] 出典：The Hacker News『New "DoubleClickjacking" Exploit Bypasses Clickjacking Protections on Major Websites』 https://thehackernews.com/2025/01/new-doubleclickjacking-exploit-bypasses.html

[12] 出典：IPA 独立行政法人 情報処理推進機構『安全なウェブサイトの作り方 - 1.9 クリックジャッキング』 https://www.ipa.go.jp/security/vuln/websecurity/clickjacking.html

[13] 出典：トレンドマイクロ『クリックの前に注意！： Facebook に潜むクリックジャック攻撃 - 脅威データベース』 https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/108/think-before-you-click-truth-behind-clickjacking-on-facebook

[14] 出典：弁護士ドットコム『Ｆａｃｅｂｏｏｋで性的嗜好が流出！？損害賠償請求は可能か』 https://www.bengo4.com/c_23/n_101/

[15] 出典：IPA 独立行政法人 情報処理推進機構『安全なウェブサイトの作り方 - 1.9 クリックジャッキング』 https://www.ipa.go.jp/security/vuln/websecurity/clickjacking.html

【クリックジャッキング対策の実装】

クリックジャッキングが仕込まれた Web ページのブロック等、主要なブラウザに対策が実装された事、また SNS 等の各サイトでも、透明にしたフレームに使用されるのを拒否する設定等の対策が浸透した事から、最近ではクリックジャッキング攻撃の成功は難しくなっていた[16]。

2.3. ダブルクリックジャッキングの脅威

【新たなクリックジャッキング ～ダブルクリックジャッキング～】

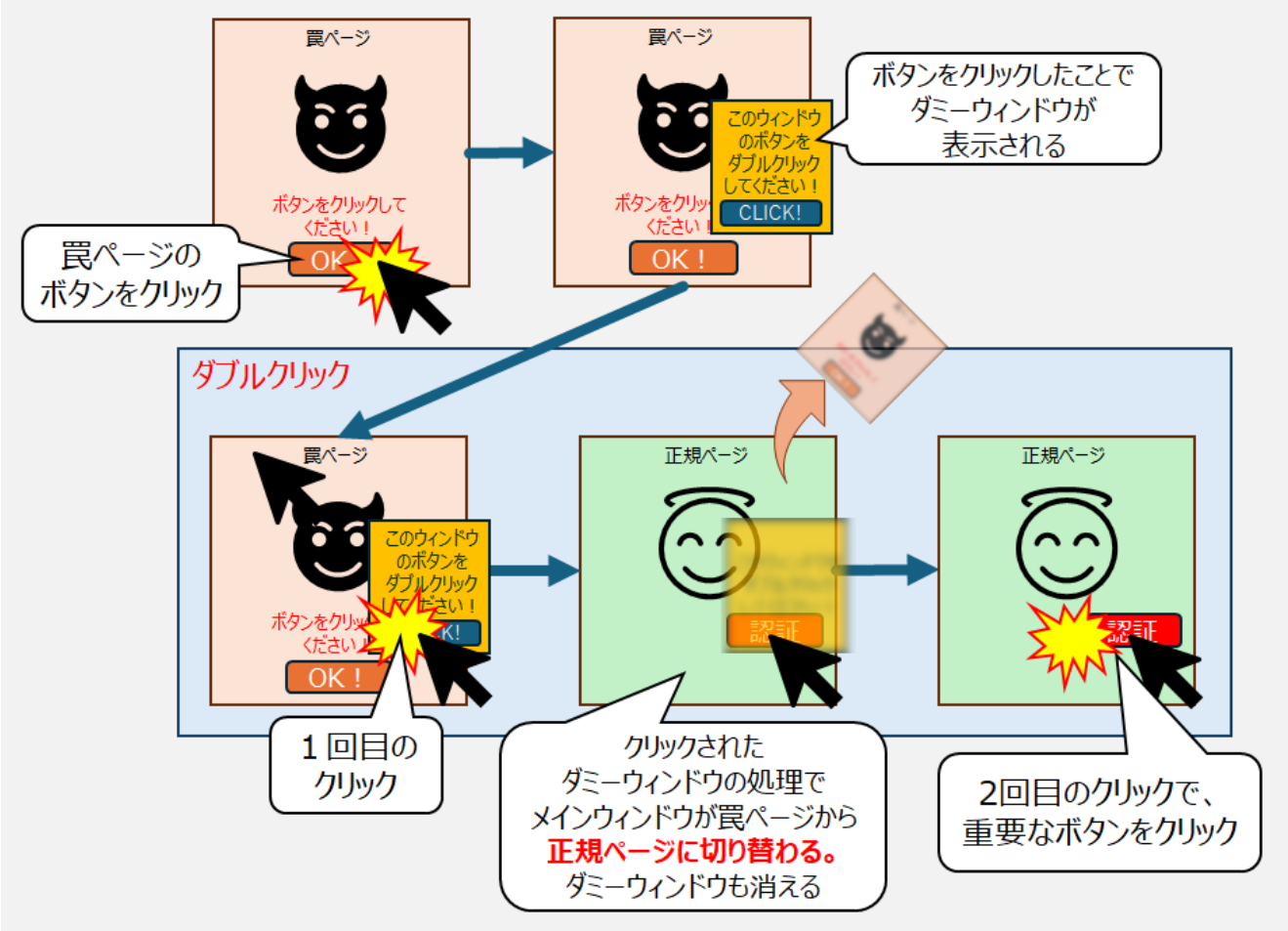

図 5 ダブルクリックジャッキングの流れ

「ダブルクリックジャッキング」（DoubleClickjacking）は、セキュリティ研究者のパウロス・イベロ氏によって 2024 年 12 月末に発表された[17]。これまでとは異なる新たなクリックジャッキングの手法で、ユーザーが 2 回クリックを行うダブルクリック動作の間

[16] 出典：徳丸浩の日記『2023 年 4 月においてクリックジャッキング未対策のサイトはどの条件で被害を受けるか』
https://blog.tokumaru.org/2023/04/clickjacking-condition.html

[17] 出典：PAULOS YIBELO Blog『DoubleClickjacking: A New Era of UI Redressing』
https://www.paulosyibelo.com/2024/12/doubleclickjacking-what.html

に、クリック対象を瞬時に変更することで、意図しない操作を実行させる。

手順は次のとおりである（図 5）。攻撃者は、罠ページにアクセスしてきたユーザーをターゲットにする。罠ページ（メインウィンドウ）には、クリックすると報酬が得られるといった罠のボタンが設けられている。ユーザーがこのボタンをクリックすると JavaScript で組まれた罠が発動する。

まず、ユーザーにダブルクリックを求めるメッセージが記されたウィンドウがメインウィンドウの上に表示される。実はこれはダミーのウィンドウで、クリックするとメインウィンドウを操作するスクリプトが組み込まれている。ユーザーが指示に従いダミーウィンドウの指定位置でダブルクリックをすると、1 回目のクリックの直後にメインウィンドウが正規サービスのページに切り替えられ、ダミーウィンドウも閉じる。この状態でユーザーが 2 回目のクリックをすると、指定位置の直下にある、切り替えられた正規サービスのページの重要なボタンをクリックしてしまう。

【ダブルクリックジャッキングの脅威】

ダブルクリックジャッキングの潜在的な影響は大きいとみられている[18]。悪用すると、セキュリティ設定の無効化、アカウントの削除、アクセスの承認、送金の承認、商取引の確認といった、ユーザーに損失を与えるクリックをさせる事が可能であると、イベロ氏は指摘している[19]。

認証関連では特に、ログインしているシステム基盤上でサードパーティアプリケーションにアクセスを許可する OAuth 認証の場合、ダブルクリックジャッキングによって悪意のあるアプリケーションに権限を付与してしまう可能性がある。イベロ氏は、OAuth 認証をサポートするほぼ全てのサイトがダブルクリックジャッキングに脆弱であると警告している。そして、ビジネス等でよく用いられている Salesforce や Slack を例にし、OAuth 認証のアクセス許可ページをクリックさせることによるアカウントの乗っ取りのデモ動画を公開している（図 6）。

他にも、誤ったクリックによりマルウェアや不審なアプリケーションをダウンロードし、意図せず感染するといった攻撃も考えられる。

図 6 salesforce アカウントの乗っ取りのデモ動画より [20]

[18] 出典：Reflectiz『DoubleClickjacking: A New Attack Vector At Large On The Web』 https://www.reflectiz.com/blog/doubleclickjacking/

[19] 出典：PAULOS YIBELO Blog『DoubleClickjacking: A New Era of UI Redressing』 https://www.paulosyibelo.com/2024/12/doubleclickjacking-what.html

[20] 出典：YouTube『Qey Shinkurt “Salesforce Account Takeover via Doubleclick”』 https://www.youtube.com/watch?v=4rGvRRMrD18

ダブルクリックジャッキングは正規サイトをユーザーが直接クリックするため、サイトを跨いだ Cookie の保護策といった、ブラウザや正規サイトに組み込まれた従来のクリックジャッキングの防御策を回避してしまう。さらにブラウザで表示される Web ページだけではなく、ブラウザ拡張機能での悪用の可能性、また、スマートフォンでも実行可能な「ダブルタップ」の可能性もイベロ氏は指摘している[21]。

【ダブルクリックジャッキングへの対策】

ダブルクリックジャッキングは、ブラウザの開発元・正規 Web ページの制作元それぞれが実装することで対策ができる[22]。

Chrome の Google 社等のブラウザの開発元に対しては、長期的な取り組みとしてダブルクリック攻撃が成立しないための新しい標準仕様の策定とブラウザへの採用が求められる。他、正規 Web ページの制作元における、悪用されない対策も欠かせない。新しい HTTP ヘッダーである「Double-Click-Protection: strict」を Web ページに実装し、Web ページでのダブルクリックの検知と防御を有効化する。また、重要な操作には、クリックだけではなく入力や確認ステップを追加して、ユーザー操作の検証を入念にする。他にも、切り替え後の Web ページとして使われないために、「Content-Security-Policy」ヘッダーの「frame-ancestors」ディレクティブを活用し、信頼できるドメインのみがページを埋め込むことが出来るよう制限する、といった対策をイベロ氏は提言している。

Web ページにアクセスするユーザー側では、端末でのセキュリティツールの活用も有効である。一般的な信頼できるセキュリティソフトを使用すれば、リアルタイムでの攻撃検知と防御が期待できる[23]。セキュリティソフト以外にも、ダブルクリックジャッキングは JavaScript で組まれているため、JavaScript の動作を制限するブラウザ拡張機能の活用も有効である。

2.4. まとめ

今回報告されたダブルクリックジャッキングは従来のクリックジャッキング対策が通じない、新たな脅威である。ダブルクリックジャッキングの被害はまだ顕在化していないが、実用化が難しくないことを考慮すると、早期の対策が求められる。対策が整うまでしばらくの間、組織はユーザーに対し、ダブルクリックジャッキングの危険性を周知し、Web ブラウジングの際には不審なサイトへのアクセスを避ける等の対策の呼びかけが必要となる可能性がある。現在、クリックジャッキング対策が普及しているのと同様に、将来的にダブルクリックジャッキング対策がブラウザや正規 Web ページで広がれば、危険性は解消されていくと考えられる。

[21] 出典：PAULOS YIBELO Blog『DoubleClickjacking: A New Era of UI Redressing』
https://www.paulosyibelo.com/2024/12/doubleclickjacking-what.html

[22] 出典：PAULOS YIBELO Blog『DoubleClickjacking: A New Era of UI Redressing』
https://www.paulosyibelo.com/2024/12/doubleclickjacking-what.html

[23] 出典：Reflectiz『DoubleClickjacking: A New Attack Vector At Large On The Web』
https://www.reflectiz.com/blog/doubleclickjacking/

3. 暴露型ランサムウェア攻撃 2024 年活動まとめ

3.1. 概要

弊社の OSINT モニタリングチームでは、暴露型ランサムウェアグループが運営する暴露サイトの投稿を日々モニタリングしている。そのモニタリング結果に基づいて、2024 年の暴露型ランサムウェアグループの活動・動向をまとめた。

3.2. ランサムウェア攻撃の増加

暴露型ランサムウェアグループとは、ランサムウェアを用いてターゲット組織のネットワークにあるファイルを暗号化／窃取した上で、復号キーとの引き換えに身代金を要求し、さらに期限までに身代金が支払われなければ、グループが運営するサイトで窃取したファイルを公開（暴露）する、と被害組織を二重に脅迫する犯罪グループである。暴露サイトの多くはダークウェブに存在しているが、誰でもアクセスできるサイトや SNS を利用するランサムウェアグループもある。

ランサムウェアグループが行った、被害組織に関する投稿の総数の推移を月ごとにまとめた（図 7）。2024 年も引き続き増加傾向が見られ、前年と比較して 2 割程度伸びていることが確認できる。

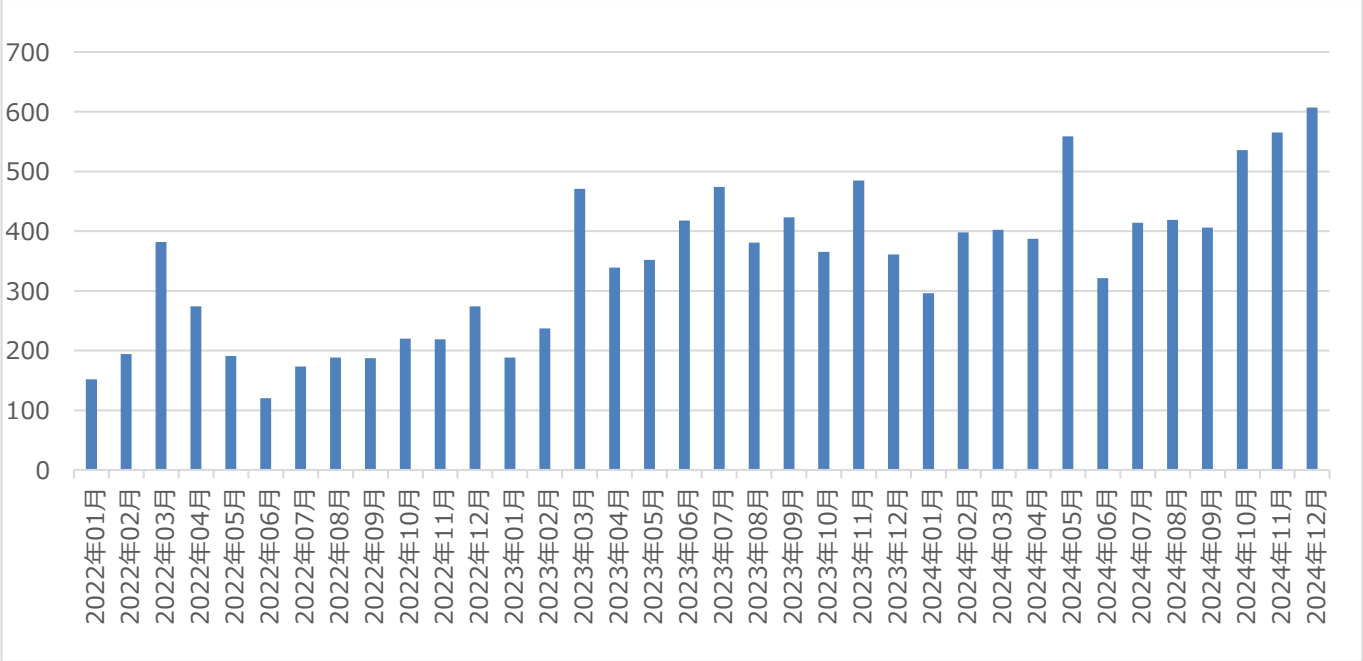

図 7 月毎のランサムウェア暴露サイトに掲載された件数

3.3. ランサムウェアグループの栄枯盛衰

2022 年頃からランサムウェアグループ中で突出した活動を続け、一大ブランドとなっていたグループが Lockbit である。だが 2024 年 2 月、NCA（英国家犯罪対策庁）と FBI（米連邦捜査局）を中心とする捜査機関による大規模かつ国際的な取り締まり作戦を実行したことにより、Lockbit の暴露サイトや IT インフラが押収されたほか、関係者が 2 名逮捕された。Lockbit はその後もサイトを移転して活動を続けたが暴露関連の投稿件数は徐々に減り、第 4 四半期には月当たりの暴露サイトへの投稿数ですら、数えられるほどに減少した。しかし、Lockbit に代わり Ransomhub 等の他の RaaS（Ransomware as a Service）が上位を占める状況に変わっただけで、暴露サイト全体における投稿数は押収作戦の

前後で変わっておらず、増加傾向に歯止めはかかっていない。

RaaS を提供するために必要な、ランサムウェアやプラットフォーム等のコードはこれまでに何種類かが漏洩している。これらを利用してランサムウェア業界へ新規参入することが容易になっている点や、暴露サイトのブランド価値や集客力はランサムウェア攻撃においてそれほど重要ではないことから、ランサムウェア犯罪ビジネスにおいて、イニシアティブを取っているのは RaaS ではなく、初期侵入を行うイニシャルアクセスブローカーや、侵入して情報の窃取や暗号化等を行うアフィリエイトであることが改めて明らかになったと言える。

月	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
LockBit3.0	62	104	59	26	178	12	38	32	22	2	5	6
Ransomhub	0	3	19	24	28	24	48	61	91	77	100	54
PLAY NEWS	6	24	48	27	35	35	20	29	43	52	19	21
Akira	25	17	16	16	20	20	30	8	12	11	10	76
HUNTERS INTERNATIONAL	14	32	18	30	11	8	18	20	14	23	23	16
Medusa	10	15	26	25	25	19	19	4	19	23	19	14
Black basta	18	18	41	23	18	15	8	0	0	12	15	21
Qilin	9	12	10	12	20	16	8	20	20	8	32	17
BianLian	18	21	16	13	14	8	12	17	18	9	13	11
Incransom	10	4	9	19	38	13	18	7	8	6	26	5

図 8 主要な暴露型ランサムウェアグループの 2024 年の投稿数

3.4. まとめ

2024 年は国際的な法執行機関による活動により、Lockbit はかつての勢いを失い、ランサムウェアグループの勢力図は大きく変化した。しかし、全体的な増加傾向には歯止めはかからなかった。ランサムウェアを使った犯罪者たちにとっては、主要な RaaS プラットフォームも選択肢の一つでしかないことが示された。

この問題の根本はサイバー犯罪者の取り締まりが徹底できていないことが大きい。これは何よりも、彼らを放置している国家が存在していることにあり、一つのプラットフォームを押収しても犯罪者のほとんどは逮捕されておらず、別のプラットフォームに移って犯罪行為が継続されている。解決策としてはサイバー犯罪者を特定する活動を行い、犯罪者の居住国家に外交的な圧力をかけることが将来的な改善につながると考えられる。

このような状況は簡単には解決しないとみられることから、企業側はセキュリティ対策を強化し、ランサムウェア攻撃に遭うリスクを下げる取り組みを続けると共にバックアップ体制を強化し、万が一ランサムウェア攻撃に遭ったときに攻撃者に収益を上げさせないよう心掛けたい。

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

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