— AUS（アルテミス・ユーザ・サポート）便り 2025/2/6号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

● NISCよりDDoS攻撃への注意喚起…年末年始に国内への攻撃多発

https://internet.watch.impress.co.jp/docs/news/1660160.html
https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf
https://www.yomiuri.co.jp/national/20250203-OYT1T50164/

このニュースをザックリ言うと･･･

- 2月4日(日本時間)、内閣サイバーセキュリティセンター(NISC)より、DDoS攻撃への注意喚起が出され、対策が呼び掛けられています。

- 昨年12月～今年1月にかけて、航空事業者・金融機関・通信事業者に対するDDoS攻撃が相次いで行われた(12月26日の日本航空以降、2月2日までに省庁等も含め64の事業者が被害を受けたとされる)ことを受けてのものとなっています。

- リスク低減に向けたセキュリティ対策として、「DDoS 攻撃による被害を抑えるための対策」「DDoS 攻撃による被害を想定した対策」および「DDoS 攻撃への加担（踏み台）を防ぐ対策」の大きく3つのカテゴリーに分けての対策が提示されています。

AUS便りからの所感等

- 例えば「DDoS 攻撃による被害を抑えるための対策」では「海外等に割り当てられたIPアドレスからの通信の遮断」「DDoS攻撃の影響を排除又は低減するための専用の対策装置やサービス(WAF・IDS・IPS・UTMその他アプライアンス等)の導入」「CDNの利用」「その他ネットワーク事業者やクラウドサービスが提供する対策の導入」「サーバー・端末・通信回線・回線装置の冗長化」等が、「DDoS 攻撃による被害を想定した対策」では「平常時からのトラフィックの監視及び監視記録の保存」「異常通信時のアラートの設定」「通報先・連絡先一覧作成など発生時の対策マニュアルの策定」等が挙げられています。

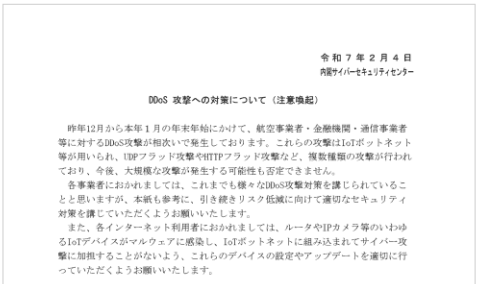
- ただしNISCでは、こういった対策には多大のコスト等がかかるものもあり、かつ全てのDDoS攻撃を未然に防げるとは限らないとしており、身近な対策として機器やシステムの設定見直し及び脆弱性の有無の確認、ソフトウェアの更新等から進めるよう呼び掛けています(概ね「DDoS 攻撃への加担（踏み台）を防ぐ対策」でも挙げられている項目となります)。

- 年末年始におけるDDoS攻撃では「ボットネット」によるPC・NASその他IoT機器を乗っ取っての絨毯爆撃が行われたとされ、このようなボットネットに組み入れられないようにするためにも、全ての機器のOS・ファームウェアを最新に保つこと等が有用と言えます。

Impress Watch

年末年始に相次いだDDoS攻撃を受け、内閣サイバーセキュリティセンターが注意喚起を実施

松永 侑貴惠　2025年2月4日 14:50



令和７年２月４日
内閣サイバーセキュリティセンター

DDoS 攻撃への対策について（注意喚起）

昨年12月から本年１月の年末年始にかけて、航空事業者・金融機関・通信事業者等に対するDDoS攻撃が相次いで発生しております。これらの攻撃はIoTボットネット等が用いられ、UDPフラッド攻撃やHTTPフラッド攻撃など、複数種類の攻撃が行われており、今後、大規模な攻撃が発生する可能性も否定できません。
各事業者におかれましては、これまでも様々なDDoS攻撃対策を講じられていることと思いますが、本紙も参考に、引き続きリスク低減に向けて適切なセキュリティ対策を講じていただくようお願いいたします。
また、各インターネット利用者におかれましては、ルータやIPカメラ等のいわゆるIoTデバイスがマルウェアに感染し、IoTボットネットに組み込まれてサイバー攻撃に加担することがないよう、これらのデバイスの設定やアップデートを適切に行っていただくようお願いいたします。

内閣サイバーセキュリティセンター （NISC）は2月4日、2024年12月から2025年1月の年末年始にかけ、DDoS攻撃が相次いで発生していることから、各事業者に向け、適切なセキュリティ対策を講じるよう注意喚起を実施した。

年末年始、NTTドコモや日本航空、三菱UFJ銀行などがDDoS攻撃を受け、一時期サービスを提供できない問題などが発生した。これらの攻撃はIoTボットネットなどが用いられており、UDPフラッド攻撃やHTTPフラッド攻撃など、複数種類のDDoS攻撃が行われていた。

●クリックジャッキング対策等も回避？新たな攻撃手法「ダブルクリックジャッキング」

https://forbesjapan.com/articles/detail/76261
https://www.paulosyibelo.com/2024/12/doubleclickjacking-what.html

このニュースをザックリ言うと･･･

- 1月6日(日本時間)、「Forbes JAPAN」誌のWebサイトにおいて、セキュリティ研究者のパウロス・イベロ氏が発表した攻撃手法が取り上げられています。

- イベロ氏が「DoubleClickjacking(ダブルクリックジャッキング)」と名付けた攻撃手法は、ダブルクリックを促す画面(以下・画面A)を表示させ、ユーザーが1回目のクリックを行った瞬間にその画面を閉じ、2回目のクリックで攻撃者が押させたいボタンを含む別の画面(以下・画面B)を表示させるというものです。

- これにより、本来ユーザーが何らかの許可を確認すべき場面で意図せず許可ボタンをクリックするよう誘導でき、また従来の「クリックジャッキング」に対して導入されている各種対策も回避可能であるとしています。

AUS便りからの所感

- 従来のクリックジャッキングでは画面A内に透明なインラインフレームを用いて画面Bを埋め込んでいたのに対し、今回の手法では親画面が「新しいウィンドウとして画面Aを開く」とともに「自身は画面Bに差し替える」手順をとる模様です。

- 現時点でブラウザー側での明確な対策は提供されていない模様ですが、イベロ氏は「許可などを行うボタンを最初は無効化し、画面上でマウスカーソルを動かす等で有効化する」仕組みによって攻撃を緩和できるとしており、一部著名なWebサイトでは既にこれを実施しているとしています。

- この手法はPCでもスマートフォンでも実行可能とされていますが、特にスマホ上ではユーザーが意図せずクリックするような仕掛けを持つ広告が取りざたされており、今回の手法と併せて今後対策が議論される可能性が考えられます。

2025.01.06 17:00

「ダブルクリック」を利用する新しく深刻な脅威、すべてのブラウザが攻撃対象

Davey Winder | Contributor

数億人のウェブユーザーが、新たに発見された危険なサイバー攻撃について警告を受けている。この攻撃はブラウザの種類を問わず、「ダブルクリック」さえすれば成立してしまう。以下に、「ダブルクリックジャッキング（ダブルクリックジャック攻撃）」について知っておくべきポイントをまとめる。

ダブルクリックは危険、新たなハック攻撃が確認される

アプリケーションのセキュリティやクライアント側の攻撃手法を研究するパウロス・イベロは、多くの脆弱性や新しいセキュリティ脅威を発見してきた実績を持つ。そのイベロが、ウェブブラウザを使うほぼすべての人に影響しかねない新たな攻撃手法「ダブルクリックジャッキング」を明らかにした。自身のブログ投稿で、ChromeやEdge、Safariをはじめとするほぼあらゆるブラウザで、ユーザーがダブルクリックを行った際に認証情報を奪われてしまう具体的な方法を技術的に示している。

● Teams設定ミスで個人情報が学内へ公開状態に…2大学で相次いで発生

https://xtech.nikkei.com/atcl/nxt/column/18/00598/111500312/
https://www.tuad.ac.jp/news/information/24164/
https://www.kuas.ac.jp/application/files/5017/3768/1947/20250124.pdf

このニュースをザックリ言うと･･･

- 1月20日(日本時間)、東北芸術工科大学より、学内で利用している「Microsoft Teams」において、チーム内関係者にのみ共有されるべき個人情報を含むデータがチーム外の同学学生・教職員からも閲覧可能状態にあったと発表されました。

- Teamsの設定ミスにより、プライバシー設定を「プライベート」ではなく「パブリック」としていたことが2024年12月19日に判明し、対応したもので、閲覧可能な状態にあったデータは計810人分の個人情報が含まれていたとされます。

- 1月24日には京都先端科学大学からも同様の設定ミスが発表され、教員間で共有していた学生の個人情報・試験成績情報が他の学生から閲覧可能な状態にあったとしています。

AUS便りからの所感

- 今回は学外の第三者が閲覧できる状態でこそなかったとはいえ、共有対象以外の人間が閲覧可能な状態にあったことが発覚するのはれっきとした問題であり、また昔からも、アクセス制限がなく、ディレクトリリストの表示で容易にわかるような場所にフォームから入力されたデータを保存する等により、認証もなしに全くの第三者が機密情報にアクセス可能な状態にあった例は枚挙にいとまがありません。

- メールではなくGoogle Drive・OneDrive・Dropbox等オンラインストレージやSlack等ビジネスチャット、Teams・Zoom等ビデオ会議でデータを共有する場面も増えている今日にあって、データの置き場所が推測されにくいURLであるとしても決して油断せず、必ずアクセス制限を行うとともに、可能であれば非ログイン状態あるいは権限の低いテスト用アカウントで実際にアクセスしてチェックすることが肝要です。

大学で続くTeamsのミスによる個人情報の学内公開、東北芸工大は4年超気付けず

piyokango　セキュリティーリサーチャー

2025.02.04

アクセス範囲を「パブリック」とする設定ミス

東北芸術工科大学は2025年1月20日、一部の職員でのみ共有されるべき個人情報が、学内の学生や職員にも閲覧可能だったとして、関係者に謝罪した。

同大によると、Teamsで共同作業を行う「チーム」で共有していたデータが、検索機能によってチーム外の人にも閲覧できることが2024年12月19日に判明。調査の結果、データにはのべ900件、810人の個人情報が含まれていた。

原因はTeamsの公開設定において、本来「プライベート」（秘密）とすべきところを、誤って学内関係者全員がアクセスできる「パブリック」（公開）としていたため。ファイルの中には、2020年4月9日から閲覧可能だったものが見つかった。