ブラウザクラッシャー

出典: フリー百科事典『ウィキペディア（Wikipedia）』

この記事は検証可能な参考文献や出典が全く示されていないか、不十分です。出典を追加して記事の信頼性向上にご協力ください。
出典検索?: "ブラウザクラッシャー" – ニュース · 書籍 · スカラー · CiNii · J-STAGE · NDL · dlib.jp · ジャパンサーチ · TWL（2020年11月）

この記事には独自研究が含まれているおそれがあります。問題箇所を検証し出典を追加して、記事の改善にご協力ください。議論はノートを参照してください。（2022年8月）

ブラウザクラッシャーとは、ウェブブラウザやオペレーティングシステム (OS) の仕様・バグを悪用するスクリプト言語または HTML 文書を記述したウェブページのこと。

概要 [編集]

ウェブブラウザで当該ページにアクセスすることにより、ウェブブラウザや OS の動作に異常を発生させる。「クラッシャー」はソフトウェアをクラッシュ[1]させる動作を意味している。ソフトウェアの構成やハードウェアに直接の破壊的な影響を及ぼす場合もある（FDDアタックなど）。

日本補では「**ブラクラ**」と略称されることもある。

HTML 記述型 [編集]

HTML を不正な形で記述することによってブラウザに不具合を起こさせる。JavaScript が動作しない環境でも動作するため脅威となる。

ウィンドウ無限表示型 [編集]

「crashme」および「You are an idiot」も参照

このタイプのブラクラが最も有名なブラクラであるといえる。このブラクラは「JS_SPAWN.A」と呼ばれ、該当のページにアクセスすると、新しいウィンドウを無限に開き続けることで、メモリの使用量が爆発的に増加し、最悪の場合フリーズする。

ユーザーがウィンドウを一つでも閉じると、ウインドウがねずみ算式に開かれる様になっている場合がほとんどである。トロイの木馬として分類されている場合があるが、ファイルやレジストリなどの改変を行わないものが大半である。しかし、悪質なものになると単にブラクラとして動作するだけでなく、ウイルスをダウンロードさせるなどの二次災害を引き起こすサイトもある。

対応策

- プロセスを強制終了する。
  - Windowsでは Ctrl + Alt + Delete キーで、タスクマネージャを開き、「プロセス」タブでウェブブラウザを終了する。このとき終了するプロセスは、Internet Explorerの場合は「iexplore.exe」、Mozilla Firefoxを使用している場合は「firefox.exe」である（Windows 9x系OSの場合、「強制終了の選択」というダイアログが表示されるので、そこから使用しているブラウザをクリックして強制終了する）。
  - macOSでは、command + option + esc キーでアプリケーションの強制終了を開き、ウェブブラウザを強制終了する。
  - Unix系OSでは ps コマンドでウェブブラウザのPIDを調べ、killコマンドでプロセスを終了する。
- 「新しいウィンドウ」ではなく、「新しいタブで開く」設定に変更する（タブブラウザ、タブブラウジングの場合）。
- 最終手段として、電源を切って再起動させる。

mailto ストーム（メイルトゥストーム） [編集]

上記と似たタイプのブラクラである。mailtoスキームを悪用して電子メールの作成画面を起動するマークアップを大量に記述し、メール作成画面を大量に開かせる。結果、閲覧者のコンピュータやブラウザを過度のリソース消費によりフリーズさせる。タグでメール新規作成画面を開かせる際、`<a href="mailto:~">`と書き、このリンクをクリックすると、ブラウザに設定されたメールクライアントが起動する。これがmailtoストームの名前の由来である。

防御策

- メール作成画面の同時表示個数に上限を設定できる電子メールクライアントを使用するか、ブラウザで使用する標準メールソフトを設定しない。
- `"F12"` キーを押して開発者ツールを起動してソースを確認し、 `img` タグの `src` 属性に `"mailto:"` が含まれていないか注意する。
  - ただし、一部の環境では `F12` をつけても開発者ツールが起動できないためオンラインのソースチェッカーを使用するなど別の方法を用いる必要がある。

電子メールクライアント側で対策（メール作成画面に上限を設けるなど）されていることも多い。

mailtoストームに類似する誤作動

- mailtoによって起動するメールクライアントを未設定にしていた場合、ブラウザがmailtoによって起動するアプリケーションを探すが、設定していないため当然みつからない。そのためブラウザの処理がループし、ブラウザが60 - 100個ほど開いてしまう。また、ブラウザに設定したメールクライアントが一見設定されている状態でも、なんらかの影響によって未設定とみなされ、上記と同様の現象が発生することがある。その場合は、一旦ブラウザのメール設定を変更し、再度戻すことで現象は回避できる。

FDD アタック・CD-ROM アタック [編集]

fileスキームを悪用してフロッピーディスク ドライブ (FDD) へのアクセスを繰り返す、CD-ROMドライブが開閉を繰り返すなど、周辺機器にアクセスさせるマークアップを多数記述し、ブラウザの反応を遅くする。場合によっては周辺機器に物理的影響を与える。特にフロッピーディスクは機器への負担が大きい。

通常Aドライブであるフロッピーディスクドライブがガチャガチャと動く。

防御策

- フロッピーディスクドライブのドライブ名をA以外にする
- URL の前に `"view-source:"` をつけてソースコードを確認し、 `img` タグの `src` 属性に `file://` が含まれていないか注意する。
  - ただし、Windows XP SP2 以降の Internet Explorer や Opera など一部の環境では `view-source:` をつけてもソースコードが確認できないため、オンラインのソースチェッカーを使用するなど別の方法を用いる必要がある。
- FDDアタックがPCのAドライブにアクセスし続けると、FDDが破損することがある。だが、FDDに最初からFDを挿入しておくと、破損は回避できる。

もっとも、Windows XP以降の市販パソコンではフロッピーディスクドライブが レガシーデバイスと化し、別売のオプション扱いとするものが出てきている。このようなパソコンにはAドライブが存在しないため、フロッピーディスクドライブアタックは効かない（やむなく使用する必要がある場合、USB接続の外付けドライブなどで代用する）。なお、Windows以外のプラットフォームは影響を受けない。

テーブルネスト [編集]

`table` タグの中に `table` タグを入れ、さらにその中に `table` タグを入れ、これを故意に深くネスティングさせたもの。古いブラウザ、特にバージョンの古い Netscape Navigator（4.x あたりまで）ではフリーズしてしまう。 意図しなくてもページレイアウトのために `table` タグを多用した場合、同じことが起こりうる。

防御策

- CSS（スタイルシート）への対応が不完全な古いブラウザしか対応できないパソコン環境（Windows95, MacOS8.x あたりまで）の使用を止め、新しいブラウザが動作できるパソコン環境に移行する。
- URL の前に `"view-source:"` をつけてソースを確認し、 `table` タグの多重入れ子が含まれていないか注意する。
  - ただし、Windows XP SP2 以降の Internet Explorer や Opera など一部の環境では `view-source:` をつけてもソース確認ができないため、オンラインのソースチェッカーを使用するなど別の方法を用いる必要がある。

concon クラッシャー [編集]

concon バグと呼ばれるバグを利用したもの。Windows の予約デバイスに関する不具合を持つファイル名やフォルダ名にアクセスさせ、OS を停止させる。CON, AUX, NUL などが該当。

防御策

- この種の脆弱性を持ち、既にMicrosoftがサポートを終了している Windows 9x系（Windows Me まで）の OS を使用しない。

Telnet ストーム [編集]

サーバとの通信に使われるtelnetサービスを悪用してDOS画面に似たプロンプトを開く。

防御策

- 該当サービスのスタートアップの種類を停止にする。

JavaScript 記述型 [編集]

クライアントサイドのスクリプトである JavaScript を悪用したもの。HTML 記述型と複合させたものもある。JavaScript の動作しない環境では作動しない。そのため、JavaScript 型は全て JavaScript を無効にすることによって回避することができる。

JavaScriptループ型 [編集]

JavaScript を使用している場合、処理をループさせている場合が多い。それは、HTML 記述型の場合、有限回しか実行させることができず、さらにソースも長くなるのに対し、JavaScript を使用すれば数行で何回でも実行させることができるからである。

本項では、無限にループさせるものとして記述する。

JavaScript の無限ループ [編集]

スクリプトが永久ループすると、CPU の使用率が 100% になりパソコンの動作が非常に鈍くなる。場合によっては、フリーズする。

防御策

- 特別な防御策は特になし。
- 最近のブラウザには一定回数以上ループした時警告を表示するブラウザがあるので、それを利用する。

ウィンドウ無限表示型 [編集]

上記のHTML 記述型と効果はほぼ同じ。最近のブラウザには標準でポップアップブロックが装備されているものが多いので、実行されにくくなってきた。

ウィンドウストーム

mailtoストーム

その他の例

mailto ストームのように、HTML 型の脅威を JavaScript の反復処理によって記述される危険性がある。FDDアタック、ソースストーム、ftpストームなどが代表例。

防御策

上記のHTML 記述型と同じ

無限アラート [編集]

アラートを多数回または無限に開かせる。一部のウェブブラウザではアラートはダイアログボックスで実装され警告を促すため最前面に表示されるようになっているため、メッセージボックスが表示されている間は操作できない。このブラクラではアラートを閉じると次のステップでまたアラートを表示する。したがって、アラートがダイアログボックスであるブラウザではアラートが終了するか、プロセスを終了しない限り操作が何もできなくなる。

防御策

- プロセスを強制終了する。
  - Windows では Ctrl+Alt+Delete キーで、タスクマネージャを開き、「プロセス」タブでウェブブラウザを終了する。このとき終了するプロセスは、Internet Explorerの場合は「iexplore.exe」、Mozilla Firefoxを使用している場合は「firefox.exe」（Windows 98 系 OS の場合、「強制終了の選択」というダイアログが表示されるので、そこから使用しているブラウザをクリックして強制終了する）。
  - UNIX 系 OS では ps コマンドでウェブブラウザの PID を調べ、kill コマンドでプロセスを終了する。
- 再起動する。

×ストーム [編集]

画像を表示できなかった時の×マークを大量に表示させ、フリーズさせる。無限に指定するものや、多くの数を指定してフリーズさせるものなどがある。

防御策

- フリーズする前（ページを読み込む前）にウィンドウを閉じる。

フルスクリーン化 [編集]

ブラウザをツールバーなしの全画面表示にしてしまう。

防御策

- ポップアップブロックを設定できるブラウザ（Windows XP SP2 の IE6、Firefox など）を使用する。
- タブブラウザ（Firefox、Microsoft Internet Explorer 7 など）を使用する。
- Windows系の場合、[Alt]+[F4] を押すことによりブラウザを閉じることができる。Mac の場合は [コマンドキー]+[Q] でブラウザを終了できる。
- Internet Explorerなどでは[F11]を押すことによってフルスクリーンを解除することができる。

ブラウザによっては、標準でポップアップブロックに対応しているため、実行されにくくなっている。

ゾンビウィンドウ [編集]

何度閉じても、ゾンビのごとく復活するウィンドウのことをいう。消した数よりも開くウィンドウが多い場合もある。この場合、ウィンドウがねずみ算式に増えることになる。悪質なポップアップ広告にしばしば使われている。

防御策

- ポップアップブロックを設定できるブラウザを使用する。

JavaScript実装のバグをついたもの [編集]

特定のブラウザーのJavaScript実装のバグをつくタイプ。

防御策

- Internet Explorer 以外のブラウザを使う

WindowsのNTFSのバグを利用したもの [編集]

Windows Vistaから8.1まででChromium系ブラウザ以外が対象。NTFSのバグを使ってブラウザやシステムを停止させる。ドライブやOSは弄らないので、再起動させたら元に戻る(2017/06/02現在は対策なし)。

防御策

- 不正なパスを検出する機能があるChrome系ブラウザなどのブラウザを使う。

I'm Feeling Lucky ブラクラ [編集]

I'm Feeling Lucky ブラクラとは、Google のトップページの、「検索」ボタンの横にある「I'm Feeling Lucky」ボタンを悪用したブラクラのことである。I'm Feeling Lucky とは、Google の機能の一つで、検索結果の一覧を表示せずに直接検索結果のトップに挙がったウェブページにジャンプする機能のことだが、その機能を利用して、ブラクラサイトが検索結果のトップに表示されるような検索語をリンク先の URL に仕掛けるとクリックした者をブラクラに誘導することが可能になる。

掲示板などにリンクが貼られていた場合、普段は多少怪しいと思うようなリンク先であっても、I'm Feeling Lucky を使った URL の場合、 `https://www.google.co.jp/#q=○○&btnI=I%27m%20Feeling%20Lucky` というような URL になり、ドメインが Google であることから安心してクリックしてしまい、ひっかかりやすいとされている。

また、 `=I%27m%20Feeling%20Lucky` の部分は省略でき、さらに btnI は `%62%74%6e%49` と URL エンコードもできるため、 `https://www.google.co.jp/#q=○○&%62%74%6e%49` となる。このように、偽装が容易である。

防御策

- 「Google」だけで安心せず、クエリ文字列に「I'm」、「Feeling」、「Lucky」などの文字列が含まれていないかどうか見る。それでも完全に防御することはできない。

ブラクラを踏まないようにするための対策 [編集]

ブラクラを踏まないようにするためにも、次のような対策を行うべきである。

- タブブラウザを使用する。
  - 正確には事前の予防策ではなく、ブラクラを踏んだ際の緊急回避手段として有効。通常のブラウザだとウィンドウを手動でこまめに閉じなければならないため、機械的な増殖に対応しきれないケースが多いが、タブブラウザの場合はブラウザひとつを閉じるだけで済むケースがほとんどである。
- アクセスする前にソースを確認する。
  - 怪しいサイトにアクセスするときは、JavaScript を切り、ブラクラチェッカーやソースチェッカーなどで調べる。
  - リンク先をファイルにダウンロードし（右クリック―「対象をファイルに保存」でデスクトップにでも）、ソースコードを調べる。UNIX コマンドが使える環境ならば wget コマンドや curl コマンドでも可能。
  - Gecko 系や Blink 系のブラウザを使用している場合は `view-source:` スキームを使ってページを表示する前にソースを確認する。
- ブラウザの設定でポップアップを無効にするように設定する。

精神的ブラクラ [編集]

派生した用語として「**精神的ブラクラ**」がある。これは、閲覧者に精神的な不快感を与えさせるグロ系や恐怖系の画像・音声・動画（死体の写真や動画など）にそれと気づかないようにアクセスさせることである。

単なる画像や動画の表示のみであるため、ブラウザやコンピュータ自体にはなんら影響はないものの、悪意を持って対象のURLをクリックさせることがブラクラと共通しているためこう名付けられた。「マインドクラッシャー」「マイクラ」とも呼ばれる。[2][3]

脚注 [編集]

[脚注の使い方]

1. ^ （英語: crash, ソフトウェアの異常終了の意で用いられている。
2. ^ 「マインドクラッシャー」 kotobank、2009年12月9日閲覧。
3. ^ 「マインドクラッシャー」 IT用語辞典バイナリ、2009年12月9日閲覧。

関連項目 [編集]

- Jodi
- 蓮コラ - 精神的ブラクラの一種。

表・話・編・歴	脆弱性、攻撃手法、エクスプロイト [隠す]
クロスサイト攻撃	クロスサイトリクエストフォージェリ (CSRF) | クロスサイトスクリプティング (XSS) | クロスサイト・クッキング | クロスサイトトレーシング | クロスゾーンスクリプティング（英語版）
インジェクション攻撃 (CWE-74)	クロスサイトスクリプティング (XSS) (CWE-79) | SQLインジェクション (CWE-89) | HTTPヘッダ・インジェクション | HTTPレスポンススプリッティング（英語版） (CWE-113) | 書式文字列攻撃 (CWE-134)
スプーフィング攻撃	DNSスプーフィング | IPスプーフィング | ARPスプーフィング | クリックジャッキング (CAPEC-103) | リファラスプーフィング（英語版） | Eメールスプーフィング（英語版） | フィッシング (CAPEC-98) | ファーミング (CAPEC-89)
セッションハイジャック関連	セッションフィクセーション (CWE-384, CAPEC-61) | セッションポイズニング（英語版） | TCPシーケンス番号予測攻撃 | クッキーモンスター攻撃（英語版）
DoS攻撃	Land攻撃 | クリアチャネル評価攻撃（英語版）
サイドチャネル攻撃	コールドブート攻撃（英語版） | Meltdown | Spectre | Lazy FP state restore（英語版） | TLBleed（英語版）
不適切な入力確認 (CWE-20)	バッファオーバーラン (CWE-119、120、121等) | Return-to-libc攻撃 | ディレクトリトラバーサル (CWE-22)
未分類	中間者攻撃 (CAPEC-94) | MITB攻撃 | MOTS攻撃（英語版） | Off-by-oneエラー (CWE-193) | ファイルインクルード脆弱性（英語版） | Mass Assignment脆弱性（英語版） | ダングリングポインタ（英語版） | DNSリバインディング | in-sessionフィッシング（英語版） | クッキースタッフィング（英語版） | 悪魔の双子攻撃（英語版） | IDNホモグラフ攻撃 | スナーフィング（英語版） | JITスプレーイング（英語版） | リプレイ攻撃 | 誕生日攻撃 | CRIME | KRACK | Intel ME（英語版）の脆弱性
対策	OP25B | Content Security Policy（英語版） | コンテントスニッフィング（英語版） | HTTP Strict Transport Security (HSTS) | ファイアウォール | 侵入防止システム (IPS) | 侵入検知システム (IDS) | Web Application Firewall (WAF) | Wi-Fi Protected Access
関連項目	マルウェア | セキュリティホール | クラッキング | 脆弱性情報データベース | **ブラウザクラッシャー** | シェルコード | Metasploit | Sshnuke | Nikto Web Scanner（英語版） | OWASP（英語版） | w3af（英語版） | 隠れ通信路（英語版）

カテゴリ: コンピュータ・ネットワーク・セキュリティ | エクスプロイト

最終更新 2022年8月7日 (日) 02:00 （日時は個人設定で未設定ならばUTC）。