

# 利用マニュアル

---

*PLATINUM DICTIONARY*



# セットアップ方法

---

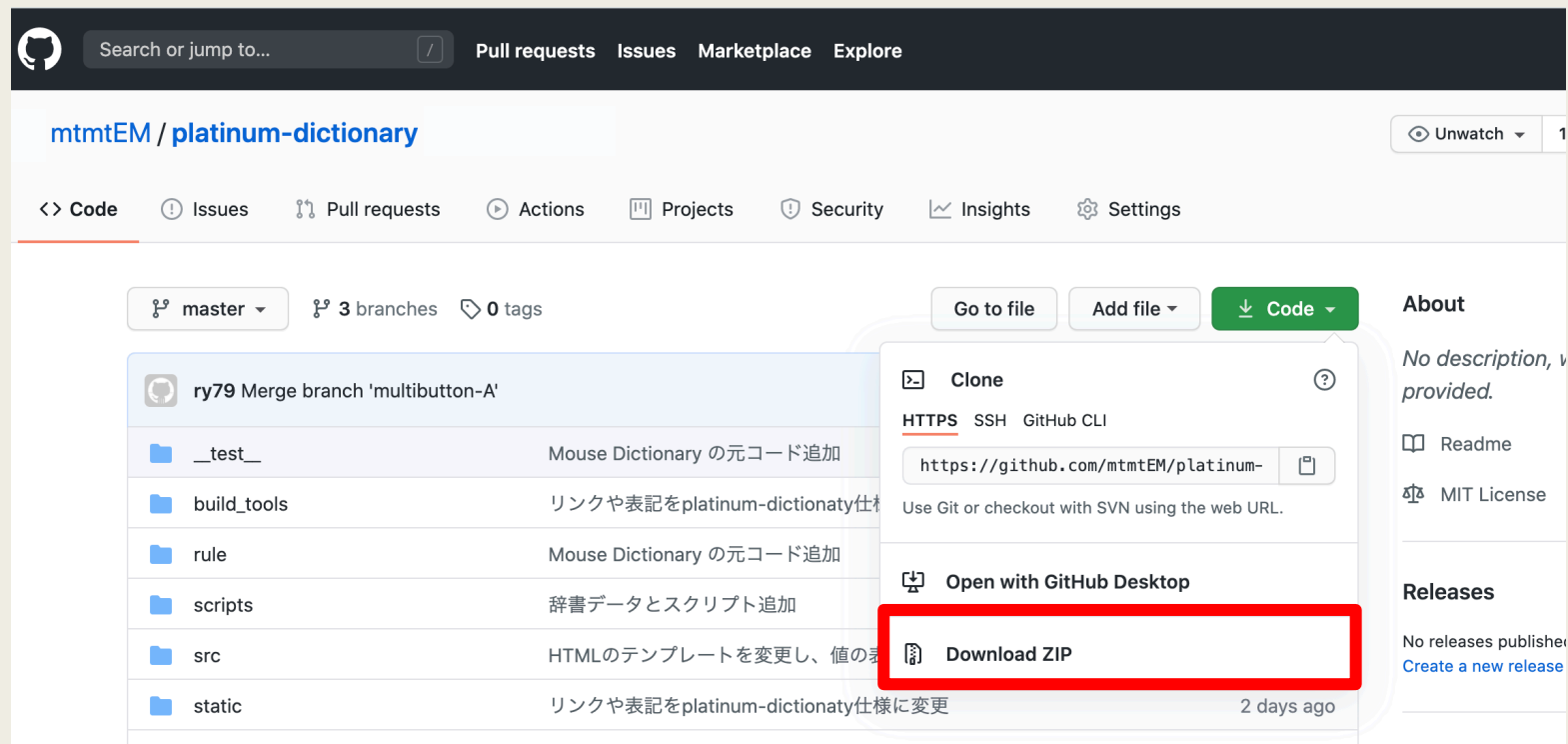
- 動作環境
- 事前準備
- 拡張機能の利用 Chrome
- 拡張機能の利用 Firefox

# 動作環境

- Chrome (85.0.4183.121)
- Firefox (81.0)
- Node 6+ (6.14.8)

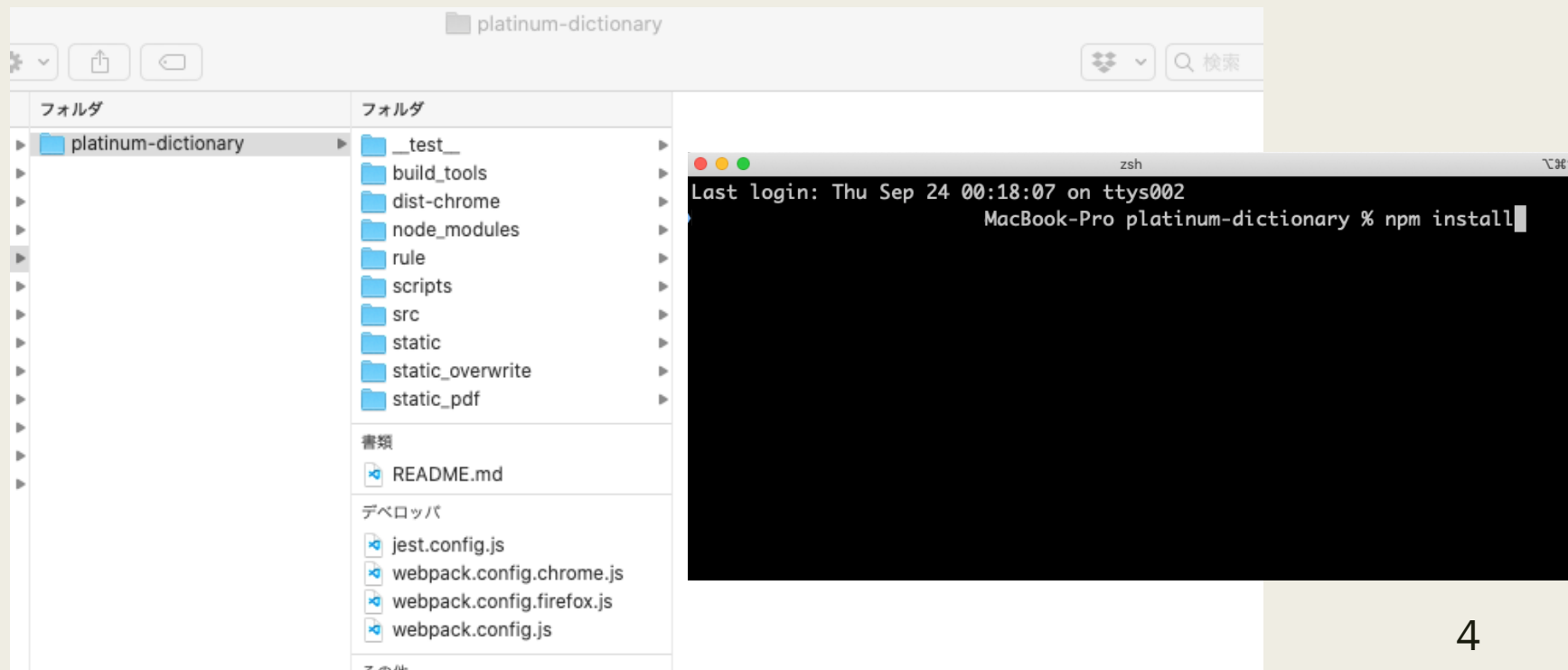
# 事前準備

1. Node.js をインストール
2. [https://github.com/mtmtEM/platinum\\_dictionary](https://github.com/mtmtEM/platinum_dictionary)からソースコードをダウンロード



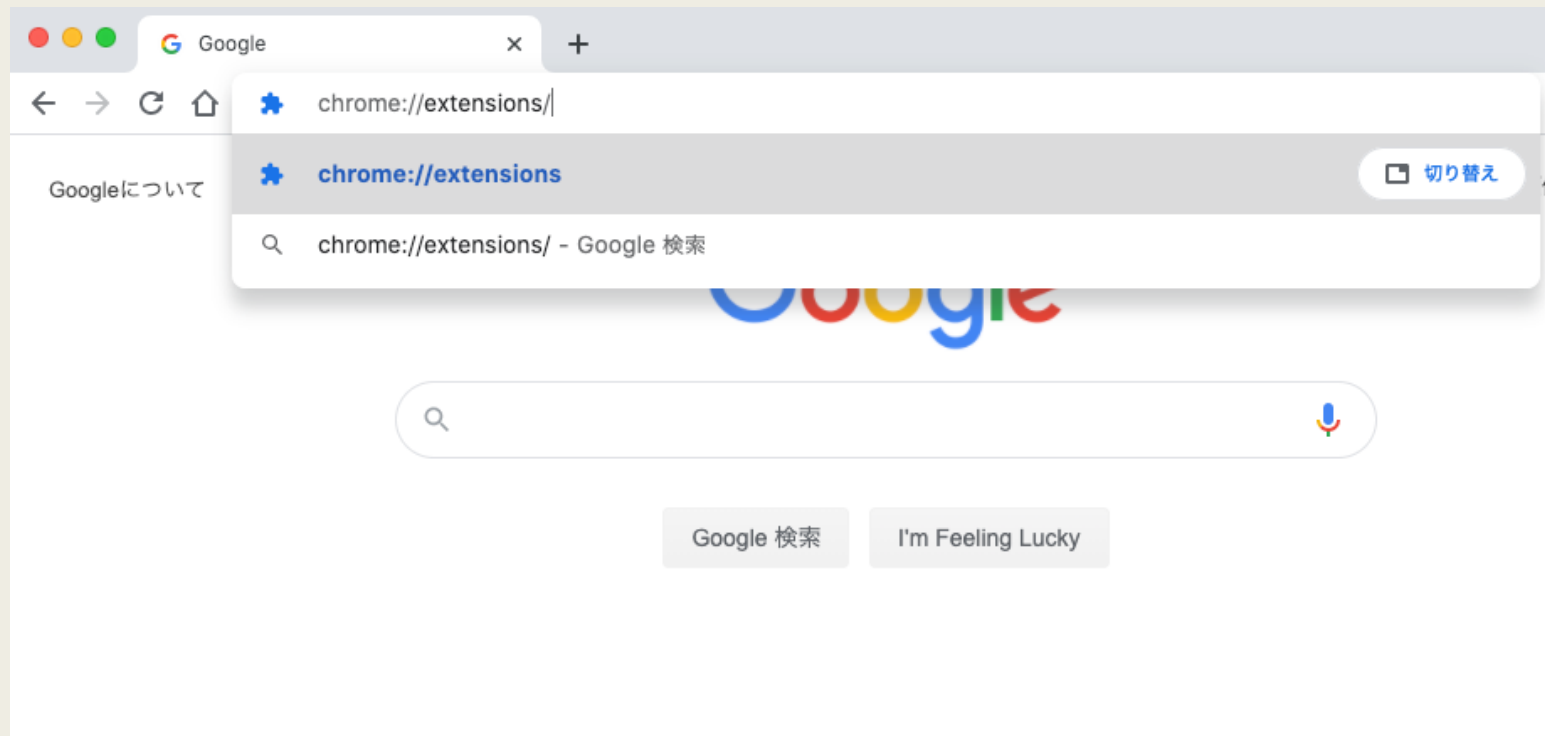
# 事前準備

3. ダウンロードしたファイルを展開
4. `$ npm install` コマンドを実行
5. `$ npm run build` コマンドを実行



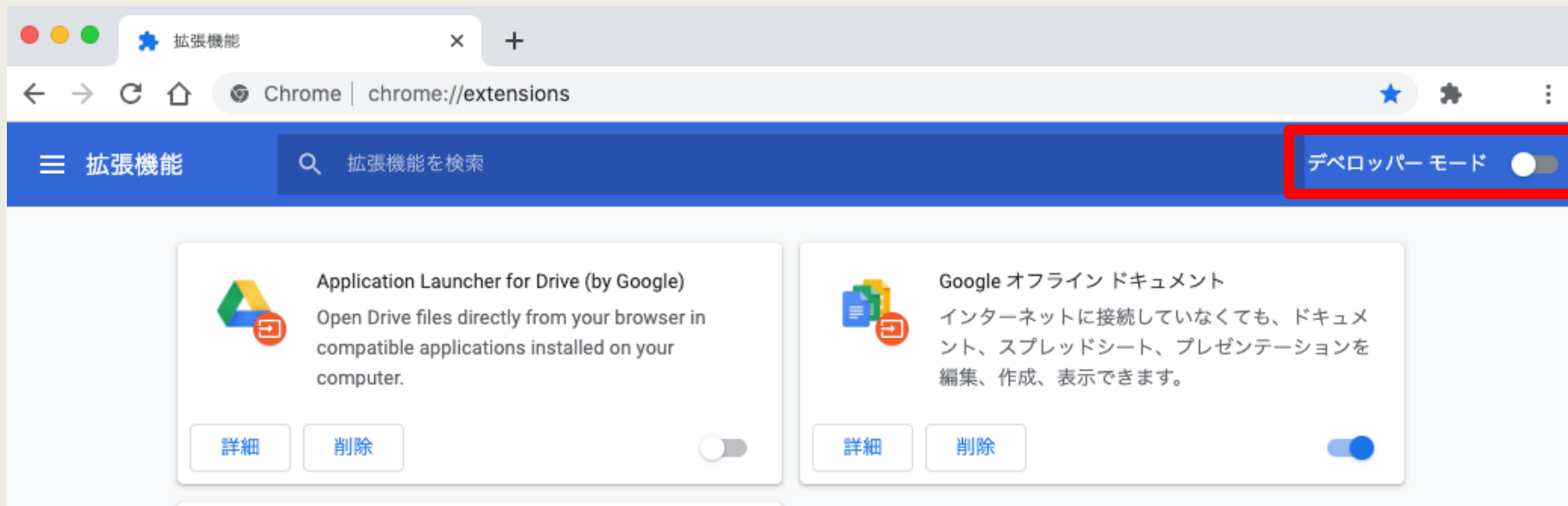
# 拡張機能の利用 Chrome

1. ChromeブラウザのURLにchrome://extensions/を入力しアクセス



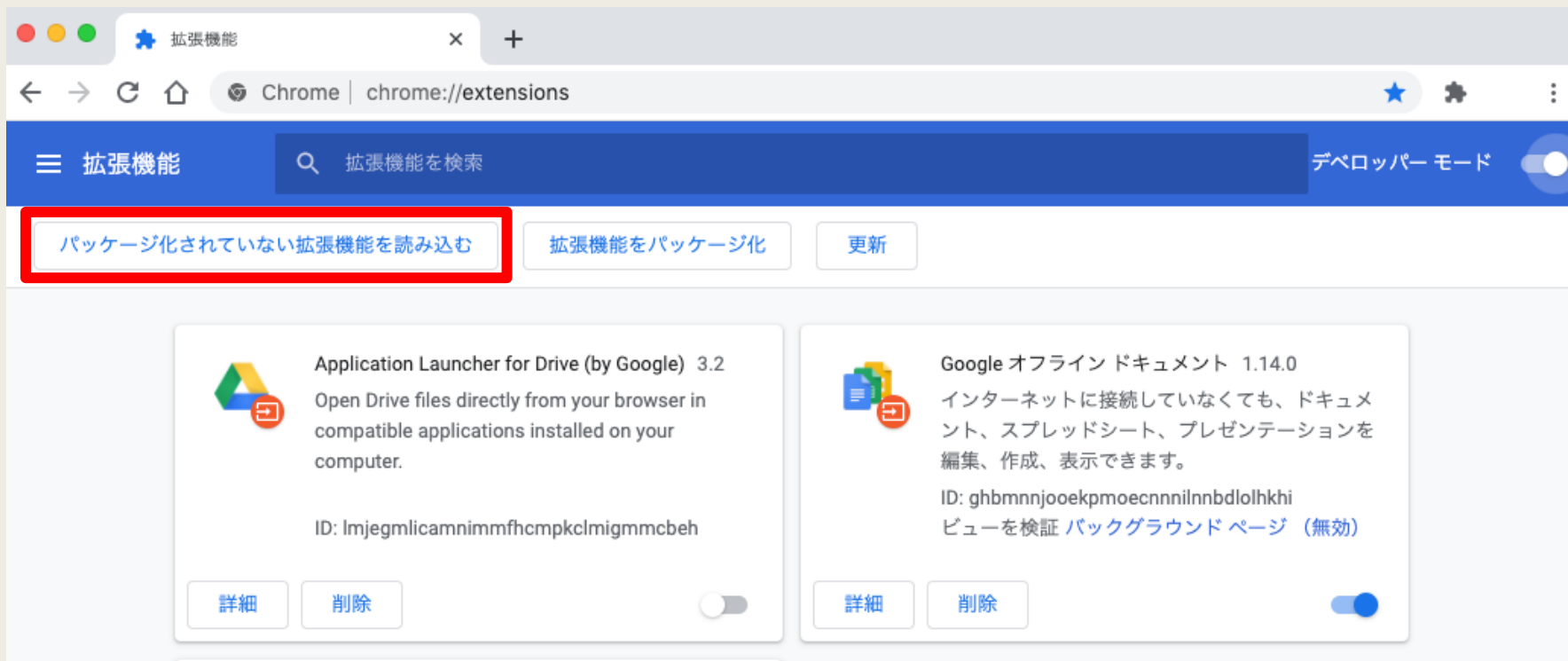
# 拡張機能の利用 Chrome

## 2. 画面右上の「デベロッパーモード」を有効にする



# 拡張機能の利用 Chrome

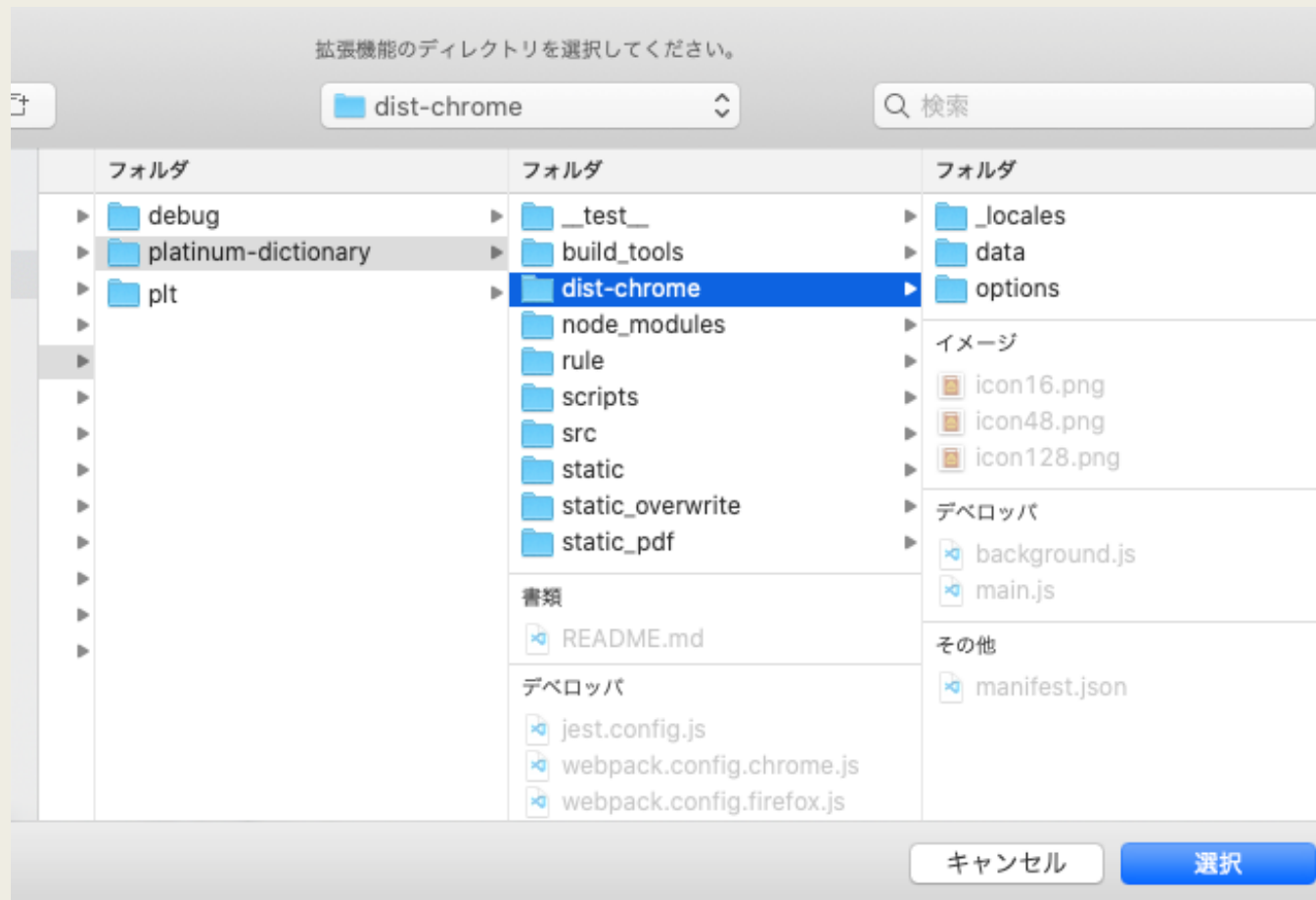
## 3. 画面左上の 「パッケージ化されていない拡張機能を読み込む」を選択





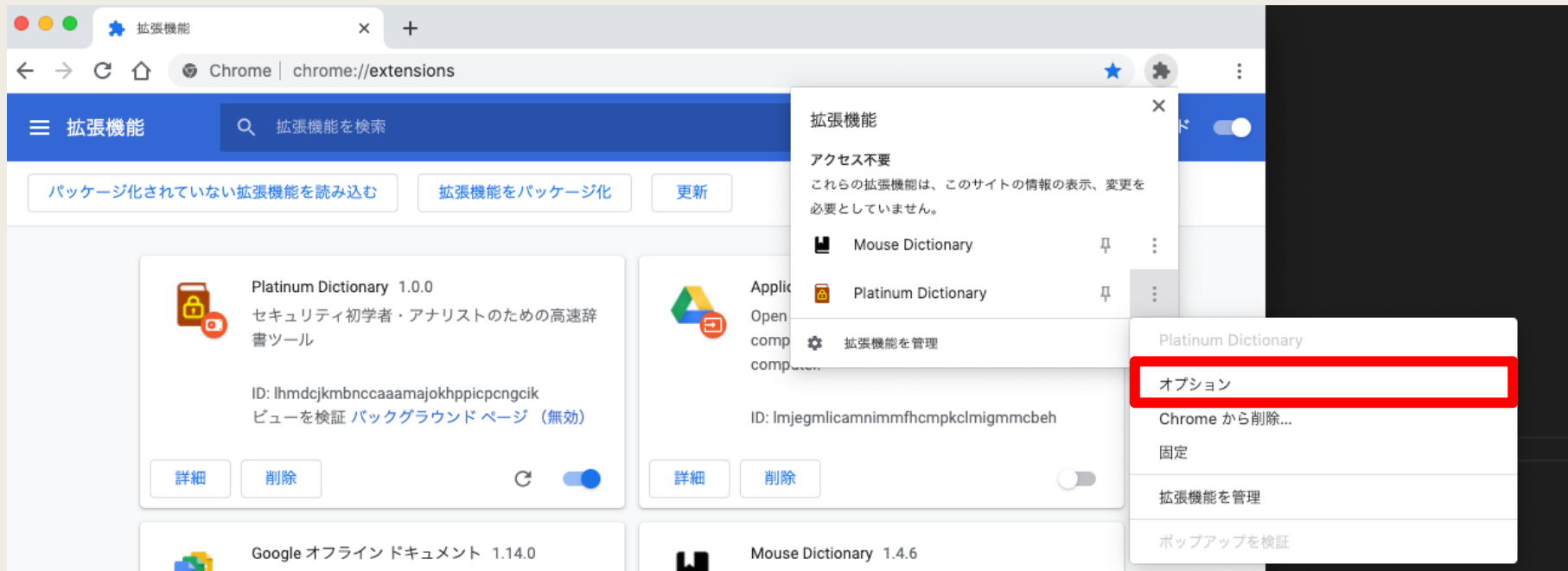
# 拡張機能の利用 Chrome

## 4. platinum\_dictionary/dist-chrome を選択



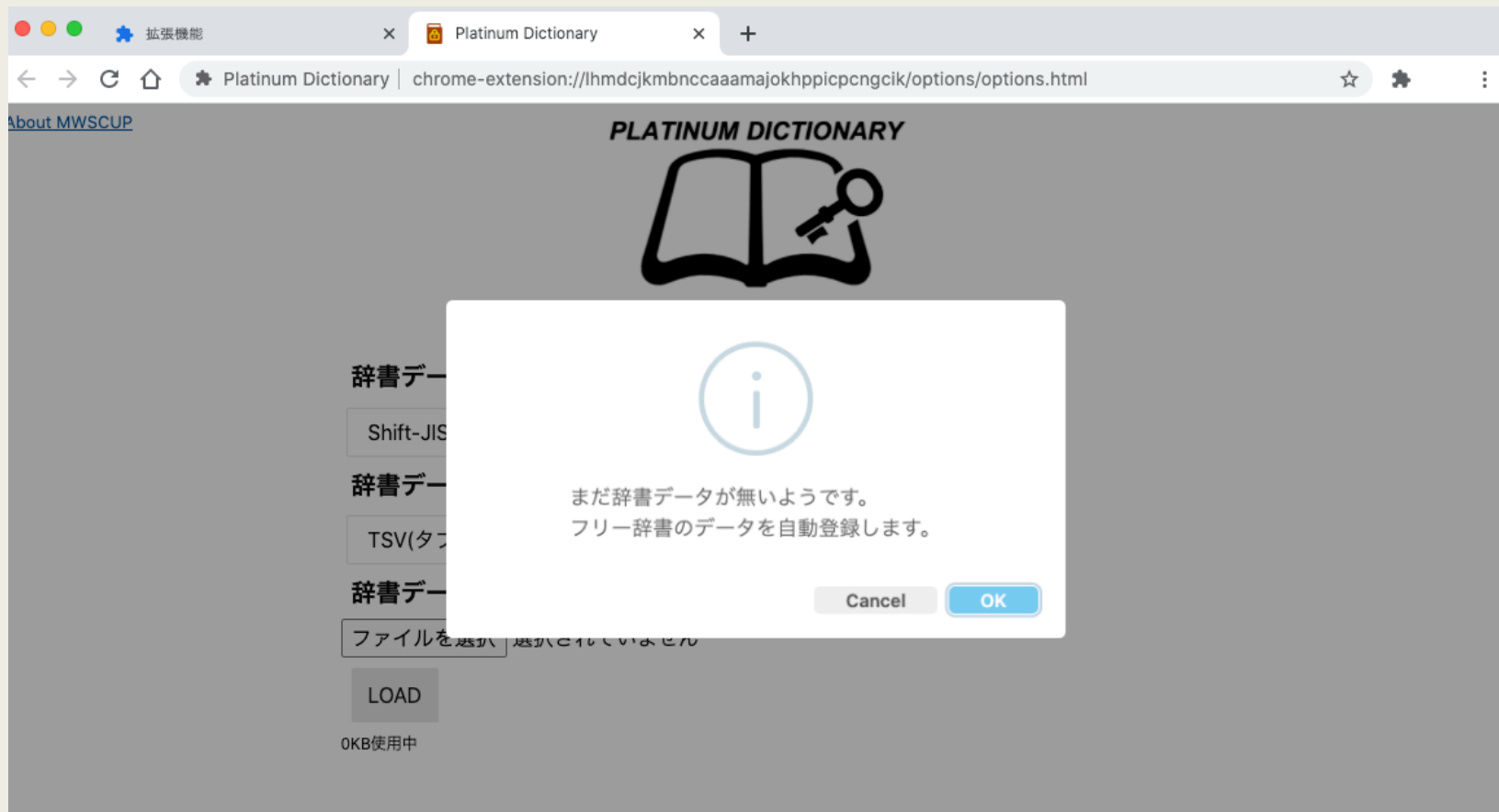
# 拡張機能の利用 Chrome

5. ブラウザ右上(URLの右)の拡張機能アイコンから  
Platinum Dictionary 縦の3点リーダーよりオプション項目  
を選択



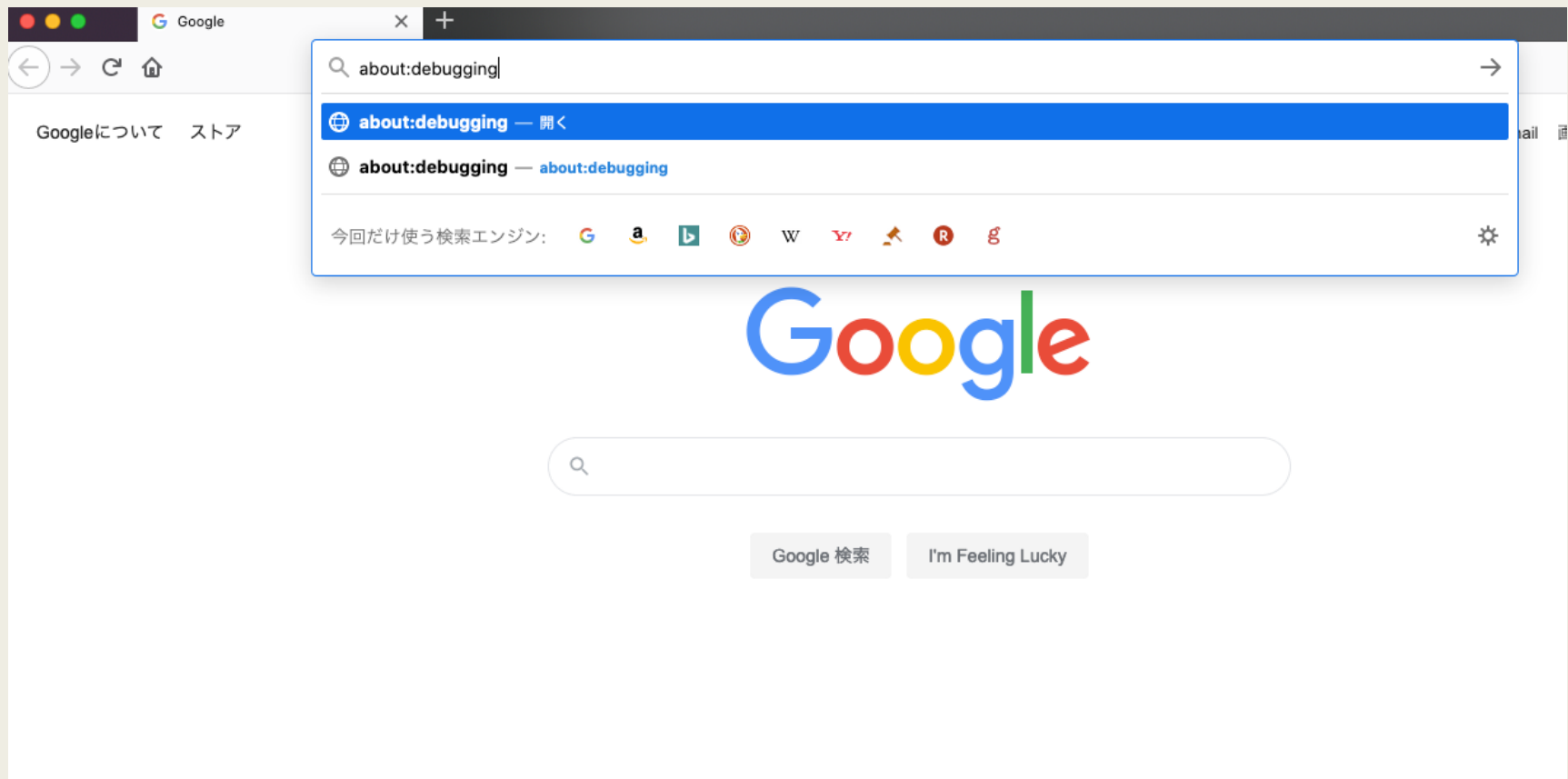
# 拡張機能の利用 Chrome

## 6. 辞書データの自動登録ポップアップでOKを選択



# 拡張機能の利用 Firefox

## 1. FirefoxブラウザのURLにabout:debuggingを入力しアクセス



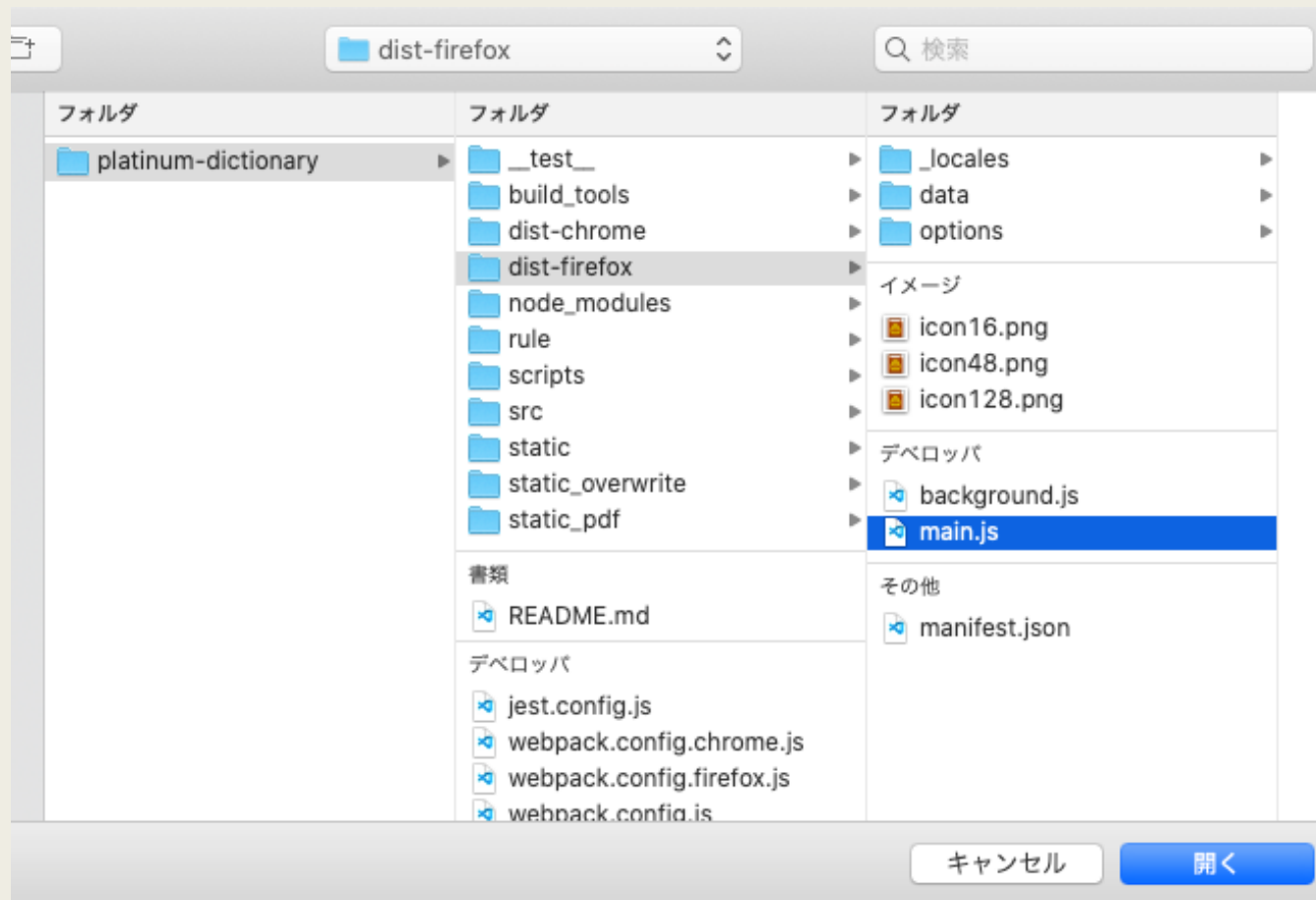
# 拡張機能の利用 Firefox

2. 左側タブの「このFirefox」をクリックし  
「一時的なアドオンを読み込む」をクリック



# 拡張機能の利用 Firefox

## 3. platinum\_dictionary/dist-firefox/main.js を選択



# 拡張機能の利用 Firefox

## 4. ブラウザ右上のPlatinum Dictionaryアイコンを 右クリックし「拡張機能を管理」を選択



# 拡張機能の利用 Firefox

## 5. Platinum Dictionary のオプション(横の3点リーダー)から設定をクリック





# 拡張機能の利用 Firefox

## 6. 辞書データの自動登録ポップアップでOKを選択



# 拡張機能の利用 Firefox

補足：Firefoxの拡張機能登録は開発用のためブラウザを再起動すると消えてしまう

永続的なインストール手順は  
"MDN web docs パッケージ化とインストール"ページを参照

[https://developer.mozilla.org/ja/docs/Mozilla/Addons/WebExtensions/Packaging\\_and\\_installation](https://developer.mozilla.org/ja/docs/Mozilla/Addons/WebExtensions/Packaging_and_installation)

# 使用方法

---

- 辞書機能
- 用語の登録
- 用語の検索
- 検索機能
- 分析機能

# 辞書機能

Webサイト中の文字列をマウスオーバーもしくは  
範囲選択を行うと登録されている用語を検索  
(画像は「ボットネット」にマウスオーバーした際の結果)

ログインしていません トーク 投稿記録 アカウント作成 ログイン

ページ ノート 閲覧

## Mirai (マルウェア)

出典: フリー百科事典『ウィキペディア (Wikipedia)』

**Mirai**（ミライ<sup>[3]</sup>、日本語の**未来**に由来するとみられる<sup>[4][註 2]</sup>）は **Linux** で動作するコンピューター大規模なネットワーク攻撃の一部に利用可能な、遠隔操作できるボットにする**マルウェア**である。**ネットワークカメラ**や**家庭用ルーター**といった家庭内のオンライン機器（IoTデバイス）を主要ターゲットとしている<sup>[6]</sup>。Mirai によって構築されたボットネットは、2016年8月<sup>[7]</sup>、**MalwareMustDie**というウェア調査報告グループによって初めて発見され、コンピュータセキュリティを得意とするジャーナリストである**ブライアン・クレブス**（英語版）のウェブサイトに行われた2016年9月20日の攻撃<sup>[8]</sup>や、**OVH**（英語版）に対する攻撃<sup>[9]</sup>、DNSサーバープロバイダの**ダ**（英語版）を標的とした**同年10月の攻撃**（英語版）といった、かつてないほどの大規模<sup>[10]</sup>かつ破壊的**DDoS攻撃**に使われてきた<sup>[11][12][13]</sup>。

Mirai の**ソースコード**は同年9月下旬<sup>[10]</sup>に、**オープンソース**として、**ハッカー**が集まるフォーラムされた<sup>[14]</sup>。そのため、Mirai の機構は他のマルウェア開発でも使われることとなった<sup>[15]</sup>。

**目次** [非表示]

- マルウェア
- DDoS攻撃での利用
- 亜種
- 

**ボットネット**

多数のコンピュータウイルスの一種であるボットに感染したコンピュータによって構成される特殊なネットワークのこと。ボットネットに接続されたコンピュータは、インターネット上から攻撃者が指示を出すことで、迷惑メールの配信や他のコンピュータへの攻撃、情報の窃取などを行うようになります。

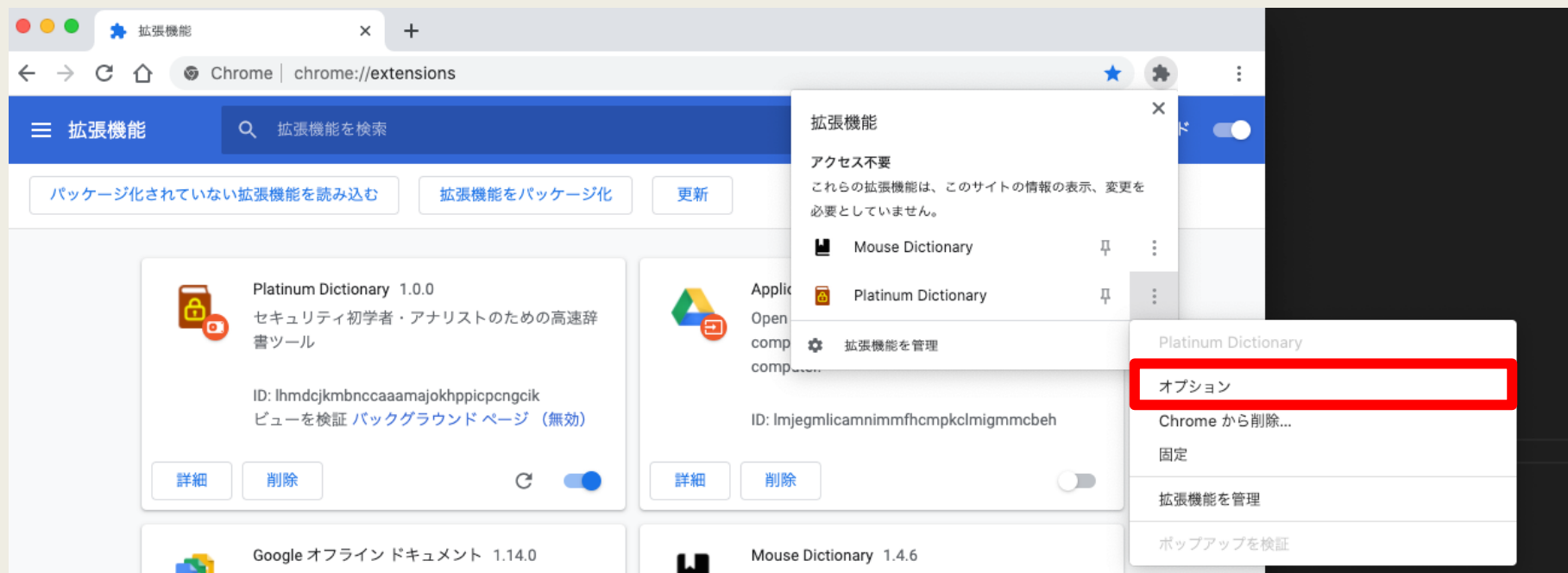
**ボット**

コンピュータを外部から遠隔操作するためのコンピュータウイルスの一種。ボットに感染してしまうと、インターネットを通じて、悪意のあるハッカーにコンピュータを遠隔操作されてしまうことがあります。外部から遠隔操作するという動作から、このようなウイルスのことをロボット（Robot）をもじってボット（BOT）と呼んでいます。基礎知識： **[コラム]** ボットとは？

https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/secu

# 用語の新規登録

ブラウザ右上のアイコンよりオプション画面に移動




# 用語の新規登録

辞書データ(テキストファイル)の文字コードを指定  
辞書データのファイル形式を選択  
対象ファイルを指定した後, Loadを実施

[About MWSCUP](#)

PLATINUM DICTIONARY



辞書データの文字コード：  
Shift-JIS ▼

辞書データの形式：  
TSV(タブ区切り) ▼

辞書データの読み込み：  
ファイルを選択 選択されていません

LOAD

1,248KB使用中

[オリジナルの拡張「Mouse Dictionary」](#)  
[PDFビューアを起動する](#)

⚙️ 設定を開く

# 用語の検索

辞書データとして登録されている用語を検索する機能  
オプション画面の「辞書を引く」より利用可能

PLATINUM DICTIONARY



辞書データの文字コード：  
Shift-JIS ▼

辞書データの形式：  
TSV(タブ区切り) ▼

辞書データの読み込み：  
ファイルを選択 選択されていません

LOAD

1,196KB使用中

[オリジナルの拡張「Mouse Dictionary」](#)

[辞書を引く](#)

設定を開く

Platinum Dictionary | chrome-extension://lhmdcjkmnbccaaamajokhppicpcngcik/dictionary/dictionary.html

PLATINUM DICTIONARY



セキュリティ用語検索

DNS SEC

辞書内容

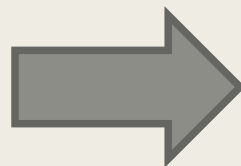
**DNS**  
DomainNameSystemの略称。インターネットに接続されたコンピューターの情報（ドメイン名とIPアドレスの対応など）を得るための仕組みです。例えば、「example.jp」にアクセスするためには、「example.jp」に対応するIPアドレスが「192.0.2.1」であるという情報が必要ですが、その対応を調べる際にDNSが利用されます。  
<https://jprs.jp/glossary/index.php?ID=0017>

**DNSSEC**  
DNSSecurityExtensionsの略称。DNS応答に電子署名を追加し、問い合わせ側で検証することでDNSの攻撃耐性を向上させる、セキュリティ拡張機能です。DNSSECは、受け取ったDNSレコードの出自（送信元で登録したデータであること）・完全性（データの欠落や改ざんのないこと）を問い合わせ側で検証できるようにするための機能をDNSに追加します。  
<https://jprs.jp/glossary/index.php?ID=0019>

# 検索機能

Webページ上の特定文字列(Hash, ドメイン, IPアドレス)  
に対して検査サイトでの検索を行う

Hash: 75ced96aa9c025ed...



Virus Total  
Hybrid Analysis  
abuse.ch



# 検索機能

Webサイト中の以下の特定の文字列を範囲選択を行うと  
パネル上にボタンが出現, 検索を実施できる

■ 観測されている検体

4月以降、数回にわたってバイナリが更新されていることを確認していますが、現時点で活動が観測されているのは以下のハッシュ値をもつ検体です。

| ファイル名                    | SHA256ハッシュ   |
|--------------------------|--|
| 81c4603681c46036.armv4l  | e11512be452867311a3c9112d2e4796e1b5073269cd4cc52544b8158eeb0c2a8 |
| 81c4603681c46036.i586    | ea005f9a03a0907b987a785fef0019959c4d16e18d1901f099e64d4daaa028c0 |
| 81c4603681c46036.mips    | 1e90ef7656efe7b41061e8e820018766c290664ad4391b5818805d08a706cf52 |
| 81c4603681c46036.mipsel  | 0c9ce3511f7a08af4c1f1ca1677f0fb2f8e2043defce067bcc48bd69ddd64455 |
| 81c4603681c46036.powerpc | 1a52148d301396a4a912d886c4cbed065a15bee875dbc796c28cee05a85eda8c |
| 81c4603681c46036.sh4     | 2732805680bb1319db5b17fead2dd48493a54e5ad54f4a026758ccb9f79482db |

■ C2 通信

C2 (Command & Control) の IP アドレスはバイナリの中にハードコードされており、過去に何度か変更されています。IJJ で確認している C2 のアドレスおよびポート番号は次のとおりです。

e11512be452867311a3c9112d2e4796e1b50732

[現在タブ] VTでハッシュ値を詳しく調べる

[新規タブ] VTでハッシュ値を詳しく調べる

[現在タブ] HAでハッシュ値を詳しく調べる

[新規タブ] HAでハッシュ値を詳しく調べる

[現在タブ] abuse.chでハッシュ値を詳しく調べる

[新規タブ] abuse.chでハッシュ値を詳しく調べる

# 分析機能

公開されているAPI機能を利用して各種サイトで検索を行う機能(バージョン1.0.0ではVTのみ対応)

• mipsel  
• powerpc  
• sh4

■ 観測されている検体

4月以降、数回にわたってバイナリが更新されていることを確認していますが、現時点で活動が観測されているのは以下のハッシュ値をもつ検体です。

| ファイル名                    | SHA256ハッシュ   |
|--------------------------|--|
| 81c4603681c46036.armv4l  | e11512be452867311a3c9112d2e4796e1b5073269cd4cc52544b8158eeb0c2a8 |
| 81c4603681c46036.i586    | ea005f9a03a0907b987a785fef0019959c4d16e18d1901f099e64d4daaa028c0 |
| 81c4603681c46036.mips    | 1e90ef7656efe7b41061e8e820018766c29064ad4391b5818805d08a706cf52  |
| 81c4603681c46036.mipsel  | 0c9ce3511f7a08af4c1f1ca1677f0fb2f8e2043defce067bcc48bd69ddd64455 |
| 81c4603681c46036.powerpc | 1a52148d301396a4a912d886c4cbcd065a15bee875dbc796c28cee05a85eda8c |
| 81c4603681c46036.sh4     | 2732805680bb1319db5b17fead2dd48493a54e5ad54f4a026758ccb9f79482db |

Platinum Dictionary

VTの分析結果を見る

サイトデータの読み取りと変更を行います ▶

オプション

Chrome から削除...

固定を解除

拡張機能を管理

ポップアップを検証

e11512be452867311a3c9112d2e4796e1b5073269cd4cc52544b8158eeb0c2a8

[現在タブ] VTでハッシュ値を詳しく調べる

[新規タブ] VTでハッシュ値を詳しく調べる

[現在タブ] HAでハッシュ値を詳しく調べる

[新規タブ] HAでハッシュ値を詳しく調べる

[現在タブ] abuse.chでハッシュ値を詳しく調べる

[新規タブ] abuse.chでハッシュ値を詳しく調べる

# 分析機能

分析結果の画面では調査結果を一覧として表示可能  
※機能の利用にあたりVTのAPIキー登録が必要

| アンチウイルスソフトごとの分析結果 |                  |           |      | 総合評価              |    |
|-------------------|------------------|-----------|------|-------------------|----|
| サービス              | カテゴリー            | 方式        | 評価   | 値の種類              | 件数 |
| ALYac             | undetected       | blacklist | null | confirmed-timeout | 0  |
| APEX              | type-unsupported | blacklist | null | failure           | 0  |
| AVG               | undetected       | blacklist | null | harmless          | 0  |
| Acronis           | type-unsupported | blacklist | null | malicious         | 0  |
| Ad-Aware          | undetected       | blacklist | null | suspicious        | 0  |
| AegisLab          | undetected       | blacklist | null | timeout           | 0  |
| AhnLab-V3         | undetected       | blacklist | null | type-unsupported  | 14 |
| Alibaba           | type-unsupported | blacklist | null | undetected        | 61 |

# その他

---

- バージョン
- 今後の追加機能について

# バージョン情報

- 1.0.0(2020/09/25) 公開バージョン

# 今後の追加機能について

- 辞書機能
  - 単語の増量
  - APTグループ, CWE番号を辞書化
  - NISTなどに大量の用語があり、説明書きを和訳して辞書化
  - 同義語の整理
  - 関連するワードの抽出
- 分析機能
  - 複数サービスの分析結果を比較できるページの作成
  - ユーザ間でAPIの設定内容の共有機能
  - 分析結果をCSVファイル等で出力する機能