

サポート詐欺に注意

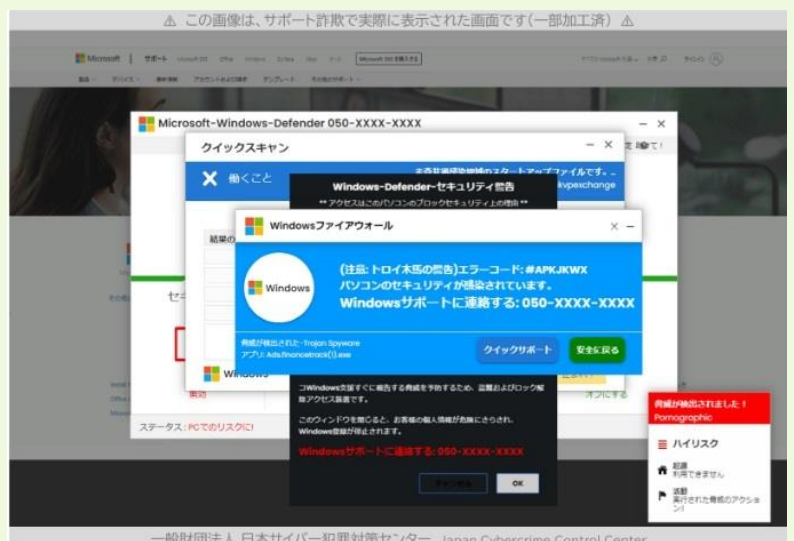


- 1 「サポート詐欺」とは、「偽のセキュリティ警告」等を表示し、金銭をだまし取ろうとする詐欺の手口です。
- 2 突然、警告画面が表示されたり、警告音が鳴っても、落ちついて、以下の手順で対応してください。

【対応手順】

〈サポート詐欺に用いられる偽警告画面の例〉

偽警告画面が表示されても・・・



出典元:一般財団法人日本サイバー犯罪対策センター (JC3)
<https://www.jc3.or.jp/threats/topics/article-396.html>



のような画面が出たら、・・・

- ③ Wi-Fiを切る (LANケーブルを抜く)
- ④ マウス操作等で、画面を閉じる (ブラウザの終了)

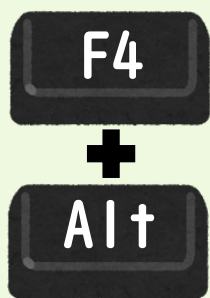
自宅で発生 → 保護者に相談
学校で発生 → 先生に相談

場合によっては保護者（先生）と相談して

警察への通報・相談

マウス操作等で、画面が閉じない（ブラウザを終了できない）時は、
キーボードによる操作（ショートカットキーの活用）を試してみてください。
（それでも閉じれないこともあります）

キーボードによる操作（ショートカットキーの活用）



【Windows の場合】
【プログラムの強制終了】

AltキーとF4キーを同時に押す。



【Mac の場合】
【プログラムの強制終了】

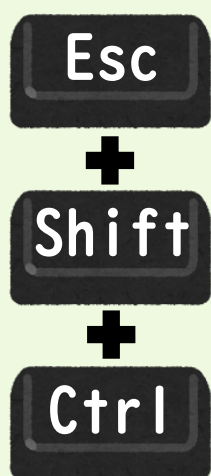
CommandキーとQキーを同時に押す。

表示されたアプリケーション一覧からブラウザアプリを選択して強制終了する。

【Windows の場合】

【タスクマネージャーからブラウザアプリを強制終了】

CtrlキーとShiftキーとEscキーを同時に押し、タスクマネージャーを起動する。



① アプリを選択

② タスクの終了をタップ
ブラウザアプリが閉じられ偽警告画面も消えます。



留意事項

ブラウザの再起動後、復元はせず、
右上の「×」印から表示を閉じてください。



Chromebook、iPadの場合

慌てずに画面を閉じて（ブラウザを終了して）ください。

また、使用したブラウザの閲覧履歴データの削除を行ってください。

（P3からのMicrosoft Edge、Google Chromeのセキュリティ機能を有効にする方法をご覧ください。）

【Microsoft Edgeのセキュリティ機能を有効にする方法】



① Microsoft Edge を開く

② ... をタップ

③ [設定] をタップ

④ [プライバシー、検索、サービス] をタップ



⑤ トラッキングの防止 「追跡防止」を嚴重にタップ

トラッキングの防止 ?

Web サイトでは、トラッカーを使用して閲覧に関する情報を収集します。Web サイトでは、この情報を使用して、サイトの改善やパーソナル設定された広告などのコンテンツの表示を行う場合があります。一部のトラッカーでは、ユーザーの情報を収集し、アクセスしたことがないサイトにその情報を送信することがあります。

追跡防止

基本

- すべてのサイトではほとんどのトラッカーを許可する
- コンテンツと広告がパーソナル設定される可能性があります
- サイトは適切に機能します
- 既知の有害なトラッカーをブロックします

バランス
(推奨)

- アクセスしたことがないサイトからのトラッカーをブロックします
- コンテンツと広告はほとんどパーソナル設定されない可能性があります
- サイトは適切に機能します
- 既知の有害なトラッカーをブロックします

嚴重

- すべてのサイトから送られるトラッカーの大部分をブロックします
- コンテンツと広告のパーソナル設定が最小限に抑えられる場合があります
- サイトの一部が機能しない可能性があります
- 既知の有害なトラッカーをブロックします

ブロックされたトラッカー
ユーザーの追跡がブロックされているサイトを表示する

例外
選択したサイトですべてのトラッカーを許可する

InPrivate で閲覧するときは、常に「嚴重」な追跡防止を使用する

嚴重に設定すると自動的にON

⑥-1 閲覧データをクリア

今すぐ行う場合は 「クリアするデータの選択」

閲覧データをクリア

これには、履歴、パスワード、Cookie などが含まれます。このプロファイルのデータのみが削除されます。 [データの管理](#)

今すぐ閲覧データをクリア

クリアするデータの選択

ブラウザを閉じるたびにクリアするデータを選択する >

すべての期間を選択

必要な項目をチェック

今すぐクリアをタップ

閲覧データをクリア

時間の範囲
すべての期間

- ☒ 閲覧の履歴
- ☒ ダウンロードの履歴
- ☒ Cookie およびその他のサイト データ
- ☒ キャッシュされた画像とファイル

8.7 MB 未済を解放します。一部のサイトでは、次のアクセス時に

今すぐクリア

キャンセル

⑥-2 閲覧データをクリア

普段の設定として、
[ブラウザを閉じるたびにクリアするデータを選択する]
を選択し設定（任意）

閲覧データをクリア

これには、履歴、パスワード、Cookie などが含まれます。このプロファイルのデータのみが削除されます。[データの管理](#)

今すぐ閲覧データをクリア

クリアするデータの選択

ブラウザを閉じるたびにクリアするデータを選択する



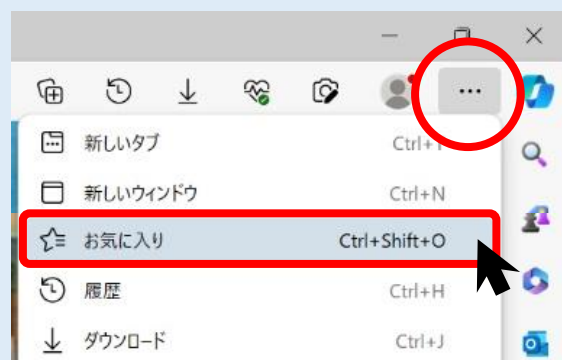
スクロール



(画面での設定を推奨しますが、各校にて確認下さい)

[参考]

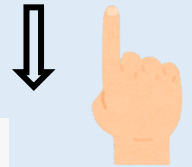
必要なものはお気に入り登録も
活用ください。また、定期的に
データの整理を行ってください。



⑦ セキュリティ

各項目の確認

スクロール



セキュリティ

Microsoft Edge のセキュリティ設定を管理

証明書の管理

HTTPS/SSL の証明書と設定を管理します


Microsoft Defender SmartScreen

Microsoft Defender SmartScreen を使って悪意のあるサイトやダウンロードから保護する

望ましくない可能性のあるアプリをブロックする

予期しない動作を引き起こす可能性がある低評価のアプリのダウンロードをブロックします

Web サイト誤入力保護

Web サイト誤入力保護に満足していますか? 

サイト アドレスを誤って入力した場合や、悪意のあるサイトに転送される可能性がある場合は警告する。

以前に許可されたすべてのサイトをクリアする

クリア

セキュア DNS を使用して、Web サイトのネットワーク アドレスを検索する方法を指定します。

既定では、Microsoft Edge は現在のサービス プロバイダーを使用します。代替 DNS プロバイダーが原因で、一部のサイトに到達できない場合があります。

☐ 現在のサービス プロバイダーを使用

現在のサービス プロバイダーが安全な DNS を提供していない可能性があります。



ON






OFF

⑧ Web 上のセキュリティを強化する

[Web 上のセキュリティを強化する]

を ON すると選択可能となり、[厳重]を設定

カスタム プロバイダーを入力してください

Web  上のセキュリティを強化する 強化されたセキュリティ モードに満足していますか?  

このモードをオンにすると、Web をより安全に閲覧し、ブラウザをマルウェアから保護するのに役立ちます。必要なセキュリティレベルを選択します。

バランス
(推奨)


- 頻繁にアクセスしないサイトにセキュリティ問題の軽減策を追加する
- ほとんどのサイトは想定どおりに動作します
- セキュリティの脅威をブロックする

厳重

- すべてのサイトにセキュリティ問題の軽減策を追加する
- サイトの一部が機能しない可能性があります
- セキュリティの脅威をブロックする

サイトでの強化されたセキュリティの管理
この機能を、選択したサイトで常にオンまたはオフに設定します

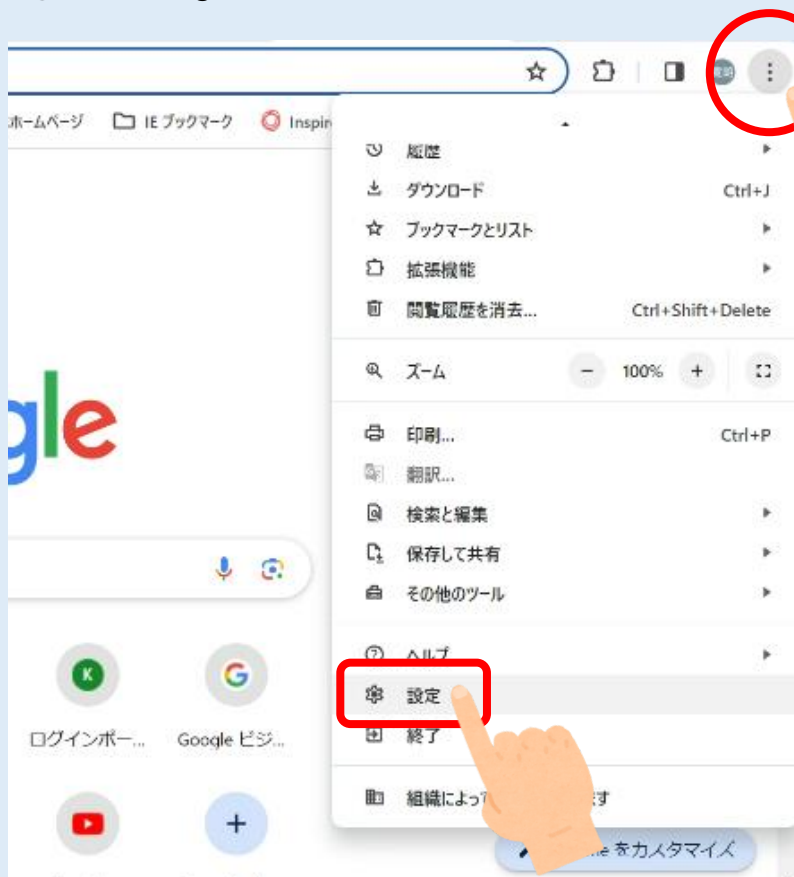
InPrivate で閲覧するときは、常に "厳密" レベルの強化されたセキュリティを使用する

厳重に設定すると自動的にON 

【Google Chromeのセキュリティ機能を有効にする方法】



① Google Chromeを開く



②

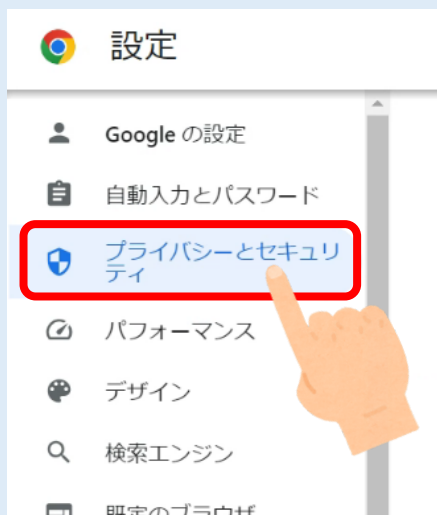


をタップ

③

【設定】

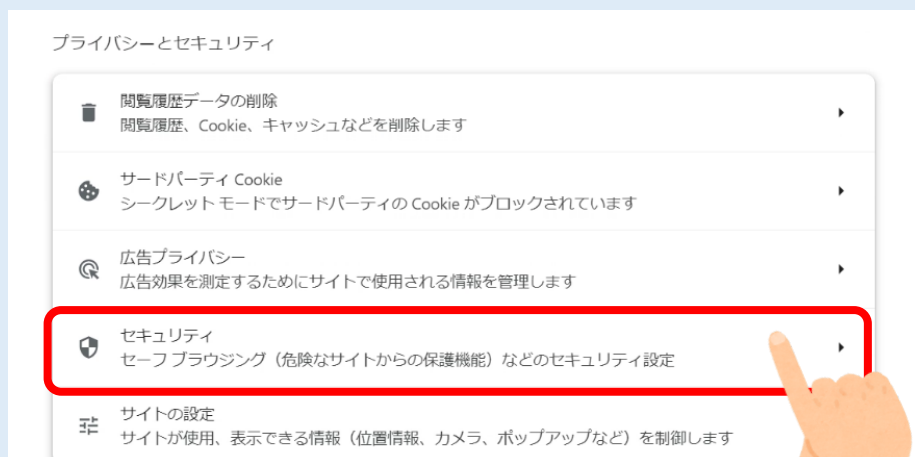
をタップ



④

【プライバシーとセキュリティ】

をタップ

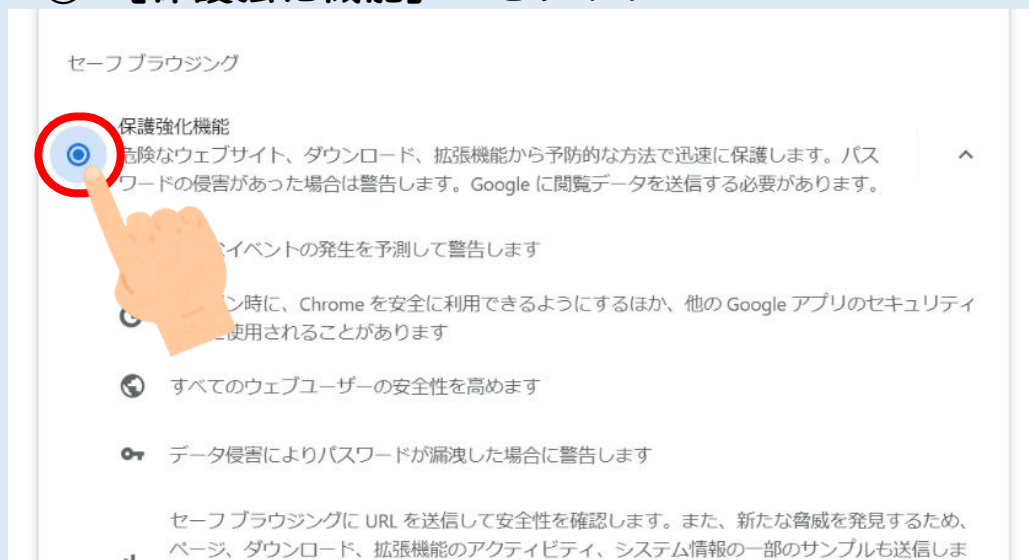


⑤

【セキュリティ】

をタップ

⑥ 【保護強化機能】 をタップ



閲覧履歴データの削除は「閲覧履歴データの削除」の選択



期間 全期間を選択

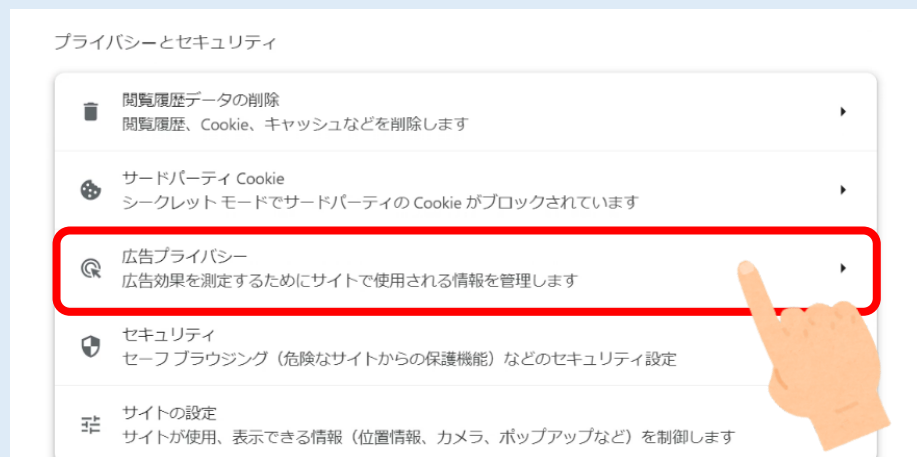
必要な項目をチェック

データの削除をタップ

[参考]

必要なものはブックマーク登録も活用ください。また、定期的にデータの整理を行ってください。





⑦ [広告プライバシー]
をタップ



⑧ [広告のトピック]
をタップ



⑨ [広告のトピック]
をOFF

OFF



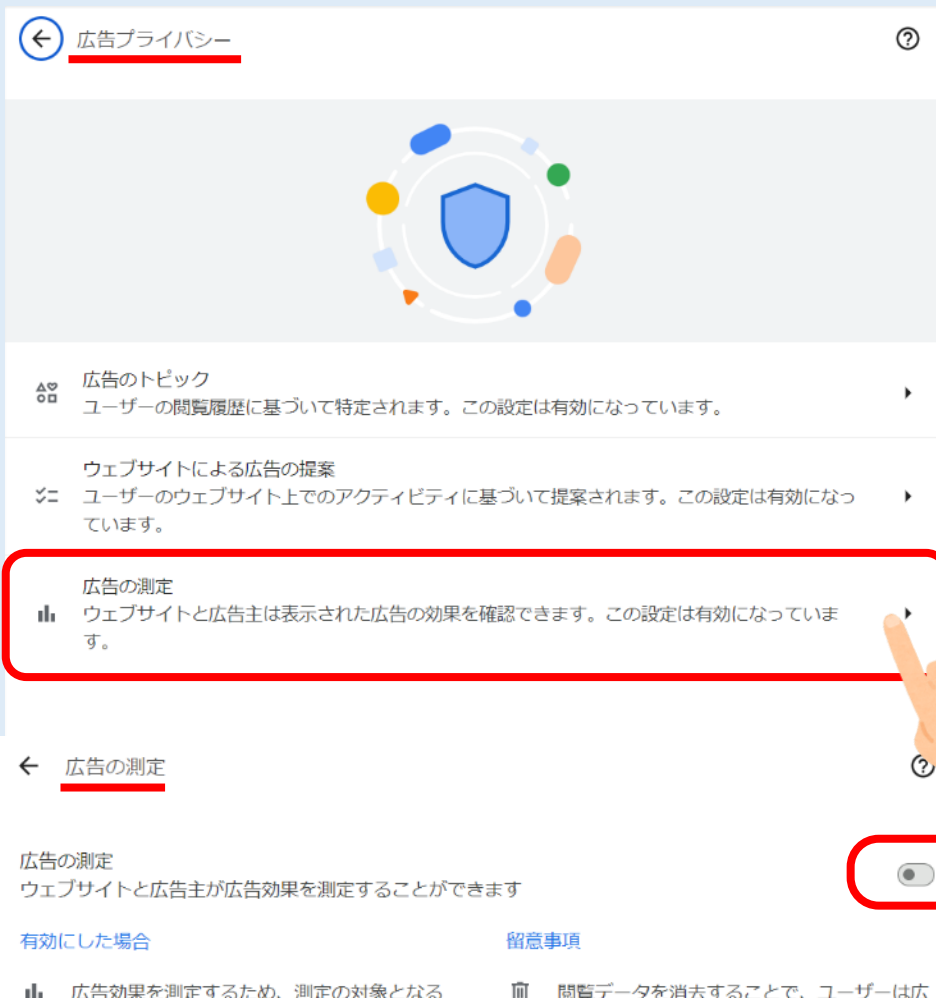
⑩ [Webサイトによる
広告の提案]

をタップ

⑪ [Webサイトによる
広告の提案]

をOFF

OFF



⑫ [広告の測定]

をタップ

⑬ [広告の測定]

をOFF

OFF

【Safariのセキュリティ機能を有効にする方法】



① ホーム画面の

「設定」

をタップ



③ 「詐欺Webサイトの警告」スイッチをオンにする。

Googleが提供するセーフブラウジング機能が有効化され、フィッシングサイトや偽サイトである可能性が高いと判定されたWEBサイトへ接続しようとしたときに警告してくれます。



④ 「Safari」



を選択し
タップ



⑤ ON

⑤ 「ポップアップブロック」
スイッチをオンにする。

不要な広告画面の立ち上げを
制御する機能です。

[参考]

「Apple IDを2ファクタ認証」で守る

2ファクタ認証によってApple IDの認証を二重化する方法もあります。

ホーム画面の

「設定」

をタップ



設定



ON

新しいデバイスでサインインするときはパスワードに加えて、信頼済みの
デバイスに送信される確認コードを入力する必要があります。