

メールアドレスの漏洩チェック等

JJ1SXA/池

メールアドレスの漏洩チェックは、ファイアーフォックスモニターがFBです、ブラウザをファイアーフォックスに切り替え、「<https://monitor.firefox.com>」のサイトに移動、アドレスを入力して、「データ侵害を確認する」ボタンを押すだけ。

あなたのプライバシーを守る方法があります。Firefox を使用しましょう。詳しくはこちら。

Firefox Monitor

ホーム アラート侵害 ヘルプ/フィードバック ログイン

オンラインのデータ侵害に含まれていないか確認しましょう。

ハッカーが誰にあなたについて知っているかを調査しましょう。一歩先に行く方法を学んでください。

メールアドレスを入力してください

データ侵害を確認する

2007 年までさかのぼって、メールアドレスがデータ侵害と検出されているか確認します。

最近追加されたデータ侵害

**StreetEasy**

侵害が検出されたのは:
2019年10月6日

漏洩したデータ:
パスワード、メールアドレス

この侵害を詳しく見る/報告する

個人情報の制御を取り戻してください。

ハッカーのハッキングは止められません。しかし、ハッキングを容易にできる悪影響は避けられます。

- 💡 ハッカーの手段を分解する >
- @ データ侵害があった後にするべきこと >
- 🔒 強力なパスワードの作り方 >
- 🔒 セキュリティの秘訣をわっと読め >

Firefox アカウントでデータ侵害の監視に登録しましょう。



新しいデータ侵害の警告を受け取る

あなたの情報が新しいデータ侵害によりさらされた場合、警告を送信します。



複数のメールアドレスを監視する

複数のメールアドレスに対してデータ侵害の監視をしましょう。



オンラインプライバシーを保護する

ライバー犯罪からデータを盗取に伴うために必要なことを見つけましょう。

登録して通知を受け取る

Firefox ブラウザは Firefox アカウントには必要ありません。Monitor サービスについての情報は受け取るでしょう。

既にアカウントをお持ちですか? [ログイン](#) >

moz://a

Firefox Monitor について よくある質問 利用規約と個人情報保護方針 GitHub

漏洩していなければ、「このメールアドレスは0個の既知のデータ侵害があります」と表示され、漏洩していると、「このメールアドレスは2個（例）の既知のデータ侵害があります」と表示されます。

クロームでも、IDやパスワードの調査ができます、Chrome拡張機能は、クロームブラウザで「<https://chrome.google.com/webstore>」を開き、「Password Checkup 拡張」で検索、見付かったら、「chromeに追加」ボタンを押すと、クロームの画面右上に、下図のような「アイコン」が常駐する。



クロームが記憶していたり、サイトで入力したりしたユーザー名 (ID) やパスワードについて漏洩の情報があれば、警告を表示する。

パスワードの漏洩もチェックしましょう、「<https://haveibeenpwned.com/Passwords>」のサイトを開き、「パスワード」を入力、右隣の窓の「pwned?」をクリックするだけ。

A screenshot of the 'Have I Been Pwned' (HIBP) website's 'Passwords' section. The page has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords (selected), API, About, and Donate. The main content area is light blue and features the title 'Pwned Passwords'. Below the title is a paragraph explaining that 555,278,657 real-world passwords were previously exposed in data breaches. A search bar with the placeholder text 'password' and a 'pwned?' button is present. Below the search bar is a section for '1Password' with a link to 'Learn more at 1Password.com'. At the bottom, there is a section titled 'Password reuse and credential stuffing' with a paragraph explaining the risks of password reuse and credential stuffing attacks. The URL 'https://haveibeenpwned.com/Passwords' is visible in the footer.

漏洩が無ければ、「Good news-no pwnage found!」と表示される、漏洩があると、「Oh no-pwned」と表示される。

パスワードの漏洩が確認できれば、即、パスワードの変更は当然のこと。

現在悪徳業者は、「名簿業者から入手する」、「マルウェアに感染させて情報を盗む」、「ウェブ上に掲載された情報を取得」、「ウェブサイトで入力させる」、「総当たり攻撃でアドレスを生成する」、「クラウドや企業のサーバーを攻撃して盗む」等々の手口でアドレスを入手している。

メールアドレスを盗まれないためには、「マルウェア対策は確実に」、「アプリの権限にも注意」、「ウェブやSNSで公開しない」、「怪しいサイトに登録しない」、「簡単なアドレスは使わない」等の注意が肝要のようです。

メールアドレスが漏れないように気を付けていても、何らかの外的要因によりアドレスが漏洩してしまうこともある、つまり、誰でも詐欺メールの標的になり得るのだ。

もしも詐欺メールが届いたら、「無視して捨てろ」が原則、詐欺メールの対応は、「どうすべきか」よりも「やってはいけないこと」の方が重要だ、やってはいけないことは、「メールに返信する」、「添付ファイルを開く」、「リンクをクリックして開く」、「安易に画像を表示する」だ、だが、詐欺メールの見分けは難しい、怪しそうなのは詐欺メールと思った方がよい。

なお、メールは「Gメール」が良さそうだ、「Gメール」の迷惑メールフィルターは、グーグルが採用する機会学習によって高い精度を誇るようです。

Win10 の標準ブラウザは、「エッジ」ですが、使い慣れた、「IE」を使っている方も多いことでしょう、斯くいう私も、未だに「IE」です。

ただ、「IE」不調時に、即ブラウザを切り替えられるように、「クローム」と「ファイアーフォックス」をダウンロードして、待機させています。

皆さんも、複数のブラウザをダウンロードして、待機させておいて、使用中のブラウザ不調時に切り替えたり、たまには気分転換で、別のブラウザを使ってWEBを見るのも良いものです。

グーグル・クロームダウンロード

<https://www.google.co.jp/chrome/>

ファイアーフォックスダウンロード

<https://www.mozilla.org/ja/firefox/new/>