

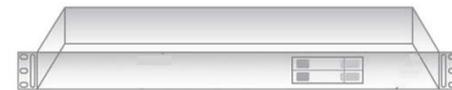
ID・パスワードだけじゃダメなんですか

～ 多要素認証やリスクベース認証から生体認証までを
用途に応じて使い分ける方法を解説 ～

株式会社 ムービット

会社概要

社名	株式会社ムービット
設立	1995年12月8日
所在地	東京都北区王子1-28-6
主な製品	Powered BLUE シリーズ アプリケーションサーバー (Linux) ソフトウェア開発



ダークWeb



ダークWeb / データやアクセス権の売買

サイバー攻撃ツールの闇市場が拡大している。身代金目的で端末内のデータを暗号化するランサムウェア、標的となる組織に不正アクセスできる権利などが売りに出され、競争が新たな高値を生み出していく。技術が高度になり、攻撃者の裾野拡大が懸念されている。「最も安い検出不能ランサムウェア」は1カ月に200万、6カ月に490万、12カ月に990万だ。

■「ランサムウェア」月120ドルから

ランサムウェアは、使った分が流通しており、近年、取引の対象は一般化する形で展開。検出を免れる形で、多様化している。

「トランプ大統領」に答える形で、多様化している。ランサムウェアは、使った分が流通しており、近年、取引の対象は一般化する形で展開。検出を免れる形で、多様化している。

サイバー攻撃 闇市場拡大

販売が確認されたサイバー攻撃用のサービスやツール

医療系大学へのアクセス権	999%
米有力企業へのアクセス権	1万%
ATM用のマルウェア	2000%~
ランサムウェアのサービス	年間900%
スパムSMSの送信サービス	25~500%
SMS送信用のソフトウェア	499%~

(出所)トレンドマイクロ

売り手で競争、脅威増す

キヤンマーケティングジャパンが確認したランサムウェアの販売サイト「同提供」



セキュリティ関係者によると、国内38社などから種別した疑いが明らかになったVPN（仮想私設網）の利用情報は、有料の会員制サイト内でやり取りされていた。サイバー攻撃をサポートするマルウェア販売や「サービス」とも呼ばれることで、「高度な技術や専門知識がなくても攻撃を実行できるようになる」という。ロシアのウイルス対策ソフト開発会社「ドクタウェーブ」のボリス・シヤロフ最高経営責任者（CEO）は「売りがあふれている」と指摘し、マルウェアなどの攻撃力が高まる「サイバー攻撃と闇市場」に懸念を示している。海外ではおとり捜査で闇市場サイトを閉鎖に追い込んだ事例もあるが、日本では捜査権限が限られる「セキュリティ」の観点から、マルウェアの流通は抑えられず、闇市場は拡大している。攻撃の発生した場合は、闇市場の取引に歯止めをかけるのは難しいという。

真相深層

マルウェアの販売は国内では不正指合電磁的記録提供の罪に当たる。たけなぐても、得意分野の不正なプログラムと技術を生かし、効率的に使用されておためしに提供されている。マルウェアの流通は国内では不正指合電磁的記録提供の罪に当たる。たけなぐても、得意分野の不正なプログラムと技術を生かし、効率的に使用されておためしに提供されている。マルウェアの流通は国内では不正指合電磁的記録提供の罪に当たる。たけなぐても、得意分野の不正なプログラムと技術を生かし、効率的に使用されておためしに提供されている。

- 医科系大学へのアクセス権 999ドル
- 米国有力企業へのアクセス権 1万ドル
- ランサムウェアのサービス 900ドル

Twitter メールアカウント漏洩

Twitterからという2億件以上の漏洩データがネットで公開、 専門家が注意喚起

掲載日 2023/01/07 13:52 更新日 2023/01/07 13:57

著者 : Yoichi Yamashita



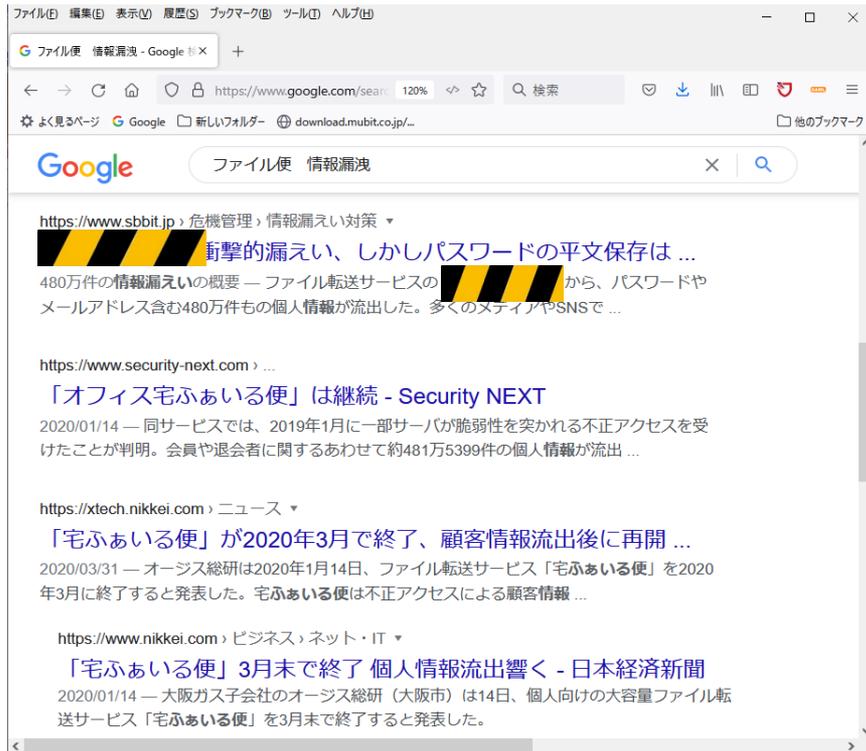
Twitterユーザーの個人情報だという2億件以上のデータが何者かによってオンラインフォーラムで公開された。過去のTwitterのセキュリティ問題から、「Have I been Pwned」など漏洩情報をまとめているサービスはTwitterからの漏洩データである可能性が高いと判断して投稿されたデータをシステムに追加。影響を受ける人々に注意を喚起している。



公開されたデータは、Eメールアドレスのほか、Twitterのユーザー名、ユーザーの本名（登録している場合）、フォロワー数、アカウント作成日などを含み、パスワードは含まれていない。

Twitterは2022年8月に、第三者がユーザーの情報を取得できるTwitter APIの脆弱性が2021年6月から数カ月にわたって存在していたことを公表した。その脆弱性を使用して取得したというデータがハッキングフォーラムに投稿されており、同社はそれらが脆弱性を修正する前に収集された情報の悪用であることを認めた。

某 ファイル交換サイト 480万件ID漏洩



2019年1月

ID メールアドレス

Passwd 生のパスワード

生年月日・性別・職業...

パスワードやメールアドレスアカウント流出チェックサイト

https://haveibeenpwned.com/



①



password

pwned?

②



Pwned Passwords

Pwned Passwords are 551,509,767 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. Read more about how HIBP protects the privacy of searched passwords.



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

NIST's guidance: check passwords against those obtained from previous data breaches

The Pwned Passwords service was created in August 2017 after NIST released guidance specifically recommending that user-provided passwords be checked against existing data breaches. The rationale for this advice and suggestions for how applications may leverage this data is described in detail in the blog post titled [Introducing 306 Million Freely Downloadable Pwned Passwords](#). In February 2018, version 2 of the service was released with more than half a billion passwords, each now also with a count of how many times they'd

- ① パスワードを入力
- ② pwned? を押す

Oh no --- pwned !

残念でした

Good news — no pwnage found!

大丈夫

リスト攻撃

パスワードリスト攻撃の概要



攻撃者は、不正に入手したID/パスワードのリストを用いてインターネットサービスに対しログインを試行



インターネットサービス

ID	パスワード
suzuki	suzuki0123
tanaka	p@ssw0rd
.....



A社

B社

C社



ID	パスワード
suzuki	suzuki0123
tanaka	p@ssw0rd
.....

利用者が複数のサービスに同じID/パスワードを設定

2022年 不正ログインなどの事案

2022年3月

「ふるさと納税サイト」 600万回の「リスト型攻撃」で被害、2000件超の個人情報流出か

2022年5月

「看護roo!」 に「パスワードリスト型攻撃」、1,877件のアカウントでポイントの不正使用を確認

2022年6月

フリマアプリ 「SNKRDUNK」 に不正アクセス、275万件の顧客情報が流出した可能性

2022年6月

「honto」も「リスト型攻撃」を確認、電子書籍サービスで被害続出

2022年7月

「読売新聞」のサイトに不正アクセス 個人情報流出の可能性

2022年7月

「サンドラッグ」/ECサイトと顧客サイトに「リスト型攻撃」による不正ログイン

2022年8月

中古販売の「ハードオフ」で会員6,186件の情報流出 公式アプリに不正ログイン発生

2022年9月

「ニトリアプリ」に不正アクセス、「リスト型攻撃」で約13万件強の顧客情報が閲覧された可能性

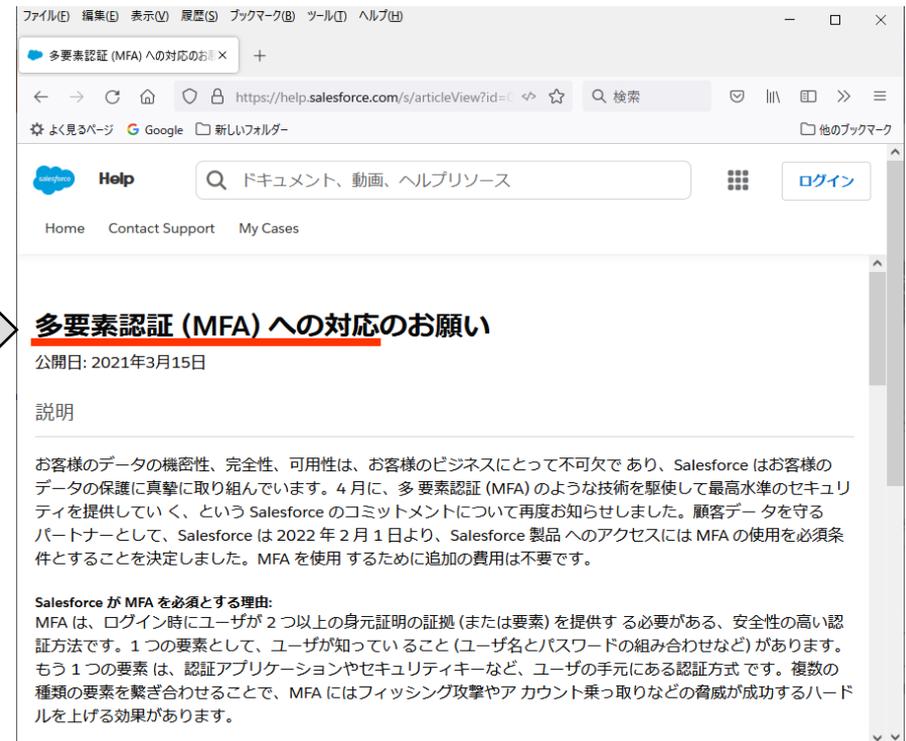
2022年10月

「スクエニ」、FF14への「リスト型攻撃を検知」 パスワード強制リセットの可能性も
認証情報の再設定を呼び掛け

多要素認証が必要とされる背景

- リモートワーク
社員の自宅や出先からのアクセス対応
- ID・パスワードの窃取対応
- 安全を担保できる仕組みが多要素認証（MFA）

Google や Salesforce 多要素認証



Google社は
「Googleアカウントの二要素認証を自動的に有効化」

SalesforceはMFAの必須化

本人確認の認証方法

強度	認証	主な特徴
● 知識認証	本人が知っている事項で認証	ID/Password 暗証番号
● 所有物認証	本人が所有している物で認証	電子証明書 セキュリティ・トークン ワンタイムパスワード・トークン スマートフォン（2経路認証）
● 生体認証	本人の生物学的な要素で認証	指紋認証 虹彩認証 静脈認証 顔認証

* 複数の認証の組合せ運用も可能

主な認証方式 利用時のポイント

認証メソッド	特徴
ID/パスワード認証	パスワードの使いまわし 漏洩している可能性あり
SMS認証	送信ごとに課金される（運用者側） エリア外だと受信できない アクセス毎にワンタイムパスワードの入力が必要
ワンタイムパスワード認証	無償のソフトウェアトークンが利用できる アクセス毎にワンタイムパスワードの入力が必要
画像認証	指定の画像を選択させる
SSLクライアント認証	SSLクライアント証明書を配布する必要がある
生体認証	認証器を用意する必要がある

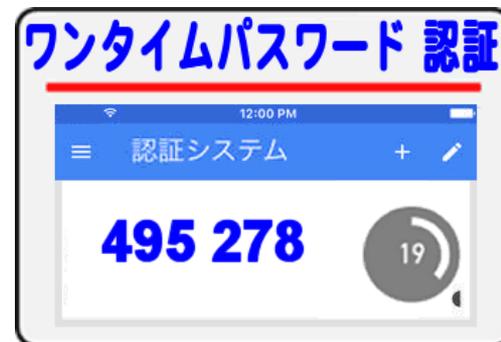
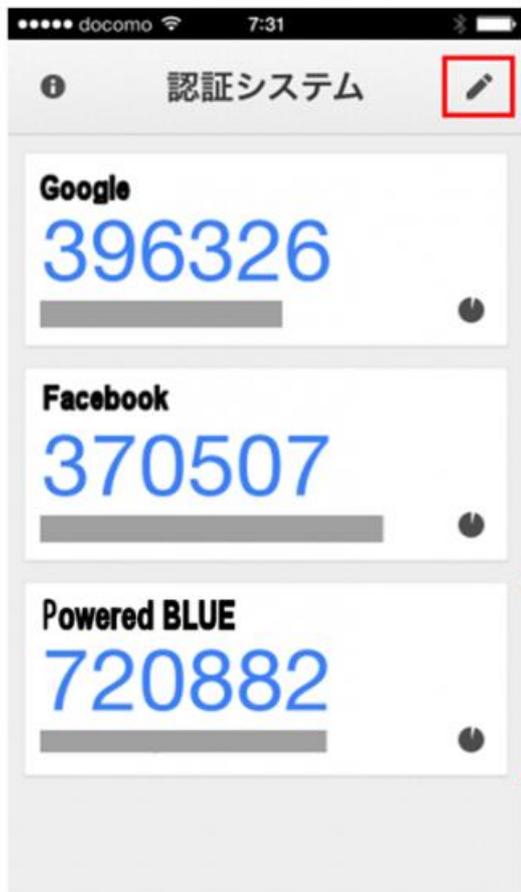
SMS認証 スマートフォンの番号に通知



G-123789 があなたの
Google 確認コードです。

ヤフー 確認コード:615716
このコードは他の人には絶対に
教えなくてください。
@login.yahoo.co.jp #[615716](#)

ワンタイムパスワード認証 ソフトウェア・トークン

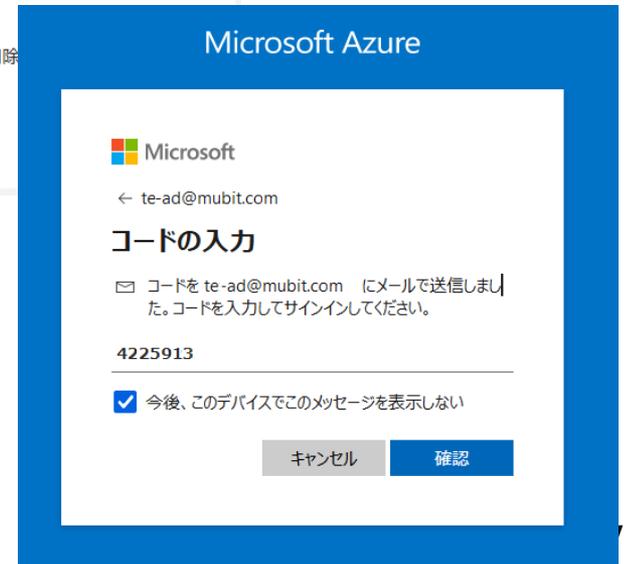


ユーザーのQRコード



ワンタイムパスワード認証

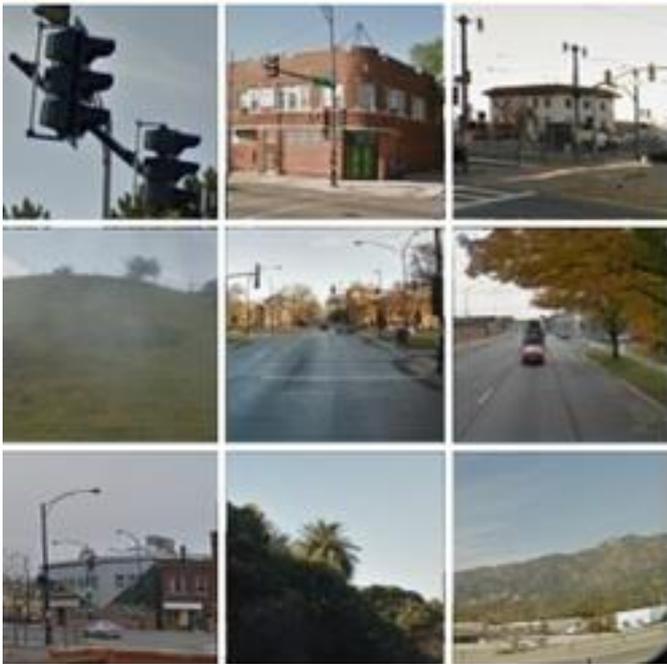
メール通知の例



画像認証

山や丘

の画像をすべて選択してください。



確認

画像の文字を入力してください。  画像や音声による認証について

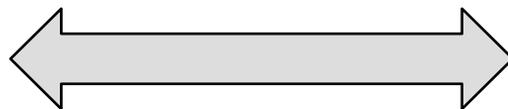
うちんおちを

 別の画像を表示する

文字の入力：

うちんおちを

■ SSLクライアント証明書



■ SSLサーバー証明書

SSLクライアント認証例 スマートフォン



証明書 有効



証明書 なし・失効

FIDO2 / (ファイドツー)

- 生体認証 を 利用 して
Web に ログイン できる 標準規格

⇒ブラウザでWebへアクセスする際の生体認証の規格



- FIDO2 の 大きなユーザーメリット は

ハード・ソフト が 対応済

FIDO2 / 対応の機器

Windows 10 / 11 / Mac / アンドロイド携帯



ブラウザ



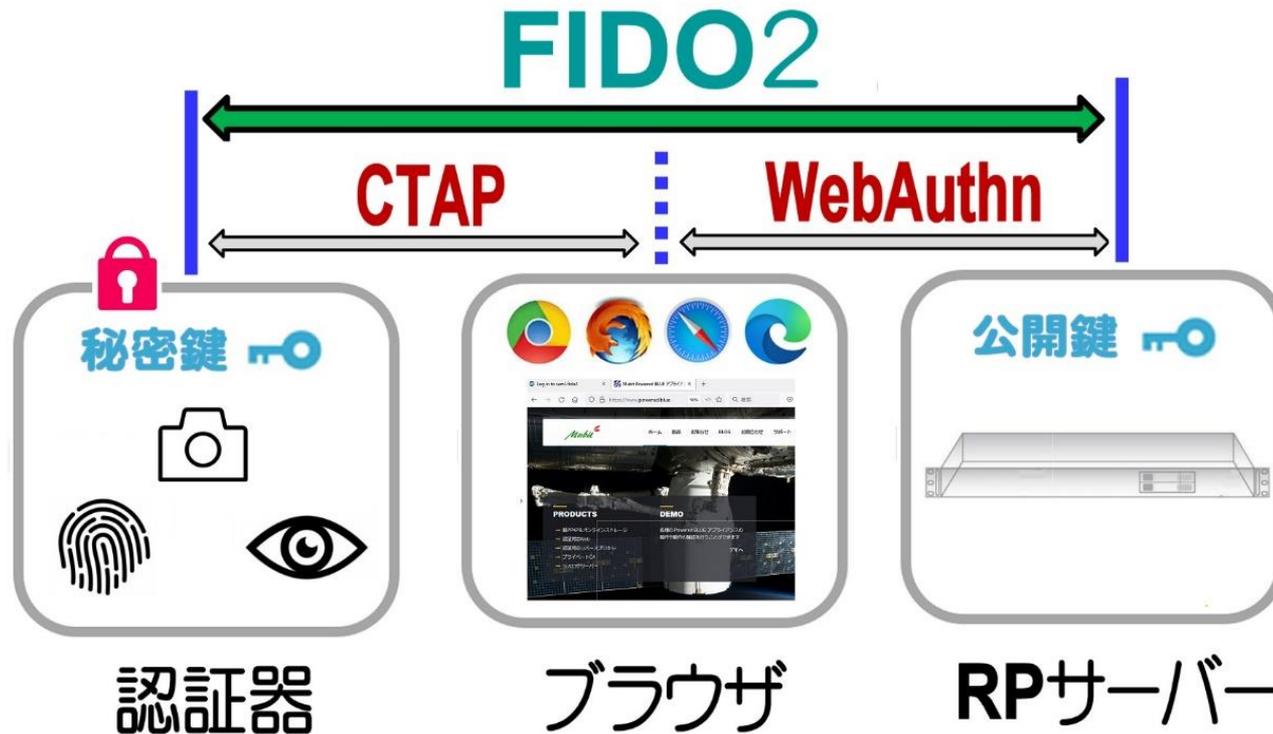
iOS



生体認証器 (USB)



生体情報の保護 FIDO2



 公開鍵暗号方式（公開鍵・秘密鍵）で通信

 生体情報は 外部へ漏洩しない

指紋認証や顔認証



生体認証 FIDO2対応 指紋認証器



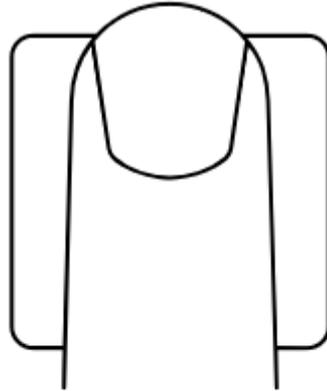
指紋登録方法-1

1) サインインオプション 2) セキュリティキーを選択

The screenshot shows the Windows Settings application. On the left is a navigation pane with 'サインイン オプション' (Sign-in options) selected and highlighted in red. The main content area is titled 'サインイン オプション' (Sign-in options) and 'デバイスへのサインイン方法の管理' (Manage sign-in methods for this device). Below this, there is a list of sign-in methods: Windows Hello 顔認証 (Windows Hello Face), Windows Hello 指紋認証 (Windows Hello Fingerprint), Windows Hello 暗証番号 (PIN) (Windows Hello PIN), **セキュリティキー** (Security key), パスワード (Password), and ピクチャ パスワード (Picture password). The 'セキュリティキー' option is highlighted with a red rectangular box. To its right, there is a '管理' (Manage) button. On the far right, there are links for '関連設定' (Related settings) and 'ロック画面' (Lock screen), and a section for '質問がありますか?' (Do you have a question?) with links to change passwords and troubleshoot PIN issues.

指紋登録手順

Windows Hello セットアップ



指紋センサーにタッチ

セットアップが完了するまで、デバイスの上にあるセンサーに指を当てて離す動作を繰り返してください。

キャンセル



指紋登録手順



生体認証 Webへのパスワードレス・アクセス

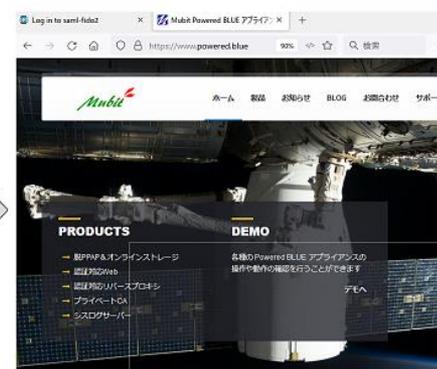
① iPhone / iPad / Android でのアクセス



① Webへアクセス

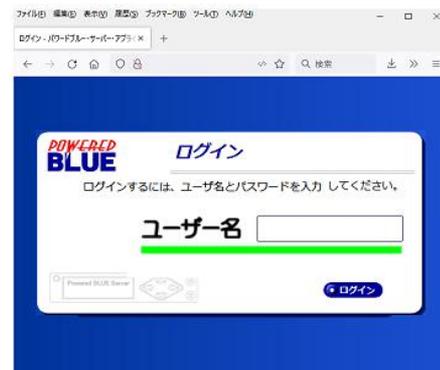
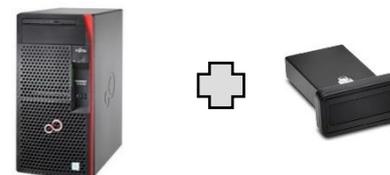


② キーにタッチ

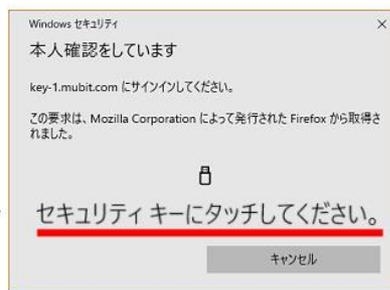


③ ターゲットWeb

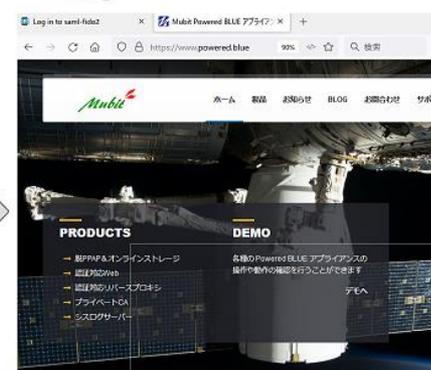
② パソコンでのアクセス



① Webへアクセス



② キーにタッチ



③ ターゲットWeb

Yahoo! かんたんログイン生体認証の案内メール

差出人 Yahoo! JAPAN <id-master@mail.yahoo.co.jp> ☆

件名 指紋・顔認証を利用してかんたんログイン Yahoo! JAPAN

宛先 .

一部のウェブメールサービスやメールソフトでは画像が表示されない場合がありますので、画像表示を設定のうえご覧ください。

おすすめ情報メール
2022年5月26日
こんにちは、*****さん

指紋・顔認証を利用して
**Yahoo! JAPANに
かんたんログイン**

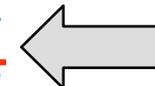
パソコンでも利用できます

パスワードや確認コードの入力不要
なりすまし防止でセキュリティ向上

設定する

- ・設定可能な端末は文末の※利用環境をご確認ください。
- ・複数の端末で利用したい場合は、端末ごとに設定が必要です。
- ・生体認証は端末上で行われるため、お客様の生体情報がYahoo! JAPANへ送信・保存されることはありません。

スマートフォンの設定はこちらもご利用いただけます。



2022/5/26 受信のメール

FIDO2



多要素認証は面倒

- 毎回のアクセスで

 - A) ID / Passwd + B) 他の認証

 - の入力が面倒

- 商用のサイトなどでのユーザー離脱を招く

リスクベース認証

1) 基本 ID/Passwd 認証

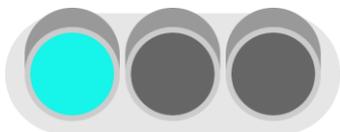
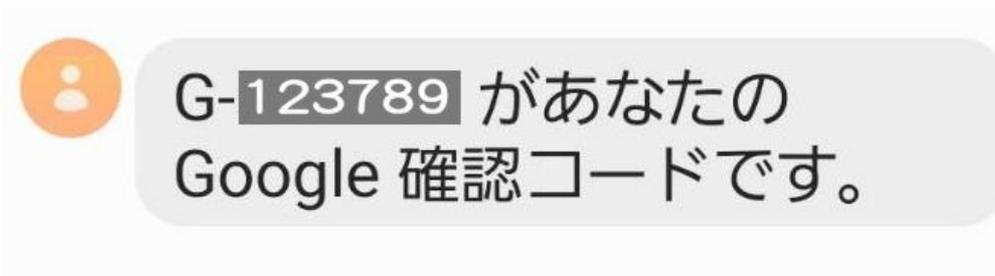
2) 追加の認証

従来のアクセスパターンと異なる

リスクベース認証 パラメータ

前回のアクセスとの比較	経過時間 各種情報
IP アドレス	社内 社外
位置情報	市内 県内 国内 国外
時間帯	平日日中 休日夜間
デバイス	スマートフォン PC タブレット
OSやブラウザ	種類 バージョン

SMS認証は安全か ？



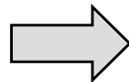
Google では SMS認証 は 使用可能



Salesforce では SMS認証 の 利用禁止

SIMスワップ

電話番号の変更が簡単



The screenshot shows a Google search results page for the query 'SIMスワップ'. The browser window title is 'SIMスワップ - Google 検索'. The search bar contains 'SIMスワップ'. The results show approximately 5,520,000 items found in 0.36 seconds. The top three results are:

- <https://eset-info.canon-its.jp/special/detail>
SIMスワップ攻撃を使って友人のWebサイトをハッキングして ...
2021/08/04 — この記事では、電話番号がいかに簡単に乗っ取られてしまうかを解説したい。なかでもSIMスワップ詐欺は後に続く犯罪行為のほんの序章に過ぎない。
- <https://eset-info.canon-its.jp/special/detail>
SIMスワップ詐欺の手口とその対策 - ESET
2021/02/09 — SIMスワップ詐欺は、別名「SIMハイジャック」や「SIM分割」とも呼ばれ、一種のアカウント乗っ取り詐欺として知られている。この攻撃を仕掛けるにあたり、 ...
- <https://ascii.jp/elem>
SIMスワップ詐欺」とはいったい何か - ASCII.jp
2021/02/09 — SIMスワップ詐欺は、別名「SIMハイジャック」や「SIM分割」とも呼ばれ、一種のアカウント乗っ取り詐欺として知られている。この攻撃を仕掛けるにあたり、 ...

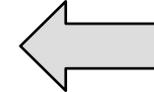
The bottom result is partially visible:

- <https://ascii.jp/elem>
SIMスワップ攻撃で電話番号は簡単に盗まれる - ASCII.jp
2021/08/04 — 結論から言うと、SIMスワップ攻撃を仕掛けるのは驚くほど容易で、攻撃者はあらゆるものが実行可能となるのだ。SIMスワッピングは、SIMハイジャック、 ...

Google SMS 非推奨へ



The screenshot shows a news article on the CNET Japan website. The title is 'グーグルの2段階認証、SMSからプロンプト方式への移行を推奨' (Google's 2-step authentication, SMS to prompt-based transition recommended). The article is dated July 18, 2017. Below the title is a navigation bar with various social media and utility icons like 'シェア 88', 'ツイート', 'B! 56', 'note', 'Pocket', '印刷', 'メール', '保存', and 'クラブ'.

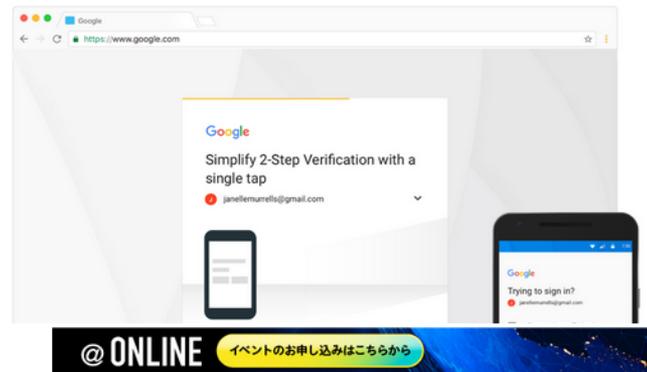


Googleが、SMSによる2段階認証から新しい認証方法への移行をユーザーに促す取り組みを今週より開始する。

米国立標準技術研究所（NIST）はSMSによる2段階認証を非推奨としている。その主な理由は、この認証方法が安全ではないからだ。攻撃者は、たとえば携帯電話事業者をだまして、SMSのメッセージを自分の携帯電話にリダイレクトさせられる。また、SMS経由で銀行からユーザーに送信されたコードを読み取る**悪質な「Android」アプリも数多く存在する。**

SMSの代わりに、GoogleがAndroidユーザーと「iOS」ユーザーに推奨しているのは、プロンプトを使った2段階認証だ。**Googleは2016年6月にこの機能を導入している。**この機能による認証がSMSによる認証より優れている点は、暗号化された接続を介して認証プロセスが実行されることにある。

Googleは今後、SMSによる2段階認証を使っているユーザーに対し、プロンプトによる認証への切り替えを求めるメッセージを表示する。馴染みのあるSMSによる認証のサポートが終了するわけではないが、**最終的にはそうなる可能性がある**とGoogleは示唆している。



画像認証 CAPTCHAは有効？

山や丘
の画像をすべて選択してください。



   **確認**

ログイン

メールアドレス

パスワード

パスワードをお忘れですか？
ログインにお困りですか？

私はロボットではありません



reCAPTCHA
プライバシー - 利用規約

メールアドレスでログイン

または

Appleでログイン

すでにメールアドレスで登録されており、且つそのメールアドレスとAppleにご登録のメールアドレスが異なる場合、新しく別のアカウントが作成されます。

Facebookログイン機能廃止のお知らせ

リスクベース認証 多要素認証の組合せポイント

認証メソッド	特徴
ID/パスワード認証	基本
●SMS認証	SIMスワップで電話番号を変更&不正取得
●ワンタイムパスワード認証	無償のソフトウェアトークンが利用できる メール通知でのワンタイムパスワード認証も可能
●画像認証	本人確認ではない（人間が操作しているかの判別）
●SSLクライアント認証	SSLクライアント証明書の端末を認証
●FIDO2 生体認証	第三者が複製しにくい

1) 基本 ID/Passwd 認証



ユーザー名 user-name

パスワード ●●●●●●●●

ログイン

2) 追加の認証

ワンタイムパスワード メール通知



リスクベース認証の導入を検討したい

お問い合わせ

お問い合わせ

購入先

お問い合わせ

お問い合わせ

お問い合わせフォーム

下記のフォームにご記入後、下のボタンを押してください。

会社名
(会社または組織名。個人の方は省略可)

ご担当者

ご連絡先 郵便番号:

ご住所

https://www.mubit.co.jp/sub/contact/call.html



Webサイト

<https://www.mubit.co.jp/sub/contact/call.html>