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

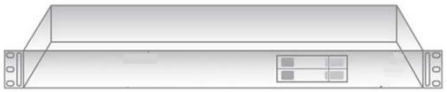
設立　　1995年12月8日

所在地　　東京都北区王子1−28−6

主な製品　　Powered BLUE シリーズ

アプライアンスサーバー（Linux）

ソフトウエア開発



ダークWeb

ダークWeb / データやアクセス権の売買

■「ランサムウエア」月120ドルから

真相深層

サイバー攻撃 闇市場拡大

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エア、標的となる組織に不正アクセスできる権利などが売り出され、競争が新たな商品を生み出していく。技術がなくても「武器」の調達が可能になり、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エア」。1カ月で120ドル、6カ月で490ドル、12カ月で900ドル――。

サブスク利用も

キヤノンマーケティングジャパンが確認したランサムウエアの販売サイトでは、サブスクリプション（定額課金）の利用プランが設けられ、最も高額なプランでは感染を容易にする追加機能も付くとされていた。

ランサムウエアは今年だけで既に3回バージョンアップされ、使い方は「よくある質問」に答える形で説明。検出を免れるウイルス対策ソフトの一覧も載せていた。

同社の西浦真一セキュリティエバンジェリストは「セールスポイントやATMから銀行のネットワークに侵入するマルウエア（悪意のあるアプリやプログラム）は2千ドルで売り出されていた。偽サイトへの誘導などに使うショートメッセージサービス（SMS）の配信を5千件350ドルで請け負うとの書き込みもあった。

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ドル
米有力企業へのアクセス権	1万ドル
ATM用のマルウエア	2000ドル～
ランサムウエアのサービス	年間900ドル
スパムSMSの送信サービス	25～500ドル
SMS送信用のソフトウエア	499ドル～

（出所）トレンドマイクロ

匿名性の高い闇サイト群「ダークウェブ」では以前から、流出したクレジットカード情報やSNS（交流サイト）アカウントが流通しており、近年、取引の対象は一段と多様化している。

トレンドマイクロによると「日本の医療系大学のネットワークに侵入するアクセス権」は999ドル、ATMから銀行のネットワークに侵入するマルウエア（悪意のあるアプリやプログラム）は2千ドルで売り出されていた。偽サイトへの誘導などに使うショートメッセージサービス（SMS）の配信を5千件350ドルで請け負うとの書き込みもあった。

売り手で競争、脅威増す

キヤノンマーケティングジャパンが確認したランサムウエアの販売サイト＝同社提供

セキュリティー関係者によると、国内38社などから漏洩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エア販売や代行サービスは「CaaS（クライム・アズ・サービス）」とも呼ばれる。CaaSを利用することで「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っている」と、トレンドマイクロの岡本勝之セキュリティエバンジェリストは警鐘を鳴らす。

売り手としては、自ら標的を探して攻撃を仕掛けなくても、得意分野の技術を生かして効率的にマルウエアを提供し、攻撃で得た収益の一定割合を成功報酬として受け取るケースもある。

機能の劣るマルウエアは市場で淘汰され、攻撃が成功しやすいほど価格は上がる。

ロシアのウイルス対策ソフト開発会社「ドクターウェブ」のボリス・シャロフ最高経営責任者（CEO）は「売り手が競い合うことでマルウエアなどの攻撃力が高まる構図になっている」と指摘する。ランサムウエアで暗号化されたデータの復旧サービスでも「数年前と比べ、データを復元できないケースが増えている」と、トレンドマイクロの岡本勝之セキュリティエバンジェリストは警鐘を鳴らす。

歯止め難しく

売り手としては、自ら標的を探して攻撃を仕掛けなくても、得意分野の技術を生かして効率的にマルウエアを提供し、攻撃で得た収益の一定割合を成功報酬として受け取るケースもある。

機能の劣るマルウエアは市場で淘汰され、攻撃が成功しやすいほど価格は上がる。

ロシアのウイルス対策ソフト開発会社「ドクターウェブ」のボリス・シャロフ最高経営責任者（CEO）は「売り手が競い合うことでマルウエアなどの攻撃力が高まる構図になっている」と指摘する。ランサムウエアで暗号化されたデータの復旧サービスでも「数年前と比べ、データを復元できないケースが増えている」（柏木凌真）

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」とセキュリティー会社スプラウトの高野聖玄社長は指摘する。「サイバー攻撃や闇市場に国境はない。国際的な捜査連携や捜査手法の見直しによって抑止力を高めていくことが必要だ」と話している。（柏木凌真）

- 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
- ランサムウエアのサービス
  900ドル

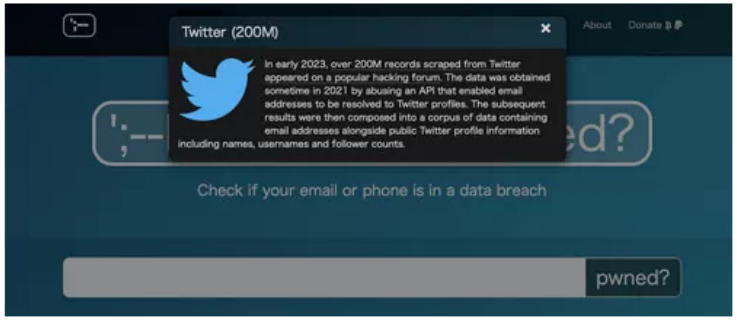
2020/9/5 日本経済新聞

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

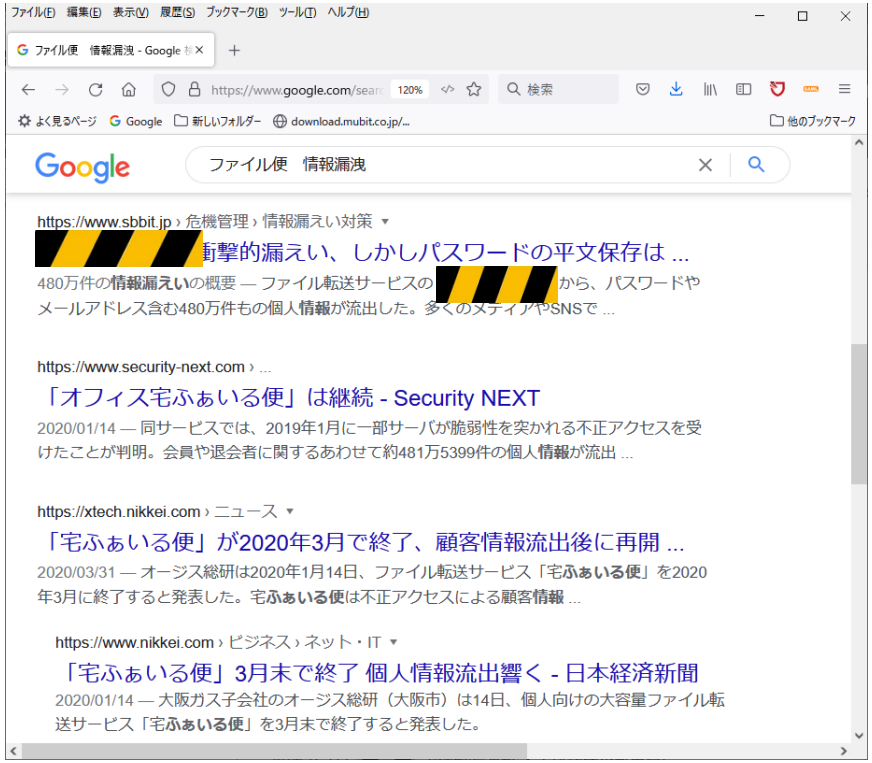
Twitterユーザーの個人情報だという2億件以上のデータが何者かによってオンラインフォーラムで公開された。過去のTwitterのセキュリティ問題から、「Have I been Pwned」など漏洩情報をまとめているサービスはTwitterからの漏洩データである可能性が高いと判断して投稿されたデータをシステムに追加。影響を受ける人々に注意を喚起している。



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

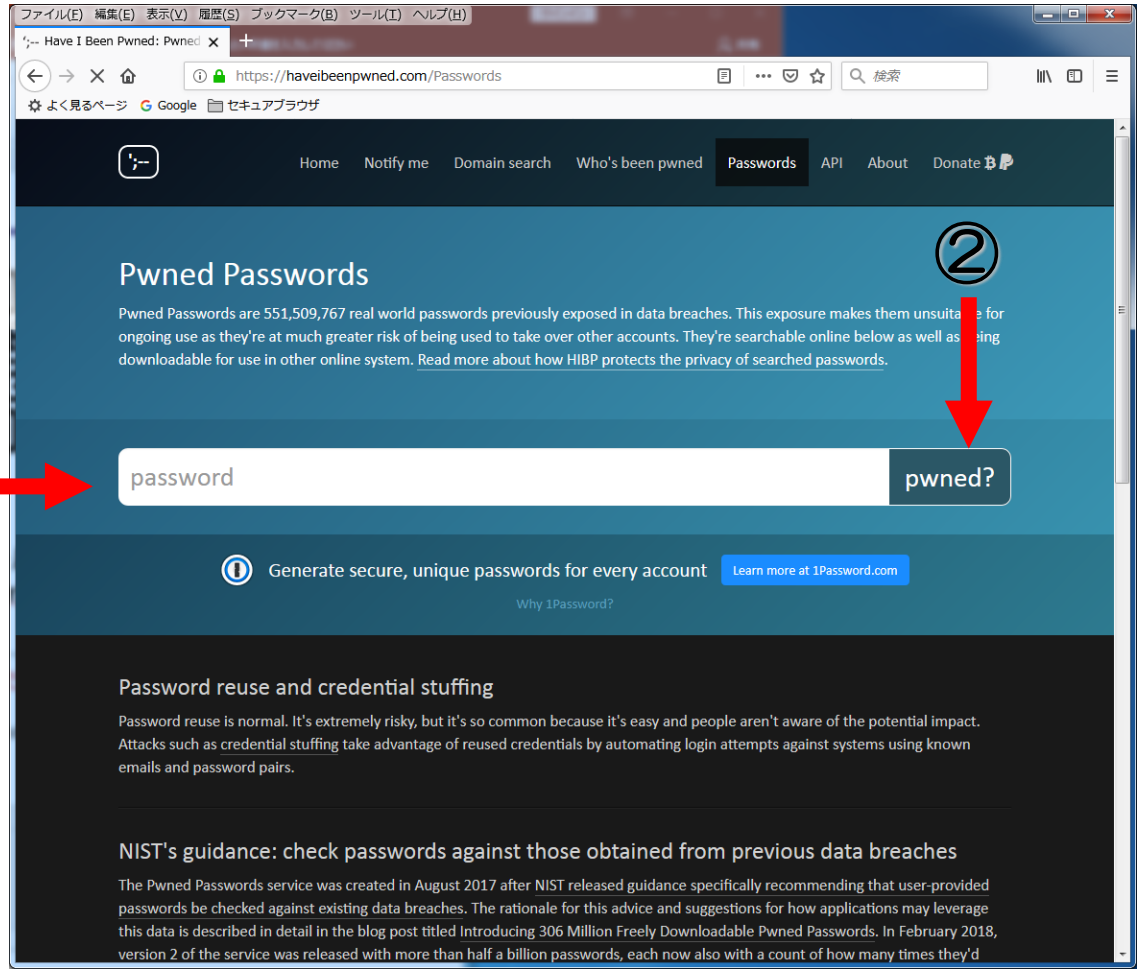
ID　　メールアドレス

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カウント流出チェックサイト

https://haveibeenpwned.com/

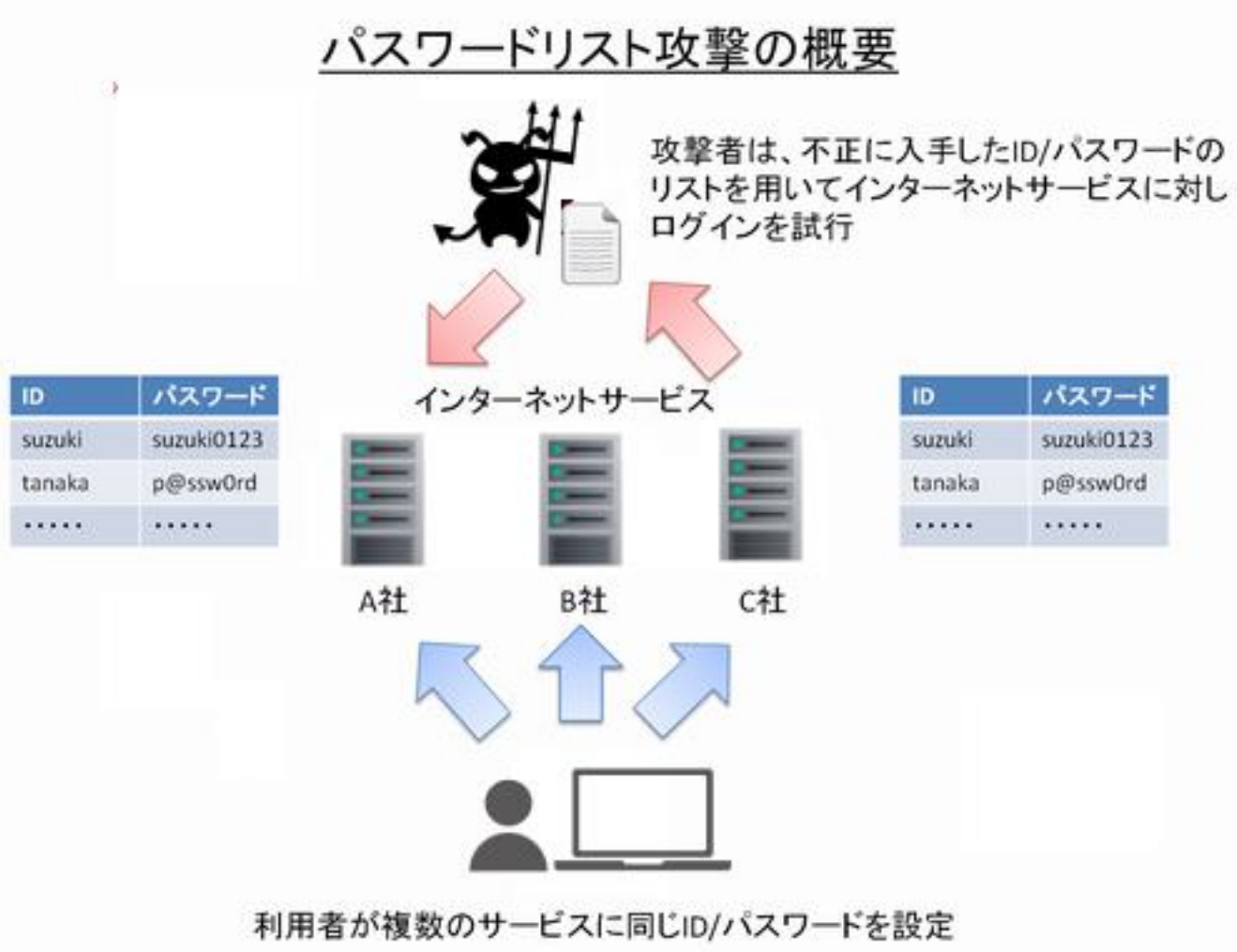


① パスワードを入力
② pwned？　を押す

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

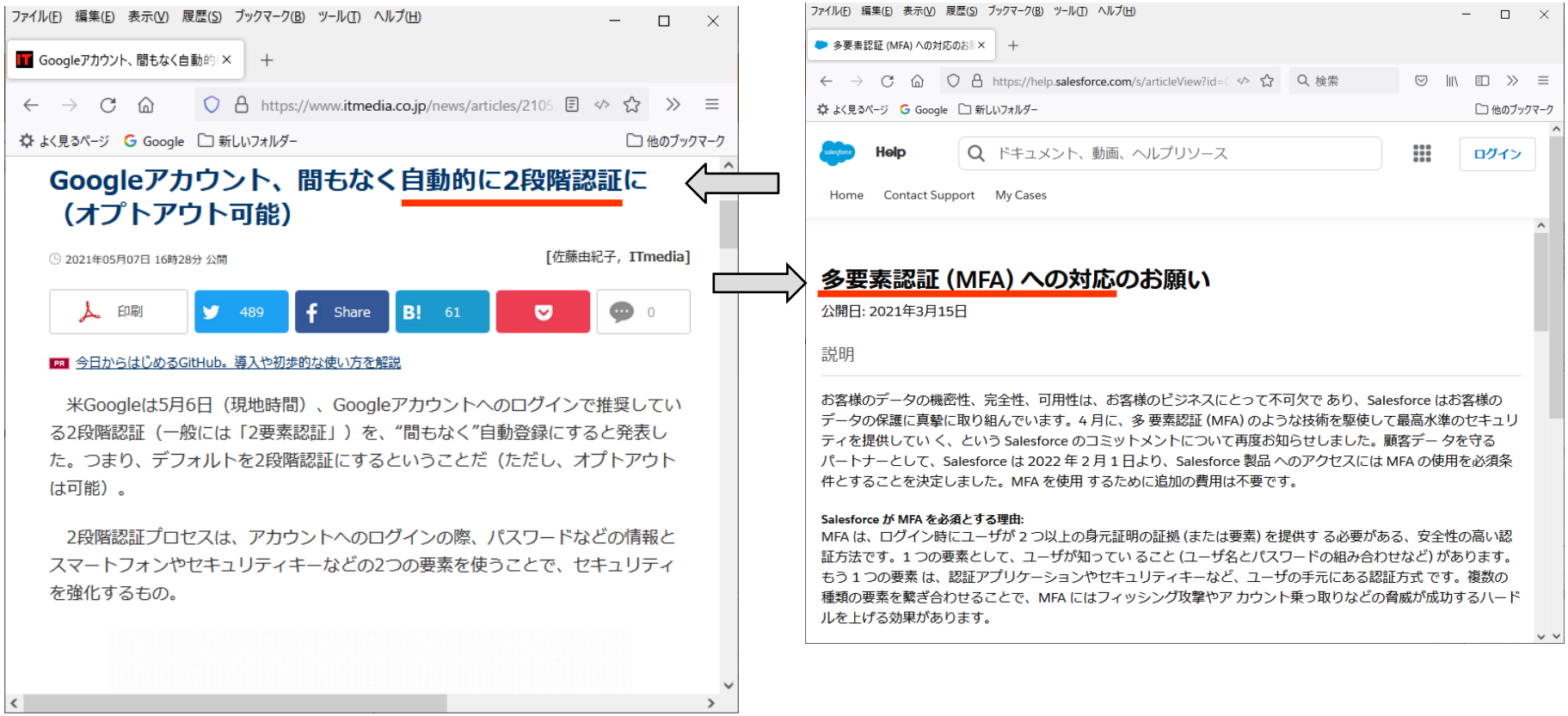
多要素認証が必要とされる背景

- 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/Passwｄ 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

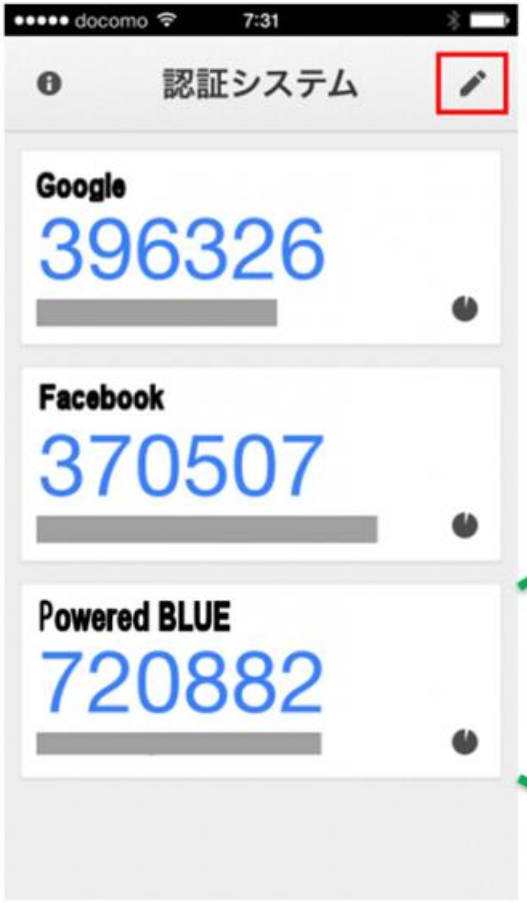
認証メソッド	特徴
ID/パスワード認証	パスワードの使いまわし　漏洩している可能性あり
SMS認証	送信ごとに課金される（運用者側） エリア外だと受信できない アクセス毎にワンタイムパスワードの入力が必要
ワンタイムパスワード認証	無償のソフトウエアトークンが利用できる アクセス毎にワンタイムパスワードの入力が必要
画像認証	指定の画像を選択させる
SSLクライアント認証	SSLクライアント証明書を配布する必要がある
生体認証	認証器を用意する必要がある

SMS認証　スマートフォンの番号に通知

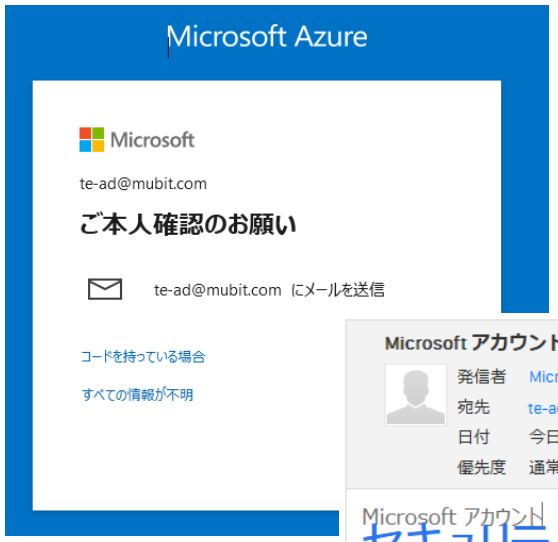
G-123789 があなたの
Google 確認コードです。

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いでください。
@login.yahoo.co.jp #615716

ワンタイムパスワード認証　ソフトウエア・トークン

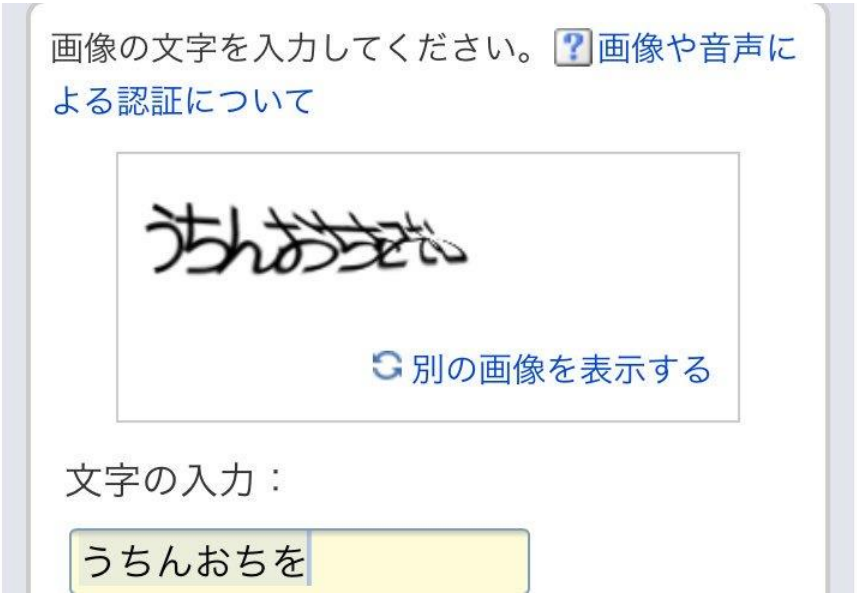


ワンタイムパスワード認証　メール通知の例



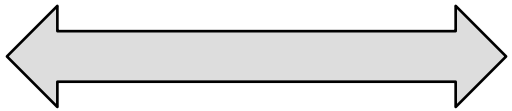
画像認証

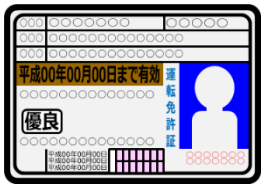

山や丘
の画像をすべて選択してください。
確認


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
別の画像を表示する
文字の入力：
うちんおちを

SSLクライアント認証

■ 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

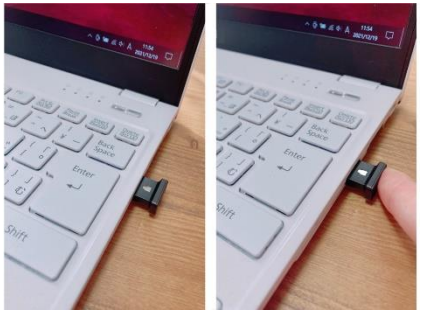



ブラウザ

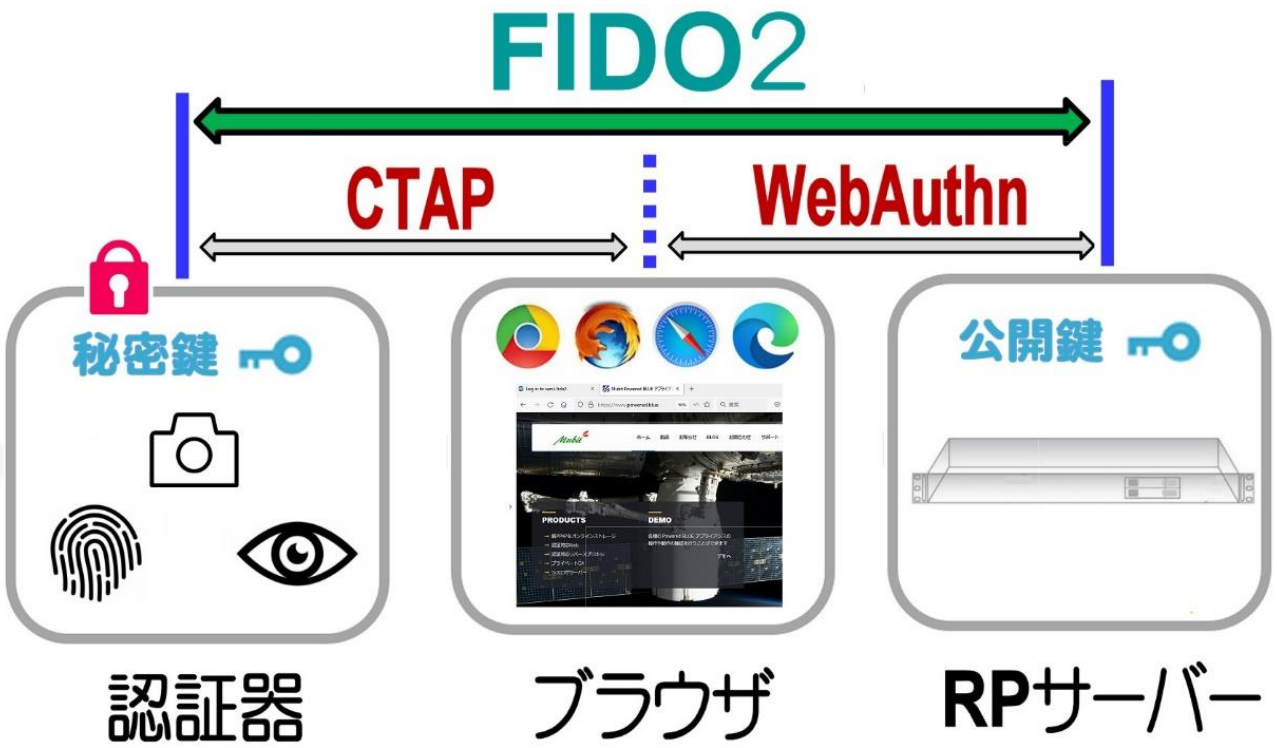
iOS

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

生体認証　FIDO2 対応　スマートフォン

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

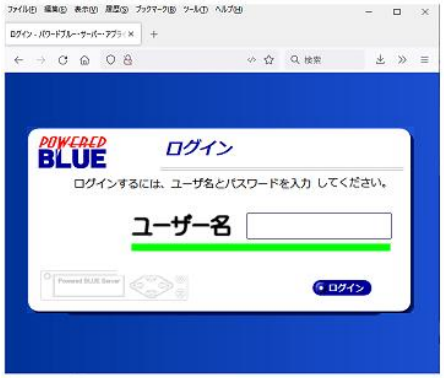
指紋登録手順


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、デバイスの上部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

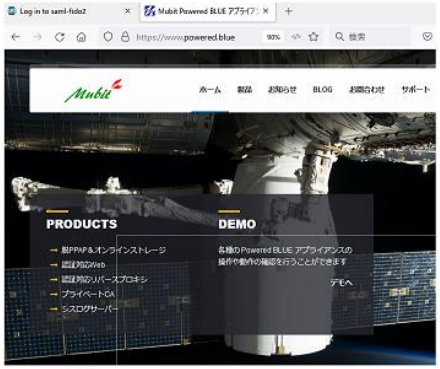
生体認証　Webへのパスワードレス・アクセス

①　iPhone / iPad / Android でのアクセス



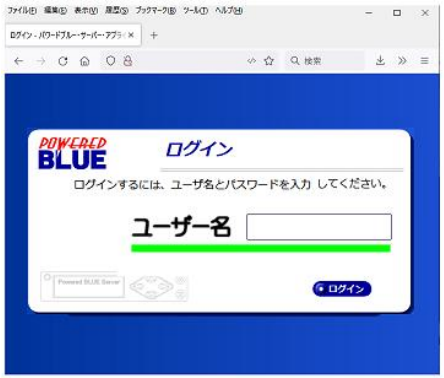
① Web へ アクセス

② キーにタッチ



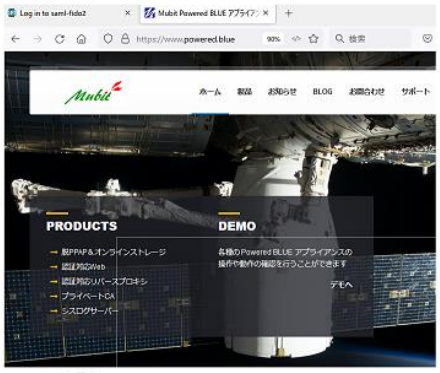
③ ターゲットWeb

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

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

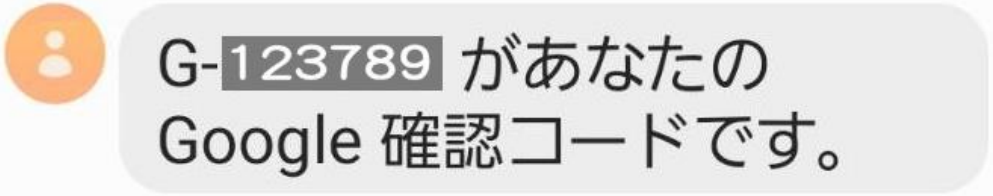
２）追加の認証

　　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　？

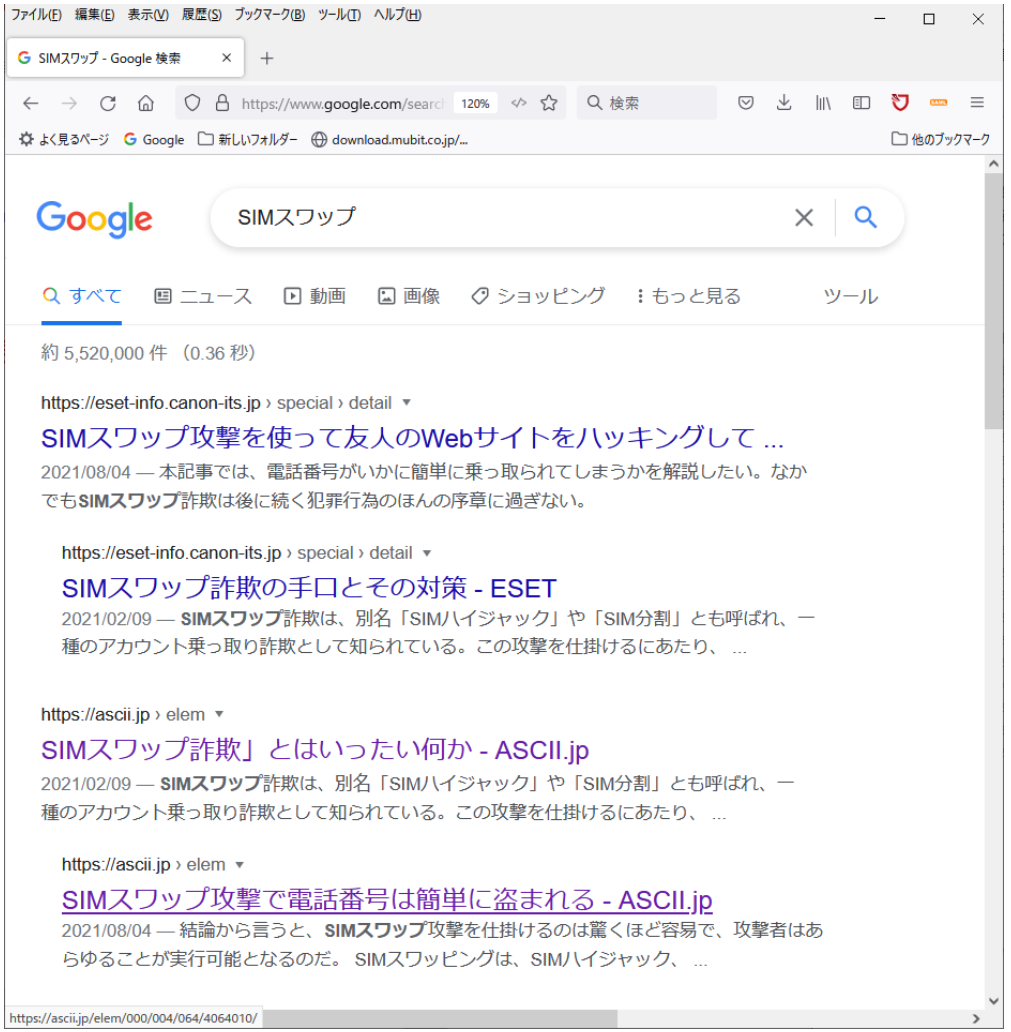


Google では　SMS認証 は 使用可能

Salesforce では　SMS認証 の 利用禁止

SIMスワップ

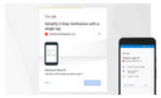
電話番号の変更が簡単



Google SMS　非推奨へ

c|net Japan　search　CNET ID

NET Japan ＞ ニュース ＞ 製品・サービス



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

am Tung （CNET News） 翻訳校正： 佐藤卓 吉武稔夫 （ガリレオ） 2017年07月18日 11時01分

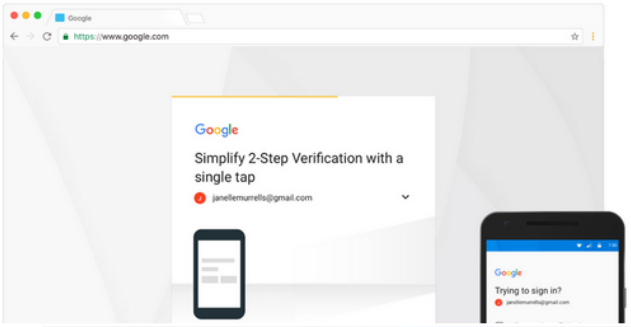
シェア 88　ツイート　一覧　B! 56　note　Pocket　89　印刷　メール　保存　クリップ

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による認証よりも優れている点は、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　CAPTCH は 有効？

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	無償のソフトウエ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

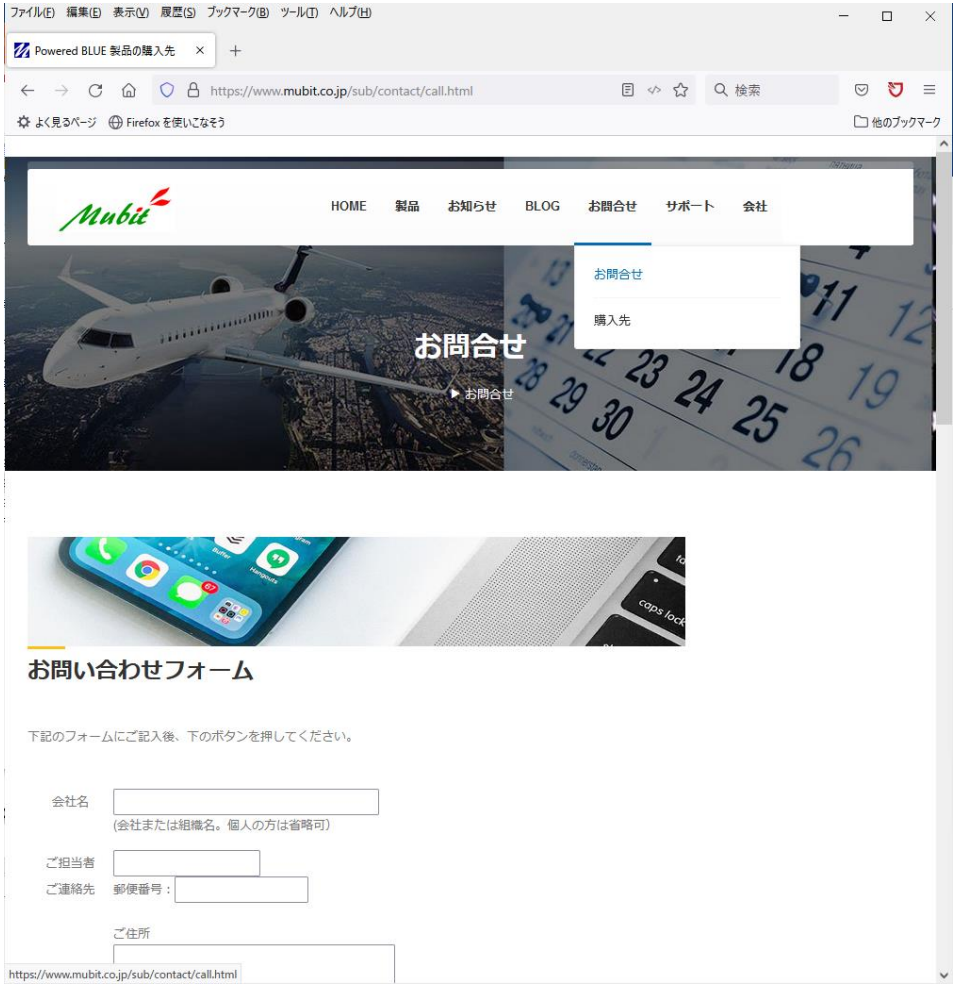
リスクベース認証　運用パターン

1）基本　ID/Passwd 認証

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



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