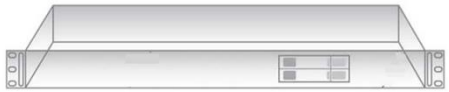
Webサイトへの多要素認証の導入方法 / FIDO2生体認証の仕組みと使い方

～　改修不要で既存Webを「生体認証」に対応させる方法も紹介　～

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



POWERED BLUE

ダークWeb

ダークWeb / データやアクセス権の売買

- 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

某　ファイル交換サイト　480万件ID漏洩

2019年1月

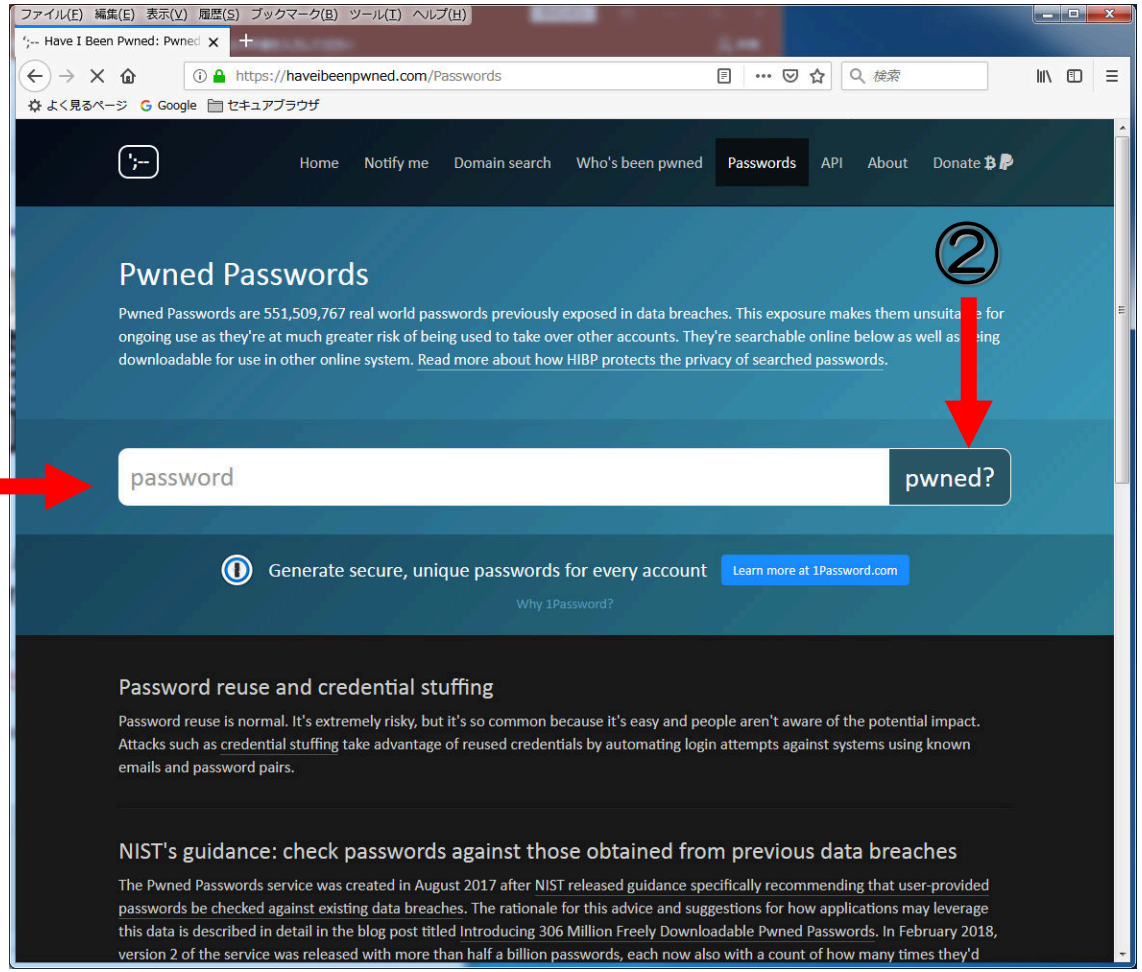
ID　　メールアドレス

Passwd　生のパスワード

生年月日・性別・職業 …

パスワード流出チェックサイト

https://haveibeenpwned.com/



①

② pwned？　を押す

① パスワードを入力

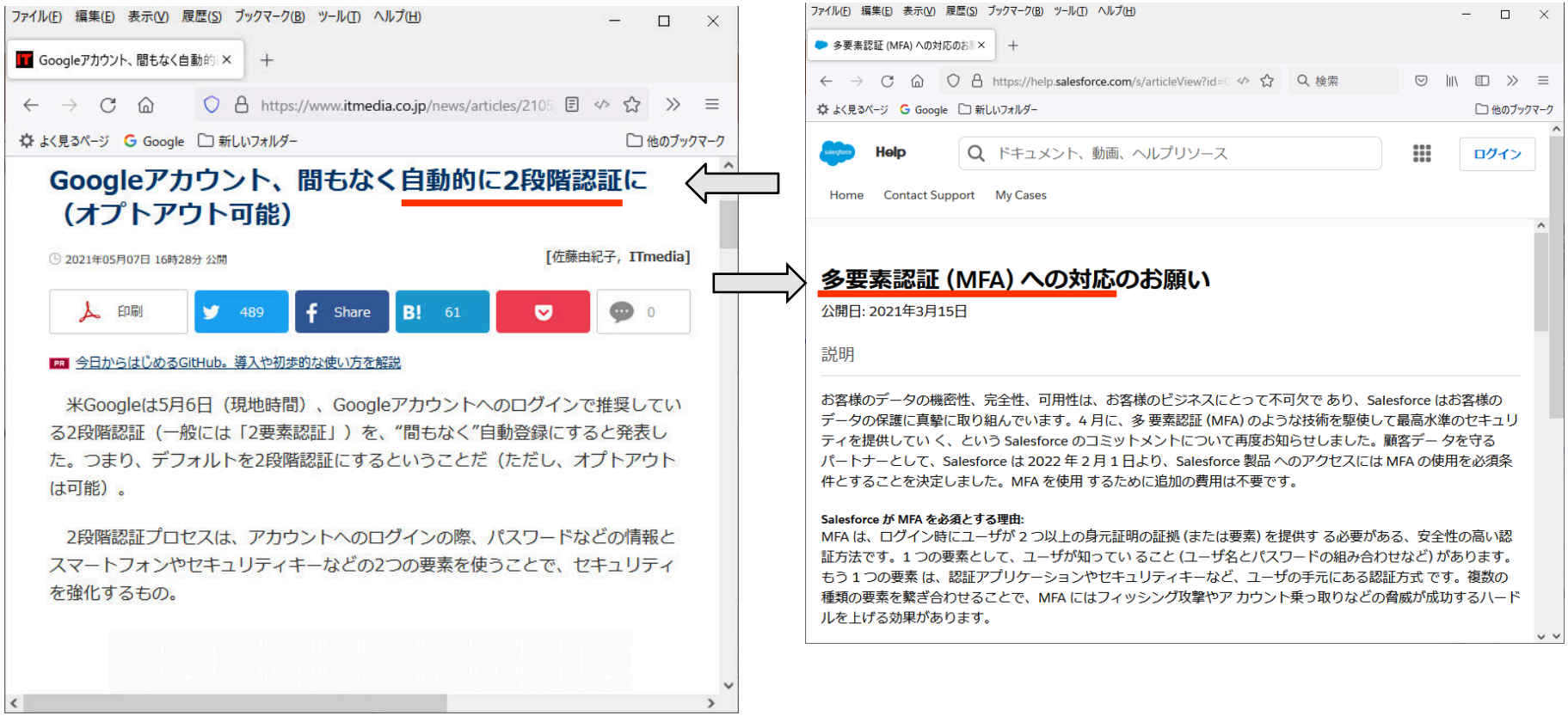
Oh no --- pwned !
残念でした

Good news — no pwnage found!
大丈夫

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



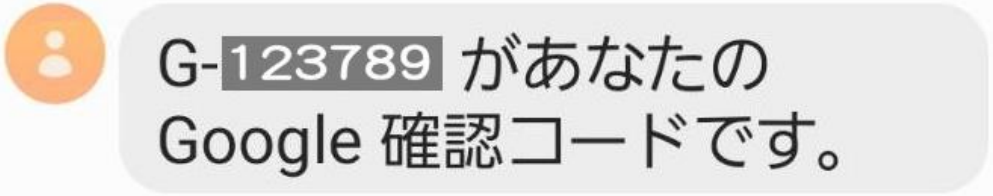
- Google社は
  「Googleアカウントの二要素認証を自動的に有効化」

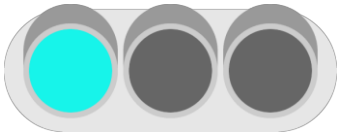
- SalesforceはMFAの必須化

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
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　？



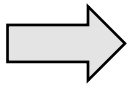


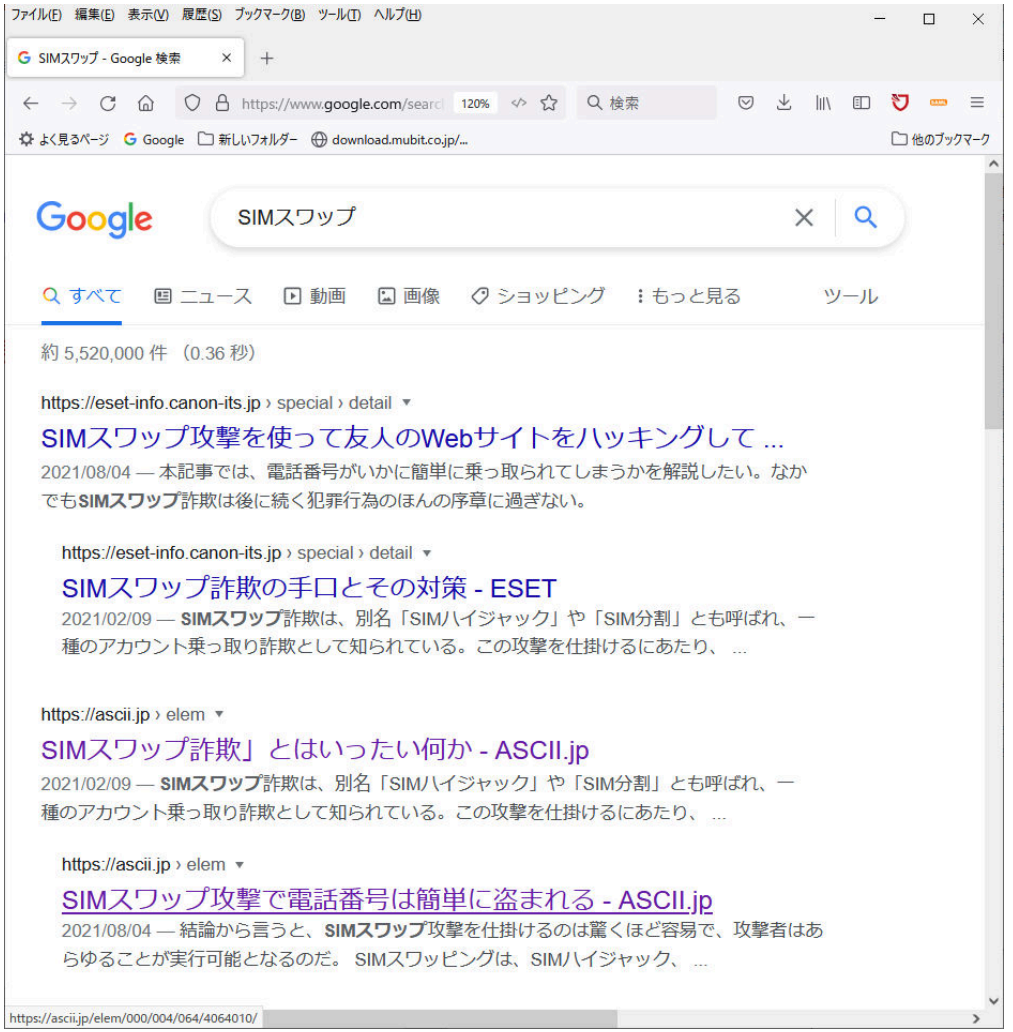
Google では　SMS認証 は 使用可能

Salesforce では　SMS認証 の 利用禁止

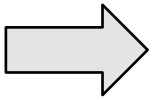
SIMスワップ

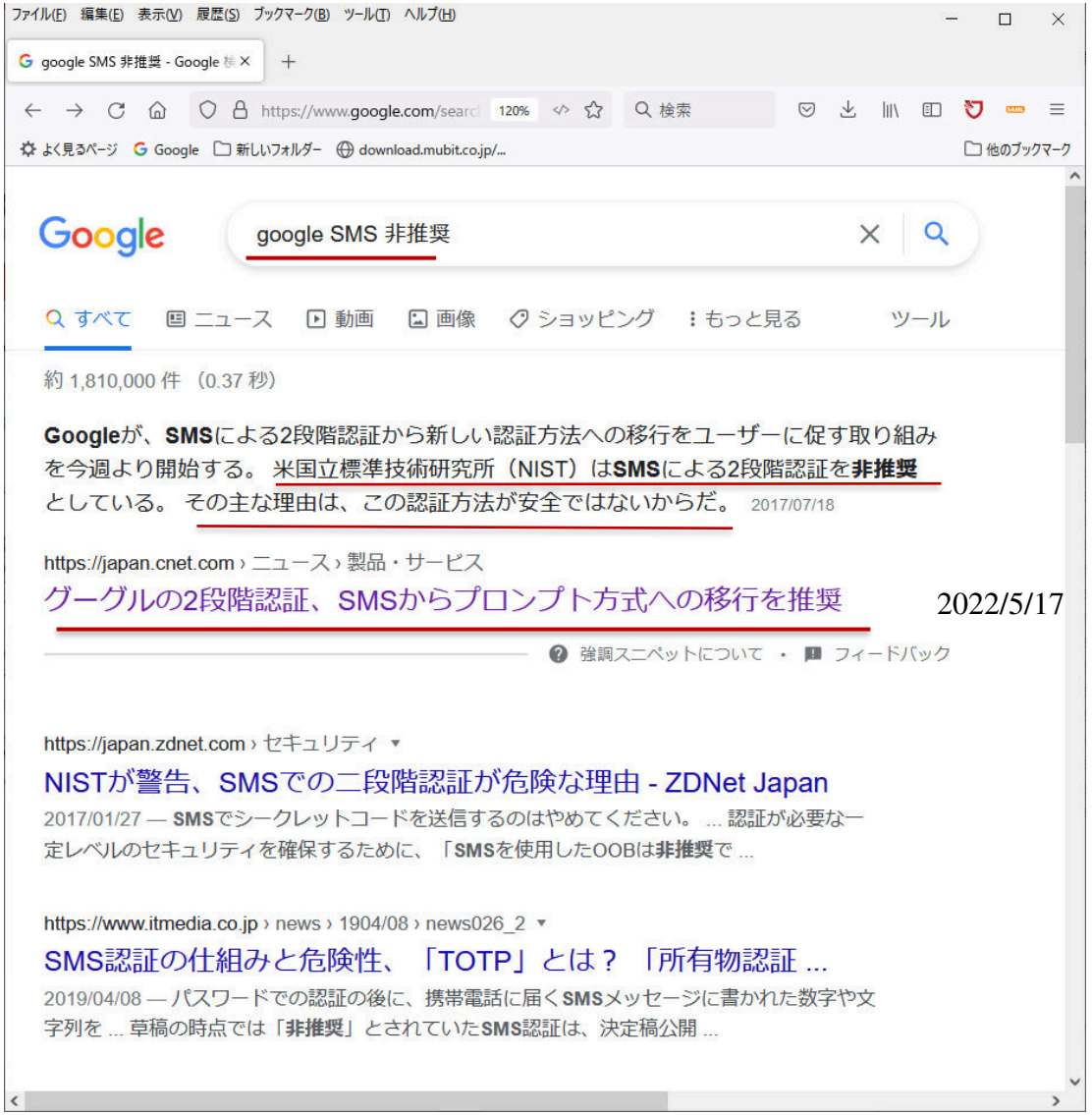
電話番号の変更が簡単





Google SMS 非推奨へ





2022/5/17 CNET Japan

生体認証とは

- 指紋認証
- 静脈認証
- 顔認証
- 虹彩認証

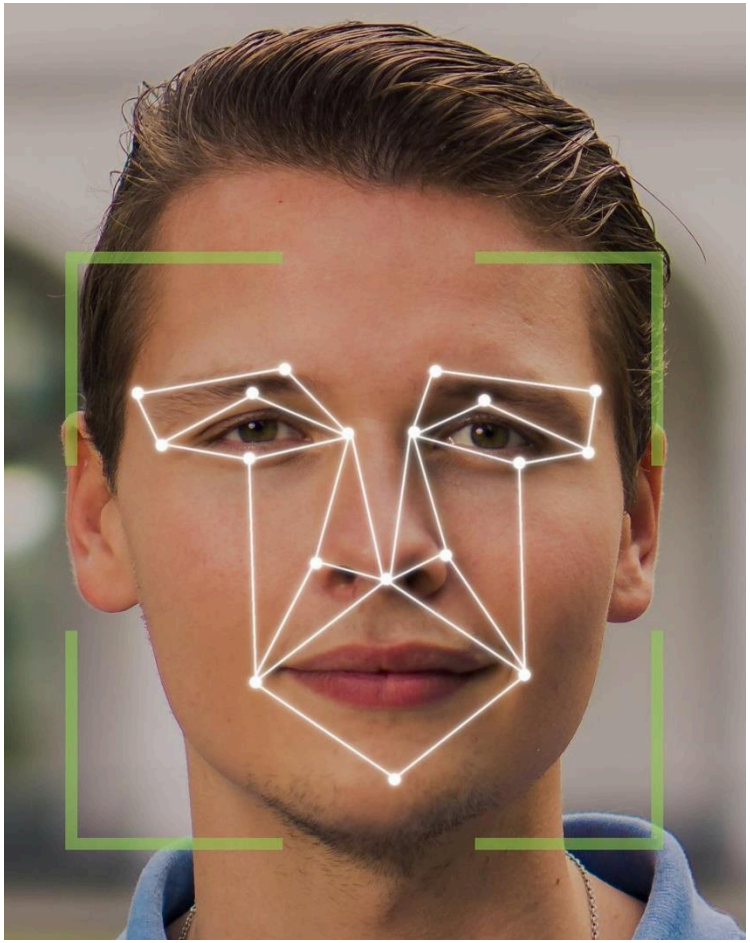
- 利用者が保有する生体「固有の情報」を利用
- 生体固有の情報は「複製が出来にくい」 ことを利用

ユーザ自身の特徴（生体情報）

認証メソッド	特徴
指紋認証	スマートフォンなどのロック解除での利用 10本の指が利用できる
顔認証	スマートフォンなどのロック解除での利用 チケットの転売防止での利用 顔は一つ
虹彩認証、網膜認証	ユーザの目の虹彩または網膜により認証する。 目は2つ
静脈認証	ユーザの指や手の静脈により認証する ATMなどで利用 登録できる静脈のポイントは複数

生体認証の判定基準

顔の目、鼻、口などの **特徴点** の位置や顔領域の位置や大きさをもとに照合



ユーザ自身の特徴（生体情報）

認証メソッド	価格	認証精度	不変性	備考
指紋認証	◎	○	◎	接触 機器の種類が豊富 指紋認証が困難な場合
顔認証	○	○	○	非接触 マスクでの認証
虹彩認証、網膜認証	△	○	◎	非接触 機器の選択肢が少ない
静脈認証	△	◎	◎	非接触 機器の選択肢が少ない

FIDO2（ファイド）/ Windows HELLO　/ eKYC

項目	特徴	生体データ保管先
FIDO2	FIDO アライアンスが標準化している Webアクセス時の生体認証の標準規格。	利用者側の端末内
Windows HELLO	Windows 10 / 11 への ログイン時の生体認証	利用者側の端末内
eKYC	オンライン経由での本人確認 免許証、パスポート、マイナンバーカードを写真撮影 本人の顔写真をアップロード	サービスの利用先

⇨ 生体データの 保管先 は 重要 です

FIDO（ファイド）アライアンス

- 2012年　FIDOアライアンス設立

  Paypal / Lenovo など参加

  パスワードのわずらわしさを解消することを
  目的として設立

- 2018年　FIDO2の規格

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

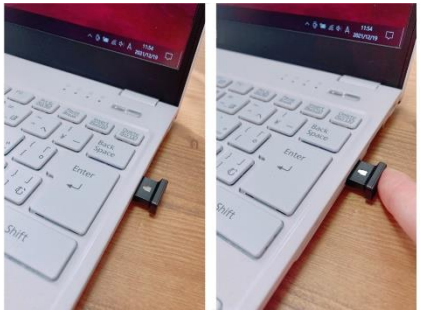



ブラウザ

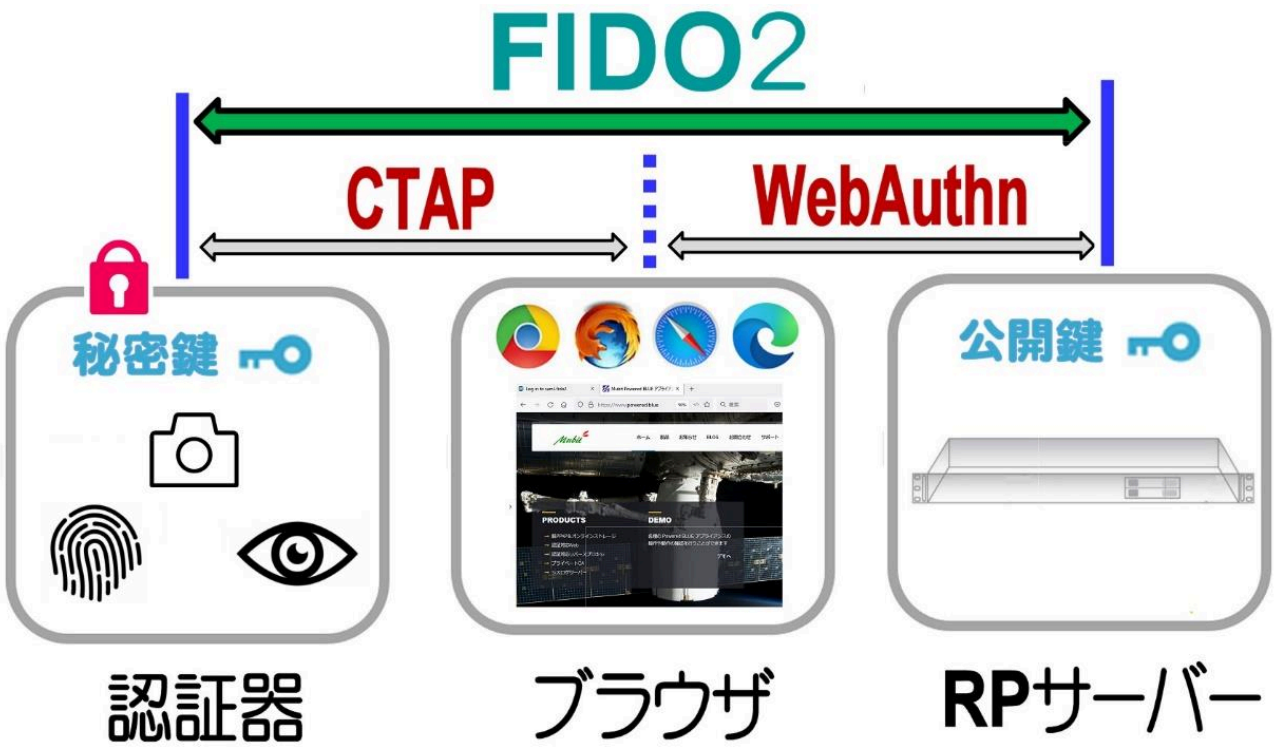
iOS

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

Yahoo サービスへのログイン　FIDO2対応

2021/12/9

2022/2/8

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

FIDO2/生体認証の特徴

パスワードレス認証

パスワードを覚える必要がない

パスワードの使いまわし・パスワードの定期的な変更　からの解放

なりすまし防止

生体情報は偽造しにくい
第3者がユーザー側の「認証器」を利用しても認証されません

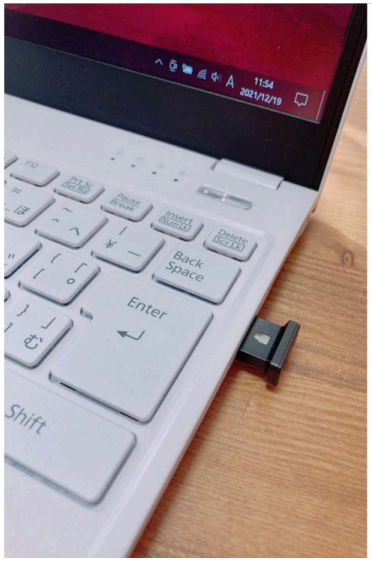
生体情報の漏洩防止

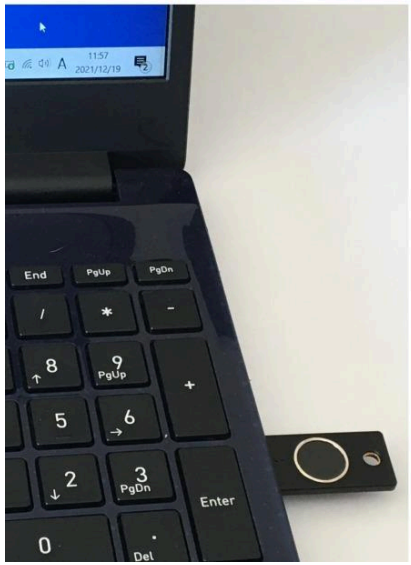
生体情報はユーザー側の「認証器」内に保護

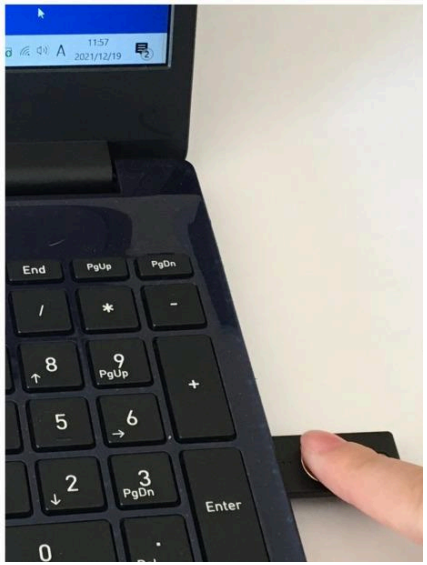
FIDO2 対応　スマートフォン・ユーザー

指紋認証や顔認証の登録方法

FIDO2 対応　指紋認証器　PCユーザー







指紋認証とは

- 10本の指が登録でき、どの指でも認証ができる
- 認証精度が安定
- 認証器が豊富
- USBタイプはPCへの接続が簡単
- 汎用のPCで利用できる
- Windows10 / 11 の標準機能で指紋登録ができる

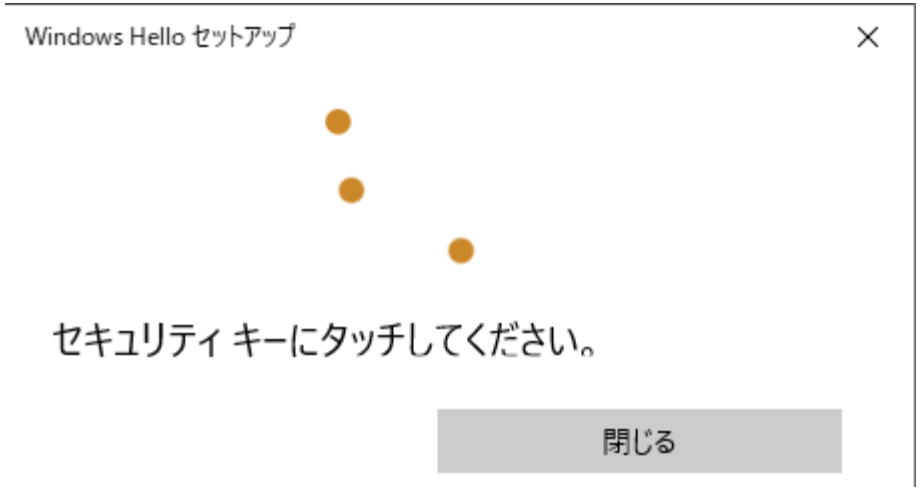
Windows 10 / 11　指紋登録手順

Windows 10 / 11　指紋登録手順

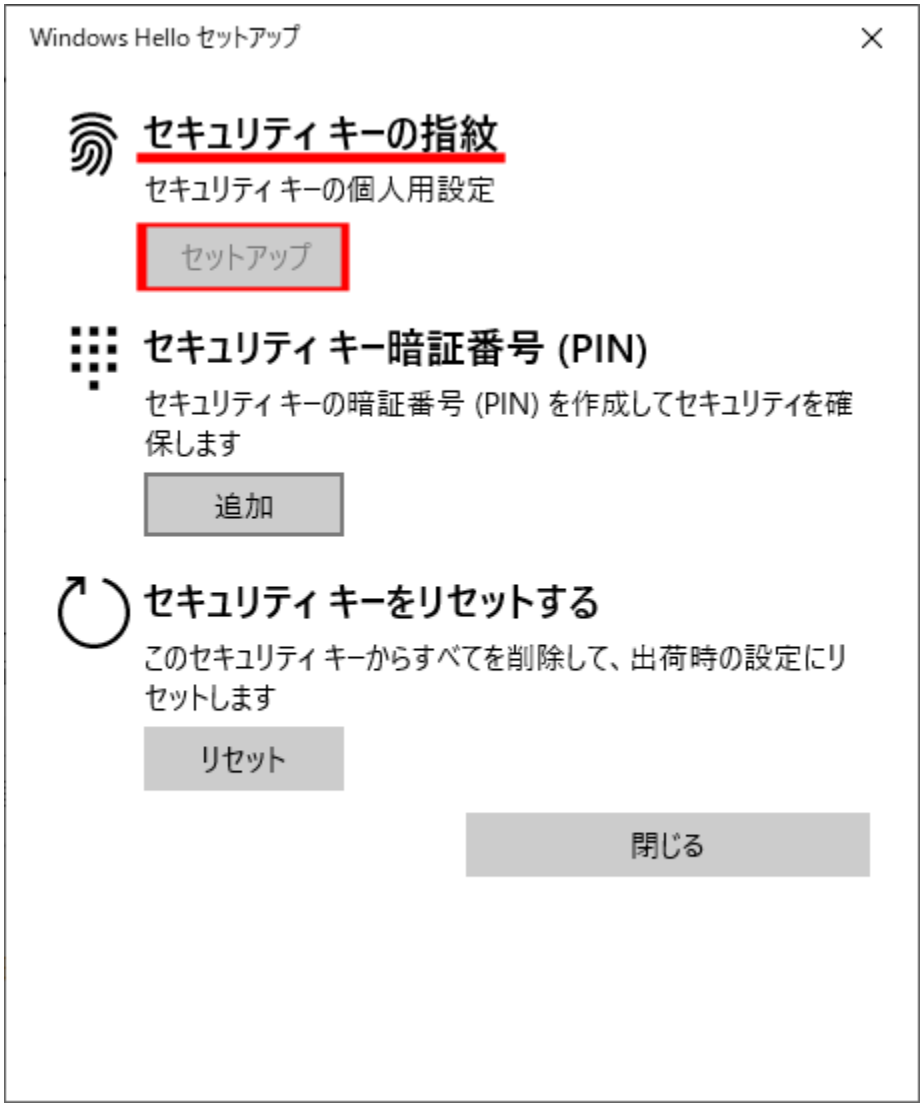
指紋登録手順


設定
ホーム
設定の検索
アカウント
ユーザーの情報
メールとアカウント
サインイン オプション
職場または学校にアクセスする
家族とその他のユーザー
設定の同期
サインイン オプション
デバイスへのサインイン方法の管理
追加、変更、削除するサインイン オプションを選択します。
Windows Hello 顔認証
カメラを使ってサインインする (推奨)
Windows Hello 指紋認証
このオプションは現在使用できません (詳細を表示するにはクリックしてください)
Windows Hello 暗証番号 (PIN)
暗証番号 (PIN) を使ってサインインする (推奨)
セキュリティ キー
物理的なセキュリティ キーを使ってサインインする
アプリケーションにログインするための物理的なセキュリティ キーを管理します。
詳細情報
管理
パスワード
アカウントのパスワードを使ってサインインする
ピクチャ パスワード
お気に入りの写真をスワイプしてタップし、デバイスのロックを解除する
サインインを求める
しばらく操作しなかった場合に、もう一度 Windows へのサインインを求めるタイミング
関連設定
ロック画面
質問がありますか?
Microsoft アカウントのパスワードを変更する
ローカル アカウントのパスワードのリセット
Windows Helloのセットアップ
PIN の問題の修正
ヘルプを表示
フィードバックの送信

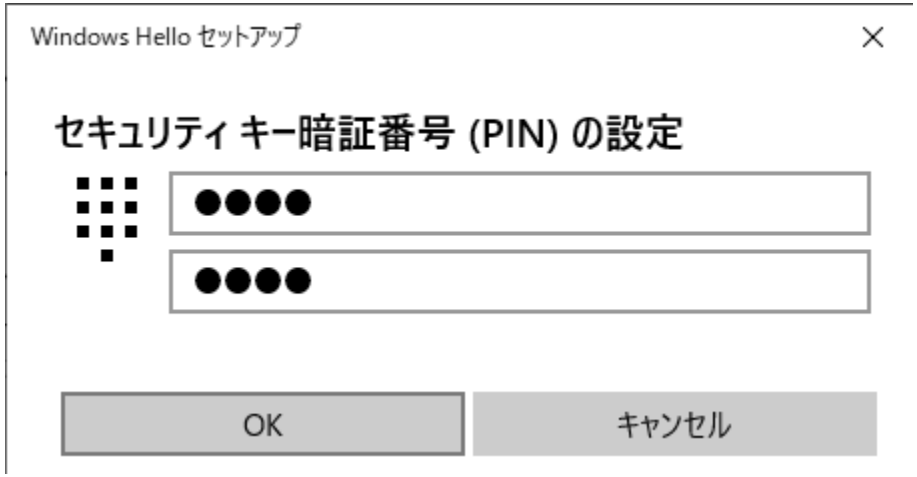
指紋登録手順



指紋登録手順


Windows Hello セットアップ
セキュリティ キーの指紋
セキュリティ キーの個人用設定
セットアップ
セキュリティ キー暗証番号 (PIN)
セキュリティ キーの暗証番号 (PIN) を作成してセキュリティを確保します
追加
セキュリティ キーをリセットする
このセキュリティ キーからすべてを削除して、出荷時の設定にリセットします
リセット
閉じる

指紋登録手順

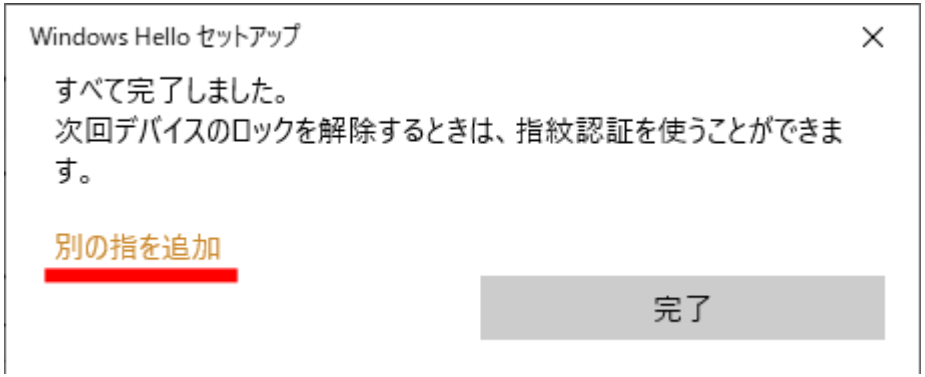


指紋登録手順


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

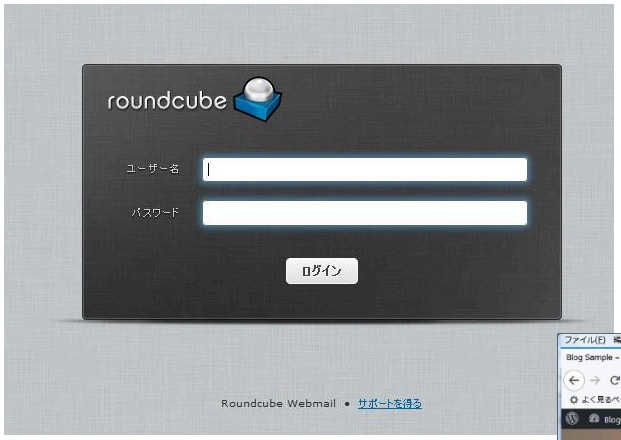
指紋登録手順

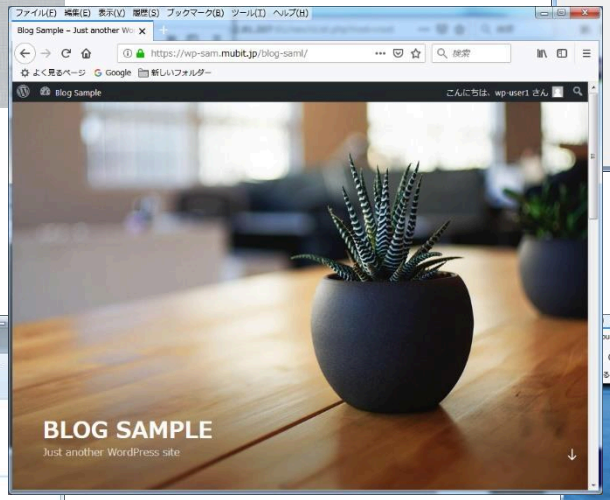
指紋登録手順

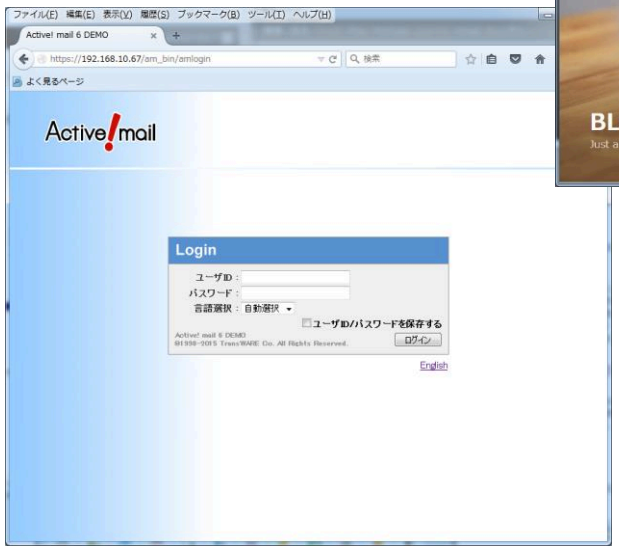


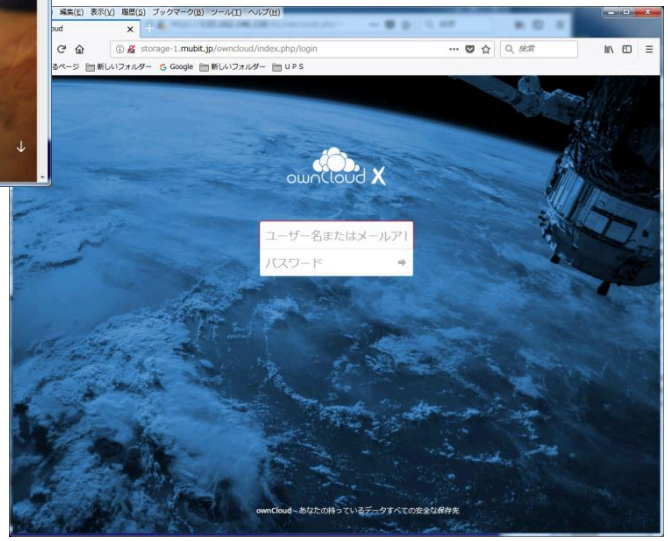
他の指も登録できます

WebサイトへのFIDO2対応生体認証の導入









Web　への生体認証の導入方法

A）新規に生体認証対応のWebを構築

B）既存Webへのアクセスに生体認証機能を導入

生体認証対応のリバースプロキシを利用

Web　への生体認証の導入方法

１）　FIDO2認証のSaaSを利用

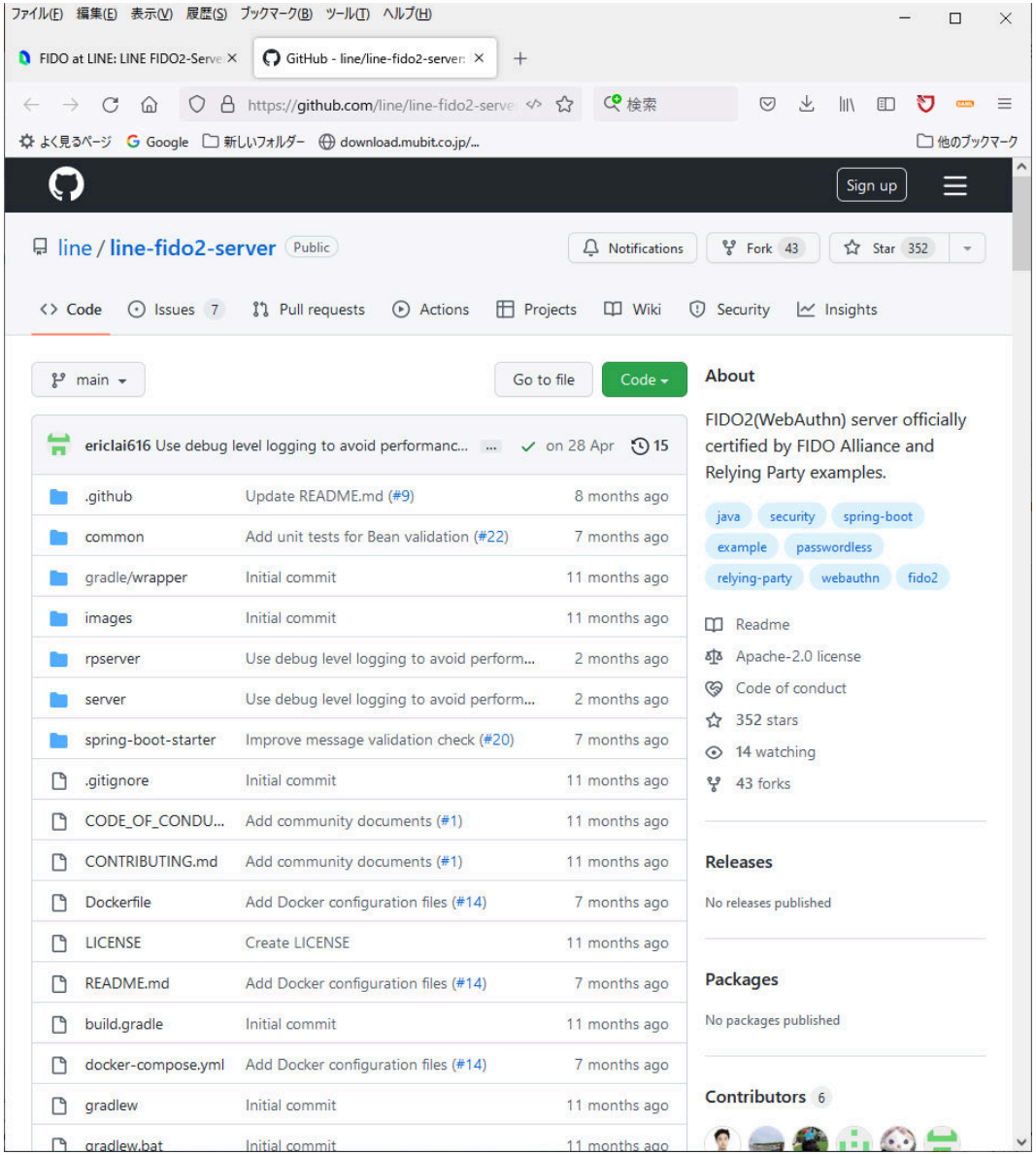
２）　FIDO2対応のWebを利用

３）　FIDO2対応のリバースプロキシを利用

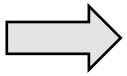
１）　FIDO2認証のSaaSを利用

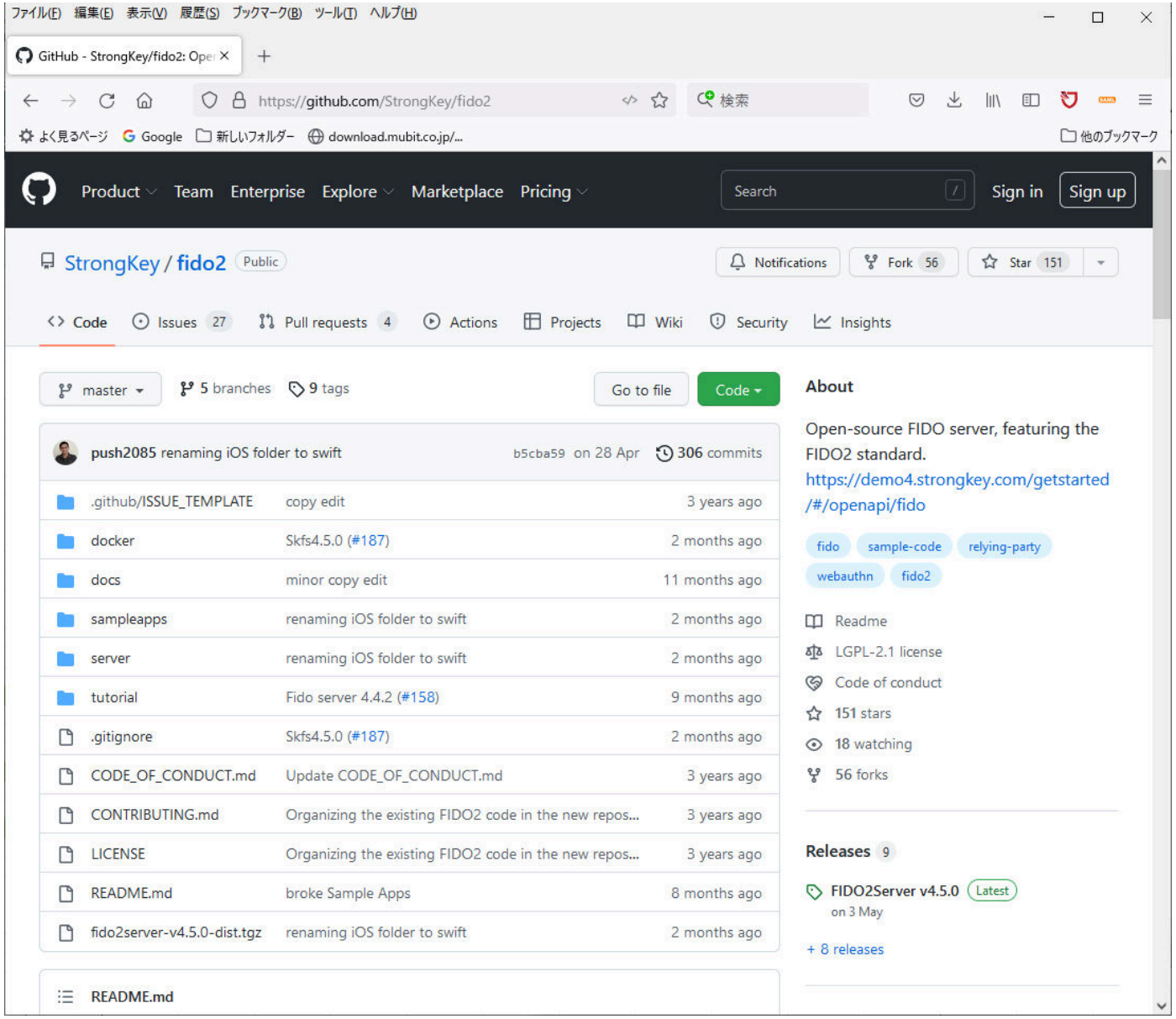
既存Web　/　API を利用してFIDO2の認証

2-1） LINE OSSのFIDO2を利用



2-2)　Strongkey community editionを利用





各種認証対応　「Powered BLUE」アプライアンス

① Web / Mail / DNS 機能 / マルチドメイン対応 / GUI

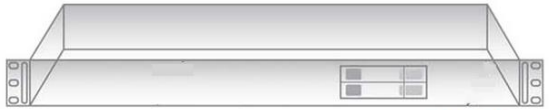
② AD認証 / OTP認証 / SSLクライアント認証
SAML認証 / Open ID Connect / 生体認証

③ リバースプロキシ

認証対応Webサーバー
①+②

POWERED BLUE

認証対応リバースプロキシ
①+②+③



POWERED BLUE

リバース
プロキシ

A) 新規構築　生体認証対応Web 「Powered BLUE Web for Biometrics」

① Web / Mail / DNS 機能 / マルチドメイン対応 / GUI

② AD認証 / OTP認証 / SSLクライアント認証
SAML認証 / Open ID Connect / 生体認証

認証対応Webサーバー
①+②

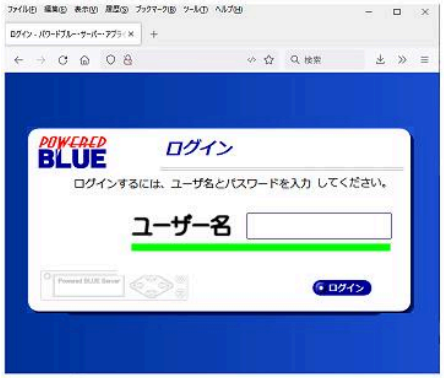
POWERED BLUE

一般的なWebコンテンツのサイト

WordPressのサイト

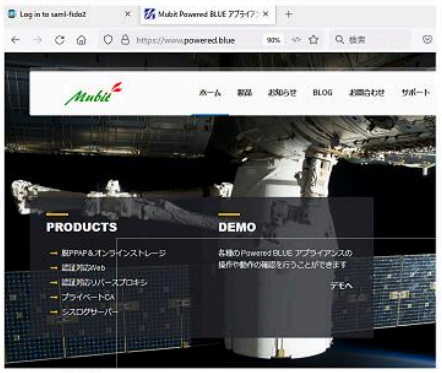
生体認証対応Webへのパスワードレス・アクセス

① iPhone / iPad / Android でのアクセス



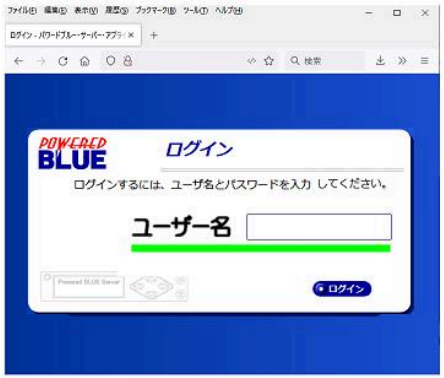
① Web へ アクセス

② キーにタッチ

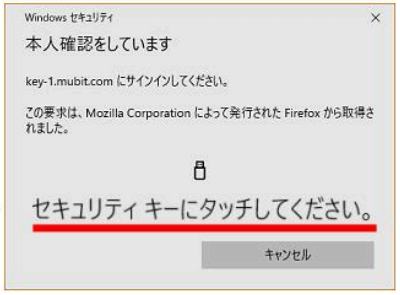


③ ターゲットWeb

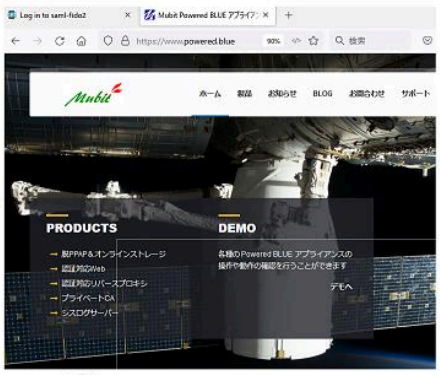
② パソコンでのアクセス



① Web へ アクセス



② キーにタッチ



③ ターゲットWeb

B) 既存Web　生体認証対応リバースプロキシ

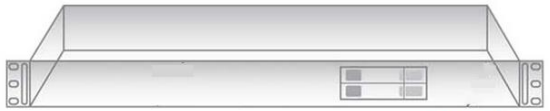
「Powered BLUE Reverse Proxy for Biometrics」

① Web / Mail / DNS 機能 / マルチドメイン対応 / GUI

② AD認証 / OTP認証 / SSLクライアント認証
SAML認証 / Open ID Connect / 生体認証

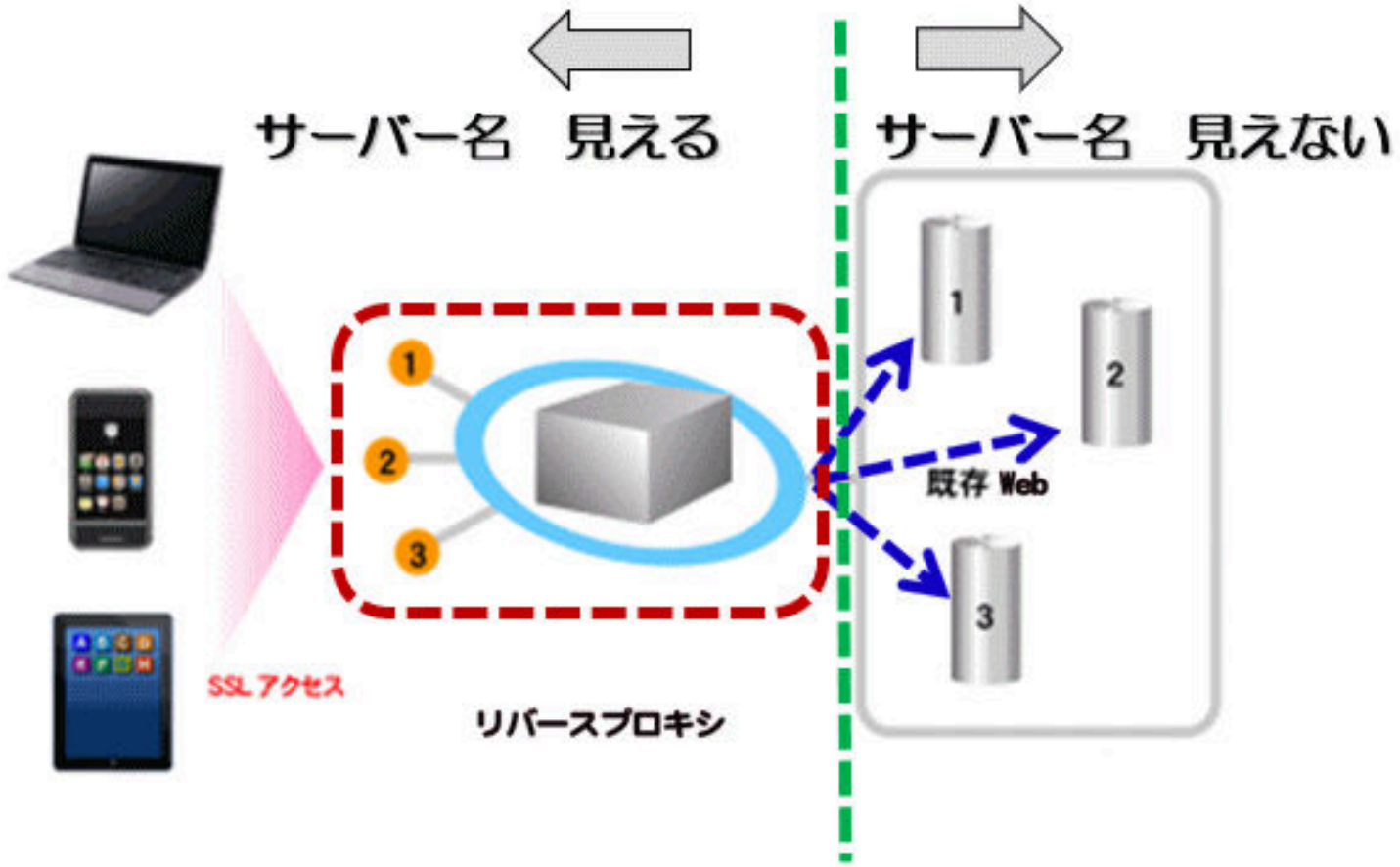
③ リバースプロキシ

認証対応リバースプロキシ
①+②+③



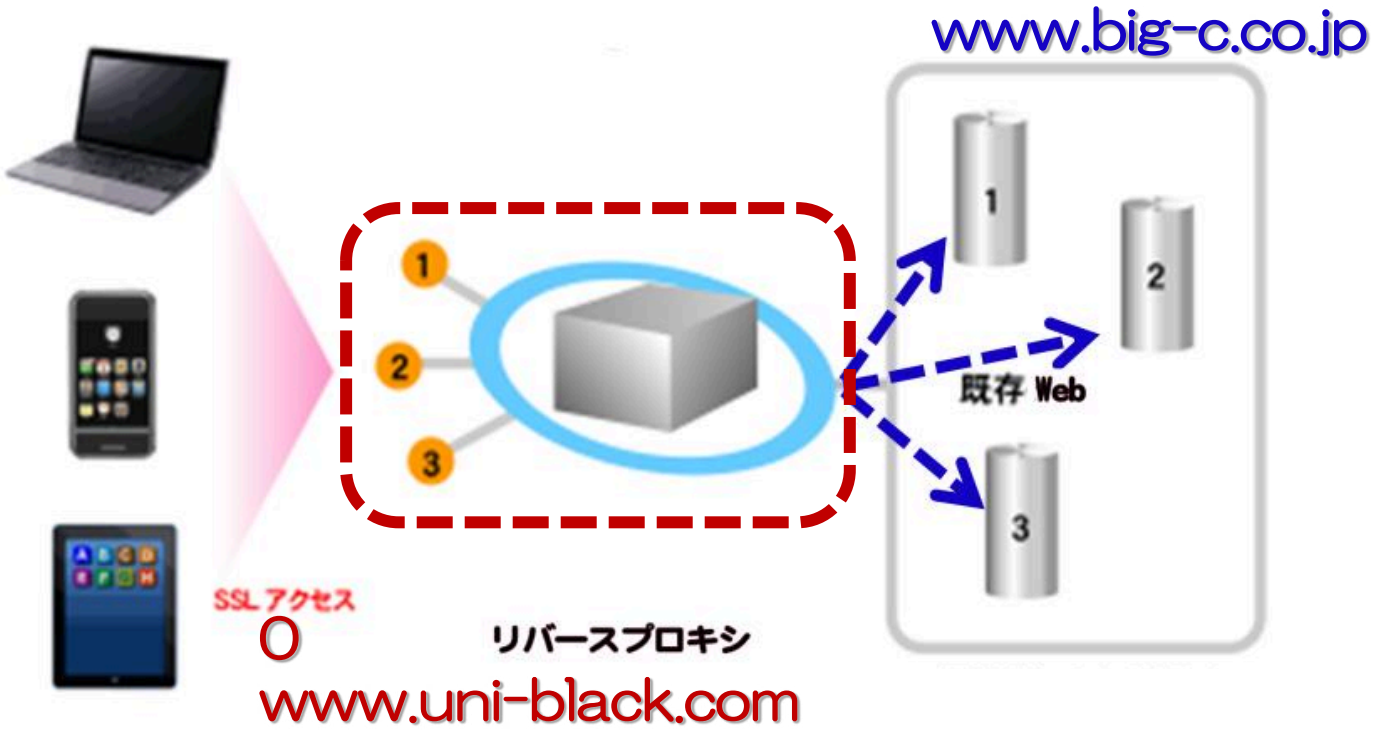
POWERED BLUE
リバース
プロキシ

リバースプロキシ　　リダイレクト先Web の 隠蔽



リバースプロキシ先を隠蔽

リバースプロキシ例　びっくろ

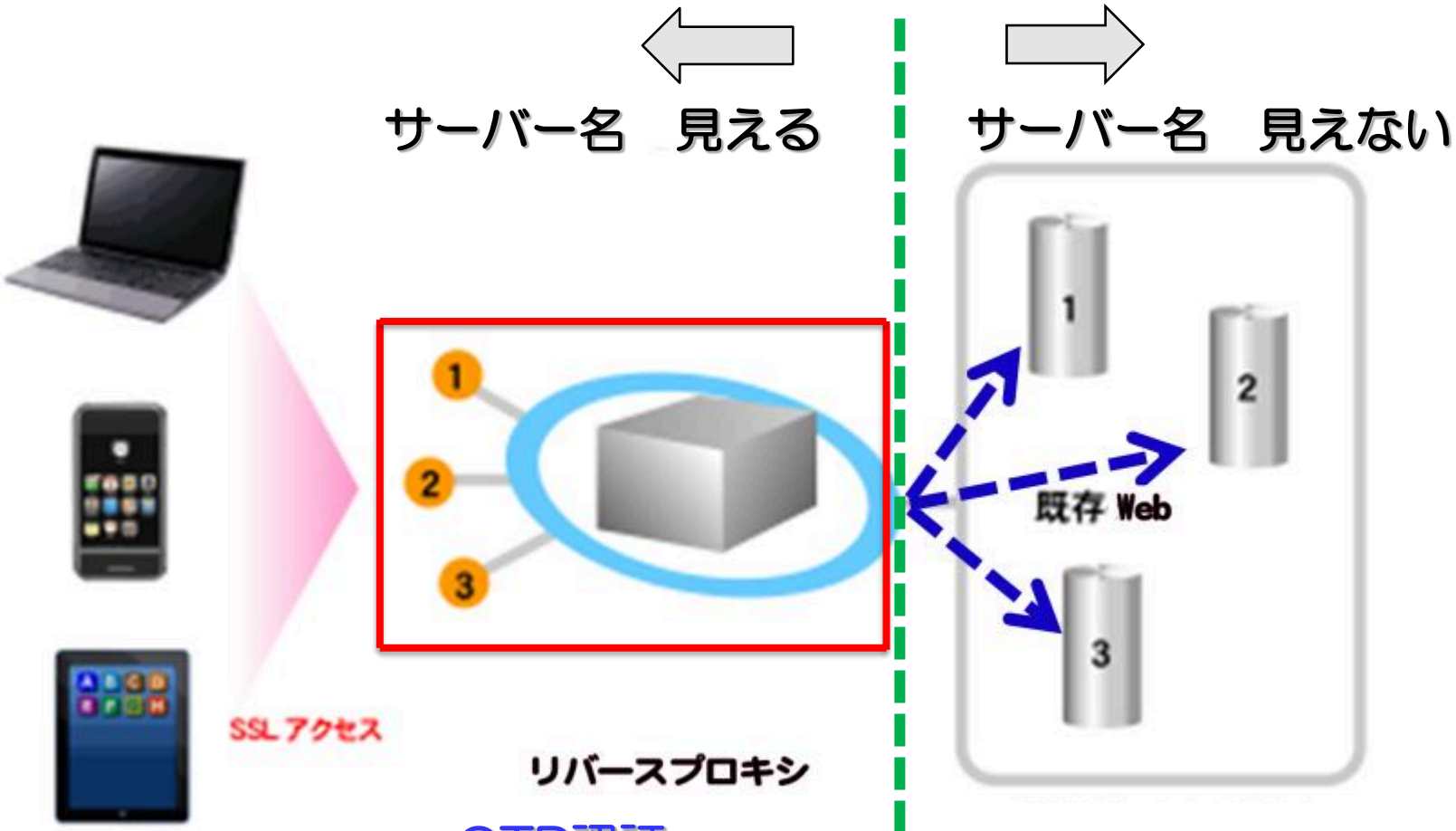


0　リバースプロキシ　　http://www.uni-black.com/

1　リバースプロキシ先　　http://www.big-c.co.jp/pc

ブラウザへのURL表示　　http://www.uni-black.com/pc

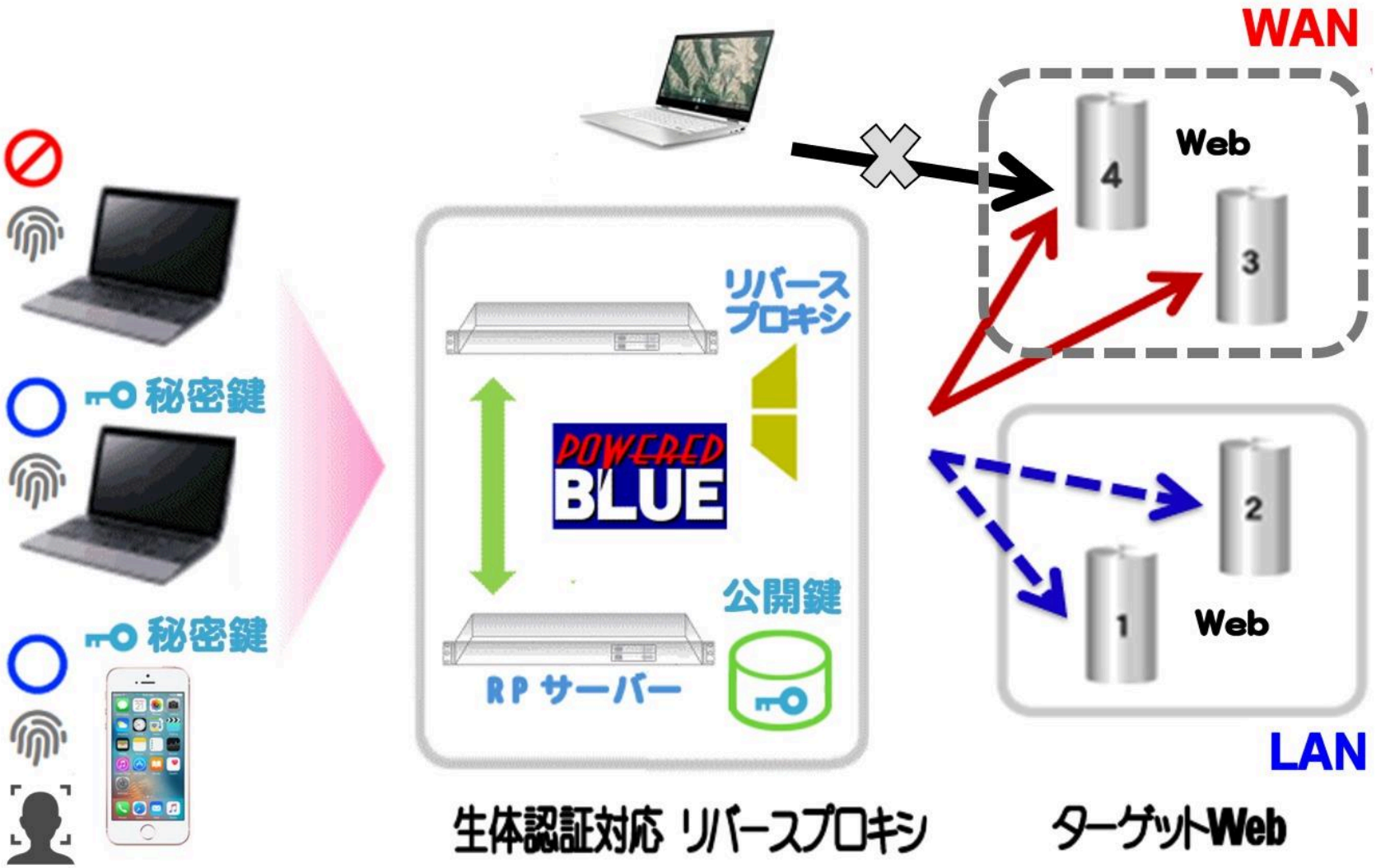
リバースプロキシへ生体認証付加　既存Webの改修不要



OTP認証
SSLクライアント認証
AD認証
SAML認証 / Open ID Connect
生体認証

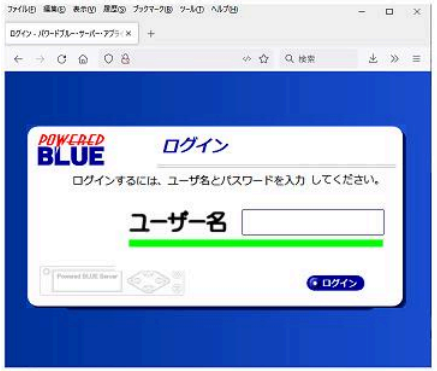
リバースプロキシへ生体認証付加　既存Webの改修不要

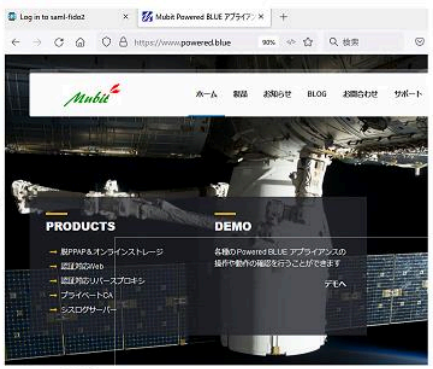
生体認証対応のリバースプロキシ　生体情報の保護



生体認証対応リバースプロキシへのパスワードレス・アクセス

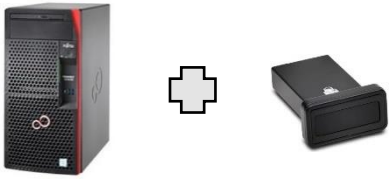
① iPhone / iPad / Android でのアクセス

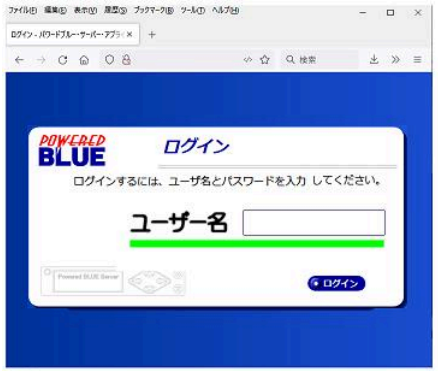


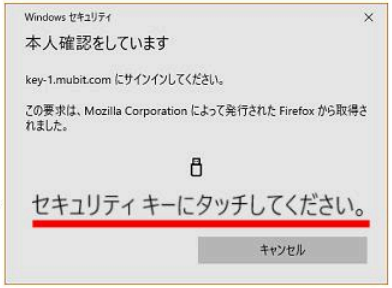


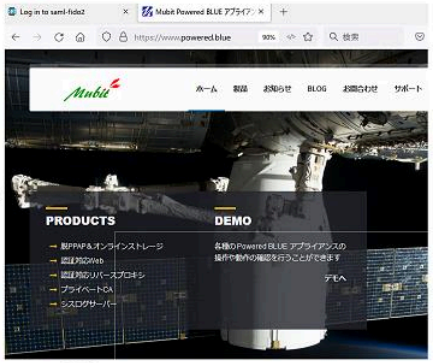
①リバースプロキシ へ アクセス　②キーにタッチ　③ターゲットWeb

② パソコンでのアクセス









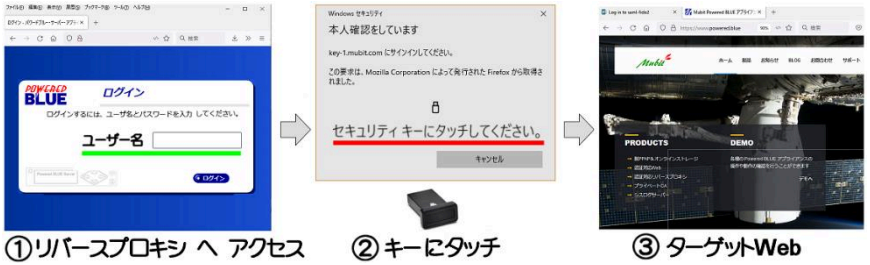
①リバースプロキシ へ アクセス　②キーにタッチ　③ターゲットWeb

生体認証は2要素認証（多要素認証）

- スマートフォン・ユーザー
  iPhone / iPad / Android 端末保有（1要素目）

- PC・ユーザー
  指紋認証器の保有（1要素目）

- 生体認証（2要素目）



①リバースプロキシ へ アクセス　②キーにタッチ　③ターゲットWeb

- パスワード（3要素目）

①リバースプロキシ へ アクセス　②キーにタッチ　③ターゲットWeb

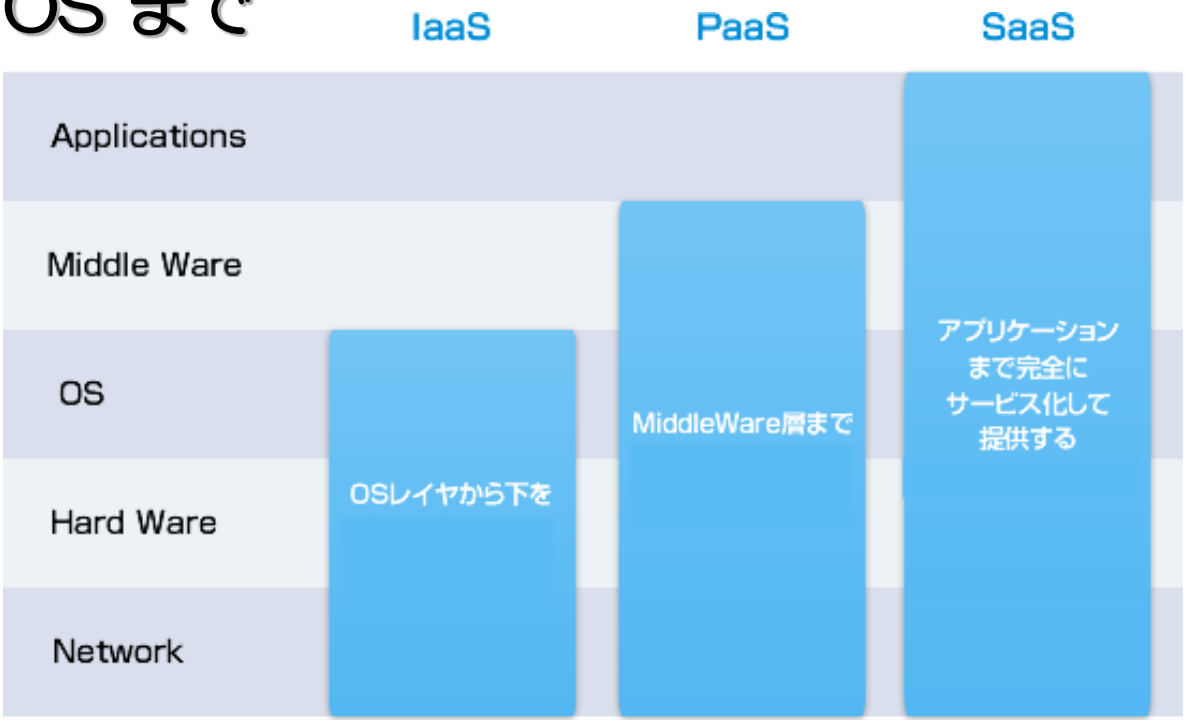
Powered BLUE アプライアンスの位置

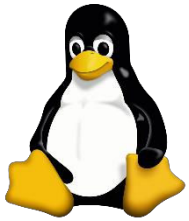
自社運用 = オールインワンのアプライアンス

Powered BLUE （OS+アプリ+GUI）

Pass

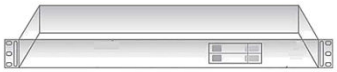
IaaS　OSまで





自社で運用

アプライアンスでの提供・動作環境



POWERED BLUE

POWERED BLUE

Microsoft Hyper-V

powered by amazon web services

FUJITSU

FUJITSU Hybrid IT Service FJcloud

- 自社管理で運用できるアプライアンス

FIDO2生体認証を導入するためには

環境	項目
インフラ	汎用のPCやスマートフォン（すでに保有している）
	ブラウザ　（対応済） 顔認証や指紋認証（スマートフォンに内蔵&使用） PC　（USBの指紋認証器を付加）

インフラやユーザー環境は整っている

おさらい　「Webサイトを生体認証に対応させる方法」

生体認証

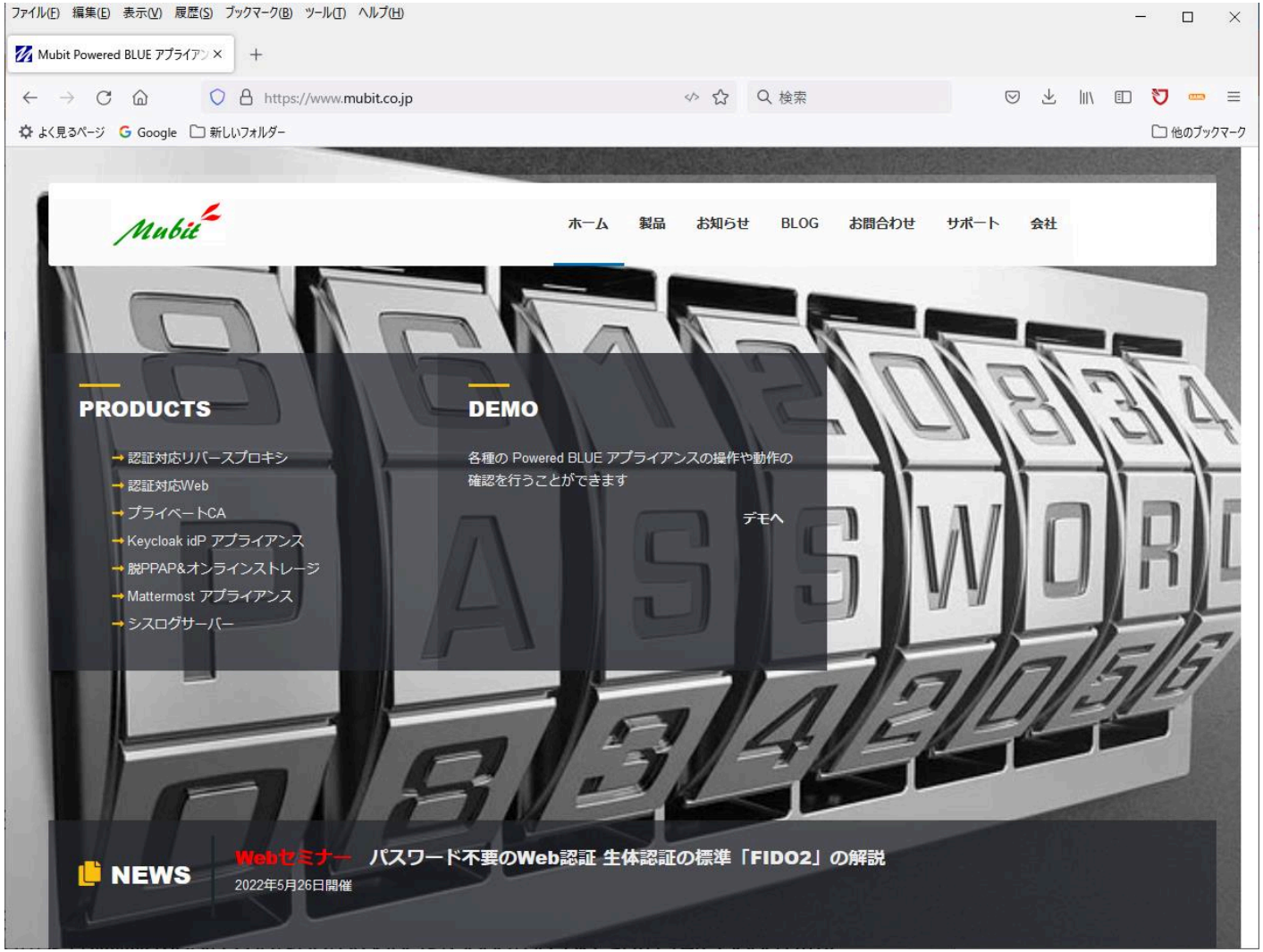
FIDO2 のユーザー環境は整っている

既存Webの修正不要

生体認証対応のリバースプロキシを利用

POWERED BLUE

リバース
プロキシ



Webサイト　https://www.mubit.co.jp/

お問合せなど

ご質問など　　Zoomの　Q&A　からお願いします

You Tube　メッセージ　から　お願いします

その他　　Webサイトの　問い合わせフォーム　から

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

お願いします