

パスワードレスのWeb認証 生体認証の標準「FIDO2」の解説

～ 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

サーフェス・Web

特定のソフトで
アクセス

一般的なブラウザ
でアクセス

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
- ランサムウェアのサービス
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



password

pwned?

②



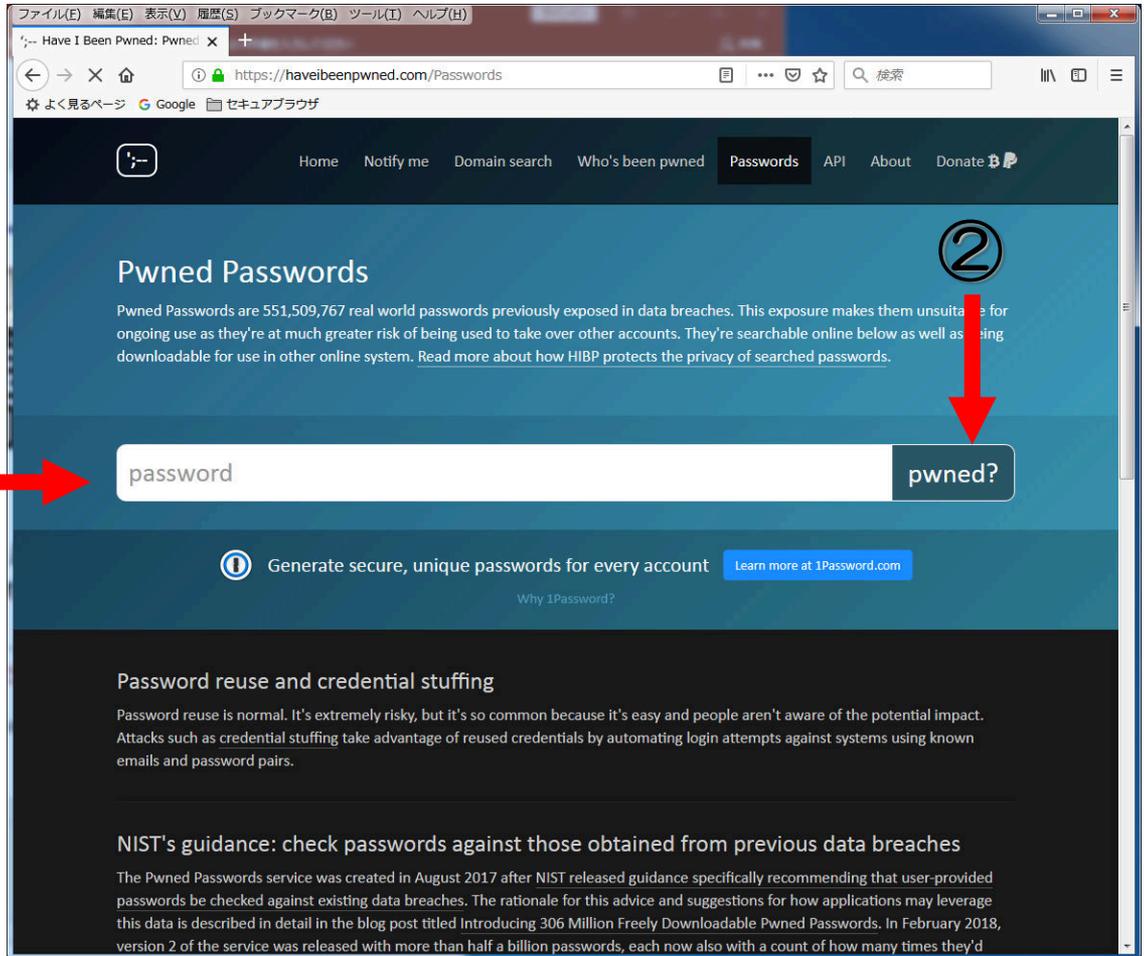
- ① パスワードを入力
- ② pwned? を押す

Oh no --- pwned !

残念でした

Good news — no pwnage found!

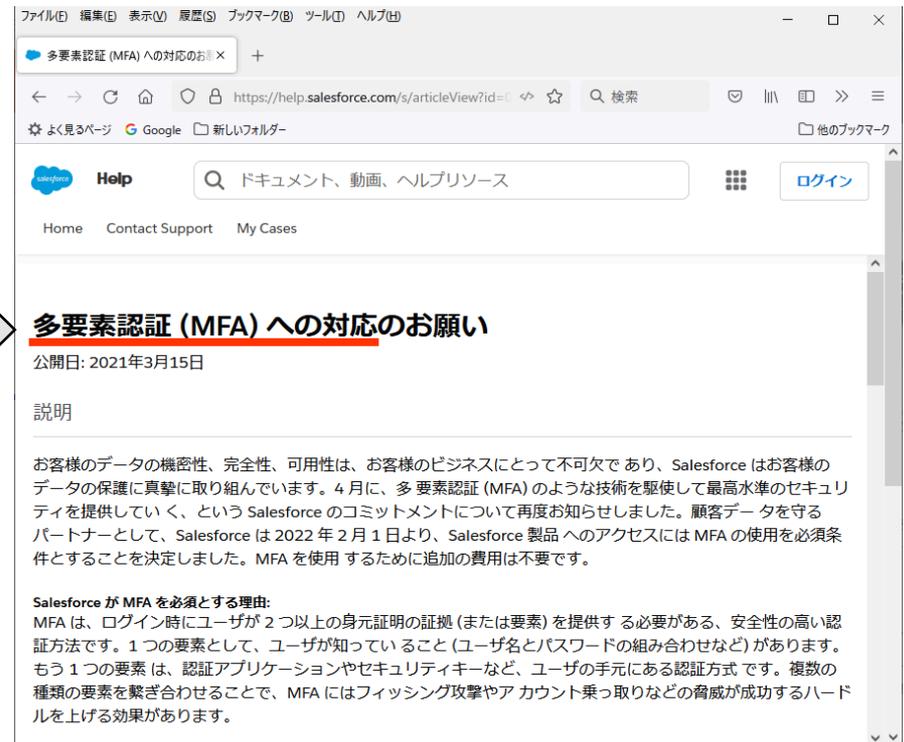
大丈夫



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

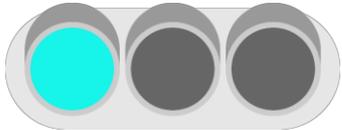
主な認証方式 利用時のポイント

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
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

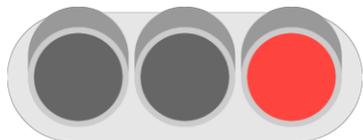
SMS認証は安全か ？



G-123789 があなたの
Google 確認コードです。



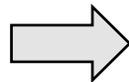
Google では SMS認証 は 使用可能



Salesforce では SMS認証 の 利用禁止

SIMスワップ

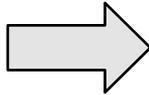
電話番号の変更が簡単



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 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、 ...
- <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



ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

google SMS 非推奨 - Google 検索

https://www.google.com/search 120% 検索

Google

google SMS 非推奨

すべて ニュース 動画 画像 ショッピング もっと見る ツール

約 1,810,000 件 (0.37 秒)

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。 2017/07/18

https://japan.cnet.com › 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 2022/5/17 CNET Japan

強調スニペットについて フィードバック

https://japan.zdnet.com › セキュリティ

NISTが警告、SMSでの二段階認証が危険な理由 - ZDNet Japan

2017/01/27 — SMSでシークレットコードを送信するのはやめてください。... 認証が必要な一定レベルのセキュリティを確保するために、「SMSを使用したOOBは非推奨で...

https://www.itmedia.co.jp › news › 1904/08 › news026_2

SMS認証の仕組みと危険性、「TOTP」とは？「所有物認証 ...

2019/04/08 — パスワードでの認証の後に、携帯電話に届くSMSメッセージに書かれた数字や文字列を ... 草稿の時点では「非推奨」とされていたSMS認証は、決定稿公開 ...

生体認証とは

■ 指紋認証

■ 静脈認証

■ 顔認証

■ 虹彩認証

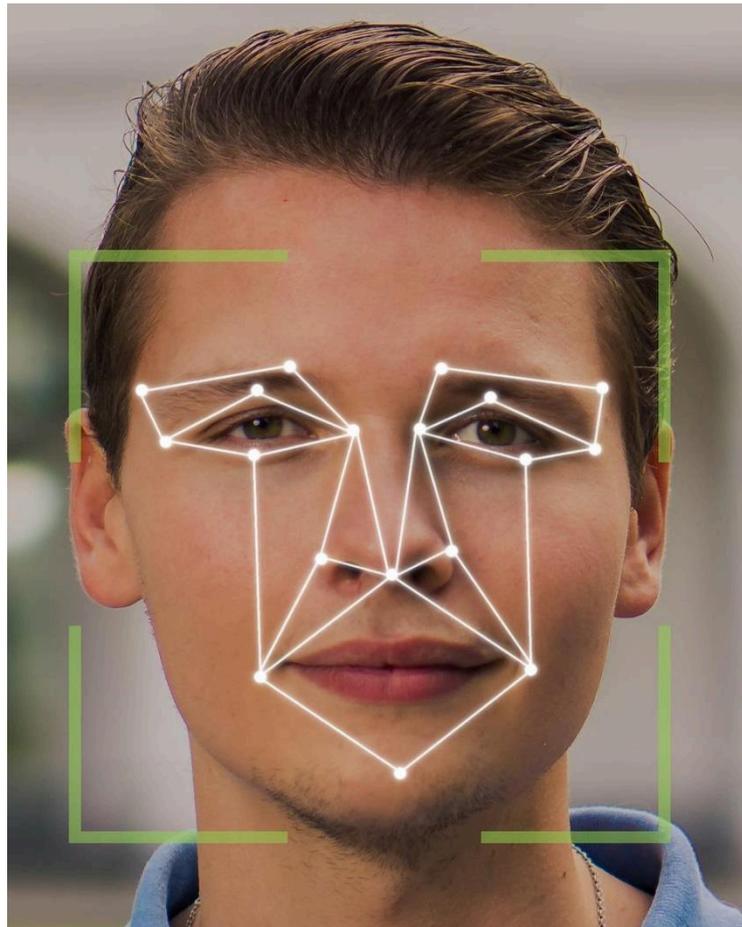
- 利用者が保有する生体「固有の情報」を利用
- 生体固有の情報は「複製が出来にくい」ことを利用

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



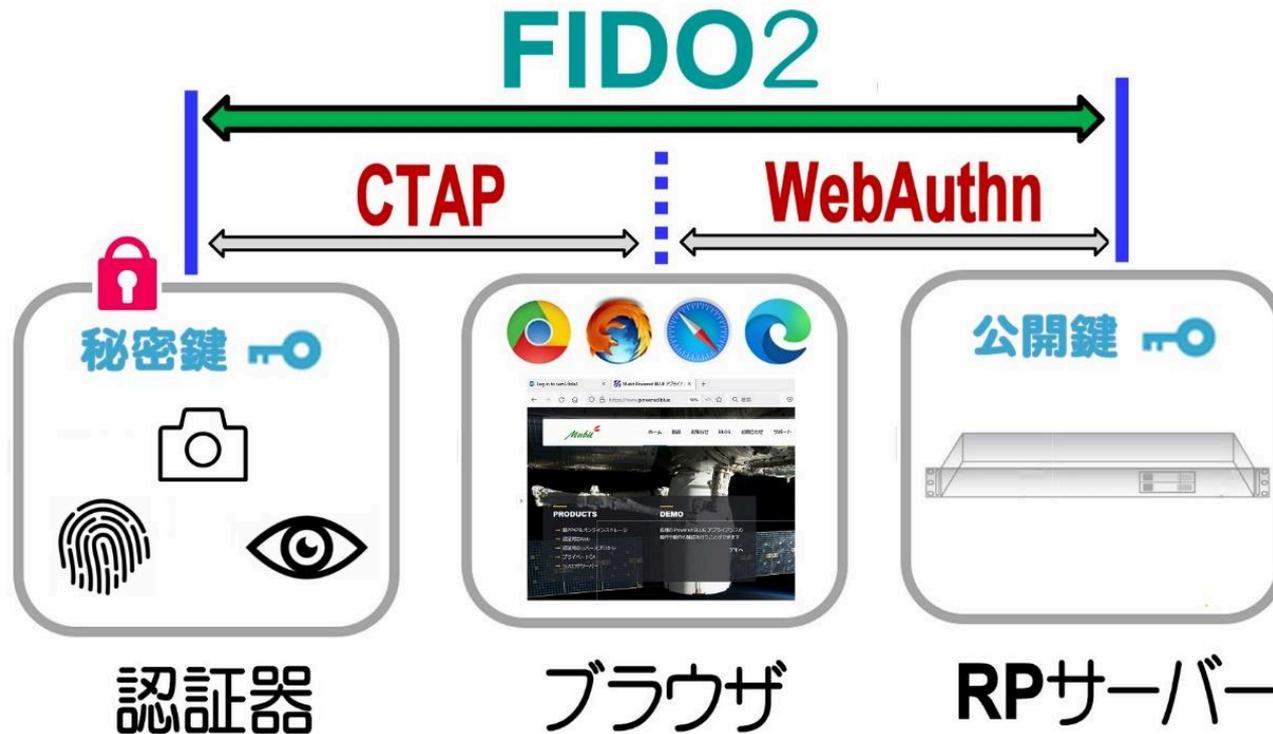
■ iOS



■ 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! 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** 

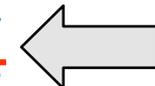
パソコンでも利用できます

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



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

指紋認証や顔認証の登録方法



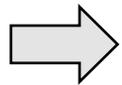
FIDO2 対応 指紋認証器 PCユーザー



Windows 10 / 11 指紋登錄手順



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

PCのフリーズを解除する手順...

関連設定

ロック画面

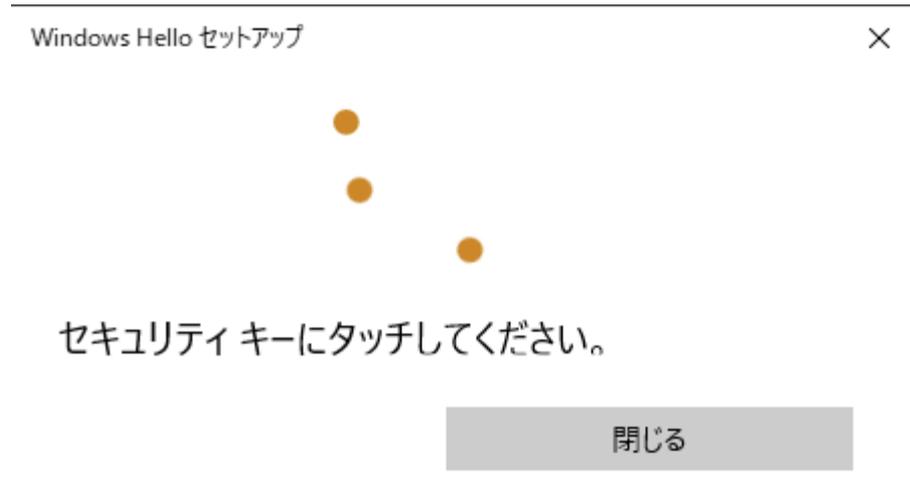
質問がありますか?

- 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

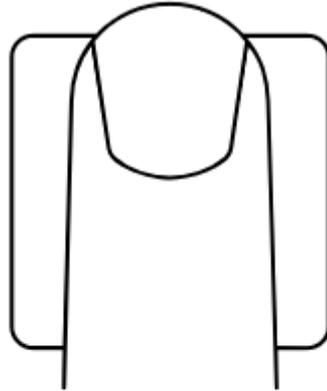
フィードバックの送信

指紋登録手順



指紋登録手順

Windows Hello セットアップ



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。

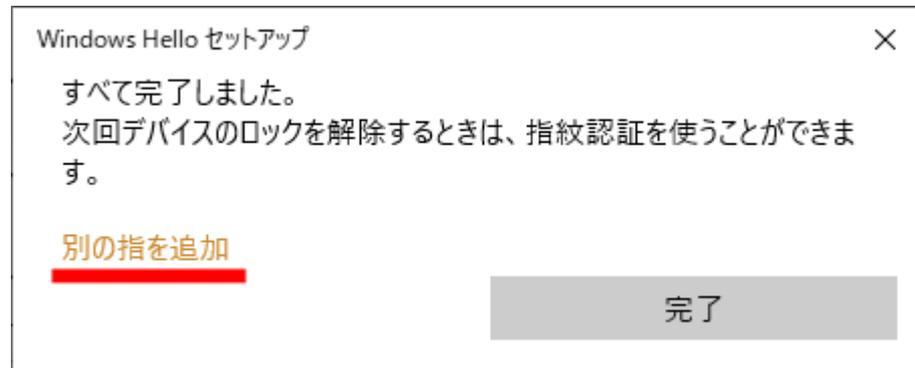
キャンセル



指紋登録手順

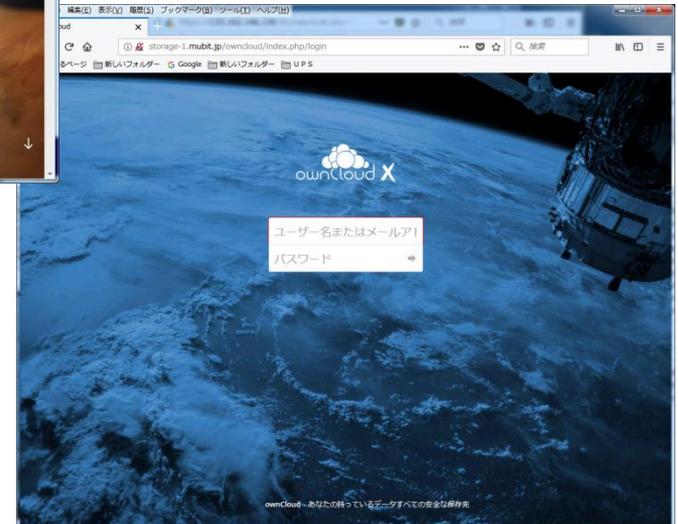
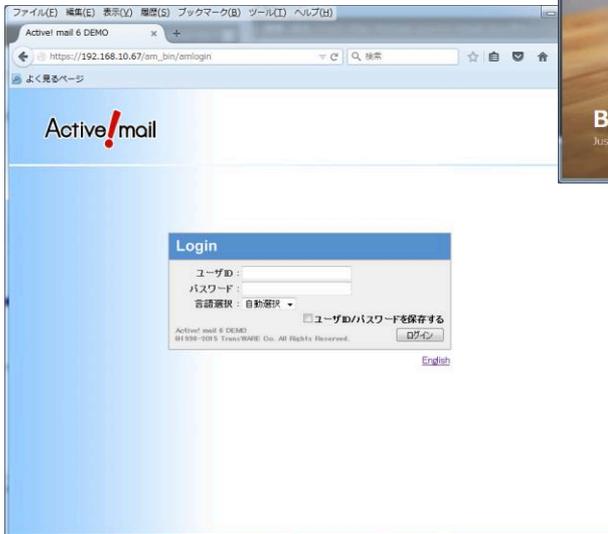
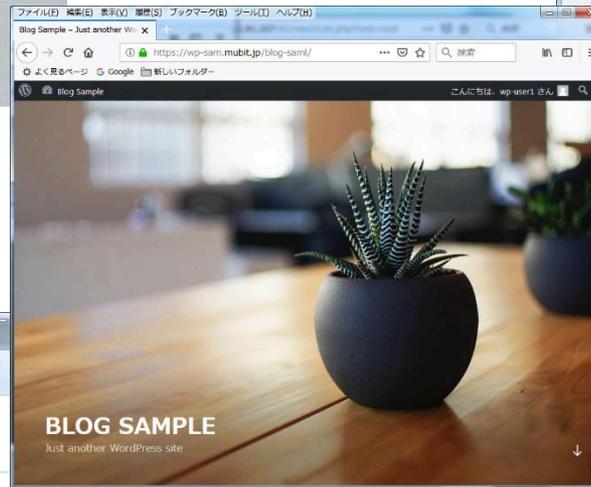
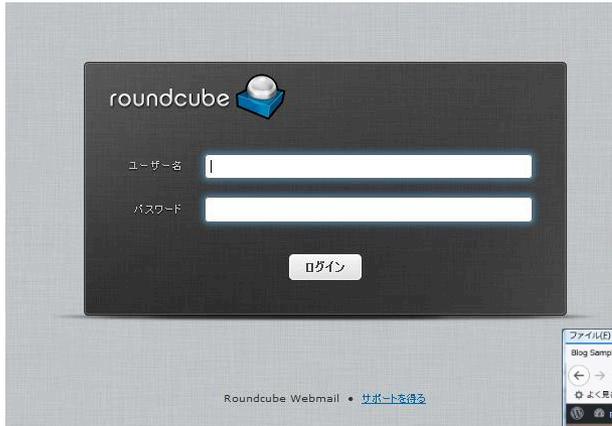


指紋登録手順



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



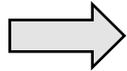
Web への生体認証の導入方法

- 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



The screenshot shows the GitHub repository page for 'line/line-fido2-server'. The browser address bar shows the URL 'https://github.com/line/line-fido2-server'. The repository is public and has 43 forks and 352 stars. The main content area displays a list of files and folders, including '.github', 'common', 'gradle/wrapper', 'images', 'rpserver', 'server', 'spring-boot-starter', '.gitignore', 'CODE_OF_CONDU...', 'CONTRIBUTING.md', 'Dockerfile', 'LICENSE', 'README.md', 'build.gradle', 'docker-compose.yml', 'gradlew', and 'gradlew.bat'. The right sidebar contains information about the repository, including the description 'FIDO2(WebAuthn) server officially certified by FIDO Alliance and Relying Party examples.', tags like 'java', 'security', 'spring-boot', 'example', 'passwordless', 'relying-party', 'webauthn', and 'fido2', and statistics such as 352 stars, 14 watching, and 43 forks.

2-2) Strongkey community editionを利用



GitHub - StrongKey/fido2: Open-source FIDO server, featuring the FIDO2 standard.

Navigation: Code (selected), Issues (27), Pull requests (4), Actions, Projects, Wiki, Security, Insights

Repository details: master (selected), 5 branches, 9 tags, Go to file, Code

Recent commits:

- push2085 renaming iOS folder to swift (b5cba59) on 28 Apr (306 commits)

File/Folder	Commit Message	Time Ago
.github/ISSUE_TEMPLATE	copy edit	3 years ago
docker	Skfs4.5.0 (#187)	2 months ago
docs	minor copy edit	11 months ago
sampleapps	renaming iOS folder to swift	2 months ago
server	renaming iOS folder to swift	2 months ago
tutorial	Fido server 4.4.2 (#158)	9 months ago
.gitignore	Skfs4.5.0 (#187)	2 months ago
CODE_OF_CONDUCT.md	Update CODE_OF_CONDUCT.md	3 years ago
CONTRIBUTING.md	Organizing the existing FIDO2 code in the new repos...	3 years ago
LICENSE	Organizing the existing FIDO2 code in the new repos...	3 years ago
README.md	broke Sample Apps	8 months ago
fido2server-v4.5.0-dist.tgz	renaming iOS folder to swift	2 months ago

About:

- Open-source FIDO server, featuring the FIDO2 standard.
- <https://demo4.strongkey.com/getstarted/#/openapi/fido>
- Tags: fido, sample-code, relying-party, webauthn, fido2
- Readme
- License: LGPL-2.1
- Code of conduct
- 151 stars
- 18 watching
- 56 forks

Releases (9):

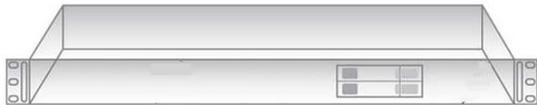
- FIDO2Server v4.5.0 (Latest) on 3 May
- + 8 releases

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

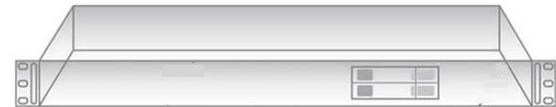
①+②



**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

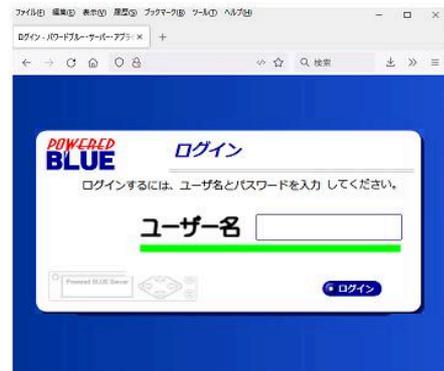


WordPressのサイト

生体認証対応Webへのパスワードレス・アクセス



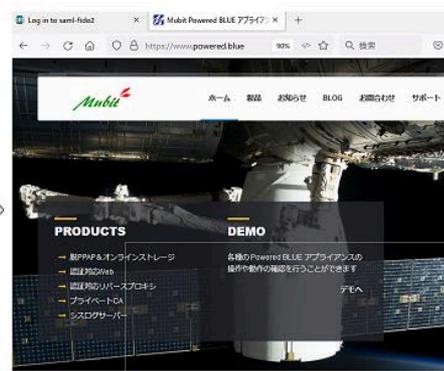
① iPhone / iPad / Android でのアクセス



① Web へ アクセス

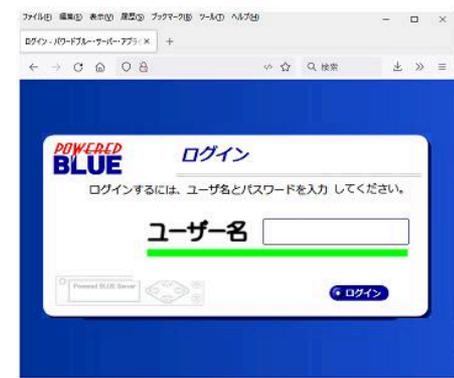
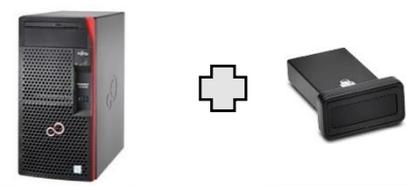


② キーにタッチ



③ ターゲットWeb

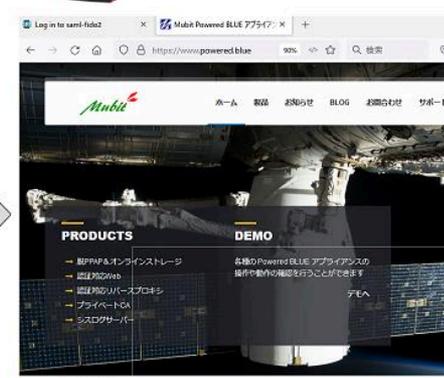
② パソコンでのアクセス



① Web へ アクセス



② キーにタッチ



③ ターゲットWeb

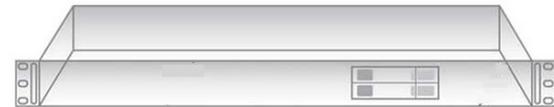
B) 既存Web 生体認証対応リバースプロキシ

「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

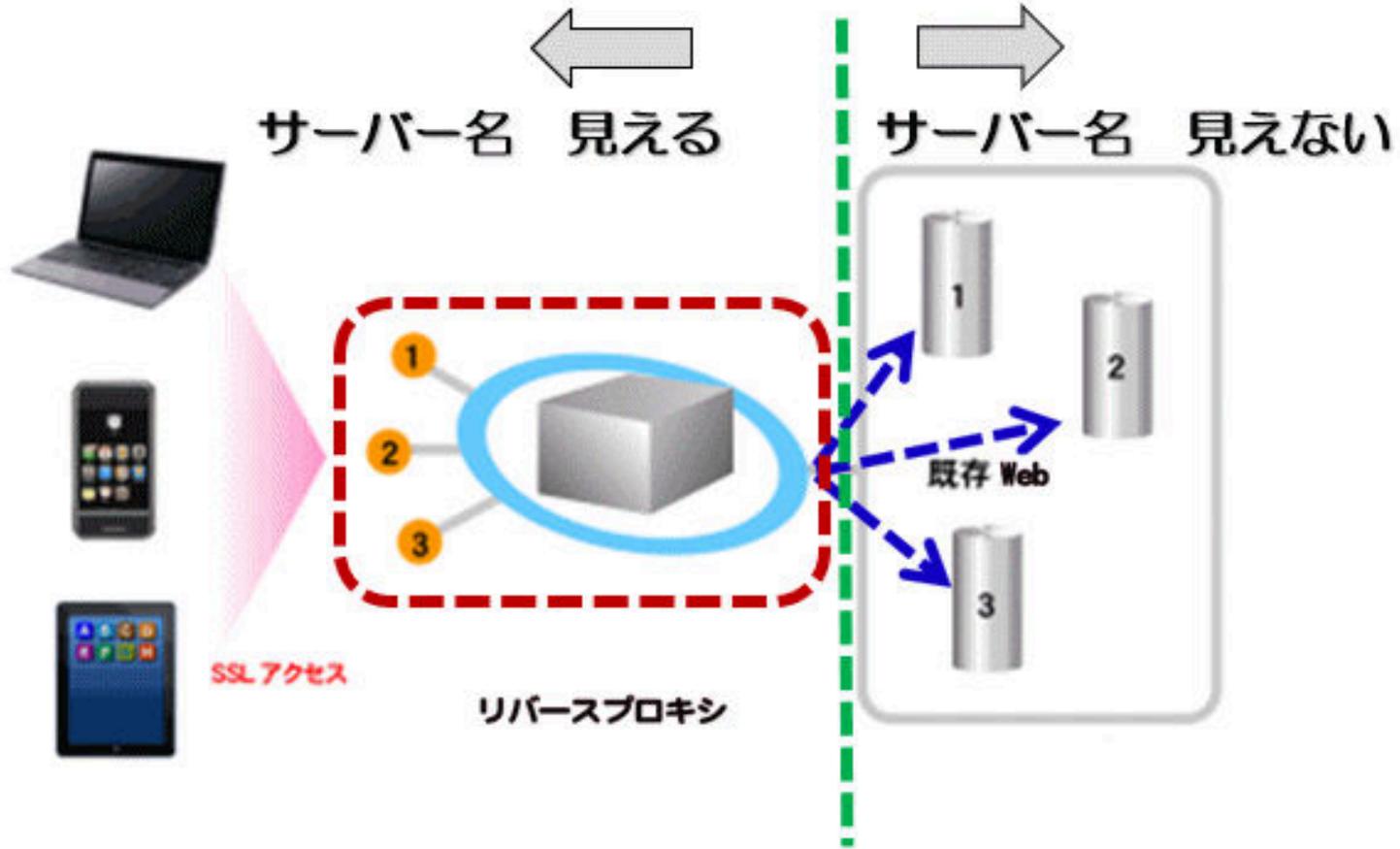
①+②+③



**POWERED
BLUE**

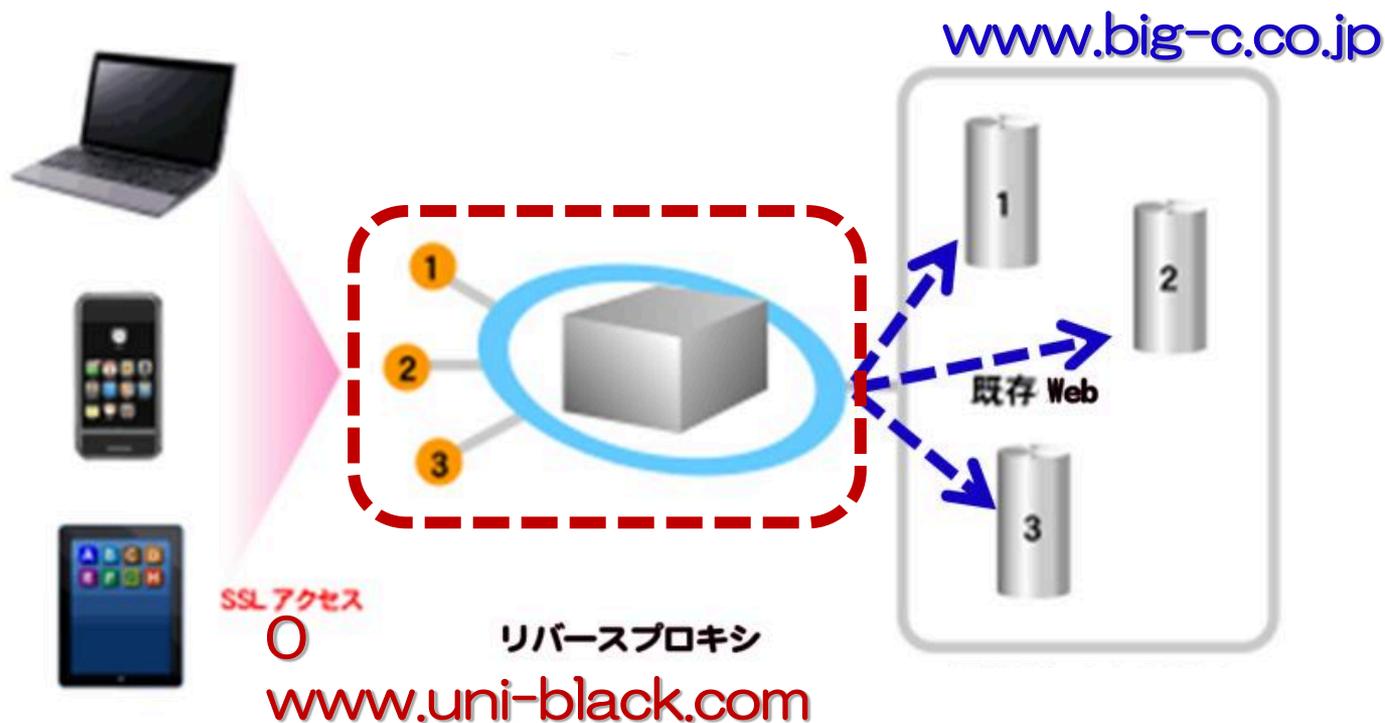
リバース
プロキシ





リバースプロキシ先を隠蔽

リバースプロキシ例 びっくろ



○ リバースプロキシ

<http://www.uni-black.com/>



1 リバースプロキシ先

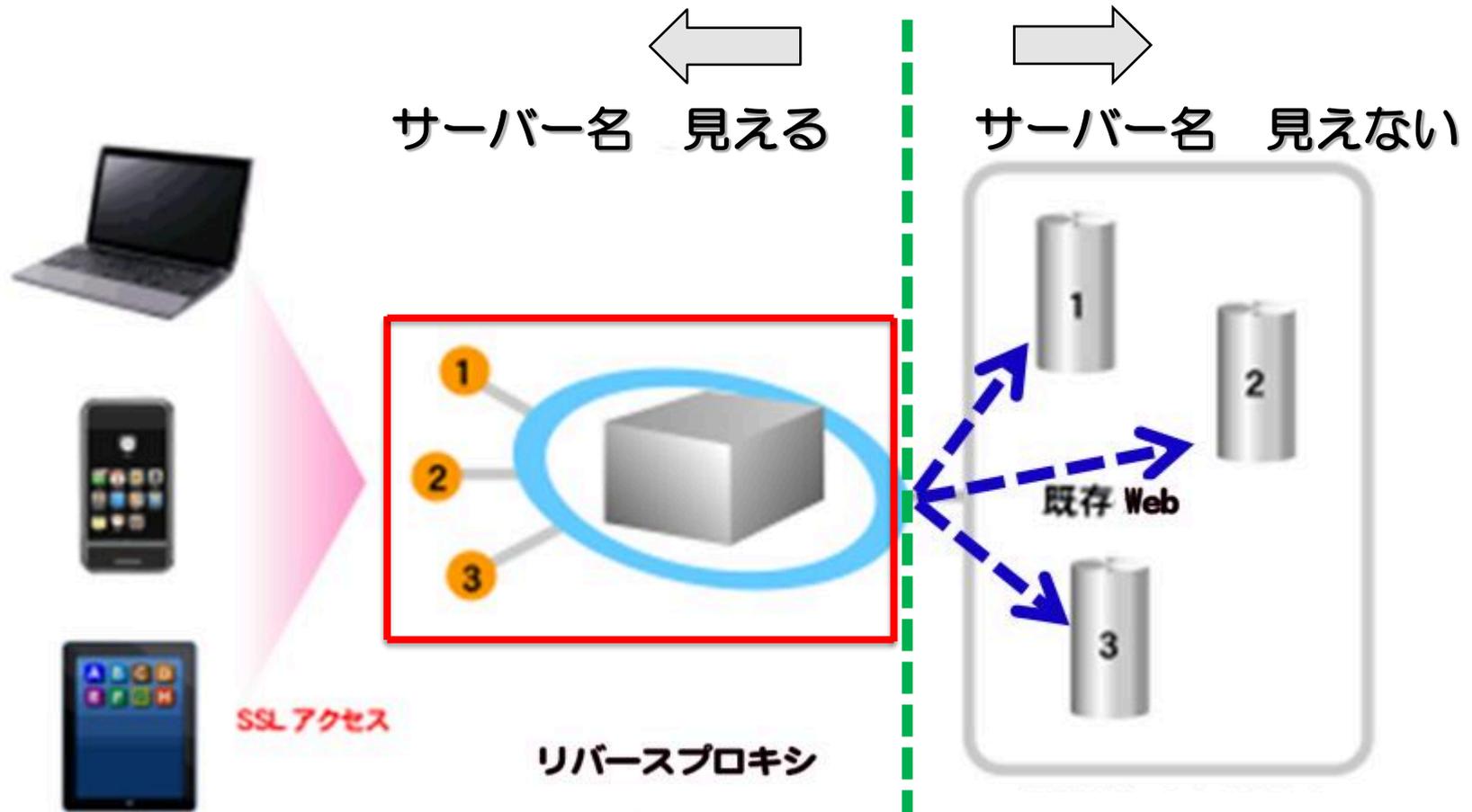
<http://www.big-c.co.jp/pc>



ブラウザへのURL表示

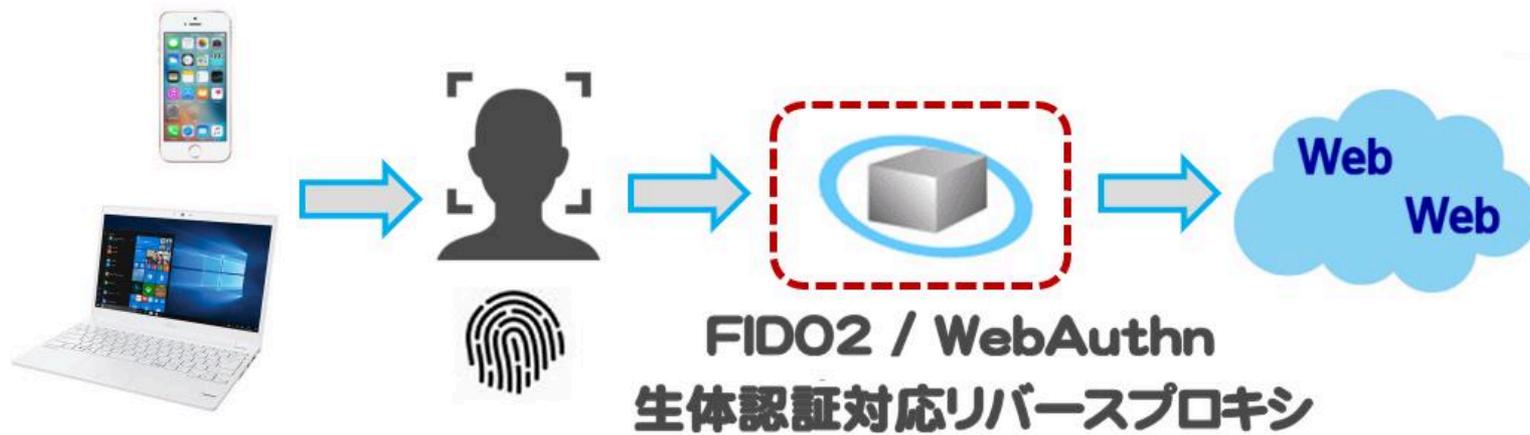
<http://www.uni-black.com/pc>

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

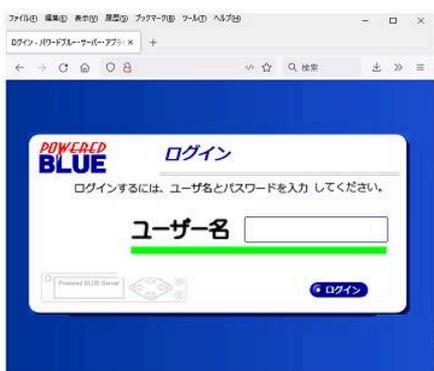
リバースプロキシへ生体認証付加 既存Webの改修不要



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



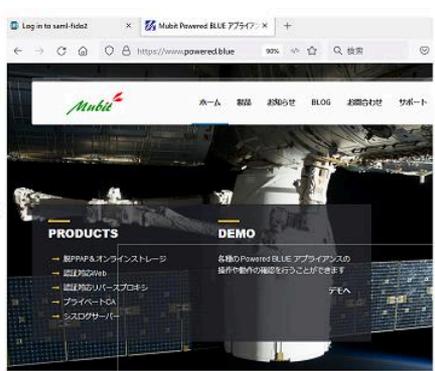
① iPhone / iPad / Android でのアクセス



① リバースプロキシへアクセス

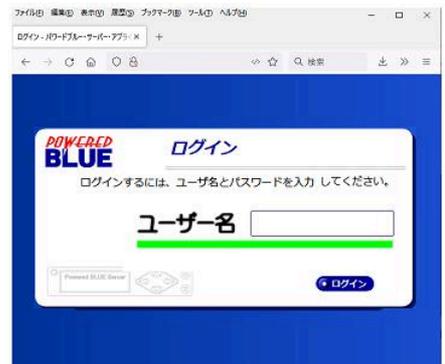


② キーにタッチ

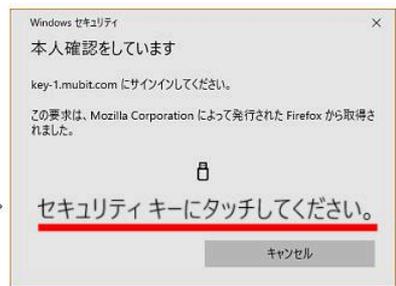


③ ターゲットWeb

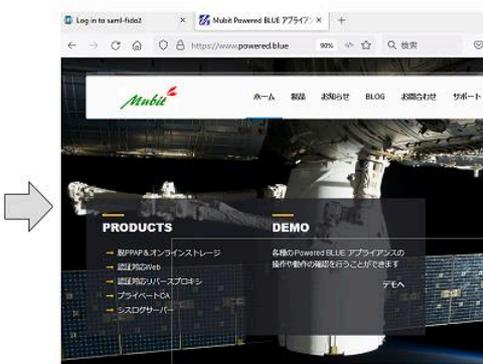
② パソコンでのアクセス



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）



パスワード（3要素目）



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

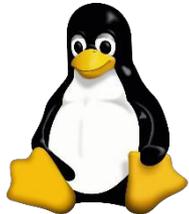
IaaS

OS まで

IaaS

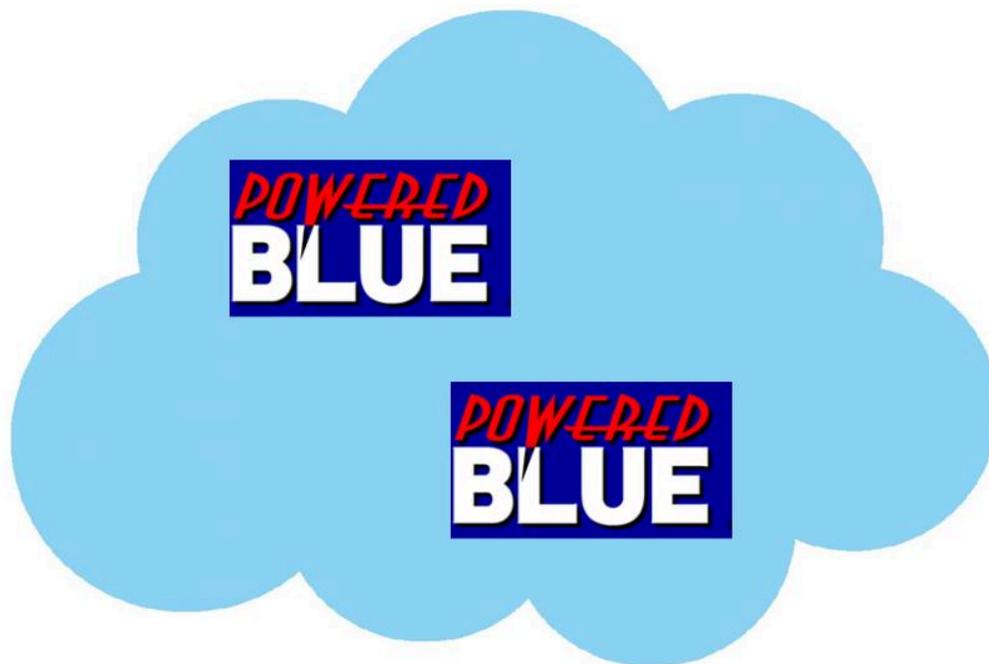
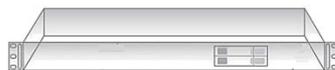
PaaS

SaaS



自社で運用

アプライアンスでの提供・動作環境



FUJITSU Hybrid IT Service FJcloud

- 自社管理で運用できるアプライアンス

Web Meetingが急速に浸透した理由



環境	項目
インフラ	ノートPCにWebカメラが搭載されていた 狭いインターネット回線でもWeb meetingを利用できる環境 Zoomが無償で利用できた

- ① インフラは整備済
- ② コロナで急速に広がった

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

■ 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



ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Mubit Powered BLUE アプライアンス × +

← → ↻ 🏠 🔒 https://www.mubit.co.jp 🔍 検索 📄 📄 📄 📄 📄 📄 📄

よく見るページ Google 📁 新しいフォルダー 📁 他のブックマーク

Mubit ホーム 製品 お知らせ BLOG お問い合わせ サポート 会社

PRODUCTS

- 認証対応リバースプロキシ
- 認証対応Web
- プライベートCA
- Keycloak idP アプライアンス
- 脱PPAP&オンラインストレージ
- Mattermost アプライアンス
- シスログサーバー

DEMO

各種の Powered BLUE アプライアンスの操作や動作の確認を行うことができます

デモへ

NEWS **Webセミナー** パスワード不要のWeb認証 生体認証の標準「FIDO2」の解説
2022年5月26日開催



Webサイト

<https://www.mubit.co.jp/>