YubiKey（FIDO2対応セキュリティキー）を活用した認証強化の実現

IceWall技術レポート

1. はじめに

本レポートでは、IceWall MFAでYubico社が提供するFIDO2対応セキュリティキー（YubiKey）を活用した認証強化を実現するための設定方法と、具体的なユースケースについてご紹介します。

9. まとめ →

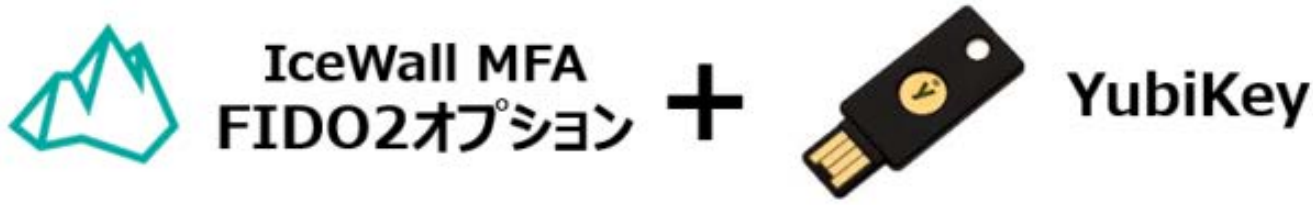
2. ソリューション概要（IceWall MFA＋YubiKey）

IceWall MFA FIDO2オプションは、各種デバイス標準の生体認証やFIDO2対応セキュリティキーと連携して、パスワードレス認証や、多要素認証を実現します。次世代認証の標準規格である「FIDO」(Fast IDentity Online)の最新版「FIDO2」および「W3C Web Authentication (WebAuthn)」に対応しています。あらかじめ暗号化されたキーがインストールされた端末からのアクセスのみ認証することで、ユーザーの利用端末を限定し、SaaSを含む幅広いWebアプリケーションの認証を強化するソリューションです。

IceWall MFA FIDO2オプションの詳細は以下ページをご参照ください。

HPE IceWall MFA FIDO2オプション →

FIDO2オプションで使用可能なデバイスの一つにYubiKeyがあります。



YubiKeyを用いたFIDO2認証では、認証の3要素のひとつである「所持」を認証要素とします。パスワード認証による「記憶」と、予め登録したセキュリティキーの「所持」を組み合わせた認証方式で、認証を強化します。またFIDO2認証を活用したいが、制約があるケースでの課題を解消します。例えば、端末にFIDO2対応の生体認証対応機能が付いていないケース、FIDO2対応スマートフォンを用いた多要素認証を実現したいが社員全員に配布できないケース、共有端末を利用しているケースなど、利用環境の制約による様々な課題を解決可能です。

3. FIDO2対応セキュリティキーYubiKeyについて

YubiKeyは、Yubico社の提供するFIDO2対応セキュリティキーです。

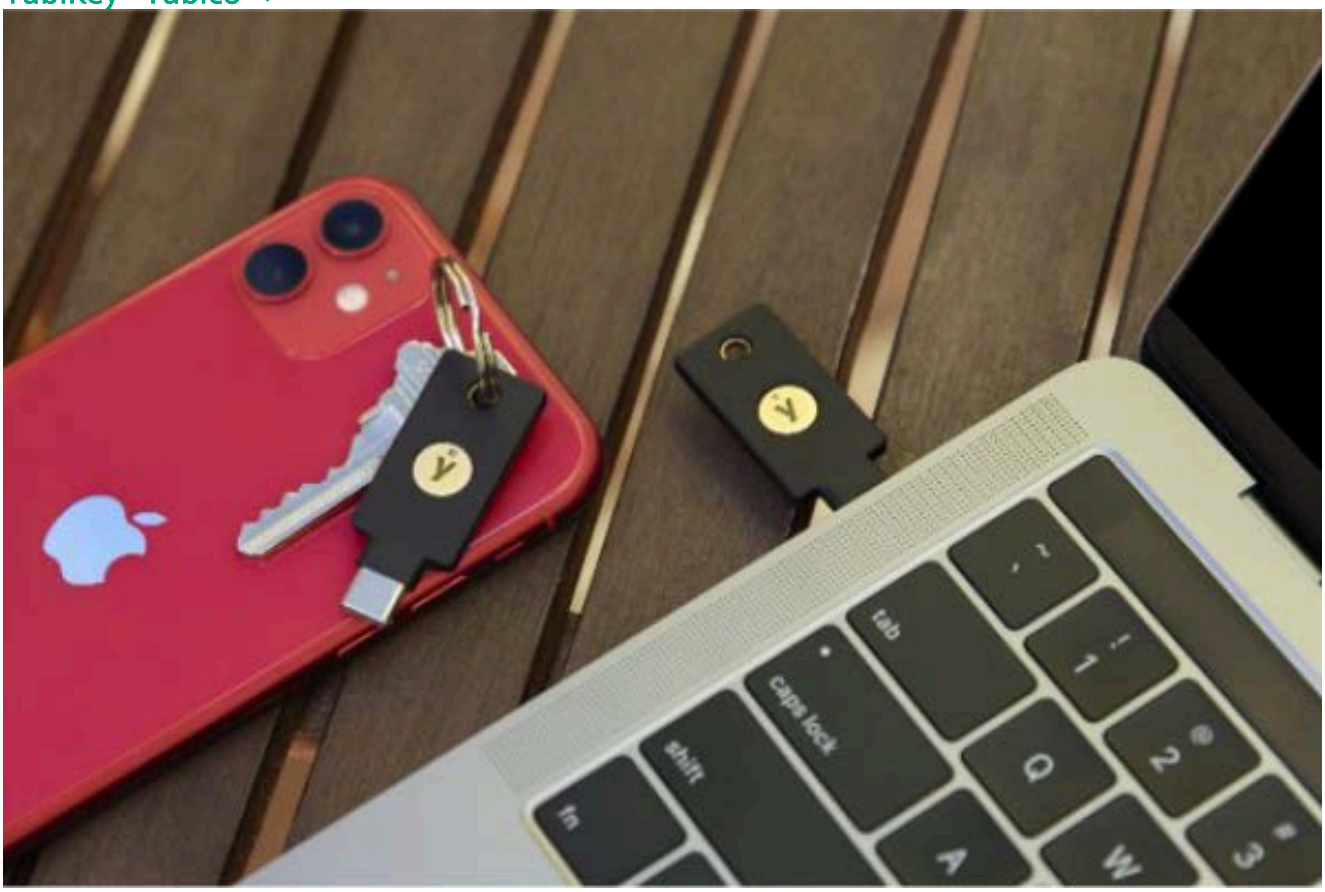
- PCにUSB接続したり、NFC搭載のスマートフォンにかざしたりするだけで、強力な多要素認証を実現。

- 認証強度がソフトウェアによる認証よりも強固。
- 電池切れによる買い替えの手間がない。

セキュリティ強度とユーザビリティの高さから、次世代の多要素認証方式として注目されています。
USB-A、USB-C、NFC、Lightningなど様々なインターフェースに対応しています。

Yubico社YubiKeyの詳細は以下ページをご参照ください。

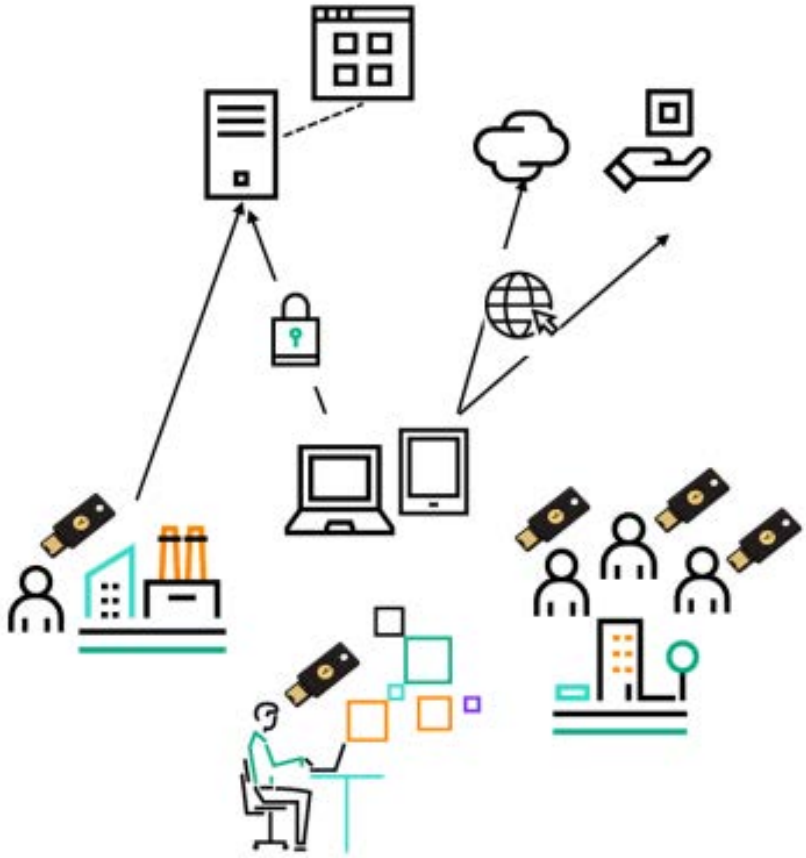
YubiKey - Yubico →



※Type-Aでも使用可

4. ソリューションのターゲットとユースケース

4.1 ソリューションのターゲット



IceWall MFAでYubiKeyを活用するソリューションは、以下のようにシステムの規模や用途を問わず、様々な環境や利用者を対象としています。

- 全業種向けシステム
- 全てのシステム用途（BtoE/BtoB/BtoC/GtoCなど）

- クラウドサービスをご利用中の方
- 社内、社外のWebアプリケーションの認証を強化したい方

- リモートワークを活用している環境
- データセンターに携帯やスマートフォンを持ち込めない環境

- 共有端末（PC/タブレット等）がある環境
- 個人端末（BYODを含む）での利用環境

4.2 ソリューションのユースケース

IceWall MFA とYubiKeyを利用したソリューションが活躍するユースケースと、YubiKey紛失や携帯忘れに対応する対策をご紹介します。

ユースケース一覧

① クラウドサービス・社内Webアプリケーション群の効率的な認証強化
② リモートワークにおける認証強化
③ 携帯やスマートフォンを持ち込めない環境における認証強化
④ 共有端末での個人認証強化
⑤ YubiKey紛失時のアクセス手段
⑥ YubiKey不携帯時のアクセス手段

ユースケース① クラウドサービス・社内Webアプリケーション群の効率的な認証強化

[課題] クラウドサービス・社内Webアプリケーション群を効率よくまとめて認証強化したい。

[対応] クラウドサービス・社内Webアプリケーションの認証をIceWall MFAによる統合認証基盤で統合し、IceWall MFA FIDO2オプションを導入。ユーザーにYubiKeyを配布する。

[導入効果] クラウドサービス・社内Webアプリケーションどちらにも手を入れることなく、YubiKey による認証強化が可能に。

ユースケース② リモートワークにおける認証強化

[課題] リモートワークを推進するにあたり社員が自宅から社内システムへ安全にアクセスできるよう認証を強化したいが、社員が使用するPCに生体認証機能が搭載されていない。

[対応]　FIDO2オプションを導入し、各社員にYubiKeyを配布する。

[導入効果] ユーザーが使用するPCの環境に依存することなくYubiKey による認証強化が可能に。

社員の利便性を落とすことなく、安全にシステムへアクセスできる。

ユースケース③ 携帯やスマートフォンを持ち込めない環境における認証強化

[課題] 利便性を考慮した多要素認証としてSMS OTPを導入したいが、データセンターなど携帯やスマートフォンの持ち込みが禁止されている環境では使用できない。

[対応] 上記環境で業務を行う社員を事前に登録し、YubiKeyを配布する。

- 通常利用の場合、IceWall MFAの認証方式選択機能（セレクター）を利用して、SMS OTPまたはFIDO2認証いずれかを選択できる画面を表示する。
- データセンターからのアクセスである場合、FIDO2認証のみを表示する。

[導入効果] SMS OTPを利用できない環境においてもYubiKeyによる認証強化が可能に。

社員が環境にかかわらず安全にシステムへアクセスできる。

ユースケース ④ 共有端末での個人認証強化

[課題] 共有端末でFIDO2認証を利用する場合、端末毎にユーザーの生体認証情報登録が必要、端末のOSアカウント上で複数ユーザーの生体認証情報が共有されてしまう。また、端末に登録できる生体認証の数に制限があり足りない。

[対応] 各ユーザーに個人用のYubiKeyを配布する。

[導入効果] YubiKeyは端末毎のユーザー情報の登録が不要なため、共有端末においてもパスワード（記憶）＋YubiKey (所持)よる認証強化が可能に。共有端末のセキュリティが向上。

※共有端末の例

サービス業店舗　(コンビニ、小売業、飲食店等)/学校/自治体(インターネット接続系PC共有)/コールセンター

ユースケース ⑤YubiKey紛失時のアクセス手段

[課題] 登録済みYubiKeyの紛失時にシステムにログインできない。

[対応] ユーザーに予め予備のYubiKeyも配布しておき、IceWall MFA の1アカウントに対して複数のYubiKeyを登録しておく。

[導入効果] YubiKey紛失時も、予備のYubiKeyでログイン可能に。ヘルプデスクへの問い合わせ・緊急対応などの運用負担も減少。

ユースケース ⑥ YubiKey不携帯時のアクセス手段

[課題] YubiKeyを忘れた場合に業務システムにログインできない。

[対応] 代わりとなる認証方式（スマートフォンのOTPソフトウェアトークンなど）を併用して、IceWall MFAの認証方式の選択機能（セレクター）にて提供する。

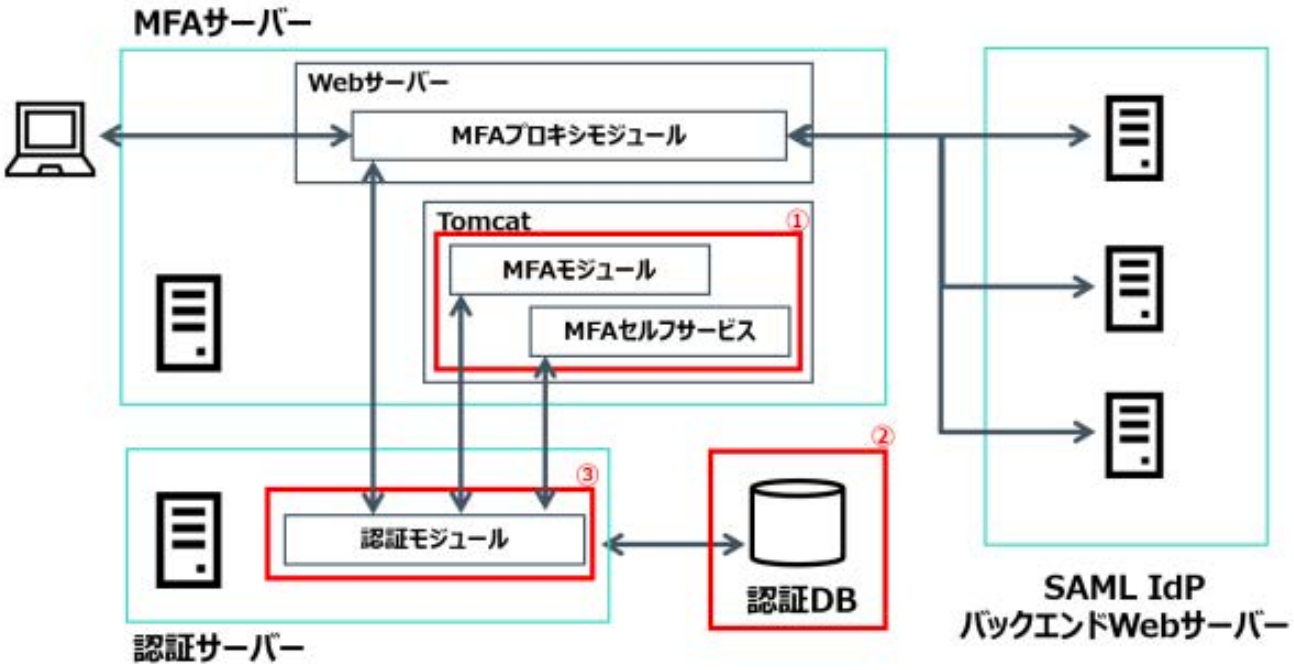
[導入効果] YubiKeyを忘れた場合にも別の認証方式で業務システムにログイン可能に。業務への影響を抑えられる。

5. IceWall MFAサーバーFIDO2オプション設定手順

IceWall MFAでYubiKeyを利用するためには、IceWall MFAサーバー側の設定と、ユーザー側でのFIDO2セキュリティキー登録設定が必要です。

本章では、IceWall MFAでYubiKeyを利用する際の、IceWall MFAサーバー側のFIDO2オプション設定についてご紹介します。

IceWall MFA FIDO2オプションは、IceWall MFAの各構成モジュール・認証DBに対して、以下の通り追加設定を行います。
詳細はIceWall MFA製品マニュアル（導入ガイド for FIDO2オプション）をご参照ください。



① MFAサーバーへのFIDO2オプションのインストール

FIDO2認証プラグイン・FIDO2セルフサービスをインストールします。

インストール後、MFAモジュールでFIDO2認証プラグイン（追加認証）を読み込むよう設定します。

/opt/icewall-mfa/mfa/config/mfa.conf

```
PLUG_IN=HELLO_ADD,config/plugin/hello/additional/hello.conf
```

FIDO2オプションの設定を行います。

/opt/icewall-mfa/self_service/config/self_hello/self_hello.conf
/opt/icewall-mfa/mfa/config/plugin/hello/additional/hello.conf

```
RPID=[ホスト名]
ORIGIN=https://[ホスト名]:[ポート番号]
```

設定後、Tomcatを再起動します。

② 認証DBの設定変更

認証テーブルにFIDO2認証で使用する以下のカラムを追加します。

表. FIDO2認証で使用するカラム

カラム名の例	必須	用途	型	サイズ
HELLO_LASTDATE	N	最終ログイン日付	文字型	14
HELLO_PREDATE	N	前回ログイン日付	文字型	14
HELLO_FAILDATE	N	ログイン失敗日付	文字型	14
HELLO_FAILCOUNT	N	認証失敗回数	数値型	3
HELLO_LOCKOUT	N	認証ロックフラグ	文字型	1
HELLO_LOCKDATE	N	認証ロック日付	文字型	14
HELLO_LOGINSTOP	N	認証停止フラグ	文字型	1
MFA_HELLO	Y	デバイス情報	文字型	4000
MFA_USERHANDLE	Y	ユーザーハンドル	文字型	30
MFA_CLGTIME	Y	チャレンジ発行日時	文字型	14

③　認証モジュールの設定変更

②で追加したカラムをFIDO2オプションで参照するよう設定します。

/opt/icewall-sso/certd/config/<使用する認証DB用ディレクトリ>/dbattr.conf

```
HELLO_LASTDATE=HELLO_LASTDATE
HELLO_PREDATE=HELLO_PREDATE
HELLO_FAILDATE=HELLO_FAILDATE
HELLO_RETRY=HELLO_FAILCOUNT
```

HELLO_LOCK=HELLO_LOCKOUT
HELLO_LOCKDATE=HELLO_LOCKDATE
HELLO_LOGINSTOP=HELLO_LOGINSTOP
HELLO=MFA_HELLO
HELLO_USERHANDLE=MFA_USERHANDLE
HELLO_CLGTIME=MFA_CLGTIME

/opt/icewall-sso/certd/config/<使用する認証DB用ディレクトリ>/cert.conf

AUTH_DEFINE=HELLO_ADD,HELLO_LASTDATE,HELLO_PREDATE,HELLO_FAILDATE,HELLO_RETRY,
HELLO_LOCK,HELLO_LOCKDATE,HELLO_LOGINSTOP

バックエンドWebサーバーへアクセスした際にパスワード認証＋FIDO2追加認証を求めるよう、認証ポリシーを設定します。

/opt/icewall-sso/certd/config/acl/child/child.acl

https://[アクセスURL]=[グループ名];;PW,HELLO_ADD

設定後、認証モジュールを停止・起動します。

6. ユーザー側のYubiKey設定手順

本章ではIceWall MFAでYubiKeyを活用するための、ユーザー側の設定手順と、利用イメージをご紹介します。

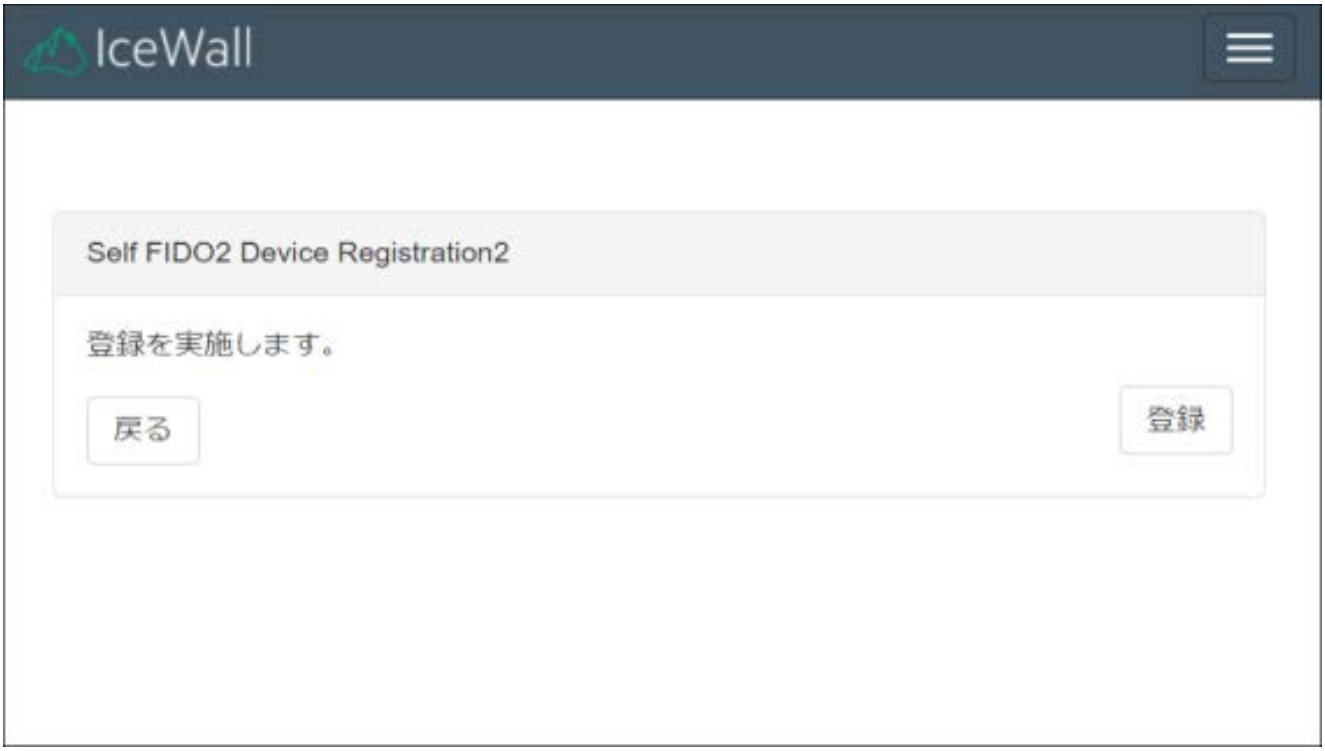
※ OSやブラウザの画面表示は、OSバージョンや環境設定により異なる場合がございます。
本レポートでは Windows10 21H1 の画面を掲載しています。

6.1 ユーザーによるYubiKey登録

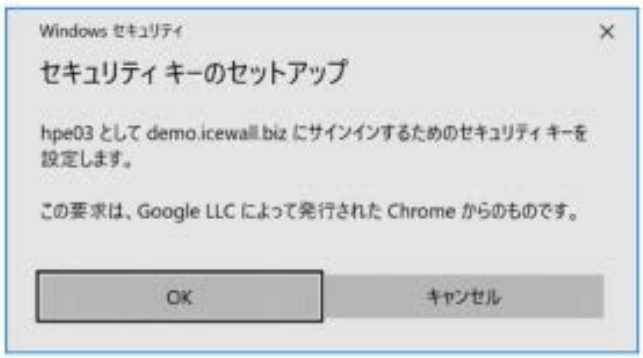
FIDO2認証に使用するデバイスとしてYubiKeyを登録します。

IceWallセルフサービスメニューにアクセスし、「デバイスの登録」をクリックします。

デバイスの名前を設定します。



「登録」をクリックします。

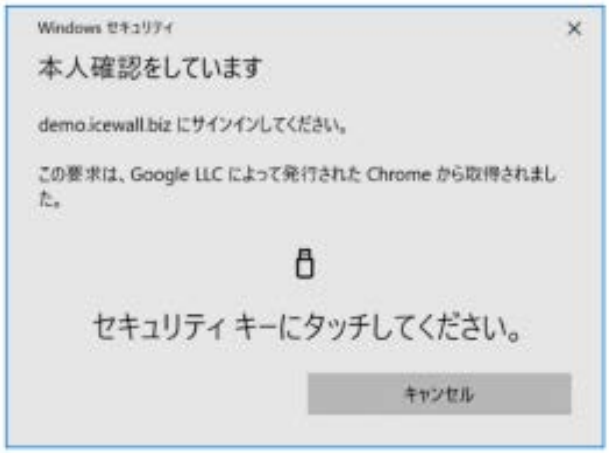


確認して「OK」をクリックします。

YubiKeyをUSBポートに挿入します。

YubiKeyに設定された暗証番号（PIN）を入力します。

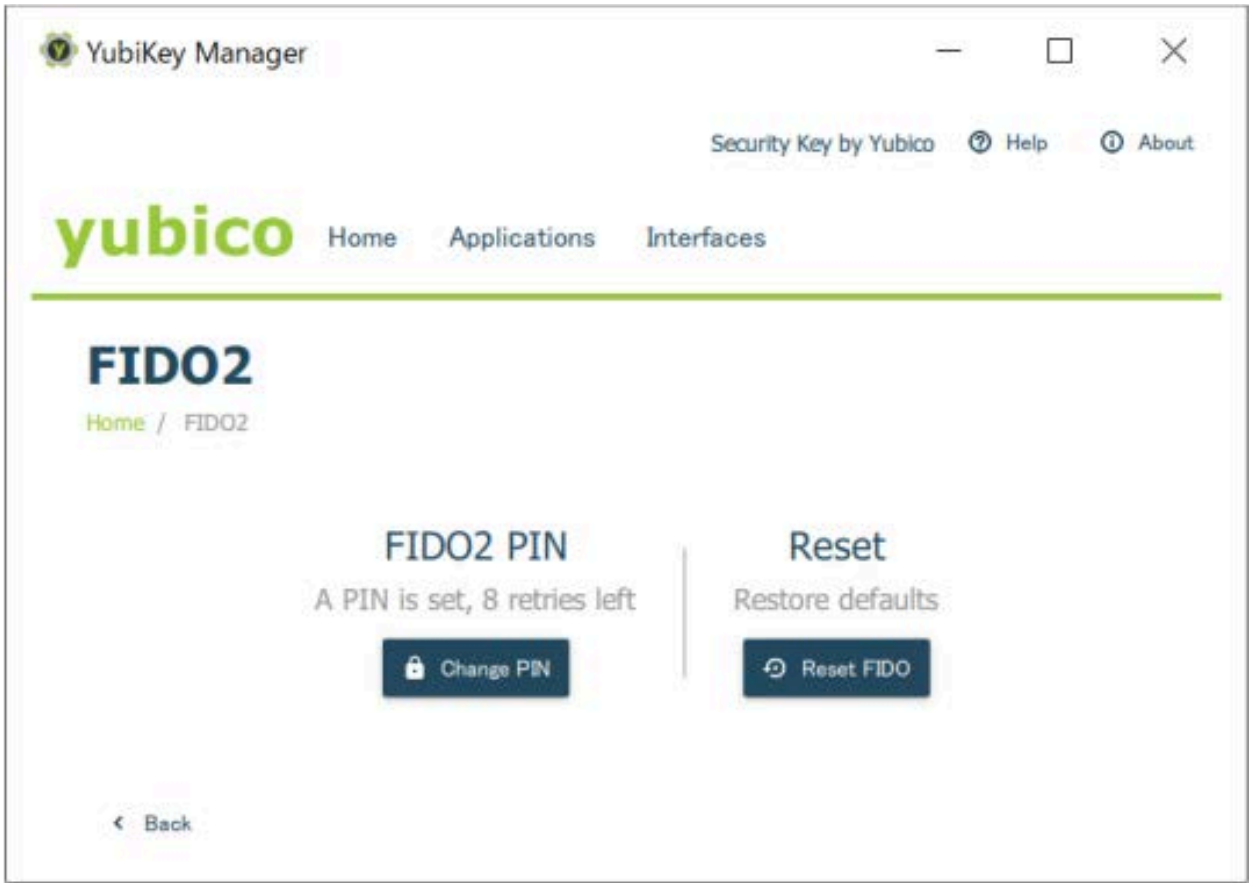
※YubiKeyにPINが設定されていない場合はPINを作成するよう求められます



YubiKeyにタッチします。

YubiKeyの登録が完了しました。

6.2 YubiKeyのPIN変更



YubiKeyではYubiKey Manager やWindows 10の設定アプリを使って、YubiKeyのPINの設定やリセットを行うことができます。

YubiKey Managerの詳細は以下ページをご参照ください。

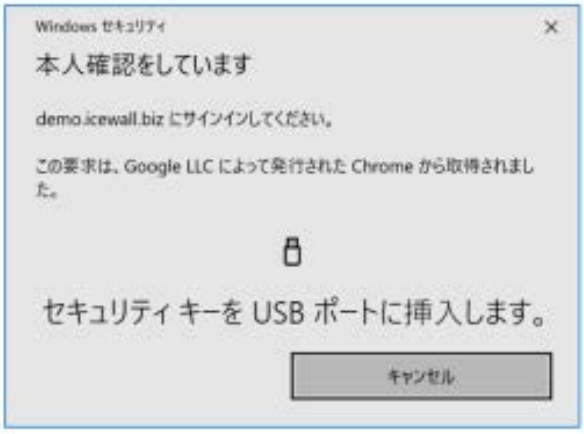
YubiKey Manager - Yubico（英語） →

7. ユーザーのYubiKey認証利用イメージ

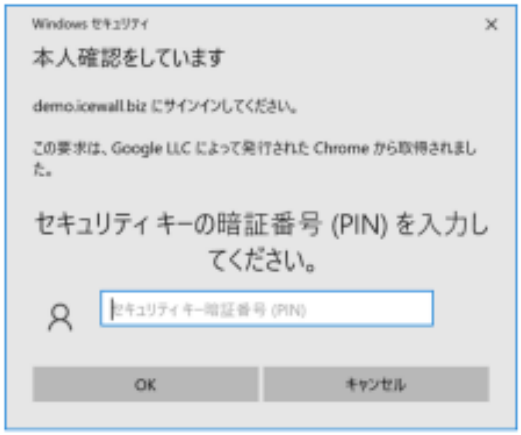
パスワード認証＋FIDO2追加認証が設定された社外クラウドサービスや社内システムに、ユーザーがアクセスした際の利用イメージをご紹介します。

バックエンドWebサーバーである社外クラウドサービスにアクセスすると、まずパスワード認証を求められます。

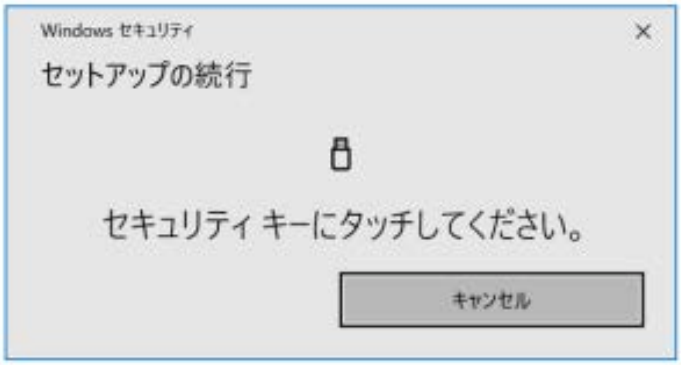
パスワード認証完了後、追加認証としてFIDO2認証が求められます。



YubiKeyをUSBポートに挿入します。



YubiKeyに設定された暗証番号（PIN）を入力します。



YubiKeyにタッチします。

FIDO2認証に成功してログインが完了し、社外クラウドサービスにアクセスできました。

SSOにより社内システムにもシームレスにアクセス可能です。

8. FIDOアライアンスの認定について

IceWall MFA FIDO2オプションは、これからの認証スタンダードとして期待されるFIDOアライアンスの認定を取得しています。FIDO2仕様に準拠しているとともに、セキュリティ面での要件をクリアしていることが検証された製品です。

FIDOアライアンスの詳細は以下ページをご参照ください。

FIDO Alliance - Open Authentication Standards More Secure than Passwords →

9. まとめ

本レポートではIceWall MFAでYubiKeyを活用した認証強化と利便性向上のシナリオについてご紹介しました。

YubiKeyを使用することで様々な環境を容易に認証強化できますので、是非ご検討ください。

2021.9.17　新規掲載

執筆者　：日本ヒューレット・パッカード合同会社

Pointnext事業統括　Pointnextデリバリー統括本部
クロス・インダストリー・ソリューション本部 認証コンサルティング部

藤 ひとみ

技術レポート一覧へ →

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ

HPE Japan ブログ

リソース

お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

日本 (ja)