IceWall技術レポート：

IceWall MFAによる多要素認証・認証ポリシーの効果的な設定方法

1. はじめに

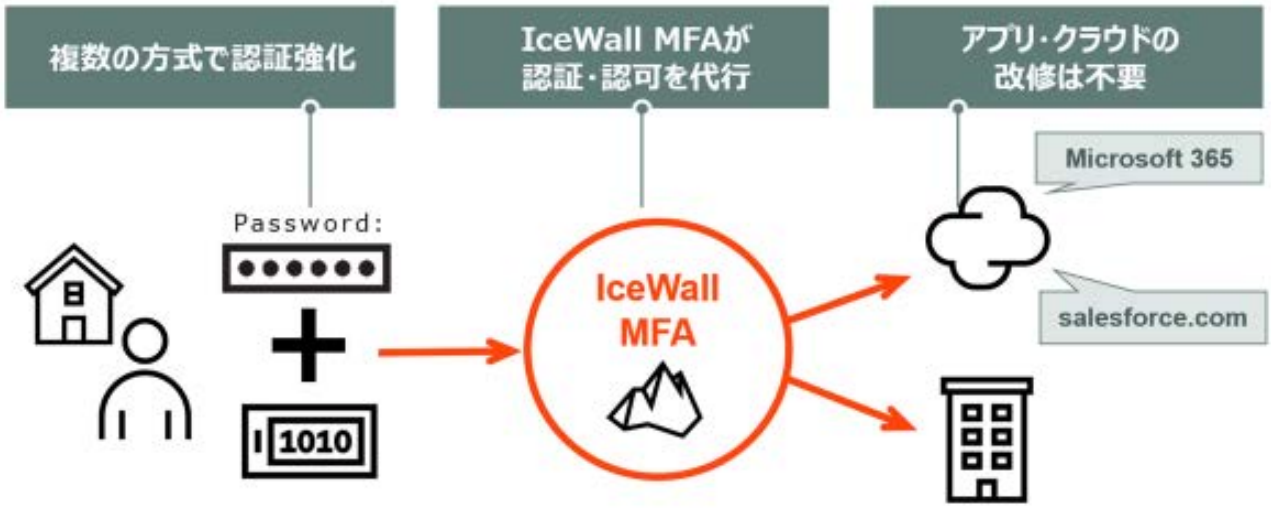
本レポートでは、実際の認証に関するニーズを例として、多要素認証プラットフォームのIceWall MFAによる多要素認証・認証ポリシーの設定方法をご紹介します。

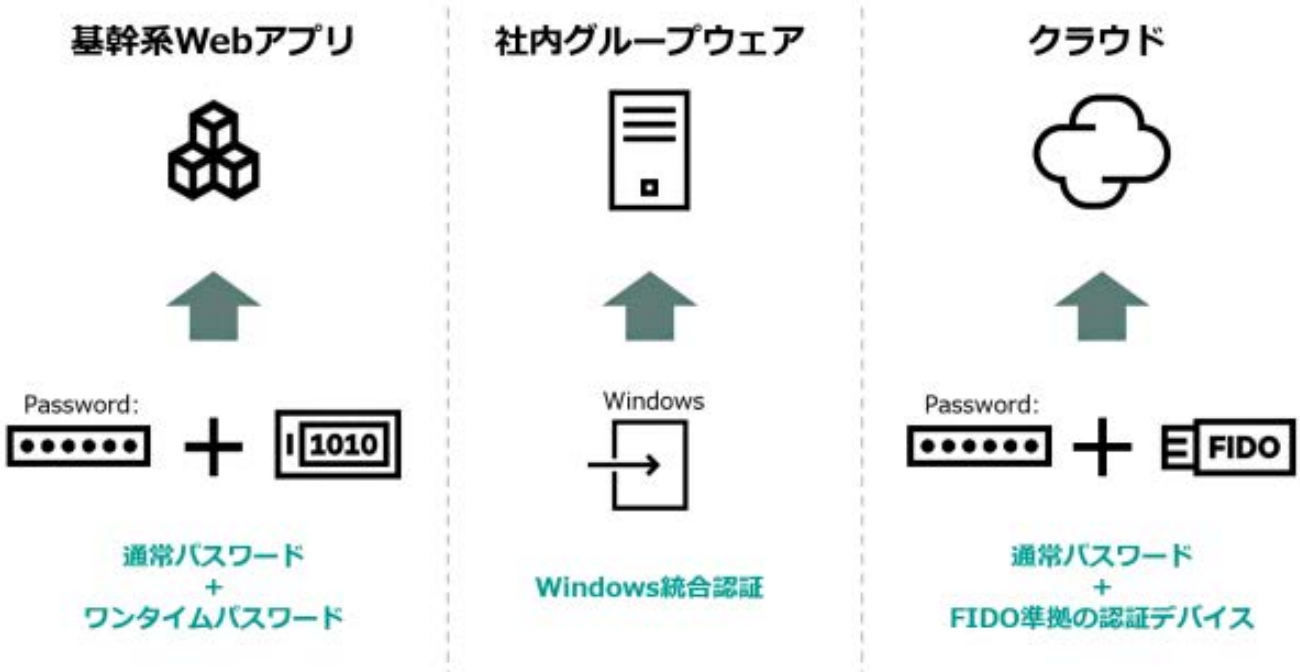
本書により、アクセス元やアクセス先など様々な条件に応じた認証方式の出し分けや、利便性とセキュリティのバランスを考慮した認証ポリシーの設定方法・具体的な動作イメージをご確認いただけます。

2.IceWall MFAとは

IceWall MFAは、アプリケーションやクラウドサービスを改修せずに、 多要素認証（Multi Factor Authentication）で認証を強化できるソリューションです。

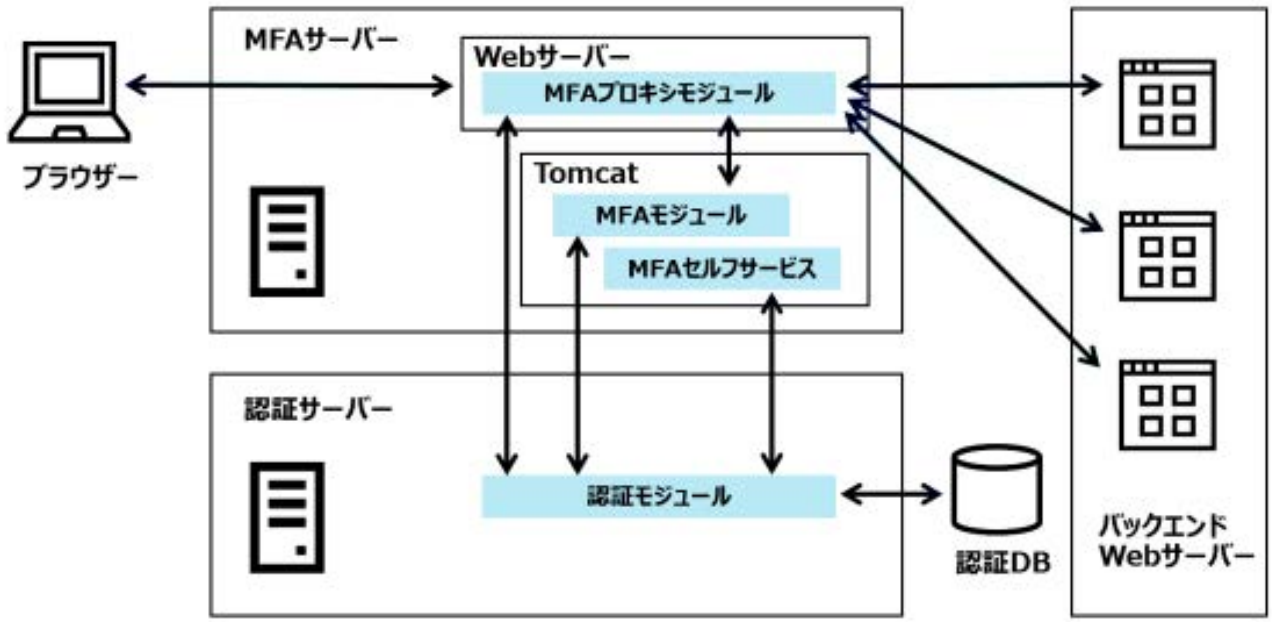
本ソリューションでは、各システムの認証要件に応じて、FIDO準拠の認証デバイス・ワンタイムパスワード・統合Windows認証・FIDO2仕様に基づく各デバイス標準の生体認証との連携、などの標準化された認証方法の組合せ（認証ポリシー）にて広い範囲のWebアプリやクラウドサービスを容易に認証強化することが可能です。
本ソリューションの機能については、IceWall MFA製品の機能をご参照ください。





3. 設定例のご紹介

本章では、代表的な多要素認証・認証ポリシーの設定例をご紹介します。



3.1. 環境の説明

以降の設定例に使用するIceWall MFAの環境をご説明します。

IceWall MFAは、次の4つのモジュールにより構成されます。

- MFAプロキシモジュール
  ユーザーからのリクエストを受け取り、バックエンドWebサーバーへのリクエストを代行するモジュールです。
- MFAモジュール
  MFA（多要素認証）機能のユーザーインターフェイス、および認証ロジックを提供するモジュール群です。認証モジュールと連携してユーザーを認証して、セッションIDをユーザーに返却します。
- 認証モジュール
  MFAモジュールからリクエストを受け、認証DBに認証情報の問い合わせを行い、セッションIDを作成して管理します。
- MFAセルフサービス
  ユーザーが自分のMFA認証に関連する設定を管理するための画面群です。

本技術レポートでご紹介する多要素認証・認証ポリシーは、上記各モジュールの設定により実装を行います。

本書では、特にその設定方法と実際の認証動作について、ご紹介させていただきます。

なお、MFAモジュールには、各多要素認証機能用のIceWall MFA認証プラグインモジュールが各製品の導入ガイドに従って、インストール・設定済みで、MFAプロキシモジュールには、バックエンドWebアプリの例として、旅費精算システム（https://travel-expense.icewall.local)、ユーザー情報管理システム（https://mfaserver01.icewall.local/MENU/iwmgr/Controller/）の2システム分のリバースプロキシ接続設定・アクセスURLの割り当てまで行われているものとします。

3.2. 設定例１（FIDO2パスワードレス認証）

Webアプリへのアクセス時の認証を、FIDO2仕様に基づく各デバイス標準の生体認証等と連携したFIDO2パスワードレス認証にする場合について、ご説明します。

①認証ポリシー設定の変更

認証モジュールのアクセスコントロールファイルにおいて、Webアプリのアクセス URL行に、FIDO2パスワードレス認証を示す認証名 "HELLO" を設定します。

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

```
https://travel-expense.icewall.local/=ALL;;HELLO
```

②認証ポリシー設定の再読み込み

設定変更後に以下の設定ファイル再読み込みコマンドを実行することで、設定変更内容が反映され、設定した認証ポリシーが有効となります。

```
# /opt/icewall-sso/certd/bin/reload-cert
```

以上でサーバー側の設定は完了となります。

③FIDO認証用のデバイス登録

FIDO認証を行う場合は、IceWallのユーザーにおいて、クライアント端末のデバイス登録作業が必要となります。ここでは、Windows 10端末（FODO認証器としてWindows Helloを使用）の場合の例をご紹介します。

Windows10端末では、まず事前にOSにおいて、Windows Helloの認証設定（PIN、指紋認証など）を行っておきます。
次に、ブラウザよりIceWall MFAセルフサービスにアクセスします。セルフサービス画面から「Helloデバイスの登録」メニューを選択し、デバイス名を指定して「登録」ボタンを押下します。
Windowsセキュリティのダイアログが表示されますので、Windows Helloで登録済みの認証方式を選択してWindows Helloの認証を行います。その後、デバイス登録完了画面が表示されましたら登録完了となります。

以上で、クライアント側の設定は完了となります。

④FIDO2パスワードレス認証の認証画面遷移

ブラウザーでFIDO2パスワードレス認証を設定したWebアプリへアクセスすると、IceWall MFAのHello認証画面が表示されます。認証ボタンを押下すると、Windowsセキュリティのダイアログが表示されますので、Windows Helloで登録済みの認証方式を選択してWindows Helloの認証を行います。認証OKの場合はWebアプリ画面が表示されます。

3.3. 設定例２（パスワード認証＋メールOTP追加認証）

Webアプリへのアクセス時の認証を、パスワードによる認証に加えて、別の認証方式でのユーザーの確認を行うようにする場合について、ご説明します。

①認証ポリシー設定の変更

認証モジュールのアクセスコントロールファイルにおいて、Webアプリのアクセスurlの行に、パスワード認証に加えてメールOTP追加認証（ユーザーにメールで通知されるワンタイムパスワードの入力による認証）を要求する認証名 “PW,MOTP” を設定します。

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

https://travel-expense.icewall.local/=ALL;;PW,MOTP

②認証ポリシー設定の再読み込み

設定変更後に以下の設定ファイル再読み込みコマンドを実行することで、設定変更内容が反映され、設定した認証ポリシーが有効となります。

```
# /opt/icewall-sso/certd/bin/reload-cert
```

以上でサーバー側の設定は完了となります。

③パスワード認証に加えてメールOTP追加認証を要求する場合の認証画面遷移

ブラウザーでWebアプリへアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。ユーザーID・パスワードを入力してログインボタンを押下します。次にメールOTP追加認証画面が表示されますので、ユーザーにメールで通知されるワンタイムパスワードを入力して送信ボタンを押下します。入力したワンタイムパスワードが正しければ、Webアプリ画面が表示されます。

3.4. 設定例3（社外アクセス時の追加認証）

社外アクセス環境（社内IPアドレス範囲の外の環境）からWebアプリへアクセスした際に、追加認証を実施する場合についてご説明します。

①拡張認証文法（RICH認証）の設定

認証モジュールの拡張認証文法ファイルにおいて、拡張認証文法（RICH認証）を設定します。ここでは、拡張認証文法の名前（RICH認証名）を“@auth01”として、社内IPアドレスからのアクセスはパスワード認証、それ以外からのアクセスはパスワード認証に加えてメールOTP認証を実行する条件式を以下のように設定します。

※社内IPアドレス範囲を192.168.23.0/24としています。

/opt/icewall-sso/certd/config/acl/child/rich.auth 設定例

```
@auth01{
if(REMOTE_ADDR=192.168.23.0-192.168.23.255){
PW
}else{
PW,MOTP
}
}
```

②認証ポリシー設定の変更

認証モジュールのアクセスコントロールファイルにおいて、Webアプリのアクセスの行に、先ほど設定したRICH認証名“@auth01”を設定します。

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

```
https://travel-expense.icewall.local/=ALL;;@auth01
```

③認証ポリシー設定の再読み込み

設定変更後に以下の設定ファイル再読み込みコマンドを実行することで、設定変更内容が反映され、設定した認証ポリシーが有効となります。

```
# /opt/icewall-sso/certd/bin/reload-cert
```

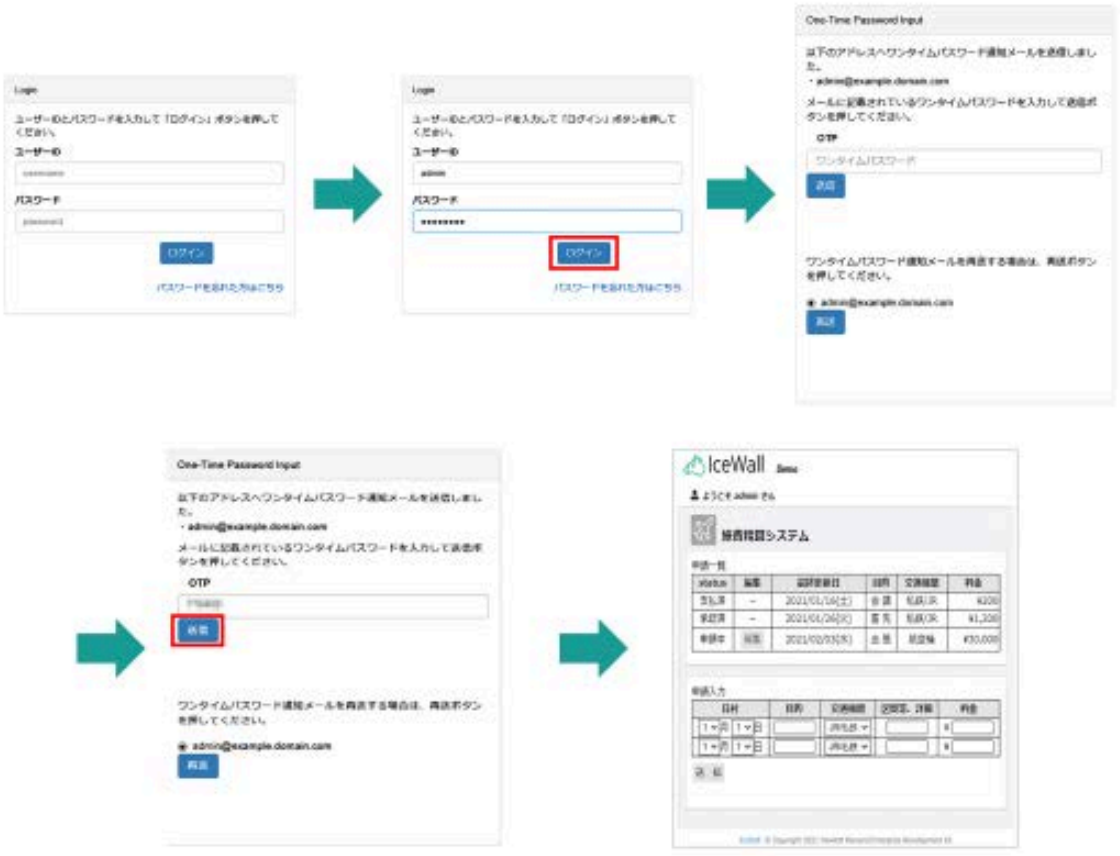
以上でサーバー側の設定は完了となります。

④社内IPアドレスからアクセス時の認証画面遷移

社内IPアドレスの端末のブラウザーでWebアプリへアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。ユーザーID・パスワードを入力してログインボタンを押下します。社内IPアドレスからのアクセスのためパスワード認証のみでWebアプリ画面が表示されます。

⑤社外IPアドレスからアクセス時の認証画面遷移

社外IPアドレスの端末のブラウザーでWebアプリへアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。ユーザーID・パスワードを入力してログインボタンを押下します。社外IPアドレスからのアクセスのためメールOTP追加認証画面が表示されますので、ユーザーにメールで通知されるワンタイムパスワードを入力して送信ボタンを押下します。入力したワンタイムパスワードが正しければ、Webアプリ画面が表示されます。



3.5. 設定例4（ユーザー属性の条件による追加認証）

ログインするユーザーの属性情報の条件によって、追加認証を実施するかどうか制御する場合についてご説明します。
また、社内IPアドレス範囲からのアクセスのみに限定する設定も合わせて行う例をご紹介します。

①拡張認証文法（RICH認証）の設定

認証モジュールの拡張認証文法ファイルにおいて、認証ポリシーに設定する拡張認証文法（RICH認証）を設定します。ここでは、定義する拡張認証文法の名前（RICH認証名）を“@auth02”として、社内IPアドレス範囲（192.168.23.0/24）からのアクセスの条件下において、役割の属性（ROLE）が管理者（"PM”または”M”）であるユーザーにはパスワード認証に加えてメールOTP認証を実行し、その他のユーザーにはパスワード認証を行う条件式を以下のように設定します。

/opt/icewall-sso/certd/config/acl/child/rich.auth 設定例

```
@auth02{
if(REMOTE_ADDR=192.168.23.0-192.168.23.255){
if(ROLE="^PM$"|ROLE="^M$"){
PW,MOTP
}else{
PW
}
}
}
```

②認証ポリシー設定の変更

認証モジュールのアクセスコントロールファイルにおいて、Webアプリのアクセスurlの行に、先ほど設定したRICH認証名“@auth02”を設定します。

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

```
https://travel-expense.icewall.local/=ALL;;@auth02
```

③認証ポリシー設定の再読み込み

設定変更後に以下の設定ファイル再読み込みコマンドを実行することで、設定変更内容が反映され、設定した認証ポリシーが有効となります。

```
# /opt/icewall-sso/certd/bin/reload-cert
```

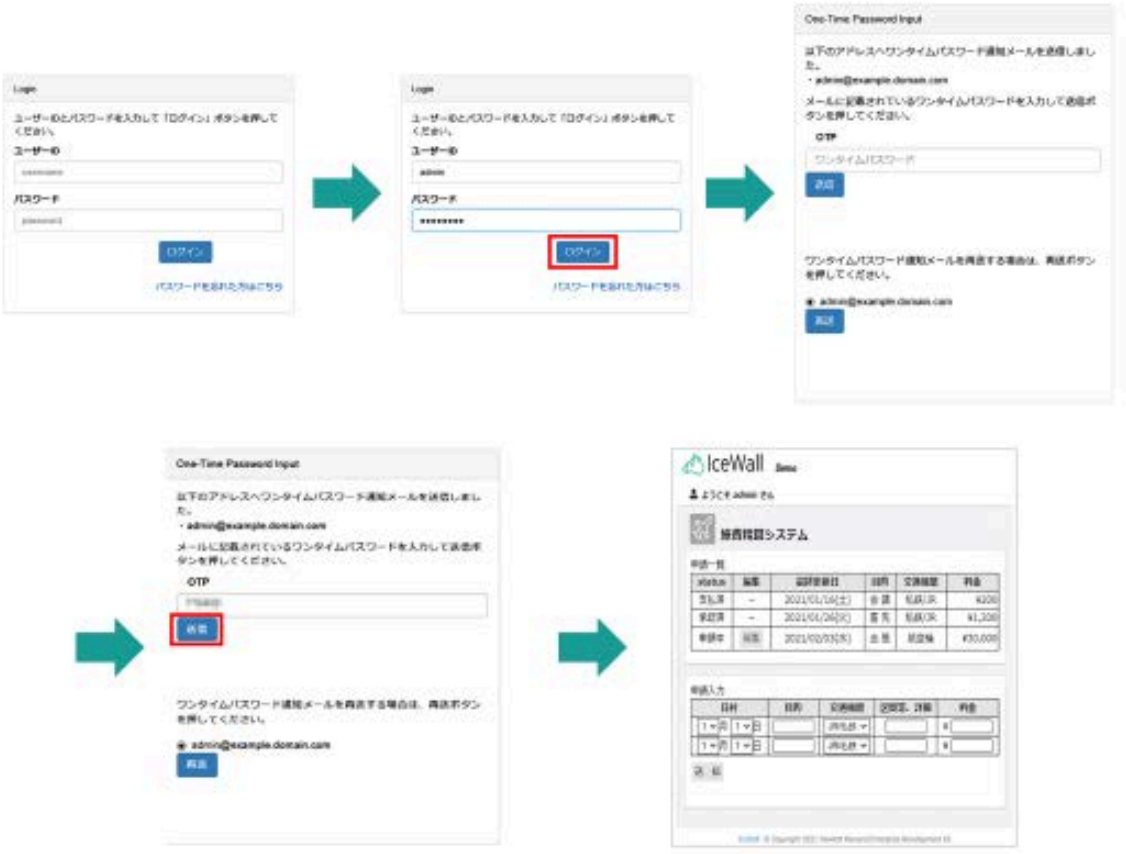
以上でサーバー側の設定は完了となります。

④社内IPアドレスから一般ユーザーでアクセス時の認証画面遷移

社内IPアドレスの端末のブラウザーでWebアプリへアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。一般ユーザーのユーザーID・パスワードを入力してログインボタンを押下します。一般ユーザーでのアクセスのためパスワード認証のみでWebアプリ画面が表示されます。

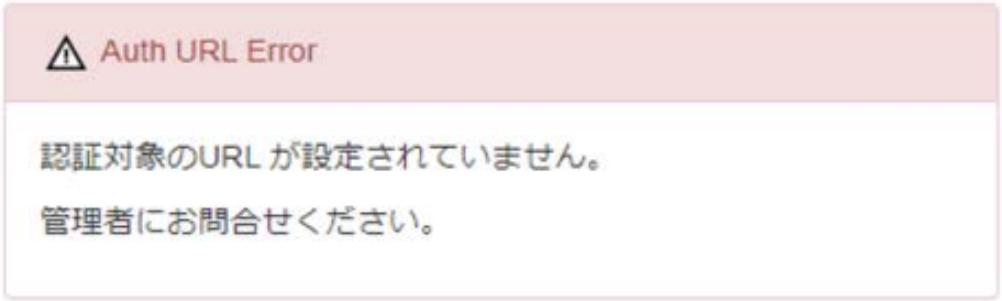
⑤社内IPアドレスから管理者ユーザーでアクセス時の認証画面遷移

社内IPアドレスの端末のブラウザーでWebアプリへアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。管理者ユーザーのユーザーID・パスワードを入力してログインボタンを押下します。管理者ユーザーでのアクセスのためメールOTP追加認証画面が表示されます。追加認証が完了するとWebアプリ画面が表示されます。



⑥社外IPアドレスからアクセス時の認証画面遷移

社外IPアドレスの端末のブラウザーでWebアプリへアクセスすると、認証ポリシーの設定外のため、認証対象のURLが設定されていない旨のエラーが表示され、Webアプリへのアクセスはブロックされます。



3.6. 設定例5（機密コンテンツアクセス時の追加認証）

標準的なコンテンツへのアクセス時にはパスワード認証のみを要求し、機密コンテンツへのアクセス時にはパスワード認証に加えて、別の認証方式でのユーザーの確認を行うようにする場合について、FIDO追加認証を要求する場合についてご説明します。

①認証ポリシー設定の変更

ここでは、例として、旅費精算システム（https://travel-expense.icewall.local）を標準的なコンテンツ、ユーザー情報管理システム（https://mfaserver01.icewall.local/MENU/iwmgr/Controller/）を機密コンテンツとします。
認証モジュールのアクセスコントロールファイルにおいて、旅費精算システムのアクセスURLの行にはパスワード認証の認証名 “PW”、ユーザー情報管理システムのアクセスURLの行にはパスワード認証に加えてFIDO追加認証を要求する認証名 “PW,HELLO” を設定します。

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

```
https://travel-expense.icewall.local/=ALL;;PW
https://mfaserver01.icewall.local/MENU/iwmgr/Controller/=ALL;;PW,HELLO
```

②認証ポリシー設定の再読み込み

設定変更後に以下の設定ファイル再読み込みコマンドを実行することで、設定変更内容が反映され、設定した認証ポリシーが有効となります。

```
# /opt/icewall-sso/certd/bin/reload-cert
```

③機密コンテンツアクセス時の認証画面遷移

ブラウザーで旅費精算システムにアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。ユーザーID・パスワードを入力してログインボタンを押下するとWebアプリ画面が表示されます。次に同じブラウザ（セッションを保持した状態）でユーザー情報管理システムにアクセスします。既にパスワード認証を行っているため、追加認証のHello認証画面が表示されます。登録したFIDOデバイスで認証をすることでユーザー情報管理システムの画面が表示されます。

（旅費精算システムにアクセス）

（ユーザー情報管理システムにアクセス）

3.7. 設定例6（ユーザーによる認証方式の選択）

Webアプリへのアクセス時の認証方式をユーザーがその場で選択できるようにする場合について、ご説明します。

①認証ポリシー設定の変更

認証モジュールのアクセスコントロールファイルにおいて、Webアプリのアクセスurlの行に、ユーザーがパスワード認証・統合Windows認証を選択できるようにする認証名 “S[PW,IWA]” を設定します。

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

```
https://travel-expense.icewall.local/=ALL;;S[PW,IWA]
```

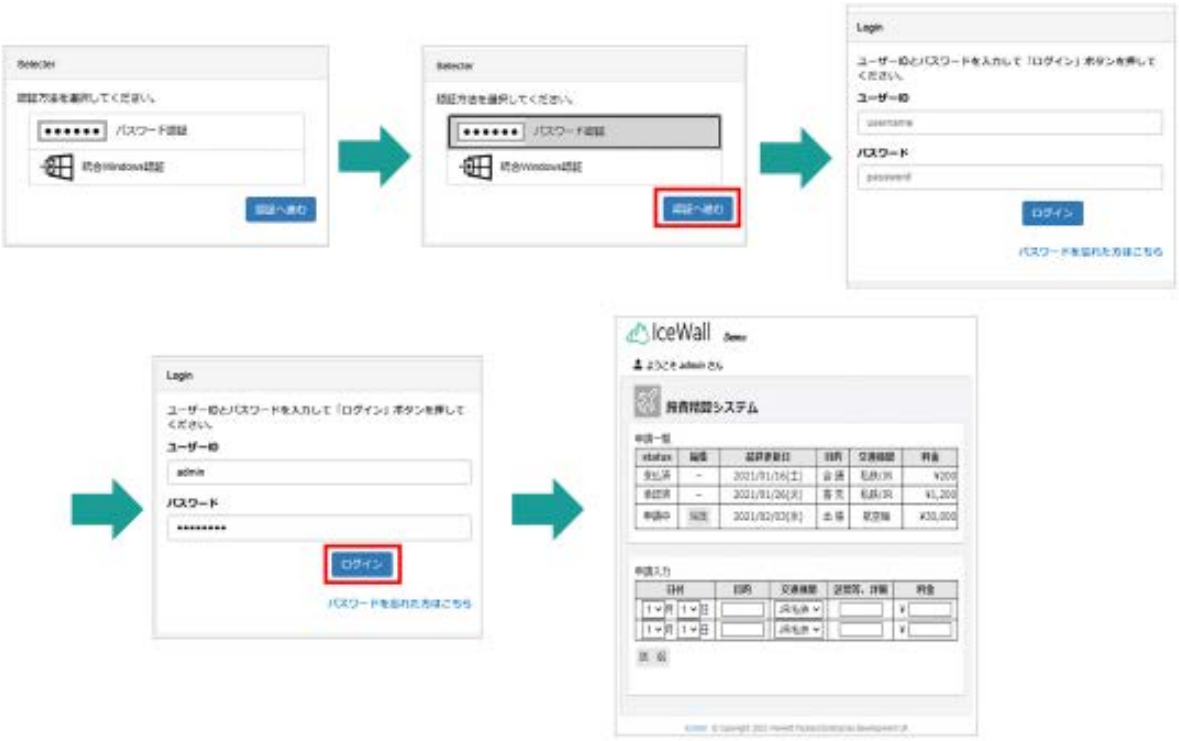
②認証ポリシー設定の再読み込み

設定変更後に以下の設定ファイル再読み込みコマンドを実行することで、設定変更内容が反映され、設定した認証ポリシーが有効となります。

```
# /opt/icewall-sso/certd/bin/reload-cert
```

③認証方式選択画面からパスワード認証を選択した場合の認証画面遷移

ブラウザーでWebアプリへアクセスすると、認証方式選択画面が表示されます。パスワード認証を選択した後に「認証へ進む」ボタンを押下します。IceWall MFAのパスワードログイン画面が表示されますので、ユーザーID・パスワードを入力してログインボタンを押下するとWebアプリ画面が表示されます。



④認証方式選択画面から統合Windows認証を選択した場合の認証画面遷移

ブラウザーでWebアプリへアクセスすると、認証方式選択画面が表示されます。統合Windows認証を選択した後に「認証へ進む」ボタンを押下すると統合Windows認証の認証処理が実行されWebアプリ画面が表示されます。

3.8. 設定例7（追加認証実施済みブラウザーでの次回以降の追加認証の省略）

追加認証時に普段利用するブラウザーとして登録することで、次回以降の一定期間内の同じブラウザーからのアクセス時には追加認証を省略できる機能（ブラウザートークン機能）を有効にする場合についてご説明します。

①追加認証プラグインへのブラウザートークンプラグインの設定

既に設定例2の設定が行われているものとします。その上で、メールOTP認証プラグインにブラウザートークンプラグインを設定する場合には、メールOTP認証プラグイン設定ファイルにおいて、以下の設定を行います。

/opt/icewall-mfa/mfa/config/plugin/motp/motp.conf 設定例

```
PRE_PROCESS=BT_PRE
POST_PROCESS=BT_POST
```

②サービスの再起動

設定変更後にTomcatの再起動を実行することで、メールOTP認証プラグインの設定変更内容が反映されます。

```
# systemctl restart tomcat
```

※systemctlコマンドを使用する際は、事前にsystemdのサービス設定がされている必要があります。

③初回認証時の画面遷移

ブラウザーでWebアプリへアクセスすると、IceWall MFAパスワードログイン画面が表示されます。パスワード認証・メールOTP追加認証後に、初回認証時のブラウザー登録画面が表示されます。普段利用するブラウザーとして登録する場合は「登録する」ボタンを押下します。その後、Webアプリ画面が表示されます。

④普段利用するブラウザーとして登録後の認証時の画面遷移

同じブラウザーを再起動して、Webアプリへアクセスすると、IceWall MFAのパスワードログイン画面が表示されますので、ユーザーID・パスワードを入力してログインボタンを押下します。普段利用するブラウザーとして登録済みのためパスワード認証のみでWebアプリ画面が表示されます。

※普段利用するブラウザーとして登録していなかった場合は、ここでもメールOTP追加認証が行われ、ブラウザー登録画面が表示されます。

3.9. 設定例8（特定URLへのアクセス時の再認証）

既に認証済みの状態であっても、特定のURLへのアクセス時には再度認証させる場合についてご説明します。

①再認証対象URL用の設定

ここでは、例として、ユーザー情報管理システム（https://mfaserver01.icewall.local/MENU/iwmgr/Controller/）を再認証対象のコンテンツとします。
MFAモジュール設定ファイルにおいて、再認証対象URLと再認証でパスワード認証を要求する認証名”PW” を以下のように設定します。

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

```
RE_AUTH=https://mfaserver01.icewall.local/MENU/iwmgr/Controller/,PW
```

MFAプロキシモジュールが動作するWebサーバー（Apache HTTP Server）の設定ファイルにおいて、次のように設定します。

/etc/httpd/conf/httpd.conf　設定例

```
< Location ~ "^/(?!MENU/iwmgr/Controller/)" >                ・・・※1

IWAUTH DFW
IWCONFIG /opt/icewall-mfa/proxy/agent/config/agent.conf
IWCONFID AGENT
```

< /Location >

< Location /MENU/iwmgr/Controller/ > ・・・※2

IWAUTH DFW
IWCONFIG /opt/icewall-mfa/proxy/agent/config/agent_reauth.conf
IWCONFID AGENT_REAUTH

< /Location >

※1 通常の認証で使用するエージェントの動作パスを設定（再認証対象URL以外で動作するように設定）
※2 再認証用エージェントの動作パスを設定（再認証対象URLで動作するように設定）

再認証用エージェントの設定ファイルを作成し、次のように設定します。

/opt/icewall-mfa/proxy/agent/config/agent_reauth.conf　設定例

```
AGENT_PATH=/MENU/iwmgr/Controller/agt          ・・・※1
COOKIENAME=IW_INFO_REAUTH                      ・・・※2
SESSION_ENC_KEY=Agent_Enc.Key-1!               ・・・※3
```

※1 認証情報を転送させるパスを再認証対象URLの配下に設定
※2 セッションIDを保持するcookie名は、通常の認証で使用するエージェントと異なるものを設定
※3 通常の認証で使用するエージェントと異なるセッションID値にするためセッションIDを暗号化

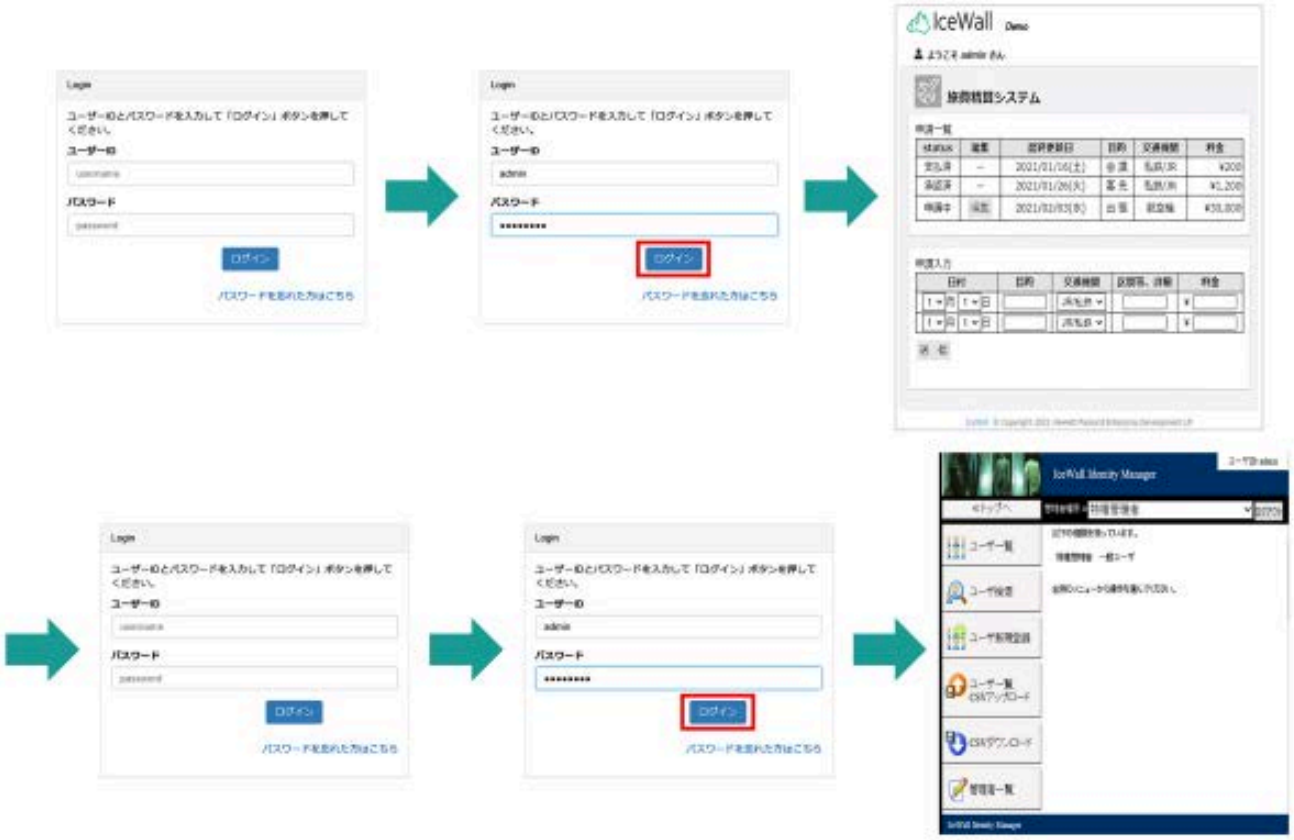
②サービスの再起動

設定変更後にTomcat・Apache HTTP Serverの再起動を実行することで、設定変更内容が反映されます。

```
# systemctl restart tomcat
# systemctl restart httpd
```

③認証時の画面遷移

ブラウザーで旅費精算システムにアクセスすると、IceWall MFAのパスワードログイン画面が表示されます。ユーザーID・パスワードを入力してログインボタンを押下するとWebアプリ画面が表示されます。次に同じブラウザ（セッションを保持した状態）でユーザー情報管理システムにアクセスします。再認証対象として設定されているため、再度IceWall MFAのパスワードログイン画面が表示されます。再度パスワード認証を行うことでユーザー情報管理システムの画面が表示されます。



4.まとめ

本レポートではIceWall MFAによる代表的な多要素認証・認証ポリシーの設定方法についてご紹介しました。
IceWall MFAではWebアプリ側の変更なしに、認証システムの設定のみで多要素認証や柔軟な認証の制御を容易に実装可能ですので、是非ご検討ください。

2021.6.4

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

鈴木 豪士

技術レポート一覧へ →

お探しの情報は見つかりましたか？

検索のサポート

ご購入方法

製品サポート

営業へのお問い合わせ

お問い合わせ先一覧

企業情報

会社情報

アクセス

お問い合わせ

採用情報

HPEについて

インクルージョン & ダイバーシティ

サステナビリティと企業責任

経営幹部

お知らせ

ニュースルーム

イベント・セミナー

新着情報

重要なお知らせ

パートナー

パートナープログラム

認定資格制度

OEMソリューション

サポート

製品サポート

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