

HP IceWall SSO

HP IceWall技術レポート:フォーム認証特集!

どうする既存の認証?
フォーム認証特集!



- » フォーム認証とは?
- » 自動フォーム認証機能とは
- » 自動フォーム認証機能の使い方

自動フォーム認証機能

さまざまな既存のWebアプリケーションのシングル・サイン・オンを可能とするHP IceWall SSO。その導入時によく問題となるのが「既存のWebアプリケーションで構築済みの認証部分をどうするか?」であるかだと思います。HP IceWall SSOを導入する際に既存の認証部分を削除できれば問題はありませんが、アプリケーションの構築上や、すでに運用されているために変更できないことは少なくありません。このような問題をクリアするために、バージョン7.0で新たに搭載された機能が「自動フォーム認証機能」です。

今回の特集ではその自動フォーム認証機能の基本的な使い方をご紹介します。なお、ここではある程度のHTMLに関する知識を必要とします。HTMLに関してわからない部分がある場合には市販の書籍等を参照してください。

フォーム認証とは?

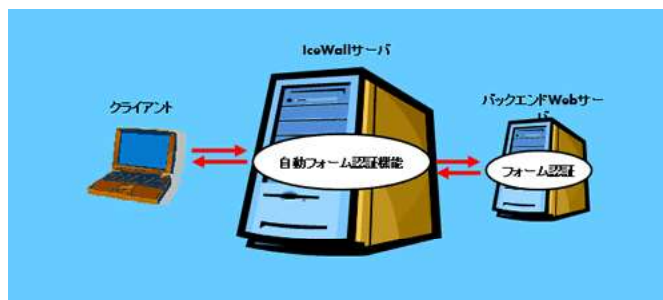
自動フォーム認証機能の解説をする前に、まず「フォーム認証」とは何かをご説明いたします。フォーム認証とは、Webサーバが標準で搭載している認証機能の「基本(Basic)認証機能」とは異なり、ユーザが入力画面を自由に作成でき、必要な情報を自由に送信して認証を行う認証方法です。例えば、ユーザIDとパスワードの他にEメールアドレスを入力して認証する、などです。フォーム認証は、データの送信方法が3通り、認証後のセッション管理方法が4通り、認証後の動作が4通りの計11通りの方法があります。その内容は次のようになります。

データ送信方法	POSTデータ
	Query String
	PostデータとQuery String
認証後のセッション管理方法	Cookieによるブラウザへの通知
	URLへのセッション情報埋め込み
	Query Stringによるブラウザへの通知
	管理なし
認証後の動作	Locationヘッダによるリダイレクト(別URLへ)
	Locationヘッダによるリダイレクト(同じURLへ)
	Refreshによるリダイレクト
	リダイレクトなしのコンテンツ

これらを組み合わせて任意のフォーム認証を構築します。

自動フォーム認証機能とは

自動フォーム認証機能とは、お客さまが作成されたフォーム認証に対してシングル・サイン・オンを実現し、既存のWebアプリケーションに手を加えることなくシームレスかつ、簡単に接続する機能です。HP IceWall SSOでは先にご紹介しました11方式のフォーム認証に対応しており、その組み合わせによって48パターンのフォーム認証形式に対応しているため、ほぼ全てのフォーム認証で使用することが可能となっています*。
* 認証方式によっては使用できない場合があります。

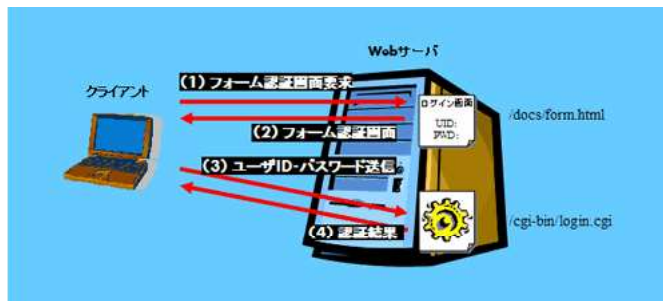


従来のHP IceWall SSOや他のシングル・サイン・オン製品では簡易的なもののみ対応しているか、または既存のフォーム認証に合わせて作り込みをしなければなりませんでした。自動フォーム認証機能では設定を行うのみのため、低コストかつスピーディーに対応することが可能となっています。

自動フォーム認証機能の使い方

1. 導入するフォーム認証の動作を理解する

この機能を使うには、まず、既存のフォーム認証がどのような構成で動作しているのかを理解しなければなりません。理解するポイントとしては「データを入力する画面はどこにあるのか」、「入力画面はどれか」「データは何で送信するのか」「データは何が必要か」「データはどこへ送信されるのか」「認証後はどうなるのか」になります。次の図のようなフォーム認証の場合を考えてみましょう。なお、認証方法は「ユーザIDとパスワードを入力する」ものとなります。



このフォーム認証の構成から、「データを入力する画面はどこにあるのか」にあたるフォーム認証画面のURLは「/docs/form.html」であること、「データはどこへ送信されるのか」にあたるユーザIDおよびパスワードの送信先URLはフォーム認証画面と異なるURLで「/cgi-bin/login.cgi」であることがわかります。さらに、「認証後はどうなるのか」にあたる認証後の動作は「認証結果が表示される」になることがわかります。

2. 設定を行うための情報を収集する

次にフォーム認証用CGIが動作するために「データは何で送信するのか」「データは何が必要か」を理解します。この動作を理解するためには、フォーム認証を行う画面のHTMLソースを参照します。上の例のフォーム認証が以下のようなHTMLソースの場合を考えてみましょう。

■ フォーム認証画面のHTMLソース

```
<HTML>
<HEAD>
<TITLE>フォーム認証</TITLE>
</HEAD>
<BODY>
<FORM METHOD="POST" ACTION="/cgi-bin/login.cgi">
  <INPUT TYPE="text" NAME="userid">
  <INPUT TYPE="password" NAME="password">
  <INPUT TYPE="submit" NAME="submit" VALUE="ログイン">
</FORM>
</BODY>
</HTML>
```

ここで注目するのは「データは何で送信するのか」にあたる「動作メソッド」、「データは何が必要か」にあたる「送信するデータ」です。データの送信先についてもここで知ることができます。

- 動作メソッドは<FORM>タグのMETHOD属性で指定されているものになります。ここでは「POST」となります。
- 送信するデータは<FORM>タグと</FORM>タグの間に記述された<INPUT>タグが対象となります。ここで対象となるのは次の2つになります。


```
<INPUT TYPE="text" NAME="userid">
<INPUT TYPE="password" NAME="password">
```

 なお、「<INPUT TYPE="submit" NAME="submit" VALUE="ログイン">」はログインするためのボタンを表示するための記述のため、対象にはなりません。

また、ここでは触れていませんでしたが、「データはどこへ送信されるのか」にあたる「データ送信先」は<FORM>タグのACTION属性で指定されているものになります。ここでは「/cgi-bin/login.cgi」となります。（これはフォーム認証の構造の時点で判明しています）

ここまでの「動作の理解」と「必要な情報の収集」でフォーム認証が以下のように動作することがわかります。

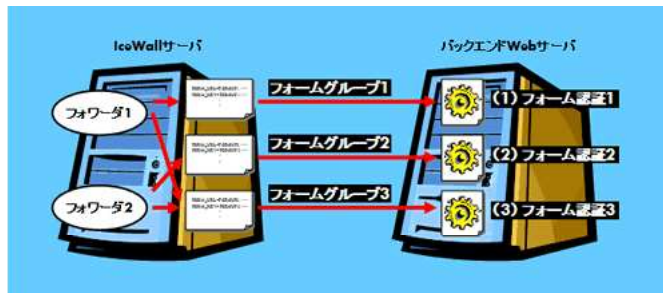
どこに	フォーム認証画面	/docs/form.html
どれか	判断用キーワード	
何で	動作メソッド	POST
どこへ	データ送信先	/cgi-bin/login.cgi
何が必要か	送信データ	userid password
どうなるか	認証後の動作	認証結果の表示

「入力画面はどれか」の部分空白になっていますが、ここではそのまま先に進みます。

3. 自動フォーム認証機能を設定する

ここでは、これまでに収集した情報を元にして自動フォーム認証機能ではどのように設定するかを説明していきます。

まず、HP IceWall SSOの自動フォーム認証機能における設定の概念を理解する必要があります。この機能では複数のフォーム認証に対応させたり、1つのフォーム認証設定を共有したりするためにフォーム設定をグルーピングする「フォームグループ」を使用しています。



先の例のフォーム認証を自動フォーム認証機能に設定すると、次のようになります。

■ フォーム認証設定ファイル（ここでは/opt/icewall-ssso/dfw/cgi-bin/form.confとします）

```
~
FORM_URL=FGROUP./docs/form.html
FORM_KEY=FGROUP.<TITLE>フォーム認証</TITLE>
FORM_METHOD=FGROUP.POST
```

```
FORM_SEND=FGROUP/cgi-bin/login.cgi
FORM_DATA_USR=FGROUP.POSTDATA.userid,UIDCLM
FORM_DATA_USR=FGROUP.POSTDATA.password,PWDCLM
```

この例ではフォームグループ名を「FGROUP」としています。

- FORM_URLはフォーム認証画面が表示されるURLを指定しています。
- FORM_KEYはフォーム認証画面を識別するためのキーワードを指定しています。これは情報収集の段階で空白になっていた「どれか」に相当する部分になります。この例の場合は固定のURLからのみの表示のため不要に思われるかもしれませんが、HP IceWall SSOのようにセッションを管理しているアプリケーションの場合は、セッションが切れた時点でURLに関係なくフォーム認証画面が表示されてしまうので、認証画面かどうかをキーワードを用いて判断するために設定します。
- FORM_METHODはデータ送信方法を指定しています。
- FORM_SENTはデータの送信先URLを指定しています。
- FORM_DATA_USRは送信するデータの名称と、その取得先を指定します。この項目の場合、データの取得先は認証DBのカラムとなります。(指定したカラムが認証DB上に存在すること、フォーム認証に必要な情報が入っているものとします)

このような設定でフォーム認証に対してシングル・サイン・オンを行うと、フォーム認証画面が表示されずに、いきなりフォーム認証結果の画面が表示されるようになります。

いかかでしょうか。この例のフォーム認証はシンプルかつ基本的な内容ですが、フォーム認証についての仕組みとその理解の仕方、それをHP IceWall SSOへ設定するための考え方がご理解いただけたかと思います。これはあくまでも基本的な内容ですが、これを理解することで様々なフォーム認証に対して設定が行えるようになります。。
これよりさらに高度かつ複雑な構成のフォーム認証に対してもHP IceWall SSOは強力的にサポートいたします。Webアプリケーションに手を加えることなく、簡単な設定のみでシングル・サイン・オンが実現できることを是非とも体験してみてください。

2003.11.20 (株)SCC I&C事業部 インターネットセキュリティ部 スーパーバイザ 鈴木 隆司 氏