



IceWall SSO

Version 10.0

自動フォーム認証設定マニュアル

日本ヒューレット・パッカード株式会社
2010 年 8 月

Printed in Japan

HP Part No. B2873-97007

Rev.100818A

ご注意

本書に記載されました内容は、予告なしに変更することがあります。

本書は内容について細心の注意をもって作成いたしましたが、万一ご不審な点や誤り、記載もれなど、お気づきの点がございましたら当社までお知らせください。

当社は、本書に記載されている誤り、あるいは備品、パフォーマンス、または本書の使用に関連して発生する偶然または必然的な損傷について責任は負いかねます。

本書の著作権は Hewlett-Packard Development Company, L.P. に帰属します。本書の一部あるいは全部についての無断複製、転載を禁じます。

本製品パッケージとして提供した本マニュアル、CD-ROM 等の媒体は本製品用だけにお使いください。

IceWall はヒューレット・パカード社の商標です。

Adobe は Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Java は、米国 Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

Microsoft および Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

Oracle は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。

目次

1 はじめに	1
1.1 文中におけるバージョン表示記号について	1
2 自動フォーム認証概要	2
2.1 IceWall SSO の自動フォーム認証でサポートされるフォーム認証の送信方法	2
2.2 制限事項	3
3 自動フォーム認証で可能な送信方式	4
3.1 直接送信方式	4
3.2 間接送信方式	6
4 自動フォーム認証に必要な情報	8
4.1 送信方式の選択	8
4.2 自動フォーム認証の対象となるコンテンツの情報	8
4.2.1 ログイン画面が表示される URL	8
4.2.2 ログイン画面を判断できるユニークなキーワード	9
4.3 送信メソッドの選択	9
4.4 認証情報の送信先 URL	9
4.5 フォーム送信データの情報	10
4.6 その他の情報の調査	11
4.6.1 フォーム認証後のリダイレクト	11
4.6.2 Cookie によるセッション管理	12
5 自動フォーム認証機能の設定	13
5.1 フォームグループについて	13
5.2 Form 認証設定ファイル	14
5.3 直接送信方式の設定方法	14
5.3.1 自動フォーム認証対象パス	15
5.3.2 自動フォーム認証判断キーワード	15
5.3.3 間接送信方式テンプレート HTML	16
5.3.4 リクエストメソッド	16
5.3.5 送信先	17
5.3.6 送信データ	18
5.4 間接送信方式の設定方法	20
5.4.1 自動フォーム対象パス	20
5.4.2 自動フォーム対象キーワード	21
5.4.3 間接送信方式テンプレート HTML	22
5.4.4 リクエストメソッド	23
5.4.5 送信先	23
5.4.6 送信データ	24
5.5 設定における注意事項	27
5.5.1 ログイン後のリダイレクト	27
5.5.2 セッション管理方法	27
5.5.3 Set-Cookie ヘッダーのフォーマットに関する注意点	28
5.5.4 自動フォーム認証に失敗した場合の動作について	28
5.5.5 Domain Gateway Option for UNIX を導入している場合	30
6 フォーム設定サンプル	31

6.1 IceWall SSO 多段自動フォームサンプル（直接送信方式）	31
6.2 IceWall SSO 多段自動フォームサンプル（間接送信方式）	31

1 はじめに

自動フォーム認証機能は、フォワーダーでバックエンド Web サーバーのフォーム認証のコンテンツに対して、IceWall SSO から自動で認証を行う機能です。本書を使用することで様々な形態のフォーム認証に対して Single Sign On を行うことができるようになります。

なお、本書の記述内容は、バックエンド Web サーバーのアプリケーションについてのある程度の知識と、フォーム認証についての基本的な知識を有する管理者向けの内容になっています。

1.1 文中におけるバージョン表示記号について

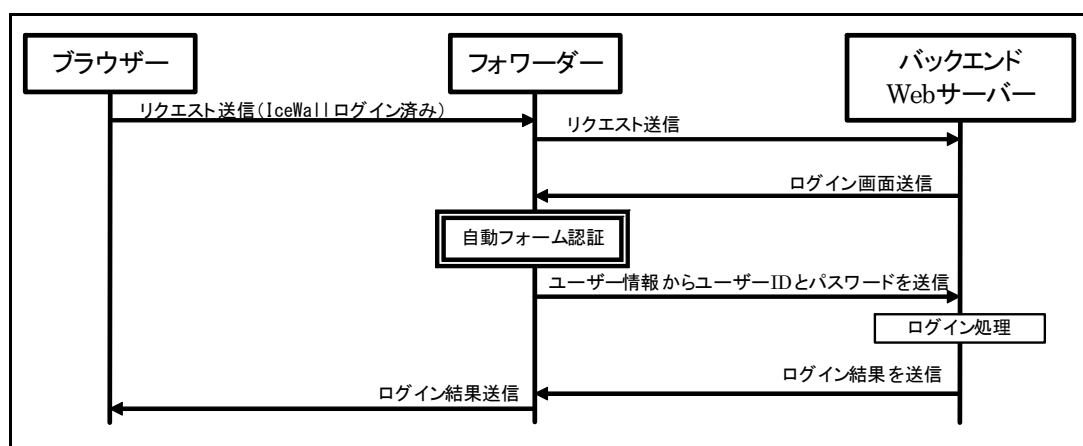
文中に付加されているバージョン表示記号は以下の意味を表します。

マーク	意味
10.0	四角で囲まれているバージョンで追加された項目です。この場合、10.0 にて追加されたことを表します。

2 自動フォーム認証概要

自動フォーム認証機能は、IceWall SSO のバックエンド Web サーバーにフォーム認証がある場合に、IceWall SSO が自動でフォームデータを送信する機能です。

この機能を使用することで、ユーザーが IceWall SSO にログインするだけでバックエンド Web サーバーのフォーム認証画面でユーザー ID・パスワード等を入力せずに、コンテンツの参照が可能となります。



IceWall SSO 経由の自動フォーム認証

2.1 IceWall SSO の自動フォーム認証でサポートされるフォーム認証の送信方法

IceWall SSO の自動フォーム認証機能でサポートされるフォーム認証の内容については以下のとおりです。

項目	内容
リクエストメソッド	• GET • POST
送信データの種類	• Query String • Post データ • Query String と Post データ
送信データの値	• 固定の文字列 • INPUT タグより取得した送信情報 • IceWall にログインしているユーザーのユーザー情報
セッション管理方法	• Cookie によるセッション管理
認証後の動作	• リダイレクトによる転送 • コンテンツ表示

自動フォーム認証が動作するためには、以下の設定内容がすべて一致する必要があります。

- URL (前方一致)
- FORM_KEY 項目 (複数設定可能)

- ・ FORM_KEY_EXCEPTION 項目（複数設定可能） **10.0**

2.2 制限事項

自動フォーム認証機能は、いくつかの制限事項があります。

- ・ 自動フォーム認証機能で使用するユーザーID とパスワードは、バックエンド Web サーバーのアプリケーションで使用するユーザーID とパスワードに一致することが前提となります。一致しない環境では必ずフォーム認証に失敗します。
- ・ 自動フォーム認証機能により、様々な形のフォーム認証に対しては自動で認証可能となりますが、すべてのフォーム認証に対して自動認証を保証するものではありません。バックエンド Web サーバーのアプリケーション側のセッション管理方式や、認証後の動作などによっては本機能を使用できない場合があることをご了承ください。

以下は自動フォーム認証機能を利用できない例です。

- (1) JAVA アプレットや ActiveX をダウンロードし、そのモジュール自体がバックエンド Web サーバーのアプリケーションに直接データを送信するもの。
 - (2) ワンタイムパスワードなどのログインごとにパスワードが変化するもの。
- ・ 後述する間接送信方式では、JavaScript をサポートしていないクライアントでは使用できません。

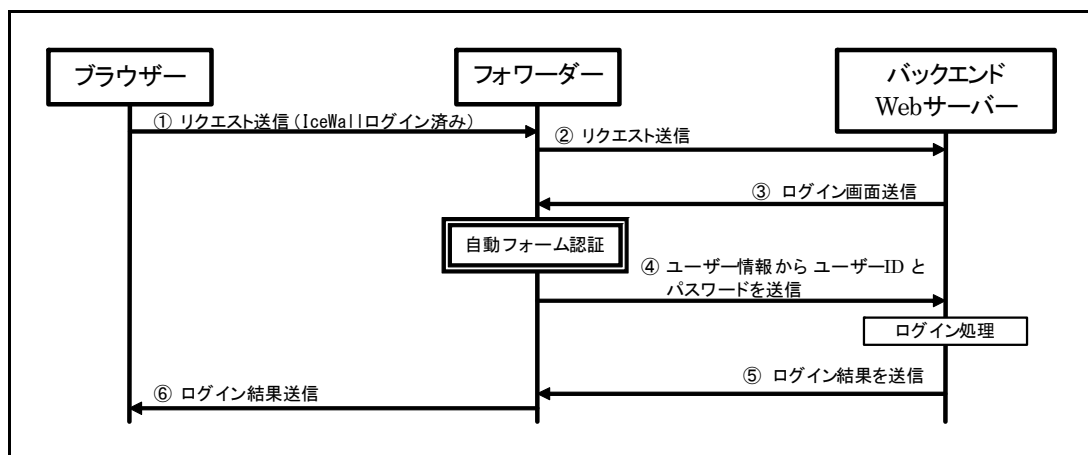
3 自動フォーム認証で可能な送信方式

IceWall SSO が自動フォーム認証で行える送信方式には、「直接送信方式」と「間接送信方式」の 2 つが存在します。一般的なフォーム認証では「直接送信方式」を使用することになりますが、認証後の動作により「直接送信方式」では対応できない場合に「間接送信方式」を使用します。

3.1 直接送信方式

直接送信方式とは、フォーム認証が必要なコンテンツに対して「フォワーダーとバックエンド Web サーバー間のみでリクエストを送受信する」方式です。

この方式は、フォーム認証が必要となった場合にフォワーダーより直接バックエンド Web サーバーへリクエストを送信するため、リクエストの送受信回数が少なく、比較的高速に処理されます。

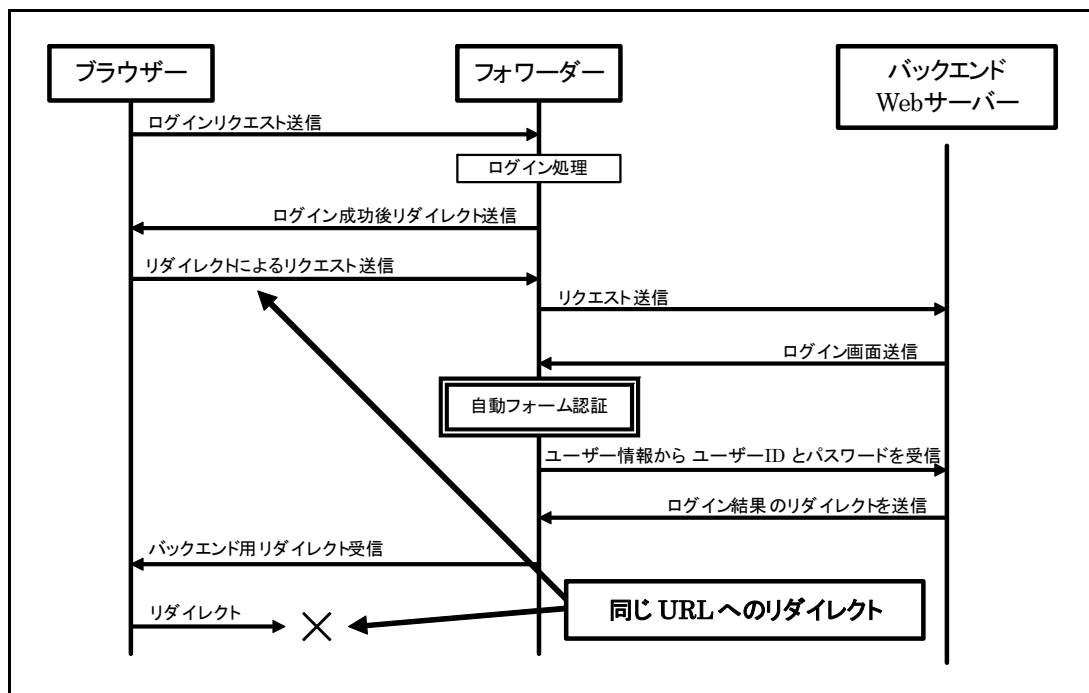


- ① ブラウザーよりフォワーダーへリクエストが送信されます。
- ② フォワーダーがバックエンド Web サーバーに対してクライアントより送信されたリクエストを送信します。
- ③ バックエンド Web サーバーはリクエストに対し認証が必要な場合、フォーム認証用ログイン画面をフォワーダーへ送信します。
- ④ フォワーダーはバックエンド Web サーバーより送信されたログイン画面を判断し、自動フォーム認証機能により、認証に必要な情報をバックエンド Web サーバーへ送信します。
- ⑤ バックエンド Web サーバーはフォワーダーより送信された情報により認証を行い、認証結果をフォワーダーへ送信します。
- ⑥ フォワーダーはバックエンド Web サーバーより送信された認証結果をクライアントに送信します。

直接送信方式が使用できないフォーム認証の条件は、以下のようになります。

- ・ 同じ URL へリダイレクトが 2 回連続でクライアントへ返る場合

※ ブラウザーの仕様による。



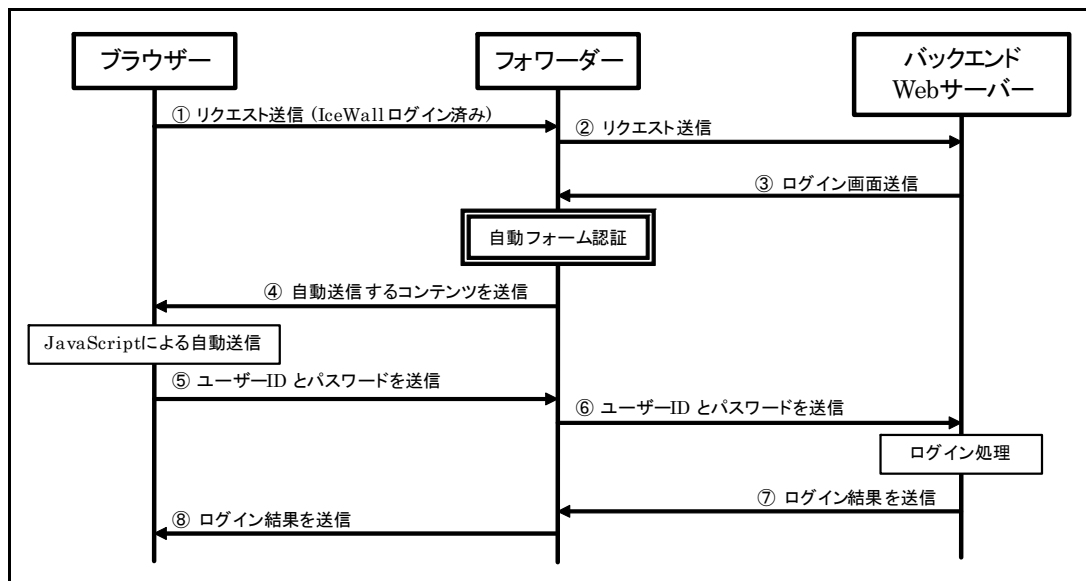
このようなシーケンスとなる場合には、以下の方法で回避するようにしてください。

- ・送信方式を「間接送信方式」に変更する。
- ・2 回目のリダイレクト前に何らかのコンテンツを表示させてからフォーム認証を行うようにする。

3.2 間接送信方式

間接送信方式とは、フォーム認証が必要なコンテンツに対して「フォワーダーから Web サーバーへ送信するフォーム認証のリクエストをクライアント経由で送信する」方式です。

この方式は、バックエンド Web サーバーのフォーム認証に必要な情報を一度ブラウザに返すため、直接送信方式よりレスポンスは低下しますが、IceWall SSO 経由でユーザー操作にて認証が可能であると確認されている場合は、確実に認証が成功する方式です。



- ① ブラウザーよりフォワーダーへリクエストが送信されます。
- ② フォワーダーがバックエンド Web サーバーに対してブラウザーより送信されたリクエストを送信します。
- ③ バックエンド Web サーバーはリクエストに対し認証が必要な場合、フォーム認証用ログイン画面をフォワーダーへ送信します。
- ④ フォワーダーはバックエンド Web サーバーより送信されたログイン画面を判断し、自動フォーム認証機能により認証に必要な情報をセットしたテンプレート HTML をブラウザーへ送信します。
- ⑤ ブラウザーはフォワーダーより送信されたテンプレート HTML から自動的にフォワーダーへリクエストを送信します。
- ⑥ フォワーダーはブラウザーから送信されたフォーム認証用リクエストをバックエンド Web サーバーへ送信します。
- ⑦ バックエンド Web サーバーはフォワーダーより送信された情報により認証を行い、認証結果をフォワーダーへ送信します。
- ⑧ フォワーダーはバックエンド Web サーバーより送信された認証結果をブラウザーに送信します。

間接送信方式では、特殊な認証方式（例えば JAVA アプレットや ActiveX を使用し、モジュールが直接 Web サーバーに認証を行うなど）以外は自動認証が可能となります。

自動フォーム認証機能では、バックエンド Web サーバーのフォーム認証画面（ログイン画面）をキーワードで判断するため、以下の条件にすべて一致する環境では無制限に自動フォーム認証が繰り返されることになります。

- (1) 間接送信方式を使用する
- (2) ログイン画面とログインエラー画面が同じ
- (3) ログイン試行回数が無制限
- (4) ログインに失敗する

このような場合には、間接送信方式で使用するテンプレート HTML を次のように修正してください。

- (1) <BODY> タグの onLoad イベントハンドラーを削除してください。
 - (2) <FORM> タグから </FORM> タグまでの間にフォーム認証ログイン用の <INPUT> タグを追加してください。
- （例）<INPUT TYPE="SUBMIT" VALUE="SUBMIT">

このように修正することで、自動フォーム認証はバックエンド Web サーバーへのログイン直前で停止し、ユーザーがログイン操作を行うこととなります。このため自動でのログインは行われなくなります。

※ あくまでも無限ループとならないための最低限の作業です。必要に応じて間接送信方式のテンプレート HTML をカスタマイズして、別画面へのリンクを追加するなどの対策を講じてください。

なお、「ログインエラー画面では一部エラーメッセージが追加で表示される」または「<INPUT> タグに入力された値が設定された状態で表示される」など、僅かでもログイン画面と異なる部分がある場合には、FORM_KEY_EXCEPTION 項目にログイン画面と異なる部分を設定することで回避することができます。

4 自動フォーム認証に必要な情報

自動フォーム認証を使用する際に、対象となるフォーム認証が「どのように動作するのか」、また「どのような情報を使用するのか」を収集する必要があります。
本章では、フォーム認証機能の各設定項目に必要な値の収集方法を解説します。

4.1 送信方式の選択

自動フォーム認証を行う送信方式を、直接送信方式・間接送信方式の2つから選択します。

送信方式の選択のために必要な情報は次の2つです。

- ・ IceWall SSO へのログインのタイミング
- ・ フォーム認証のログイン直後の動作

以下の条件に該当する場合には、直接送信方式ではなく間接送信方式を使用しなければなりません。

バックエンド Web サーバーのフォーム認証で表示されるログイン画面の URL と、ログイン後に表示されるコンテンツの URL が同じ、かつ IceWall SSO へのログイン直後に自動フォーム認証を行う場合

上記条件の場合、以下のことが可能な場合は直接送信方式が使用可能です。

- ・ フォワーダー設定ファイルの REDIRECT 項目を設定する。
- ・ IceWall SSO にログインした直後のコンテンツを自動フォーム認証対象としない。

一般的なフォーム認証では「直接送信方式」を使用しますが、このような条件に該当する場合には「間接送信方式」を使用しなければなりません。

4.2 自動フォーム認証の対象となるコンテンツの情報

自動フォーム認証の対象となるコンテンツの情報を収集します。
必要な情報は次の2つです。

- ・ フォーム認証用のログイン画面が表示される URL (パス)
- ・ ログイン画面を判断できるユニークなキーワード

4.2.1 ログイン画面が表示される URL

対象となるログイン画面の URL の「バックエンド Web サーバー側のパス部分」のみを使用します。特定の URL にアクセスした場合のみログイン画面が表示されるのか、特定のディレクトリ以下をアクセスした場合にログイン画面が表示されるかにより指定するパスが異なります。

(例) `http://www.xxxxxx.co.jp/fw/dfw/ALIAS/docs/index.html`
[対象が特定 URL のみの場合] `/docs/index.html`

[対象が特定ディレクトリ以下の場合] /docs/
[対象のパスが不定な場合] /

パスは前方一致で比較されます。

4.2.2 ログイン画面を判断できるユニークなキーワード

対象となるログイン画面に含まれるユニークなキーワードを使用して、ログイン画面が表示されたかどうかを判断します。キーワードは他のコンテンツで使用されていないものを選択してください。

(例) <TITLE>XXXXX LoginPage</TITLE>

※ キーワードは複数個設定することが可能です。ユニーク化のために複数個のキーワードを指定することを推奨します。

4.3 送信メソッドの選択

自動フォーム認証で送信するメソッドを「GET」と「POST」から選択します。
ログイン画面に記述されている FORM タグの METHOD 属性に設定されている値を送信メソッドとして指定します。

(例) <FORM METHOD="POST" ACTION="/cgi-bin/login.cgi">

この場合、送信メソッドは「POST」となります。

GET メソッドの場合には引数 (Query String) のみ、POST メソッドを使用する場合には POST データのみ、または POST データと引数 (Query String) が送信可能です。

※ GET、POST メソッド以外のメソッドによるフォーム認証はサポートされていません。

4.4 認証情報の送信先 URL

自動フォーム認証で認証情報を送信する URL を取得します。
通常は、ログイン画面に記述されている FORM タグの ACTION 属性に設定されている値を指定します。

(例) <FORM METHOD="POST" ACTION="/cgi-bin/login.cgi">

この場合、送信先 URL は「/cgi-bin/login.cgi」となります。

送信先の URL については、必ずしも設定する必要はありません。設定されない場合は、IceWall SSO がログイン画面に含まれる FORM タグの ACTION 属性に設定されている値を自動的に取得します。送信先 URL が、ログイン画面を表示するごとに異なるなど、固定の値ではない場合には、送信先 URL を設定せずに自動的に取得するようにしてく

ださい。

POST メソッドで、固定の引数 (Query String) を送信したい場合には、次のように送信先 URL に含めることも可能です。

(例) /cgi-bin/login.cgi?name=value

ただし、引数 (Query String) の内容が動的に変更される場合は、送信先 URL を自動取得するようにしてください。

4.5 フォーム送信データの情報

自動フォーム認証で使用するバックエンド Web サーバーのフォーム認証に必要な送信データをすべて収集します。

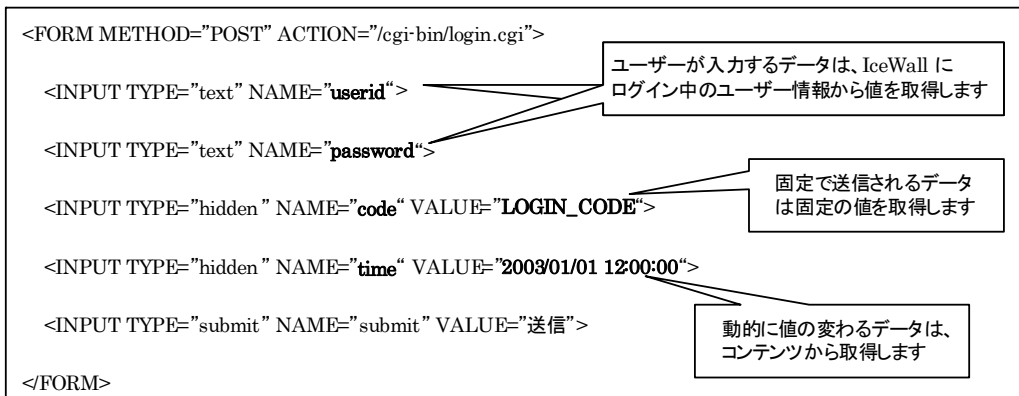
収集対象は、ログイン画面に記述されているすべての INPUT タグの NAME 属性と VALUE 属性に設定されている値です。(ただし、TYPE 属性が「Submit」のものは除きます)

送信するデータは次の 3 つに分類されます。

- (1) ユーザーが個別に入力、または選択する値
ユーザー ID やパスワードを入力する項目、あらかじめ初期値が格納されていて編集可能な項目、または選択式となっている項目が該当します。
- (2) バックエンド Web サーバーのアプリケーション側から固定で格納される値
バックエンド Web サーバーのアプリケーション側で必要な情報で、ユーザーには入力させる必要がない項目が該当します。このような値は通常、INPUT タグの TYPE 属性の値が「hidden」のように設定されています。
- (3) バックエンド Web サーバーのアプリケーション側から動的に格納される値
バックエンド Web サーバーのアプリケーション側よりユーザー別に動的に値が変化し、かつユーザーには入力させる必要がない項目です。(2) 同様、通常は INPUT タグの TYPE 属性の値が「hidden」に設定されています。

以下はフォーム送信データの判断例です。

(例) フォーム送信データの例



[ユーザーが個別に入力または選択する値]

- ・ NAME 属性値「**userid**」
- ・ NAME 属性値「**password**」

[アプリケーション側から固定で格納される値]

- ・ NAME 属性値「**code**」 VALUE 属性値「**LOGIN_CODE**」

[アプリケーション側から動的に格納される値]

- ・ NAME 属性値「**time**」

このように送信するデータの名称と、どのような（どこから取得する）値を送信するかを判断します。

なお、自動フォーム認証機能では VALUE 属性の値に固定の値、ログインユーザーのユーザー情報、ログイン画面に設定されている値を使用して送信することが可能です。動的な値を送信したい場合は、ユーザー情報やログイン画面から取得できる値を使用します。

4.6 その他の情報の調査

自動フォーム認証対象となるフォーム認証のログイン後動作や、セッション管理方法についての情報を収集します。

代表的なパターンは次の 2 つです。

- ・ フォーム認証後にリダイレクトで別の URL へ転送する。
- ・ Cookie 発行によるセッション管理。

4.6.1 フォーム認証後のリダイレクト

自動フォーム認証対象となるフォーム認証がログイン後にリダイレクトする場合、リダイレクト先のホストがフォワーダー設定ファイルの HOST 項目または SHOST 項目に記述されたホストであるか調査します。

未登録のホストの場合は、HOST 項目または SHOST 項目に追加します。

4.6.2 Cookie によるセッション管理

自動フォーム認証対象となるフォーム認証のセッション管理方法を調査します。
セッション管理にCookieを使用している場合、以下のことに注意しなければなりません。

- Set-cookie ヘッダーの domain 属性
domain 属性が記述されていて、そのドメインが IceWall サーバーのホストのドメインではない場合、キーワード変換を使用して domain 属性を削除します。
- Set-cookie ヘッダーの secure 属性
secure 属性が記述されていて、クライアントとフォワーダーの間が SSL を使用していない場合、キーワード変換を使用して secure 属性を削除します。
- Cookie の個数
ブラウザが保持できる Cookie の最大数を超える Cookie がブラウザに送信された場合、IceWall SSO の認証 Cookie が削除されてしまう場合があります。
Cookie を多数使用する場合、不要な Cookie を削除するようなコンテンツを経由するか、フォワーダー設定ファイルの COOKIEALWAYS 項目に 1 を設定する必要があります。

5 自動フォーム認証機能の設定

本章では、自動フォーム認証機能の設定方法を解説します。

ここで解説する自動フォーム認証機能の設定値は、「4 自動フォーム認証に必要な情報」を参照して事前に対象となるフォーム認証の情報が収集されている必要があります。

「直接送信方式」と「間接送信方式」では、同じ設定項目でも一部設定方法が異なるものがあります。自動フォーム認証の設定は、ホスト設定ファイルまたは Form 認証設定ファイルに記述します。

なお、各設定項目の詳細については「IceWall SSO リファレンスマニュアル」を参照してください。

5.1 フォームグループについて

自動フォーム認証機能では、対象となるバックエンド Web サーバーに複数のフォーム認証が存在する場合、それぞれのフォーム認証に対して個別の設定を行うことができます。このような設定を可能とするために、自動フォーム認証機能では「グループ」の概念を導入しています。1 つのフォーム認証用に設定されたグループを「フォームグループ」と呼びます。

フォームグループは、1 つのフォーム認証に対して 1 つのグループで設定します。

同一のコンテンツ内に複数のフォーム認証が存在する場合でも個別に設定することが可能です。

(例) 同じバックエンド Web サーバーの 2 つのフォーム認証に対する設定

<pre># FORM1 Configuration FORM_URI=AAA/docs/login.html FORM_KEY=AAA,<TITLE>LoginPage</TITLE> FORM_METHOD=AAA,POST FORM_SEND=AAA,/cgi-bin/cert.cgi FORM_DATA_STR=AAA,POSTDATA,LOGINUID,user001 FORM_DATA_USR=AAA,POSTDATA,PASSWORD,password</pre>	} FORM1 に対する設定 フォームグループ:AAA
<pre># FORM2 Configuration FORM_URI=BBB/user.html FORM_KEY=BBB,<TITLE>UserLogin</TITLE> FORM_HTML=BBB/bbb_login.html FORM_METHOD=BBB,GET FORM_SEND=BBB,/cgi-bin/login.cgi FORM_DATA_STR=BBB,NOENCVAL,LOGINUID,user001 FORM_DATA_USR=BBB,NOENCVAL,PASSWORD,password</pre>	} FORM2 に対する設定 フォームグループ:BBB

5.2 Form 認証設定ファイル

Form 認証設定ファイルは、自動フォーム認証機能の設定項目を記述する設定ファイルです。ファイル名は任意の名前で設定します。

自動フォーム認証機能の設定は通常、ホスト設定ファイルに記述しますが、Form 認証設定ファイルはフォーム認証ごとに設定ファイルを分割して管理する場合や、複数のホスト設定ファイルから1つのフォーム認証設定を共有させる場合などに使用します。

Form 認証設定ファイルの設定は、ホスト設定ファイルに以下のように設定します。

```
FORM_FILE= (フォームグループ名) , (Form 認証設定ファイル名)
```

(例) Form 認証設定ファイルパスが /opt/icewall-ss0/dfw/cgi-bin/form.conf の場合
FORM_FILE=FGROUP,/opt/icewall-ss0/dfw/cgi-bin/form.conf

ホスト設定ファイルにて FORM_FILE 項目が設定された場合、Form 認証設定ファイルより自動フォーム認証機能の設定項目を取得します。このため、1つのフォームグループに1つだけ設定可能な項目をホスト設定ファイルと Form 認証設定ファイルにそれぞれ記述した場合、Form 認証設定ファイルに記述した設定が有効となります。

(Form 認証設定ファイル例)

【 ホスト設定ファイル 】

```
# FORM1 Configuration
FORM_FILE=AAA,/form.conf ← フォームグループ名をAAAに設定
```

【 Form 認証設定ファイル (form.conf) 】

```
# FORM1 Configuration
FORM_URL=AAA,/docs/login.html
FORM_KEY=AAA,<TITLE>LoginPage<TITLE>
FORM_METHOD=AAA,POST
FORM_SEND=AAA,/cgi-bin/cert.cgi
FORM_DATA_STR=AAA,POSTDATA,LOGINUID,user001
FORM_DATA_USR=AAA,POSTDATA,PASSWORD,password
```

} 同じくフォームグループ名を
AAA に設定する

この場合、ホスト設定ファイルに「FORM_METHOD=AAA,GET」と記述されていても Form 認証設定ファイルの「FORM_METHOD=AAA,POST」が有効となります。

5.3 直接送信方式の設定方法

直接送信方式を使用する場合の設定方法について解説します。

直接送信方式では、間接送信方式で利用されるテンプレート HTML は使用しません。

ここで設定する内容は、ホスト設定ファイルと Form 認証設定ファイルのどちらに設定しても構いません。ただし、Form 認証設定ファイルを使用する場合には、ホスト設定ファイルに FORM_FILE 項目の設定を行ってください。

ここではサンプルとしてフォームグループ名を「FGROUP」と定義します。

5.3.1 自動フォーム認証対象パス

自動フォーム認証を行うコンテンツのパスを設定します。「4.2.1 ログイン画面が表示される URL」で収集した情報を設定します。

■ FORM_URL 項目

FORM_URL= (フォームグループ名) , (対象パス)

- ・ この項目はフォームグループ内で1つだけ設定できます。
- ・ パスは前方一致でチェックを行います（あるディレクトリ以下という設定が可能）
- ・ この項目は必須項目です。

[設定例]

/docs/loginpage.html にアクセスするとフォーム認証要求される場合

FORM_URL=FGROUP,/docs/loginpage.html

/docs/ 以下をアクセスするとフォーム認証要求される場合

FORM_URL=FGROUP,/docs/

そのサーバーにアクセスすると、対象パスに関係なくフォーム認証要求される場合

FORM_URL=FGROUP,/

5.3.2 自動フォーム認証判断キーワード

自動フォーム認証を行うログイン画面として判断できるキーワードを設定します。「4.2.2 ログイン画面を判断できるユニークなキーワード」で収集した情報を設定します。

■ FORM_KEY 項目

FORM_KEY= (フォームグループ名)、(検索キーワード)

- ・ この項目はフォームグループ内で複数個の設定することができます。
- ・ 検索キーワードを複数設定した場合、すべての検索キーワードが一致した場合のみフォーム認証が行われます。
- ・ この項目は必須項目です。

[設定例]

フォーム認証用ログイン画面の「<TITLE>Login Page</TITLE>」と
「UserLoginPage」を検索キーワードとして使用する場合

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>  
FORM_KEY=FGROUP,UserLoginPage
```

■ FORM_KEY_EXCEPTION 項目 **10.0**

```
FORM_KEY_EXCEPTION= (フォームグループ名) , (検索キーワード)
```

- ・ この項目はフォームグループ内で複数個の設定することができます。
- ・ FORM_KEY 項目とは逆に検索キーワードが含まれない場合に対象となります。
- ・ FORM_KEY_EXCEPTION 項目は FORM_KEY 項目が設定されていない場合には使用できません。
- ・ 検索キーワードを複数設定した場合、1 項目でも検索キーワードが一致した場合はフォーム認証が行われません。

[設定例]

フォーム認証用ログイン画面に「<TITLE>Login Page</TITLE>」と
「UserLoginPage」が含まれ、「UserID Error ReLogin」が含まれない場合を対象とする場合

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>  
FORM_KEY=FGROUP,UserLoginPage  
FORM_KEY_EXCEPTION=FGROUP,UserID Error ReLogin
```

5.3.3 間接送信方式テンプレート HTML

直接送信方式では間接送信テンプレート HTML は使用しません。このため、この設定は行いません。

5.3.4 リクエストメソッド

自動フォーム認証で送信するリクエストメソッドを設定します。「4.3 送信メソッドの選択」で収集した情報を設定します。

■ FORM_METHOD 項目

```
FORM_METHOD= (フォームグループ名) , (メソッド名)
```

- ・ この項目はフォームグループ内で 1 つだけ設定できます。
- ・ この項目は必須項目です。

[設定例]

POST メソッドでフォーム認証を行っている場合

```
FORM_METHOD=FGROUP,POST
```

5.3.5 送信先

自動フォーム認証の送信先パスを設定します。「4.4 認証情報の送信先 URL」で収集した情報を設定します。

■ FORM_SEND 項目

```
FORM_SEND= (フォームグループ名) , (送信先パス)
```

- ・この項目はフォームグループ内で1つだけ設定できます。
- ・この設定項目を設定しない場合、ログイン画面の **FORM** タグの **ACTION** 属性に設定されている値を自動的に取得します。(動的な **Query String** がある場合などは設定を省略し、自動取得しなければなりません)
- ・「http」「https」「/」「.」からのパスの記述が可能です。
- ・「http」「https」からの絶対パスの場合、そのホストがフォワーダー設定ファイルの **HOST** 項目または **SHOST** 項目に設定されていなければなりません。
- ・パスに **Query String** が付加される場合は、そのまま送信先パスの後ろに付加されます。

[設定例]

ログイン画面が表示されるサーバーと同じサーバー上のファイル「/cgi-bin/cert.cgi」へフォーム認証を行う場合

```
FORM_SEND=FGROUP,/cgi-bin/cert.cgi
```

ログイン画面が表示されるサーバーと同じサーバー上のファイル「./cert.cgi」へフォーム認証を行う場合

```
FORM_SEND=FGROUP,./cert.cgi
```

ログイン画面が表示されるサーバーと異なるサーバー上のファイル「http://www.other.jp/cgi-bin/cert.cgi」へフォーム認証を行う場合

```
FORM_SEND=FGROUP,http://www.other.jp/cgi-bin/cert.cgi
```

※ www.other.jp は **HOST** 項目に設定しておかなければなりません

ログイン画面が表示されるサーバーと同じサーバー上のファイル「/cgi-bin/cert.cgi」へ固定の引数（Query String）「aaa=%2Fbbb」を付けて送信する場合

```
FORM_SEND=FGROUP,/cgi-bin/cert.cgi?aaa=%2Fbbb
```

※ Query String は URL エンコードされた状態で記述してください。

5.3.6 送信データ

自動フォーム認証の送信データを設定します。「4.5 フォーム送信データの情報」で収集した情報を設定します。

送信データは固定の値、ユーザー情報の値、コンテンツから取得した値が設定可能です。

※ 送信データの設定は間接送信方式での設定方法とは異なります

■ FORM_DATA_STR 項目

固定の値を送信データとして使用します。

```
FORM_DATA_STR=(フォームグループ名),(送信データ種別),(属性名),(属性値)
```

- ・ 送信データ種別には「POSTDATA」と「QUERY」のいずれかを指定します。
- ・ この項目はフォームグループ内で複数個の設定が可能です。

[設定例]

Post データで以下のタグ情報をそのまま送信する場合

```
<INPUT TYPE="text" NAME="userid" VALUE="user001">
```

```
FORM_DATA_STR=FGROUP,POSTDATA,userid,user001
```

Query String で以下のタグ情報をそのまま送信する場合

```
<INPUT TYPE="password" NAME="password" VALUE="pwd01">
```

```
FORM_DATA_STR=FGROUP,QUERY,password,pwd01
```

■ FORM_DATA_USR 項目

ユーザー情報の値を送信データとして使用します。

```
FORM_DATA_USR=(フォームグループ名),(送信データ種別),(属性名),(認証 DB カラム名)
```

- ・ 送信データ種別には「POSTDATA」と「QUERY」のいずれかを指定します。
- ・ 認証 DB カラム名には認証モジュールより送信されたユーザー情報を指定します。
- ・ 認証 DB カラム名には以下の予約語が用意されています。
 - DEFAULTUID : ログイン時のユーザー ID を使用
 - DEFAULTPWD : ログイン時のパスワードを使用※
- ・ この項目はフォームグループ内で複数個の設定が可能です。

※ IceWall Cert Protocol (ICP) 2.0 を使用する場合は、リクエスト制御設定ファイル (request.acl) にてパスワードを送信可能な設定にする必要がありますので、ご注意ください。

[設定例]

以下のタグ情報を認証 DB カラム PWDCLM から取得した値で Post データとして送信したい場合

<INPUT TYPE="password" NAME="password">

FORM_DATA_USR=FGROUP,POSTDATA,password,PWDCLM

以下のタグ情報を認証 DB カラム INFOCLM から取得した値で Query String として送信したい場合

<INPUT TYPE="text" NAME="info">

FORM_DATA_USR=FGROUP,QUERY,info,INFOCLM

■ FORM_DATA_PAGE 項目

ログイン画面内の INPUT タグの NAME 属性値および VALUE 属性値を送信データとして使用します。

FORM_DATA_PAGE= (フォームグループ名) , (送信データ種別) , (送信属性名) , (検索属性名)

- ・送信データ種別には「POSTDATA」と「QUERY」のいずれかを指定します。
- ・コンテンツに同じ属性名の INPUT タグが複数ある場合は、一番上が対象となります。
- ・この項目はフォームグループ内で複数個の設定が可能です。

[設定例]

以下のタグの値をそのまま Post データとして送信する場合

<INPUT TYPE="hidden" NAME="data" VALUE="data-value">

FORM_DATA_PAGE=FGROUP,POSTDATA,data,data

以下のタグの送信属性名を information に変更し、Query String として送信する場合

<INPUT TYPE="hidden" NAME="info" VALUE="info-value">

FORM_DATA_PAGE=FGROUP,QUERY,information,info

■ FORM_DATA_PAGE_REF 項目 **10.0**

FORM_DATA_PAGE 項目で取得した値に含まれる実体参照を元の文字に置換するかを設定します。

FORM_DATA_PAGE_REF= (フォームグループ名) , (フラグ)

- ・ この項目はフォームグループ内で1つだけ設定できます。
- ・ フラグには以下の値を設定します。
 - 0 : 実体参照を置換しない
 - 1 : 実体参照を置換する

[設定例]

FORM_DATA_PAGE 項目を使用して取得したフォーム情報に、実体参照が含まれる際に元の文字へ戻す場合

FORM_DATA_PAGE_REF=FGROUP,1

送信データはフォーム認証で必要とするデータをすべて設定します。
ここまでの設定で直接送信方式の設定は終了となります。

5.4 間接送信方式の設定方法

間接送信方式を使用する場合の設定方法について解説を行います。基本的な設定方法は直接送信方式と同じですが、間接送信方式では間接送信方式テンプレート HTML の設定を行います。

ここで設定する内容は、ホスト設定ファイルと Form 認証設定ファイルのどちらに設定しても構いません。ただし、Form 認証設定ファイルを使用する場合には、ホスト設定ファイルに FORM_FILE 項目の設定を行ってください。

ここではサンプルとしてフォームグループを「FGROUP」と定義します。

5.4.1 自動フォーム対象パス

自動フォーム認証を行うコンテンツのパスを設定します。「4.2.1 ログイン画面が表示される URL」で収集した情報を設定します。

■ FORM_URL 項目

FORM_URL= (フォームグループ名) , (対象パス)

- ・ この項目はフォームグループ内で1つだけ設定できます。
- ・ パスは前方一致でチェックを行います (あるディレクトリ以下という設定が可能)
- ・ この項目は必須項目です。

[設定例]

/docs/loginpage.html にアクセスするとフォーム認証要求される場合

```
FORM_URL=FGROUP,/docs/loginpage.html
```

/docs/ 以下をアクセスするとフォーム認証要求される場合

```
FORM_URL=FGROUP,/docs/
```

そのサーバーにアクセスするとパスに関係なくフォーム認証要求される場合

```
FORM_URL=FGROUP,/
```

5.4.2 自動フォーム対象キーワード

自動フォーム認証を行うログイン画面として判断できるキーワードを設定します。
「4.2.2 ログイン画面を判断できるユニークなキーワード」で収集した情報を設定します。

■ FORM_KEY 項目

```
FORM_KEY= (フォームグループ名) , (検索キーワード)
```

- ・この項目はフォームグループ内で複数個の設定することができます。
- ・検索キーワードを複数設定した場合、すべての検索キーワードが一致した場合のみフォーム認証が行われます。
- ・この項目は必須項目です。

[設定例]

フォーム認証用ログイン画面の「<TITLE>Login Page</TITLE>」と

「UserLoginPage」をキーワードとして使用する場合

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>  
FORM_KEY=FGROUP,UserLoginPage
```

■ FORM_KEY_EXCEPTION 項目 10.0

```
FORM_KEY_EXCEPTION= (フォームグループ名) , (検索キーワード)
```

- ・この項目はフォームグループ内で複数個の設定することができます。
- ・検索キーワードを複数設定した場合、1 項目でも検索キーワードが一致した場合はフォーム認証が行われません。
- ・FORM_KEY 項目とは逆にキーワードが含まれない場合に対象となります。
- ・FORM_KEY_EXCEPTION 項目は FORM_KEY 項目が設定されていない場合には使用できません。

[設定例]

フォーム認証用ログイン画面に「<TITLE>Login Page</TITLE>」と「UserLoginPage」が含まれ、「UserID Error ReLogin」が含まれない場合を対象とする場合

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>  
FORM_KEY=FGROUP,UserLoginPage  
FORM_KEY_EXCEPTION=FGROUP,UserID Error ReLogin
```

5.4.3 間接送信方式テンプレート HTML

自動フォーム認証で送信する間接送信方式テンプレート HTML のパスを設定します。間接送信方式の場合、直接送信方式のフォワーダーバックエンド Web サーバー間のリクエストとは異なり、フォーム認証に必要な情報を 1 度ブラウザへ送信します。ブラウザにはコンテンツとして送信するため、その基本となる HTML が間接送信方式テンプレート HTML となります。

間接送信方式テンプレート HTML では、フォーム認証に必要な次の情報をすべて格納する必要があります。

- ・ 送信先 URL (FORM タグの ACTION 属性)
- ・ 送信メソッド (FORM タグの METHOD 属性)
- ・ 送信データ (INPUT タグの NAME および VALUE 属性)

これらの情報は設定ファイルやログイン画面から取得しますが、取得した値をテンプレート HTML へ格納するために「キーワード変換機能」を使用します。このため、テンプレート HTML には上記のデータを格納するためのキーワードを記述しておく必要があります。

また、間接送信方式のテンプレート HTML は、ブラウザより自動でフォーム認証を行わせるため、JavaScript によるスクリプトを記述しておかなければなりません。

■ FORM_HTML 項目

テンプレート HTML ファイルを指定します。

```
FORM_HTML= (フォームグループ名) , (テンプレート HTML ファイル名)
```

- ・ この項目はフォームグループ内で 1 つだけ設定できます。
- ・ 間接送信方式では必須項目です。

[設定例]

間接送信テンプレート HTML ファイルが /opt/icewall-ssso/dfw/cgi-bin/autologin.html の場合

```
FORM_HTML=FGROUP,/opt/icewall-ssso/dfw/cgi-bin/autologin.html
```

間接送信テンプレート HTML の例です。

送信先 URL 用の置換キーワードとして「\$ACTION」、送信メソッド用の置換キーワードとして「\$METHOD」、送信データ「USERID」属性の値の置換キーワードとして「\$UID」、送信データ「PASSWD」属性の値の置換キーワードとして「\$PWD」をそれぞれ設定しています。

```
<HTML>
<HEAD>
<TITLE>AutoLogin Page</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--
function LoadData()
{
    document.form.submit();
}
//-->
</SCRIPT>
</HEAD>
<BODY onLoad="LoadData();">

<FORM NAME="form" METHOD="$METHOD" ACTION="$ACTION">
  <INPUT TYPE="hidden" NAME="USERID" VALUE="$UID">
  <INPUT TYPE="hidden" NAME="PASSWD" VALUE="$PWD">
</FORM><P><BR>
<DIV ALIGN="center">フォーム認証中です</DIV>
</BODY>
</HTML>
```

ブラウザからの自動送信用
JavaScriptです。

送信する情報の置換キーワードに関する詳細は「5.4.6 送信データ」で解説します。

5.4.4 リクエストメソッド

自動フォーム認証で送信するリクエストメソッドを設定します。「4.3 送信メソッドの選択」で収集した情報を設定します。

■ FORM_METHOD 項目

FORM_METHOD= (フォームグループ名) , (メソッド名)

- ・ この項目はフォームグループ内で1つだけ設定できます。
- ・ この項目は必須項目です。

[設定例]

POST メソッドでフォーム認証を行っている場合

FORM_METHOD=FGROUP,POST

5.4.5 送信先

自動フォーム認証の送信先パスを設定します。「4.4 認証情報の送信先 URL」で収集した情報を設定します。

■ FORM_SEND 項目

FORM_SEND= (フォームグループ名) , (送信先パス)

- ・この項目はフォームグループ内で1つだけ設定できます。
- ・この設定項目を設定しない場合、ログイン画面の FORM タグの ACTION 属性に設定されている値を自動的に取得します。(動的な Query String がある場合などは設定を省略し、自動取得しなければなりません)
- ・「http」「https」「/」「.」からのパスの記述が可能です。
- ・「http」「https」からの絶対パスの場合、そのホストがフォワーダー設定ファイルの HOST 項目または SHOST 項目に設定されていなければなりません。
- ・パスに Query String が付加される場合は、そのまま送信先パスの後ろに付加されます。

[設定例]

ログイン画面が表示されるサーバーと同じサーバー上のファイル「/cgi-bin/cert.cgi」へフォーム認証を行う場合

FORM_SEND=FGROUP,/cgi-bin/cert.cgi

ログイン画面が表示されるサーバーと同じサーバー上のファイル「./cert.cgi」へフォーム認証を行う場合

FORM_SEND=FGROUP,./cert.cgi

ログイン画面が表示されるサーバーと異なるサーバー上のファイル「http://www.other.jp/cgi-bin/cert.cgi」へフォーム認証を行う場合

FORM_SEND=FGROUP,http://www.other.jp/cgi-bin/cert.cgi

※ www.other.jp は HOST 項目に設定しておかなければなりません

ログイン画面が表示されるサーバーと同じサーバー上のファイル「/cgi-bin/cert.cgi」へ固定の引数 (Query String) 「aaa=%2Fbbb」を付けて送信する場合

FORM_SEND=FGROUP,/cgi-bin/cert.cgi?aaa=%2Fbbb

※ Query String は URL エンコードされた状態で記述してください。

5.4.6 送信データ

自動フォーム認証の送信データを設定します。「4.5 フォーム送信データの情報」で収集した情報を設定します。

送信データは固定の値、ユーザー情報の値、コンテンツから取得した値が設定可能です。

送信データは間接送信方式テンプレート HTML にキーワードを記述し、送信する値に置換して IceWall SSO がクライアントへ送信する仕組みになります。

置換する値に対して URL エンコードを行うことも可能です。

間接送信方式テンプレート HTML に記述するキーワードは、各設定項目の（キーワード）に設定した値に「\$」を付けて記述します。

■ FORM_DATA_STR 項目

固定の値を送信データとして使用します。

```
FORM_DATA_STR=(フォームグループ名),(送信データ種別),(属性名),(属性値)
```

- ・ 送信方法には「ENCVAL」と「NOENCVAL」のいずれかを指定します。
- ・ この項目はフォームグループ内で複数個の設定が可能です。

[設定例]

以下のタグ情報に対して値を「user001」とし、URL エンコードせずに間接送信テンプレート HTML の置換キーワード \$PAGEKEY-UID へ格納してブラウザへ送信する場合

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

```
FORM_DATA_STR=FGROUP,NOENCVAL,PAGEKEY-UID,user001
```

間接送信テンプレートには以下のように記述します。

```
<INPUT TYPE="hidden" NAME="userid" VALUE="$PAGEKEY-UID">
```

POST メソッドの場合に、以下のタグ情報に対して値を「pwd01」とし、URL エンコードを行った引数として間接送信テンプレート HTML の置換キーワード \$PAGEKEY-PWD へ格納してブラウザに送信したい場合

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

```
FORM_DATA_STR=FGROUP,ENCVAL,PAGEKEY-PWD,pwd01
```

間接送信方式テンプレート HTML には以下のように記述します。

```
<FORM METHOD="POST" ACTION="/cgi-bin/cert.cgi?password=$PAGEKEY-PWD">
```

■ FORM_DATA_USR 項目

ユーザー情報の値を送信データとして使用します。

```
FORM_DATA_USR=(フォームグループ名),(送信データ種別),(属性名),(認証 DB カラム名)
```

- ・送信データ種別には「ENCVAL」と「NOENCVAL」のいずれかを指定します。
- ・認証 DB カラム名には認証モジュールより送信されたユーザー情報を指定します。
- ・認証 DB カラム名には以下の予約語が用意されています。

DEFAULTUID : ログイン時のユーザー ID を使用

DEFAULTPWD : ログイン時のパスワードを使用※

- ・この項目はフォームグループ内で複数個の設定が可能です。

※ IceWall Cert Protocol (ICP) 2.0 を使用する場合は、リクエスト制御設定ファイル (request.acl) にてパスワードを送信可能な設定にする必要がありますので、ご注意ください。

[設定例]

以下のタグ情報に対して値を認証 DB カラム PWDCLM から取得し、URL エンコードなしで Post データとして送信したい場合。置換キーワードは \$PAGEKEY-PWD。

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

```
FORM_DATA_USR=FGROUP,NOENCVAL,PAGEKEY-PWD,PWDCLM
```

間接送信方式テンプレート HTML には以下のように記述します。

```
<INPUT TYPE="hidden" NAME="password" VALUE="$PAGEKEY-PWD">
```

POST メソッドの場合に、以下のタグ情報に対して値を認証 DB カラム INFOCLM から取得し、URL エンコードを行った Query String として送信したい場合。置換キーワードは \$PAGEKEY-INFO。

```
<INPUT TYPE="text" NAME="info">
```

```
FORM_DATA_USR=FGROUP,ENCVAL,PAGEKEY-INFO,INFOCLM
```

間接送信方式テンプレート HTML には以下のように記述します。

```
<FORM METHOD="POST" ACTION="/cgi-bin/cert.cgi?info=$PAGEKEY-INFO">
```

■ FORM_DATA_PAGE 目

ログイン画面中に含まれる INPUT タグの NAME 属性名、VALUE 属性値を送信データとして使用します。

```
FORM_DATA_PAGE= (フォームグループ名) , (送信データ種別) , (送信属性名) , (検索属性名)
```

- ・送信データ種別には「ENCVAL」と「NOENCVAL」のいずれかを指定します。
- ・コンテンツに同じ属性名の INPUT タグが複数ある場合は、一番上が対象となります
- ・この項目はフォームグループ内で複数個の設定が可能です。

[設定例]

以下のタグの VALUE 値「data-value」を NAME 値「data」をキーワードとして取得し、URL エンコードせずに間接送信テンプレート HTML の置換キーワード \$PAGEKEY-DATA へ格納してブラウザに送信したい場合

```
<INPUT TYPE="hidden" NAME="data" VALUE="data-value">
```

```
FORM_DATA_PAGE=FGROUP,NOENCVAL,PAGEKEY-DATA,data
```

間接送信方式テンプレート HTML には以下のように記述します。

```
<INPUT TYPE="hidden" NAME="data" VALUE="$PAGEKEY-DATA">
```

POST メソッドの場合に、以下のタグの VALUE 値「info-value」を NAME 値「info」をキーワードとして取得し、URL エンコードを行った引数で間接送信テンプレート HTML の置換キーワード \$PAGEKEY-INFO へ格納してブラウザに送信したい場合

```
<INPUT TYPE="hidden" NAME="info" VALUE="info-value">
```

```
FORM_DATA_PAGE=FGROUP,ENCVAL,PAGEKEY-INFO,info
```

間接送信方式テンプレート HTML には以下のように記述します。

```
<FORM METHOD="POST" ACTION="/cgi-bin/cert.cgi?info=$PAGEKEY-INFO">
```

5.5 設定における注意事項

自動フォーム認証対象のフォーム認証が、ログイン後のリダイレクトやセッション管理で Cookie を使用している時は、フォワーダー設定ファイルに設定を追加しなければならない場合があります。

5.5.1 ログイン後のリダイレクト

自動フォーム認証対象となるフォーム認証がログイン後にリダイレクトする場合、リダイレクト先のホストがフォワーダー設定ファイルの HOST、SHOST 項目に設定されていないホストの場合は、その項目に追加を行います。

(例) リダイレクト先ホスト「www.yyyyyy.co.jp」が未設定

```
HOST=ALIAS=www.yyyyyy.co.jp  
SVRFILE=ALIAS,./host.conf
```

5.5.2 セッション管理方法

セッション管理に Cookie を使用していて、以下のことに当てはまる場合は設定の追加を行います。

- Set-Cookie ヘッダー domain 属性
domain 属性が記述されていて、そのドメインが IceWall サーバーのホストのドメインではない場合、ホスト設定ファイルでキーワード変換を使用して domain 属性を削除します。

(例) Set-Cookie: name=value; domain=zzz.co.jp

```
REPKEY=domain=zzz.co.jp,
```

- Set-Cookie ヘッダー secure 属性
secure 属性が記述されていて、IceWall が SSL を使用していない場合、ホスト設定ファイルでキーワード変換を使用して secure 属性を削除します。

(例) Set-Cookie: name=value; secure

```
REPKEY=; secure,
```

5.5.3 Set-Cookie ヘッダーのフォーマットに関する注意点

直接送信方式を行う場合、以下の点に注意してください

- Set-Cookie ヘッダーのセパレーターとして使用できる文字は「;」のみです。
- 複数の Cookie を Set-Cookie ヘッダーへ記述することはできません。複数の Cookie をセットしたい場合は、Set-Cookie ヘッダーをそれぞれ複数行記述してください。

誤った記述方法

```
Set-Cookie: 名前 1= 値 1; 名前 2= 値 2; expires= 日時; path= 送信パス; domain= ドメイン名
```

```
Set-Cookie: 名前 1= 値 1; expires= 日時; path= 送信パス; domain= ドメイン名
```

正しい記述方法

```
Set-Cookie: 名前 1= 値 1; expires= 日時; path= 送信パス; domain= ドメイン名
```

```
Set-Cookie: 名前 2= 値 2; expires= 日時; path= 送信パス; domain= ドメイン名
```

5.5.4 自動フォーム認証に失敗した場合の動作について

送信データの不備（パスワード間違い等）により自動フォーム認証に失敗し、再度バックエンド Web サーバーからログイン画面が送信された場合、バックエンド Web サーバーから送信されたログイン画面がそのままクライアントに送信されます。

これは、自動フォーム認証の結果に対して、再度自動フォーム認証が行われるということがないためです。

ただし、バックエンド Web サーバーからのフォーム認証の結果がリダイレクトレスポンスの場合、リダイレクトによりアクセスされたコンテンツが自動フォーム認証の対象と判断されると、自動フォーム認証のループが発生する可能性があることに注意してください。

5.5.5 Domain Gateway Option for UNIX を導入している場合

Domain Gateway Option for UNIX は、IceWall SSO へのログインでは「ユーザー ID のみ」で認証されるフェデレーション認証を使用しています。このため、自動フォーム認証ではログイン時に入力されたパスワードを指定する「DEFAULTPWD」が使用できないことに注意してください。

6 フォーム設定サンプル

本章では自動フォーム認証設定のサンプルとして、IceWall SSO の多段構成時における後段 IceWall SSO への自動ログインの設定内容をご紹介します。

6.1 IceWall SSO 多段自動フォームサンプル（直接送信方式）

IceWall SSO の多段構成で直接送信方式を使用する場合のサンプルです。

■ ホスト設定ファイル

ここでは、IceWall SSO のログインに関するフォーム認証設定を From 認証設定ファイルに行うものとします。フォームグループ名は「IW」です。

```
# IceWall SSO 多段フォーム認証
FORM_FILE=IW,/form_iw.conf
```

■ Form 認証設定ファイル (form_iw.conf)

IceWall SSO が多段構成の場合は、後段 IceWall SSO がログイン時に必要としているデータが自動フォーム認証機能の設定を行う前段 IceWall SSO 側で自身へのログイン要求と誤認識されないようにしなければなりません。ここでは、後段の IceWall SSO にてログイン情報に関する設定 (POSTKEY_LOGIN 項目) を変更しているものとします。後段 IceWall SSO へのログインで使用するユーザー ID・パスワードは、前段 IceWall SSO へのログインで使ったものをそのまま使用する例です。

また、IceWall SSO がログイン要求時に動的に設定する項目では、送信データを固定の文字列やユーザー情報ではなく、送信されたログイン画面より取得していることに注目してください。

```
# IceWall SSO 多段フォーム認証
FORM_METHOD=IW,POST
FORM_SEND=IW,/fw/dfw
FORM_URL=IW,/fw/dfw
FORM_KEY=IW,IceWall SSO - Login -
FORM_DATA_USR=IW,POSTDATA,ACCOUNTUID,DEFAULTUID
FORM_DATA_USR=IW,POSTDATA,PASSWORD,DEFAULTPWD
FORM_DATA_PAGE=IW,POSTDATA,HIDEURL,HIDEURL
FORM_DATA_PAGE=IW,POSTDATA,LOGIN,LOGIN
```

6.2 IceWall SSO 多段自動フォームサンプル（間接送信方式）

IceWall SSO の多段構成を行う場合、前段 IceWall SSO のログイン直後のアクセスで後段 IceWall SSO へのログインが発生することが十分に考えられます。

IceWall SSO はログイン直後にリダイレクトレスポンスをブラウザーに送信するため、

前段 IceWall SSO のログイン直後に後段 IceWall SSO のログインが発生する場合には、同じ URL に対して 2 回連続でリダイレクトレスポンスをブラウザに送信することになります。この場合「2 回連続のリダイレクトが実行されない」ブラウザ側の制限により、ブラウザ側でログインシーケンスが停止してしまいます。これを回避するために間接送信方式を使用します。

■ ホスト設定ファイル

直接送信方式同様に、IceWall のログインに関するフォーム認証設定を From 認証設定ファイルに行うものとします。フォームグループ名は「IW」です。

```
# IceWall SSO 多段フォーム認証
FORM_FILE=IW,./form_iw.conf
```

■ Form 認証設定ファイル (form_iw.conf)

直接送信方式と設定が異なるのは、間接送信テンプレート HTML が設定されていることと、データ送信の設定が異なることです。データ送信に関する設定では、間接送信テンプレート HTML へ必要な情報を格納するための置換キーワードが設定されています。

```
FORM_METHOD=IW,POST
FORM_SEND=IW,/fw/dfw
FORM_URL=IW,/fw/dfw
FORM_HTML=IW,./autologin_iw.html
FORM_KEY=IW,IceWall SSO - Login -
FORM_DATA_USR=IW,NOENCVAL,IW-USERID,BACKUID
FORM_DATA_PSW=IW,NOENCVAL,IW-PASSWORD,BACKPWD
FORM_DATA_PAGE=IW,NOENCVAL,IW-HIDEURL,HIDEURL
FORM_DATA_LOGIN=IW,NOENCVAL,IW-LOGINKEY,LOGIN
```

■ 間接送信テンプレート HTML (autologin.html)

Form 認証設定ファイルにて設定された送信データの置換用キーワードが、間接送信テンプレート HTML 内では「\$ 置換キーワード」のように記述しなければならないことに注意してください。

```
<HTML>
<HEAD>
<TITLE>Login Page</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--
function LoadData()
{
    document.form.submit();
}
//-->
```

```
</SCRIPT>
</HEAD>
<BODY onLoad="LoadData();">
<FORM NAME="form" METHOD="$METHOD" ACTION="$ACTION">
  <INPUT TYPE="hidden" NAME="ACCOUNTUID" VALUE="$IW-USERID">
    <INPUT TYPE="hidden" NAME="PASSWORD" VALUE="$IW-
PASSWORD">
  <INPUT TYPE="hidden" NAME="HIDEURL" VALUE="$IW-HIDEURL">
  <INPUT TYPE="hidden" NAME="LOGIN" VALUE="$IW-LOGINKEY">
</FORM><P><BR>
<DIV ALIGN="center">IceWall にログインしています </DIV>
</BODY>
</HTML>
```