



IceWall SSO

Version 10.0

Web Application 開発者マニュアル

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. B2873-97008

Rev.100819A

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・パッカー社社の商標です。

Adobe は Adobe Systems Incorporated の米国及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 及びその子会社、関連会社の米国及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 基本構成	2
3 基本機能	3
3.1 ログイン機能	3
3.2 ログアウト機能	3
3.3 アクセス制御機能	3
3.4 セッション管理機能	3
3.5 情報継承機能	4
3.6 URL 変換機能	4
3.7 キーワード変換機能	5
3.8 リバースプロキシ機能	5
3.9 パスワード変更機能	5
3.10 アクセス記録機能	5
3.11 SSL 通信機能	5
3.12 フェイルオーバー機能	5
3.13 クライアント認証機能	5
3.14 自動フォーム認証機能	5
4 IceWall SSO によるアプリケーション開発の概要	6
4.1 動作モデル	7
4.1.1 IceWall SSO 経由で静的コンテンツを表示する場合	7
4.1.2 IceWall SSO 経由で CGI を実行する場合	8
5 バックエンド Web サーバーとの接続方法	10
5.1 認証を必要としないバックエンド Web サーバーとの接続	10
5.2 ベーシック認証を必要とするバックエンド Web サーバー	10
5.3 HTTP ヘッダーよりユーザー ID を取得するアプリケーション	10
5.4 フォーム認証を必要とするアプリケーション	10
6 バックエンド Web サーバー側での制約	12
6.1 HTTP リクエストヘッダー（フォワーダー → バックエンド Web サーバー）	12
6.1.1 注意が必要なヘッダー	12
6.1.2 追加されるヘッダー	13
6.1.3 HTTP ヘッダーに含まれる文字コードについて	14
6.1.4 URL に含まれる特殊文字のエンコードについて	14
6.2 HTTP レスポンスヘッダー（バックエンド Web サーバー → フォワーダー）	15
6.2.1 注意が必要なヘッダー	15
6.2.2 HTTP ヘッダーに含まれる文字コードについて	15
6.3 バックエンド Web サーバーとの通信	15
6.3.1 通信プロトコルのバージョンについて	15
6.3.2 KeepAlive 設定について	15
6.3.3 クライアントからのベーシック認証送信について	16
6.3.4 リバースプロキシモードにおけるベーシック認証設定について	16
6.3.5 SSL 接続のバージョンおよび使用できる暗号化方式について	16

6.3.6 Apache の SSL 3.0 cipher について	16
6.3.7 日本語のフォルダー名およびファイル名について	16
6.4 環境変数	17
6.4.1 REMOTE_ADDR および REMOTE_HOST	17
6.4.2 REMOTE_USER	17
6.4.3 CLIENT_CERT(Web サーバーが Apache の場合は SSL_CLIENT_CERT)	17
6.5 セッション管理	17
6.5.1 セッションの例	18
6.5.2 セッション管理の利用例	19
6.5.3 セッションタイムアウトに関する考慮点	19
7 HTML 構文	21
7.1 タグの記述方法	21
7.1.1 大文字小文字の扱い	21
7.1.2 属性値の扱い	21
7.1.3 文字コードの扱いについて	22
7.2 認識不可能なタグの記述	22
7.2.1 タグ名にスペース / タブ / 改行が含まれている場合	22
7.2.2 属性名にスペース / タブ / 改行が含まれている場合	22
7.2.3 タグ名と属性名の間にスペース / タブ / 改行がない場合	23
7.2.4 他の属性値と属性名の間にスペース / タブ / 改行がない場合	23
8 URL 変換	24
8.1 URL 変換の対象コンテンツ	24
8.2 URL 変換の変換対象	24
8.2.1 自動的に変換される URL	25
8.2.2 変換する必要のない URL	26
8.2.3 変換する設定を行っても変換されない URL	26
8.2.4 変換不可能な URL	27
8.2.5 抽出対象となる URL	27
8.2.6 1 つのタグ内で属性名の異なる複数の属性の URL 変換 10.0	28
8.3 URL 記述制限	29
8.3.1 ホスト名記述の統一	29
8.3.2 ドキュメントルートをさかのぼるパス	30
8.3.3 "http" もしくは "/" で始まらない URL	30
8.3.4 コメント内に記述された URL	30
8.3.5 BASE タグ使用時の URL 変換	31
8.3.6 URL と引数 (Query String) のセパレーターについて	31
8.3.7 バックエンド Web サーバー上のコンテンツの絶対 URL を記述する際の制限	32
8.4 Java アプレット	32
8.4.1 ダウンロード	32
8.4.2 アプレットからの IceWall SSO 経由の通信	32
8.5 ActiveX	33
8.5.1 ダウンロード	33
8.6 その他のファイル	34
8.6.1 ダウンロード	34
9 キーワード変換	35

9.1 キーワード変換機能の注意事項	35
9.1.1 変換対象	35
9.1.2 大文字小文字の区別	35
9.1.3 ユニークな検索文字列の使用	35
9.1.4 検索文字列の予約語化	36
9.1.5 コンテンツの文字コードについて	36
9.1.6 変換できない文字列 10.0	36
9.2 特定キーワード変換機能	36
9.2.1 特定キーワードとは	36
9.2.2 変換順序	36
9.2.3 特定キーワード一覧 10.0	37
9.2.4 特定キーワードの使用例	38
9.2.5 制限事項	39
10 JavaScript	40
10.1 クライアントサイド JavaScript	40
10.1.1 スクリプトにより出力されるタグ内の URL	40
10.1.2 関数の引数として使用される URL	40
10.1.3 クロスサイトスクリプティング対策フィルター使用時の注意	41
10.2 サーバーサイド JavaScript	41
10.2.1 サーバーオブジェクト	42
11 VBScript	43
11.1 VBScript 使用時の注意事項	43
11.1.1 スクリプトにより出力されるタグ内の URL	43
11.1.2 クロスサイトスクリプティング対策フィルター使用時の注意	43
11.2 アクティブサーバーページ (ASP)	43
11.2.1 Request オブジェクト	43
12 XML	45
13 バックエンド Web サーバーで設定された Cookie の扱い	46
13.1 Cookie に domain 属性が指定されていない場合	46
13.2 Cookie に domain 属性が指定されている場合	46
13.3 Cookie に path 属性が指定されていない場合	46
13.4 Cookie に path 属性が指定されている場合	47
13.5 Cookie に secure 属性が指定されている場合	47
13.6 使用可能な Cookie の上限について	47
13.7 Set-Cookie ヘッダーのフォーマットに関する注意点	47
14 エージェント導入における制限について	49
14.1 認証機能の排除	49
14.2 URL 変換およびキーワード変換について	49
14.3 アクセスログについて	49
14.4 クライアント証明書使用時について	49

1 はじめに

IceWall SSO は、複数のバックエンド Web サーバーのアプリケーションに対して、Single Sign On 型の認証と認可機能を提供するソフトウェアです。IceWall SSO を使用することで、バックエンド Web サーバーのアプリケーション開発者は認証、認可およびセキュリティの開発工数を減らすことができます。

本書は IceWall SSO を用いたバックエンド Web サーバーのアプリケーション開発に必要とされる情報を記述します。

基本的にはログインやアクセス制御を行う SSO モードでの動作を中心に記述しますが、認証を必要としない Reverse Proxy モードにおける注意点や、Agent Option を使用した場合の動作は、解説が必要な部分のみ記載します。

なお、Agent Option の導入および使用方法については「IceWall SSO 導入ガイド for Agent Option」、IceWall MCRP を使用した場合のバックエンド Web サーバーのアプリケーション開発については「IceWall MCRP Web Application 開発者マニュアル」をそれぞれ参照してください。

1.1 文中におけるバージョン表示記号について

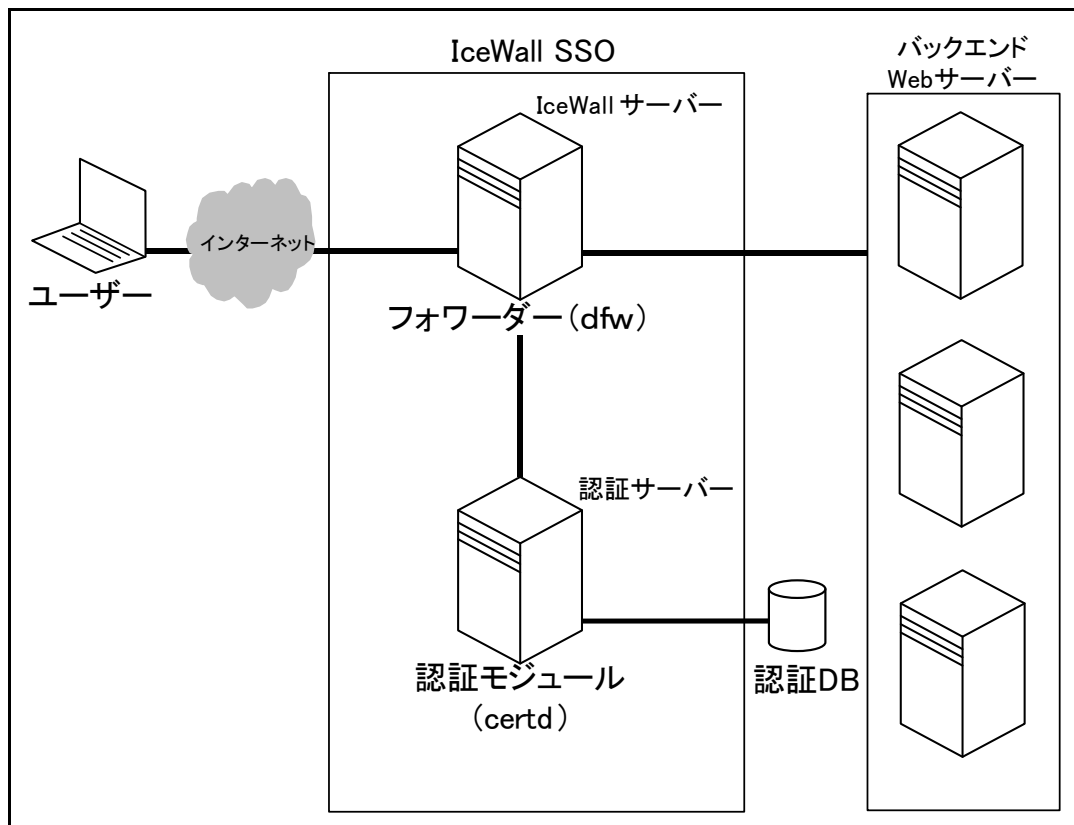
記述中に付加されているバージョン表示記号は以下の意味を表します。

表示記号	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。
⑩.0	楕円で囲まれているバージョンで仕様変更もしくは機能追加された項目です。この場合、10.0 にて仕様変更または機能追加されたことを表します。

2 基本構成

IceWall SSO は Single Sign On 型認証を実現するためのミドルウェアで、フォワーダー (dfw)、認証モジュール (certd) の 2 つのモジュールから構成されています。

なお、フォワーダーが動作するサーバーを「IceWall サーバー」、認証モジュールが動作するサーバーを「認証サーバー」と呼びます。



3 基本機能

IceWall SSO が提供する機能は、次のとおりです。

3.1 ログイン機能

ユーザーがバックエンド Web サーバー上のコンテンツにアクセスを開始する際に使用する機能です。ユーザー ID、パスワードなどの認証を認証 DB（ディレクトリサービスやデータベース）と連携して行います。

3.2 ログアウト機能

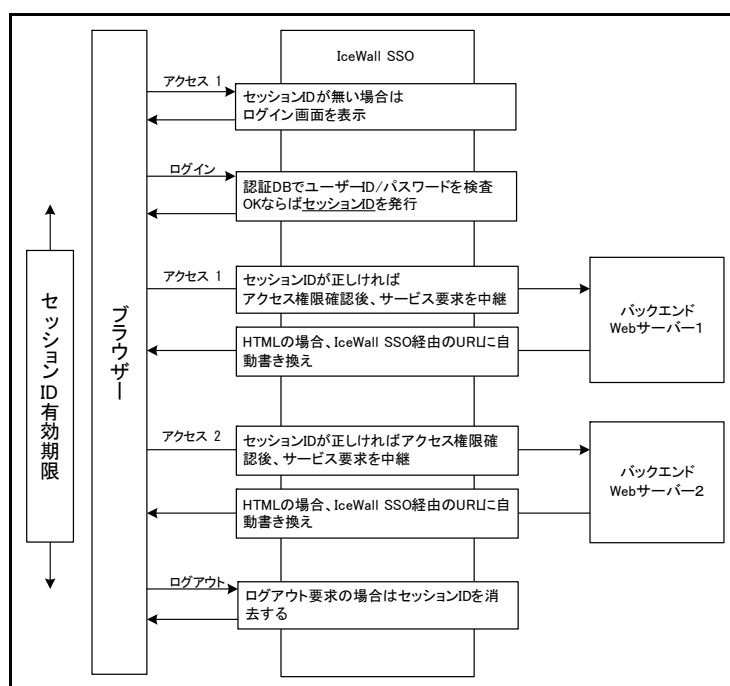
ユーザーがバックエンド Web サーバーへのアクセスを終了する際に使用する機能です。本機能を使用すると、ユーザーはバックエンド Web サーバーにアクセスできなくなります。（再びバックエンド Web サーバーにアクセスするためには「ログイン機能」を使用します）

3.3 アクセス制御機能

認証されたユーザーの所属するグループの認可情報に基づいて、バックエンド Web サーバー上のコンテンツへのアクセスを制御する機能です。

3.4 セッション管理機能

IceWall SSO では Single Sign On の管理にセッション ID を利用します。セッション ID により認証（ログイン状態）の確認をするとともに、ユーザーのアクセス制御（URL ごとのアクセス許可／禁止）を実施する機能です。



注) セッション ID は、ブラウザには Cookie または URL-Cookie (Query-String ではなく、URL のパスの一部にセッション ID を埋め込む形式) として設定されます。Cookie の名称は任意に指定可能です (デフォルトは IW_INFO です)。

3.5 情報継承機能

ユーザーのログイン情報、認証 DB 上の情報を、HTTP ヘッダーの形でバックエンド Web サーバーに渡す機能です。バックエンド Web サーバーのアプリケーションは、この情報を環境変数などとして受け取ります。指定された認証 DB のカラムの内容をバックエンド Web サーバーに渡すためには、IceWall SSO 設定ファイル (ホスト設定ファイル) で指定します。

3.6 URL 変換機能

バックエンド Web サーバーから受信したコンテンツに含まれる URL を、IceWall サーバー経由の URL に変更する機能です。バックエンド Web サーバー情報をユーザーより隠蔽するために使用します。

コンテンツの中の URL は、すべて IceWall サーバーのサブディレクトリに変換されるため、ユーザーにはあたかも 1 台の Web サーバーにアクセスしているように見えます。

3.7 キーワード変換機能

バックエンド Web サーバーから受信した、コンテンツに含まれる文字列を、指定した文字列に変換する機能です。上記 URL 変換機能が変換できない文字列に対して使用することができます。

3.8 リバースプロキシ機能

クライアントからのアクセス要求を、IceWall サーバーがバックエンド Web サーバーに代行して受け付ける機能です。IceWall サーバーは URL を解析し、バックエンド Web サーバーに情報を中継します。

クライアントからのアクセスは、すべて IceWall サーバーを経由するので、IceWall サーバーを要塞化することで、非常にセキュリティの高いシステムを構築できます。

3.9 パスワード変更機能

ユーザー自らが、認証 DB 上のパスワードを変更するための機能です。設定ファイルで詳細なパスワードポリシーの設定ができます。

3.10 アクセス記録機能

IceWall サーバー経由でユーザーがアクセスした記録を残す機能です。管理者はこの記録により、ユーザーごとの利用頻度や操作履歴を分析できます。

3.11 SSL 通信機能

IceWall サーバーとバックエンド Web サーバ間には HTTP 通信の他に HTTPS(HTTP over SSL) 通信も使用できます。したがって、インターネット上にあるバックエンド Web サーバーに対しても、安全な Single Sign On が可能です。

3.12 フェイルオーバー機能

システム可用性の向上のため、フォワーダーが代替バックエンド Web サーバーおよび代替認証サーバーを使用できる機能です。

3.13 クライアント認証機能

クライアント証明書を利用した本人確認を行う機能です。ブラウザーにクライアント証明書を入れることにより、より高度な本人確認を実現します。

3.14 自動フォーム認証機能

バックエンド Web サーバーのアプリケーションへログインするための認証フォームに対して自動的にログインを行う機能です。さまざまな形態のフォームに対応が可能です。

4 IceWall SSO によるアプリケーション開発の概要

IceWall SSO は、ブラウザからの情報をバックエンド Web サーバーに中継します。このとき、HTTP ヘッダー情報は IceWall SSO により一部変更および追加されます。

IceWall SSO は、バックエンド Web サーバーから送信されたコンテンツ内の URL を、IceWall SSO のパスに変換してブラウザに返します。これにより、バックエンド Web サーバーのコンテンツ内の URL を、IceWall サーバーのサブディレクトリとしてブラウザに見せることができます。また、バックエンド Web サーバーから送信された HTTP ヘッダー情報も、IceWall SSO により一部変更および追加されます。

IceWall SSO を利用したシステムのアプリケーションを開発する場合、次の各項目を考慮する必要があります。

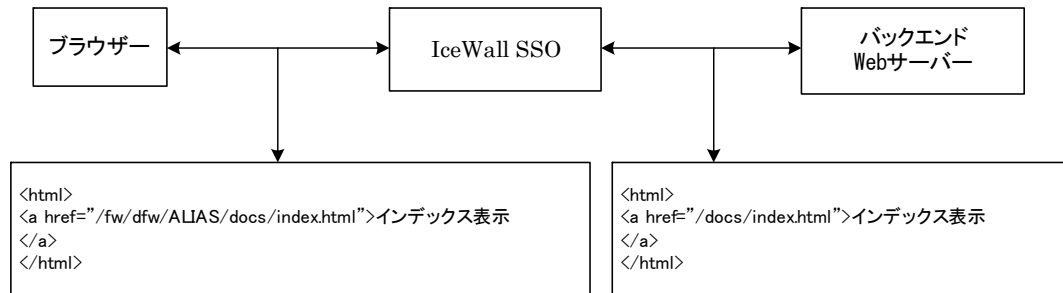
- (1) IceWall サーバーからバックエンド Web サーバーへの接続方式の検討
- (2) IceWall サーバーからバックエンド Web サーバーへ引き渡される情報
- (3) バックエンド Web サーバーへ引き渡される情報の利用方法
- (4) IceWall SSO で対応している HTML 構文
- (5) URL 変換機能およびキーワード変換機能
- (6) (5) の変換機能の対象となるホスト名または文字列
- (7) JavaScript を使用している場合は、その注意事項
- (8) IceWall SSO のタイムアウトとアプリケーションのタイムアウト

これらの項目を考慮した上でアプリケーション開発者は、必要に応じてコンテンツの見直し、また IceWall SSO 管理者に対して IceWall SSO 側の環境設定を依頼してください。

4.1 動作モデル

IceWall SSO の動作説明に下記のモデルを使用します。

4.1.1 IceWall SSO 経由で静的コンテンツを表示する場合



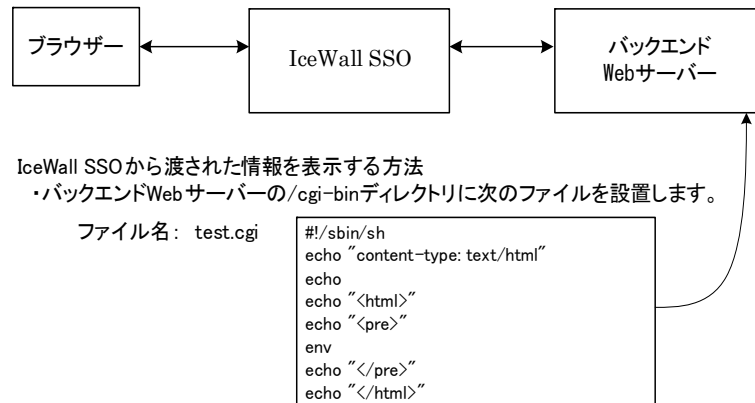
IceWall SSO は、バックエンド Web サーバーの HTML の中に記述された URL から IceWall SSO 経由の URL への書き換えを自動的に行います。上記の例では、バックエンド Web サーバーを“ALIAS”として定義しています。

バックエンド Web サーバーでは、特定のスクリプト (JavaScript など) を除き、IceWall SSO を意識することなく HTML コンテンツを準備することができます。(JavaScript については「10 JavaScript」を参照してください)

IceWall SSO が自動的に書き換える HTML タグの例

- <a href=
- <base href=
- <frame src=
- <form action=
- <base target=
- <img src=
- <script src=
- <body background=
- <td background=
- <tr background=
- <table background=
- <applet codebase=
- <input src=

4.1.2 IceWall SSO 経由で CGI を実行する場合



(1) IceWall SSO から渡された情報を表示する方法

- ・バックエンド Web サーバーの/cgi-bin ディレクトリに次のファイルを設置します。
ファイル名: test.cgi
- ・この CGI をブラウザから起動します。
URL=http://[IceWall SSO のホスト名]/fw/dfw/ALIAS/cgi-bin/test.cgi
- ・CGI で利用できる情報がブラウザに表示されます。

```
_=/usr/bin/env
LANG=C
HTTPS=OFF
HTTP_JYUUSYO=Tokyo-to
HTTP_NAME=Taro Yamada
PATH=/sbin:/usr/sbin:/usr/bin
REMOTE_HOST=127.0.0.1
HTTP_HOST= バックエンド Web サーバー
GATEWAY_INTERFACE=CGI/1.1
HTTP_ACCEPT_ENCODING=gzip
HTTP_SERVER_SOFTWARE=Netscape-Enterprise/3.6 SP3
HTTP_CONNECTION=close
SERVER_SOFTWARE=Netscape-Enterprise/3.6 SP3
HTTP_UID=user01
SERVER_URL=http:// バックエンド Web サーバー
REQUEST_METHOD=GET
HTTP_ACCEPT_CHARSET=Shift_JIS,*,utf-8
HTTP_USER_AGENT=Mozilla/4.7 [ja] (WinNT; I)
HTTP_ACCEPT=image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
HTTP_ACCEPT_LANGUAGE=ja,en
SCRIPT_NAME=/cgi-bin/test.cgi
SERVER_PORT=80
SERVER_PROTOCOL=HTTP/1.0
REMOTE_ADDR=127.0.0.1
TZ=JST-9
HTTP_COOKIE=IW_INFO=458f8945e6d0edfbc6f642a98a3ba8
```

(2) IceWall SSO から渡された情報を基に表示内容を変更する方法

- ・ バックエンド Web サーバーの /cgi-bin ディレクトリに次のファイルを設置します。
(IceWall SSO からユーザー情報として Name ヘッダーが送信される場合の例です)

ファイル名: test2.cgi

```
#!/sbin/sh
echo "content-type: text/html"
echo
echo "<html>"
echo "<h1>ようこそ"
echo $HTTP_NAME
echo "さん</h1>"
echo "</html>"
```

- ・ この CGI をブラウザから起動します。
URL=http://[IceWall SSO のホスト名]/fw/dfw/ALIAS/cgi-bin/test2.cgi
- ・ ブラウザーには利用者情報を反映した画面が表示されます。

ようこそ Taro Yamada さん

5 バックエンド Web サーバーとの接続方法

5.1 認証を必要としないバックエンド Web サーバーとの接続

認証を必要としないバックエンド Web サーバーとの接続では特に考慮する問題はありません。

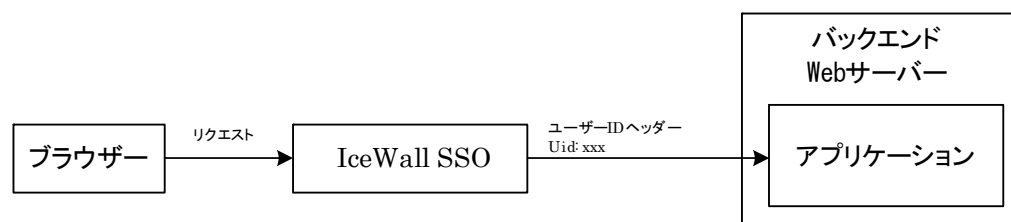
5.2 ベーシック認証を必要とするバックエンド Web サーバー

IceWall SSO からバックエンド Web サーバーにはベーシック認証を使用して接続することが可能です。デフォルトでは、IceWall のログイン時に入力したユーザー ID とパスワードをベーシック認証のユーザー ID とパスワードに使用することができます。バックエンド Web サーバーで認証を行うユーザー ID とパスワードを認証 DB の任意のカラムを選択することで、IceWall のユーザー ID とパスワードとは異なるユーザー ID とパスワードでバックエンド Web サーバーのベーシック認証とすることも可能です。



5.3 HTTP ヘッダーよりユーザー ID を取得するアプリケーション

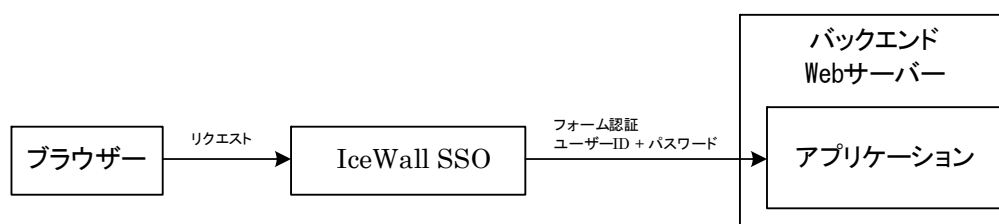
IceWall SSO は、リクエストを行ったユーザーのユーザー ID を HTTP ヘッダーでバックエンド Web サーバーへ通知します。バックエンド Web サーバー上のアプリケーションでユーザー ID を環境変数またはヘッダー情報として取得することができます。



5.4 フォーム認証を必要とするアプリケーション

IceWall SSO は、バックエンド Web サーバーのフォーム認証に対して自動的にログインを行い接続することが可能です。その際のユーザー ID・パスワードは固定値、認証 DB のユーザー情報などから任意に選択できます。また、ログイン後にセッション情報など

が Cookie によりクライアントへ通知されるようなアプリケーションでも、自動ログインは対応しています。



6 バックエンド Web サーバー側での制約

IceWall SSO のバックエンド Web サーバーには、以下の制約があります。

6.1 HTTP リクエストヘッダー（フォワーダー → バックエンド Web サーバー）

ブラウザからの HTTP ヘッダーは、基本的に変更されることなくフォワーダーからバックエンド Web サーバーへ送られます。バックエンド Web サーバー側では、その値を HTTP ヘッダー情報として受け取ることができます (CGI プログラムがこの値を参照するには、通常 “HTTP_ ヘッダー名” という名前の環境変数を参照します。例：HTTP_USER_AGENT)。

ただし、以下の点にご注意ください。

- ・ 注意が必要なヘッダーが存在します。(ホスト名など)
- ・ 一部追加されるヘッダーが存在します。
- ・ 認証 DB 上の情報をバックエンド Web サーバーに渡すことができます。
- ・ 特定のヘッダーを送信することを禁止したい場合は、それらのヘッダーをフォワーダーの設定ファイルに指定します。
- ・ ブラウザーよりヘッダーが「xxx_xxx」のように送信された場合でも、「Xxx-Xxx」のように変換されて送信されます。変換のルールは次のとおりです。
 - (1) 先頭を大文字に変換する
 - (2) 「_」を「-」に変換する。
 - (3) 変換された「-」の次の文字を大文字に変換する。
 - (4) これら以外はすべて小文字に変換する。

6.1.1 注意が必要なヘッダー

以下のヘッダーは IceWall SSO により制御が行われるものです。これらのヘッダーはリバースプロキシモードでも同様に制御されます。

ヘッダー名	内容
Referer	リンク元のオリジナル URL です。IceWall サーバー経由のパス名ではありません。
Host	バックエンド Web サーバーのホスト名およびポート番号が送信されます。
Authorization	ブラウザから送信されたものは転送されません。
Destination	COPY、MOVE メソッドでの対象 URI です。IceWall サーバー経由のパス名ではありません。 (主に WebDAV プロトコルで使用されます)

6.1.2 追加されるヘッダー

ブラウザより送信されたヘッダー以外で IceWall SSO が独自に追加するヘッダーです。これらのヘッダーは SSO モードでのみ追加されます。

ヘッダー名	内容
Authorization	ベーシック認証用データを以下のフォーマットで渡します。 Basic ユーザー ID: パスワード (斜体部分は base64 にてエンコードされています) 設定によりこのヘッダーを渡すか否かを指定できます。 (REMOTE_USER を参照します)
セッション ID 名 (10.0)	ログインごとに発行されるユニークなセッション ID (32 桁 /64 桁) を COOKIENAME として設定した名称で Cookie として渡します。(HTTP_COOKIE から取得します) デフォルト: IW_INFO
Session (10.0)	ログインごとに発行されるユニークなセッション ID (32 桁 /64 桁) ※を渡します。(HTTP_SESSION を参照します) バージョン 10.0 より送信ヘッダー名を HEADER_NAME_SID 項目にて自由に変更することが可能です。
Uid (10.0)	ユーザー ID を引き渡します。(HTTP_UID を参照します) バージョン 10.0 より送信ヘッダー名を HEADER_NAME_UID 項目にて自由に変更することが可能です。
トランザクション ID (10.0)	1 回のブラウザからのアクセスごとに発行されるユニークなトランザクション ID を引き渡します。 送信ヘッダー名は、HEADER_NAME_TID 項目にて自由に変更することが可能です。
認証 DB カラム (属性) 名	(構成ファイル中で指定された) カラム名とそのカラムの内容を渡します。(“HTTP_認証 DB カラム名” を参照します)
Description	構成ファイルで “DESCRIPTION” というカラム名を指定した場合にその内容を渡します。(“HTTP_DESCRIPTION” を参照します)
DescriptionNN	“DESCRIPTION” というカラムの内容を「,」で分割し複数のヘッダーとして引き渡します。 ヘッダー名の「NN」は 2 桁のシーケンシャル No. となります。(1 ~ 9 の場合は 01 ~ 09 と必ず 2 桁とします) 例: Description が data1,data2,data3 の場合 Description01: data1 Description02: data2 Description03: data3 構成ファイルで “DESCRIPTION” というカラム名を指定した場合にのみ有効です。(“HTTP_DESCRIPTIONNN” を参照します)

ヘッダー名	内容
任意ヘッダー名	ホスト設定ファイル (sample.conf) の HEADER 項目にて、追加指定された値を渡します。(“HTTP_任意ヘッダー名”を参照します)

※ バックエンドにてセッション ID を取得する場合には、桁数が 32 桁の場合と 64 桁の場合を考慮する必要がありますのでご注意ください。 **10.0**

6.1.3 HTTP ヘッダーに含まれる文字コードについて

IceWall SSO は、HTTP ヘッダーの文字コード変換は行いません。IceWall SSO に認証 DB のユーザー情報を HTTP ヘッダーで転送するように設定した場合も、同様に認証 DB から IceWall SSO が取得した形式の文字コードで送信されます。(変換なし)

ヘッダーの値に漢字やカタカナなどの日本語 (2 バイト文字) が含まれている場合、バックエンド Web サーバーのアプリケーションによっては、リクエストを受信した時点でエラー扱いとなるものもあります。このため、ユーザー情報をバックエンド Web サーバーへ転送する場合は、文字コードに注意する必要があります。

認証 DB の種類	文字コードの扱い
ORACLE	文字コードは ORACLE の言語設定により異なります。
LDAP,MSAD,NED	DB 上に Unicode(UTF-8) で保存されている場合は、IceWall SSO の機能で Shift_JIS などに変換することが可能です。ただし、認証 DB に Microsoft Active Directory を使用する場合は、文字コード変換機能がサポートされていません。
CSV	CSV ファイルに保存されている文字コードがそのまま使用されます。
MySQL	DB 上に保存されている文字コードがそのまま使用されます。

6.1.4 URL に含まれる特殊文字のエンコードについて

ブラウザより送信された URL に特殊文字が含まれている場合、以下に示す文字以外を 16 進コードに変換して、バックエンド Web サーバーへ送信します。なお、URL の後ろに付加される引数 (Query String) は変換されません。

- _ . ! ~ * ' () /

(例) \$ → %24 空白 → %20

また、セミコロン (;) については設定ファイルにて変換の ON / OFF が指定できます。

6.2 HTTP レスponseヘッダー（バックエンド Web サーバー → フォワーダー）

バックエンド Web サーバーより送信された HTTP ヘッダーは、基本的に変更されることなくクライアントへ送られますが、IceWall サーバーの設定ファイルにて送信の制御や任意のヘッダーの追加などが行えます。また、Content-length ヘッダーが送信されない場合には、IceWall サーバーの設定ファイルにて追加の ON / OFF を制御することができます。

6.2.1 注意が必要なヘッダー

以下のヘッダーは、IceWall により制御が行われるものです。これらのヘッダーはリバースプロキシモードでも同様に制御されます。

ヘッダー名	内容
Last-Modified	アクセスしたコンテンツの最終更新日付です。
Location	リダイレクト先として接続する URL です。IceWall サーバー経由の URL に変換されます。

6.2.2 HTTP ヘッダーに含まれる文字コードについて

バックエンド Web サーバーより送信された HTTP ヘッダーの文字コードについては、IceWall SSO での文字コード変換は行わずにブラウザへ送信します。

ヘッダーの値に漢字やカタカナなどの日本語（2 バイト文字）が含まれている場合も同様に、文字コード変換は行わずにブラウザへ送信します。日本語を使用した場合のブラウザの動作は、ブラウザの仕様に依存します。

6.3 バックエンド Web サーバーとの通信

6.3.1 通信プロトコルのバージョンについて

IceWall SSO は、バックエンド Web サーバーとの通信に、HTTP プロトコルのバージョン 1.0 を使用します。ブラウザより IceWall SSO に対してバージョン 1.1 で接続を行っても、IceWall SSO とバックエンド Web サーバーとの通信は、無条件でバージョン 1.0 となります。

6.3.2 KeepAlive 設定について

IceWall SSO からバックエンド Web サーバー間の通信では、バックエンド Web サーバーの KeepAlive の設定を無効、または KeepAliveTimeout の設定を 0（ゼロ）としてください。

バックエンド Web サーバーの設定によっては、KeepAlive の設定により、レスポンス遅延の原因となる場合があります。

もし、KeepAlive の設定を変更できないバックエンド Web サーバーの場合は、ホスト設定ファイルの「CLOSETIME」項目を設定し、フォワーダーとバックエンド Web サーバー間の切断待ち時間を調整してください。

ただし、バックエンド Web サーバーが Microsoft Internet Information Services の場合は、Web サーバーインスタンスの KeepAlive 設定は有効にして使用することをお勧めします。無効にして使用すると、コンテンツが表示されても、Web サーバーからの通信が完了しないままの状態になる場合があります。

6.3.3 クライアントからのベーシック認証送信について

バックエンド Web サーバーより送信されたベーシック認証要求をブラウザに送信した場合、ブラウザ側でユーザー ID とパスワードを入力しても、その情報はバックエンド Web サーバーへは転送されません。フォワーダーがリバースプロキシモードで動作している場合と、認証不要対象に設定された URL の場合も同様に転送されません。

6.3.4 リバースプロキシモードにおけるベーシック認証設定について

リバースプロキシモードで動作している場合は、IceWall SSO によるユーザー認証が発生しないため、バックエンド Web サーバーに対してのベーシック認証は行えません。また、認証不要対象に設定された URL に対しても同様にベーシック認証は行えません。

6.3.5 SSL 接続のバージョンおよび使用できる暗号化方式について

SSL Option を使用してバックエンド Web サーバーと SSL 通信を行う場合、サポートされるバージョンは SSL 3.0 のみとなります。SSL 2.0 は接続できません。

また、IceWall SSO で使用できる暗号化方式は IceWall サーバー上で「openssl ciphers」コマンドを実行することで確認することができます。

フォワーダー自体には制限がなく、IceWall サーバーの動作環境に依存します。

6.3.6 Apache の SSL 3.0 cipher について

バックエンド Web サーバーが Apache の場合、SSL 3.0 の cipher として「TripleDES」を設定しないようにしてください。設定している場合は、通信パフォーマンスが著しく低下する場合があります。

6.3.7 日本語のフォルダー名およびファイル名について

URL は、RFC2396(URI) にて規定されている Unreserved Characters 以外の文字は URL エンコードされた形でリクエストされるため、日本語のフォルダー名やファイル名もアクセスが可能です（すべての日本語を保証するものではありません）。

6.4 環境変数

環境変数は、CGI プログラムあるいは SSI(Server Side Include) が、実行中に参照するものです。これらの変数には、ブラウザからのアクセスが IceWall サーバーを経由した場合と、経由しない場合で値が変化するものがあります。

6.4.1 REMOTE_ADDR および REMOTE_HOST

通常は、リクエストを要求したクライアントの IP アドレスおよびホスト名が環境変数 REMOTE_ADDR、REMOTE_HOST (CGI の場合) にそれぞれセットされます。ただし、この要求がフォワーダーを経由した場合には、IceWall サーバーの IP アドレスおよびホスト名が環境変数に設定されます。

クライアントの IP アドレスおよびホスト名を取得する場合は、IceWall サーバーで取得できる環境変数を HTTP ヘッダーとして送信することで取得することが可能となります。以下はその設定例です。

```
HEADER=REMOTE_ADDR,REMOTE_ADDR
```

```
HEADER=REMOTE_HOST,REMOTE_HOST
```

なお、バックエンド Web サーバーでこの情報は HTTP ヘッダー情報として送信されるため、環境変数 HTTP_REMOTE_ADDR、HTTP_REMOTE_HOST として取得しなければなりません。

6.4.2 REMOTE_USER

IceWall SSO は、認証されたユーザー ID およびパスワードを Authorization ヘッダーにてベーシック認証形式で送信することができます。バックエンド Web サーバー側でベーシック認証機能の設定を行うことにより、環境変数 REMOTE_USER で認証済みユーザー ID が参照できます。

6.4.3 CLIENT_CERT(Web サーバーが Apache の場合は SSL_CLIENT_CERT)

ブラウザとフォワーダー間でクライアント証明書を使用している場合、証明書情報はバックエンド Web サーバーには転送されません。この証明書情報が必要な場合は以下の設定を IceWall サーバーに行うことで取得が可能となります。

○フォワーダーの Web サーバーが Apache HTTP Server の場合に、クライアントの証明書のサブジェクト DN を転送する場合

```
HEADER=SSL_CLIENT_S_DN,SSL_CLIENT_S_DN
```

この証明書情報は HTTP ヘッダーの 1 つとして送信されるため、フォワーダーとバックエンド Web サーバー間の認証には使用できません。また、バックエンド Web サーバー側で環境変数として取得する場合は「HTTP_SSL_CLIENT_S_DN」となります。

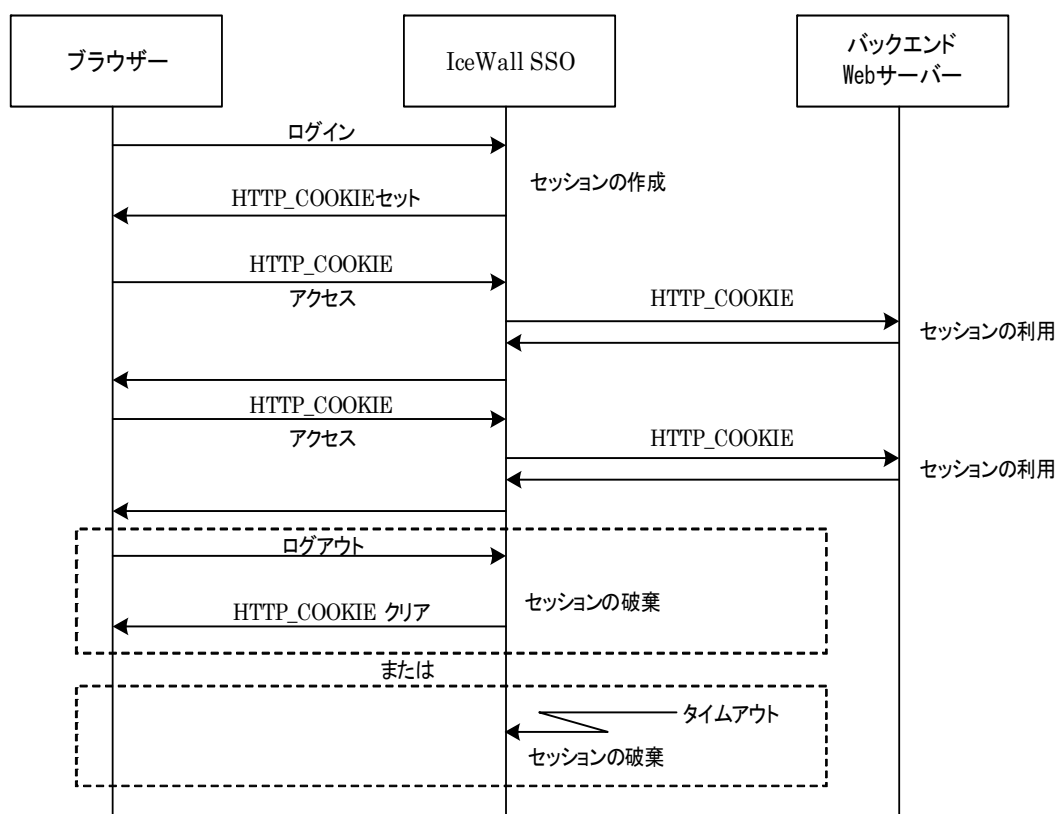
6.5 セッション管理

IceWall SSO では、ログインしたユーザーに対してセッション ID を発行します。セッション ID は、IceWall SSO へのログイン後からログアウトするまでの間有効です。こ

の間は、バックエンド Web サーバーに対して、いつも同じセッション ID が送信されます。バックエンド Web サーバーのアプリケーションでは、本セッション ID を参照することで、ログイン後の継続した処理であることが判断できます。また、ログアウト操作を行わないで放置された場合のことも考慮した、最終アクセスからの経過時間によって自動でログアウトを行う機能も備えられています。

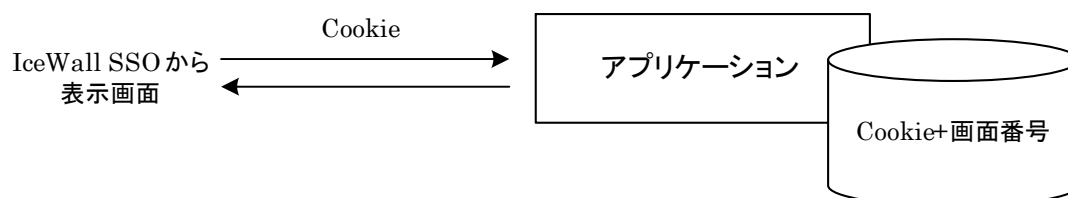
6.5.1 セッションの例

以下に IceWall SSO のセッションの例を記述します。



6.5.2 セッション管理の利用例

IceWall SSO のセッション ID とアプリケーションが管理する画面番号により、画面遷移を実現する場合の例を記述します。前提条件として、データベースに画面管理用のテーブルを作成し、アプリケーションにて画面遷移を管理します。



上記のような構成で、IceWall SSO のセッションと画面番号を管理することにより、画面のシーケンスが正しく流れていることを確認できます。正しく流れていれば次の画面を表示し、不正な順番であれば最初の画面に戻すなどの制御を行うことができます。

6.5.3 セッションタイムアウトに関する考慮点

IceWall SSO の自動タイムアウトとは別に、バックエンド Web サーバー側のアプリケーションにてタイムアウト管理を行う場合は、以下の点を考慮してください。

IceWall SSO のタイムアウトとアプリケーションのタイムアウトについて

- (1) バックエンド Web サーバー側のアプリケーションにてタイムアウト管理を行う場合には、IceWall SSO のタイムアウトよりアプリケーションのタイムアウトを長く設定します。
- (2) IceWall SSO のタイムアウトよりアプリケーションのタイムアウトが短い場合 IceWall SSO のセッション中に、アプリケーション側でタイムアウトが発生する可能性があります。
- (3) IceWall SSO のタイムアウトよりアプリケーションのタイムアウトが長い場合 通常は、IceWall SSO のタイムアウトがアプリケーションのタイムアウトより先に発生しますが、利用の仕方次第では、アプリケーションで先にタイムアウトが発生する可能性があります。

タイムアウト処理の対応について

- (1) IceWall SSO のタイムアウトより先にアプリケーション側でタイムアウトが発生した場合
アプリケーション側でタイムアウトが発生した場合、アプリケーション側でタイムアウト画面を表示するなどエラー処理を行ってください。
- (2) IceWall SSO のタイムアウトがアプリケーションのタイムアウトより先に発生した場合
IceWall SSO のタイムアウトが発生した場合は、アプリケーションの処理が途中でであっても、IceWall SSO の認証用ログインページが表示されます。ここでの認

証後のアプリケーションシーケンスは、IceWall SSO のセッション ID を参照するか・しないかによって、動作が以下のように異なります。

- ・ IceWall SSO のセッション ID を参照しない場合
認証後は、認証前に行っていた処理を継続できます。
- ・ IceWall SSO のセッション ID を参照する場合
認証後は、新たなセッション ID が生成されるため、中断された処理を継続しようとする、セッション ID の不整合が発生します。この場合の回避方法は、以下の 2 とおりとなります。
 - (方法 1) アプリケーション側で、旧セッション ID に対するログアウト処理を行います。旧セッション ID を削除後、新セッション ID によりアプリケーション側の新セッションを開始するものとして、Top 画面へ遷移します。
 - (方法 2) 旧セッション ID を新セッション ID に更新し、Top 画面へ遷移します。(事実上セッション ID を参照しないことと同じになります)

*タイムアウト時の POST データについて

IceWall SSO では、ログイン処理後のアクセスは GET メソッドにより行われます。このため、POST でのデータ処理を行うタイミングで IceWall SSO のタイムアウトが発生した場合は、その直前の画面で操作された POST データは破棄され、IceWall SSO のデータ送信エラー画面が表示されます。
この場合はフォームデータを再入力させるなどのリカバリーが必要となります。

なお、8.0 R3 以降のバージョンでは「POST データ継承機能」を使用することで、IceWall SSO のタイムアウト時に送信された POST データを IceWall SSO へのログイン後に再送させる機能が搭載されています。ただし、以下の制限があることに注意してください。

- ・ Content-type が application/x-www-form-urlencoded である。
- ・ POST データのデータ長が 1024 バイト以内である。
- ・ JavaScript に対応したブラウザを使用する。

7 HTML 構文

IceWall SSO で HTML 構文を使用する場合は、以下の項目に注意してください。

7.1 タグの記述方法

IceWall SSO を使用する場合は HTML 構文は、標準リファレンス (HTML4.01) に準拠していることが前提となっています。HTML 構文がリファレンスに準拠している場合は、特に制限事項はありません。

7.1.1 大文字小文字の扱い

タグを記述する場合に大文字小文字の区別はありません。また、1 つのタグ名に大文字小文字が混在していても構いません。

例. 大文字小文字の扱い

すべて大文字にて記述

```
<A HREF="http://www.hp.com/">Hewlett-Packard</A>
```

すべて小文字にて記述

```
<a href="http://www.hp.com/">Hewlett-Packard</a>
```

大文字小文字混在で記述

```
<A HrEf="http://www.hp.com/">Hewlett-Packard</a>
```

7.1.2 属性値の扱い

タグ内の属性名と値を繋ぐ「=」は、その前後のスペース / タブの有無に関係なく動作します。また、属性値に対するダブルクォート (またはシングルクォート) は、次の例のように、必須ではありません。

例. アンカータグの場合

属性名と値を繋ぐ「=」の前後にスペース / タブなし

```
<a href="http://www.hp.com/">Hewlett-Packard</a>
```

属性名と値を繋ぐ「=」の前後またはどちらかにスペース / タブがある

```
<a href = "http://www.hp.com/">Hewlett-Packard</a>
```

```
<a href= "http://www.hp.com/">Hewlett-Packard</a>
```

```
<a href="http://www.hp.com/">Hewlett-Packard</a>
```

属性値がダブルクォートで挟まれていない

```
<a href=http://www.hp.com/>Hewlett-Packard</a>
```

7.1.3 文字コードの扱いについて

バックエンド Web サーバーのコンテンツの文字コードとして Shift_JIS、EUC および Unicode (UTF-8) がサポートされています。ただし、IceWall SSO で日本語など ASCII 文字以外の文字コードを利用したコンテンツを利用する場合については、以下の点に注意する必要があります。

- (1) タグ文字については ASCII 文字であること。
- (2) 2 バイト文字については、キーワード変換や URL 変換対象外のものであれば、そのまま IceWall SSO を通過することができます。
- (3) サポートされていないマルチバイト文字についても、キーワード変換での利用は可能です。ただしこの場合、設定ファイルへ対象となる文字コードで記述する必要があります。
- (4) 途中にヌル文字が入るような文字列は使用できません。例えば Unicode のように、半角文字を使用するとヌル文字が自動的に挿入される文字コードの場合は、半角文字が使用できません。

7.2 認識不可能なタグの記述

一般的なブラウザで認識できるタグでも、IceWall SSO では認識できないものがあります。

7.2.1 タグ名にスペース / タブ / 改行が含まれている場合

通常、HTML に記述されたスペース / タブ / 改行は無視されますが (<PRE> タグなどは除く)、IceWall SSO は『「<」 + タグ名』を 1 つの文字列として検索し認識するため、スペース / タブ / 改行を含むタグ名は認識できません。

1. タグ名の間にスペース / タブ / 改行がある

```
<i mg src="title.gif">
<i
mg src="title.gif">
```

2. 「<」とタグ名の間にスペース / タブ / 改行がある

```
< a href="http://www.hp.com/">Hewlett-Packard</a>
<
a href="http://www.xxx.hp.com/">Hewlett-Packard</a>
```

7.2.2 属性名にスペース / タブ / 改行が含まれている場合

IceWall SSO は、属性名自体を 1 つの文字列として検索し認識するため、スペース / タブ / 改行を含む属性名を認識できません。

例．属性名に改行、タブおよび空白文字が含まれている

```
<a href="http://www.hp.com/">Hewlett-Packard</a>
<a href="http://www.hp.com/">Hewlett-Packard</a>


```

7.2.3 タグ名と属性名の間にスペース / タブ / 改行がない場合

タグ名と属性名の間にスペース / タブ / 改行がない場合、その属性名は認識できません。

例．タグ名と属性名が連続している

```
<ahref="http://www.hp.com/">Hewlett-Packard</a>
<imgsrc="title.gif">
```

7.2.4 他の属性値と属性名の間にスペース / タブ / 改行がない場合

他の属性値と属性名の間にスペース / タブ / 改行がない場合、その属性名は認識できません

例．他の属性値と属性名が連続している

```
<body bgcolor="#000000"background="title.gif">

```

8 URL 変換

IceWall SSO の URL 変換機能について説明します。

8.1 URL 変換の対象コンテンツ

IceWall SSO は URL 変換機能にて、バックエンド Web サーバーから受信した HTML 構文のタグ内に記述されている URL を IceWall SSO 経由の URL へ変換します。また、同様に HTTP の Location ヘッダー（詳細は「6.2.1 注意が必要なヘッダー」を参照）、Set-Cookie ヘッダー（詳細は「13.4 Cookie に path 属性が指定されている場合」を参照）についても URL 変換を行います。

なお、変換対象となるコンテンツは、IceWall サーバーの設定ファイルにて MIME タイプを（例：text/html）を設定します。このため、Content-type ヘッダーが送信されない場合は変換対象のコンテンツにはなりません（Location ヘッダーおよび Set-Cookie ヘッダーは変換されます）。

URL の変換は文字列置換で行われるため、以下の種類のコンテンツを変換対象に指定した場合は、正しく URL 変換が行われず、またはコンテンツが損傷する場合があります。

- ・テキストとバイナリが混在するような（例：MIME マルチパート）コンテンツ
- ・HTTP 圧縮されているコンテンツ
- ・画像ファイルや PDF ファイルなどのバイナリファイル

このように URL 変換はテキスト形式の HTML コンテンツや XHTML コンテンツを対象とした機能です。以降では、HTML コンテンツに含まれる URL の変換ルールを説明します。

8.2 URL 変換の変換対象

URL 変換機能は、IceWall サーバーの設定ファイルで設定した（URLKEY 項目）タグ名と属性名に記述されている値を URL として扱い、変換を行います。URL 以外の項目を含むタグの場合、またはタグ外に URL が記述されている場合には、後述のキーワード変換機能を使用する必要があります。

注）IceWall サーバーの設定ファイルに初期設定されている URLKEY 項目は、以下のとおりです。

```
URLKEY=A,HREF
URLKEY=BASE,HREF
URLKEY=FRAME,SRC
URLKEY=FORM,ACTION
URLKEY=BASE,TARGET
URLKEY=IMG,SRC
URLKEY=SCRIPT,SRC
URLKEY=BODY,BACKGROUND
URLKEY=TD,BACKGROUND
URLKEY=TR,BACKGROUND
```

```
URLKEY=TABLE,BACKGROUND
URLKEY=APPLET,CODEBASE
URLKEY=INPUT,SRC
URLKEY=LINK,HREF
```

なお、コンテンツからタグ名を検索する際には完全一致で行われますが、タグ属性名は URLCONV_ATTR_FLG 項目の設定により比較方法が異なります。 ⑩.0

(1) URLCONV_ATTR_FLG=1 の場合

- ・タグ属性名の比較方法が完全一致となります。

(2) URLCONV_ATTR_FLG=1 の場合

- ・タグ属性名の比較方法が前方一致となります。

8.2.1 自動的に変換される URL

URL 変換機能により IceWall SSO 経由の URL へ自動的に変換されるパス (URL) は、次の 2 種類です。

- (1) 「http」から記述される絶対パス (SSL Option 購入済みの場合は「https」も含む)
IceWall サーバーにバックエンド Web サーバー名として設定されたホスト名を含む絶対パスの URL は自動的に変換されます。設定されていないバックエンド Web サーバーへの絶対パスは変換されません。

例. dfw.conf の HOST 項目が HP=www.hp.com の場合
(IceWall SSO フォワーダーパス : /fw/dfw)

バックエンド Web サーバーのコンテンツに

```
<a href="http://www.hp.com/">Hewlett-Packard へのリンク </a>
```

と記述されている場合、URL 変換機能により自動的に以下の URL に変換されます。

```
<a href="/fw/dfw/HP/">Hewlett-Packard へのリンク </a>
```

以下のような記述の場合は、HOST 項目が設定されていないため変換されません。

```
<a href="http://www.xyz.co.jp/">XYZ Corp へのリンク </a>
```

この場合、HOST 項目に XYZCorp=www. xyz. co. jp のように設定を追加することで、自動的に URL 変換が行われるようになります。

(2) 「/」から記述されるドキュメントルートからの絶対パス

ドキュメントルートからの絶対パス指定で記述されている URL は、その URL が記述されているコンテンツを持つバックエンド Web サーバーに対する URL へ自動的に変換されます。

例. dfw.conf の HOST 項目が HP=www.hp.com の場合
(IceWall SSO フォワーダーパス : /fw/dfw)

IceWall SSO 経由で www.hp.com へアクセスし、取得したコンテンツに

 お知らせ
と記述されている場合、URL 変換機能により自動的に以下の URL に変換されます。
 お知らせ

8.2.2 変換する必要のない URL

URL の記述方法によっては、URL 変換機能による変換が不要となるものもあります。変換不要となるパス (URL) は、次の 2 種類です。

(1) カレントディレクトリからの相対パス (../ など)

カレントディレクトリからの相対パスで記述された URL は、ブラウザでそのリンクが選択されると、ブラウザが現在参照しているコンテンツの位置を元に、ブラウザ側で URL を作成してアクセスします。よって、IceWall SSO 経由でコンテンツを表示した場合には、ブラウザ側にて IceWall SSO 経由の URL を作成して目的のリンクにアクセスされます。

例. ブラウザーが参照している URL が `http://host.co.jp/fw/dfw/HP/data1/` の場合

表示されているコンテンツに以下のような URL が記述されているとします。

Data2 のお知らせ

このとき、ブラウザ側でこのリンクが選択された場合、ブラウザ側で URL を以下のように作成してアクセスを行います。

`http://host.co.jp/fw/dfw/HP/data2/info/index.html`

(2) ファイル名のみ (index.html など)

「(1) カレントディレクトリからの相対パス (../ など)」と同様にファイル名だけのリンクの場合は、それが選択されたときにブラウザ側でアクセスすべきパスを作成するため、URL 変換は不要となります。

8.2.3 変換する設定を行っても変換されない URL

URL 変換機能により変換されると、誤動作の原因となるものは変換されません。URL 変換がされない場合、実際の URL がブラウザに表示されてしまう場合がありますのでご注意ください。

変換されないパス (URL) は、次のとおりです。

(1) URL 変換済みの URL (/fw/dfw/sys/index.html など)

バックエンド Web サーバーより取得したコンテンツ内に IceWall SSO 経由の URL が記述されている場合は、URL 変換を行いません。ただし、フォワーダーのパスが実際に動作しているものと異なる場合は、変換が行われるので注意が必要です。

例. dfw.conf の HOST 項目が `HP=www.hp.com` の場合

(IceWall SSO: host.co.jp、フォワーダーパス : /fw/dfw)

バックエンド Web サーバーのコンテンツに

`<a href="/fw/dfw/HP/data1/info/">Data1 のお知らせ </a>`

と記述されている場合は、既に IceWall SSO 経由の URL であると判断されるため、URL 変換は不要となります。

ただし、フォワーダーのパス部分が

`<a href="/fz/dfw/HP/data1/info/">Data1 のお知らせ </a>`

のように実際に動作している内容と異なる場合は、

`<a href="/fw/dfw/HP/fz/dfw/HP/data1/info/">Data1 のお知らせ </a>`

のように、意図していない URL に変換されます。

なお、IceWall SSO 経由の URL を絶対パス指定で以下のように記述した場合は、URL のホスト名が dfw.conf の HOST 項目に定義されていないため、変換は行われません。

`<a href="http://www.xyz.co.jp/fw/dfw/HP/data1/info/">Data1 のお知らせ </a>`

(2) Query String 内の URL

Query String 内にバックエンド Web サーバーの URL が存在した場合でも URL 変換は行われません。

変換が必要な場合はキーワード変換を行う必要があります。

8.2.4 変換不可能な URL

URL の記述方法によっては、URL 変換による自動変換が有効にならない場合があります。この場合は、後述するキーワード変換機能を使用してください。

- ・ JavaScript のイベントハンドラー指定 (OnClick="location.replace('/index.html')"
など)

URL 変換機能は、「http://」で始まる絶対パスや「/」から始まるドキュメントルートからの相対パスを自動変換します。これら以外の文字で始まるパス (URL) はすべてカレントディレクトリからの相対パスまたはファイル名指定のパスと認識されるためです。

- ・ 設定と実際の記述との不一致
フォワーダー設定ファイル (dfw.conf) の HOST 項目が IP アドレスで記述され、コンテンツ内の URL はホスト名で記述されているような場合は、フォワーダーが名前解決できないため URL 変換は行われません。

8.2.5 抽出対象となる URL

IceWall SSO では URLCONV_FLG 項目、ATTRQUOT_FLG 項目の設定により、以下のように記述された URL を変換対象として抽出します。

(1) URLCONV_FLG=0 の場合

- ・ ダブルクォートで囲まれた URL
(例 : `<a href="www.svr.com/">`)
- ・ 前後どちらか一方にのみダブルクォートが記述された URL
(例 : `<a href="www.svr.com/> <a href=www.svr.com/">`)
- ・ シングルクォートで囲まれた URL
(例 : `<a href='www.svr.com/'>`)

- ・ 前後どちらか一方にのみシングルクォートが記述された URL
(例 : `<a href='www.svr.com/'> <a href=www.svr.com/'>`)
- ・ ダブルクォートとシングルクォートの組み合わせで囲まれた URL
(例 : `<a href="www.svr.com/'> <a href='www.svr.com/'>`)
- ・ ダブルクォート、シングルクォートが記述されていない URL
(例 : `<a href=www.svr.com/'>`)

(2) URLCONV_FLG=1、ATTRQUOT_FLG=0 の場合

- ・ ダブルクォートで囲まれた URL
(例 : `<a href="www.svr.com/'>`)
- ・ シングルクォートで囲まれた URL
(例 : `<a href='www.svr.com/'>`)
- ・ ダブルクォートとシングルクォートの組み合わせで囲まれた URL
(例 : `<a href="www.svr.com/'> <a href='www.svr.com/'>`)
- ・ ダブルクォート、シングルクォートが記述されていない URL
(例 : `<a href=www.svr.com/'>`)
- ・ 属性値内に括弧 (「<」や「>」) が記述された URL
(例 : `<a href="/index.cgi?name=aaaaa>bbbbbb"'>`)

(3) URLCONV_FLG=1、ATTRQUOT_FLG=1 の場合

- ・ ダブルクォートで囲まれた URL
(例 : `<a href="www.svr.com/'>`)
- ・ シングルクォートで囲まれた URL
(例 : `<a href='www.svr.com/'>`)
- ・ ダブルクォート、シングルクォートが記述されていない URL
(例 : `<a href=www.svr.com/'>`)
- ・ 属性値内に括弧 (「<」や「>」) が記述された URL
(例 : `<a href="/index.cgi?name=aaaaa>bbbbbb"'>`)

8.2.6 1つのタグ内で属性名の異なる複数の属性の URL 変換 **10.0**

URLCONV_ATTR_FLG 項目に 1 を設定することにより、1 つのタグ内で属性名の異なる複数の属性の URL を変換することが可能です。

例. 1つのタグの属性名の異なる複数の属性を変換する場合
(フォワードパス : /fw/dfw)

以下の設定を行います。

フォワード設定ファイル

HOST=HP=www.hp.com

ホスト設定ファイル

URLCONV_ATTR_FLG=1

URLKEY=INPUT,VALUE1

URLKEY=INPUT,VALUE2

バックエンド Web サーバーのコンテンツに

```
<input value1="http://www.hp.com/index.html" value2="http://www.hp.com/index.html">
と記述されている場合、属性 value1 と属性 value2 が以下の URL に変換されます。
<input value1="/fw/dfw/HP/index.html" value2="/fw/dfw/HP/index.html">
```

8.3 URL 記述制限

IceWall SSO にて変換される URL の記述に対して、次の制限事項があります。

- (1) 同一のホスト名に対しての記述を統一する。
- (2) ドキュメントルート（さかのぼるパス）を記述しない。
- (3) 最大 URL 文字数（Query String を含む）は 512 バイトまでとする。
- (4) ホスト名のみの URL は、必ず "/" で終結する。
- (5) コンテンツ内で HTML 構文を % 表記している場合には、URL 変換の対象にならない。
 （例） を <a%20href=…。> と表記した場合など

8.3.1 ホスト名記述の統一

IceWall SSO の仕様として、ホスト名の URL 変換は文字列のパターンマッチングを用います。フルドメイン名とホスト名のみの、または大文字および小文字のホスト名が混在する場合には、別のホスト名として認識されます。設定ファイルには各々のホスト名を設定する必要があります。

1. 大文字・小文字が混在しているホスト名を 1 つのエイリアス名へ変換する場合

設定ファイルの定義が

```
HOST=HP=www.hp.com
```

（ホスト名：www.hp.com エイリアス名：HP）

の場合は、

- (1) http://www.hp.com/ → エイリアス化可能
- (2) http://WWW.HP.COM/ → エイリアス化不可能

となります。(2) を (1) と同じエイリアス名にエイリアス化するには、次のように 2 行設定する必要があります。

```
HOST=HP=www.hp.com
```

```
HOST=HP=WWW.HP.COM
```

（ホスト名：www.hp.com エイリアス名：HP

ホスト名：WWW.HP.COM エイリアス名：HP）

2. ホスト名のみのフルドメイン名を 1 つのエイリアス名へ変換する場合

設定ファイルの定義が

```
HOST=HP=www.HP.com
```

（ホスト名：www.hp.com エイリアス名：HP）

の場合は、

となります。(2) を (1) と同じエイリアス名にエイリアス化するには、次のように 2 行設定する必要があります。

```
HOST=HP=www.HP.com
```

```
HOST=HP=www
```

(ホスト名: www.hp.com エイリアス名: XXXCorp
ホスト名: www エイリアス名: XXXCorp)

ホスト名による記述と IP アドレスによる記述が混在している場合も、同様にホスト情報を追加定義する必要があります。

8.3.2 ドキュメントルートをさかのぼるパス

カレントディレクトリからの相対パスが IceWall SSO を経由してブラウザへ出力された場合、アクセスされた URL を元にブラウザ側にて自動的に IceWall SSO 経由の URL を作成します。ただし、ドキュメントルートをさかのぼるパスの場合、ホストのエイリアス名や IceWall SSO 自体へのパスは正しく作成されません。

例. URL にドキュメントルートをさかのぼるパスが指定された場合

(フォワーダーパス: /fw/dfw エイリアス名: HP)

image ファイル (.././../image/title.gif) が「/data/info1/index.html」で指定されている場合、IceWall サーバー経由で次のようなアクセスが期待されます。

/fw/dfw/HP/data/info1/././../image/title.gif

しかし、ブラウザ側では相対パスを認識し次のパスをアクセスします。

/fw/dfw/image/title.gif

結果として title.gif は表示されません。

新規に作成するコンテンツの場合、ドキュメントルートをさかのぼるパスの指定は避けて URL を記述してください。既存のコンテンツで修正することができない場合は、後述のキーワード変換機能を使用してパスを変換してください。

8.3.3 "http" もしくは "/" で始まらない URL

属性名の直後に "http"(および https) もしくは "/" で始まる URL が指定されない場合で、かつ URL 変換が必要な場合は、後述するキーワード変換設定を行う必要があります。

例. "http" もしくは "/" で始まらない URL が指定されている場合

(フォワーダーパス: /fw/dfw エイリアス名: HP)

次の場合、

<meta http-equiv="Refresh" content="10;url=http://www.hp.com">

"10;URL=http://www.hp.com" は、URL とは認識されませんが、以下の設定を行うことで例外的に変換されます。

URLKEY=META,CONTENT

<meta> タグ以外で上記のような記述を行う URL についてはキーワード変換が必要となります。

8.3.4 コメント内に記述された URL

タグがコメントタグ内に記述されている場合でも、そのタグが変換対象ならば、IceWall SSO は URL 変換を行います。

例．コメントタグ内に記述されている URL の場合
(フォワーダーパス：/fw/dfw エイリアス名：HP)

URL が次のように記述されている場合、

```
<!--<a href="http://www.hp.com/">-->
```

コメントの有無に関係なく変換が行われます。

```
<!-- <a href="/fw/dfw/HP/">-->
```

このように変換されますが、ブラウザ側ではコメントとして扱われます。

8.3.5 BASE タグ使用時の URL 変換

コンテンツ内に <base> タグが記述されている場合、このコンテンツのすべての URL は <base> タグで指定されているバックエンド Web サーバー上のコンテンツとみなして IceWall SSO は変換を行います。ただし、ホスト名を含む絶対パスで記述されている URL は影響を受けません。

例．<BASE> タグが記述されているコンテンツの URL 変換

(フォワーダーパス：/fw/dfw エイリアス名：HP IceWall サーバー名：icewall.hp.com)

バックエンド Web サーバー [www.hp.com] 上に存在するコンテンツの URL は、通常次のように変換されます。

```
<a href="http://www.hp.com/index.html">
```

変換後 →

```
<a href="/index.html">
```

変換後 →

このコンテンツに <base href="http://www.xyz.co.jp/"> (エイリアス名を XYZCorp とします) の記述を追加すると、すべての URL が次のように変換されます。

```
<base href="http://www.xyz.co.jp/">
```

変換後 → <base href="http://icewall.hp.com/fw/dfw/XYZCorp/">

```
<a href="http://www.hp.com/index.html">
```

変換後 → (影響されません)

```
<a href="/index.html">
```

変換後 → (影響されます)

また「8.3.4 コメント内に記述された URL」に記述したように、<BASE> タグがコメントタグ内に記述されている場合も、上記と同様の変換が行われます。

8.3.6 URL と引数 (Query String) のセパレーターについて

URL と Query String を区別するためのセパレーターは、「?」を使用するようにしてください。

また、Servlet のセッション ID のように、「;」をセパレーターとしてサポートする Web アプリケーションサーバーがバックエンド Web サーバーとして存在する場合、IceWall

SSO は「;」をセパレーターとして認識しないため、URL エンコードを行って送信します。URL エンコードされた「;」がセパレーターとして認識できない Web アプリケーションサーバーの場合は、IceWall サーバーにて「;」を変換しない設定を有効 (URL_SCOLON=1) にしてください。

8.3.7 バックエンド Web サーバー上のコンテンツの絶対 URL を記述する際の制限

フォワーダーは URL 変換機能でコンテンツに含まれる絶対 URL の変換を行うが、IPv6 で絶対 URL を記述する場合には以下の制限があります。

- ・ホストを IPv6 形式の IP アドレスで記述する場合は角括弧「[~]」が必要です。

```
http://[2001:0db8:0:0:0:0:0:1]/index.html  
http://[2001:0db8:0:0:0:0:0:1]:81/index.html
```

以下は、IPv6 形式の IP アドレスですが角括弧「[~]」がないので、正常に比較ができないため URL 変換は行われません。

```
http://2001:0db8:0:0:0:0:0:1/index.html  
http://2001:0db8:0:0:0:0:0:1:81/index.html
```

- ・ホストを IPv6 のホスト名で記述する場合は角括弧「[~]」は不要です。

IPv6 をホスト名で記述する場合は IPv4 と同じく角括弧「[~]」を付けません。角括弧「[~]」が付く場合は正常に比較ができないため URL 変換は行われません。

```
http://www.iwdfw.com/index.html  
http://www.iwdfw.com:81/index.html
```

8.4 Java アプレット

8.4.1 ダウンロード

IceWall SSO を経由して Java アプレットをダウンロードしても、問題なく動作しますが、Java アプレット内で保持している URL は変更されません。保持している URL が絶対パスの場合は変換が必要となるため、その場合は Java アプレット内の URL を IceWall SSO を経由したものに修正する必要があります。

8.4.2 アプレットからの IceWall SSO 経由の通信

getDocumentBase() と「相対パス」を組み合わせると、IceWall SSO 経由で他のドキュメントにアクセスできます。

例 .

- ① URL url = new URL(getDocumentBase(), "sample.htm");
- ② URL url = new URL(getDocumentBase(), "../test/sample.htm");

8.5 ActiveX

8.5.1 ダウンロード

IceWall SSOを経由してActiveXをダウンロードしても、問題なく動作しますが、ActiveX 内で保持している URL は変更されません。保持している URL が絶対パスの場合は変換が必要となるため、その場合は ActiveX 内の URL を IceWall SSO を経由したものに修正する必要があります。

8.6 その他のファイル

8.6.1 ダウンロード

Java アプレット・ActiveX 以外のファイルを IceWall 経由でダウンロードを行った場合でも問題なく動作しますが、次の点に注意してください。

- Flash などのリッチコンテンツの場合も Java アプレットや ActiveX と同様に絶対パスの URL が埋め込まれている場合は、IceWall SSO を経由したものに変更する必要があります。
- ダウンロードを行うファイルが設置されているバックエンド Web サーバー側で対象ファイルの MIME 設定を行っておく必要があります。(一般的に MIME 設定が行われていないファイルの MIME は text/plain となるため)

9 キーワード変換

IceWall SSO のキーワード変換機能について説明します。

9.1 キーワード変換機能の注意事項

キーワード変換機能を使用する場合には、いくつかの注意点があります。

9.1.1 変換対象

キーワード変換の対象はバックエンド Web サーバーからのレスポンスのみです。バックエンド Web サーバーへ送信するリクエストには使用することはできません。

変換対象となるコンテンツは、URL 変換同様に IceWall サーバーの設定ファイルに指定した MIME タイプのコンテンツのみです。Content-type ヘッダーが送信されない場合や、zip などで圧縮されたコンテンツ、PDF ファイル、画像ファイルなどのバイナリファイルや MIME マルチパートのコンテンツは対象となりません。

また、キーワード変換機能は、変換対象のレスポンス全体（HTTP ヘッダーとコンテンツの両方）に使用することができ、すべてのバックエンド Web サーバーに対する変換設定か、バックエンド Web サーバー別の変換設定かを指定できます。

9.1.2 大文字小文字の区別

キーワード変換機能は検索文字列の大文字と小文字を区別します。したがって、キーワードの定義を行う場合は、元の文字列を確認し、大文字小文字が一致するように検索文字列を設定する必要があります。

9.1.3 ユニークな検索文字列の使用

コンテンツまたは HTTP ヘッダー内の検索文字列を定義する場合、該当する箇所に対してのみ変換が行われるように、検索文字列をバックエンド Web サーバー単位にユニークなものとする必要があります。検索文字列の最小部分のみが定義された場合、変換機能は検索文字列の予期しない箇所にも適用される可能性があります。

例． 検索文字列の定義

（フォワーダーパス：/fw/dfw エイリアス名：HP）

コンテンツが次のような場合で、

```
<html>
<head>
<title>This is http://www.hp.com</title>
</head>
<body>
<meta http-equiv="Refresh" content="10;url=http://www.hp.com/index2.html">
</body>
```

```
</html>
さらにキーワード変換用の定義が次の場合、
REPKEY=http://www.hp.com,/fw/dfw/HP/
(検索文字列：http://www.hp.com
置換文字列：/fw/dfw/HP/)
<meta> タグ内の文字列のみならず、<title> タグ内の文字列も変換されます。
これを回避するために、ユニークな検索文字列として、キーワード前後の文字を含めて
次のように定義します。
REPKEY=10:url=http://www.hp.com, 10:url=/fw/dfw/HP/
(検索文字列：10;URL=http://www.hp.com
置換文字列：10;URL=/fw/dfw/HP/)
```

9.1.4 検索文字列の予約語化

キーワード変換用に定義された検索文字列は、バックエンド Web サーバーごとの予約語となります。このため、新規にコンテンツを作成する場合には、その文字列を記述しないように注意するか、検索文字列を再定義する必要があります。

9.1.5 コンテンツの文字コードについて

バックエンド Web サーバーのコンテンツの文字コードとして Shift_JIS、EUC および Unicode (UTF-8) がサポートされています。ただし、キーワード変換にて日本語などの 2 バイト文字の変換を行う場合は、コンテンツの文字コードで設定する必要があります。

9.1.6 変換できない文字列 **10.0**

キーワード変換では、カンマ「,」は REPKEY 項目のセパレーターとして予約されているため設定することができません。また制御コード「¥r」「¥n」「¥t」も設定することができません。これらの文字をキーワードとして設定したい場合は REPKEY_EXT 項目でそれぞれ文字列「¥,」「¥r」「¥n」「¥t」と設定してください。

9.2 特定キーワード変換機能

キーワード変換は、設定ファイルで任意に変換を定義できる通常のキーワード変換と特定キーワード変換と呼ばれる変換の 2 種類が存在しています。

9.2.1 特定キーワードとは

IceWall SSO にてあらかじめ予約されているキーワードで、実行時に IceWall SSO の動作環境やログインしているユーザーの情報に置換するキーワードです。

9.2.2 変換順序

IceWall SSO に搭載されている各変換機能の変換順序は以下のとおりです。

- (1) HTTP ヘッダー内 URL 変換
- (2) キーワード変換機能 (ホスト設定ファイルの REPKEY 項目)
- (3) 拡張キーワード変換機能 (ホスト設定ファイルの REPKEY_EXT 項目)
- (4) URL 変換機能 (ホスト設定ファイルの URLKEY 項目)
- (5) 特定キーワード変換機能

9.2.3 特定キーワード一覧 (10.0)

定義可能な特定キーワードは以下のとおりです。

キーワード	変換内容
\$USER_ID	ログインしているユーザーのユーザー ID に置換されます。 Client Certificates Option 使用時にはログイン前でもアクセスしたユーザーのユーザー ID に置換することが可能です。
\$PASSWORD	ログインを行ったユーザーのパスワードに置換されます。 認証 DB に格納される暗号化されたパスワードではなく、ログイン時に入力された値となります。
\$DFW	フォワーダーのパスに置換されます。 (例) /fw/dfw ただし、URL-Cookie 方式の場合は次のように置換されます。 パスワード変更時： (例) /fw/dfw/xxx ~ xxx/ パスワード変更用エイリアス ログアウト時： (例) /fw/dfw/xxx ~ xxx/ ログアウト用エイリアス
\$REQUEST_URL	ブラウザよりリクエストされたパスに置換されます。 (例：Cookie 方式) /fw/dfw/ALIAS/index.html (例：URL-Cookie 方式) /fw/dfw/xxx ~ xxx/ALIAS/index.html ただし、URL の後ろに追加される引数 (Query String) は含まれません。
\$HIDEURL	ブラウザよりリクエストされたパスよりフォワーダーのパス部分を除いたパスに置換されます。 (例：Cookie 方式) /ALIAS/index.html (例：URL-Cookie 方式) /xxx ~ xxx/ALIAS/index.html このキーワードには、URL の後ろに追加される引数 (Query String) が含まれます。
\$ALIAS	コンテンツを取得したバックエンド Web サーバーに対するエイリアス名に置換されます。
\$IW_INFO	ログインユーザーのセッション ID に置換されます。 認証 Cookie に含まれる認証情報部分のみとなります。
\$KEY_LOGIN	ログイン処理を判断するためのキーとなる文字列に置換されます。
\$KEY_LOGOUT	ログアウト処理を判断するためのキーとなる文字列に置換されます。

キーワード	変換内容
\$KEY_PWDCHG	パスワード変更処理を判断するためのキーとなる文字列に置換されます。
\$PWDCHG_URL	パスワード変更画面を表示するための URL に置換されます。
\$LOGOUT_URL	ログアウト画面を表示するための URL に置換されます。
\$TOPPAGE_URL 10.0	トップページを表示するための URL に置換されます。
\$PWDHIDEURL 10.0	Agent 連携パスワード変更時に Agent への戻る URL 情報を引き継ぐための URL に置換されます。
\$IWTID 10.0	アクセスを行ったユーザーのトランザクション ID に置換されます。 TRANSID 項目が ON の場合にのみ、変換されるキーワードとなります。

9.2.4 特定キーワードの使用例

URL-Cookie 方式 (SESSION=1) におけるキーワード変換機能で IceWall 経由の URL に変換する場合の例です。

例．URL-Cookie 方式におけるキーワード変換設定

JavaScript 内で以下の記述があった場合はキーワード変換が必要です。

```
location.url = 'http://www.hp.com/info/index.html';
```

通常の Cookie 方式 (dfw.conf の SESSION=0) では、以下のような設定となります。
(フォワーダーのパスが /fw/dfw、www.hp.com のエイリアス名が HP の場合)

```
REPKEY='http://www.hp.com, /fw/dfw/HP'
```

URL-Cookie 方式の場合は URL 内にセッション ID が含まれています。セッション ID はログインごとに値が異なり、固定の値を指定することができないため、特定キーワードを使用します。

```
REPKEY='http://www.hp.com, /fw/dfw/$IW_INFO/HP'
```

このように設定を行うと、\$IW_INFO 部分が実行時にログインしているユーザーのセッション ID に置換されます。

IceWall SSO の動作環境に依存しない (例えば開発環境と本番環境で CGI Prefix が異なっているなど) IceWall 経由の URL への変換を行う例です。

例．動作環境に依存しないキーワード変換設定

JavaScript 内で以下の記述があった場合はキーワード変換が必要です。

```
var url = '/mail/list.html';
```

通常、キーワード設定を行う場合は動作している環境によりフォワーダーのパス名やエイリアス名を以下のように直接指定します。（フォワーダーのパスが /fw/dfw、エイリアス名が HP の場合）

```
REPKEY=var url = '/',var url = '/fw/dfw/HP/
```

この設定ではフォワーダーのパス名やエイリアス名が変更された場合、このキーワードの設定も変更する必要があります。この部分を特定キーワードの「\$DFW」「\$ALIAS」を使用することで汎用的なキーワード設定が可能となります。

```
REPKEY=var url = '/',var url = '$DFW/$ALIAS/
```

このように設定を行うと \$DFW および \$ALIAS が動作している環境の値に置換されます。
なお、この特定キーワードを URL-Cookie 方式で使用する場合、以下のような設定となります。

```
REPKEY=var url = '/',var url = '$DFW/$IW_INFO/$ALIAS/
```

9.2.5 制限事項

特定キーワードとして予約されている文字列をキーワード変換機能で他の値に変換する設定を行った場合は、特定キーワードとして機能しなくなります。

以下の設定を行った場合は特定キーワードとして機能しなくなります。

例） REPKEY=\$USER_ID,XXX

Version 8.0 より、特定キーワードの悪用を防ぐ機能がクロスサイトスクリプティング機能の 1 つとして搭載されています。その機能を使用した場合、キーワードは値に変換されずにそのままコンテンツに残ることに注意してください。

例．

バックエンド Web サーバーのコンテンツですべての特定キーワード変換を許可しない場合
CTRL_SPKEY=

バックエンド Web サーバーのコンテンツで \$USER_ID と \$ALIAS の変換のみを許可する場合
CTRL_SPKEY=\$USER_ID,\$ALIAS

10 JavaScript

IceWall SSO で JavaScript を使用する場合は、以下の点に注意してください。

10.1 クライアントサイド JavaScript

クライアントサイド JavaScript を使用する場合は、記述する構文は、標準リファレンスに準じているものであれば特に制限はありません。ただし、スクリプト内で URL を制御する必要がある場合は、URL 変換機能またはキーワード変換機能を使用して、IceWall SSO 経由の URL へ変換する必要があります。

変換される URL には、スクリプト内の記述方法により、2 種類が存在します。

- (1) スクリプトにより出力されるタグ内の URL
- (2) 関数の引数として使用される URL

10.1.1 スクリプトにより出力されるタグ内の URL

スクリプトから動的にコンテンツを出力する場合、出力される内容がタグ形式のものであれば、URL 変換機能の変換対象として扱われます。

ただし、出力されるタグの属性値がエスケープ文字 (\) から始まる場合、その属性値はカレントディレクトリからの相対パスと判断され、変換の対象とはなりませんので注意が必要です。

例． スクリプトにより出力されるタグの場合

(フォワーダーパス : /fw/dfw エイリアス名 : HP)

ドキュメント内のスクリプトに次のように記述されている場合、

```
document.write('<a href="http://www.hp.com/">Hewlett-Packard</a>');
```

出力されるタグ部分が URL 変換の対象となり、スクリプトがクライアントで実行される前に次のように変換されます。

```
document.write('<a href="/fw/dfw/HP/">Hewlett-Packard</a>');
```

タグの属性値がエスケープ文字を使用して次のように記述されている場合、

```
document.write('<a href="\http://www.hp.com/">Hewlett-Packard<a>');
```

カレントディレクトリからの相対パスとして判断されるため、変換されません。

10.1.2 関数の引数として使用される URL

関数の引数として URL が使用される場合、URL 変換機能の変換対象とはなりませんので、キーワード変換機能を使用する必要があります。

例． 関数の引数として URL が指定されている場合

(フォワーダーパス : /fw/dfw エイリアス名 : HP)

タグ (例 : アンカー) に次のように記述されている場合、

```
<a href="JavaScript:Func01('/index.html')">Hewlett-Packard</a>
```

キーワード変換の項目として次を追加設定する必要があります。
 REPKEY=Func01('/index.html'),Func01('/fw/dfw/HP/index.html')
 (検索文字列 : Func01('/index.html')
 置換文字列 : Func01('/fw/dfw/HP/index.html'))

また、OnClick() などでコールされる関数を独自に作成し、その関数内で引数をハードコードした場合も、上記と同様にキーワード変換機能を使用する必要があります。

以下が記述されている場合、
 <script language=JavaScript>
 function Func010 {
 location.replace('/index.html');

</SCRIPT>

キーワード変換の項目として以下を追加設定する必要があります。
 (検索文字列 : location.replace('/index.html')
 置換文字列 : location.replace('/fw/dfw/HP/index.html'))

10.1.3 クロスサイトスクリプティング対策フィルター使用時の注意

バックエンドWebサーバーからのコンテンツに対するクロスサイトスクリプティング対策フィルターを使用する場合、スクリプト内の不等号の記述によってはタグの開始・終了と誤認識される場合があります。このような場合は、コメント文にてスクリプト内で使用している不等号と対になる不等号を追加して「<」と「>」の数を一致させるようにしてください。

例．不等号の数が一致しない場合

次のようなスクリプトの場合、

```
<script language=JavaScript>
.
  for( i = 0; i < 10; i++ ){
    .
  }
</script>
```

「<」と「>」の数が一致しないため、for() ステートメント以降のタグで正しく認識できない場合があります。このような場合には次のようにコメントを追加するようにしてください。

```
<script language=JavaScript>
.
  for( i = 0; i < 10; i++ ){
    .
  }
<!-- -->
</script>
```

10.2 サーバーサイド JavaScript

サーバーサイド JavaScript を使用する場合、スクリプトの構文自体は IceWall SSO に影響されません。スクリプトが出力するコンテンツの HTML 構文、およびクライアント

サイド JavaScript 構文がリファレンスに準じているならば、確認する項目は既出の各章にて記載した項目のみになります。

10.2.1 サーバーオブジェクト

通常、サーバーオブジェクトのホスト名プロパティには、サーバーサイド JavaScript が動作する Web サーバー名が格納されます。しかし、コンテンツが IceWall SSO を経由した場合には、バックエンド Web サーバーのホスト名 (IP アドレス) とポート番号が「ホスト名 (IP アドレス) : ポート番号」の形式で格納されます。

これは IceWall SSO の仕様となりますので、このプロパティに依存するスクリプトの記述は避けてください。

11 VBScript

IceWall SSO で VBScript を使用する場合は、以下の点に注意してください。

11.1 VBScript 使用時の注意事項

11.1.1 スクリプトにより出力されるタグ内の URL

スクリプトから動的にコンテンツを出力する場合、出力される内容がタグ形式のものであれば、URL 変換の対象として扱われます。

ただし、出力されるタグの属性値がエスケープ文字 (\) から始まる場合、その属性値はカレントディレクトリからの相対パスと判断され、変換の対象とはなりませんので注意が必要です。

11.1.2 クロスサイトスクリプティング対策フィルター使用時の注意

バックエンド Web サーバーからのコンテンツに対するクロスサイトスクリプティング対策フィルターを使用する場合、スクリプト内の不等号の記述によってはタグの開始・終了と誤認識される場合があります。このような場合は、コメント文にてスクリプト内で使用している不等号と対になる不等号を追加して「<」と「>」の数を一致させるようにしてください。

例．不等号の数が一致しない場合

次のようなスクリプトの場合、

```
<script language=VBScript>  
.  
  for (i = 0; i<10; i++){  
    .  
  }  
</script>
```

「<」と「>」の数が一致しないため、for () ステートメント以降のタグで正しく認識できない場合があります。このような場合には次のようにコメントを追加するようにしてください。

```
<script language=VBScript>  
.  
  for (i = 0; i<10; i++){  
    .  
  }  
  <!-- -->  
</script>
```

11.2 アクティブサーバーページ (ASP)

11.2.1 Request オブジェクト

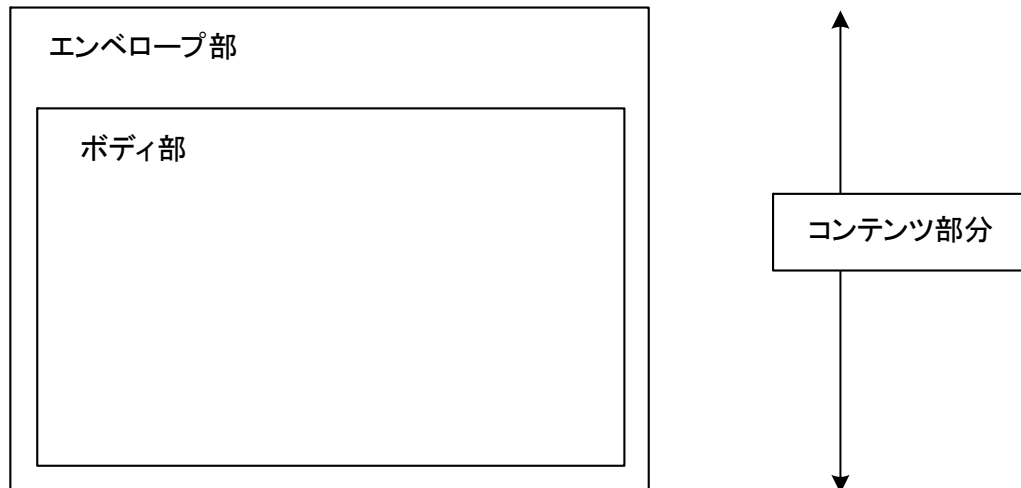
通常、Request オブジェクトの ServerVariables コレクションには、Request オブジェクトが動作するバックエンド Web サーバー名が格納されます。しかし、コンテンツが IceWall SSO を経由した場合には、バックエンド Web サーバーのホスト名 (IP アドレス

)とポート番号が「ホスト名 (IP アドレス) : ポート番号」の形式で格納されます。このコレクションに依存するスクリプトの記述は避けてください。

12 XML

IceWall SSO は、XML データを画像などのバイナリ・データとして扱います。

XML のデータ形式
Content-type: text/xml



エンベロープ部に記述されるエンコード URL は、IceWall SSO の URL 変換の対象とならないため、そのまま転送されます。また、ボディ部のデータ内容として URL を使用した場合も、URL 変換の対象とならないため、そのまま転送されます。

ただし、使用する XML ファイルがすべてテキスト形式の場合には、IceWall サーバーの設定ファイルで XML ファイルの MIME タイプを設定し、キーワード変換機能を使用することで変換を行うことができます。

13 バックエンド Web サーバーで設定された Cookie の扱い

IceWall SSO では、バックエンド Web サーバーが設定した Cookie を以下のように扱います。

13.1 Cookie に domain 属性が指定されていない場合

domain 属性が指定されない場合、ブラウザは「IceWall SSO のエイリアス名以下のパス」を Cookie の有効範囲とみなします。このため、Cookie は発行されたバックエンド Web サーバーにのみ送信されます。(他のバックエンド Web サーバーには送信されません)

13.2 Cookie に domain 属性が指定されている場合

IceWall SSO は、Cookie の domain 属性を自動で変換する機能は搭載されていません。バックエンド Web サーバーに対して Cookie を送信させるためには、キーワード変換を用いて domain 属性を IceWall SSO のドメインに変換する必要があります。

13.3 Cookie に path 属性が指定されていない場合

Cookie に path 属性が指定されていない場合、ブラウザでは Cookie がセットされた時点のパスを記憶して、それ以下のパスにアクセスする場合に限り、Cookie を送信します。

例． Cookie の path 属性が設定されていない場合の動作

(フォワーダーパス : /fw/dfw エイリアス名 : HP)

Cookie をセットしようとしているバックエンド Web サーバープログラムが以下の URL とします。

/foobar/set_cookie.cgi

このパスにアクセスして Cookie がセットされた場合、ブラウザ側では Cookie は以下のパスでセットされたものと認識されます。

/fw/dfw/HP/foobar/set_cookie.cgi

この Cookie が Web サーバーに送信されるのは、パスの先頭に「/fw/dfw/HP/foobar/」が含まれている場合のみとなります。アクセスされたパスが以下のような場合は、Web サーバーに対して発行された Cookie を送信しません。

/fw/dfw/HP/cgi-bin/ ～ (/fw/dfw/HP/以降が一致しない)

/fw/dfw/XYZCorp/ (/fw/dfw/以降が一致しない)

13.4 Cookie に path 属性が指定されている場合

Cookie に path 属性が指定されている場合、IceWall SSO は自動的に IceWall SSO 上のパスに変換します。

例えば path=/foobar がセットされている場合、IceWall SSO は下記のように変換してブラウザに送ります。

```
path=/fw/dfw/HP/foobar
```

ただし、属性値がダブルクォートで括られている場合は以下のように変換されます。

(例) path="/foobar" の場合

```
path=/fw/dfw/HP"/foobar"
```

このような場合は、キーワード変換機能を使用して対応してください。

13.5 Cookie に secure 属性が指定されている場合

IceWall SSO は、Cookie の secure 属性を自動的に変換する機能はありません。このため、ブラウザとフォワーダーの間の通信が HTTP プロトコルの場合は、キーワード変換機能を使用して secure 属性を削除する必要があります。ブラウザとフォワーダーの間の通信が HTTPS(SSL) プロトコルの場合は、キーワード変換を使用する必要はありません。

13.6 使用可能な Cookie の上限について

1 つのブラウザが保存可能な Cookie の上限数は、ブラウザの種類により異なりますが、IceWall SSO はセッション管理用に 1 つの Cookie を使用するため、アプリケーション側で使用可能な Cookie の数はブラウザの上限数 - 1 個です。上限数以上の Cookie を使用した場合は、最も古い Cookie が削除される = IceWall SSO のセッション管理用の Cookie が削除され、再度ログインが要求されます。

このため、アプリケーション側で Cookie を使用する場合は、使用する Cookie の数を極力減らすか、不要となった場合には Cookie を消去するなどの対応が必要です。

なお、IceWall サーバーには IceWall SSO のセッション管理用 Cookie を維持するための機能が搭載されています。アプリケーション側での対応が難しい場合には、この機能を使用して回避してください。ただし、この機能を使用することでアクセスごとにブラウザへ IceWall SSO のセッション管理用 Cookie が送信されることと、アプリケーション側で使用する Cookie の最も古いものが 1 つ消去されることに注意してください。

13.7 Set-Cookie ヘッダーのフォーマットに関する注意点

Set-Cookie ヘッダーのフォーマットについて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

14 エージェント導入における制限について

Web サーバーに対してエージェントを導入する場合の制限は以下のとおりです。

14.1 認証機能の排除

ベーシック認証などの認証機能が既存の Web サーバーに設定されている場合、その認証機能を排除または機能を停止するようにしてください。エージェントは既存の Web サーバーに直接導入するため、フォワーダーのようにベーシック認証やフォーム認証を制御することができないためです。

14.2 URL 変換およびキーワード変換について

エージェントは既存の Web サーバーに「Web サーバーの一部」として直接導入されるため、コンテンツ内の URL を変換する必要がありません。このため、URL 変換機能は搭載されていません。また、同様にキーワード変換機能も搭載されていません。エージェント導入後、コンテンツに対して何らかの変更を行わなければならない場合には、直接コンテンツを修正する必要があります。

14.3 アクセスログについて

エージェントはアクセスログを出力しません。アクセスログが必要な場合は、Web サーバーが出力するアクセスログを参照してください。

14.4 クライアント証明書使用時について

フォワーダーではクライアント証明書情報の取得先を任意に指定することが可能となっていますが、エージェントでは Web サーバー標準の名称で取得されることに注意してください。