



IceWall SSO

Version 10.0

導入ガイド

Linux 版

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. B2873-93001

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 各項目におけるバージョン表示記号について	1
2 動作環境	2
2.1 フォワーダー (dfw) 動作環境	2
2.2 認証モジュール (certd) 動作環境	2
2.3 その他	4
3 インストール方法	5
3.1 フォワーダーのインストール	5
3.2 認証モジュールのインストール	6
3.3 インストール作業後の設定	8
3.3.1 暗号化ライブラリに関する設定	8
3.3.2 LDAP サーバーのパスワード設定	9
3.4 推奨する設定	9
3.4.1 Web サーバーインスタンスの KeepAlive 設定	9
3.4.2 SSL 通信を使用する際の SSLSessionCache の設定	9
4 アンインストール方法	10
4.1 フォワーダーのアンインストール	10
4.2 認証モジュールのアンインストール	10
5 インストール結果の確認方法	11
5.1 各モジュールの動作を簡単に確認する	11
5.1.1 フォワーダーの確認	11
5.1.2 認証モジュールの確認	13
5.2 サンプル画面表示による確認	13
5.3 インストールファイルの確認	14
5.3.1 フォワーダーパッケージ	14
5.3.2 認証モジュールパッケージ	16
5.4 バージョン情報の確認について	18
5.4.1 フォワーダーの確認方法	18
5.4.2 認証モジュールの確認方法	19
6 従来バージョンからのバージョンアップについて	21
6.1 バージョンアップ手順	21
6.2 従来バージョン共通の注意事項	22
6.3 8.0 以前のバージョン共通の注意事項	23
6.4 従来バージョン別の注意事項	23
6.4.1 5.1i からのバージョンアップの場合	24
6.4.2 5.1iSP1、5.1iSP2 からのバージョンアップの場合	24
6.4.3 6.0、6.0SP1、6.0.1SE からのバージョンアップの場合	24
6.4.4 7.0 からのバージョンアップの場合	24
6.4.5 7.0SP1、7.0SP2、7.0SP3、7.0.1SE からのバージョンアップの場合	25
6.4.6 8.0、8.0.1(8.0R1)、8.0 R2、8.0 R3 からのバージョンアップの場合	25
7 制限事項	26
7.1 FailOver Option 使用時の注意点	26

7.2 Range 指定されたコンテンツのサイズについて	26
7.3 IE6.x を使用して SSL 環境でファイルがダウンロードできない	26
8 ドキュメント参照方法	27
9 注意事項	28
10 関連 URL、お問い合わせ先	29

1 はじめに

本書では、IceWall SSO の導入、設定についての情報が記述されています。

1.1 各項目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それぞれ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。
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 動作環境

IceWall SSO の動作環境について記述します。最新の動作環境については日本ヒューレット・パッカード株式会社のホームページ (<http://www.hp.com/jp/icewall/>) でご確認ください。

2.1 フォワーダー (dfw) 動作環境

- ・ サーバー
HP ProLiant またはそれ相当の互換機 (HP 推奨のもの)

- ・ OS
Red Hat Enterprise Linux 5.4(x86 64bit) 以降 **10.0** *1

*1 NSA Security-Enhanced Linux (SELinux) を有効にした環境での動作は保証されません。

- ・ Web サーバー
Red Hat Enterprise Linux 5.4 以降の場合
Apache HTTP Server 2.2.3 以降 (64bit) **10.0** *2*3

*2 OS ベンダー提供のパッケージのみサポートいたします。お客様ご自身でコンパイルされたものはサポートされません。

*3 MPM:prefork のみサポートいたします。

- ・ 注意点
1. UserExit ルーチンの開発は Enterprise Edition のみでサポートされます。Standard Edition の場合は、SE Forwarder upgrade License の追加購入によりサポートされます。

2.2 認証モジュール (certd) 動作環境

- ・ サーバー
HP ProLiant またはそれ相当の互換機 (HP 推奨のもの)

- ・ OS
Red Hat Enterprise Linux 5.4(x86 64bit) 以降 **10.0** *4

*4 NSA Security-Enhanced Linux (SELinux) を有効にした環境での動作は保証されません。

- ・ データベース (認証 DB)
Oracle Database 11g Release 1 Standard Edition(要 Oracle Net) **10.0**

Oracle Database 11g Release 1 Enterprise Edition(要 Oracle Net) **10.0**
 Oracle Database 11g Release 2 Standard Edition(要 Oracle Net) **10.0**
 Oracle Database 11g Release 2 Enterprise Edition(要 Oracle Net) **10.0**
 Sun Java System Directory Server 7.0 **10.0**
 Novell eDirectory Server 8.8 以降
 HP Directory Server 8.1 **10.0**
 Microsoft Active Directory (Microsoft Windows Server 2008) **10.0**
 Microsoft Active Directory (Microsoft Windows Server 2008 SP2) **10.0**
 Microsoft Active Directory (Microsoft Windows Server 2008 R2) **10.0**
 Microsoft Active Directory Lightweight Directory Services
 (Microsoft Windows Server 2008)
 Microsoft Active Directory Lightweight Directory Services
 (Microsoft Windows Server 2008 SP2)
 Microsoft Active Directory Lightweight Directory Services
 (Microsoft Windows Server 2008 R2)
 テキスト認証 DB(CSV 形式)
 MySQL Server 5.1.40 以降 **10.0**
 OpenLDAP 2.4.16 以降 **10.0**

・ 注意点

1. 認証 DB が Oracle の場合、Oracle Net Services が必要です。この場合、以下の組み合わせのみサポートされます。

データベース	クライアント
Oracle Database 11g Release 1 Standard Edition	Oracle Net R11.1.0
Oracle Database 11g Release 1 Enterprise Edition	
Oracle Database 11g Release 2 Standard Edition	Oracle Net R11.2.0
Oracle Database 11g Release 2 Enterprise Edition	

2. 認証 DB が Microsoft Active Directory の場合、以下の制限があります。
 - ・ パスワード履歴の保存機能はサポートされません。
 - ・ ユーザー認証時のパスワード有効期限チェックはできません。
3. 認証 DB が CSV の場合、以下の制限があります。
 - ・ FailOver Option は使用できません。
4. 認証 DB が MySQL の場合、MySQL AB 社製品のデータベースサーバー「MySQL」と接続用 ODBC Driver「MyODBC」が必要です。
 それぞれのサポート対象バージョンは以下のとおりです。
 - ・ MyODBC(Connector/ODBC) 5.1.6 以降
 - ・ unixODBC(ODBC Driver Manager) 2.2.14 以降
 カーネルパラメーター maxdsiz_64bit の値が十分であることを確認してください。認証モジュールは 2GByte を超えるメモリを確保しますが、maxdsiz_64bit に設定された値を超えることはで

きません。確保したいメモリの容量よりも多めにカーネルパラメーター `maxdsiz_64bit` の値を設定する必要があります。カーネルパラメーターの設定の方法は HP-UX のマニュアルを参照してください。

5. UserExit ルーチンの開発は Enterprise Edition のみサポートされます。Standard Edition の場合は SE User Certification Server upgrade License の追加購入によりサポートされます。

2.3 その他

- ブラウザー

最新の動作確認済みのブラウザーは、以下の URL を参照してください。

<http://h50146.www5.hp.com/products/software/security/icewall/ss0/spec/browser.html>

次章よりインストール方法等についての説明を行いますが、Web サーバーおよびデータベースについては以下の用語で記述します。

用語	対応プロダクト
Apache	Apache HTTP Server 2.2.3
ORACLE	Oracle Database 11g Release 1 Standard Edition Oracle Database 11g Release 1 Enterprise Edition Oracle Database 11g Release 2 Standard Edition Oracle Database 11g Release 2 Enterprise Edition
LDAP	Sun Java System Directory Server 7.0 HP Directory Server 8.1 OpenLDAP 2.4.16
NED	Novell eDirectory 8.8 Novell eDirectory 8.8.1
MSAD	Microsoft Active Directory Microsoft Active Directory Lightweight Directory Services
CSV	テキスト認証 DB ファイル
MySQL	MySQL 5.1.40

3 インストール方法

IceWall SSO のインストールは、各モジュール個別に行います。

インストールを行う場合は、そのモジュールが既にインストールされていないことを確認してから実施してください。(上書きインストールはできません。インストールされている場合には、まずアンインストールを行ってください)

確認は次の方法で行います。

(1) root ユーザーでインストールを行うサーバーへログインします。

(2) 次のコマンドを実行します。

```
# rpm -qa | grep "IceWall-SSO"
```

(3) インストールを行うモジュールが表示された場合はアンインストールを行ってください。

なお、各オプション製品のインストール方法については、それぞれの導入ガイドを参照してください。

3.1 フォワーダーのインストール

以下の手順でインストールを行います。

(1) root ユーザーでインストールを行うサーバーへログインします。

(2) CD-ROM ドライブに IceWall SSO の CD-ROM を挿入します。

次のコマンドで CD-ROM をマウントします。

```
# mount -t iso9660 /dev/cdrom /mnt/cdrom
```

※ マウントポイントが /mnt/cdrom の場合の例です。マウントポイントが存在しない場合は mkdir コマンドで作成してください。

(3) 次のコマンドでインストールを行います。

```
# rpm -ivh --nodeps /mnt/cdrom/SSO/linux/IceWall-SSO-dfw-10.0.0-1.x86_64.rpm
```

(4) 次のコマンドでインストールされたことを確認します。

```
# rpm -qa | grep "IceWall-SSO-dfw"
```

- (5) 次のコマンドでフォワーダーに関するディレクトリやファイルのオーナーを Apache の実行ユーザーに変更します。この例では、Apache の実行ユーザーを apache:apache としています。

```
# chown -R apache:apache /opt/icewall-ssso/dfw
```

- (6) Apache にフォワーダーの設定を行います。フォワーダーはライブラリ検索用環境変数、CGI 用 PATH、ドキュメント用 PATH の設定が必要です。以下の変更例を参考にしてください。（これらは、サンプルを表示するための設定例です）

- ① Apache の設定ファイル（httpd.conf） ファイルを修正します。

<httpd.conf 変更例>

```
Alias /img/ "/opt/icewall-ssso/dfw/html/image/"

SetEnv LD_LIBRARY_PATH "/opt/icewall-ssso/lib/dfw:/usr/lib64"

ScriptAlias /fw/ "/opt/icewall-ssso/dfw/cgi-bin/"

<Directory "/opt/icewall-ssso/dfw/cgi-bin">
    AllowOverride All
    Options ExecCGI
    SetHandler cgi-script
    Order allow,deny
    Allow from all
</Directory>
```

- ② Apache を再起動します。

なお、Apache は標準でディレクトリ内のファイル一覧が表示される設定となっていますので、一覧が表示されない設定に変更してください。

3.2 認証モジュールのインストール

以下の手順でインストールを行います。

- (1) root ユーザーでインストールを行うサーバーへログインします。
- (2) CD-ROM ドライブに IceWall SSO の CD-ROM を挿入します。

次のコマンドで CD-ROM をマウントします。

```
# mount -t iso9660 /dev/cdrom /mnt/cdrom
```

※ マウントポイントが /mnt/cdrom の場合の例です。マウントポイントが存在しない場合は mkdir コマンドで作成してください。

- (3) 使用する認証 DB のインストールパッケージ名を選択して、次のコマンドでインス

ツールを行います。

```
# rpm -ivh --nodeps /mnt/cdrom/SSO/linux/[インストールパッケージ名]
```

IceWall SSO のバージョンによりインストールパッケージ名が異なることに注意してください。

認証 DB	インストールパッケージ名
Oracle11g 版	IceWall-SSO-certdd_oracle1110-10.0.0-1.x86_64.rpm
MySQL 版	IceWall-SSO-certdd_odbc-10.0.0-1.x86_64.rpm
LDAP 版	IceWall-SSO-certdd_ldap-10.0.0-1.x86_64.rpm
OpenLDAP 版	IceWall-SSO-certdd_openldap-10.0.0-1.x86_64.rpm
NED 版	IceWall-SSO-certdd_ned-10.0.0-1.x86_64.rpm
MSAD 版	IceWall-SSO-certdd_msad-10.0.0-1.x86_64.rpm
CSV 版	IceWall-SSO-certdd_csv-10.0.0-1.x86_64.rpm

(4) 次のコマンドでインストールされたことを確認します。

```
# rpm -qa | grep [ターゲット名]
```

インストールパッケージ	ターゲット名
Oracle11g 版	IceWall-SSO-certdd_oracle1110 10.0
LDAP 版	IceWall-SSO-certdd_ldap
NED 版	IceWall-SSO-certdd_ned
MSAD 版	IceWall-SSO-certdd_msad
CSV 版	IceWall-SSO-certdd_csv
OpenLDAP 版	IceWall-SSO-certdd_openldap
MySQL 版	IceWall-SSO-certdd_odbc

(5) 次のコマンドで認証モジュール実行用ユーザーを作成します。

```
# useradd -g users iwadmin
```

(6) 認証モジュールコマンドの設定内容を変更します。

認証 DB に ORACLE を利用される場合のみ以下のファイルを変更してください。
(LDAP、NED、MSAD、CSV および MySQL を使用される場合には変更の必要はありません)

/opt/icewall-ss0/certdd/bin/start-cert

/opt/icewall-ss0/certdd/bin/end-cert

/opt/icewall-ss0/certdd/bin/info-cert

/opt/icewall-ss0/certdd/bin/reload-cert

```
/opt/icewall-ssso/certd/bin/logout-cert
/opt/icewall-ssso/certd/bin/cdump-cert
```

例えば、Oracle11g 版の start-cert は下記のようにになります。

```
#!/bin/sh

export ORACLE_HOME=/home/oracle/app/oracle/product/11.1.0/client_1
export IW_HOME=/opt/icewall-ssso
export SHLIB_PATH=$ORACLE_HOME/lib:$IW_HOME/lib/certd
export LD_LIBRARY_PATH=$SHLIB_PATH
export TWO_TASK=ORCL

$IW_HOME/certd/bin/certd -c $IW_HOME/certd/config/cert.conf
```

この中の ORACLE_HOME をオラクル製品がインストールされているディレクトリ名に変更してください。設定するディレクトリ名は、oracle ユーザーでログインし、次のコマンドで表示されるものです。

```
$ env | grep ORACLE_HOME
```

SHLIB_PATH は枠内で設定している内容に変更してください。

TWO_TASK には接続するデータベースの接続識別子を設定してください。

- (7) 認証モジュールに関するディレクトリおよびファイルのオーナーを、(5) で作成したユーザーに変更します。

使用コマンド例

```
#chown -R iwadmin:users /opt/icewall-ssso/certd
```

3.3 インストール作業後の設定

インストール後に、IceWall SSO を動作させるための以下の設定を行ってください。

3.3.1 暗号化ライブラリに関する設定

認証モジュールをインストールすると以下のパスワード暗号化ライブラリがインストールされます。

ライブラリ名	用途
libiwPwDHash.sl	パスワード暗号化ライブラリ

使用する DB によって、認証モジュール設定ファイル (cert.conf) の PWDLOGINHASH 設定項目、PWDCHGHASH 設定項目を変更する必要があります。

詳細は「IceWall SSO リファレンスマニュアル」を参照してください。

3.3.2 LDAP サーバーのパスワード設定

ユーザーのパスワード暗号化アルゴリズムは任意に指定できますが、LDAP 版で **SHA** 以外を使用する場合は、LDAP サーバーインスタンスのパスワードの暗号化を **ClearText** (暗号化なし) に設定してください。

3.4 推奨する設定

IceWall SSO を動作させる上で必須ではありませんが、推奨の設定があります。

3.4.1 Web サーバーインスタンスの KeepAlive 設定

バックエンド Web サーバーのインスタンスの **KeepAlive** 設定は **OFF** にしてください。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** 設定を **ON** することを推奨します。**OFF** にして使用した場合、コンテンツが表示されてもフォワーダーのタイムアウトまで通信が切断されないため、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。

3.4.2 SSL 通信を使用する際の SSLSessionCache の設定

バックエンド Web サーバーが **Apache HTTP Server** で **SSL** 通信を使用する場合は、**Apache** 側の設定で **SSLSessionCache** ディレクティブにて共有メモリを使用するように指定してください。この設定を行わない場合、パフォーマンスが低下する場合があります。

4 アンインストール方法

IceWall SSO のアンインストールは、インストールと同様にモジュール別に行います。

4.1 フォワーダーのアンインストール

以下の方法でアンインストールを行います。

- (1) root ユーザーでアンインストールを行うサーバーへログインします。
- (2) Apache を停止します。
- (3) Apache の設定ファイルよりフォワーダーを動作させるための設定を削除します。
- (4) 次のコマンドでアンインストールを行います。

```
# rpm -e IceWall-SSO-dfw
```

4.2 認証モジュールのアンインストール

以下の方法でアンインストールを行います。

- (1) root ユーザーでアンインストールを行うサーバーへログインします。
- (2) 認証モジュールが動作中は以下の停止コマンド (end-cert) で停止します。

```
# /opt/icewall-ss0/certd/bin/end-cert
```

- (3) 次のコマンドでアンインストールを行います。ターゲット名は以下より選択してください。

```
# rpm -e [ ターゲット名 ]
```

インストールパッケージ	ターゲット名
Oracle11g 版	IceWall-SSO-cert0_oracle1110 10.0
LDAP 版	IceWall-SSO-certd_ldap
NED 版	IceWall-SSO-certd_ned
MSAD 版	IceWall-SSO-certd_msad
CSV 版	IceWall-SSO-certd_csv
OpenLDAP 版	IceWall-SSO-certd_openldap
MySQL 版	IceWall-SSO-certd_odbc

5 インストール結果の確認方法

IceWall SSO のインストールが正しく行われたかどうかを判断するために、以下の 3 つの確認を行ってください。

5.1 各モジュールの動作を簡単に確認する

インストールしたモジュールごとに、以下の確認を行ってください。

5.1.1 フォワーダーの確認

Web サーバーのユーザーでフォワーダーの動作を確認します。ここでは Web サーバーのユーザーを `apache` とします。`root` ユーザーでログインした後、以下の手順でフォワーダーの動作確認を行ってください。(カレントディレクトリにコンフィグレーションファイルがあることが前提になるため、この手順に従ってください)

Red Hat Enterprise Linux v.5.4 (x86 64bit) の場合

```
# cd /opt/icewall-ss0/dfw/cgi-bin/  
# sudo -u apache env LD_LIBRARY_PATH=/opt/icewall-ss0/lib/dfw HT  
TP_HOST=localhost ./dfw
```

以下のような内容が出力されることを確認してください。

```
<html>  
<head>  
<title>IceWall SSO - No Alias Error</title>  
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">  
<meta http-equiv="Pragma" content="no-cache">  
  
<style type="text/css">  
<!--  
BODY, TD {  
    font-family: Verdana, Arial, Helvetica, Sans-serif;  
    font-size: 12px;  
}  
a:hover {  
    color: #ff3300;  
    text-decoration: underline;  
}  
.title {  
    font-size: 18px;  
    font-family: Verdana, Arial, Helvetica, Sans-serif;  
}
```

```

.sub-title {
    font-size: 16px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
    line-height: 18px;
}
.sub-title2 {
    font-size: 14px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
}
.footer {
    font-size: 11px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
}
-->
</style>

</head>

<body bgcolor="#006699" text="#000000" link="#336699" alink="#ff3300"
topmargin="0" marginheight="0">

<center>
<table border="0" width="80%" height="92%" bgcolor="#ffffff"
cellpadding="0" cellspacing="0">
    <tr>
        <td height="28" align="center">
            <table border="0" width="100%" height="28" cellpadding="1"
cellspacing="0">
                <tr>
                    <td bgcolor="#99ccff"></td>
                </tr>
            </table>
        </td>
    </tr>
    <tr>
        <td height="100%" align="center">
            <table border="0" width="420" cellpadding="0" cellspacing="0">
                <tr bgcolor="#cc3333">
                    <td width="18" height="35"></td>
                    <td width="175" height="35"></td>
                    <td width="227" height="35" align="right"><font color="#ffffff"> ■
</font>&nbsp;</td>
                </tr>
            </table>
            <table border="0" width="420" cellpadding="0" cellspacing="0">
                <tr>
                    <td bgcolor="#666666">
                        <table border="0" width="420" cellpadding="3" cellspacing="1">
                            <tr>
                                <td height="180" bgcolor="#ffffff" align="center">
                                    <div class="sub-title"><b>- No Alias Error -</b></div><br>
                                    
                                    <p><div class="sub-title2"><b>エイリアスが指定されていません </
b></div>
                                </td>

```



```
        </tr>
      </table>
    </td>
  </tr>
</table>
</td>
</tr>
<tr>
  <td height="15" align="center">
    <table border="0" width="100%" height="15" cellpadding="1"
cellspacing="0">
      <tr>
        <td bgcolor="#99ccff"></td>
      </tr>
    </table>
  </td>
</tr>
</table>
</center>

</body>
</html>
```

5.1.2 認証モジュールの確認

認証モジュールを起動するには、iwadmin ユーザーで起動コマンド (start-cert) を実行します。

```
$ /opt/icewall-ss0/certd/bin/start-cert
```

注) 事前に、SQL*Plus、ldapsearch、ice コマンド等で使用する認証 DB へアクセスできることを確認してください。

起動コマンド (start-cert) を実行した後に、次のコマンドで認証モジュールが動作していることを確認してください。

```
$ ps -ef | grep certd
```

動作していない場合には、エラーが発生した可能性があります。エラーログファイル (/opt/icewall-ss0/logs/certerr.log) を確認してください。

5.2 サンプル画面表示による確認

IceWall SSO システム全体の動作を確認するために、「IceWall SSO サンプル設定ガイド」に従って認証 DB の設定と Web サーバーの設定を行い、サンプル画面の表示を確認することをお勧めします。

詳細については、「IceWall SSO サンプル設定ガイド」を参照してください。

5.3 インストールファイルの確認

各パッケージのファイルは/opt/icewall-ss0以下のディレクトリにインストールされますが、インストールを行うパッケージの種類によりインストールされるファイルが異なります。インストール後は /opt/icewall-ss0 ディレクトリ以下のファイル構成を確認してください。

5.3.1 フォワーダーパッケージ

ディレクトリおよびファイル名 (権限)			
/dfw(775)	/cgi-bin(775)	dfw(755) dfw.conf(644) sample.conf(644) html.conf(644) chtml.conf(644) form.conf(644) autologin.html(644) iw_postdata.html(644)	
	/chtml(755)	/image(755) - i-error.gif(444) - i-line.gif(444) - i-logout.gif(444) - i-title.gif(444) access_error.html(644) datasend_error.html(644) filter_get_error.html(644) filter_html_error.html(644) filter_post_error.html(644) filter_request_error.html(644) 10.0 filter_svr_error.html(644) login.html(644) login_force.html(644) login_group_error.html(644) login_limit_error.html(644) login_lock_error.html(644) login_postlimit_error.html(644) 10.0 login_pwd_error.html(644) login_stop.html(644) login_userid_error.html(644) logout.html(644) logout_error.html(644) logout_no.html(644) logout_ok.html(644) max_postsize_err.html(644) pwdchg.html(644) pwdchg_err.html(644) pwdchg_nologin.html(644) pwdchg_ok.html(644) pwdchg_oldpasserr.html(644) pwdchg_policy_err.html(644) pwdchg_postlimit_err.html(644) 10.0 pwdchg_pwvioerr.html(644) pwdchg_repasserr.html(644) pwdchg_warning.html(644) request_acl_error.html(644) 10.0 system_alias_error.html(644) system_backend_error.html(644) system_busy_database.html(644) 10.0 system_certd_error.html(644) system_error.html(644)	

ディレクトリおよびファイル名 (権限)			
		system_ldap_error.html(644) system_server_error.html(644) system_timeout_bkend.html(644) system_timeout_certd.html(644) usr_ext1.html(644) usr_ext2.html(644) usr_ext3.html(644) usr_ext4.html(644) usr_ext5.html(644) usr_ext6.html(644)	
	/html(755)	/image(755)	arrow.gif(444) arrow2.gif(444) curve_b.gif(444) curve_r.gif(444) error.gif(444) footer.gif(444) header.gif(444) title_b.gif(444) title_r.gif(444)
		access_error.html(644) datasend_error.html(644) filter_get_error.html(644) filter_html_error.html(644) filter_post_error.html(644) filter_request_error.html(644) 10.0 filter_svr_error.html(644) login.html(644) login_cert.html(644) login_cert_error.html(644) login_error.html(644) login_force.html(644) login_group_error.html(644) login_limit_error.html(644) login_lock_error.html(644) login_postlimit_error.html(644) 10.0 login_pwd_error.html(644) login_stop.html(644) login_userid_error.html(644) logout.html(644) logout_error.html(644) logout_no.html(644) logout_ok.html(644) max_postsize_err.html(644) pwdchg.html(644) pwdchg_err.html(644) pwdchg_nologin.html(644) pwdchg_ok.html(644) pwdchg_oldpasserr.html(644) pwdchg_policy_err.html(644) pwdchg_postlimit_err.html(644) 10.0 pwdchg_pwvioerr.html(644) pwdchg_repasserr.html(644) pwdchg_warning.html(644) request_acl_error.html(644) 10.0 system_alias_error.html(644) system_backend_error.html(644) system_busy_database.html(644) 10.0 system_certd_error.html(644) system_error.html(644) system_ldap_error.html(644) system_server_error.html(644) system_timeout_bkend.html(644)	

ディレクトリおよびファイル名 (権限)			
		system_timeout_certd.html(644) usr_ext1.html(644) usr_ext2.html(644) usr_ext3.html(644) usr_ext4.html(644) usr_ext5.html(644) usr_ext6.html(644)	
/iwpmdd(775)	/bin(775)	iwpmdd(755) iwpmdd(755)	
	/conf(775)	iwpmdd.conf(644)	
	/data(775)		
	/run(775)		
	/script(775)	iwpmdd_analyselogs.pl(755) iwpmdd_calccoverage_perf.pl(755) iwpmdd_count_errlog.pl(755) iwpmdd_printdata_perf.pl(755) iwpmdd_printdata_screen.pl(755) iwpmdd_printheadr_perf.pl(755)	
	/tmp(775)		
/lib(555)	/dfw(555)	libDfwExit.so(777) ※ リンク libsidcrypto.so(777) ※ リンク libssl.so(777) ※ リンク libcrypto.so(777) ※ リンク libCryptoExit.so(777) ※ リンク	
	libDfwExit.sl(555) libsidcrypto.sl(555) libssl.sl(555) libcrypto.sl(555) libDfwCryptoExit.sl(555)		
/logs(777)			
/messages(555)	/C(555)	icewall_dfw.cat(444) ⑩⑩	
/developkit(775) 10.0	/dfw(755)	/DfwExit(755)	Makefile(644) dfwinterface.c(644) dfwinterface.h(444)
		/DfwCryptoExit(755)	Makefile(644) iwcrypto.c(644) iwcrypto.h(444) libcpt.a(444)

5.3.2 認証モジュールパッケージ

ディレクトリおよびファイル名 (権限)			
/certd(775)	/bin(775)	certd(755) logout-cert(755) ⑩⑩ cdump-cert(755) ⑩⑩ start-cert(755) end-cert(755) info-cert(755) reload-cert(755)	
	/config(775)	cert.conf(644) cert.grp(644) cert.acl(644) dbattr.conf(644) logdbattr.conf(644) ※ ORACLE 版のみ pwdforbid.conf(644) request.acl(644) sample.csv(644) ※ CSV 版のみ	

ディレクトリおよびファイル名（権限）			
/iwpmc(775)	/bin(775)	iwpmc(755) iwpmcd(755)	
	/conf(775)	iwpmc.conf(644)	
	/data(775)		
	/run(775)		
	/script(775)	iwpmc_analyselog.pl(755) iwpmc_calcaverage_info.pl(755) iwpmc_calcaverage_perf.pl(775) iwpmc_printdata_info.pl(755) iwpmc_printdata_perf.pl(755) iwpmc_printdata_screen.pl(755) iwpmc_printhead_info.pl(755) iwpmc_printhead_perf.pl(755)	
	/tmp(775)		
/lib(555)	/certd(555)	libDB.so(777) ※リンク libPH.so(777) ※リンク libCertExit.so(777) ※リンク libCryptoExit.so(777) ※リンク 10.0 libExCryptoExit.so(777) ※リンク libCreateSidExit.so(777) ※リンク libiwDBCrypto.so(777) ※リンク 10.0 libiwDBCryptoExit.so(777)※リンク 10.0 libcrypto.so(777) ※リンク libssl.so(777) ※リンク LDAP 版、OpenLDAP 版、 NED 版、MSAD 版のみ liblber.so(777) ※リンク LDAP 版、OpenLDAP 版、 NED 版、MSAD 版のみ libldap.so(777) ※リンク LDAP 版、OpenLDAP 版、 NED 版、MSAD 版のみ libsasl2.so(777) ※リンク LDAP 版、OpenLDAP 版、 NED 版、MSAD 版のみ	
	libCertExit.sl(555) libCryptoExit.sl(555) libExCryptoExit.sl(555) libCreateSidExit.sl(555) libiwORA1110.sl(555) ※ ORACLE 版のみ 10.0 libiwODBC.sl(555) ※ MySQL 版のみ libiwLDAP.sl(555) ※ LDAP 版、OpenLDAP 版、NED 版、MSAD 版のみ libiwCSV.sl(555) ※ CSV 版のみ libiwPwdHash.sl(555) 10.0 liblber.sl(555) ※ LDAP 版、OpenLDAP 版、NED 版、MSAD 版のみ libldap.sl(555) ※ LDAP 版、OpenLDAP 版、NED 版、MSAD 版のみ libsasl2.sl(555) ※ LDAP 版、OpenLDAP 版、NED 版、MSAD 版のみ libcrypto.sl(555) libssl.sl(555) ※ LDAP 版、OpenLDAP 版、NED 版、MSAD 版のみ 10.0 libiwDBCrypto.sl(555) 10.0 libiwDBCryptoExit.sl(555) 10.0		
/lib32(555)	libcrypto.sl(555)	※ MSAD 版以外	
※ MSAD 版以外	/mkuser(555)	libcrypto.so(777)	※リンク MSAD 版以外
/logs(777)			
/messages(555)	/C(555)	icewall_certd.cat(444) 10.0	
/developkit(775) 10.0	/certd(775) 10.0	/CertExit(775)	Makefile(644) iwintface.c(644) iwintface.h(444)
		/PwdLib(775)	Makefile(644) iwphash.c(644) iwphash.h(444)

ディレクトリおよびファイル名 (権限)			
		/CryptoExit(755)	Makefile(644) iwcrypto.c(644) iwcrypto.h(444) libcpt.a(444)
		/ExCryptoExit(755)	Makefile(644) csexicpcrypto.c(644) csexicpcrypto.h(444) iwcrypto.h(444) libcpt.a(444)
		/SidExit(755)	Makefile(644) iwcreatesid.c(644) iwcreatesid.h(444)
		/DBCryptoExit(755)	Makefile(644) csexdbcrypto.c(644) csexdbcrypto.h(444)
/sample_src(775)	/ICP20(755)	/sample1(755)	Makefile(644) Sample1.java(644) sample1.c(644)
		/sample2(755)	Makefile(644) Sample2.java(644) sample2.c(644)
		/agent(755)	Makefile(644) mod_sample.c(644)
/tools(775) ※ MSAD 版以外	mkuser(755) mkuser.seed(644) TEMPLATE.sql(644) TEMPLATE.ldif(644) TEMPLATE.csv(644) add_test_user.sql(644) cre_sequence.sql(644) cre_tbl_history.sql(644) cre_tbl_test.sql(644) DATA.txt(644)	※ MSAD 版以外 ※ MSAD 版以外 ※ ORACLE 版、MySQL 版のみ ※ LDAP 版、OpenLDAP 版、NED 版のみ ※ CSV 版のみ ※ ORACLE 版、MySQL 版のみ ※ ORACLE 版のみ ※ ORACLE 版のみ ※ ORACLE 版のみ ※ ORACLE 版、MySQL 版のみ ※ MSAD 版以外	

5.4 バージョン情報の確認について

インストール後に、本バージョンのバイナリがインストールされているかの確認を行います。この情報は、トラブルが発生した際にサポートへ問い合わせる場合にも必要です。

5.4.1 フォワーダーの確認方法

フォワーダーのバージョン情報を確認する方法は、以下のとおりです。

- (1) バイナリがあるディレクトリまで移動します。

```
# cd /opt/icewall-ssso/dfw/cgi-bin
```

- (2) 以下のコマンドを入力します。

```
# strings dfw | grep '@(#)'
```

- (3) 以下の内容が表示されます。

例)

```
@(#)IceWall SSO dfw
@(#)Version: 10.00.00.xxxxxxxX
@(#)OS : Linux 2.6.18
@(#)CPU: x86_64
@(#)Bit: 64bit
@(#) (c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```

5.4.2 認証モジュールの確認方法

認証モジュールでバージョン情報を確認するモジュールは、認証モジュール本体のバイナリ、認証 DB 接続ライブラリの 2 つとなります。確認する方法は、以下のとおりです。

<認証モジュール本体のバイナリ>

(1) バイナリがあるディレクトリまで移動します。

```
# cd /opt/icewall-ss0/certd/bin
```

(2) 以下のコマンドを入力します。

```
# strings certd | grep '@(#)'
```

以下の内容のものが表示されます。

例)

```
@(#)IceWall SSO certd
@(#)Version: 10.00.00.xxxxxxxX
@(#)OS : Linux 2.6.18
@(#)CPU: x86_64
@(#)Bit: 64bit
@(#) (c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```

<認証 DB 接続ライブラリ>

(1) バイナリがあるディレクトリまで移動します。

```
# cd /opt/icewall-ss0/lib/certd
```

(2) 以下のコマンドを入力します。

```
# strings libDB.so | grep '@(#)'
```

(3) 以下の内容が表示されます。

なお、なお、認証 DB の違いにより出力される内容が異なります。

例) Oracle11g 版

```
@(#)IceWall SSO Database Plug-in Oracle 11.1.0.6.0
@(#)Version: 10.00.00.xxxxxxxX
@(#)OS : Linux 2.6.18
@(#)CPU: x86_64
@(#)Bit: 64bit
@#)(c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```


6 従来バージョンからのバージョンアップについて

従来バージョンをご使用中で、本バージョンにバージョンアップを行う場合、次の方法で行ってください。

※ 一部のバイナリのみ置き換えるなど、以下の手順以外でのバージョンアップについてはサポート対象外となりますのでご注意ください。

6.1 バージョンアップ手順

以下のようにバージョンアップを行います。

- (1) IceWall サーバーの Web サーバーを停止します。
- (2) 認証サーバーの認証モジュールを停止します。
- (3) IceWall サーバー、認証サーバーで使用中の各設定ファイルのバックアップを行います。
- (4) IceWall サーバー、認証サーバーでそれぞれ独自に開発した UserExit やパスワード暗号化ライブラリなどを使用している場合は、それらのバックアップを行います。
- (5) IceWall サーバー、認証サーバーの各ログファイルが必要な場合はそれらのバックアップを行います。
- (6) 8.0 以前のバージョンからのバージョンアップを行う場合、従来バージョンのインストール時に、/usr/lib ディレクトリ以下に設定したライブラリのシンボリックリンクを削除します。
8.0 以降のバージョンからのバージョンアップを行う場合は (7) へ進んでください。
- (7) 従来バージョンの IceWall のアンインストールを行ってください。アンインストール方法については、従来バージョンの「IceWall SSO 導入ガイド」を参照してください。
- (8) 本バージョンのインストールを行います。
- (9) (4) にてバックアップを行った場合、それらのライブラリを /opt/icewall-sso/lib ディレクトリ以下へリストアします。認証サーバーにて、パスワード暗号化ライブラリを標準で設定されているものから変更している場合は、ライブラリのリンクを変更してください。(ただし、従来バージョンのライブラリはそのまま使用することができないため、後述の注意事項を参照してください)
- (10) (3) でバックアップを行った設定ファイルをリストアします。
- (11) 認証モジュールの受信ポート番号を変更している場合は、認証モジュールコマンド (end-cert、reload-cert、info-cert、logout-cert、cdump-cert) 内のポート番号を変更してください。

以上でバージョンアップは終了です。

IceWall SSO は設定ファイルの下位互換性が保証されているため、従来バージョンで使用していたものをそのまま使用することができます。

※ ただし、パスワード禁止文字列設定ファイルについてはデフォルトで正規表現となるため、部分一致となります。従来通りの完全一致とするためには、禁止文字列の前後をハット [^] とダラー [\$] で囲む必要があります。

6.2 従来バージョン共通の注意事項

バージョンアップを行うにあたり、従来の各バージョン共通で注意しなければならない点があります。

- (1) 認証モジュールコマンド (start-cert、end-cert、reload-cert、info-cert、logout-cert、cdump-cert) に何らかの処理を追加していた場合は、必ず本バージョンの認証モジュールコマンドに追加するようにしてください。認証モジュールコマンド自身は従来バージョンのものを使用することはできません。
- (2) CTYPE 項目のデフォルト値が「なし」に変更されたため、次のパラメーターをホスト設定ファイルへ追加してください。
CTYPE=text/html
- (3) 独自開発した UserExit ルーチンを使用している場合には、リビルドしてください。
- (4) 独自開発したパスワード暗号化ライブラリを使用している場合には、リビルドしてください。
- (5) 本バージョンよりモジュールの bit 数は 64bit となっています。8.0R3 以前のバージョンで、32bit 版のランタイムライブラリを指定している場合は、バージョンアップ時に 64bit 版のランタイムライブラリを指定するようにしてください。 **10.0**
- (6) フォワーダーが内部のホスト設定として固定で保持している、エイリアス名「LOCALHOST」ホスト名「localhost」ポート番号「80」を使用している場合は、フォワーダー設定ファイルの HOST 項目設定の一番上に次のパラメーターを設定してください。
HOST=LOCALHOST=localhost:80 **10.0**
- (7) アクセスログに出力される 3 つの時間の桁数がミリ (1/1000) 秒からマイクロ (1/1000000) 秒に変更されたため、監視などで使用している場合は注意してください。
10.0
- (8) 1 つのパスワード暗号化ライブラリで MD5、SHA1、SHA256、PLAIN と複数のハッシュが扱えるようにライブラリが統合されました。認証 DB 内のハッシュに合わせて認証モジュール設定ファイル (cert.conf) の PWDLOGINHASH 項目を設定してください。 **10.0**
- (9) 従来のバージョンにて、接頭辞なしの MD5 で暗号化ライブラリ (libiwPMHO.sl) を使用していた場合、以下の点に注意してください。 **10.0**
 - ・パスワード変更機能使用時の注意点
パスワード変更機能によってパスワードを変更する場合、新パスワードを認証 DB へ格納する際に接頭辞 {MD5} が付加されます。そのため、認証 DB のカラム (属性) のデータサイズを 37 バイトへ拡張してください。

- ・ログイン時のハッシュ方式の設定方法

BIND 認証を使用しないログイン時には、PWDLOGINHASH に AUTO-MD5 を設定してください。

BIND 認証を使用するログイン時には、PWDLOGINHASH に MD5 を設定してください。

- (10) 動作情報出力コマンド (info-cert) で出力されるメッセージが変更されました。詳しくは「IceWall SSO ユーザーズマニュアル」を参照してください。 **10.0**
- (11) 64 バイト長でセッション ID を生成する設定の場合は、UserExit で取得されるセッション ID の長さも 64 バイト長とする対応が必要になります。 **10.0**
- (12) メッセージカタログファイル名が変更されました。詳しくは「IceWall SSO リファレンスマニュアル」の、フォワーダー設定ファイルおよび認証モジュール設定ファイルの CATALOG 設定項目を参照してください。 **10.0**
- (13) 本バージョンより、パスワードポリシーに関する設定はフォワーダーから認証モジュールへ移行しています。これまでのバージョンどおりフォワーダーでの設定も有効ですが、認証モジュール側へ移行することをお勧めします。
パスワードポリシーに関する設定をフォワーダー側で設定したままバージョンアップを行うと、認証モジュール側の初期値が有効になってしまう場合があります。この場合、フォワーダー側の設定と同じものを認証モジュール側にも設定を行ってください。 **10.0**

6.3 8.0 以前のバージョン共通の注意事項

バージョンアップを行うにあたり、10.0 以前の各バージョン共通で注意しなければならない点があります。

- (1) ライブラリの構成が変更されています。従来は /usr/lib 以下に必要なリンクを作成していましたが、リンクはすべて /opt/icewall-ssso/lib/dfw と /opt/icewall-ssso/lib/certd 以下に移動しています。詳細は「5.3 インストールファイルの確認」を参照してください。
また、これに伴いフォワーダーが動作する Web サーバーの設定を変更する必要があります。詳細は「3.1 フォワーダーのインストール (6)」を参照してください。

6.4 従来バージョン別の注意事項

IceWall SSO は、これまでのバージョンで様々な機能追加や仕様変更が行われています。そのため、元のバージョン別に注意する点が異なります。

6.4.1 5.1i からのバージョンアップの場合

- ・バックエンド Web サーバーへ If-modified-since ヘッダーが転送されるようになっていきます。従来どおりの仕様に動作させる場合は、ホスト設定ファイルに以下の設定を追加してください。

HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND

- ・認証モジュールの UserExit ルーチンの仕様が変更されています。UserExit ルーチンのソースコードの修正が必要です。

6.4.2 5.1iSP1、5.1iSP2 からのバージョンアップの場合

- ・認証モジュールの UserExit ルーチンの仕様が変更されています。UserExit ルーチンのソースコードの修正が必要です。
- ・バックエンド Web サーバーへ If-modified-since ヘッダーが転送されるようになっていきます。従来どおりの仕様に動作させる場合は、ホスト設定ファイルに以下の設定を追加してください。

HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND

- ・認証 DB として MSAD を使用している場合、次のパラメーターを認証モジュール設定ファイルへ追加してください。

LDAPBIND=1

LDAPPCHG=0

LDAPLANG=0

6.4.3 6.0、6.0SP1、6.0.1SE からのバージョンアップの場合

- ・認証モジュールの UserExit ルーチンの仕様が変更されています。UserExit ルーチンのソースコードの修正が必要です。
- ・バックエンド Web サーバーへ If-modified-since ヘッダーが転送されるようになっていきます。従来どおりの仕様に動作させる場合は、ホスト設定ファイルに以下の設定を追加してください。

HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND

- ・認証 DB として MSAD を使用している場合、次のパラメーターを認証モジュール設定ファイルへ追加してください。

LDAPBIND=1

LDAPPCHG=0

LDAPLANG=0

6.4.4 7.0 からのバージョンアップの場合

- ・バックエンド Web サーバーへ If-modified-since ヘッダーが転送されるようになっていきます。従来どおりの仕様に動作させる場合は、ホスト設定ファイルに以下の設定を追加してください。

HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND

- ・ 認証 DB として MSAD を使用している場合、次のパラメーターを認証モジュール設定ファイルへ追加してください。

LDAPBIND=1
LDAPPCHG=0
LDAPLANG=0

6.4.5 7.0SP1、7.0SP2、7.0SP3、7.0.1SE からのバージョンアップの場合

- ・ 認証 DB として MSAD を使用している場合、次のパラメーターを認証モジュール設定ファイルへ追加してください。

LDAPBIND=1
LDAPPCHG=0
LDAPLANG=0

- ・ 認証 DB として NED を使用している場合、次のパラメーターを認証モジュール設定ファイルへ追加してください。

LDAPBIND=1
LDAPPCHG=1
LDAPLANG=1

6.4.6 8.0、8.0.1(8.0R1)、8.0 R2、8.0 R3 からのバージョンアップの場合

- ・ 「以前のバージョン共通の注意事項」のみです。

7 制限事項

本バージョンを使用するにあたり、以下の制限事項が存在します。

7.1 FailOver Option 使用時の注意点

レプリケーション構成（マスター・レプリカ）の認証モジュールの両方でリクエストを処理することは、障害時を除きサポートされません。障害復旧後は、マスターのみで処理されるように運用するようにしてください。レプリケーション構成時には、マスター・レプリカ間でレプリケーション処理が行われるため認証モジュールへのリクエストをマスター・レプリカでわけても負荷分散にはなりませんのでご注意ください。

7.2 Range 指定されたコンテンツのサイズについて

変換対象となるコンテンツに対して Range 指定された場合、ブラウザー・フォワーダー間とフォワーダー・Web サーバー間では、コンテンツ変換によりコンテンツサイズが異なるため、取得する位置がずれてしまう場合があります。

7.3 IE6.x を使用して SSL 環境でファイルがダウンロードできない

SSL で動作する Web サーバーに対して Microsoft Internet Explorer 6.x を使用する場合、HTTP ヘッダーに「Pragma: no-cache」が存在するとファイルがダウンロードできない問題があります。これは Microsoft Internet Explorer 6.x の問題であり、IceWall を経由せずに直接 Web サーバーと接続しても発生します。この問題が発生した場合はマイクロソフト社へお問い合わせください。

8 ドキュメント参照方法

CD-ROM 内のマニュアル、ドキュメントは、PDF ファイルで提供されています。これらを読むためには、アドビシステムズ社の Adobe Reader が必要になります。

注) Adobe Reader は、アドビシステムズ社のホームページより無償でダウンロードできます。インストール方法や使用方法については、Adobe Reader のマニュアル等を参照してください。

9 注意事項

製品に含まれるサンプルファイルについてのすべての権利は、Hewlett-Packard Development Company, L.P. が保有します。ただし、それについてはサポート対象外です。

IceWall SSO のパッチについては、IceWall サポートページからダウンロードしてください。

10 関連 URL、お問い合わせ先

< IceWall SSO 関連 >

製品情報

日本ヒューレット・パッカード株式会社

(<http://www.hp.com/jp/icewall/>)

株式会社 SCC

(<http://www.scc-kk.co.jp/>)

サポート情報

IceWall サポートページ

(<https://icewall.scc-kk.co.jp/>)

< その他 >

日本オラクル株式会社

(<http://www.oracle.co.jp/>)

サン・マイクロシステムズ株式会社

(<http://www.sun.co.jp/>)

アドビ システムズ 株式会社

(<http://www.adobe.com/jp/>)

レッドハット株式会社

(<http://www.redhat.co.jp/>)

Apache Software Foundation

(<http://www.apache.org/>)

ノベル株式会社

(<http://www.novell.co.jp/>)

マイクロソフト株式会社

(<http://www.microsoft.com/japan/>)