



IceWall SSO

Version 10.0

導入ガイド for Client Certificates Option

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. B2873-97003

Rev.100820A

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。

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written
by Eric Young (ey@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence
[including the GNU Public Licence.]

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
1.2 文中における用語について	1
2 Client Certificates Option 導入時のシステム概要	2
2.1 システム構成と処理の流れ	2
2.2 ユーザー認証の制限	2
3 認証 DB に保存する証明書情報	4
3.1 証明書発行時および証明書更新時	4
3.2 ユーザー認証時	4
4 設定方法	5
4.1 Web サーバーの設定追加	5
4.1.1 Apache の設定方法	5
4.2 認証 DB の拡張	5
4.2.1 ORACLE 版	6
4.2.2 NED 版、LDAP 版、OpenLDAP 版 10.0	6
4.2.3 CSV 版	6
4.2.4 MySQL 版	7
4.3 認証モジュールの認証 DB 設定の拡張	7
4.3.1 ORACLE 版、CSV 版および MySQL 版	7
4.3.2 NED 版、LDAP 版、OpenLDAP 版 10.0	7
4.4 認証モジュールのログカラム設定ファイルの拡張	8
4.5 認証モジュールにおける証明書使用時の動作設定	8
4.6 フォワーダーにおける証明書使用時の動作設定	9
4.7 フォワーダーの HTML 設定の追加	10
4.8 プロセスのリスタート	10
4.9 ロードバランサーの SSL アクセラレーター機能を使用する場合	10
4.9.1 SSL アクセラレーター機能の前提	10
4.9.2 フォワーダーの設定	11
5 UserExit ルーチンの拡張	12
6 設定例	13
6.1 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (ORACLE 版)	13
6.2 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (LDAP 版)	14
6.3 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (OpenLDAP 版)	15
6.4 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (NED 版)	16
6.5 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (CSV 版)	17
6.6 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (MySQL 版)	18
6.7 ログカラム設定ファイル (logdbattr.conf) の設定例 (ORACLE 版のみ)	19

1 はじめに

Client Certificates Optionとは、クライアント証明書によりクライアントとIceWallサーバー間で安全かつ確実な本人確認を実現するための製品です。

ご注意

認証 DB として Microsoft Active Directory を使用する場合、本オプションは利用することができませんので、あらかじめご了承ください。

1.1 文中におけるバージョン表示記号について

文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。

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。

1.2 文中における用語について

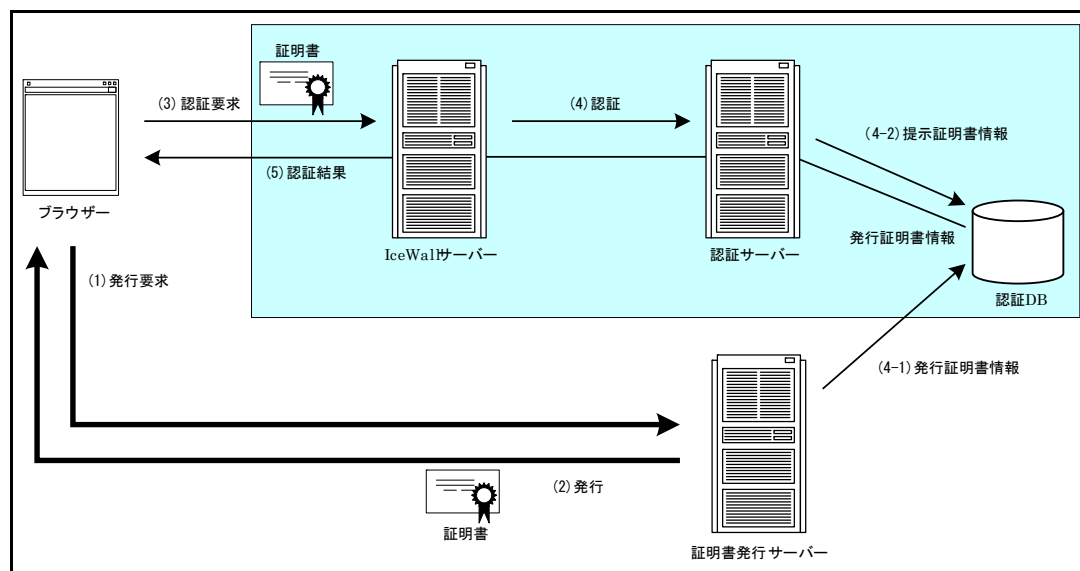
これ以降では、以下の用語を使用して記述する場合があります。

用語	意味
ORACLE 版	Oracle Database 11g 10.0
LDAP 版	Sun Java System Directory Server
	Netscape Directory Server
	Red Hat Directory Server
OpenLDAP 版	OpenLDAP
NED 版	Novell eDirectory
MySQL 版	MySQL Server
Apache	Apache HTTP Server
	HP-UX Apache-Based Web Server

2 Client Certificates Option 導入時のシステム概要

Client Certificates Option を導入する場合に前提となるシステム構成および処理の流れを以下に説明します。

2.1 システム構成と処理の流れ



- (1) クライアントが証明書発行のリクエストを行います。
- (2) 証明書発行サーバーで証明書の発行を行い、発行された証明書の情報を認証 DB へ保存します。発行された証明書はクライアントのブラウザにインストールします。
- (3) 証明書を使用して IceWall SSO へ認証要求を行います。IceWall サーバーに提示された証明書を解釈し認証に必要な情報を取得します。
- (4) 取得した証明書情報を認証サーバーへ送信し認証を行います。
 - (4-1) 認証 DB に保存されている発行証明書情報を取得し証明書の有効性チェックを行います。
 - (4-2) 認証された場合は提示された証明書の情報を認証 DB へ保存します。
- ※ 証明書発行後に初めて行う認証を「初回認証」と呼びます。更新された証明書で初めて行う認証を「更新後初回認証」と呼びます。
- (5) 認証された結果が IceWall サーバーよりブラウザに通知されます。

2.2 ユーザー認証の制限

クライアント証明書を使用しますと、ユーザー認証で以下の制限が追加されます。

- (1) ブラウザーについて

ユーザーID による認証の場合は、任意のクライアントよりログインが可能でしたが、証明書を使用する場合は、証明書がブラウザ（または外部メディア）にインストールされている必要があります。

(2) 証明書使用後のユーザー ID による認証

証明書による認証を行ったユーザーは、それ以降の認証では証明書を使用せずに、ユーザー ID を入力する認証（以下、ユーザー ID 認証）は禁止されます。（設定で制限を解除することが可能です）

(3) 証明書更新時の証明書の有効性

ユーザー認証に使用される証明書は、1 世代（現行の証明書）のみです。ただし証明書の更新を行った後に、更新された新しい証明書で認証を行うまでは、現行の証明書による認証が可能です。

(4) 証明書の情報として利用可能な文字

cn および ou には利用可能な文字に以下の制限が存在します。

領域名	利用可能な文字（※すべて半角文字）
cn	英数字 - .
ou	英数字 - . _

なお、.（ピリオド）は末尾に使用することはできません。

3 認証 DB に保存する証明書情報

Client Certificates Option では、クライアント証明書の同一性の確認を行うために、証明書の情報を認証 DB へ保存する必要があります。以下に保存する情報を保存タイミング別に記載します。

3.1 証明書発行時および証明書更新時

クライアント証明書の発行時および証明書の更新時に認証 DB へ証明書情報を保存しなければなりません。保存する情報は次のとおりです。

(保存は、証明書発行サーバーまたは管理者による手作業にて行います)

データ名	内容
発行時シリアル No.	発行したクライアント証明書のシリアル No. (X.509 領域名は SerialNumber) と発行者名称 (X.509 領域名は Issuer) を組み合わせてユニークな証明書情報として認証 DB へ保存します。保存する際のデータフォーマットは「シリアル No.: 発行者名称」です。
発行時発行者名称	

3.2 ユーザー認証時

クライアント証明書発行および更新後に行う最初のユーザー認証時に、認証モジュールより認証 DB へ証明書情報が保存されます。保存される証明書情報は次のとおりです。

(保存は IceWall SSO が行います)

データ名	内容
提示時シリアル No.	ブラウザより提示された証明書より取得したシリアル No. (X.509 領域名は SerialNumber) と発行者名称 (X.509 領域名は Issuer) と認証 DB に保存されている発行時の値と比較し、内容が一致する場合に限り発行時に保存したデータをコピーして保存します。データフォーマットは「シリアル No.: 発行者名称」です。
提示時発行者名称	
証明書有効期限	ブラウザより提示された証明書の有効期限 (X.509 領域名は Validity) を保存します。データフォーマットは「YYYYMM DDhhmmss」です。
証明書発行フラグ	証明書の発行状態を保存します。 0: 証明書発行済み 1: 証明書未発行 2: 証明書発行済みで未使用
証明書使用状況フラグ	証明書の使用状況を保存します。 0: 証明書による初回認証を行っていない 1: 証明書による初回認証済み

4 設定方法

Client Certificates Option の設定は以下の手順で行います。IceWall SSO は既に導入済みであり、正常に動作する環境を前提としています。

なお、追加で IceWall SSO のモジュールをインストールする必要はありません。

4.1 Web サーバーの設定追加

IceWall サーバー上の Web サーバーの設定ファイルに、Web サーバーよりブラウザに対してクライアント証明書を要求する命令の記述を追加します。

4.1.1 Apache の設定方法

設定を行う Web サーバーの設定ファイル (Apache 2.x の場合は ssl.conf) に対して以下のように設定します。

SSL で動作する設定の VirtualHost が <VirtualHost_default_:443> の場合、下記の枠内の設定例のように追加します。

```
<VirtualHost _default_:443>
:
SSLCACertificatePath /opt/hpws/apache/
SSLCACertificateFile /opt/hpws/apache/cacert.pem
SSLVerifyClient 2
SSLVerifyDepth 10
:
<Directory "/opt/icewall-ss0/dfw/cgi-bin">
:
    SSLOptions +StdEnvVars +ExportCertData
:
</Directory>
</VirtualHost>
```

設定する値は環境により異なりますので、これらの設定の詳細については、Web サーバーのマニュアルを参照してください。

4.2 認証 DB の拡張

クライアント証明書情報を保存する認証 DB のカラム (属性) を用意します。

発行時シリアル No.、提示時シリアル No. には、証明書のシリアル No. と発行者名称が格納されます。以下の説明ではサイズを 256 としていますが、使用する証明書のシリアル No. と発行者名称のデータサイズを確認した上で決定してください。

※ ORACLE 版と MySQL 版は、必要なカラムを追加した上でテーブルを作成することを前提としています。作成済みのテーブルにカラムを追加する場合は、各データベース製品のマニュアルを参照してください。

4.2.1 ORACLE 版

認証 DB のカラムに下記の項目を追加します。

認証テーブル (SQL : cre_tbl_test.sql ファイルに追加)

RASERIAL	varchar(256)	NULL,
BSSERIAL	varchar(256)	NULL,
VDATE	char(14)	NULL,
CERT	char(1)	DEFAULT 1 NOT NULL,
APENABLE	char(1)	DEFAULT 0 NOT NULL

※ cre_tbl_test.sql ファイルへカラムを追加するときは、各項目はカンマで区切られることと、最後の項目の後ろにはカンマが不要であることに注意してください。

ログ出力テーブル (SQL : cre_tbl_history.sql ファイルに追加)

RASERIAL	varchar(256)
----------	--------------

4.2.2 NED 版、LDAP 版、OpenLDAP 版 10.0

使用する認証 DB の属性を以下の表に基づき決定します。

用途	型	サイズ	内容
発行時シリアル No.	文字型	256	証明書サーバーにて発行された証明書のシリアル No. と発行者名称を格納します。
提示時シリアル No.	文字型	256	ブラウザより提示された証明書のシリアル No. と発行者名称を格納します。
証明書有効期限	文字型	14	ブラウザより提示された証明書の有効期限を格納します。
証明書発行フラグ	文字型	1	証明書の発行フラグを格納します。
証明書使用状況フラグ	文字型	1	証明書使用状況フラグを格納します。

※ 使用する属性は新規に作成するか、Directory Server が標準で持つ属性を使用してください。

4.2.3 CSV 版

テキスト認証 DB のカラムに下記の項目を追加します。

RASERIAL,BSSERIAL,VDATE,CERT,APENABLE

4.2.4 MySQL 版

認証 DB のカラムに下記の項目を追加します。

認証テーブル (SQL : cre_tbl_test.sql ファイルに追加)

RASERIAL	varchar(256)	NULL,
BSSERIAL	varchar(256)	NULL,
VDATE	char(14)	NULL,
CERT	char(1)	DEFAULT 1 NOT NULL,
APENABLE	char(1)	DEFAULT 0 NOT NULL

※ cre_tbl_test.sql ファイルへカラムを追加するときは、各項目はカンマで区切られることと、最後の項目の後ろにはカンマが不要であることに注意してください。

4.3 認証モジュールの認証 DB 設定の拡張

認証モジュールの認証 DB カラム情報ファイル (/opt/icewall-ssso/certd/config/dbattr.conf) にクライアント証明書用カラム情報を追加します。

追加する項目は以下のとおりです。

項目名	必須	内容
RASERIALNO	○	証明書発行サーバーが保存する証明書のシリアル No. および発行者名称を保存するカラム名を指定します。
IWSERIALNO	○	ブラウザより提示された証明書のシリアル No. および発行者名称を保存するカラム名を指定します。
CERTEXPDATE	○	ブラウザより提示された証明書の有効期限を保存するカラム名を指定します。
GETCERT	×	証明書発行フラグを格納するカラム名を指定します。
ONLINE	×	証明書使用状況フラグを格納するカラム名を指定します。

4.3.1 ORACLE 版、CSV 版および MySQL 版

認証 DB カラム情報ファイル (dbattr.conf) に追加する内容 (例)

RASERIALNO=RASERIAL
IWSERIALNO=BSSERIAL
CERTEXPDATE=VDATE
GETCERT=CERT
ONLINE=APENABLE

※ MySQL 版は 8.0 R2 以降

4.3.2 NED 版、LDAP 版、OpenLDAP 版 10.0

認証 DB カラム情報ファイル (dbattr.conf) に追加する内容 (例)

```
RASERIALNO=destinationIndicator
IWSERIALNO=preferredDeliveryMethod
CERTEXPDATE=x500UniqueIdentifier
GETCERT=registeredAddress
ONLINE=teltexTerminalIdentifier
```

※ この例では Sun Java System Directory Server が標準で用意している属性を指定しています。

4.4 認証モジュールのログカラム設定ファイルの拡張

ORACLE 版でログを履歴 DB に出力している場合、認証モジュールのログカラム設定ファイル (/opt/icewall-ss0/certd/config/logdbattr.conf) に証明書用カラムの項目の追加が必要です。

追加する項目は以下のとおりです。

項目名	必須	内容
SERIAL	○	発行時に保存した証明書のシリアル No. および発行者名を保存するカラム名を指定します。

ログカラム設定ファイル (logdbattr.conf) に追加する内容 (例)

```
SERIAL=RASERIAL
```

4.5 認証モジュールにおける証明書使用時の動作設定

認証モジュール設定ファイル (cert.conf) とリクエスト制御設定ファイル (request.acl) に以下の項目が設定可能です。

各項目の設定方法および設定例等の詳細は「IceWall SSO リファレンスマニュアル」を参照してください。

認証モジュール設定ファイル (cert.conf)

項目名	必須	内容
PARALOGIN	×	クライアント証明書による初回認証後に、ユーザー ID によるログインを許可するかどうかの設定を行います。
ACCCTRLFLG	×	クライアント証明書を使用する場合のアクセス制御のセキュリティレベルを設定します。

リクエスト制御設定ファイル (request.acl)

項目名	必須	内容
ACCCTRL	×	ユーザーID とパスワードによるログインやクライアント証明書とパスワードによるログインなどのログイン種別に関係なく、アクセス種別による制御を設定します。 8.0R2

4.6 フォワーダーにおける証明書使用時の動作設定

フォワーダーの設定ファイル (dfw.conf) およびホスト設定ファイル (任意のファイル名) に以下の項目が設定可能です。

各項目の設定方法および設定例等の詳細は「IceWall SSO リファレンスマニュアル」を参照してください。

フォワーダー設定ファイル (dfw.conf)

項目名	必須	内容
CC_UID	○	クライアント証明書よりユーザー ID を取得する領域名の設定を行います。
CC_UIDKEYS	×	クライアント証明書のユーザーID 格納領域から、ユーザー ID として取得する開始位置を指定するための文字列の設定を行います。
CC_UIDKEYE	×	クライアント証明書のユーザーID 格納領域から、ユーザー ID として取得する終了位置を指定するための文字列の設定を行います。 - 検索文字列の長さは制限しません。 - 検索文字列を指定しない場合、CC_UID 項目の最後までがユーザー ID の対象となります。 - デフォルト値はありません。
CC_ENVNAME	×	クライアント証明書情報を取得する環境変数名の設定を行います。
CC_DECODE_FLG	×	クライアント証明書使用時にフォワーダーが証明書をデコードするかどうかを設定します。 8.0R1
CC_ENVUID	×	クライアント証明書情報のユーザー ID が含まれる環境変数名を設定します。 8.0R1
CC_ENVSERIAL	×	クライアント証明書情報のシリアル番号が含まれる環境変数名を設定します。 8.0R1
CC_ENVEXPIRE	×	クライアント証明書情報の有効期限情報が含まれる環境変数名を設定します。 8.0R1
CC_ENVISSUER	×	クライアント証明書情報の証明書発行者情報が含まれる環境変数名を設定します。 8.0R1

ホスト設定ファイル（任意のファイル名）

項目名	必須	内容
HEADER	×	クライアント証明書の証明書データを証明書発行サーバーへ送信するように設定を行います。 ※ クライアント証明書をオンライン発行する場合に必要

4.7 フォワーダーの HTML 設定の追加

フォワーダーの HTML 設定ファイル (html.conf) に以下の項目を設定します。

項目名	必須	内容
LOGIN_CERT	×	クライアント証明書によるログインを行うログインページを指定します。
LOGIN_ERR_1STCERT	×	クライアント証明書による初回認証済みの場合の初回認証済みエラーページを指定します。
LOGIN_ERR_SERIAL	×	クライアント証明書によるログイン時のシリアルNo. エラーページを指定します。

※ これらの設定はインストールされた時点で設定されています。

4.8 プロセスのリスタート

これまでの設定追加および拡張を行った後に、以下のプロセスをリスタートします。

- ・ IceWall サーバーの Web サーバーインスタンス
- ・ 認証モジュール

注) IceWall サーバーには、サーバー証明書および信頼する CA 局 (Trusted Certificate Authority) の証明書がインストールされ、SSL3.0 で通信できる必要があります。

4.9 ロードバランサーの SSL アクセラレーター機能を使用する場合

ブラウザー—IceWallサーバー間にロードバランサー製品を設置して「SSLアクセラレーター機能」を使用した場合、ロードバランサーにて SSL 接続およびクライアント証明書の確認が行われます。

この構成では、ロードバランサー— IceWall サーバー間の接続は HTTP で行われます。IceWall SSO は、8.0.1(8.0R1) 以降のバージョンで、このような構成でも本オプションが使用できるようになっています。

4.9.1 SSL アクセラレーター機能の前提

SSL アクセラレーター機能を使用した場合、ロードバランサーによりクライアント証明書がデコードされ、証明書基本領域に格納されている情報が HTTP ヘッダーで IceWall

SSO へ送信されるものとし、次の情報が送信されることを前提とします。

- ・ ユーザー ID を含む領域の値（領域名：Subject など）
- ・ シリアル No（領域名：SerialNumer の値）
- ・ 証明書有効期限（領域名：notAfter の値）
- ・ 発行者名（領域名：Issuer の値）

4.9.2 フォワーダーの設定

HTTP ヘッダーで送信されたクライアント証明書の各情報を取得するために、フォワーダーに次の設定を行います。

フォワーダー設定ファイル（dfw.conf）

```
DFW_PROTOCOL=1
CC_DECODE_FLG=0
CC_ENVUID=[ ユーザー ID が取得できる環境変数 ]
CC_ENVSERIAL=[ シリアル No を取得できる環境変数 ]
CC_ENVEXPIRE=[ 証明書有効期限を取得できる環境変数 ]
CC_ENVISSUER=[ 発行者名を取得できる環境変数 ]
```

DFW_PROTOCOL 項目は、ロードバランサーにて SSL アクセラレーター機能を使用している場合でも、フォワーダーが SSL 接続されているものとして動作させるための設定です。

CC_DECODE_FLG 項目は、クライアント証明書の情報を個別に取得することを設定します。この設定を行わなければ、クライアント証明書の各種情報を個別に取得することができません。

CC_ENVUID 項目に設定した環境変数から取得する情報がユーザー ID のみではない場合、CC_UIDKEYS 項目と CC_UIDKEYE 項目を使用して、必要の情報を取得するようにしてください。

また、ロードバランサーの SSL アクセラレーター機能を使用する場合は「4.1 Web サーバーの設定追加」で行う設定は不要になります。

5 UserExit ルーチンの拡張

本オプションを導入した場合、UserExit ルーチンが一部拡張され以下の処理が可能となります。

- ・ログイン処理

- (1) ユーザー ID によるログインか証明書によるログインかどうかを判断できるようになります。
- (2) 強制的に「初回認証済みエラー」を発生させることができます。
- (3) 強制的に「証明書シリアル No エラー」を発生させることができます。

なお、拡張される内容の詳細については「IceWall SSO UserExit ルーチン開発者マニュアル」を参照してください。

6 設定例

認証モジュールの認証 DB カラム情報ファイル (dbattr.conf)、ログカラム設定ファイル (logdbattr.conf) の設定例を以下に示します。

6.1 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (ORACLE 版)

```
#-----
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 15:35 $
#-----
#-----
# [ Authentication Database Table's Column Info ]
#   UID      : UserID.
#   PASSWORD  : Password.
#   PWDEXPDATE : Password Expiration Date.
#   PWDHISTORY : Password History.
#   PCHGOK    : Password Change OK/NG.
#   PCHGDATE  : Password Change Date.
#   PLOGINDATE : Login Date.
#   LLOGINDATE : Last Login Date.
#   FLOGINDATE : Login Failure Date.
#   PWDRETRY  : Password Retry Count.
#   PWDLOCK   : Account Lock ON/OFF.
#   LOGINOK   : Login OK/NG.
#   LOCKDATE  : Account Lock Date.
#   LOGINSTAT : Login Status.
#
# [ for Client Certificate Option Define ]
#   RASERIALNO : RA Serial Number.
#   IWSERIALNO : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT    : Client Certificate Regist/Download Switch.
#   ONLINE    : Certificate Login Status.
#-----
UID=USERID
PASSWORD=PASSWD
PWDEXPDATE=PASSWDEXP
PWDHISTORY=PASSWDHIS
PCHGOK=PASSCHANGE
PCHGDATE=CHGDATE
PLOGINDATE=LOGONDATE
LLOGINDATE=LASTDATE
FLOGINDATE=LOGONFAIL
PWDRETRY=FAILCOUNT
PWDLOCK=LOCKOUT
LOGINOK=LOGONSTOP
LOCKDATE=LOCKDATE
LOGINSTAT=LOGSTATUS
RASERIALNO=RASERIAL
```

```

IWSERIALNO=RASERIAL
CERTEXPDATE=VDATE
GETCERT=CERT
ONLINE=APENABLE

```

6.2 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (LDAP 版)

```

#-----
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 16:02 $
#-----
#-----
# [ Authentication Directory Attributes Info ]
#   UID      : UserID.
#   PASSWORD  : Password.
#   PWDEXPDATE : Password Expiration Date.
#   PWDHISTORY : Password History.
#   PCHGOK    : Password Change OK/NG.
#   PCHGDATE  : Password Change Date.
#   PLOGINDATE : Login Date.
#   LLOGINDATE : Last Login Date.
#   FLOGINDATE : Login Failure Date.
#   PWDRETRY  : Password Retry Count.
#   PWDLOCK   : Account Lock ON/OFF.
#   LOGINOK   : Login OK/NG.
#   LOCKDATE  : Account Lock Date.
#   LOGINSTAT : Login Status.
#
# [ for Client Certificate Option Define ]
#   RASERIALNO : RA Serial Number.
#   IWSERIALNO : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT    : Client Certificate Regist/Download Switch.
#   ONLINE     : Certificate Login Status.
#-----
UID=uid
PASSWORD=userPassword
PWDEXPDATE=passwordExpirationTime
PWDHISTORY=passwordHistory
PCHGOK=mobile
PCHGDATE=manager
PLOGINDATE=pager
LLOGINDATE=displayName
FLOGINDATE=givenName
PWDRETRY=passwordRetryCount
PWDLOCK=employeeNumber
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
RASERIALNO=roomNumber
IWSERIALNO=telexnumber

```

```

CERTEXPDATE=homePhone
ONLINE=registeredAddress
GETCERT=facsimileTelephoneNumber

```

6.3 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (OpenLDAP 版)

```

#-----
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: dbattr.conf $ $Revision: 2 $ $Date: 10/04/21 15:08 $
#-----
#-----
# [ Authentication Directory Attributes Info ]
#   UID      : UserID.
#   PASSWORD  : Password.
#   PWDEXPDATE : Password Expiration Date.
#   PWDHISTORY : Password History.
#   PCHGOK    : Password Change OK/NG.
#   PCHGDATE  : Password Change Date.
#   PLOGINDATE : Login Date.
#   LLOGINDATE : Last Login Date.
#   FLOGINDATE : Login Failure Date.
#   PWDRETRY  : Password Retry Count.
#   PWDLOCK   : Account Lock ON/OFF.
#   LOGINOK   : Login OK/NG.
#   LOCKDATE  : Account Lock Date.
#   LOGINSTAT : Login Status.
#
# [ for Client Certificate Option Define ]
#   RASERIALNO : RA Serial Number.
#   IWSERIALNO : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT    : Client Certificate Regist/Download Switch.
#   ONLINE    : Certificate Login Status.
#-----
UID=uid
PASSWORD=userPassword
PWDEXPDATE=departmentNumber
PWDHISTORY=userPKCS12
PCHGOK=mobile
PCHGDATE=employeeType
PLOGINDATE=pager
LLOGINDATE=displayName
FLOGINDATE=givenName
PWDRETRY=roomNumber
PWDLOCK=employeeNumber
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
RASERIALNO=jpegPhoto
IWSERIALNO=registeredAddress
CERTEXPDATE=homePhone

```

```
GETCERT=facsimileTelephoneNumber
ONLINE=telexNumber
```

6.4 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (NED 版)

```
#-----
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 18:22 $
#-----
#-----
# [ Authentication Directory Attributes Info ]
#   UID      : UserID.
#   PASSWORD  : Password.
#   PWDEXPDATE : Password Expiration Date.
#   PWDHISTORY : Password History.
#   PCHGOK    : Password Change OK/NG.
#   PCHGDATE  : Password Change Date.
#   PLOGINDATE : Login Date.
#   LLOGINDATE : Last Login Date.
#   FLOGINDATE : Login Failure Date.
#   PWDRETRY  : Password Retry Count.
#   PWDLOCK   : Account Lock ON/OFF.
#   LOGINOK   : Login OK/NG.
#   LOCKDATE  : Account Lock Date.
#   LOGINSTAT : Login Status.
#
# [ for Client Certificate Option Define ]
#   RASERIALNO : RA Serial Number.
#   IWSERIALNO : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT    : Client Certificate Regist/Download Switch.
#   ONLINE     : Certificate Login Status.
#-----
UID=cn
PASSWORD=userPassword
PWDEXPDATE=x500UniqueIdentifier
PWDHISTORY=userSMIMECertificate
PCHGOK=mobile
PCHGDATE=jobCode
PLOGINDATE=pager
LLOGINDATE=displayName
FLOGINDATE=givenName
PWDRETRY=workforceID
PWDLOCK=employeeNumber
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
RASERIALNO=masvDefaultRange
IWSERIALNO=telexNumber
CERTEXPDATE=homePhone
ONLINE=registeredAddress
```

```
GETCERT=facsimileTelephoneNumber
```

6.5 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (CSV 版)

```
#-----
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 15:10 $
#-----
#-----
# [ Authentication Database Table's Column Info ]
#   UID      : UserID.
#   PASSWORD  : Password.
#   PWDEXPDATE : Password Expiration Date.
#   PWDHISTORY : Password History.
#   PCHGOK    : Password Change OK/NG.
#   PCHGDATE  : Password Change Date.
#   PLOGINDATE : Login Date.
#   LLOGINDATE : Last Login Date.
#   FLOGINDATE : Login Failure Date.
#   PWDRETRY  : Password Retry Count.
#   PWDLOCK   : Account Lock ON/OFF.
#   LOGINOK   : Login OK/NG.
#   LOCKDATE  : Account Lock Date.
#   LOGINSTAT : Login Status.
#
# [ for Client Certificate Option Define ]
#   RASERIALNO : RA Serial Number.
#   IWSERIALNO : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT    : Client Certificate Regist/Download Switch.
#   ONLINE     : Certificate Login Status.
#-----
UID=USERID
PASSWORD=PASSWD
PWDEXPDATE=PASSWDEXP
PWDHISTORY=PASSWDHIS
PCHGOK=PASSCHANGE
PCHGDATE=CHGDATE
PLOGINDATE=LOGONDATE
LLOGINDATE=LASTDATE
FLOGINDATE=LOGONFAIL
PWDRETRY=FAILCOUNT
PWDLOCK=LOCKOUT
LOGINOK=LOGONSTOP
LOCKDATE=LOCKDATE
LOGINSTAT=LOGSTATUS
RASERIALNO=RASERIAL
IWSERIALNO=BSSERIAL
CERTEXPDATE=VDATE
GETCERT=CERT
ONLINE=APENABLE
```

6.6 認証 DB カラム情報ファイル (dbattr.conf) の設定例 (MySQL 版)

```

#-----
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 16:47 $
#-----
#-----
# [ Authentication Database Table's Column Info ]
#   UID      : UserID.
#   PASSWORD  : Password.
#   PWDEXPDATE : Password Expiration Date.
#   PWDHISTORY : Password History.
#   PCHGOK    : Password Change OK/NG.
#   PCHGDATE  : Password Change Date.
#   PLOGINDATE : Login Date.
#   LLOGINDATE : Last Login Date.
#   FLOGINDATE : Login Failure Date.
#   PWDRETRY  : Password Retry Count.
#   PWDLOCK   : Account Lock ON/OFF.
#   LOGINOK   : Login OK/NG.
#   LOCKDATE  : Account Lock Date.
#   LOGINSTAT : Login Status.
#
# [ for Client Certificate Option Define ]
#   RASERIALNO : RA Serial Number.
#   IWSERIALNO : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT    : Client Certificate Regist/Download Switch.
#   ONLINE     : Certificate Login Status.
#-----
UID=USERID
PASSWORD=PASSWD
PWDEXPDATE=PASSWDEXP
PWDHISTORY=PASSWDHIS
PCHGOK=PASSCHANGE
PCHGDATE=CHGDATE
PLOGINDATE=LOGONDATE
LLOGINDATE=LASTDATE
FLOGINDATE=LOGONFAIL
PWDRETRY=FAILCOUNT
PWDLOCK=LOCKOUT
LOGINOK=LOGONSTOP
LOCKDATE=LOCKDATE
LOGINSTAT=LOGSTATUS
RASERIALNO=RASERIAL
IWSERIALNO=BSSERIAL
CERTEXPDATE=VDATE
GETCERT=CERT
ONLINE=APENABLE

```

6.7 ログカラム設定ファイル (logdbattr.conf) の設定例 (ORACLE 版のみ)

```
#-----  
# IceWall SSO 10.0 Configuration File for Certification Module.  
# $Workfile: logdbattr.conf $ $Revision: 1 $ $Date: 10/03/27 15:35 $  
#-----  
#-----  
# [ Access Log Database Table's Column Info ]  
# NO   : Sequential Numer of Log.  
# TIME : Output Time of Log.  
# UID  : UserID.  
# KIND : Kind of Log Message.  
# RESULT: Proccess Result Code.  
# MSG  : Log Message.  
# CLIP : IP Address of Client.  
#-----  
NO=UKENO  
TIME=UKEDATE  
UID=USERID  
KIND=KIND  
RESULT=RESCODE  
MSG=MESSAGE  
CLIP=IPADDR
```