

Offirio SynergyWare

認証プロキシ for LDAP


設定ガイド

本書は、Offirio SynergyWare 認証プロキシ for LDAP の概要とセットアップ、運用の仕方などを説明しています。
必要に応じてお読みいただき、お役立てください。

マークの意味

！重要 使用上、必ず守っていただきたいことを記載しています。この表示を無視して誤った取り扱いをすると、製品の故障や、動作不良の原因となる可能性があります。

参考 補足説明や参考情報を記載しています。

 関連した内容の参照ページを示しています。

掲載画面

- 本書の画面は実際の画面と多少異なる場合があります。また、OS の違いや使用環境によっても異なる画面となる場合がありますので、ご注意ください。
- 本書に掲載する Windows の画面は、特に指定がない限り Windows Server 2003 の画面を使用しています。

Windows の表記

Microsoft® Windows® 2000 Server Operating System
日本語版

Microsoft® Windows Server® 2003 Operating System
日本語版

本書では、上記の OS (オペレーティングシステム) をそれぞれ「Windows 2000 Server」「Windows Server 2003」と表記しています。また、これらの総称として「Windows」を使用しています。

本製品を日本国外へ持ち出す場合の注意

本製品は日本国内仕様のため、本製品の修理・保守サービスおよび技術サポートなどの対応は、日本国外ではお受けできませんのでご了承ください。また、日本国外ではその国の法律または規制により、本製品を使用できないことがあります。このような国では、本製品を運用した結果罰せられることがあります。当社といたしましては一切責任を負いかねますのでご了承ください。

ご注意

- 本書の内容の一部または全部を無断転載することを禁止します。
- 本書の内容は将来予告なしに変更することがあります。
- 本書の内容にご不明な点や誤り、記載漏れなど、お気付きの点がありましたら弊社までご連絡ください。
- 運用した結果の影響については前項に関わらず責任を負いかねますのでご了承ください。
- 本製品が、本書の記載に従わずに取り扱われたり、不適当に使用されたり、弊社および弊社指定以外の、第三者によって修理や変更されたことなどに起因して生じた障害等の責任は負いかねますのでご了承ください。

商標

Windows

Microsoft、Windows、Windows Server は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Java

Copyright 2007, Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

This product includes code licensed from RSA Security, Inc.

Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

Java および Java 関連の商標およびロゴは、米国 Sun Microsystems, Inc. の米国およびその他の国における登録商標です。

HSQldb

Copyright © 1995-2000 by the Hypersonic SQL Group.

All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 HYPERSONIC SQL GROUP, 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.

This software consists of voluntary contributions made by many individuals on behalf of the Hypersonic SQL Group.

BlowfishJ

Copyright 1997-2005 Markus Hahn

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

JavaService

Copyright © 2000, Alexandria Software Consulting
All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
- Neither name of Alexandria Software Consulting nor the names of the contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDERS 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.

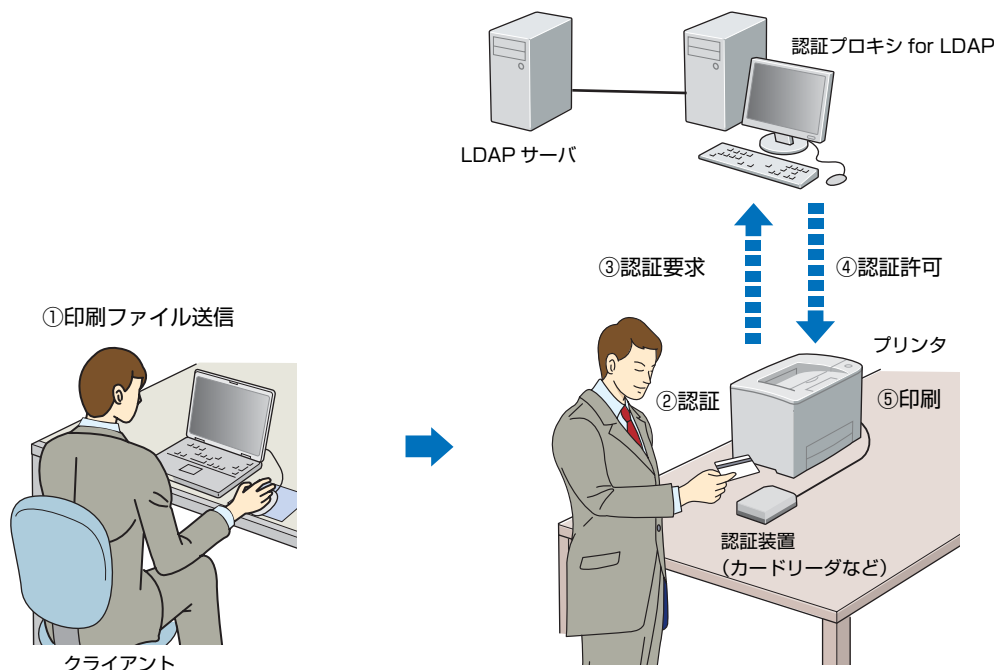
その他の製品名は各社の商標または登録商標です

もくじ

認証プロキシ for LDAP とは.....	5
ソフトウェア構成 ...	6
システム構成 ...	6
システム条件 ...	6
セットアップ	7
セットアップの流れ ...	7
旧バージョンからのアップデートについて ...	7
インストール ...	8
認証プロキシ管理の起動 ...	10
起動用パスワードの登録 ...	10
モジュールの設定 ...	11
マクロの設定 ...	16
マクロチェック ...	17
全体的な動作確認 ...	17
認証プロキシ管理の終了 ...	18
詳細設定	19
起動用パスワードの変更 ...	19
ログの設定 ...	19
モジュールの有効化／無効化 ...	20
接続用パスワードの設定 ...	21
稼働状況の確認.....	22
サービスステータスの確認 ...	22
ログの確認 ...	23
こんなときは	24
ローカルデータベースの更新（CSV ファイルのエク スポート） ...	24
トラブルシューティング ...	25
メッセージとサービスステータス ...	32
マクロの文法 ...	37
カスタム設定 ...	48
Offirio SynergyWare ID Print との連携 ...	49
Offirio SynergyWare 認証プロキシ for MFP との連 携 ...	50
アンインストール ...	52
設定の初期化 ...	52

認証プロキシ for LDAP とは

Offirio SynergyWare 認証プロキシ for LDAP（以下「認証プロキシ for LDAP」）は、LDAP サーバでユーザー管理を統一に行っている利用者に対し、そのユーザー管理形態に応じた認証環境を提供します。



認証プロキシ for LDAP を導入するメリット

- すでに設置されている LDAP サーバのユーザー情報が利用できます。
- プリンタなどの認証処理をログで確認できます。

認証プロキシ for LDAP でできること

- LDAP サーバを参照し、該当ユーザーに関する属性値の取得と取得した属性値に基づく認証ができます。
- ローカルデータベース機能で、LDAP サーバに登録されていない情報を補った認証処理ができます。
- マクロ文で複雑な認証条件を設定することができるため、環境に応じた高度な認証処理ができます。
- 管理ツールで、認証プロキシサービスが参照する設定ファイルや認証用マクロファイルの設定を変更したり、編集したりすることができます。
- 認証プロキシサービスの稼働処理や認証処理をログに保存できます。また、管理ツールで閲覧できます。
- Offirio SynergyWare ID Print と連携して使用できます。
🔗 本書 49 ページ「Offirio SynergyWare ID Print との連携」
- Offirio SynergyWare 認証プロキシ for MFP と連携して使用できます。
🔗 本書 50 ページ「Offirio SynergyWare 認証プロキシ for MFP との連携」

ソフトウェア構成

本製品には、以下のソフトウェアが含まれています。

認証プロキシサービス	認証サービスを提供します。 <ul style="list-style-type: none"> 認証要求を受信して、認証処理を行います。認証処理手順は、認証マクロファイルで設定できます。 認証結果を返信します。 稼動ログ（認証処理結果含む稼動状況）を記録します。 稼動ステータス（正常稼動中／異常履歴あり／エラー発生中）を保持し、管理ツールに送信します。
認証プロキシ管理	認証条件の設定や稼動状況の参照ができます。 <ul style="list-style-type: none"> 認証プロキシサービスに適用する設定ファイルやマクロファイルを編集できます。 認証プロキシサービスの各設定を行います。 認証プロキシサービスの稼動ステータスや稼動ログを閲覧できます。

システム構成

本製品に必要なシステム構成は以下の通りです。

ネットワーク接続	各ネットワーク機器（LDAP サーバ・認証プロキシ for LDAP 搭載用サーバ・プリンタ）が、相互に通信可能な LAN 環境に接続されていること
Network プロトコル	TCP/IP、UDP/IP
LAN 速度	10Mbps 以上
LDAP サーバ	LDAP v3 準拠
その他のハードウェア	認証プロキシ for LDAP 搭載用サーバ
認証要求の同時処理数	20 まで
認証要求元の数	200 台まで



認証要求数と認証要求元の数、認証処理の内容（マクロの行数や使用する認証モジュールの種類など）によって少なくなることがあります。

システム条件

認証プロキシサービスおよび認証プロキシ管理を搭載するサーバのシステム条件は以下の通りです（2008年3月現在）。

対象 OS	<ul style="list-style-type: none"> Windows 2000 Server Windows Server 2003（32bit(x86) 版）
-------	--

本ソフトウェアはネットワーク環境で使用するため、サーバソフトウェアとしての使用を許諾されていない OS にサーバ用ソフトウェアをインストールして使用すると、Microsoft 社の使用許諾契約に違反する場合があります。詳細は、OS の使用許諾契約をご確認ください。

CPU	Intel® Pentium® III 1.2GHz 以上
RAM	768MB 以上
ハードディスク	30MB 以上
表示装置	解像度 800 × 600 以上のモニタ
インターフェイス	Ethernet × 1、USB/PS2 インターフェイス × 2（キーボード、マウス用）

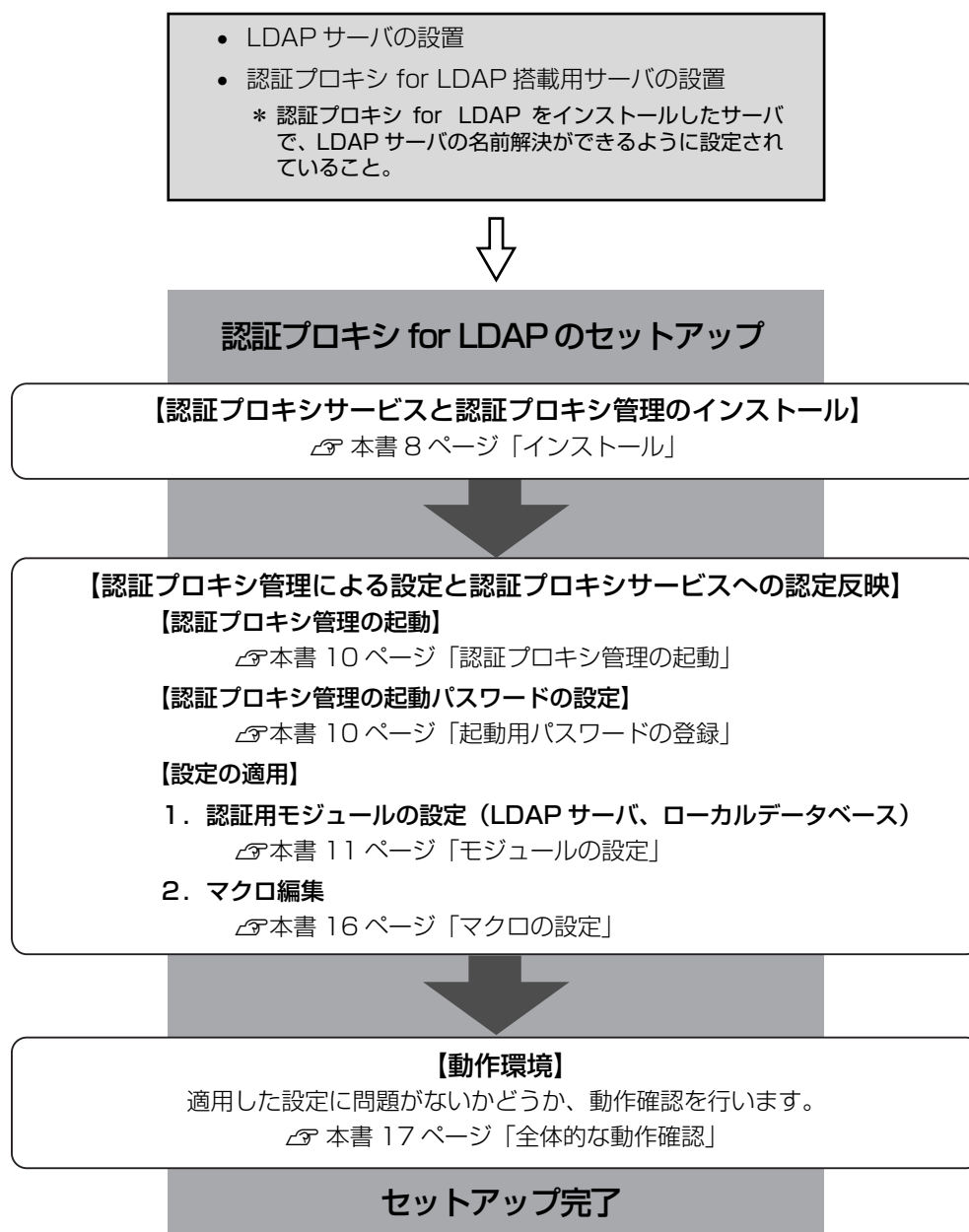


ハードディスクの容量は、ローカルデータベースへのユーザー情報登録件数に依存します。さらに多くの容量を必要とする場合があります。

セットアップ

セットアップの流れ

本製品は、必要なサーバが設置された環境に対してセットアップを行います。セットアップの流れは以下の通りです。



旧バージョンからのアップデートについて

本ソフトウェアは、下記のソフトウェアからのアップデートができます。

製品名 : Offirio SynergyWare 認証プロキシ (Windows に表示される名称は「EpsonNet 認証プロキシ」)

製品型番 : SWNPV1

バージョン : 1.0x (x には a、b、c などのアルファベットが入ります)

旧バージョンのソフトウェアがインストールされている環境に本ソフトウェアをインストールすると、過去の設定情報を保持したままアップデートできます。

インストール

認証プロキシサービスと認証プロキシ管理をインストールします。

手順は Windows Server 2003 を例に説明しています。

1 ソフトウェアCD-ROMをCD-ROMドライブにセットします。

セットアップ準備中の画面が表示されます。

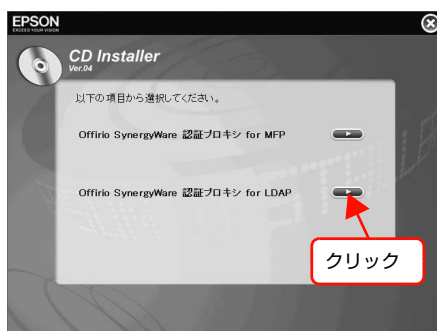
参考

画面が表示されないときは、[マイコンピュータ] - [CD-ROM ドライブ] アイコンの順にクリックして [EPSetup.exe] アイコンをダブルクリックします。



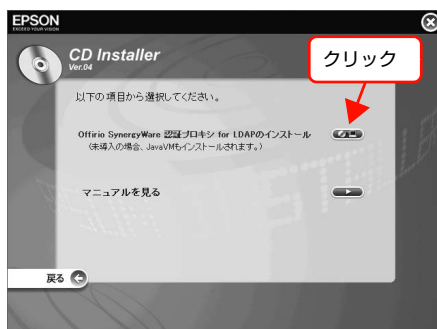
ダブルクリック

2 [Offrio SynergyWare 認証プロキシ for LDAP] の [] をクリックします。



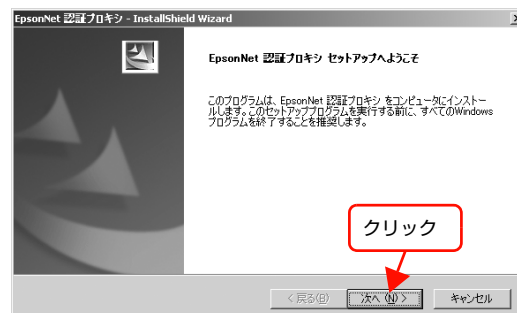
クリック

3 [Offrio SynergyWare 認証プロキシ for LDAP のインストール] の [] をクリックします。



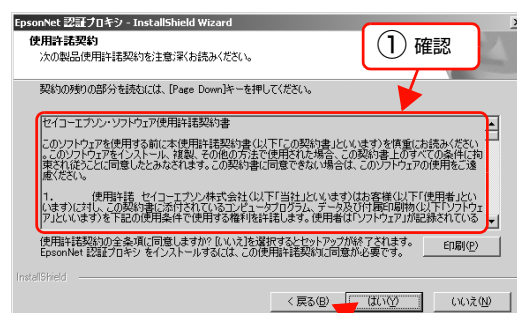
クリック

4 [次へ] をクリックします。



クリック

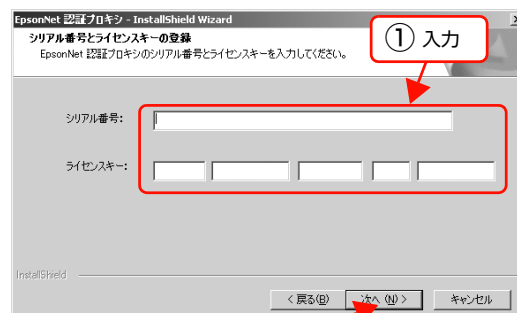
5 内容を確認して [はい] をクリックします。



① 確認

② クリック

6 パッケージに記載のシリアル番号とライセンスキーを入力して [次へ] をクリックします。



① 入力

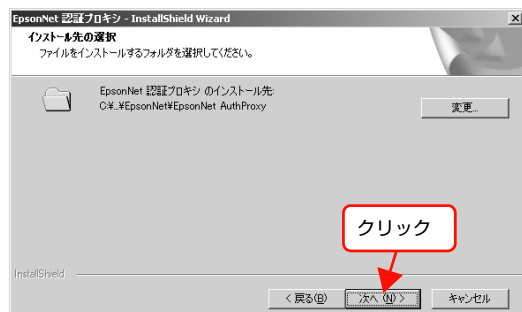
② クリック

参考

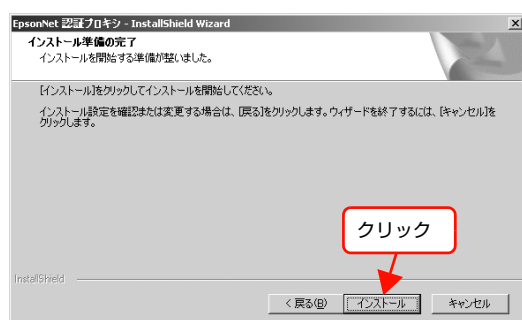
本製品は、ネットワーク上でライセンス管理を行っています。同一ライセンスキーで動作する別の認証プロキシサービスを発見すると、後からインストールされた認証プロキシサービスは認証処理機能を停止します。認証処理結果は常に「認証サーバ処理エラー」となります。

また、稼働ログには次のように表示されます。
System Duplicate license has been detected. :
コンピュータの IP アドレス

- 7** インストール先を確認して [次へ] をクリックします。
インストール先を変更するときは、[変更] をクリックしてください。



- 8** [インストール] をクリックします。



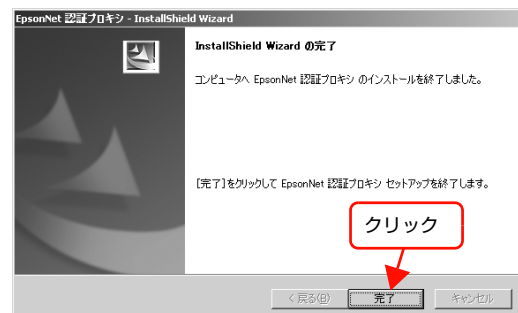
- 9** Java に関するメッセージが表示されたら、[OK] をクリックします。
- 「適切な Version の Java が見つかりません。Java をインストールします。」と表示されたときは、[OK] をクリックし、画面に従って Java をインストールしてください。



- 「適切な Version の Java がインストールされていることを確認しました。」と表示されたときは、[OK] をクリックします。



- 10** [完了] をクリックします。



以上で終了です。

参考

認証プロキシサービスの起動について

- 認証プロキシサービスは、インストール時に Windows のサービスとして登録、開始されます。そのため、認証プロキシサービスの起動に必要な作業はありません。
- 管理者が認証プロキシサービスを停止した場合は、以下の手順で起動してください。
 - [スタート] - [プログラム] または [すべてのプログラム] - [管理ツール] - [サービス] の順にクリックします。
 - [EpsonNet Authentication Proxy Service] をダブルクリックして [開始] をクリックします。

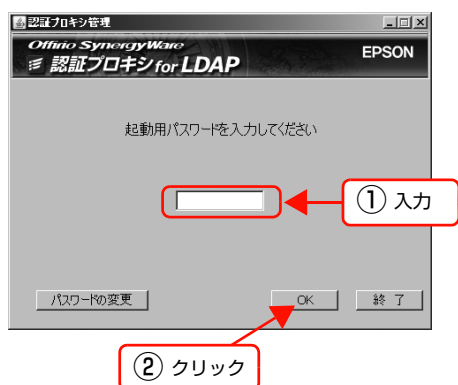
認証プロキシ管理の起動

認証プロキシサービスの各設定は、認証プロキシ管理で行います。

以下の手順で認証プロキシ管理を起動します。

- 1 [スタート] - [プログラム] または [すべてのプログラム] - [EpsonNet] - [認証プロキシ] - [認証プロキシ管理] の順にクリックします。
初めて起動したときは、起動用パスワードを登録します。
📖 本書 10 ページ「起動用パスワードの登録」

- 2 起動用パスワードを入力して [OK] をクリックします。

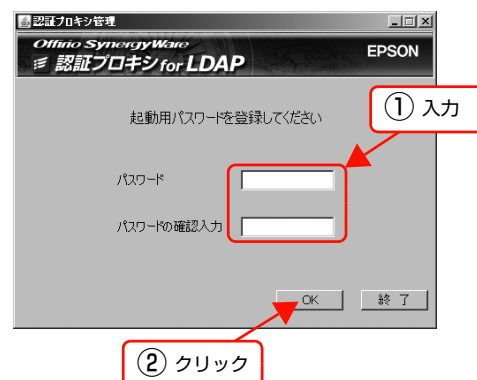


以上で終了です。

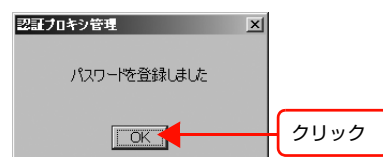
起動用パスワードの登録

認証プロキシ管理をインストール後、初めて起動したときは、起動用パスワードを登録します。

- 1 [パスワード] と [パスワードの確認入力] をそれぞれ入力して、[OK] をクリックします。
英数字それぞれ 1 字以上含む半角英数、5 文字以上 10 文字以内で入力してください。大文字、小文字は区別して認識されます。記号は使用できません。



- 2 [OK] をクリックします。



以上で終了です。

参考

- 起動用パスワードは変更できます。
📖 本書 19 ページ「起動用パスワードの変更」
- 起動用パスワードを忘れると、認証プロキシ管理は起動できません。再インストールして、パスワードを登録し直してください。認証サービスは動作を継続しています。

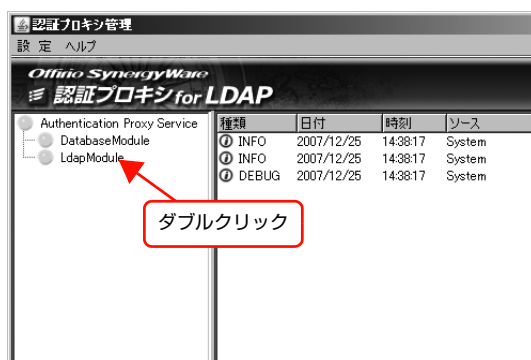
モジュールの設定

各認証用モジュールに接続するための設定を行います。

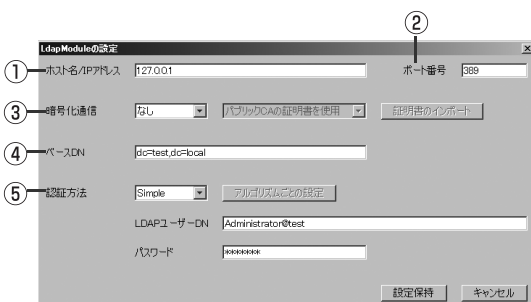
LDAP モジュール

LDAP サーバに接続するための設定を行います。

- 1 **[LdapModule] をダブルクリックします。**
[LdapModule] を右クリックして [モジュール設定] をクリックしても、設定画面が開けます。



- 2 **各設定を指定します。**



①ホスト名 /IP アドレス

LDAP サーバのホスト名、または IP アドレスを入力します。

ホスト名は FQDN 形式で入力してください。FQDN 形式で入力しないと、検索されないことがあります。半角スペース区切りで複数の LDAP サーバが指定できます。

初期設定：127.0.0.1

②ポート番号

認証データを通信するポート番号を入力します。LDAP サーバと同じ番号を入力してください。

- SSL 通信を使用する場合は、非暗号化通信のポート番号とは別のポート番号を指定します。
- StartTLS 通信を使用する場合は、非暗号化通信のポート番号を指定します。

初期設定：389（入力範囲：1～65535）

③暗号化通信

暗号化通信の選択をします。

なし / SSL / StartTLS

初期設定：なし

SSL または StartTLS を選択すると、サーバ証明書または CA 証明書のインポートが必要になる場合があります。

クライアント認証はサポートしていません。

以下を参照して設定してください。

📖 本書 12 ページ「暗号化通信 (SSL / StartTLS)」

④ベース DN

LDAP ツリー内における参照箇所を DN 形式で指定します。

⑤認証方法

LDAP サーバにアクセスするときの認証方式を選択します。LDAP サーバの環境の認証方法を選択してください。下行の認証方法ほどセキュリティ強度が高くなります。

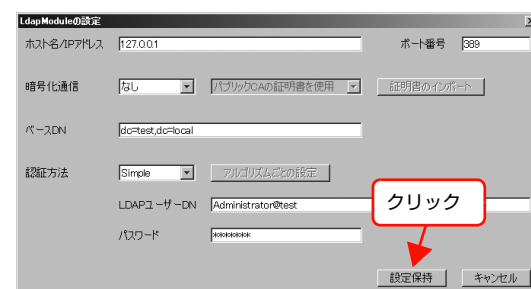
anonymous	ID とパスワードを必要としない認証形式です。匿名でアクセスします。
Simple	ID とパスワードを暗号化しないで送付します。
Cram-MD5	ID とパスワードを簡単なダイジェスト認証で送付します。
Digest-MD5	一般的な LDAP サーバで使用可能な認証形式です。ID とパスワードをダイジェスト認証で送付します。
Kerberos V5	Kerberos 認証を行います。krb5.conf ファイルにて KDC サーバの指定が必要です。

初期設定：Simple

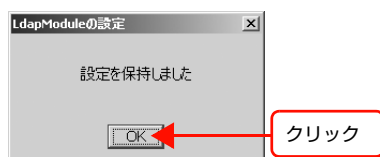
認証方法によって設定方法が異なります。以下を参照して設定してください。

📖 本書 13 ページ「認証方法の設定」

- 3 **各設定を指定した後に、[設定保持] をクリックします。**



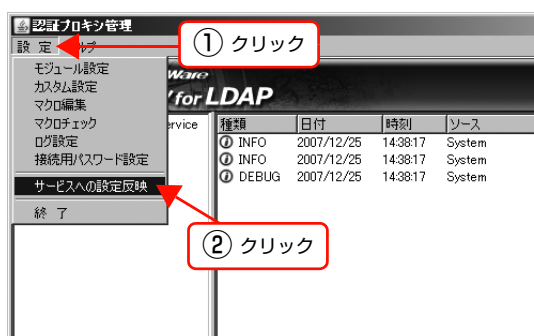
4 [OK] をクリックします。



「LdapModule の設定」画面が閉じます。

5 [設定] - [サービスへの設定反映] の順にクリックします。

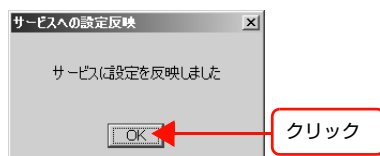
保持中の設定が、認証プロキシサービスに反映されます。



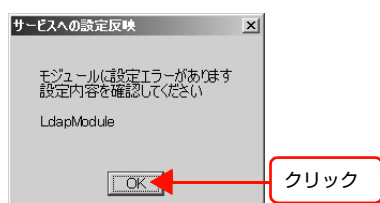
処理中画面が表示されます。

設定反映処理が終了すると、「サービスに設定を反映しました」と表示されます。

6 [OK] をクリックします。

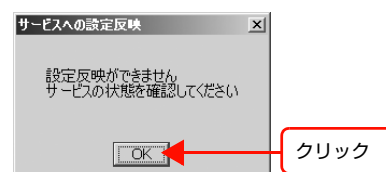


設定に不適切な内容があると設定エラー画面が表示され、設定は反映されません。設定内容を確認し、正しく設定し直してください。



次の画面が表示された場合は、通信エラーが発生しています。認証プロキシサービスのステータスや認証プロキシサービスが Windows のサービスとして開始しているかどうか確認してください。確認の仕方は以下を参照してください。

本書 32 ページ「メッセージとサービスステータス」



以上で終了です。

参考

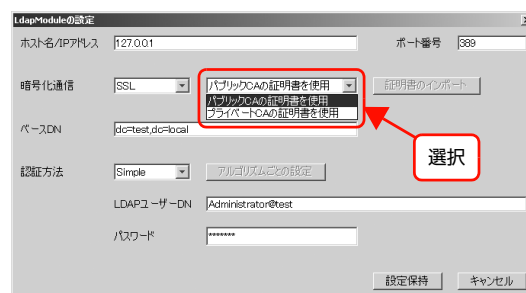
- 「サービスへの設定反映」を行わないと、認証プロキシ管理で指定した各設定は認証プロキシサービスに適用されません。設定を変更する場合は、必ず「サービスへの設定反映」を行ってください。
- 「サービスへの設定反映」を行うと、すべての認証プロキシ管理の設定が認証プロキシサービスに適用されます。各設定をすべて指定し終えてから「サービスへの設定反映」を行っても適用できますが、設定を変更することに「サービスへの設定反映」を行うことをお勧めします。この操作で、その都度設定エラーが確認できます。

暗号化通信(SSL / StartTLS)

SSL または StartTLS を選択した場合は、パブリック CA (公的な認証機関) が発行した証明書を使用するか、プライベート CA 発行の証明書を使用するかを指定します。

プライベート CA 発行の証明書を使用する場合は、CA 証明書またはサーバ証明書をインポートする必要があります。X.509DER 形式、X.509PEM 形式の CA 証明書またはサーバ証明書のファイルをインポートしてください。

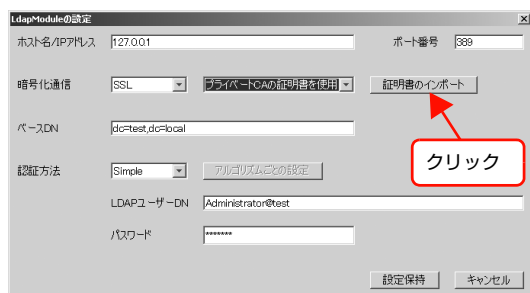
1 [パブリック CA の証明書を使用] または [プライベート CA の証明書を使用] を選択します。



「パブリック CA の証明書を使用」を選択した場合は、JRE (Java Runtime Environment) に標準添付されるパブリック CA の証明書が使用されます。「設定保持」をクリックして、「サービスへの設定反映」を行ってください。

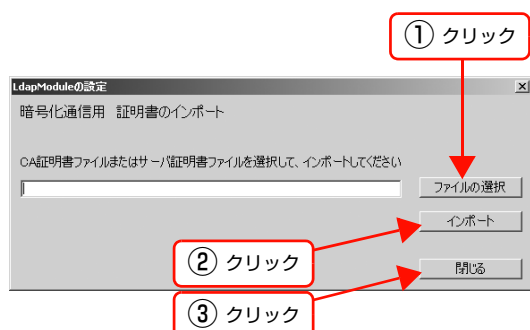
「プライベート CA の証明書を使用」を選択した場合は、手順 2 へ進みます。

2 「証明書のインポート」をクリックします。



「暗号化通信 証明書のインポート」画面が表示されます。

3 ファイルを選択してインポートします。



- ① 「ファイルの選択」をクリックしてファイルを選択します。
ファイルのパスが入力されます。
- ② 「インポート」をクリックします。
インストールディレクトリに [cacerts] ファイルが生成され、その中に証明書がインポートされます。
- ③ 「閉じる」をクリックします。
「LdapModule の設定」画面に戻ります。

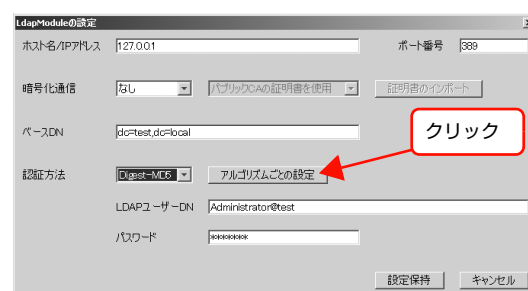
以上で終了です。

認証方法の設定

認証方法によって、アルゴリズムごとの設定、LDAP ユーザー DN、パスワードの設定が必要になります。下表を参照して、「必要」と記載されている項目を設定してください。

認証方法	アルゴリズムごとの設定	LDAP ユーザー DN、パスワード
Anonymous	不要	不要
Simple	不要	必要
Cram-MD5	不要	必要
Digest-MD5	必要	必要
Kerberos V5	必要	必要

1 Digest-MD5、Kerberos V5 を選択した場合は、[アルゴリズムごとの設定]をクリックします。

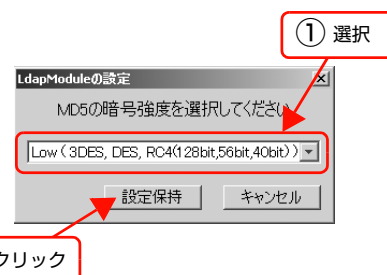


それぞれの設定画面が表示されます。

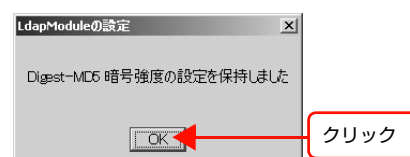
Digest-MD5 の場合

暗号強度を選択します。

- ① 暗号強度を選択します。
Low / Medium / High
(初期設定：Low)
- ② 「設定保持」をクリックします。



- ③ 「OK」をクリックします。



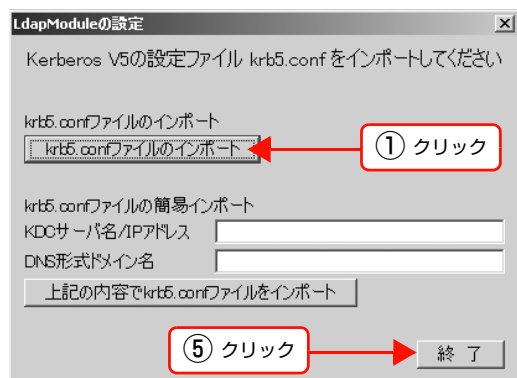
「LdapModule の設定」画面に戻ります。

Kerberos V5 の場合

Kerberos 認証サーバ (KDC サーバ) の指定に関する krb5.conf ファイルをインポートします。

• krb5.conf ファイルのインポート

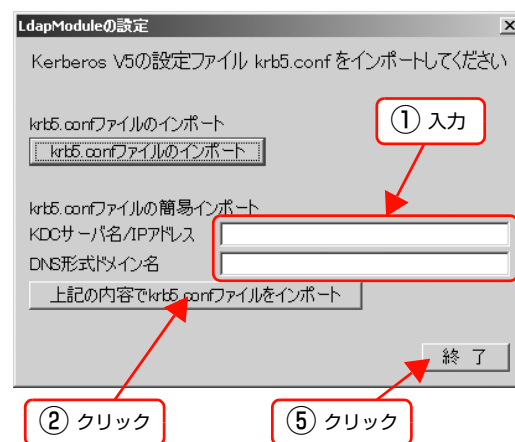
KDC サーバ向けにあらかじめ用意されているファイルを取り込む場合に設定します。



- ① [krb5.conf ファイルのインポート] をクリックします。
ファイル選択画面が表示されます。
- ② インポートする krb5.conf ファイルを選択して [OK] をクリックします。
「krb5.confファイルが存在します ファイルを上書きしてインポートしますか?」と表示されます。
- ③ [OK] をクリックします。
「krb5.conf ファイルをインポートしました」と表示されます。
- ④ [OK] をクリックします。
「krb5.conf ファイルのインポート」画面に戻ります。
- ⑤ [終了] をクリックします。
「LdapModule の設定」画面に戻ります。

• krb5.conf ファイルの簡易インポート

簡易的に krb5.conf ファイルを生成して、そのファイルをインポートする場合に設定します。

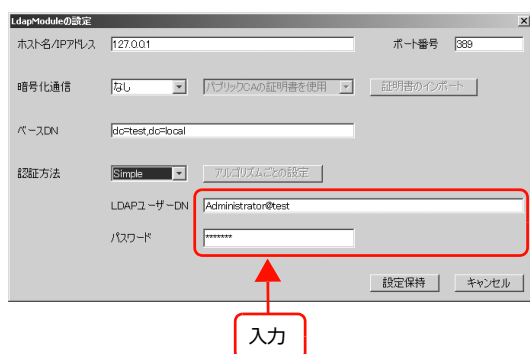


- ① KDC サーバ名 /IP アドレスと DNS 形式ドメイン名を入力します。
例 : KDC サーバ : 192.168.100.100
(IP アドレスでも FQDN 形式でも可)
DNS 形式ドメイン名 : test.local
- ② [上記の内容で krb5.conf ファイルをインポート] をクリックします。
「以下の内容でkrb5.confファイルをインポートしますか?」と表示されます。
- ③ [OK] をクリックします。
「krb5.confファイルが存在します ファイルを上書きしてインポートしますか?」と表示されます。
- ④ [OK] をクリックします。
「krb5.conf ファイルをインポートしました」と表示されます。
- ⑤ [OK] をクリックします。
「krb5.conf ファイルのインポート」画面に戻ります。
- ⑥ [終了] をクリックします。
「LdapModule の設定」画面に戻ります。

参考

「krb5.conf ファイルのインポート」と「krb5.conf ファイルの簡易インポート」の両方を実行したときは、最後に実行したファイルがインポートされます。

- 2 Simple、Cram-MD5、Digest-MD5、Kerberos V5 を選択した場合は、LDAP ユーザー DN、パスワードをそれぞれ入力します。



以上で終了です。

ローカルデータベースモジュール

- ローカルデータベースは簡易的な機能のため、運用中のデータベース更新ができません。認証プロキシ管理でデータベースのインポートを実行したときのみ更新できます。
- 認証処理の際は Read アクセスのみ可能です。データベースの情報は固定的な情報として参照できます。

ローカルデータベースモジュールの設定

CSV ファイルをインポートして、ローカルデータベースを登録します。

参考

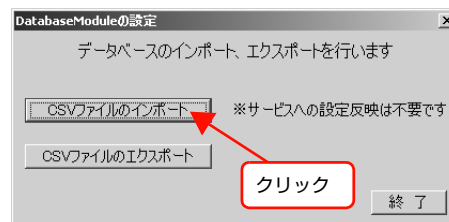
CSV ファイルに記載するデータには規定があります。
 本書 16 ページ「CSV ファイルについて」

- 1 [DatabaseModule] をダブルクリックします。

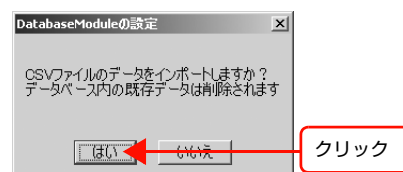
[DatabaseModule] を右クリックして [モジュール設定] をクリックしても、設定画面が開けます。



- 2 [CSV ファイルのインポート] をクリックします。



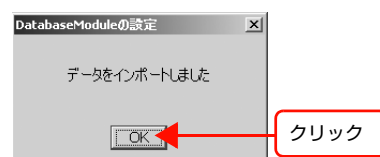
- 3 [はい] をクリックします。



- 4 インポートする CSV ファイルを選択して [OK] をクリックします。

処理中画面が表示された後、インポートした CSV ファイルがローカルデータベースに反映されます。

- 5 [OK] をクリックします。



- 6 [終了] をクリックして「DatabaseModule の設定」画面を閉じます。

ここでは、「サービスへの設定反映」は必要ありません。

以上で終了です。

CSV ファイルについて

CSV ファイルに記載するデータは、次の規定に従ってください。

- ローカルデータベースにインポートできるファイルサイズは5 MB までです。
- 列は A ～ J 列(10 列)まで、1 列 128 バイト相当までです。
- 各列に対し、列名を付ける必要はありません。
- 1 列目がデータベースの A 列、2 列目: B 列、3 列目: C 列、… 10 列目: J 列として格納されます。
- ローカルデータベースにインポートできる最大行数は 2 の 63 乗 - 1 行です。認証プロキシサービスのインストール先ハードウェアや OS などの許容量に応じた行数のデータがインポートできます。
- 行を特定するための情報となるプライマリキーは、CSV ファイルで指定する必要はありません。データベースエンジン側で用意され、プライマリキーに対して各行に連番が付けられます。
- CSV ファイル中の要素に「" (半角ダブルクォート)」や「, (半角コンマ)」が必要な場合は、それぞれ、「""」、 「,"」としてください。
- 改行した時点で次の列となります。

参考

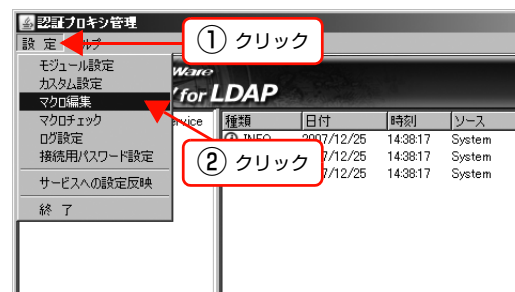
ローカルデータベースは、CSV ファイルにエクスポートして編集し、再度インポートすることで更新できます。

本書 24 ページ「ローカルデータベースの更新 (CSV ファイルのエクスポート)」

マクロの設定

認証処理内容をマクロ文で記述することにより設定します。

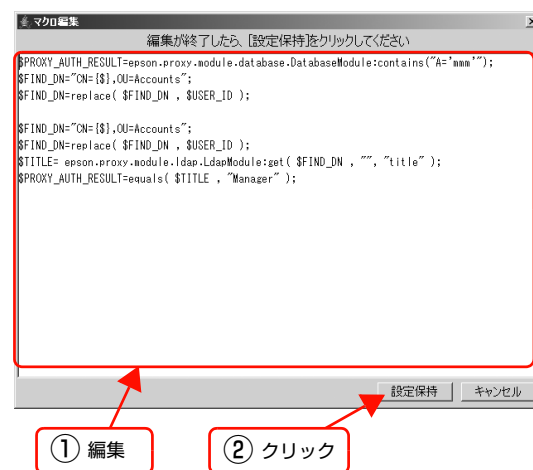
- 1 [設定] - [マクロ編集] の順にクリックします。



- 2 テキストを編集して [設定保持] をクリックします。

マクロは、本製品独自の文法で記載します。記述方法は、以下を参照してください。

本書 37 ページ「マクロの文法」



- 3 [OK] をクリックします。



「マクロ編集」画面が閉じます。

- 4 「サービスへの設定反映」を行います。

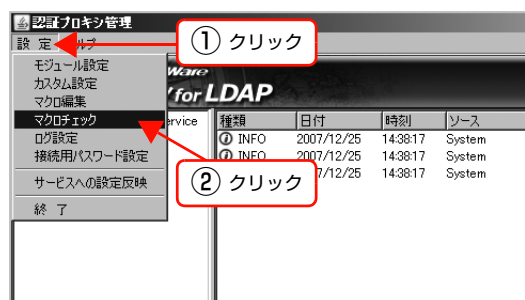
12 ページの手順 5 ～ 6 と同様の手順で、設定を認証プロキシサービスに反映します。

以上で終了です。

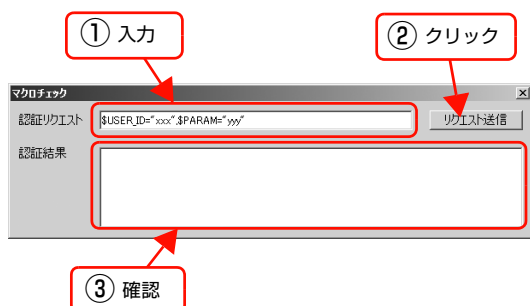
マクロチェック

認証プロキシサービスが管理者の想定通りの動作をするか、動作中の認証プロキシサービスにリクエストを送って確認します。

- 1 [設定] - [マクロチェック] の順にクリックします。



- 2 認証リクエストを入力して [リクエスト送信] をクリックします。
「認証リクエスト」に、変数 = ' 値 1', 変数 = ' 値 2'……と入力します。



参考

- ここで入力された変数とその値は、マクロで規定された認証処理で参照されます。
- \$USER_ID は、ユーザーの識別情報を示す変数です。

[リクエスト送信] をクリックすると、「認証リクエスト」で送信した内容に対する認証処理結果が以下のように表示されます。

認証された場合：

\$PROXY_AUTH_RESULT="TRUE"

認証されない場合：

\$PROXY_AUTH_RESULT="FALSE"

認証される場合とされない場合を想定した認証リクエストを実行し、それぞれ正しい結果が表示されることを確認してください。

- 3 マクロチェックが終わったら、画面右上の [×] をクリックしてマクロチェック画面を閉じます。

以上で終了です。

全体的な動作確認

適用した設定に問題がないかどうか、動作確認を行います。

- 1 サービスステータスにエラーがないか確認します。
本書 22 ページ「サービスステータスの確認」

- 2 認証操作を行います。

- 3 稼動ログを参照して想定通りの認証結果になっていることを確認します。

認証された場合：

「PROXY_AUTH_RESULT=TRUE」と表示されます。

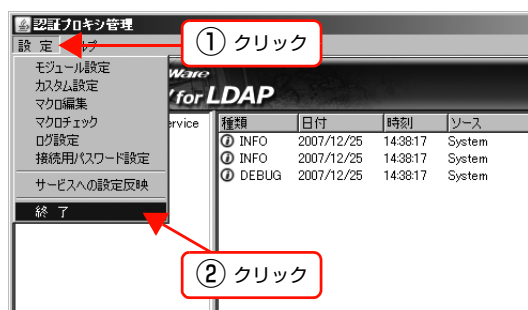
認証されない場合：

「PROXY_AUTH_RESULT=FALSE」と表示されます。

以上で終了です。

認証プロキシ管理の終了

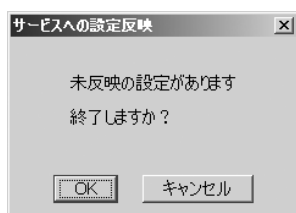
「設定」 - 「終了」の順にクリックして、認証プロキシ管理を終了します。画面右上の「×」をクリックしても終了できます。



参考

未反映の設定があったときは

「サービスへの設定反映」が行われていない設定があると次のダイアログが表示されます。



- 未反映の設定を破棄して認証プロキシ管理を終了する場合は、[OK] をクリックします。
- 認証プロキシ管理の終了を中止する場合は、[キャンセル] をクリックします。

詳細設定

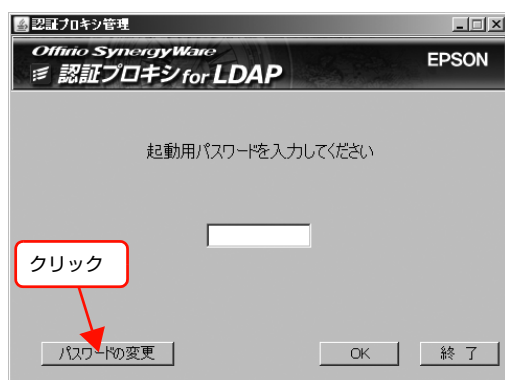
認証プロキシ管理の以下の設定について説明します。

- 起動用パスワードの変更：起動用パスワードは変更できます。
- ログの設定：稼動ログの表示の仕方やログ削除を設定できます。
- モジュールの有効／無効：認証用モジュールごとに有効にするか、無効にするかが設定できます。
- 接続用パスワードの設定：他のソフトウェアと連携するためのパスワードを設定します。

起動用パスワードの変更

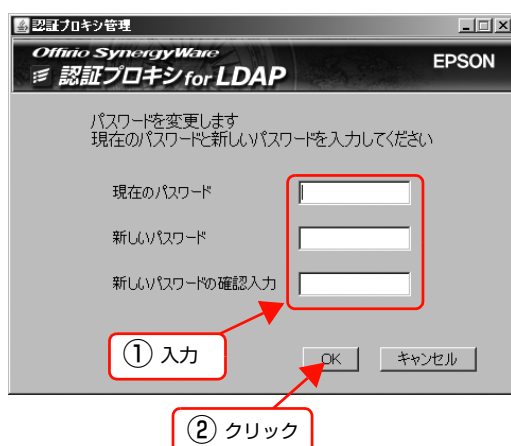
- 1 パスワード入力画面で、[パスワードの変更] をクリックします。

本書 10 ページ「認証プロキシ管理の起動」

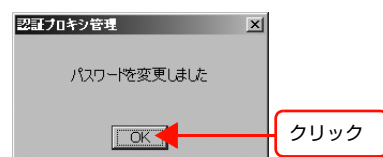


- 2 [現在のパスワード]、[新しいパスワード]、[新しいパスワードの確認入力] をそれぞれ入力して [OK] をクリックします。

英字数字それぞれ 1 字以上含む半角英数、5 文字以上 10 文字以内で入力してください。大文字、小文字は区別して認識されます。記号は使用できません。



- 3 [OK] をクリックします。

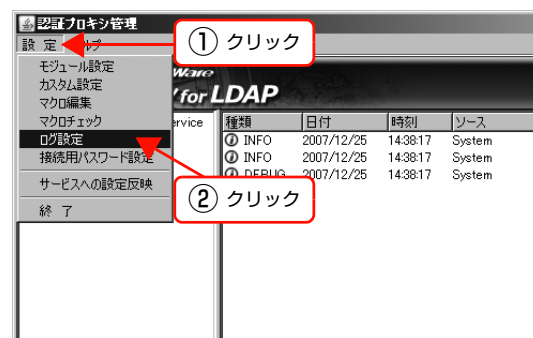


パスワードの変更が完了すると、パスワード入力画面が表示されます。

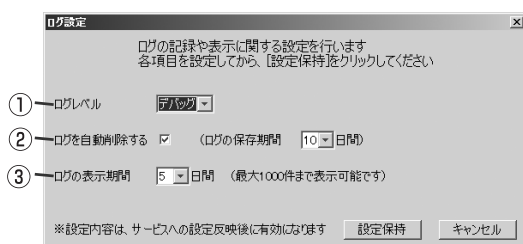
以上で終了です。

ログの設定

- 1 [設定] - [ログ設定] の順にクリックします。



- 2 「ログレベル」、「ログの表示」、「ログを自動削除する」をそれぞれ選択して「設定保持」をクリックします。



①ログレベル

稼動ログの取得レベルを選択します。

簡易	基本的な稼動履歴、およびエラー情報を記録します。
詳細	「簡易」に加えて、認証リクエストの内容や認証処理結果を記録します。
デバッグ	「詳細」に加えて、設定やマクロの動作確認を行うために必要な稼動情報を記録します。

初期設定：デバッグ

②ログを自動削除する

ログを自動削除するかどうかを設定します。チェックすると自動削除します。自動削除する場合は、何日前までのログを保持するかを設定をします。

1日／3日／5日／10日／15日／30日

初期設定：自動削除する、10日

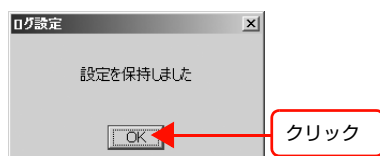
③ログの表示期間

何日前までのログを表示するかを選択します。

1日／3日／5日／10日／15日／30日

初期設定：5日

- 3 「OK」をクリックします。



「ログ設定」画面が閉じます。

- 4 「サービスへの設定反映」を行います。

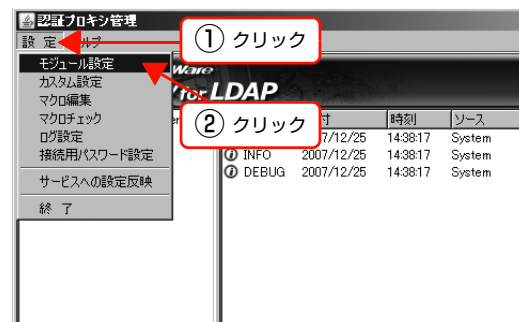
12 ページの手順 5 ～ 6 と同様の手順で、設定を認証プロキシサービスに反映します。

以上で終了です。

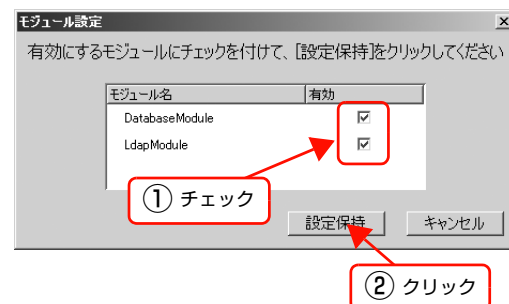
モジュールの有効化／無効化

初期設定では、LDAP モジュールとローカルデータベースモジュールは有効になっています。

- 1 「設定」 - 「モジュール設定」の順にクリックします。



- 2 無効化する認証用モジュールの有効のチェックを外して「設定保持」をクリックします。有効にする場合は、「有効」をチェックします。



- 3 「OK」をクリックします。



「ログ設定」画面が閉じます。

- 4 「サービスへの設定反映」を行います。

12 ページの手順 5 ～ 6 と同様の手順で、設定を認証プロキシサービスに反映します。

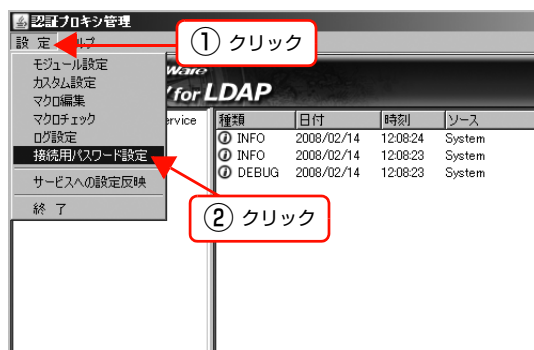
以上で終了です。

接続用パスワードの設定

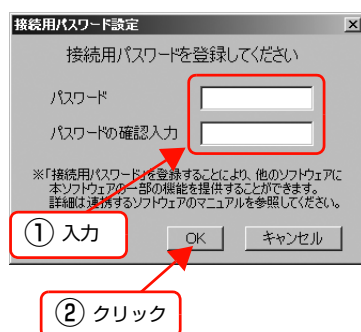
接続用パスワードを登録することにより、他のソフトウェアに本ソフトウェアの一部の機能を提供することができます。 詳細は連携するソフトウェアのマニュアルを参照してください。

パスワードの設定方法は以下の通りです。

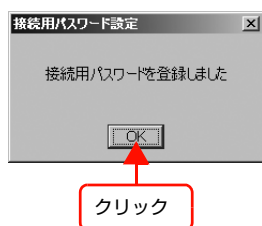
- 1 【設定】 - 【接続用パスワード設定】 の順にクリックします。



- 2 パスワードを入力して、[OK] をクリックします。



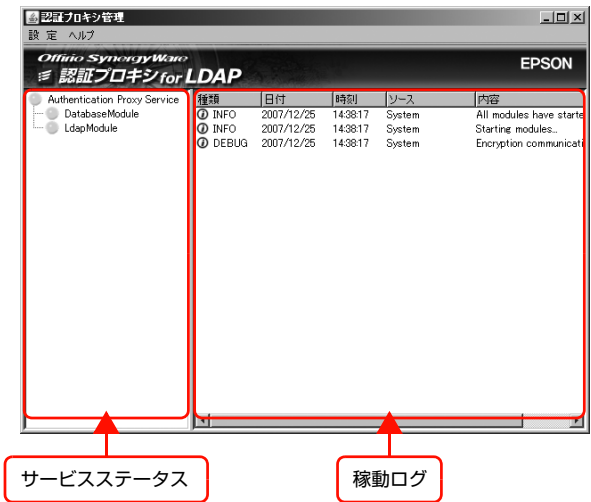
- 3 【OK】 をクリックします。



以上で終了です。

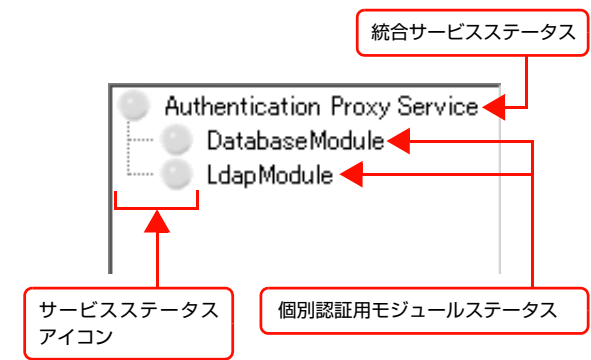
稼動状況の確認

認証プロキシ管理を起動して表示されるメイン画面で、各認証用モジュールのサービスステータスと認証プロキシサービスの稼動ログが確認できます。



サービスステータスの確認

サービスステータスの表示は、「統合サービスステータス」と「個別認証用モジュールステータス」の2つがあり、それぞれにサービスステータスアイコンがあります。

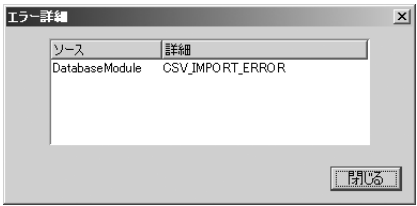


種類	内容
統合サービスステータス	次の2つのステータスを統合して示します。 <ul style="list-style-type: none">認証マクロ処理機能などの基本処理機能に関するステータス個別認証用モジュールステータス
個別認証用モジュールステータス	認証用モジュールごとの個別ステータスを示します。

サービスステータスアイコンの色で、ステータス状態が確認できます。色の意味は以下の通りです。

表示色	ステータス状態	内容
緑	正常稼動中	正常に稼動しています。
黄	異常履歴あり	現在は正常に稼動していますが、一時的な通信失敗など突発的な原因により認証処理が正常に終了しなかった履歴があります。
赤	エラー発生中	設定上の誤りがある、通信待ち受けポートが利用できないなど、継続的に認証処理ができない状態になっています。

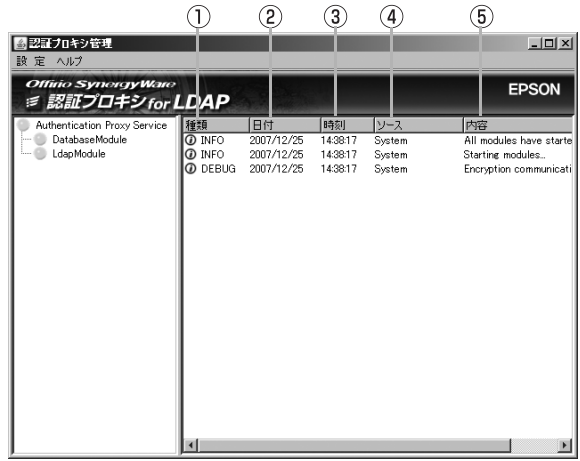
表示色が黄または赤のときにサービスステータスアイコンを右クリックして「エラー確認」をクリックすると、詳細を確認できます。



サービスステータスの詳細は、以下を参照してください。
本書 32 ページ「メッセージとサービスステータス」

ログの確認

稼動ログは、5 秒おきに更新されます。エラーは赤字で表示されます。最新の 1000 件までのログが表示されます。



ログの内容は以下の通りです。

① 種類

ERROR	エラー情報（エラー発生の記録）
INFO	<ul style="list-style-type: none">認証プロキシサービスの基本的な動作の記録認証要求の受信と認証結果の送信の記録
DEBUG	デバッグ情報（設定、マクロの動作確認を行うために必要な稼動情報に関する記録）

② 日付

そのログが書き込まれた日付

③ 時刻

そのログが書き込まれた時刻

④ ソース

ログを出力した認証用モジュールまたはマクロ (System、LdapModule、DatabaseModule 等)

⑤ 内容

処理結果やイベント情報など

参考

- 「種類」の表示内容（ログレベル）は指定できます。
📖 本書 19 ページ「ログの設定」
- 表示するログの日数、ログ自動削除および保持しておく期間は変更できます。
📖 本書 19 ページ「ログの設定」
- ログファイルはインストールディレクトリにあり、テキストエディタで開けます。また、任意のフォルダにコピーして保存することもできます。画面に表示されない古いログを参照したいときは、ログファイルを直接参照してください。

こんなときは

その他の運用方法や困ったときの対処方法などを説明します。

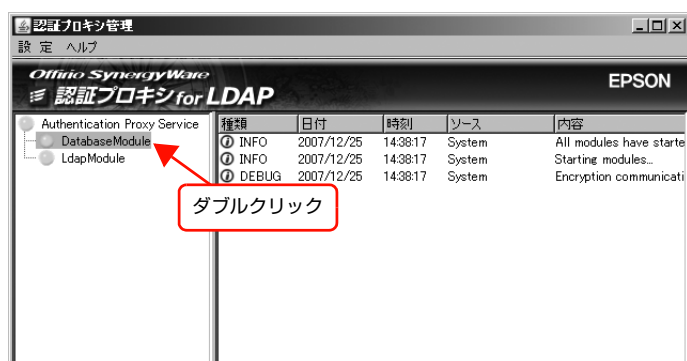
ローカルデータベースの更新(CSV ファイルのエクスポート)

CSV ファイルをエクスポートできます。エクスポートした CSV ファイルを編集して再度インポートすると、ローカルデータベースを更新できます。

1

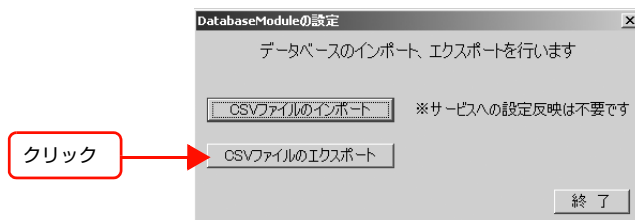
【DatabaseModule】をダブルクリックします。

【DatabaseModule】を右クリックして【モジュール設定】をクリックしても、設定画面が開けます。



2

【CSV ファイルのエクスポート】をクリックします。



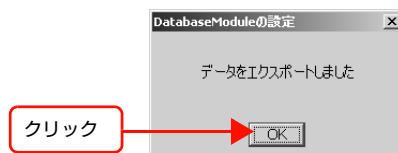
3

ファイルの出力先とファイル名を指定して【OK】をクリックします。

CSV ファイルがエクスポートされます。

4

【OK】をクリックします。



5

【終了】をクリックして「DatabaseModule の設定」画面を閉じます。

6

エクスポートされた CSV ファイルを、テキストエディタ等で編集します。

7






編集した CSV ファイルをインポートします。

📖 本書 15 ページ「ローカルデータベースモジュールの設定」






以上で終了です。

トラブルシューティング

トラブルが発生したときは、下記の対処方法に従って操作してください。

	トラブル状態	対処方法
サービス 全般	認証プロキシ管理を起動すると、「サービスが起動していません」と表示される	 WindowsのサービスでEpsonNet Authentication Proxy Service が「開始」になっているか、確認してください。 なお、EpsonNet Authentication Proxy Service は自動的に開始するように設定されています。停止を指示しない限り停止しません。
	認証サービスが認証リクエストを受け付けない (Windows Server 2003)	 認証プロキシサービス搭載サーバで Windows ファイアウォールが有効になっています。無効にするか、または以下の設定を行ってください。 <例：Windows Server 2003 の場合> ①[スタート] - [コントロールパネル] - [ネットワークとインターネット接続] - [Windows ファイアウォール] の順にクリックします。 ②[例外] タブをクリックして [ポートの追加] をクリックします。 ③以下の名前 (任意) とポート番号を入力し、[TCP] を選択して [OK] をクリックします。 名前 : 認証プロキシ (TCP) (←任意の名称) ポート番号 : 59230 ④再度、[ポートの追加] をクリックします。 ⑤以下の名前 (任意) とポート番号を入力し、[UDP] を選択して [OK] をクリックします。 名前 : 認証プロキシ (UDP) (←任意の名称) ポート番号 : 59230 ⑥以下の名前 (任意) とポート番号を入力し、[UDP] を選択して [OK] をクリックします。 名前 : 認証プロキシ (UDP 2) (←任意の名称) ポート番号 : 59231 ⑦[プログラムおよびサービス] の欄に上記で指定した 3 つの名前が追加されていることを確認して、各チェックボックスをチェックします。 ⑧[OK] をクリックします。
	認証処理結果に \$PROXY_ERROR が必ず含まれる	 稼働ログの認証処理結果を参照の上、マクロの記述に誤りがないか、確認してください。 ログレベルを [詳細] または [デバッグ] に設定すると、認証要求内容および認証処理結果がログに記録されます。 ☞ 本書 19 ページ「ログの設定」  本製品を同一ライセンスキーで重複インストールしている場合は、アンインストールしてください。 認証プロキシサービスは同一ライセンスキーでの重複インストールを検出すると、後からインストールした認証プロキシサービスは認証処理機能を停止して、\$PROXY_ERROR を含む認証処理結果を返し続けます。 ☞ 本書 52 ページ「アンインストール」
認証プロキシ 管理全般	認証プロキシ管理の起動用パスワードを忘れてしまった	 再インストールしてください。 ☞ 本書 8 ページ「インストール」 起動用パスワードを忘れると認証プロキシ管理が起動できないため、再インストールを設定し直してください。 なお、認証サービス自体は動作を継続します。

	トラブル状態	対処方法
設定ファイル	設定ファイルの内容を削除してしまい復旧できない（カスタム設定での設定編集時）	<p>✓ 「サービスへの設定反映」を行う前： 認証プロキシ管理を終了して、再起動してください。カスタム設定で削除した設定が復帰します。 📖 本書 52 ページ「設定の初期化」</p> <p>✓ 「サービスへの設定反映」を行った後： 付録の設定値を参照して、カスタム設定のテキストエディタで入力してください。 📖 本書 48 ページ「カスタム設定」</p>
	設定ファイルを初期の状態に戻したい	<p>✓ 付録の設定値を参照して、カスタム設定のテキストエディタで入力してください。 📖 本書 48 ページ「カスタム設定」</p>
	設定ファイル自体を削除してしまった	<p>✓ 再インストールしてください。 設定ファイルは暗号化されているため、一般的なテキストエディタでの編集および作成はできません。 📖 本書 8 ページ「インストール」</p>
マクロファイル	マクロファイルの内容を削除してしまい復旧できない（マクロ編集時）	<p>✓ 「サービスへの設定反映」を行う前： 「認証プロキシ管理」を終了して、再起動してください。削除したマクロが復帰します。 📖 本書 18 ページ「認証プロキシ管理の終了」、本書 10 ページ「認証プロキシ管理の起動」</p> <p>✓ 「サービスへの設定反映」を行った後： 復帰できません。最初からマクロを記述し直してください。 📖 本書 16 ページ「マクロの設定」</p>
	マクロファイル自体を削除してしまった	<p>✓ 再インストールしてください。 マクロファイルは暗号化されているため、一般的なテキストエディタでの編集および作成はできません。 📖 本書 8 ページ「インストール」</p>
マクロの記述	「マクロ編集」でマクロを編集し[設定保持]をクリックすると、文法エラーを指摘される	<p>✓ マクロ文に文法エラーがあると、エラーの場所、関連する変数や関数が表示されます。マクロ関数の一覧を参照して、適切な文法でマクロ文を記述してください。 📖 本書 37 ページ「マクロの文法」</p>
	「マクロ編集」でマクロを編集し[設定保持]をクリックすると、文法エラーを指摘される（モジュールの関数）	<p>✓ 「モジュール設定」で、当該の認証用モジュールを「有効」に設定してからマクロ文を記述してください。 マクロ文で使用しようとしている関数が、認証用モジュール（LdapModule、DatabaseModule）で提供されている場合は、これらの関数が「モジュール設定」で「有効」に設定されている必要があります。 📖 本書 20 ページ「モジュールの有効化／無効化」</p>

	トラブル状態	対処方法
設定の反映	設定を変更したが、設定通りに動作しない	 「サービスへの設定反映」を行ってください。 「サービスへの設定反映」を行わないと、認証プロキシ管理の設定は認証プロキシサービスに適用されません。 📖 本書 12 ページ手順 5 ~ 6
	カスタム設定で記述した設定が有効にならない	 行の先頭に「#」が付いていないことを確認してください。  同じ設定キーが2行以上記載されていないか確認してください。 2 行以上記載されている場合、後の行の設定が有効となります。 loglevel=info loglevel=debug と記載されている場合、loglevel=debug が有効となります。 📖 本書 48 ページ「カスタム設定」
設定ファイル/ マクロファイルのバックアップ	設定ファイルとマクロファイルのバックアップを取っておきたい	 proxy_setting (設定ファイル)、macro (マクロファイル) というファイル名でインストールフォルダに保存されています。 これらのファイルをコピー保存しておき、再インストール後にファイルを置き換えることは可能です。ただし、管理者は、認証プロキシ管理の起動用パスワードを記憶しておく必要があります。 さらに、使用環境に応じて、krb5.conf ファイルや cacerts ファイルもバックアップを取る必要があります。
Ldap Module	認証プロキシに送付した認証要求に対する認証結果の戻りが遅い	 指定しているLDAPサーバのホスト名／IP アドレスの中に無効なものが入っていないか確認してください。 複数の LDAP サーバを指定している場合、指定した順にアクセスを試みます。 先に登録されている LDAP サーバのホスト名／IP アドレスに無効なもの（アクセスできないもの）が含まれていると、タイムアウト処理にかかる時間が長くなるため、認証結果の戻りが遅くなります。 📖 本書 11 ページ「LDAP モジュール」  認証プロキシサービスをインストールしたサーバで、LDAP サーバの名前解決ができていないか確認してください。 LdapModule を使用するには、DNS 等で LDAP サーバの名前解決ができるように設定しておく必要があります。OS の取扱説明書を参照して設定してください。 <ul style="list-style-type: none"> • DNS サーバ LDAP サーバの登録（正引き、逆引き） • 認証プロキシサービスをインストールしたサーバ DNS サーバの指定 DNS サフィックスの指定  マクロにてLdapModuleのget関数を用いて複数の属性値を取得している場合は、multiget 関数の使用をお勧めします。 複数の属性値を取得するにあたり、multiget 関数を使用すると、get 関数を使用する場合と比べて LDAP サーバへの通信回数を削減することができます。これにより認証結果の戻りが早くなる可能性があります。 📖 本書 46 ページ「LdapModule のモジュール関数」
	指定した認証アルゴリズムでLDAPサーバにアクセスできない	 LDAPサーバ側の設定を確認して、LDAPサーバ側で有効となっている認証アルゴリズムを選択してください。 LDAP サーバの設定によっては、認証プロキシサービス側で指定する認証アルゴリズムをサポートしていないことがあります。 📖 本書 13 ページ「認証方法の設定」

	トラブル状態	対処方法
Ldap Module	認証アルゴリズムを Kerberos V5 にすると、LDAP サーバにアクセスできない	<p> Kerberos V5 認証に対応しているか、krb5.conf ファイルをインポートしているか確認してください。 アクセス先の LDAP サーバが Kerberos V5 認証に対応している必要があります。 また、「アルゴリズムごとの設定」で krb5.conf ファイルをインポートする必要があります (krb5.conf ファイルには KDC サーバの所在とドメイン名の情報が記載されています。"Key Distribution Center")。 本書 13 ページ「認証方法の設定」</p> <p>Kerberos 認証を行うには、DNS 等で KDC サーバの名前解決ができるように、認証プロキシサービスをインストールしたサーバで DNS の設定などを行う必要があります。OS の取扱説明書を参照して設定してください。</p> <ul style="list-style-type: none"> • DNS サーバ KDC サーバの登録 (正引き、逆引き) • 認証プロキシサービスをインストールしたサーバ DNS サーバの指定 DNS サフィックスの指定 <p> 「krb5.conf ファイルのインポート」または「krb5.conf ファイルの簡易インポート」を行った場合は、以下の手順で、過去に取得した Kerberos 認証チケットを破棄してください。</p> <p>1 「サービスへの設定反映」を行います。 本書 12 ページ手順 5 ～ 6</p> <p>2 一旦、[認証プロキシ管理] を終了します。 本書 18 ページ「認証プロキシ管理の終了」</p> <p>3 Windows に登録された [EpsonNet Authentication Proxy Service] を再起動します。 ① [スタート] - [プログラム] または [すべてのプログラム] - [管理ツール] - [サービス] の順にクリックします。 ② [EpsonNet Authentication Proxy Service] をダブルクリックして [停止] をクリックします。 ③ 停止の状態になったら [開始] をクリックします。</p>
	認証アルゴリズムを Kerberos V5 にしてマクロで bindauth 関数を使用すると、認証処理が行われない	<p> bindauth 関数を使用する場合は、LDAP サーバ側で有効となっている認証アルゴリズムのうち、Kerberos V5 以外の認証アルゴリズムを選択してください。 認証プロキシサービスは bindauth 関数 (バインド認証処理) において、Kerberos V5 認証をサポートしていません。他の認証アルゴリズムを指定してください。 本書 13 ページ「認証方法の設定」</p>
	SSL、StartTLS 用の証明書ファイルをインポートできない	<p> X.509DER フォーマットまたは X.509PEM フォーマットのファイルをインポートしてください。 本書 12 ページ「暗号化通信 (SSL / StartTLS)」</p>
	OpenSSL の CA 証明書 (X.509PEM フォーマット) をインポートできない	<p> -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- までの部分を抜き出したファイルをインポートしてください。 OpenSSL が生成した CA 証明書には、上記の部分以外の文字も記述されています。 本書 12 ページ「暗号化通信 (SSL / StartTLS)」</p>

	トラブル状態	対処方法
Ldap Module	StartTLS で通信できない	 LDAP サーバのポート番号を確認してください。 ポート番号が SSL 用のポート番号（636）になっているときは、StartTLS の場合、平文での LDAP 通信と同じポート番号（389）で通信します。 <small>📖 本書 11 ページ「LDAP モジュール」</small>
	LdapModule の設定で「パブリック CA の証明書を使用」を選択して暗号化通信を行おうとしたが、LDAP サーバと通信できない	 「プライベートCAの証明書を使用」を選択して証明書をインポートしてください。 「パブリック CA の証明書を使用」を選択した場合、Java Runtime Environment に組み込まれている CA 証明書を使用します。Java Runtime Environment では、代表的な CA 証明書が組み込まれていますが、組み込まれていない CA 証明書もあります。 <small>📖 本書 12 ページ「暗号化通信（SSL / StartTLS）」</small>
Database Module	10列以上のCSVファイルをインポートしてしまった	 11 列目以降の列に記述したデータは無視されます。実際にはインポートされません。 <small>📖 本書 16 ページ「CSV ファイルについて」</small>
	マクロ文に DatabaseModule の関数を挿入すると、文法エラーは指摘されないが、マクロチェッカーで認証テストを行うと、ログにエラーが表示される	 データベース内で有効な列は、J 列（10 列目）までです。参照列は、A 列から J 列までとしてください。 K 列（11 列目）以降の列を参照しようとすると、認証時にエラーになります。 <small>📖 本書 16 ページ「CSV ファイルについて」</small>
	DatabaseModule を使用した認証処理結果に、\$PROXY_AUTH_RESULT=FALSEが常に含まれている	 CSV ファイルのインポートを行っていない場合は、インポートしてください。 <small>📖 本書 15 ページ「ローカルデータベースモジュールの設定」</small>  DatabaseにインポートされているデータをCSVファイルにエクスポートして、引数を確認してください。 マクロに記載したDatabaseModuleのモジュール関数の引数に誤りがないか、確認してください。 A 列の値が XXX であるところを参照したいときは、以下のように記述します。 contains("A=XXX") XXX をクォートでくくります。 contains("A=XXX") と記述すると正常に認証処理を行えません。 <small>📖 本書 24 ページ「ローカルデータベースの更新（CSV ファイルのエクスポート）」</small>

エラーが発生したときの検証方法

エラーが発生したときの、原因検証の仕方を説明します。



稼動ログを参照して、不正な処理の履歴を確認します。

サービスステータスおよび稼動ログを参照して、エラーが発生していないか確認します。

📖 本書 22 ページ「稼動状況の確認」



認証プロキシサービス、LDAP サーバ等の設定を確認します。

サービスステータスおよび稼動ログを参照して、エラーが発生していないか確認します。

- ・ 各機器の電源を入れ、ネットワーク接続状態を確認します。
- ・ 認証プロキシサービスの設定を確認します。
- ・ 認証プロキシサービスに認証要求を送信する機器、ソフトウェアの設定を確認します。
- ・ LDAP サーバ内に格納されているデータを確認します。
- ・ LDAP サーバ側の通信用設定、認証設定を確認します。
- ・ 認証プロキシサービスを導入したサーバに、Windows ファイアウォールのような通信フィルタリングソフトが導入されている場合は、本製品における通信を妨げないよう設定を無効にします。設定の詳細は各機器の取扱説明書を参照してください。



認証プロキシサービス搭載サーバで Windows ファイアウォールを無効にするか、以下の設定を行います。

<例：Windows Server 2003 の場合>

- ① [スタート] - [コントロールパネル] - [ネットワークとインターネット接続] - [Windows ファイアウォール] の順にクリックします。
- ② [例外] タブをクリックして [ポートの追加] をクリックします。
- ③ 以下の名前（任意）とポート番号を入力し、[TCP] を選択して [OK] をクリックします。
名前：認証プロキシ（TCP）（←任意の名称）
ポート番号：59230
- ④ 再度、[ポートの追加] をクリックします。
- ⑤ 以下の名前（任意）とポート番号を入力し、[UDP] を選択して [OK] をクリックします。
名前：認証プロキシ（UDP）（←任意の名称）
ポート番号：59230
- ⑥ 以下の名前（任意）とポート番号を入力し、[UDP] を選択して [OK] をクリックします。
名前：認証プロキシ（UDP 2）（←任意の名称）
ポート番号：59231
- ⑦ [プログラムおよびサービス] の欄に上記で指定した 3 つの名前が追加されていることを確認して、各チェックボックスをチェックします。
- ⑧ [OK] をクリックします。



特定のユーザーのみに認証エラーが発生するときは、認証プロキシサービスへの認証要求に含まれる認証情報が正しいかどうか確認します。



1 認証プロキシ管理を起動します。

📖 本書 10 ページ「認証プロキシ管理の起動」



2 ログレベルを「詳細」にします。

ログレベルが「詳細」になっていない場合は「詳細」に変更します。

📖 本書 19 ページ「ログの設定」



3 メイン画面にて稼動ログを表示します。



4 認証操作を実施します。



5 稼動ログを参照して認証要求に含まれるユーザー識別子が適切かどうか確認します。

適切でない場合：認証プロキシサービスに認証要求を送信する機器、ソフトウェアの設定を確認します。

適切である場合：次の手順に進みます。

6

認証プロキシ管理で、マクロを表示し内容が適切かどうか確認します。

🔗 本書 16 ページ「マクロの設定」

7

認証プロキシ管理で、マクロ内で使用している個別認証用モジュール (LdapModule、DatabaseModule) に対する設定を確認します。

以上で終了です。

メッセージとサービスステータス

認証プロキシ管理で表示されるメッセージと対処方法は以下の通りです。

メッセージ	状況・対処方法
サービスが起動していません	認証プロキシサービスが「開始」の状態になっていません。 [スタート] - [プログラム] または [すべてのプログラム] - [管理ツール] - [サービス] の順にクリックし、EpsonNet Authentication Proxy Service を「開始」の状態にしてください。
モジュールに設定エラーがあります 設定内容を確認してください	認証用モジュールに不適切な設定があります（特にカスタム設定で記述した場合に表示されます）。
設定反映ができません サービスの状態を確認してください	認証プロキシサービスが起動していないので、「サービスへの設定反映」が実行できません。[スタート] - [プログラム] または [すべてのプログラム] - [管理ツール] - [サービス] の順にクリックし、EpsonNet Authentication Proxy Service の開始状態を確認してください。 このエラーメッセージは、認証プロキシ管理を起動後、認証プロキシサービスを停止して「サービスへの設定反映」を実行したときに表示されます。 認証プロキシサービスが開始されていない状態で認証プロキシ管理を起動したときは、「サービスが起動していません」とダイアログ表示されます。
設定は変更されていません	「サービスへの設定反映」が実行されましたが、前回「サービスへの設定反映」を行った時点から現時点までの間に設定保持された設定がないため、設定反映処理が行われませんでした。
未反映の設定があります 終了しますか？	「サービスへの設定反映」を行っていない設定保持中の設定がある状態で、認証プロキシ管理を終了しようとしています。 [OK] をクリックすると、未反映の設定を破棄して認証プロキシ管理を終了します。 📖 本書 18 ページ「未反映の設定があったときは」
マクロ文法エラー (エラー箇所が表示されます)	マクロ文の文法にエラーがあります。 エラー箇所を確認の上、マクロの文法や関数一覧を参照して、マクロ文の記述を見直してください。 📖 本書 37 ページ「マクロの文法」
無効な関数がマクロに含まれています (エラー箇所が表示されます)	マクロ文に無効な関数が含まれています。 [モジュール設定] の [有効] のチェックを外された認証用モジュールが提供する関数をマクロ文でしようとしているときに表示されます。 📖 本書 37 ページ「マクロの文法」
マクロに利用できない文字があります (エラー箇所が表示されます)	禁則文字（< など）がマクロ文に使用されています。このような禁則文字を引数に入力させるような関数はありません。 📖 本書 37 ページ「マクロの文法」
LDAP ユーザー DN が入力されていません	LDAPModule の設定画面の「LDAP ユーザー DN」が入力されていません。LDAP ユーザー名を入力してください。 📖 本書 13 ページ「認証方法の設定」
パスワードが入力されていません	LDAPModule の設定画面の「パスワード」が入力されていません。パスワードを入力してください。 📖 本書 13 ページ「認証方法の設定」
相対パスが指定されています 絶対パスで指定してください	ファイルが相対パス（例えば cacert.pem のようなファイル名のみ）で指定されています。 [ファイルの選択] をクリックしてファイルを選択し、C:¥xxx¥cacert.pem のように絶対パスで指定してください。
フォルダが指定されています ファイルを指定してください	C:¥xxx¥yyy のようなフォルダが指定されています。 [ファイルの選択] をクリックしてファイルを選択し、C:¥xxx¥cacert.pem のように絶対パスで指定してください。
証明書ファイルに不備があります	LDAPModule の設定画面の「暗号化通信用 証明書のインポート」で、インポートできないファイルが指定されています。 X.509DER 形式、X.509PEM 形式の CA 証明書またはサーバ証明書のファイルをインポートしてください。 📖 本書 12 ページ「暗号化通信 (SSL / StartTLS)」

メッセージ	状況・対処方法
KDCサーバ名/IPアドレスが入力されていません	LdapModule の設定画面の「Kerberos V5 の設定」の「KDC サーバ名 /IP アドレス」が入力されていません。 IP アドレス、ホスト名を以下の形式で入力してください。 例 IP アドレス 192.168.10.1 IP アドレス : ポート番号 192.168.10.1:88 ホスト名 kdc.test.local ホスト名 : ポート番号 kdc.test.local:88 ホスト名を入力する場合は、FQDN形式などDNS で名前解決できるものを指定してください。 📖 本書 14 ページ「krb5.conf ファイルの簡易インポート」
DNS 形式ドメイン名が入力されていません	LdapModule の設定画面の「Kerberos V5 の設定」の「DNS 式ドメイン名」が入力されていません。Kerberos 認証の環境に合わせて入力してください。 例 test.local 📖 本書 14 ページ「krb5.conf ファイルの簡易インポート」
ファイルが存在します ファイルを上書きしますか？	krb5.conf ファイルのインポート時 krb5.conf ファイルが、認証プロキシ for LDAP のインストールフォルダ内にあります。 DatabaseModule の CSV ファイルのエクスポート時 エクスポート先に、指定したファイルと同じ名前のファイルがあります。 上書きする場合は [OK] を、上書きしない場合は [キャンセル] をクリックしてください。
krb5.conf ファイルをインポートできませんでした。	DatabaseModule の設定画面で krb5.conf ファイルをインポートしようとしたましたが、ファイルの書き込みができませんでした。 <ul style="list-style-type: none"> インポート先のファイル(認証プロキシ for LDAP のインストールフォルダ内の ktr5.conf) が読み取り専用になっています。読み取り専用属性を解除してください。 Windows の設定で、インポート先のフォルダ (認証プロキシ for LDAP のインストールフォルダ) への書き込み権限がありません。アクセス権を確認してください。
指定されたファイルに書き込めません 別のファイルを指定してください	DatabaseModule の設定画面で CSV ファイルをエクスポートしようとしたますが、ファイルの書き込みができませんでした。 <ul style="list-style-type: none"> 指定したファイルが読み込み専用になっています。別のファイルを指定してください。 Windows の設定で、指定したファイルのあるフォルダへの書き込み権限がありません。書き込み権限のある別の場所にファイルを指定してください。
データベース処理中にエラーが発生しました	CSV ファイルのインポート／エクスポートの処理中に、何らかのエラーが発生しました。または、インポートしようとしている CSV ファイルの内容が不適切です。 エラー内容に応じて、エラー情報が以下のように稼動ログに記録されます。 <ul style="list-style-type: none"> インポート時のエラー Importing CSV file read error. Database access error during importing CSV file. エクスポート時のエラー Exporting CSV file read error. Database access error during exporting CSV file. CSV ファイルのエラー Import file format error.

認証プロキシ管理のサービスステータスは以下の通りです。

状態	対処方法
<System> MACRO_EXECUTE_ERROR	
マクロ実行処理中にエラーが発生しました。 • マクロ処理で使用するよう定義されている変数が、認証要求の中に含まれていません。 • マクロ関数の用法に間違いがあります（引数に数値以外の文字が入っているなど）。	マクロ文や認証要求に含まれる認証情報が適切か、内容を確認してください。 認証情報については、認証要求を送信するソフトウェア、機器等の取扱説明書を参照してください。
<LdapModule> LDAP_JAAS_CONF_FILE_NOT_FOUND	
インストールフォルダ内に gsseg_jaas.conf ファイルがありません。	Kerberos V5 認証を行う場合、gsseg_jaas.conf ファイルを参照します。インストールフォルダの gsseg_jaas.conf ファイルを編集したり、インストールフォルダから削除したりしないでください。 万一、編集／削除してしまった場合は、gsseg_jaas.conf ファイルを作ります。テキストエディタで以下の内容を記述し、ファイル名を「gsseg_jaas.conf」と付けてインストールフォルダに保存してください。 <pre>/** * DO NOT EDIT THIS FILE * * Login Configuration for JAAS. * * Specify that Kerberos v5 is a required login module for the * example classes: GssExample and Mutual. */ epson.proxy.module.Ldap.GssapiLDAPLoginHandler{ com.sun.security.auth.module.Krb5LoginModule required; };</pre>
<LdapModule> LDAP_KRB5_CONF_FILE_NOT_FOUND	
インストールフォルダ内に krb5.conf ファイルがありません。	Kerberos V5 認証を行う場合、krb5.conf ファイルを参照します。認証方法に Kerberos V5 を選択したときは、必ず krb5.conf ファイルをインポートしてください。 📖 本書 14 ページ「Kerberos V5 の場合」
<LdapModule> LDAP_TRUSTSTORE_FILE_NOT_FOUND	
インストールフォルダに cacerts ファイルがありません。 • 暗号化通信に SSL または StartTLS を選択して「プライベート CA の証明書を使用」を選択しましたが、証明書をインポートしていません。 • cacerts ファイルが削除されました。	「プライベート CA の証明書を使用」場合は、証明書をインポートしてください。 または「パブリック CA の証明書を使用」を選択してください。 📖 本書 12 ページ「暗号化通信（SSL / StartTLS）」
<LdapModule> LDAP_CONNECTION_ERROR	
認証プロキシサービスが、LDAP サーバと通信できません。	次のことを確認してください。 <ul style="list-style-type: none"> • 認証プロキシサービスと LDAP サーバの通信設定は適切か。 • 各機器の接続状態に不具合がないか。 • 通信経路のどこかで通信フィルタリングを行っていないか。
<LdapModule> LDAP_KERBEROS_ERROR	
Kerberos V5 認証ができません。	Kerberos V5 認証用に指定した LDAP ユーザー DN、パスワードが正しいかどうか確認してください。 📖 本書 13 ページ「認証方法の設定」

状態	対処方法
<LdapModule> LDAP_BIND_KRB_NOT_SUPPORTED	
認証アルゴリズムに Kerberos V5 が指定されている状態で、マクロで bindauth 関数を使用されています。もしくは他のソフトウェアからバインド認証要求を受信しています。	LDAP サーバ側で有効になっている認証アルゴリズムのうち、Kerberos V5 以外の認証アルゴリズムを選択してください。 認証プロキシサービスは、bindauth 関数（バインド認証処理）において Kerberos V5 認証をサポートしていません。 🔗 本書 13 ページ「認証方法の設定」
<LdapModule> LDAP_AUTH_ERROR	
LDAP サーバへのアクセス認証で、認証エラーが発生しアクセスできません。	LDAP サーバへのアクセス認証用に指定した LDAP ユーザー DN、パスワードが正しいかどうか確認してください。 🔗 本書 13 ページ「認証方法の設定」
<LdapModule> LDAP_AUTHENTICATION_MECHANISM_NOT_SUPPORTED_ERROR	
指定した認証方法は LDAP サーバが対応していないため、LDAP サーバへのアクセス認証が通りません。	LDAP サーバが対応している認証方法を確認し、認証方法を選択し直してください。 🔗 本書 13 ページ「認証方法の設定」
<LdapModule> LDAP_MACRO_ERROR	
認証処理中に、LdapModule の関数処理でエラーが発生しました。 <ul style="list-style-type: none"> LdapModule のモジュール関数の引数で指定されたエントリがありません。 検索フィルタの指定内容が不適切です。 	マクロに記述された LdapModule のモジュール関数の引数に誤りがないか、確認してください。 🔗 本書 16 ページ「マクロの設定」 上記に問題がない場合は、認証要求に含まれる変数値に誤りがないか、確認してください。認証要求の内容は、ログレベルを [詳細] または [デバッグ] に指定すると稼動ログに記録されます。 🔗 本書 19 ページ「ログの設定」、本書 23 ページ「ログの確認」
<LdapModule> LDAP_SERVER_SIDE_SETTING_ERROR	
LDAP サーバ側の処理で何らかのエラーが発生しました。	認証プロキシサービス側の稼動ログを参照し、LDAP サーバ側の設定、ログ等を確認してください。 🔗 本書 23 ページ「ログの確認」
<LdapModule> LDAP_CONTEXT_EXCEPTION	
LDAP サーバへのアクセス処理中にその他の何らかのエラーが発生しました。	稼動ログを参照してください。 🔗 本書 23 ページ「ログの確認」
<LdapModule> LDAP_CONTAINS_NO_SUCH_VARIABLE <LdapModule> LDAP_GET_NO_SUCH_VARIABLE	
認証リクエスト内に、マクロ処理で使用する変数が入っていません。	マクロまたは認証要求の内容に誤りがないか、確認してください。 認証要求の内容は、ログレベルを [詳細] または [デバッグ] に指定すると稼動ログに記録されます。 🔗 本書 19 ページ「ログの設定」、本書 23 ページ「ログの確認」
<DatabaseModule> CSV_IMPORT_ERROR	
CSV ファイルのインポート処置中にエラーが発生しました。	「メッセージとサービスステータス」の「データベース処理中にエラーが発生しました」を参照してください。 🔗 本書 33 ページ
<DatabaseModule> CSV_EXPORT_ERROR	
CSV ファイルのエクスポートでエラー（SQL 処理またはファイル書き込み処理エラー）が発生しました。	「メッセージとサービスステータス」の「データベース処理中にエラーが発生しました」を参照してください。 🔗 本書 33 ページ

状態	対処方法
<DatabaseModule> SQL_INJECTION_SUSPICION	
DatabaseModule の引数に SQL インジェクション（データベースの内容を改ざん、削除するなど不正な処理の埋め込み）の疑いのあるものが指定されているため、データベースアクセス処理が中止されました。	DatabaseModuleの引数に不正な値が入る可能性として次の2点があります。 <ul style="list-style-type: none">マクロ内でDatabaseModuleのモジュール関数の引数に直接記述されています。マクロを修正してください。 📖 本書 16 ページ「マクロの設定」マクロ内でDatabaseModuleのモジュール関数の引数に指定される変数の部分に、認証要求に含まれる変数が代入されています。認証要求の内容を確認してください。確認方法は、認証要求を送信する側のソフトウェア、機器等の取扱説明書を参照してください。

マクロの文法

認証プロキシのマクロは独自の文法を採用しています。以下に説明する用法や関数に準じて、マクロを編集してください。

マクロの基本用法

変数と文字列リテラル

【変数】

マクロ中の変数は "\$ 変数名 " という形式で記述します。

\$X

ユーザー認証情報として、プリンタの認証デバイスプラグインから送られた情報も変数として利用できます。USER_ID という変数を利用するときは、以下のように記述します。

\$USER_ID

なお、変数を初期化したり、null 値を入れたりする必要はありません。

また、以下はシステムで利用する変数のため、変数値を書き換える際は注意してください。

\$USER_ID	ユーザーの識別情報を表します。
\$PROXY_AUTH_RESULT	認証結果を表します。 マクロではこの変数が最終的に " TRUE " または " FALSE " 値になるようにします。
\$IP_ADDR	認証要求元の IP アドレスを表します。
\$PROXY_ERROR	認証プロキシがエラーになったときのエラー原因が含まれています。

認証プロキシサービスは、以下の変数にパスワード文字列が代入されているものとして扱います。稼動ログに認証履歴が記録される際、代入値が ***** に置き換えられた上で記録されます。LdapModule の bindauth 関数使用時に使用してください。

\$PASSWORD
\$PASS

【定数(文字列リテラル)】


固定した文字列はダブルクォーテーションから始め、ダブルクォーテーションで閉じて記述します。

例えば、文字列 Hello を使いたいときは以下のように記述します。

```
"Hello"
```

以降、この固定文字列を文字列リテラルと呼びます。なお、文字列リテラル中でそのままでは書き表せない以下の文字はエスケープ記号を使用します。

\\	"\" を表します。
\t	タブを表します。
\n	改行を表します。
\r	行頭を表します。
\"	ダブルクォートを表します。


参考 マクロで扱える最大文字数は、改行を含めて 65535 文字です。

代入文

代入文を記述すると、ある変数に対しての値が代入できます。

前述の USER_ID 変数の値を別の変数に代入するときは、以下のように記述します。行の最後には ";" (セミコロン) を付けてください。

```
$X=$USER_ID;
```

代入文では、固定文字列 (文字列リテラル) も使用できます。

```
$X="Hello";
```

以下のように関数を呼び出した結果を代入することもできます。

```
$X>equals( $Y , $Z );
```

ただし、値が入っていない変数の値を右辺に指定すると、マクロ処理時に実行時エラーが発生します。

```
$foo="aaaa";
$bar=$foo ←これは良い
$bar=$baz ←値が入っていない (今まで使用していない) 変数を利用したため、エラーになる
```

関数呼び出し

マクロに用意されている高度な処理を行うときに関数を呼び出します。関数には基本関数とモジュール関数の 2 つの種類があります。基本関数は文字列を操作するための関数です。また、モジュール関数は認証方法に依存する関数で、その処理内容は各個別認証モジュールの中で定義されます。本製品では、LdapModule と DatabaseModule の 2 種類の認証モジュールがあり、それぞれに LDAP やデータベースに関連した関数が用意されています。

基本関数の呼び出し

基本関数を呼び出すには以下のように記述します。引数の数は関数の用途によって異なります。

```
関数名 ( 引数 1 , 引数 2 , ..... );
```

具体例は次の通りです。

```
$X>equals( $Y , $Z );
```

この例では基本関数 equals を呼び出し、変数 Y と変数 Z の内容が同じかどうかを判断します。

内容が同じ場合の変数 X の値は TRUE, 異なる場合は FALSE になります。

文字列リテラルを引数にすることもできます。

```
$X>equals( $Y , "AAA" );
```

この例では基本関数 equals を呼び出し、変数 Y の値が文字列 AAA であるかどうかを確認します。

内容が同じ場合の変数 X の値は TRUE, 異なる場合は FALSE になります。

モジュール関数の呼び出し

本製品では、LdapModule と DatabaseModule の 2 種類の認証モジュールを用意しています。それぞれのモジュールが提供する機能を利用するには、以下のようにモジュール関数を呼び出します。モジュール関数を呼び出す場合は、関数の前にモジュール名とコロンを付けます。

```
モジュール名 : 関数名 ( 引数 1 , 引数 2 , ..... );
```

LdapModule に、指定されたデータが LDAP サーバ上にあるかどうかを確認する contains という関数があります。これ呼び出すときは、以下のように記述します。

```
$X=epson.proxy.module.ldap.LdapModule:contains( "uid=xxx,eee=xxx,xxxx=3333");
```

その他の関数も、同様の用法で記述してください。

IF 文

変数の値によって処理を変更しなければならないときは、IF 文で以下のように記述します。

```
if( 条件値 ){ 文 ; 文 ; ..... }else{ 文 ; 文 ; ..... }
```

ただし、else 以下はなくてもかまいません。

```
if( 条件値 ){ 文 ; 文 ; ..... }
```

以下は、変数 x に特定の値が入っているときに認証される記述例です。

```
$EQ_RESULT>equals( $x , "XXXXX" );  
if( $EQ_RESULT ){  
$PROXY_AUTH_RESULT="TRUE";  
}else{  
$PROXY_AUTH_RESULT="FALSE";
```

マクロの終了動作、マクロ実行中のエラー

マクロでエラーになってしまう処理を記述すると、エラーとなるステップが呼ばれたところでマクロは中断されます。さらに、中断されたマクロはその状態で終了してしまいます。

以下は、addInt() 関数なのに数字が引数に渡されていないためエラーとなる記述例です。

```
$X=addInt( "ABCDEF" , "GHIJKLMN" );  
$Y=subInt( "10" , "9" );  
$PROXY_AUTH_RESULT>equals( $Y , "1" );
```

この場合、数字でないために 1 行目の addInt() 関数の処理中にエラーが発生します。

addInt() 処理中にエラーが起きているため、addInt() の結果を代入している変数 X にも値が入りません。

addInt() 以降、2 行目以降の subInt()、equals() も実行されません。

以下のような場合にマクロが中断します。

- 値の入っていない変数を右辺値にした場合
- 値の入っていない変数で関数を呼び出した場合
- LdapModule が何らかの不都合で LDAP サーバにアクセスできない場合など、各モジュールの関数の呼び出し結果が null を返す場合。

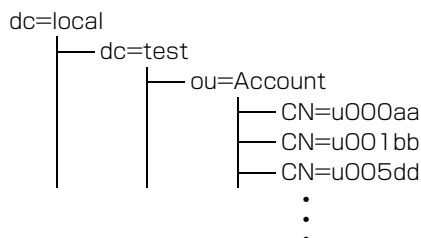
前述のエラーの例では、最終行で PROXY_AUTH_RESULT に値を代入する箇所まで処理が到達していません。つまり、認証結果を表す PROXY_AUTH_RESULT には値が入っていない状態でマクロが中断終了されるため、自動的に PROXY_AUTH_RESULT には FALSE が入り、認証結果失敗として終了します。

ただし、マクロの中断までに PROXY_AUTH_RESULT に値が代入されていると、その値が認証結果となります。

マクロサンプル

以降の LdapModule を使用する記述サンプルでは、LDAP サーバのデータツリー構造を以下とし、「LdapModule の設定」のベース DN で dc=test,dc=local を指定しているものとします。

LDAP サーバのデータツリー構造



LDAP データツリーのエン트리として各ユーザーが CN=XXXXXX として登録されている環境でユーザーの登録有無を確認する場合

```

$FIND_DN="CN={$.}OU=Accounts"; ←①
$FIND_DN=replace( $FIND_DN , $USER_ID ); ←②
$PROXY_AUTH_RESULT= Epson.Proxy.Module.Ldap.LdapModule:contains( $FIND_DN, "" ); ←③

```

- ① ユーザー ID を検索するテンプレート文を FIND_DN にセット
- ② テンプレート FIND_DN 中の {\$} 部分を認証デバイスからきた USER_ID (ユーザー認証情報) の値に置換して再セット
- ③ LDAP サーバに問い合わせ

contains の 2 番目の引数 (検索フィルタ) に "" を指定すると、(objectclass=*) と指定したものと見なして検索を行います。つまり、検索フィルタをかけずにエントリの存在を確認することになります。

RFC2254 の LDAP 検索フィルタを用いて cardID 属性で該当するユーザーを検索する場合

```

$FILTER="(cardID={$.})"; ←①
$FILTER=replace( $FILTER , $USER_ID ); ←②
$PROXY_AUTH_RESULT= Epson.Proxy.Module.Ldap.LdapModule:contains( "OU=Accounts", $FILTER ); ←③

```

- ① LDAP サーバ検索フィルタのテンプレート文
- ② \$FILTER の {\$} を \$USER_ID の値に置換
- ③ 検索範囲を "OU=Accounts"、検索フィルタを \$FILTER と指定し、LDAP サーバに問い合わせ

RFC2254 の LDAP 検索フィルタを用いて Active Directory に登録されたログインユーザー名を検索し、ユーザーの登録有無を確認する場合

```

$FILTER="( sAMAccountName ={$.})"; ←①
$FILTER=replace( $FILTER , $USER_ID ); ←②
$PROXY_AUTH_RESULT= Epson.Proxy.Module.Ldap.LdapModule:contains( "OU=Accounts", $FILTER ); ←③

```

- ① LDAP サーバ検索フィルタのテンプレート文
- ② \$FILTER の {\$} を \$USER_ID の値に置換
- ③ 検索範囲を "OU=Accounts"、検索フィルタを \$FILTER と指定し、LDAP サーバに問い合わせ

Active Directory では、ログインユーザー名は sAMAccountName 属性として記憶されています。上記のようにマクロを記述することで、Windows のログインユーザー名を参照してユーザー登録の有無を確認できます。

LDAP サーバ上に該当するユーザー識別子の属性(title)に応じて認証処理を行う場合

```
$FIND_DN="CN={ $ },OU=Accounts"; ←①
$FIND_DN=replace( $FIND_DN , $USER_ID ); ←②
$TITLE= epon.proxy.module.ldap.LdapModule:get( $FIND_DN , "", "title" ); ←③
$PROXY_AUTH_RESULT>equals( $TITLE , "Manager" ); ←④
```

- ① ユーザー ID を検索するテンプレート文
- ② FIND_DN の { \$ } を USER_ID の値に置換
- ③ LDAP サーバに問い合わせ、title に割り当てられた属性値を取得
- ④ 取得した属性値が Manager のときは認証を許可

\$PROXY_AUTH_RESULT が "TRUE" となったときに、そのエントリから複数の属性を指定して取得する場合

```
$FILTER="( CN = { $ })"; ←①
$FILTER=replace( $FILTER , $USER_ID ); ←②
$PROXY_AUTH_RESULT= epon.proxy.module.ldap.LdapModule:contains( "", $FILTER); ←③

if($PROXY_AUTH_RESULT){ ←④
    epon.proxy.module.ldap.LdapModule:multiget("", $FILTER, "title", $TITLE, "mail", $MAIL); ←⑤
}
```

- ① LDAP サーバ検索フィルタのテンプレート文
- ② \$FILTER の { \$ } を \$USER_ID の値に置換
- ③ 検索フィルタを \$FILTER と指定し、LDAP サーバに問い合わせ
- ④ \$PROXY_AUTH_RESULT の値が "TRUE" であるか否かを判断。"TRUE" の場合は⑤に進む
- ⑤ title、mail の属性値を LDAP サーバに問い合わせ、各々の属性値を \$TITLE、\$MAIL に代入する

LDAP サーバに対してユーザーID とパスワードを指定しバインド認証を行う場合

```
$SUFFIX_DN=",DC=test,DC=local"; ←①
$USER_ID=replace("CN={ $ }",$USER_ID);
$ACCOUNT=addstring($USER_ID,$ SUFFIX_DN); ←②
$PROXY_AUTH_RESULT=epon.proxy.module.ldap.LdapModule:bindauth($ACCOUNT,$PASSWORD); ←③
```

- ① ユーザー DN の末尾とする DN 文字列を定義
- ② \$USER_ID に割り当てられた文字列と、\$SUFFIX_DN に割り当てられた文字列を連結し \$ACCOUNT に代入
- ③ \$ACCOUNT と \$PASSWORD で、LDAP サーバへバインド認証を行い、認証結果を \$PROXY_AUTH_RESULT に代入

上記の例では、ユーザー認証情報で \$USER_ID="u000aa" と指定されていた場合、\$ACCOUNT="CN=u000aa,DC=test,DC=local"; となります。

なお、bindauth 関数は、Kerberos V5 認証に対応していませんので、別の認証アルゴリズムを指定してください。

📖 本書 13 ページ「認証方法の設定」

Active Directoryに対してユーザーID、ドメイン名、パスワードを指定しバインド認証を行う場合

```
$DOMAIN="test"; ←①
$ACCOUNT=replace("{${$}@", $USER_ID); ←②
$ACCOUNT=addstring($ACCOUNT, $DOMAIN); ←③
$PROXY_AUTH_RESULT=epson.proxy.module.Ldap.LdapModule:bindauth($ACCOUNT, $PASSWORD); ←④
```

- ① ドメイン名を定義
- ②、③ バインド認証用のアカウント名の文字列を生成
- ④ バインド認証

上記の例では、ユーザー認証情報で \$USER_ID="u000aa" と指定されていた場合、\$ACCOUNT="u000aa@test" となります。

なお、bindauth 関数は、Kerberos V5 認証に対応していませんので、別の認証アルゴリズムを指定してください。

📖 本書 13 ページ「認証方法の設定」

認証要求中の \$USER_ID に「カード識別番号」が入り、マクロ処理でその「カード識別番号」を「ユーザーID」に変換したい場合

※ データベースには、A 列をカード識別番号、B 列をユーザー ID とした CSV ファイルが、あらかじめインポートされているものとします。

```
$SQL=replace( "A='{${$}'" , $USER_ID ); ←①
$TEMP=epson.proxy.module.database.DatabaseModule:contains( $SQL ); ←②
if($TEMP){
    $USER_ID=epson.proxy.module.database.DatabaseModule:get($SQL,"B"); ←③
    $PROXY_AUTH_RESULT="TRUE"; ←④
}else{
    $PROXY_AUTH_RESULT="FALSE"; ←⑤
}
```

- ① データベースに問い合わせる検索文を作成
- ② データベースに該当するデータがあるか確認
- ③ 該当データがあった場合に、\$USER_ID 変数をデータベースの B 列から取得したユーザー ID で上書き

③で \$USER_ID に入力されたユーザー識別情報をもとに、さらに LDAP サーバにアクセスしてユーザー登録の有無を確認したり、属性情報を取得したりすることも可能です。

マクロ関数一覧

equals(文字列 A, 文字列 B)	<p>文字列 A と文字列 B が合致するかを調べ、合致する場合は TRUE を、そうでない場合は FALSE を返します。</p> <p>例 \$X=equals("AAA" , "BBB");</p> <p>結果 変数 X に FALSE が代入されます。</p>
contains(文字列 A)	<p>文字列 A で指定された変数が利用されているかを調べ、利用されている場合は TRUE を、そうでない場合は FALSE を返します。</p> <p>例 1 \$USER_ID がプリンタ側から送られるユーザー認証情報の場合における \$X=contains(\$USER_ID);</p> <p>結果 1 USER_ID はユーザー識別情報として使われているので、変数 X を TRUE になります。</p> <p>例 2 \$Y="xxxxx"; \$X=contains(\$Z);</p> <p>結果 2 変数 Z は使用されていないので、変数 X を FALSE になります。</p>
startsWith(文字列 A, 文字列 B);	<p>文字列 A が文字列 B で開始されるかを調べ、開始されている場合は TRUE を、そうでない場合は FALSE を返します。</p> <p>例 \$X=startsWith("ABCDE" , "AB");</p> <p>結果 変数 X は TRUE になります。</p>
endsWith(文字列 A, 文字列 B);	<p>文字列 A が文字列 B で終了しているかを調べ、終了している場合は TRUE を、そうでない場合は FALSE を返します。</p> <p>例 \$X=endsWith("ABCDE" , "AB");</p> <p>結果 変数 X は FALSE になります。</p>
replace(文字列 A, 文字列 B);	<p>文字列 A 中の {\$} という表記を文字列 B で置き換えた文字列が返されます。 文字列 A 中に {\$} がない場合は、文字列 A をそのまま返します。 文字列 A 中に複数回 {\$} がある場合は、最初の {\$} のみが文字列 B で置き換えられます。</p> <p>例 1 \$X=replace("It is {\$} today." , "fine");</p> <p>結果 1 変数 X は It is fine today. になります。</p> <p>例 2 \$X=replace("It is rainy today." , "fine");</p> <p>結果 2 変数 X は It is rainy today. になります。</p> <p>例 3 \$X=replace("{\$} is {\$} today." , "It");</p> <p>結果 3 変数 X は It is {\$} today. になります。</p>
toUpper(文字列 A, 文字列 B)	<p>文字列を大文字にした文字列を返します。 小文字がない場合は、そのまま返します。</p> <p>例 \$X=toUpper("It is fine today.");</p> <p>結果 変数 X は IT IS FINE TODAY. になります。</p>

toLowerCase(文字列 A, 文字列 B)	<p>文字列を小文字にした文字列を返します。 大文字がない場合は、そのまま返します。</p> <p>例 \$X=toLowerCase("It is fine today.");</p> <p>結果 変数 X は it is fine today. になります。</p>
length(文字列 A)	<p>文字列 A の長さを求めた値が入ります。 日本語の文字も 1 文字とカウントされます。</p> <p>例 \$X=length("今日は天気です.");</p> <p>変数 X は 8 になります。</p>
addstring(文字列 A , 文字列 B);	<p>文字列 A の後ろに文字列 B を連結した内容を返します。文字列として足されます。</p> <p>例 1 \$X="It's fine "; \$Y="today."; \$Z=addstring(\$X , \$Y);</p> <p>結果 1 変数 Z は It's fine today. となります。</p> <p>例 2 \$X="1"; \$Y="2"; \$Z=addstring(\$X , \$Y);</p> <p>結果 2 変数 Z は 12 となります。</p>
substring(文字列 A , 開始点文字位置 , 終了点文字位置);	<p>文字列 A を開始点から終了点までを取り出した部分文字列を返します。 なお、開始点は部分文字列の何文字目からを示す値であり、終了点は部分文字列に含まれる最後の文字が何文字目までかを示す値です。</p> <p>例 \$X=substring("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "2", "25");</p> <p>結果 変数 X は BCDEFGHIJKLMNOPQRSTUVWXYZ となります。</p>
indexOf(文字列 A, 文字列 B)	<p>文字列 A が文字列 B を含んでいるかを調べます。 文字列 A 中に文字列 B が含まれる場合は、文字列 A の何文字目から含まれるかを返します。 文字列 A が文字列 B を含まない場合は、-1 を返します。</p> <p>例 \$X=indexOf("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "BC");</p> <p>結果 変数 X は 2 となります。</p>
addInt(文字列 A, 文字列 B)	<p>値同士を足します。文字列 A, 文字列 B はともに整数を入れます。 なお、2 の 63 乗 -1 行が最大値、最小値は -2 の 63 乗となり、それ以上／以下は桁あふれが生じます。</p> <p>例 \$X=addInt("1", "2");</p> <p>結果 変数 X は 3 となります。</p>
subInt(文字列 A, 文字列 B)	<p>文字列 A から文字列 B の値を引きます。文字列 A, 文字列 B ともに整数を入れます。 なお、最大値は 2 の 63 乗 -1 行、最小値は -2 の 63 乗となり、それ以上／以下は桁あふれが生じ、最大値 +1 は最小値、最小値 -1 は最大値となります。</p> <p>例 \$X=subInt("1", "2");</p> <p>結果 変数 X は -1 となります。</p>

LdapModule のモジュール関数

contains(文字列 A, 文字列 B)	<p>指定された DN のデータのうち、指定した検索フィルタの条件に一致するものが LDAP サーバ上にあるかどうかを確認し、結果を TRUE または FALSE で返します。</p> <p>検索フィルタは RFC2254 にて定義される形式です。</p> <p>なお、検索フィルタとして長さ 0 の文字列 (カラ文字) を指定した場合は、"objectclass=*" と指定したものと同一となります。</p> <p>contains(DN 情報, 検索フィルタ);</p> <p>例</p> <pre>\$X=epson.proxy.module.ldap.LdapModule:contains("CN=xxxxx,OU=Accounts", "objectclass=*");</pre> <p>結果</p> <p>LDAP サーバ上に "CN=xxxxx,OU=Accounts" で指定される DN のデータがあれば X に TRUE が、そうでない場合は X に FALSE が入ります。</p>
get(文字列 A , 文字列 B, 文字列 C)	<p>指定された DN のデータのうち、指定した検索フィルタの条件に一致するものが LDAP サーバ上にあるかどうか検索し、ある場合は指定された属性のデータが取得されます。</p> <p>検索フィルタは RFC2254 にて定義される形式です。</p> <p>なお、検索フィルタとして長さ 0 の文字列 (カラ文字) を指定した場合は、"objectclass=*" と指定したものと同一となります。</p> <p>get(DN 情報, 検索フィルタ, 属性名);</p> <p>例</p> <pre>\$X= epson.proxy.module.ldap.LdapModule:get("CN=xxxxx,OU=Accounts" , "objectclass=*" , "title");</pre> <p>結果</p> <p>LDAP サーバ上に "CN=xxxxx,OU=Accounts" で指定される DN のデータが存在し、その DN で指定されたデータの title 属性から取得できた値が X に入ります。該当する属性がない場合は、空文字列 "" を返します。</p>
get2(文字列 A , 文字列 B, 文字列 C)	<p>指定された DN のデータのうち、指定した検索フィルタの条件に一致するものが LDAP サーバ上にあるかどうか検索し、ある場合は指定された属性のデータが取得されます。</p> <p>検索フィルタは RFC2254 にて定義される形式です。</p> <p>なお、検索フィルタとして長さ 0 の文字列 (カラ文字) を指定した場合は、"objectclass=*" と指定したものと同一となります。</p> <p>get2(DN 情報, 検索フィルタ, 属性名);</p> <p>例</p> <pre>\$X= epson.proxy.module.ldap.LdapModule:get2("CN=xxxxx,OU=Accounts" , "objectclass=*" , "title");</pre> <p>結果</p> <p>LDAP サーバ上に "CN=xxxxx,OU=Accounts" で指定される DN のデータがあって、その DN で指定されたデータの title 属性から取得できた値が X に入ります。該当する属性がない場合は、その時点でマクロが終了します。</p>
multiget(文字列 A, 文字列 B, 文字列 C, 文字列 D, …..)	<p>指定された DN のデータのうち、指定した検索フィルタの条件に一致するものが LDAP サーバ上にあるかどうか検索し、ある場合は指定された属性のデータを取得します。一度の LDAP 検索で複数の属性を取得します。</p> <p>可変長引数で、取得属性の指定と取得した属性を収納する変数の組を足すことができます。</p> <p>multiget(DN 情報, 検索フィルタ, 取得属性名 1 , 変数 1, 取得属性名 2 , 変数 2 , …..);</p> <p>例</p> <pre>\$X= epson.proxy.module.ldap.LdapModule:multiget("CN=xxxxx,OU=Accounts" , "objectclass=*" , "title" , \$x , "mail" , \$y);</pre> <p>以下のように左辺に変数を指定せず、関数のみを記載することもできます。</p> <pre>epson.proxy.module.ldap.LdapModule:multiget("CN=xxxxx,OU=Accounts" , "objectclass=*" , "title" , \$x , "mail" , \$y);</pre> <p>結果</p> <p>LDAP サーバ上に "CN=xxxxx,OU=Accounts" で指定される DN のデータが存在し、その DN で指定されたデータの title 属性から取得できた値が \$x に、mail 属性が \$y に入ります。該当する属性がない場合、それぞれに空文字列 "" を返します。</p> <p>また、検索処理が正常に行われた場合、\$X には "TRUE" が入ります。</p>

<p>multiget2(文字列 A, 文字列 B, 文字列 C, 文字列 D,...)</p>	<p>指定された DN のデータのうち、指定した検索フィルタの条件に一致するものが LDAP サーバ上にあるかどうか検索し、ある場合は指定された属性のデータを取得します。一度の LDAP 検索で複数の属性を取得します。</p> <p>可変長引数で、取得属性の指定と取得した属性を収納する変数の組を足すことができます。</p> <p>multiget2(DN 情報, 検索フィルタ, 取得属性名 1, 変数 1, 取得属性名 2, 変数 2, ...);</p> <p>例</p> <pre>\$X= epson.proxy.module.ldap.LdapModule:multiget2("CN=xxxxx,OU=Accounts", "objectclass=" , "title" , \$x , "mail" , \$y);</pre> <p>以下のように左辺に変数を指定せず、関数のみを記載することもできます。</p> <pre>epson.proxy.module.ldap.LdapModule:multiget2("CN=xxxxx,OU=Accounts", "objectclass=" , "title" , \$x , "mail" , \$y);</pre> <p>結果</p> <p>LDAP サーバ上に "CN=xxxxx,OU=Accounts" で指定される DN のデータが存在し、その DN で指定されたデータの title 属性から取得できた値が \$x に、mail 属性が \$y に入ります。該当する属性がない場合、該当する属性にアクセスした時点でマクロが終了します。</p>
<p>bindauth(文字列 A, 文字列 B)</p>	<p>指定したユーザー DN、パスワードで LDAP サーバへアクセスできるかどうかで認証（バインド認証）を行います。</p> <p>bindauth(ユーザー DN, パスワード)</p> <p>例</p> <pre>\$X= epson.proxy.module.ldap.LdapModule:bindauth("CN=xxxx,dc=yyy,dc=zzz", "abcde123");</pre> <p>結果</p> <p>バインド認証が通った場合は "TRUE"、バインド認証が通らなかった場合は "FALSE" を返します。</p>

DatabaseModule のモジュール関数

contains(文字列 A)	<p>指定された where 条件に一致するものが内部データベース内にあるかどうかを確認し、結果を TRUE または FALSE で返します。</p> <p>contains(where 条件);</p> <p>例</p> <pre>\$X=epson.proxy.module.database.DatabaseModule:contains("A='u00023'");</pre> <p>結果</p> <p>内部データベース内に A 列すなわち、インポートさせた列の 1 列目に、u00023 に一致する行が存在する場合は X に TRUE が、そうでない場合は X に FALSE が入ります。</p> <p>参考</p> <p>引数では、</p> <p>A = 'u00023' のように = の前後に半角スペースが入ってもかまいません。</p> <p>'u00023 ' のようにクォートの中に半角スペースを入れると、</p> <p>[半角スペース]u00023[半角スペース] として扱われます。処理結果が変わりますので注意してください。</p>												
get(文字列 A , 文字列 B)	<p>指定された where 条件に一致するものが内部データベース内にあるかどうかを確認し、ある場合は、取得対象列名で指定した列のデータが取得されます。</p> <p>get(where 条件, 取得対象列名);</p> <p>例</p> <pre>\$X=epson.proxy.module.database.DatabaseModule:get("A='u00023'", "B");</pre> <p>結果</p> <p>内部データベース内の A 列（インポートさせた列の 1 列目）に u00023 に一致する行が存在する場合は、その行において列 B に格納されている文字列を返します。例えば、データベースに以下のようなデータが登録されている場合は、\$X に "manager" が代入されます。</p> <table><tr><th>A</th><th>B</th><th>C</th></tr><tr><td>u00004</td><td>assistant</td><td>aaaa</td></tr><tr><td>u00023</td><td>manager</td><td>bbbb</td></tr><tr><td>u00056</td><td>assistant</td><td>cccc</td></tr></table> <p>u00023 に一致する行が存在しない場合はカラ文字を返します。</p>	A	B	C	u00004	assistant	aaaa	u00023	manager	bbbb	u00056	assistant	cccc
A	B	C											
u00004	assistant	aaaa											
u00023	manager	bbbb											
u00056	assistant	cccc											

カスタム設定

認証プロキシサービスが参照する設定ファイルを、認証プロキシ管理で直接編集することができます。認証プロキシ管理の画面で指定する設定も、カスタム設定で指定できます。

以下の設定は、カスタム設定でのみ指定できます。

- 認証リクエスト受信ポート番号
[proxy.receiving.port]
- LDAP サーバへのアクセスタイムアウトの設定
[ldap.connect.timeout]
- LDAP サーバにバイナリ形式で格納されている属性値を、Base64 でエンコードされた文字列として取得するための設定
[ldap.binary.access.attribute]

！重要

- 設定ファイルは、認証用マクロ以外のあらゆる設定情報を保持するファイルです。設定を誤ると、認証サービスが正常に動作しないことがあります。編集は注意して行ってください。
- 通常は、[カスタム設定] を用いず、他の各設定画面にて設定を行ってください。

参考

- 設定ファイルは暗号化されています。認証プロキシ管理を使用しないと編集できません。
- 編集した設定ファイルは、「サービスへの設定反映」が行われるまで有効になりません。

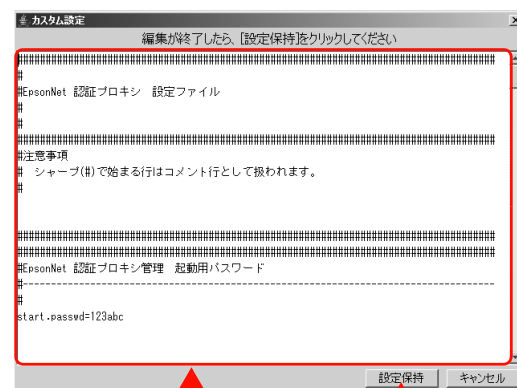
1 [設定] - [カスタム設定] の順にクリックします。



2

テキストを編集して [設定維持] をクリックします。

設定方法は、設定ファイルのコメントを参照してください。

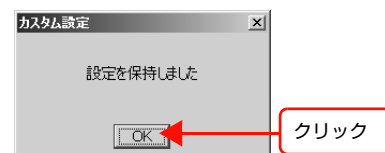


参考

- 設定を無効にしたい場合は、行の先頭に「#」を挿入します。必須の設定項目を無効にすると、認証プロキシサービスが正常に動作しなくなります。
- 同じ設定キーについて 2 行、別の設定値を記述した場合、2 行目の設定が有効になります。

3

[OK] をクリックします。



参考

認証プロキシサービスで使用できない認証用モジュールを指定して [設定維持] をクリックすると、エラーメッセージが表示され、設定は保持されません。[OK] ボタンをクリックすると、「カスタム設定」画面に戻りますので、認証用モジュールを指定し直してください。

4

「サービスへの設定反映」を行います。

12 ページの手順 5 ～ 6 と同様の手順で、設定を認証プロキシサービスに反映します。

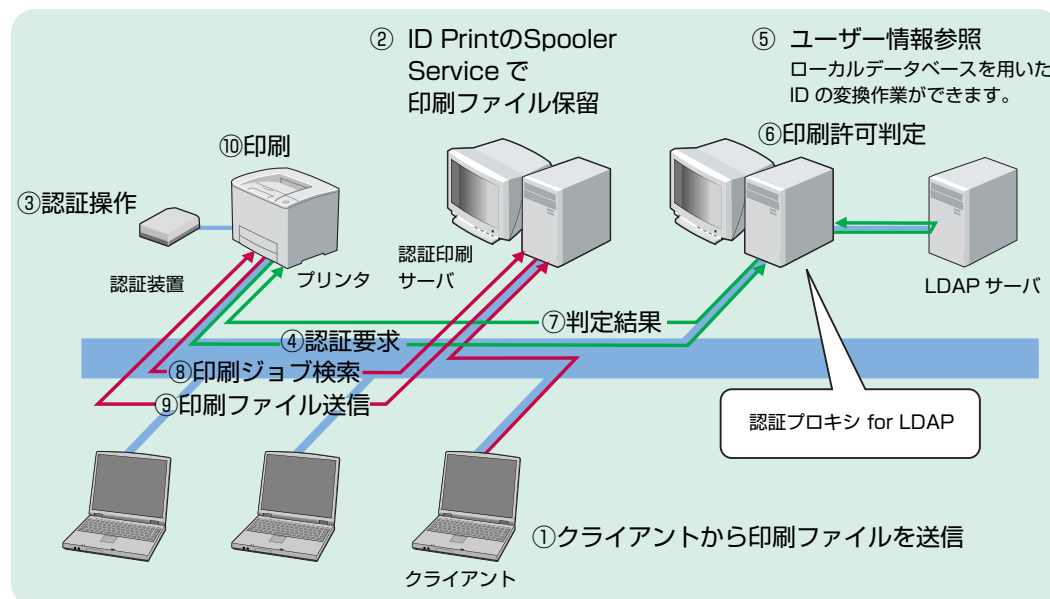
以上で終了です。

Offirio SynergyWare ID Print との連携

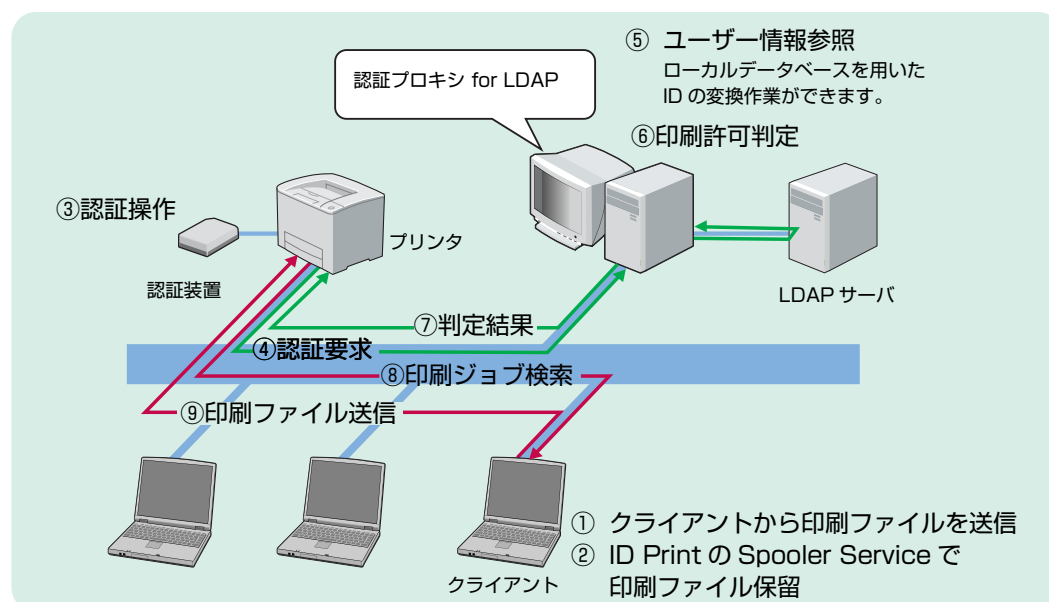
本製品は、エプソンの認証印刷システム「ID Print」と連携して運用できます。その場合の認証印刷の流れは下図の通りです。

ID Printと連携するには、プラグインが必要です。Offirio SynergyWare ID Print (Ver.1.5x) と連携する場合は、ソフトウェア CD-ROM 内の [PLUGIN] - [Auth プロキシ] フォルダに収録されている取扱説明書『Offirio SynergyWare ID Print 認証プロキシ for LDAP との連携について』（PDF）を参照してください。EpsonNet ID Print (Ver.1.0) と連携する場合は、エプソンのホームページからプラグインと取扱説明書をダウンロードしてください。

サーバ経由の場合

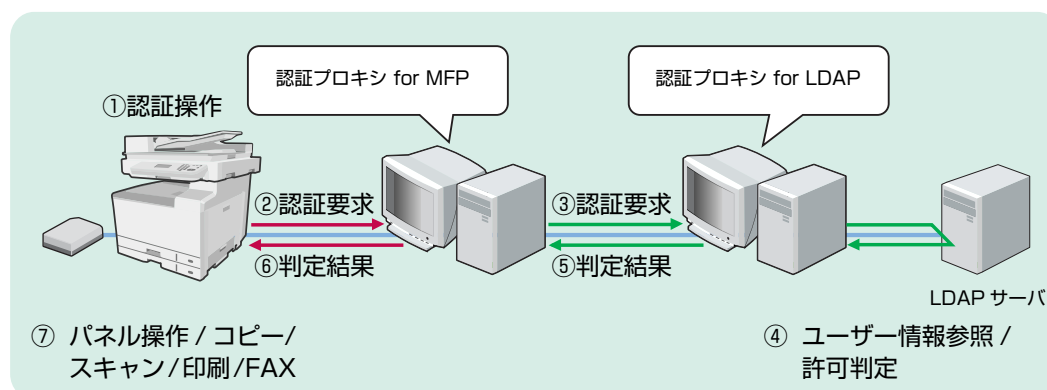


直接印刷の場合



Offirio SynergyWare 認証プロキシ for MFP との連携

本システムは、Offirio SynergyWare 認証プロキシ for MFP (以下「認証プロキシ for MFP」) と連携して運用できます。



※認証プロキシ for MFP と認証プロキシ for LDAP は、同じコンピュータにインストールすることもできます。

マクロサンプル

連携する場合は、以下のサンプルをもとにマクロを設定してください。

Active Directory の場合

```
$ROOT_DN="dc=test,dc=local"; ←①
$DOMAIN="test.local"; ←②
$SEARCH_FILTER=replace("sAMAccountName={}",$USER_ID); ←③
if($CARD_AUTH){ ←④
    $PROXY_AUTH_RESULT=epson.proxy.module.ldap.LdapModule:contains("",$SEARCH_FILTER); ←⑤
}else{
    $ACCOUNT=replace("{">@",$USER_ID); ←⑥
    $ACCOUNT=addstring($ACCOUNT,$DOMAIN); ←⑦
    $PROXY_AUTH_RESULT=epson.proxy.module.ldap.LdapModule:bindauth($ACCOUNT,$PASSWORD); ←⑧
}
if($PROXY_AUTH_RESULT){
    epson.proxy.module.ldap.LdapModule:multiget("",$SEARCH_FILTER,"sAMAccountName",$CN,"displayName",
$DISPLAY_NAME,"sn",$SN,"givenName",$GIVEN_NAME,"homeDirectory",$HOME_DIRECTORY,"mail",$MAIL); ←⑨
}
```

①、② ROOT_DN とドメイン名を定義します。"" で囲まれている文字列は LDAP サーバの設定に合わせて変更してください。

③ ユーザー ID 検索条件を \$SEARCH_FILTER に設定します。"" で囲まれている文字列の「sAMAccountName」は属性名です。LDAP サーバの設定に合わせて変更してください。

④ カード認証が否か判定します。

⑤ LDAP サーバにユーザー登録の有無を問い合わせます。

⑥、⑦ バインド認証用のアカウント名の文字列を生成します。

⑧ バインド認証を行います。

CS-9000 シリーズ (CS-9000/CS-9200) のみの環境で使用する場合は、⑥、⑦、⑧のみ記述してください。

⑨ ⑤または⑧で \$PROXY_AUTH_RESULT="TRUE" となった場合は、認証プロキシ for MFP と連携するためのユーザー属性情報を取得します。

"sAMAccountName","displayName","sn","givenName","homeDirectory","mail" の文字列は属性名です。LDAP サーバの設定に合わせて変更してください。

その他の LDAP サーバの場合

```

$ROOT_DN="dc=test,dc=local"; ←①
$BASE_DN="ou=users,dc=test,dc=local"; ←②
$SEARCH_FILTER=replace("description={}",$USER_ID); ←③
if($CARD_AUTH){ ←④
    $PROXY_AUTH_RESULT=epon.proxy.module.ldap.LdapModule:contains("$BASE_DN",$SEARCH_FILTER);
←⑤
}else{
    $ACCOUNT=replace("cn={}",$USER_ID); ←⑥
    $ACCOUNT=addstring($ACCOUNT,$BASE_DN); ←⑦
    $PROXY_AUTH_RESULT=epon.proxy.module.ldap.LdapModule:bindauth($ACCOUNT,$PASSWORD); ←⑧
}
if($PROXY_AUTH_RESULT){
    epon.proxy.module.ldap.LdapModule:multiget("", $SEARCH_FILTER,"cn",$CN,"displayName",$DISPLAY_NAME,"sn",$SN,"givenName",$GIVEN_NAME,"homeDirectory",$HOME_DIRECTORY,"mail",$MAIL); ←⑨
}

```

- ①、② ROOT_DN と BASE_DN を定義します。"" で囲まれている文字列は LDAP サーバの設定に合わせて変更してください。
- ③ ユーザー ID 検索条件を \$SEARCH_FILTER に設定します。"" で囲まれている文字列の「description」は属性名です。LDAP サーバの設定に合わせて変更してください。
- ④ カード認証が否か判定します。
- ⑤ LDAP サーバにユーザー登録の有無を問い合わせます。
- ⑥ バインド認証用のアカウント名の文字列を生成します。"" で囲まれている文字列の「cn」は属性名です。LDAP サーバの設定に合わせて変更してください。
- ⑦ バインド認証用のアカウント名の文字列を生成します。
- ⑧ バインド認証を行います。
- CS-9000 シリーズ (CS-9000/CS-9200) のみの環境で使用する場合は、⑥、⑦、⑧のみ記述してください。
- ⑨ ⑤または⑧で \$PROXY_AUTH_RESULT="TRUE" となった場合は、認証プロキシ for MFP と連携するためのユーザー属性情報を取得します。
- "cn","displayName","sn","givenName","homeDirectory","mail" の文字列は属性名です。LDAP サーバの設定に合わせて変更してください。

マクロチェック

マクロ文の動作確認をするには、[マクロチェック] で下記のように指定します。

- カード認証の場合
\$CARD_AUTH="TRUE",\$USER_ID="aaaauser"
- カード認証でない場合 (パスワード認証の場合)
\$CARD_AUTH="FALSE",\$USER_ID="aaaauser",\$PASSWORD="bbbbbbbb"

\$USER_ID、\$PASSWORD に割り当てる文字列は、ご利用の環境に応じて指定してください。

[マクロチェック] の方法は以下を参照してください。

📖 本書 17 ページ「マクロチェック」

アンインストール

インストールしたソフトウェアは以下の手順で削除（アンインストール）できます。アンインストールは Administrator 権限を持つユーザーがログオンした状態で行ってください。

参考

必要に応じて、次のファイルのバックアップを取っておいてください。

- 設定ファイル
- マクロファイル
- cacerts ファイル（証明書インポートを行う場合）
- krb5.conf ファイル（Kerberos V5 認証を行う場合）
- データベースのエクスポート、CSV ファイル生成（DatabaseModule を使用している場合）

1 Windows の [コントロールパネル] で [プログラムの追加と削除] または [アプリケーションの追加と削除] をクリックします。

2 [EpsonNet 認証プロキシ] を選択して [変更と削除] をクリックします。

以上で終了です。

設定の初期化

本製品は以下の手順で設定を初期化できます。

1 本製品をアンインストールします。
🔗 本書 52 ページ「アンインストール」

2 本製品をインストールします。
🔗 本書 8 ページ「インストール」

以上で終了です。