

Offirio SynergyWare

LDAP 連携ツール

操作ガイド

本書は、LDAP サーバから Offirio SynergyWare PrintDirector にユーザー情報を取り込むためのLDAP 連携ツールの使い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。

LDAP 連携ツールとは.....	3
環境設定.....	5
ユーザー情報の取り込みと更新の実行	11
こんなときは.....	12

マークの意味



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。



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

- お使いの機種により表示される画面が異なる場合がありますのであらかじめご了承ください。
- 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

Microsoft® Windows Server® 2008 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」、「Windows Server 2008」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

EPSON、EXCEED YOUR VISION はセイコーエプソンの登録商標です。

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。

その他の製品名は各社の商標または登録商標です。

本製品の不具合に起因する付随的損害

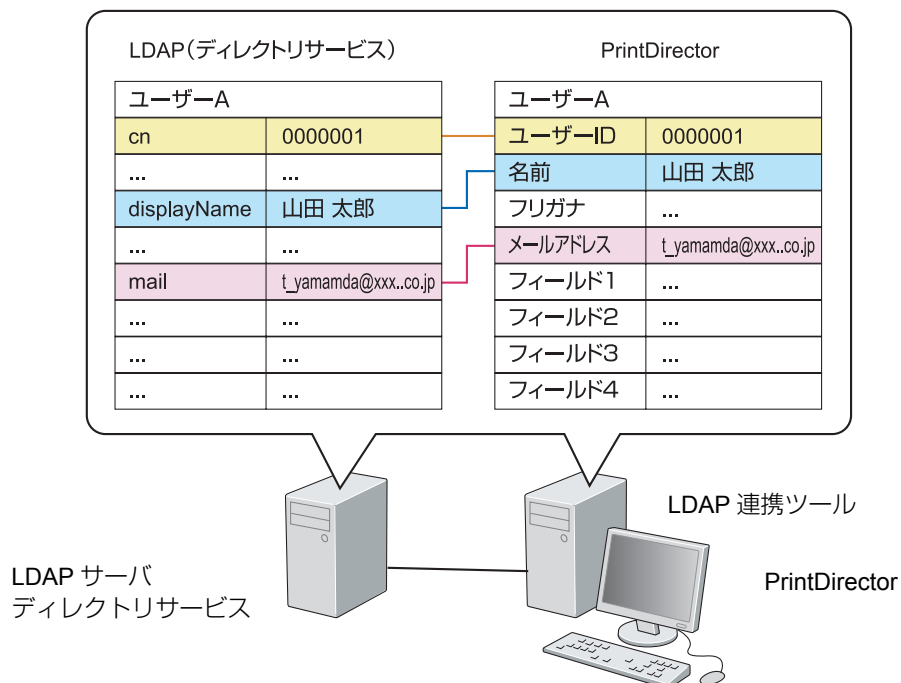
万一、本製品の不具合によって所期の結果が得られなかったとしても、そのことから生じた付随的な損害（本製品を使用するために要した諸費用、および本製品を使用することにより得られたであろう利益の損失等）は、補償致しかねます。

著作権

写真・書籍・地図・図面・絵画・版画・音楽・映画・プログラムなどの著作権物は、個人（家庭内その他これに準ずる限られた範囲内）で使用するために複製する以外は著作権者の承認が必要です。

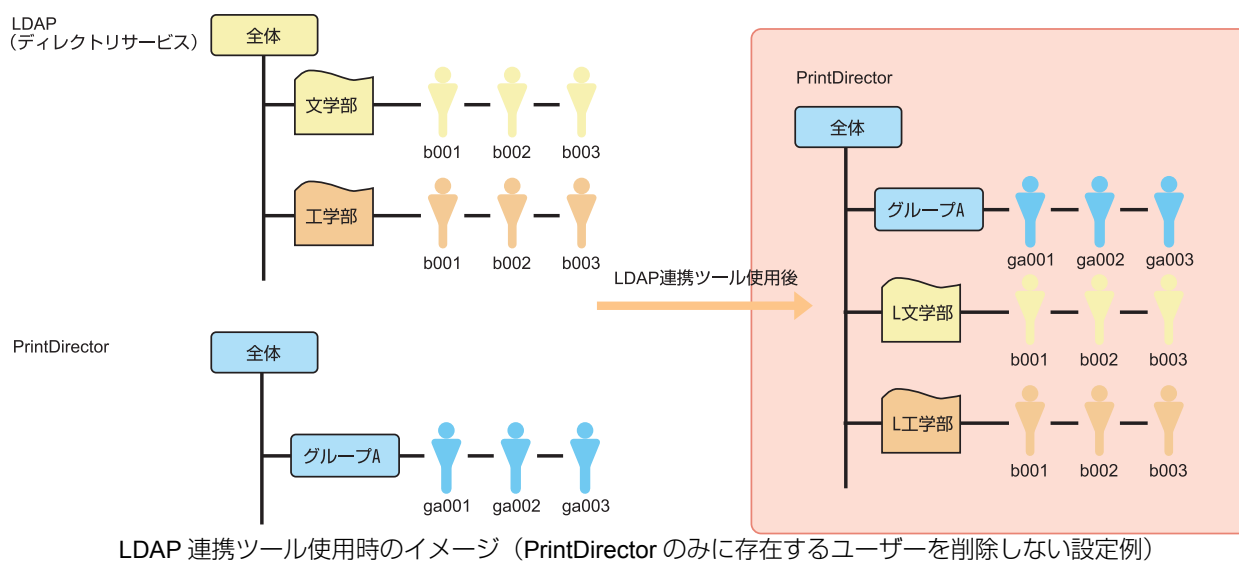
LDAP 連携ツールとは

LDAPサーバ(ディレクトリサービス)から Offirio SynergyWare PrintDirector にユーザー情報を取り込むためのツールです。本ツールは、Offirio SynergyWare PrintDirector インストール時に一緒にインストールされます。



LDAP 連携ツールでできること

- ディレクトリサービスから情報を取得して、Offirio SynergyWare PrintDirector にユーザー情報を登録できます。
- Offirio SynergyWare PrintDirector に登録済みのユーザーの基本情報をディレクトリサービスに登録されている情報と同じように更新できます (ただし、ディレクトリサービスの情報が書き換えられるわけではありません)。
- ディレクトリサービスに存在しないユーザーを Offirio SynergyWare PrintDirector から削除できます。



LDAP 連携ツール使用時のイメージ (PrintDirector のみに存在するユーザーを削除しない設定例)

参考

本ツールは、本ツールの実行時にディレクトリサービスに登録されている情報を取り込むだけで、常時ディレクトリサービスと連携し、情報を更新することはできません。ただし、OS のタスクスケジューラなどに組み込んで更新することができます。

🔗 11 ページ「ユーザー情報の取り込みと更新の実行」

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・PrintDirector 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

システム条件

システム条件は以下の通りです（2009 年 12 月現在）。

PrintDirector インストールサーバ OS * 1	<ul style="list-style-type: none"> • Windows 2000 Server/Advanced Server（Service Pack4 以降） • Windows Server 2003 Enterprise Edition/Standard Edition（Service Pack1 以降） • Windows Server 2008 Enterprise Edition/Standard Edition（Service Pack2 以降）* 2 <p>32bitOS で本ソフトウェアをネットワーク環境で使用する場合、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 にインストールして使用すると、マイクロソフトコーポレーションの使用許諾に違反する場合があります。詳細については、OS の使用許諾契約をご確認ください。</p>
連携可能な ディレクトリサービス	<ul style="list-style-type: none"> • Active Directory (Windows 2000 Server/Windows Server 2003/Windows Server 2008) • OpenLDAP Ver2.3.x

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ことがあります。詳細は、OS の使用許諾契約をご確認ください。

* 1 :64bit OS は使用できません（Windows Server 2003/Window Server 2008/Window Server 2008 R2）。

* 2 : Windows Server 2008 は、Windows Messenger Service による通知機能を使用できません。

CPU	Intel® Pentium® 4 1.0GHz 以上
RAM	512MB 以上
ハードディスク	300MB 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）



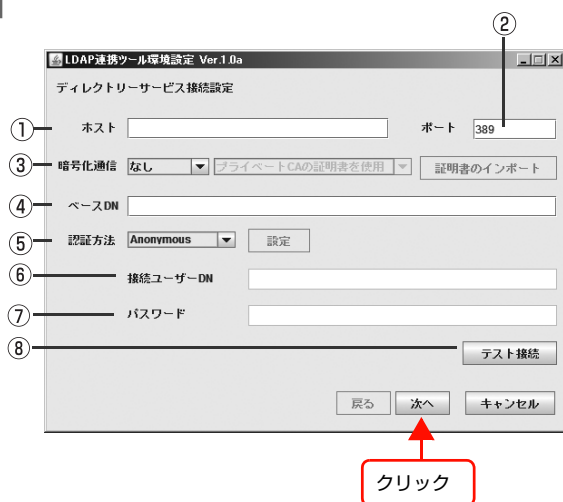
- ハードディスクの容量は、ローカルデータベースへのユーザー情報登録件数に依存します。さらに多くの容量を必要とすることがあります。
- 取得可能なユーザー数および PrintDirector への登録ユーザー数は、およそ 20000 人です。

環境設定

LDAP サーバと通信するための環境を設定します。
手順は Windows Server 2003 を例に説明しています。

1 [スタート] - [プログラム] (または [すべてのプログラム]) - [EpsonNet] - [PrintDirector] - [Tools] - [LDAP 連携ツール環境設定] の順にクリックします。

2 各項目を設定して、[次へ] をクリックします。



①ホスト名

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 形式で入力することをお勧めします。FQDN 形式で入力しないと、LDAP サーバに接続されないことがあります。

②ポート

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ことがあります。

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。

🔗 9 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：anonymous

認証方法によって、アルゴリズムごとの設定、認証ユーザー 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	設定	認証ユーザー 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

Digest-MD5 または Kerberos V5 を選択するときは、以下を参照して設定してください。

🔗 10 ページ「認証方法の設定」

⑥接続ユーザーDN

LDAP サーバにアクセスするときのユーザー ID を入力します。[anonymous] を選択したときは設定不要です。

⑦パスワード

LDAPサーバにアクセスするときの接続ユーザーDNのパスワードを入力します。

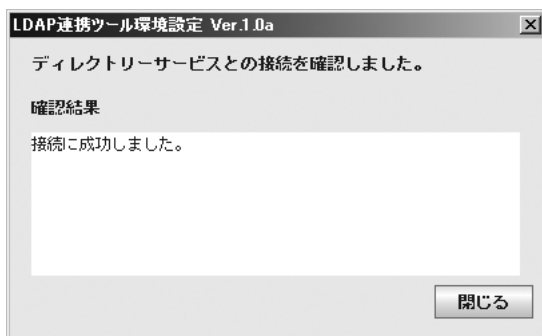
[anonymous] を選択したときは設定不要です。

⑧テスト接続

入力した項目で実際に LDAP サーバに試験的に接続します。

クリックすると接続結果の画面を表示します。接続に失敗したときは、エラーコードも表示します。

成功例：



失敗例：



ログファイルが以下のフォルダに生成されます。
ProgramFiles\EpsonNet PrintDirector\files

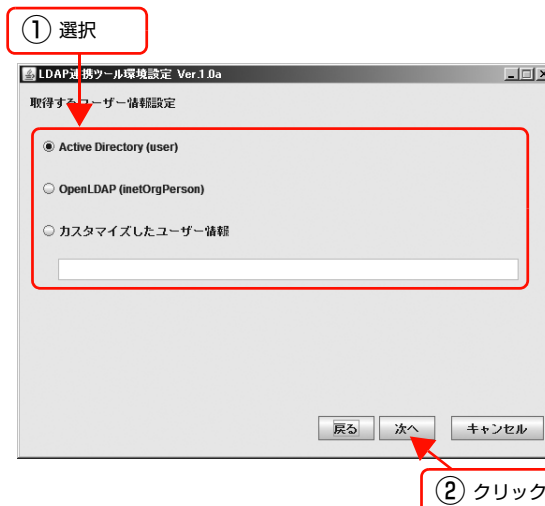
ログファイルには、処理結果のステータスとエラーの詳細が記録されます。ステータスは以下の 3 種類が記録されます。

ERROR	処理が続行できない問題が発生しました。
WARN	処理は続行できますが、データや処理内容に問題があります。
INFO	正常に処理されました。

3 LDAPサーバから取得するユーザーの種類を選択して、[次へ] をクリックします。

ユーザー情報の種類をカスタマイズしているときは、[カスタマイズしたユーザー情報] を選択して、情報（例：myUserPerson）を入力してください。

入力可能文字列は、英数字と記号（ハイフン (-)、セミコロン (;)、ピリオド (.)）です。

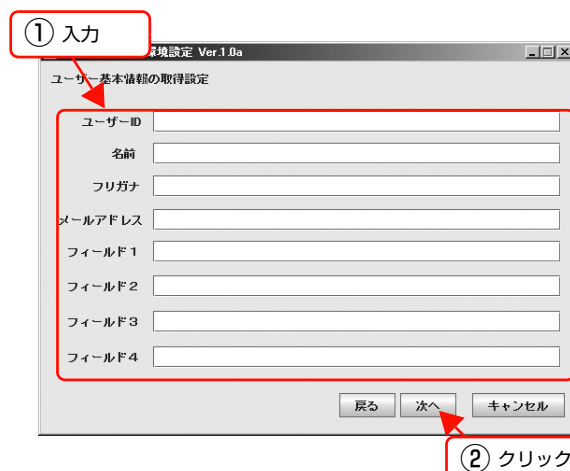


4 Offrio SynergyWare PrintDirector の属性にLDAPサーバ側のユーザー情報の属性をマッピングします。

各項目にユーザー情報の属性を入力して、[次へ] をクリックします。

入力可能な文字は次の通りです。

ユーザー ID	<ul style="list-style-type: none"> 英数字 記号（ハイフン (-)、セミコロン (;)、ピリオド (.)） PrintDirector は、ユーザー ID を重複しない値として管理し、マッピングします。
名前 フリガナ メールアドレス フィールド X	<ul style="list-style-type: none"> 英数字 記号（ハイフン (-)、セミコロン (;)、ピリオド (.)） 空文字

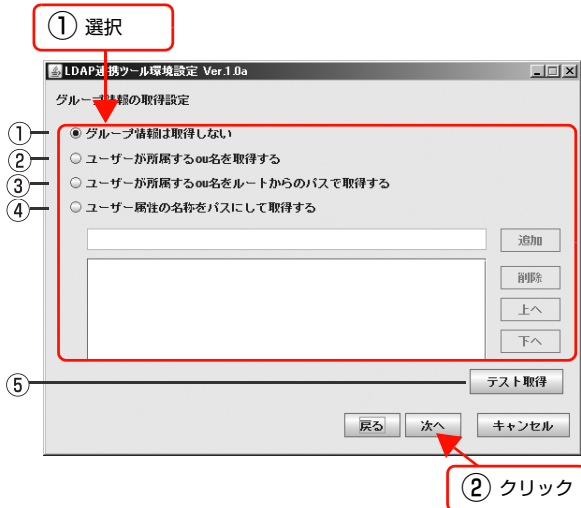


5 Offirio SynergyWare PrintDirector のグループ情報をLDAPサーバ側のどの情報から取得するか設定します。

各項目にユーザー情報の属性を入力して、[次へ] をクリックします。

参考

[ベース DN] で指定したドメインに対して、情報を検索します。サブドメインの情報は検索しません。



① グループ情報は取得しない

新規に取得したユーザーは全体グループに登録します。既存のユーザーは現在のグループ情報のまま変更しません。

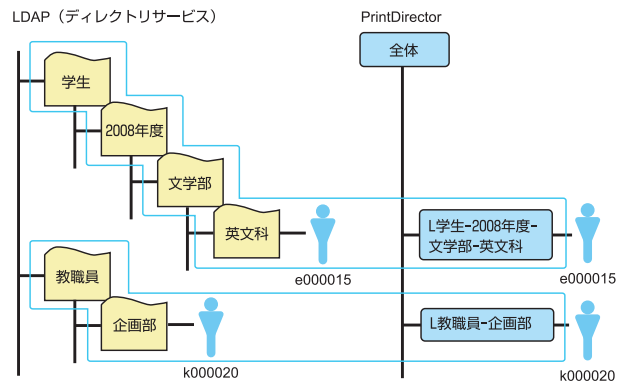
② ユーザーが所属する ou 名を取得する

LDAP 情報から自動生成されたグループ名と手動で作成したグループ名を識別できるようにするため、ユーザーが所属する ou 名の先頭に「L」を付けて、Offirio SynergyWare PrintDirector のグループ名として取得します (例: L 総務部)。

新規に登録したユーザーは全体グループと取得したグループに登録します。既存のユーザーはグループの所属を変更します。

③ ユーザーが所属する ou 名のルートからの名称をつなげて取得する

グループ情報のツリーのルートからユーザーが所属する ou 名までをハイフン (-) でつなげて先頭に「L」を付けて、Offirio SynergyWare PrintDirector のグループ名として取得します (例: LXX 事業部 - 総務部)。新規に登録したユーザーは全体グループと取得したグループに登録します。既存のユーザーはグループの所属を変更します。



参考

ou ツリーのルートから最大 15 のグループ情報を取得します。

④ ユーザー属性から名称をつなげて取得する

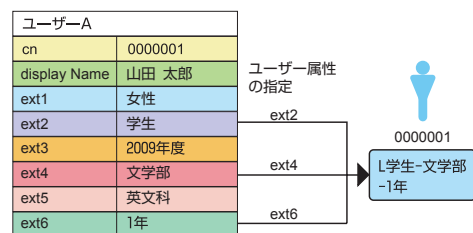
ユーザー属性を任意に指定し、取得したユーザー属性をハイフン (-) でつなげて先頭に「L」を付けて、Offirio SynergyWare PrintDirector のグループ名として取得します (例: LXX 事業部 - 総務部)。

最大 5 つまで属性を指定できます。

新規に登録したユーザーは全体グループと取得したグループに登録します。既存のユーザーはグループの所属を変更します。

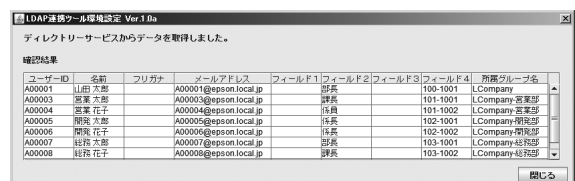
入力欄に取得したい属性を入力し [追加] をクリックします。

LDAP(ディレクトリサービス)



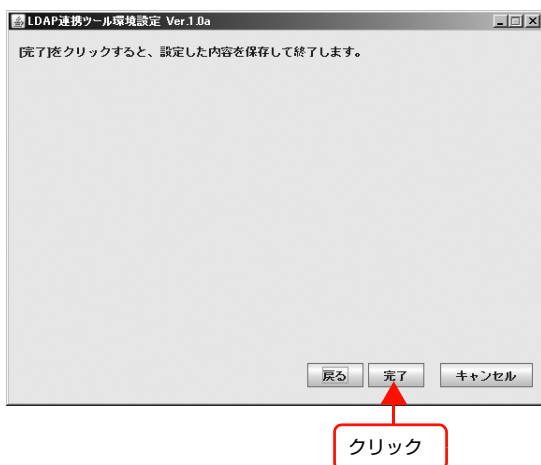
⑤ テスト取得

設定した情報で LDAP サーバから情報を 20 件分取得して、結果を画面で表示します。



6

[完了] をクリックします。

**参考**

- ユーザー ID が重複したときは、後から見つかったユーザー ID のユーザー情報を登録せず、ログファイルに記録します。
- グループ名が 20 文字を超えるときは、グループ名の先頭から 18 文字に加えて、00 から 99 の連番で表示します。

変更前：

L 学生 -2009 年度 - 理工学部 - 環境建築工学科 - 男子

変更後：

L 学生 -2009 年度 - 理工学部 - 環境 00

以上で、LDAP サーバからユーザー情報を取得するための準備ができました。

続いて LDAP 連携ツールで Offirio SynergyWare PrintDirector にユーザー情報の取り込みを実行します。

暗号化通信(SSL / StartTLS)

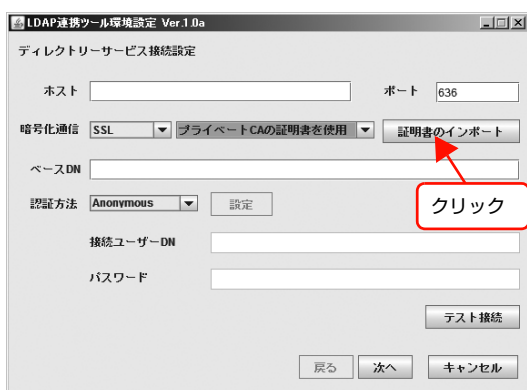
SSL または StartTLS を選択した場合は、パブリック CA (公的な認証機関) が発行した証明書を使用するか、プライベート CA 発行の証明書を使用するかを指定します。プライベート CA 発行の証明書を使用する場合は、CA 証明書またはサーバ証明書をインポートする必要があります。X.509DER 形式、X.509PEM 形式の CA 証明書またはサーバ証明書のファイルをインポートしてください。

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。



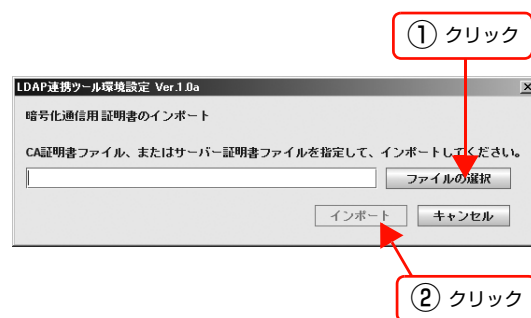
「パブリック CA の証明書を使用」を選択した場合は、JRE (Java Runtime Environment) に標準添付されるパブリック CA の証明書が使用されます。「プライベート CA の証明書を使用」を選択した場合は、手順 2 へ進みます。

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。
[cacerts] ファイルが以下のフォルダに生成され、その中に証明書がインポートされます。

生成フォルダ：

```
Program Files\EpsonNet\  
EpsonNet Application Server\Tomcat\  
webapps\epsonnet\data\com\epson\epso  
nnet\ldaptools\config
```

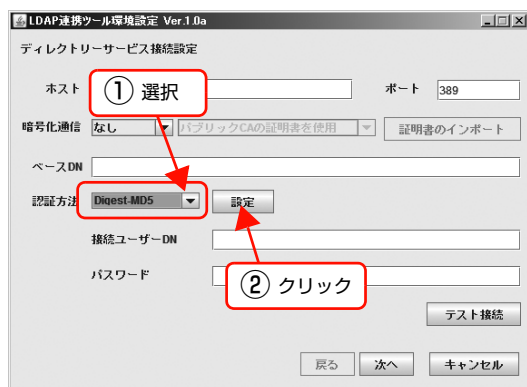
以上で終了です。

認証方法の設定

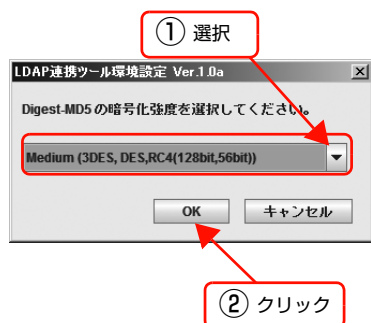
認証方法によって、次の設定が必要です。

Digest-MD5 の場合

- 1 認証方法に [Digest-MD5] を選択して、[設定] をクリックします。



- 2 暗号強度を選択して、[OK] をクリックします。
暗号強度を選択します。
Low / Medium / High (初期設定 : Medium)

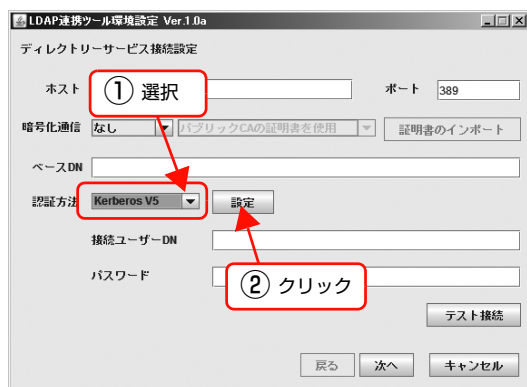


「ディレクトリサービス接続設定」画面に戻ります。

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。

- 1 認証方法に [Kerberos V5] を選択して、[設定] をクリックします。

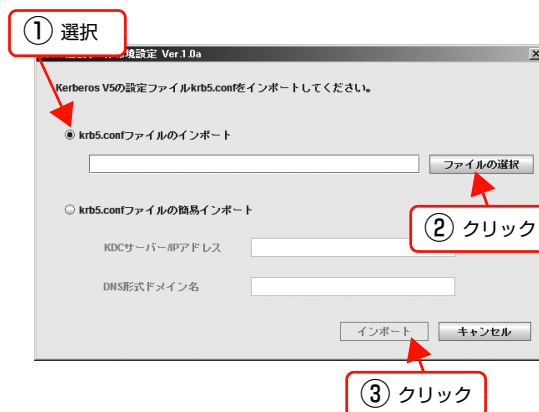


- 2 Kerberos 認証サーバ (KDC サーバ) の指定に関する krb5.conf ファイルをインポートします。

• 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ときに設定します。

[ファイルの選択] をクリックして、krb5.conf ファイルを選択し、[インポート] をクリックします。



• krb5.conf ファイルの簡易インポート

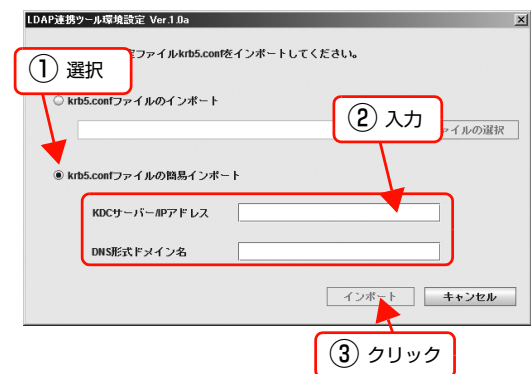
簡易的に krb5.conf ファイルを生成して、そのファイルをインポートするときに設定します。

KDC サーバ名 / IP アドレスと DNS 形式ドメイン名を入力して、[インポート] をクリックします。

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



「ディレクトリサービス接続設定」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。

以上で終了です。

ユーザー情報の取り込みと更新の実行

LDAP サーバから Offirio SynergyWare PrintDirector にユーザー情報を取り込みます。

手順は Windows Server 2003 を例に説明しています。

!重要

連携ツールを実行すると指定した条件で自動的にユーザー情報の取得とグループの作成をします。

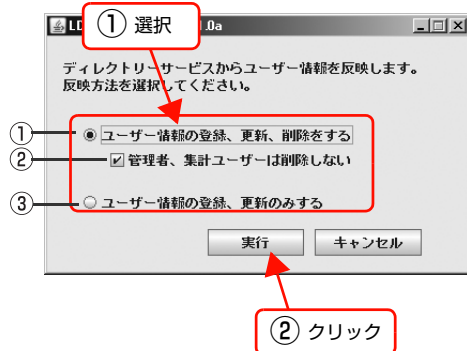
グループの作成方法を誤ると、意図しないユーザーグループの設定がされる可能性がありますので、十分に設定内容を確認の上、実行してください。

PrintDirector が以下の状態のときは、ユーザー情報の取り込みと更新をしないでください。

- * 印刷制限の運用時間帯
- * 印刷制限の設定内容変更中
- * ユーザー情報の変更中
- * エクスポートインポートツール実行中

1 [スタート] - [プログラム] (または [すべてのプログラム]) - [EpsonNet] - [PrintDirector] - [Tools] - [LDAP 連携ツール] の順にクリックします。

2 更新方法を選択して、[実行] をクリックします。



①ユーザー情報の登録、更新、削除を行う

LDAP サーバ側のユーザー情報に同期して、Offirio SynergyWare PrintDirector 側のユーザー情報を登録、更新、削除します。

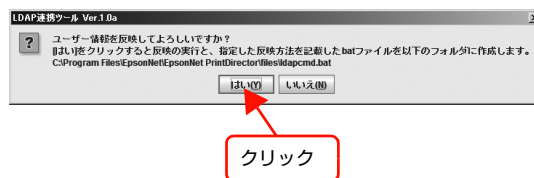
②管理者、集計ユーザーは削除しない

チェックを付けるとユーザー情報を削除する際に、Offirio SynergyWare PrintDirector に登録してある管理ユーザー、集計ユーザーを削除しません。チェックを付けて実行することをお勧めします。

③ユーザー情報の登録、更新のみを行う

LDAP サーバ側のユーザー情報に合わせて、Offirio SynergyWare PrintDirector 側のユーザー情報を登録、更新します。ユーザーの削除はしません。

3 画面の内容を確認して、[はい] をクリックします。

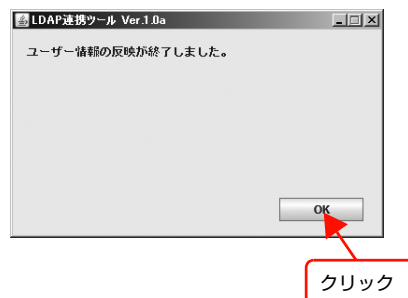


参考

bat ファイルには、今回の設定値が記述されています。今回の設定と同条件で定期的に行うなどの際に、OS のタスクスケジューラなどに組み込んで使用してください。

4 [OK] をクリックします。





更新対象となるユーザー数によって、処理に時間がかかることがあります。



以上で終了です。

こんなときは

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
LDAP サーバにアクセスできない	<p> PrintDirector 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。</p> <p>LDAP 連携ツールを使用するには、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 のマニュアルを参照して設定してください。</p> <ul style="list-style-type: none"> • DNS サーバ LDAP サーバの登録（正引き、逆引き） • PrintDirector 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
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	<p> 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。</p> <p>LDAP サーバの設定によっては、LDAP 連携ツール環境設定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。</p> <p>☞ 10 ページ「認証方法の設定」</p>
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。</p> <p>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。</p> <p>また、「Kerberos V5 の認証方法の設定」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")。</p> <p>☞ 10 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、PrintDirector 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 のマニュアル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） • PrintDirector 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> アクセス先の LDAP サーバが Windows Server 2008 のときに、ドメイン機能レベルが Windows Server 2008 になっているか確認してください。</p> <p>アクセス先の Windows Server 2008 の Active Directory のドメイン機能レベルが Windows Server 2008 になっている必要があります。</p> <p>ドメイン機能レベルが Windows Server 2000、もしくは Windows Server 2003 の設定で Kerberos 認証するには、Windows Server 2008 の Active Directory に登録しているユーザーアカウントの設定を変更する必要があります。</p> <p>(1) アクセス先の Windows Server 2008 の [スタート] メニュー - [管理ツール] - [Active Directory ユーザーとコンピュータ] を選択します。</p> <p>(2) [Active Directory ユーザーとコンピュータ] から本ツール「ディレクトリサービス接続設定」画面の [接続ユーザー DN] 項目に指定したユーザーアカウントのプロパティを開きます。</p> <p>☞ 5 ページ「@接続ユーザー DN」</p> <p>(3) プロパティの [アカウント] - [アカウント オプション] の中から [このアカウントに Kerberos DES 暗号化を使う] にチェックを付けます。</p> <p>設定内容の詳細は OS のマニュアルを参照してください。</p>

トラブル状態	対処方法
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。 <small>🔗 9 ページ「暗号化通信 (SSL / StartTLS)」</small></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。 <small>🔗 9 ページ「暗号化通信 (SSL / StartTLS)」</small></p>
StartTLS で通信できない	<p> 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>🔗 9 ページ「暗号化通信 (SSL / StartTLS)」</small></p> <p> LDAP サーバのホスト名を確認してください。 ホスト名を IP アドレスで指定すると、StartTLS で通信できないことがあります。そのときは、ホスト名を FQDN 形式で指定してください。 <small>🔗 5 ページ「環境設定」</small></p>
本ツール「ディレクトリーサービス接続設定」の「暗号化通信」で「パブリック CA 証明書を使用」を選択して暗号化通信しようとしたが、LDAP サーバと通信できない	<p> 「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」を選択したときは、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>🔗 9 ページ「暗号化通信 (SSL / StartTLS)」</small></p>
テスト接続やテスト取得実行時に「LDAP: error code49」が表示される	<p> 「ベース DN」 または 「パスワード」 の設定を確認してください。 「ベース DN」または「パスワード」の記述に誤りがあるため、認証に失敗しました。</p>
テスト接続に失敗する	<p> ログファイルを確認してください。 テスト接続の結果をログファイルに書き出します。 ProgramFiles\EpsonNet PrintDirector\files ログファイルを参照して対処してください。 <small>🔗 6 ページ「⑧ テスト接続」：失敗例</small></p>