

構成手順 7: EIMユーザーの作成

1. KDC (鍵配布センター)の構成

2. ユーザーのドメイン参加

3. KDCへiSeries P2を登録

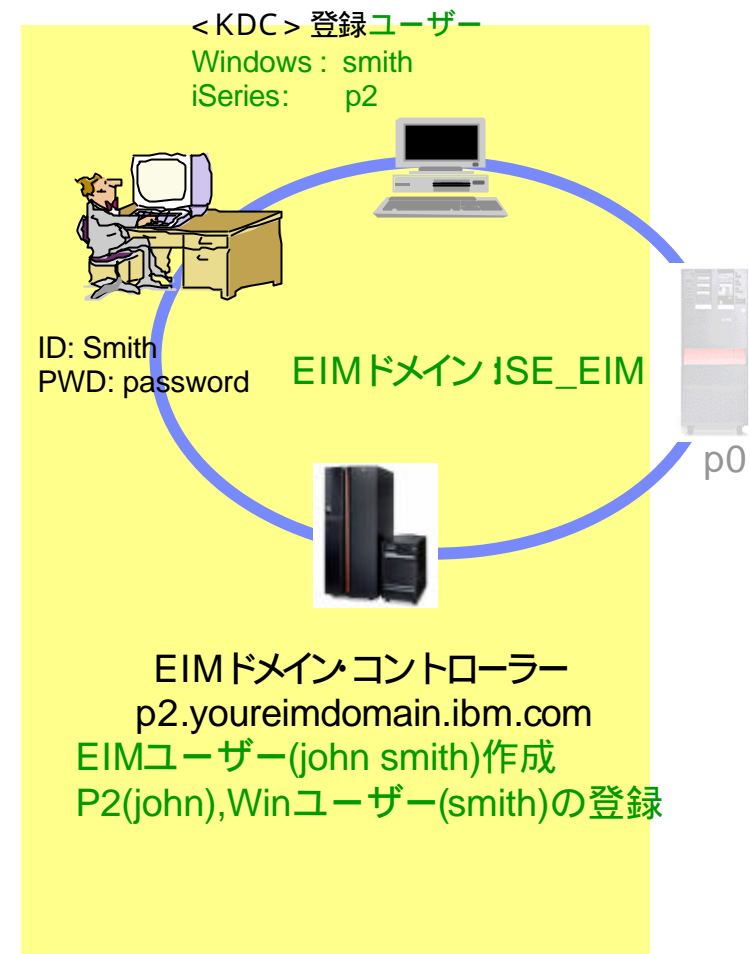
4. P2 でネットワーク認証サービス(NAS)の構成

5. P2で、EIMドメイン・コントローラーの構成

6. 管理対象として5で作成したEIMドメインを登録

→ 7. P2で、EIMユーザーの作成

8. P2で、ユーザーのマッピング情報の登録



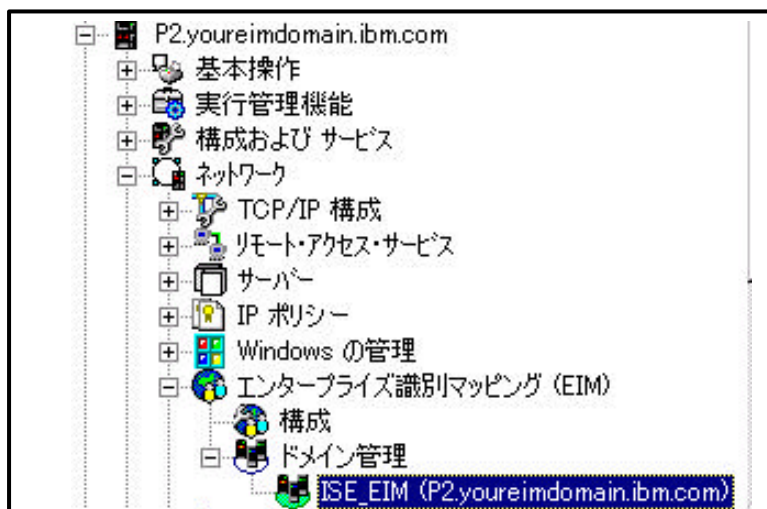
Notes: 構成手順7

ここでは、EIMユーザーを作成します。

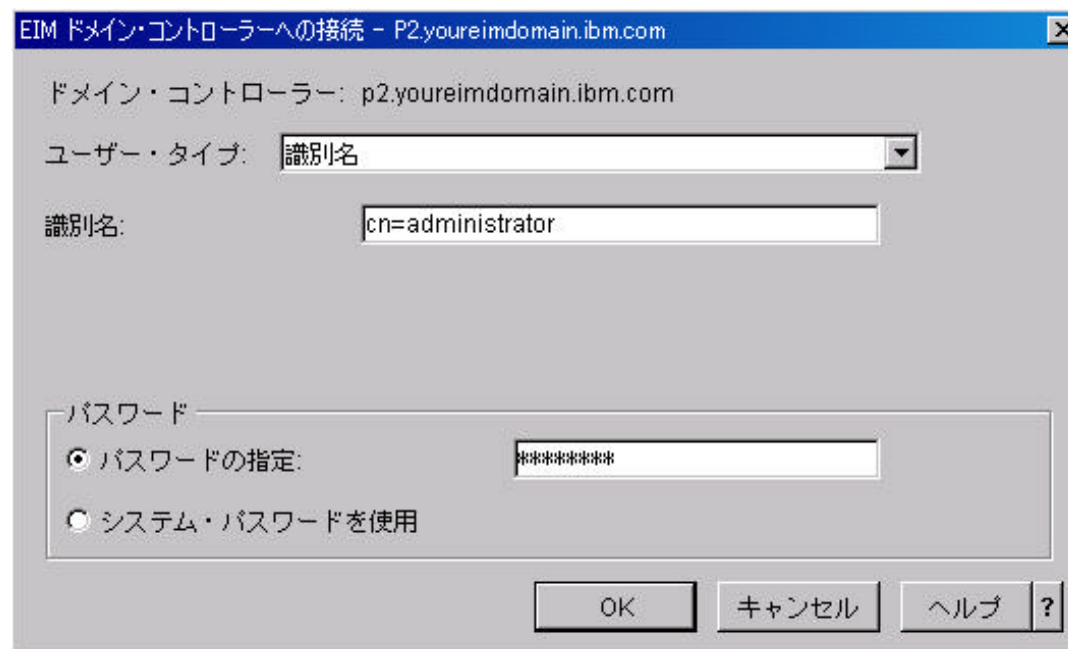
EIMユーザーとは、EIMドメインコントローラーで識別するユーザーです。

このEIMユーザーに対して、各システムに存在するユーザーID(マッピング情報)を登録します。

7. EIMユーザーの新規作成 ステップ1



1. 追加が成功すれば、ドメイン管理の下に追加したEIMドメイン名が表示されます。
2. ドメインをクリックすれば、EIMドメイン・コントローラーへの接続画面が表示されます。
手順5ステップ3で指定したパスワードでサインオン



Notes: 7. EIMユーザーの新規作成 ステップ1

構成手順6で、ドメインの追加が完了すれば、iSeriesナビゲーター上のドメイン管理の下に、ドメインISE_EIMが追加ます。

1. ドメイン管理をクリックします。追加したEIMドメイン名が表示されます。
2. ドメインをクリックすれば、EIMドメイン・コントローラーへの接続画面が表示されます。

EIMユーザー管理の権限が付与されているユーザーでサインオンします。

ここでは、手順ステップ3で指定したパスワードでサインオンします。

(参考)接続画面において

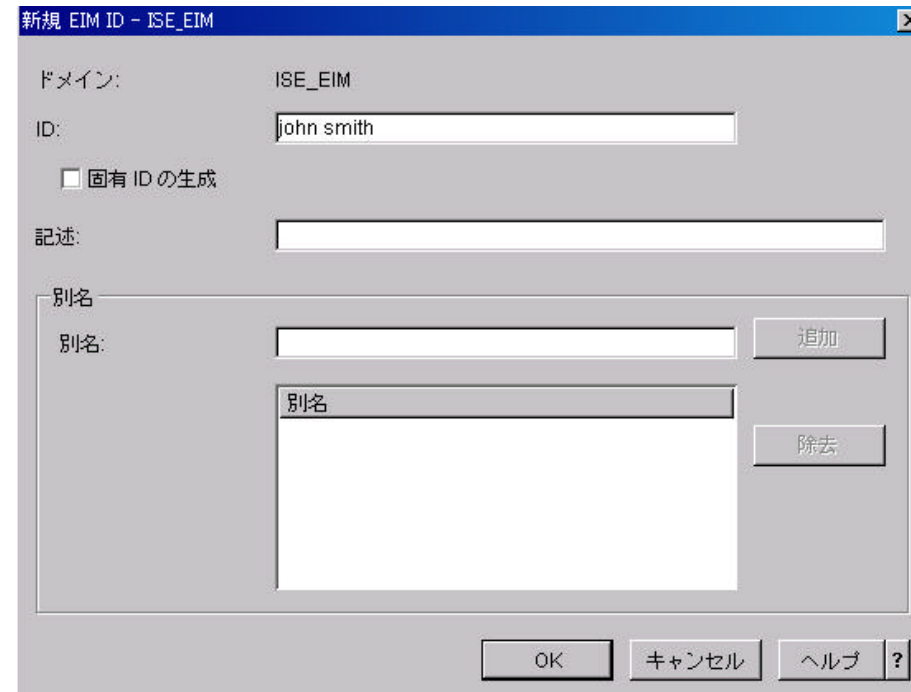
システム・パスワードの使用：サインオンする時に使用したパスワードと同じものを使用する場合に選択します。

7. EIMユーザーの新規作成

ステップ2



3. IDを右クリックし、新規IDを選択。
4. EIMユーザー名を入力。(任意)
(ここでは john smith)

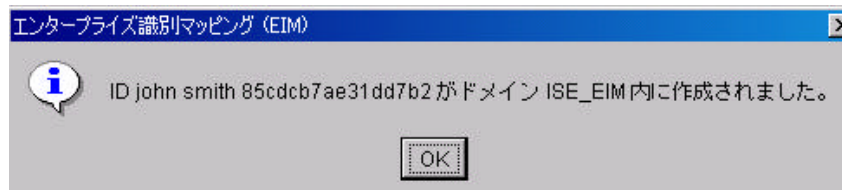


Notes: 7. EIMユーザーの新規作成 ステップ1

3. ドメイン下に表示されるIDを右クリックし、新規IDを選択します。
4. 新規EIM ID画面が表示されます。EIMユーザー名(任意)を入力します。

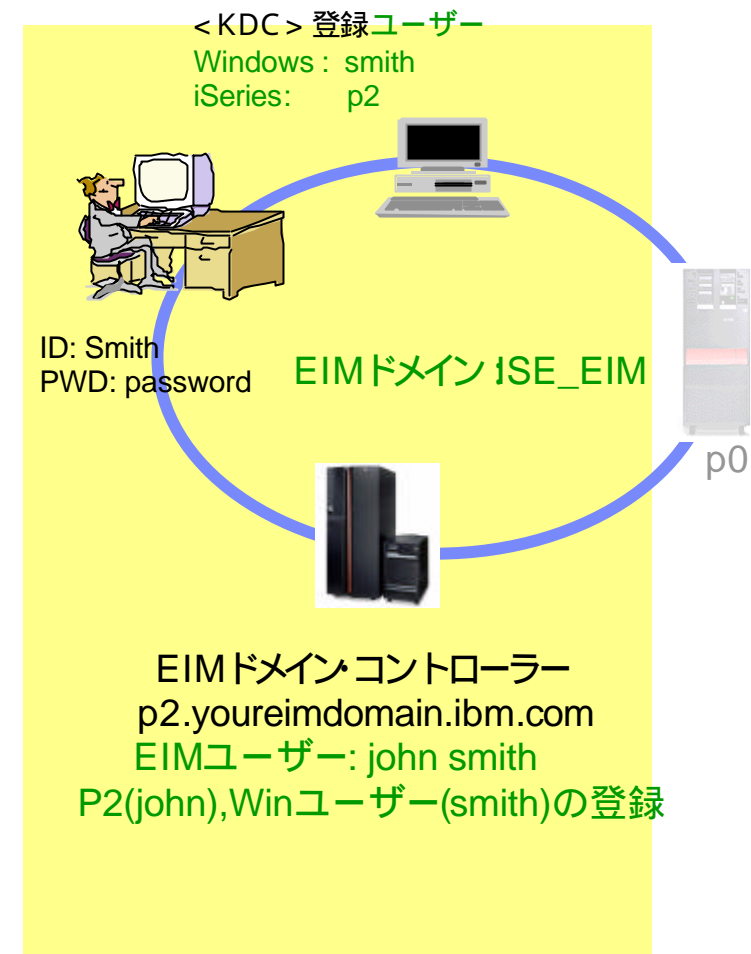
固有IDの生成：

重複する EIM ID がドメインに存在する場合、固有IDを生成することにより区別します。
ドメインに重複するID が存在している時には、このオプションを選択する必要があります。



構成手順 8: ユーザーのマッピング情報の登録

1. KDC (鍵配布センター)の構成
2. ユーザーのドメイン参加
3. KDCへiSeries P2を登録
4. P2 でネットワーク認証サービス(NAS)の構成
5. P2で、EIMドメイン・コントローラーの構成
6. 管理対象として5で作成したEIMドメインを登録
7. P2で、EIMユーザーの作成
8. P2で、ユーザーのマッピング情報の登録



Notes: 構成手順8

構成手順7で作成したEIMユーザーに対して、各システムに存在するユーザーID(マッピング情報)を登録します。

ここでは

■ Windowsユーザー : smith

■ P2ユーザー : john

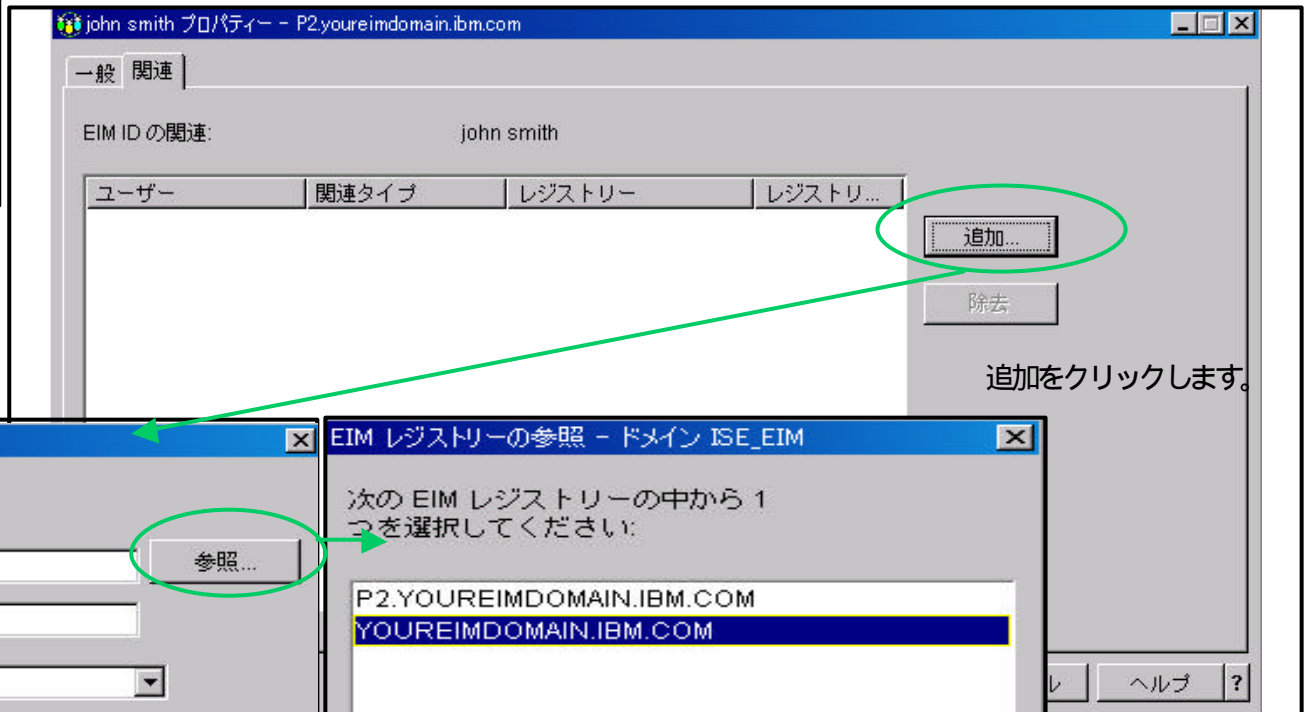
を登録します。

8. ユーザーのマッピング情報の登録 ステップ1

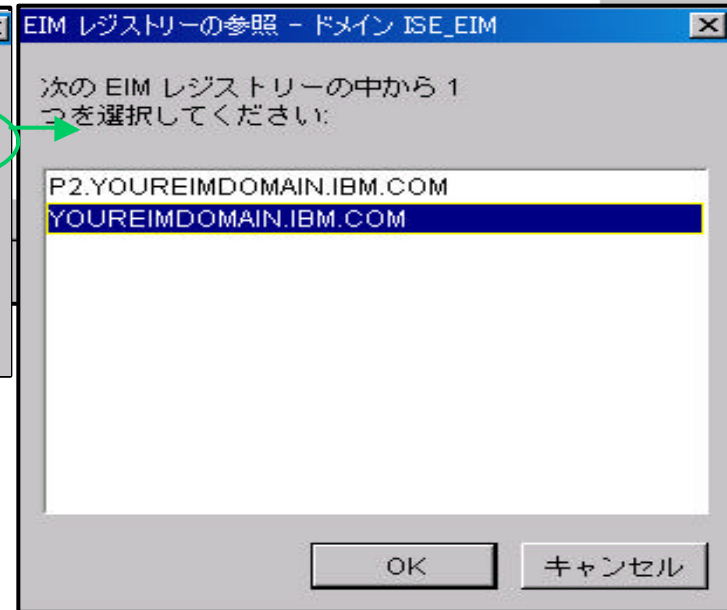
作成したEIMユーザーに、他システムの利用者ID/パスワードを登録します。



1. 特定のEIMユーザー(john smith)を右クリックし、プロパティを選択。
2. 関連タグを開く。
3. 追加をクリック。



追加をクリックします。



4. PCユーザー(Kerberosに登録されているユーザー) smithを登録。
 - レジストリー :Kerberosレジストリー (YOUREIMDOMAIN.IBM.COM)
 - ユーザー :PCサインオン・ユーザー(smith)
 - 関連タイプ :ソース

Notes: 8. ユーザーのマッピング情報の登録 ステップ1

手順7で作成したEIMユーザーに対して、他システムのユーザーID/パスワードを登録します。
ステップ1では、PCユーザーを登録します。

1. IDをクリックし、右画面にEIMユーザーが一覧表示されます。特定のEIMユーザーを右クリックし、プロパティを選択します。
2. プロパティ画面が表示されます。関連タグをクリックします。
3. 追加をクリックします。
4. PCユーザー(Kerberosに登録されているユーザー) smithを登録。
 - レジストリー :Kerberosレジストリー
参照をクリックします。現在登録済みのレジストリーが一覧表示されます。一覧よりレジストリーを選択できます。
 - ユーザー :PCサインオン・ユーザー(smith)
 - 関連タイプ :ソース

(参考)

ターゲット:検索対象となるユーザー

ソース:マッピング検索をかけるもとのユーザー

8. ユーザーのマッピング情報の登録

ステップ2

関連の追加 - john smith

EIM ID : john smith

レジストリー: P2.YOUREIMDOMAIN.IBM.COM

ユーザー: JOHN

関連タイプ: ターゲット

5. p2ユーザー john を登録。
- レジストリー :OS/400 レジストリー (p2.youreimdomain.ibm.com)
 - ユーザー :OS/400 ユーザー(john)
 - 関連タイプ :ターゲット

john smith プロパティ - P2.youreimdomain.ibm.com

一般 関連

EIM ID の関連: john smith

ユーザー	関連タイプ	レジストリー	レジストリー・タイプ
JOHN	ターゲット	P2.YOUREIMDOMAIN.IBM.COM	OS/400
smith	ソース	YOUREIMDOMAIN.IBM.COM	Kerberos - 大文字小文字

OK キャンセル ヘルプ ?

Notes: 構成手順8

ステップ2では、p2ユーザーを登録します。

- p2ユーザー :john を登録。
- レジストリー :OS/400 レジストリー(p2.youreimdomain.ibm.com)
- ユーザー :OS/400 ユーザー(john)
- 関連タイプ :ターゲット

登録が完了すれば、OKをクリックします。

9. EIMの利用

EIMを利用したシングル・サインオンでシステムにアクセスします。
前提：Windowsに、Smithでサインオン。

The screenshot shows the 'P2.youreimdomain.ibm.com プロパティ' (Properties) dialog box. The 'サインオン情報' (Sign-on information) tab is selected. The 'Kerberos プリンシパルを使用、プロンプトなし' (Use Kerberos principal, no prompts) option is selected and circled in green. The 'サインオンのタイムアウト' (Sign-on timeout) is set to 30 seconds. The 'iSeries ナビゲーター' (iSeries Navigator) window is also visible, showing the 'サインオン・ユーザー' (Sign-on user) field with 'John' entered, which is also circled in green.

- 対象システムp2を右クリックし、プロパティを選択
- 接続タグを開く
- Kerberos プリンシパルを使用、プロンプトなし を選択する。
- OKをクリック。

5. サインオン・プロンプトが表示されることなくアクセスされます。
WindowsユーザーSmithが、iSeriesP2ユーザーJOHNとマッピングされているのが分かります。

Notes: 9. EIMの利用

ここでは、iSeriesナビゲーターからシングルサインオンでp2へアクセスします。
iSeriesナビゲーターで、p2への接続プロパティを変更する必要があります。

1. クライアントはWindowsに、ログイン先 :YOUREIMDOMAIN、ユーザー :smith、パスワード :password でサインオンします。
2. iSeriesナビゲーターを立ち上げます。
3. P2.youreimdomain.ibm.comシステムを右クリックし、プロパティを選択します。
4. 接続タグを開き、'Kerberosプリンシパルを使用、プロンプトなし'を選択します。
5. OKをクリックします。
6. iSeriesナビゲーターを一度閉じ、再度立ち上げます。

iSeriesナビゲーターより、P2.youriemdomain.ibm.comをクリックします。

サインオン・プロンプトが表示されることなく p2にアクセスできます。

右画面で、ユーザーsmithでWindowsにサインオンしたにも関わらず、p2ではjohnでサインオンされていることが確認できます。

シングル・サインオン対象システムを追加したい

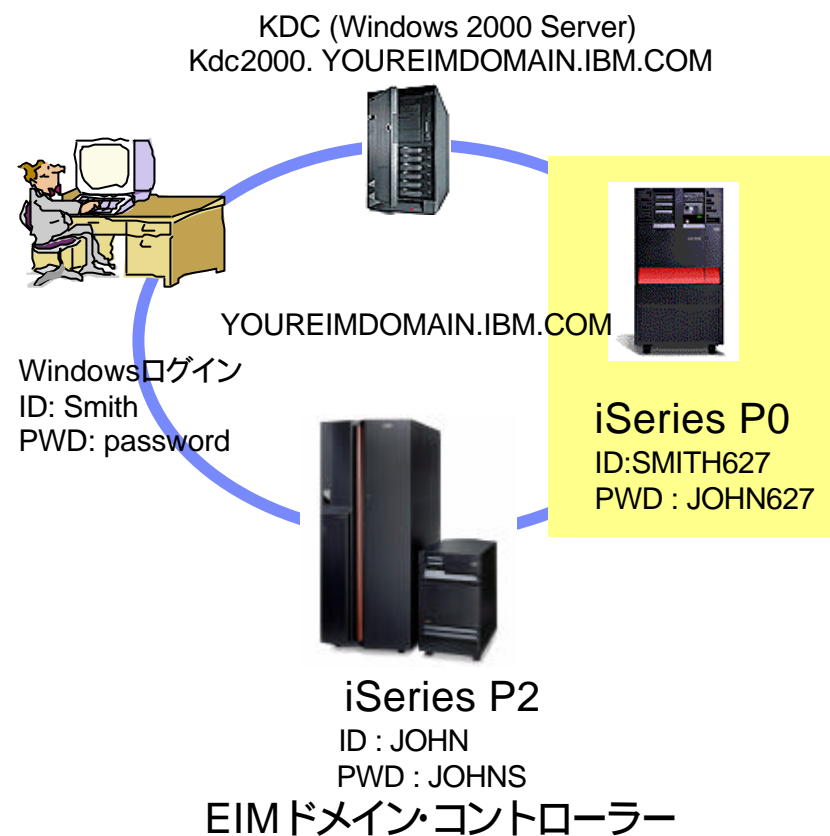
1. KDCへiSeries P0 をユーザーとして登録

→ 2. iSeriesP0でネットワーク認証サービス(NAS)の構成

1, 2 ともに前述と同じ手順。説明は省略。

→ 3. P0で、P2をドメイン・コントローラーとしてEIMの構成

→ 4. P2ドメイン・コントローラーからP0ユーザー情報の登録



Notes: シングル・サインオン対象システムを追加したい

構成手順1-8で、最低限のシングル・サインオン環境は構成完了です。
ここでは、シングル・サインオン対象のシステムP0を追加する場合の手順を紹介します。

シングル・サインオン対象のシステムを追加する手順は以下の通りです。

1. KDCへP0をユーザーとして登録します。
2. P0で、ネットワーク認証サービスを構成します。
3. P0で、EIMを構成します。P2をEIMドメインコントローラーとして設定します。
4. P2のEIMドメインコントローラーから、P0のユーザー情報(smith627)を登録します。

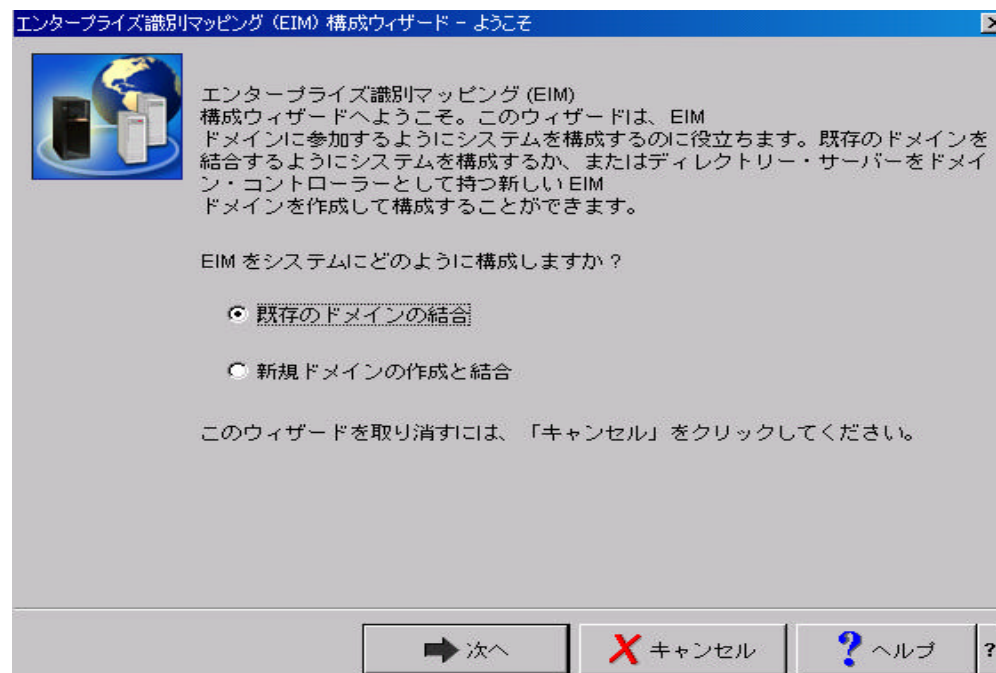
ステップ1, 2は、p2の構成時と同様です。手順3, 4をご参照ください。

対象システムに P0 を追加

ステップ3. P0 EIM構成



1. iSeriesナビゲーターより、P0に対して、ネットワーク
エンタープライズ識別マッピング(EIM) と展開。
2. 構成を右クリックし、構成を選択。
3. ウィザードが開始されます。
既存のドメインの結合 を選択



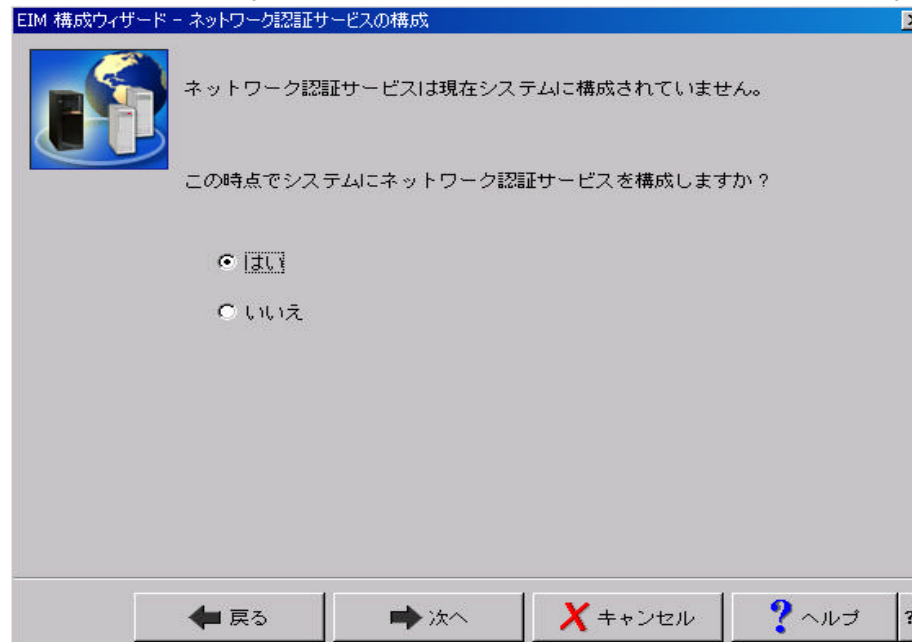
Notes:対象システムに P0 を追加 ステップ3. P0 EIM構成

ステップ1, 2は、p2の構成時と同様です。(手順3, 4をご参照ください。)
ここでは「ステップ3 P0 EIM構成」の手順を説明します。

1. iSeriesナビゲーターより、P0 ネットワーク エンタープライズ識別マッピング(EIM) と展開します。
2. 構成を右クリックし、構成を選択します。
3. ウィザードが開始されます。既存のドメインの結合を選択します。

(参考)

NASが構成されていないとき、ドメイン作成時にNASの構成ができます。
はいを選択すれば、NAS構成ウィザードが開始されます。手順は前述のNAS構成手順と同一です。



対象システムに P0 を追加

ステップ3. P0 EIM構成

EIM 構成ウィザード - ドメイン・コントローラーの指定

EIM ドメイン・コントローラーは、ドメイン内のすべての EIM データへのアクセスを制御します。

システムに結合させたい EIM ドメインのドメイン・コントローラーの名前は？

ドメイン・コントローラー名:

接続

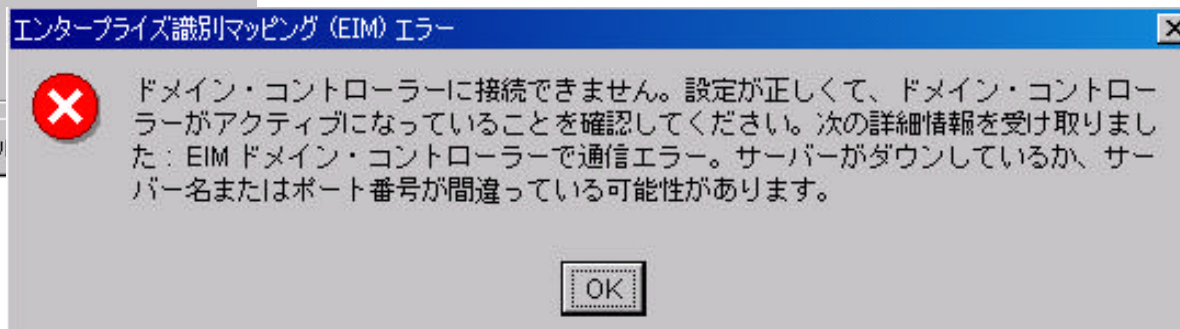
セキュア接続 (SSL または TLS) を使用

ポート:

接続の検査

← 戻る 次へ → ✕ キャンセル

4. ドメイン・コントローラーの指定画面が表示されます。
 - ドメイン・コントローラー名
EIM ドメイン・コントローラーとして構成済みのシステム (p2.youreimdomain.ibm.com)
 - ポート : デフォルトのまま
5. 接続検査をしてエラーが出れば、以下の点を確認してください。
 - 指定したコントローラーのシステム名は正しいか?
 - コントローラーのシステムの名前解決ができていないか?
DNSの指定 or ホスト・テーブルの登録



Notes:対象システムに P0 を追加 ステップ3. P0 EIM構成

4. ドメイン・コントローラーの指定画面が表示されます。
 - ドメイン・コントローラー名
EIMドメイン・コントローラーとして構成済みのシステム(p2.youreimdomain.ibm.com)を指定します。
 - ポート
デフォルトのまま(389)
5. 接続検査をクリックしてEIMドメイン・コントローラーp2への接続を確認します。
接続検査をしてエラーが出れば、以下の点を確認してください。
 - 指定したコントローラーのシステム名は正しいか?
 - コントローラーのシステムの名前解決ができているか? DNSの指定 or ホスト・テーブルの登録

対象システムに P0 を追加

ステップ3. P0 EIM構成

EIM 構成ウィザード - 接続のユーザーを指定

ウィザードがEIM構成を完了するためには、ウィザードが許可ユーザーを使ってドメイン・コントローラーに接続しなければなりません。
EIM 構成ウィザードに使用させたいユーザーは何ですか？

ユーザー・タイプ: 識別名およびパスワード

ユーザー

識別名: cn=administrator

パスワード: *****

確認パスワード: *****

接続の検査

← 戻る → 次へ X キャンセル ? ヘルプ

6. P2のEIM管理ユーザー/パスワードを指定。
7. EIMドメイン(ISE_EIM)を選択。

EIM 構成ウィザード - ドメインの指定

EIMドメインは、ドメイン・コントローラーと一組の参加ユーザー・レジストリーから成ります。このシステムがいったんドメインを結合すれば、管理者はEIMを使用して、このシステムのユーザーからEIMドメイン内の識別名へのマッピングを作成することができます。
このシステムに結合させたいドメインは？

ドメイン:

ドメイン	親 DN
ISE_EIM	

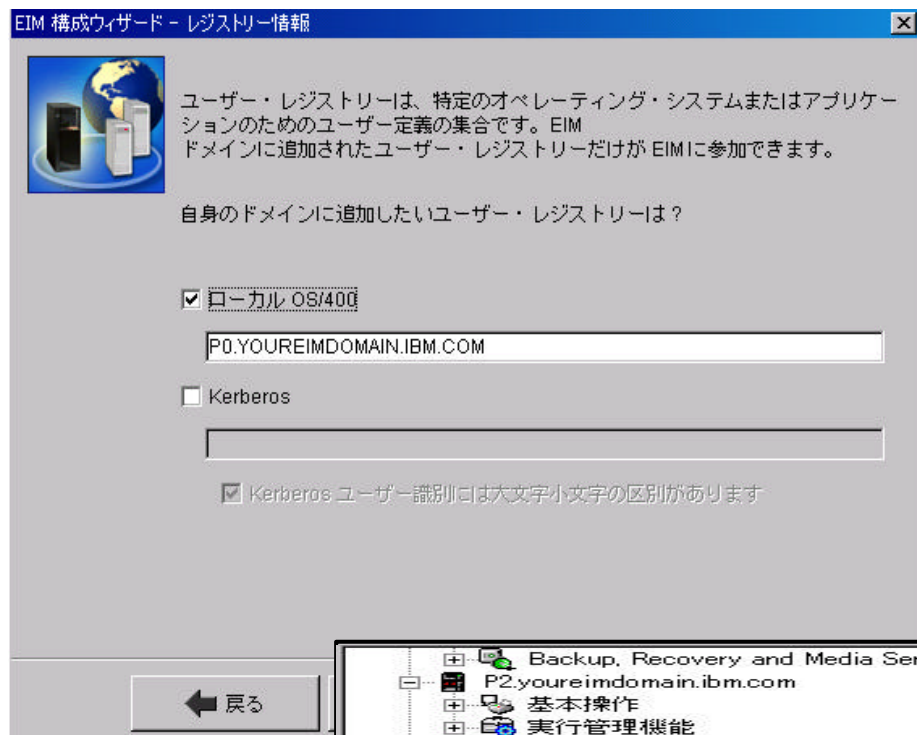
← 戻る → 次へ X キャンセル ? ヘルプ

Notes:対象システムに P0 を追加 ステップ3. P0 EIM構成

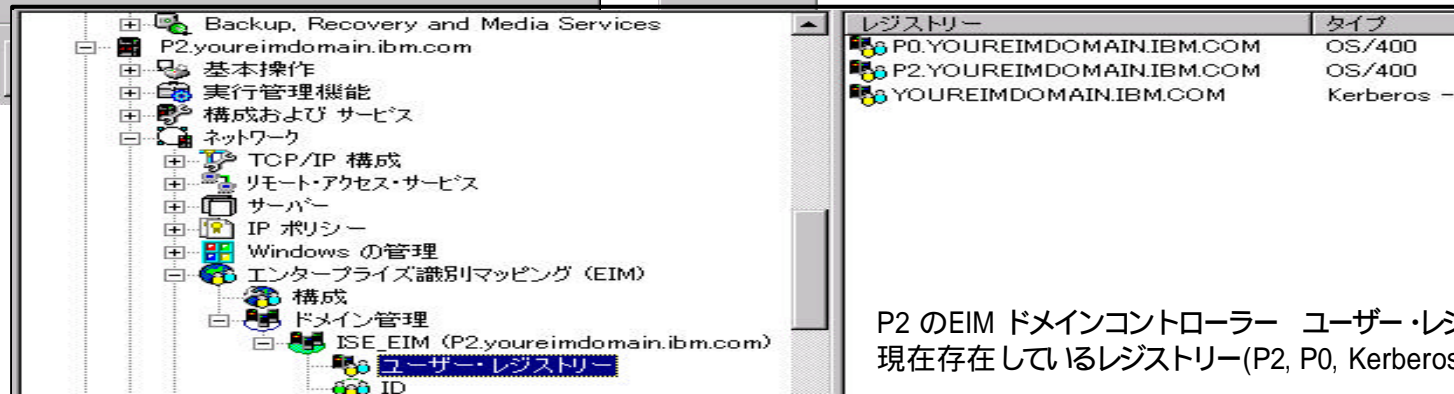
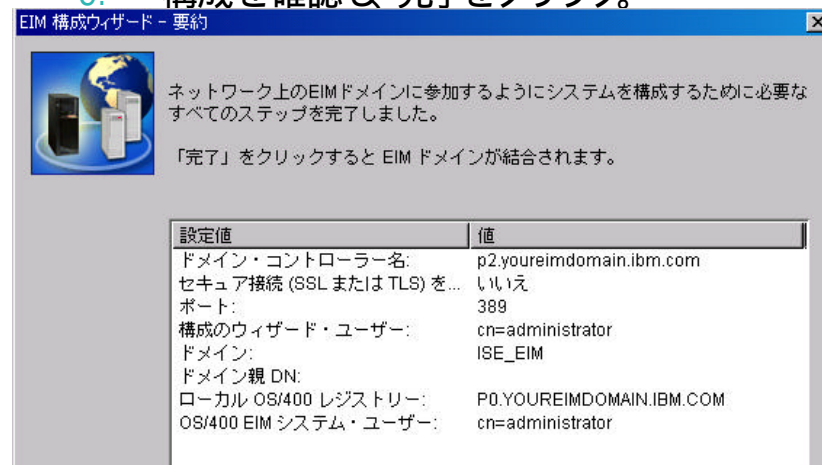
6. P2システムにおいての、LDAP管理権限を持つユーザーとパスワードを入力します。
 7. EIMドメインを指定します。
- すでに構成済みのEIMドメインが一覧表示されます。
ここでは、ISE_EIMを選択します。このEIMドメインは、P2システムで構成済みのものです。

対象システムに P0 を追加

ステップ3. P0 EIM構成



8. レジストリー情報画面では、自身のシステム P0を追加。
(注) Kerberosは、P2のEIM構成時に追加済みであるため、必要なし。
9. 構成を確認し、完了をクリック。



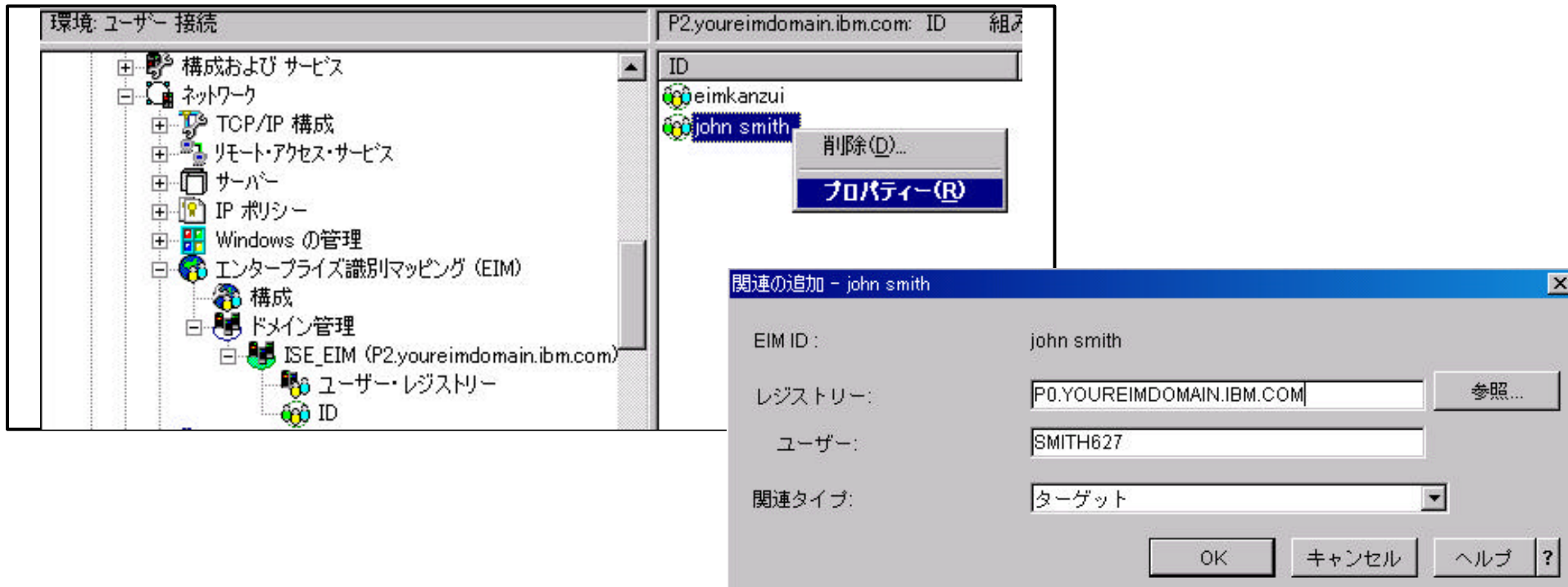
Notes:対象システムに P0 を追加 ステップ3. P0 EIM構成

8. レジストリー情報画面が表示されます。ローカルシステムP0を追加します。
Kerberosは、選択しません。P2のEIM構成時に追加済みです。
9. 構成情報を確認し、完了をクリックします。

構成が完了すれば、EIMドメインコントローラであるp2から、ISE_EIMに追加されていることを確認します。
P2から、ネットワーク EIM ドメイン管理と展開し、ユーザー・レジストリーをクリックします。右画面に、p0が追加されていれば成功です。

対象システムに P0 を追加

ステップ4. P2 ドメイン・コントローラーからP0のユーザー情報を登録



1. P2 ネットワーク エンタープライズ識別マッピング ドメイン管理
2. EIMドメイン名を展開し、IDをクリック。
3. 右画面上のjohn smith を右クリックし、プロパティを選択。
4. 関連の追加画面が表示されれば、以下の情報を入力。
 - レジストリー： 参照からP0を選択
 - ユーザー： SmithのP0上のIDを入力
 - 関連タイプ： ターゲット

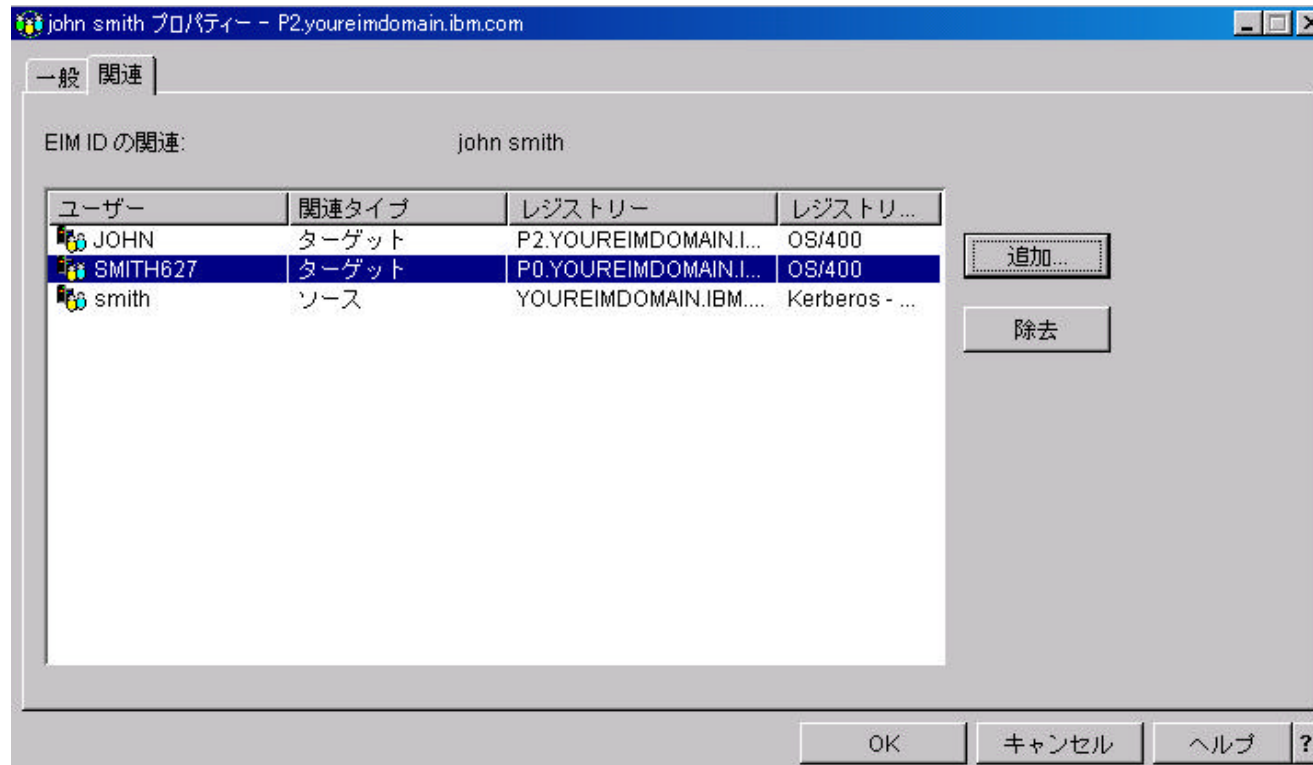
Notes:対象システムに P0 を追加 ステップ4. P0ユーザー登録

1. iSeriesナビゲーターより、P2 ネットワーク エンタープライズ識別マッピング ドメイン管理と展開します。
2. EIMドメイン名を展開し、IDをクリックします。
3. 右画面にEIMユーザーjohn smith が表示されます。john smithを右クリックし、プロパティを選択します。
4. 関連の追加画面が表示されれば、以下の情報を入力します。
 - レジストリー： 参照からP0を選択
 - ユーザー： SmithのP0に存在するユーザーIDを入力
 - 関連タイプ： ターゲット

対象システムに P0 を追加

4. P2からP0のユーザー情報を登録

5. ユーザー情報が更新されていることを確認。

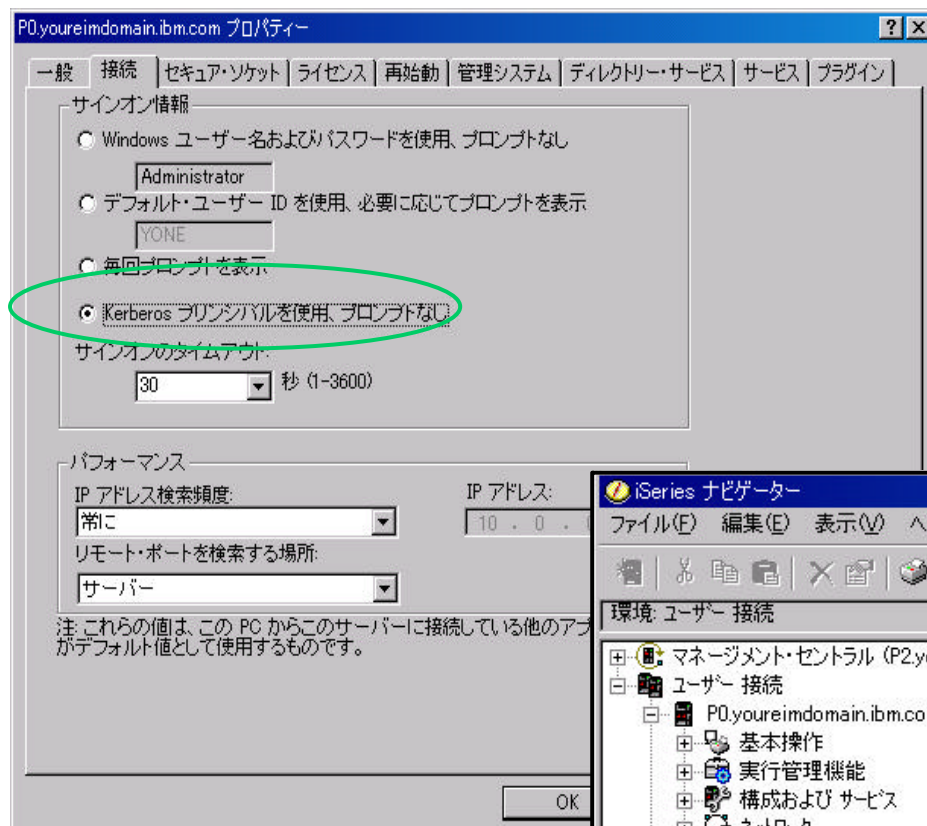


Notes:対象システムに P0 を追加 ステップ4. P0ユーザー登録

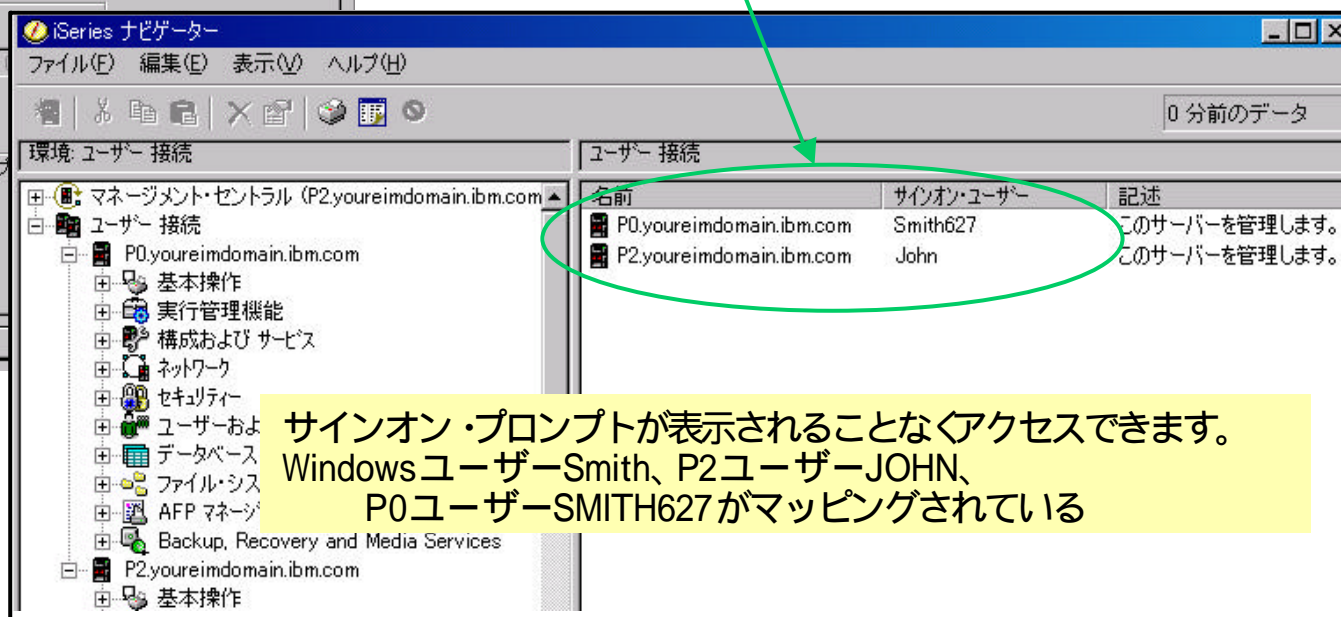
5. OKをクリックすると、john smithにマッピングされるユーザーの一覧が表示されます。ユーザー情報が更新されていることを確認します。

EIMの利用

前提：Windowsに、Smithでサインオン。



1. P0を右クリックし、プロパティを選択
2. 接続タグを開く
3. Kerberos プリンシパルを使用、プロンプトなしを選択する。
4. OKをクリック。
5. P2, P0にアクセス



Notes:EIMの利用

ここでは、iSeriesナビゲーターからシングルサインオンでp0, p2へアクセスします。
iSeriesナビゲーターで、p0への接続プロパティを変更する必要があります。

1. クライアントはWindowsに、ログイン先 :YOUREIMDOMAIN、ユーザー :smith、パスワード :password でサインオンします。
2. iSeriesナビゲーターを立ち上げます。
3. P0.youreimdomain.ibm.comシステムを右クリックし、プロパティを選択します。
4. 接続タグを開き、'Kerberosプリンシパルを使用、プロンプトなし'を選択します。
5. OKをクリックします。
6. iSeriesナビゲーターを一度閉じ、再度立ち上げます。

iSeriesナビゲーターより、P0.youriemdomain.ibm.comをクリックします。

サインオン・プロンプトが表示されることなく p0にアクセスできます。

右画面で、ユーザーsmithでWindowsにサインオンしたにも関わらず、p0ではsmith627でサインオンされていることが確認できます。

まとめ

構成手順：


1. KDC (鍵配布センター)の構成
2. ユーザーのドメイン参加
3. KDCへシステムを登録
4. ネットワーク認証サービス(NAS)の構成
5. EIMドメインの構成
6. EIMユーザーの作成
7. ユーザーのマッピング情報の登録
8. アプリケーションの設定 / 実行

考慮点：

- システム・デザインが重要
- KDCの知識が必要。

(ここでは、Windows2000 ServerのActiveDirectory)

(付録)パラメーターは正しいですか？

パラメーター	KDC	iSeries
krvsrv400/ホスト名 	Ktpass ユーザー・ドメイン名	kinit
ホスト名	(krvsrv400/)ホスト名	iSeriesホスト名のサーバー名 DNS登録済みiSeriesホスト名

参考資料 :

Information Center :

<http://publib.boulder.ibm.com/series/v5r2/ic2962/index.htm>

EIM

LDAP

ネットワーク認証サービス

ITSO W/S Materials :

[2003 Forum:EL06:Use EIM to Enable SSO for your iSeries](#)

Active Directoryとは :

http://www.atmarkit.co.jp/fwin2k/operation/adprimer001/adprimer001_01.html

Windows 2000 Kerberos Authentication :

<http://www.microsoft.com/windows2000/docs/kerberos.doc>