

3. KDCへiSeriesP2の追加 ステップ3

Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-1999 Microsoft Corp.

```
C:¥>ktpass -princ krbsvr400/p2.youreimdomain.ibm.com@YOUREIMDOMAIN.IBM.COM -mapuser p2 -pass password
Successfully mapped krbsvr400/p2 to p2.
Key created.
Account has been set for DES-only encryption.
```

C:¥>

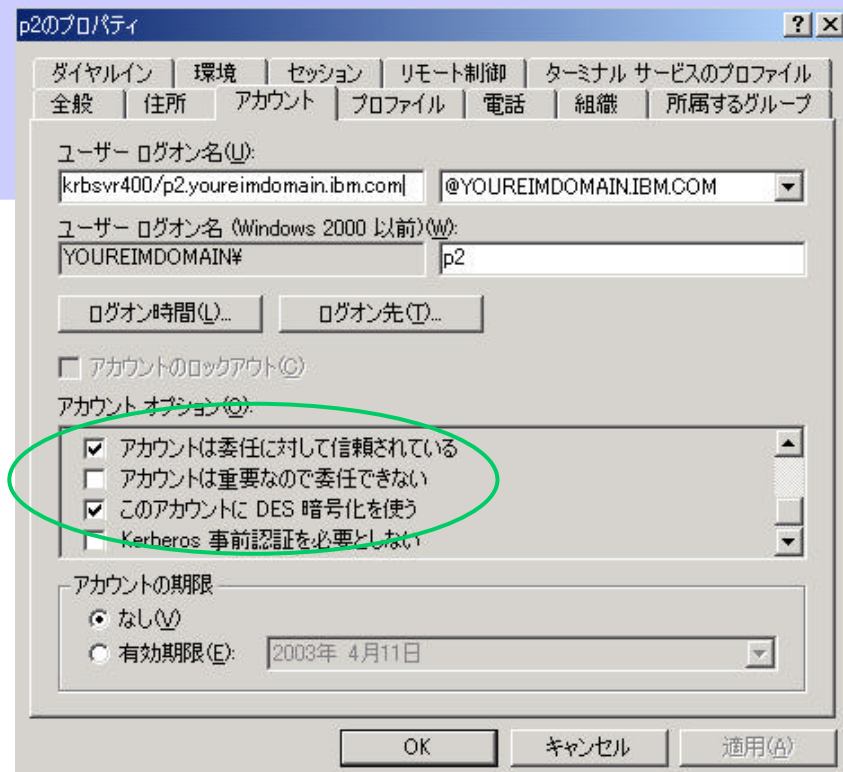
5. コマンド・プロンプトの実行

```
ktpass -princ プリンシパル名@ドメイン名
-mapuser ユーザー名 -pass パスワード
```

プリンシパル名 : krbsvr400/ホスト名
パスワード : 手順2ステップ2で設定したパスワード

6. ユーザーp2の属性変更

「アカウントは委任に対して信頼されている」にチェック



Notes: 3. KDCへiSeriesP2の追加 ステップ3

P2がユーザーとして追加できれば、P2に対してKerberosチケットを発行します。
Windows 2000 Server から Ktpass コマンドを実行します。

5. ktpass -princ krbsvr400/ホスト名@KDCドメイン名 -mapuser XX -pass YY を実行します。
- XXはActiveDirectoryで追加したユーザー名、YYはユーザーp2追加時に設定したパスワードを指定します。
 - ホスト名には、フルシステム名を登録してください。ただし、ドメイン名(p2.youreimdomain.ibm.com)は必須ではありません。
iSeriesコマンド:CFGTCP オプション12で確認できるホスト名のみ登録で構成可能です。
ここでは、krbsvr400/p2.youreimdomain.ibm.com@YOUREIMDOMAIN.IBM.COM -mapuser p2 -pass passwordを実行します。

メッセージ:

Successfully mapped krbsvr400/p2.youreimdomain.ibm.com to p2.

Key created.

Account has been set for DES-only encryption.

が表示されれば、チケット発行が完了です。

6. ユーザーP2の属性を変更します。
1. P2を右クリックし、プロパティを選択します。
 2. アカウントタグ内 アカウントオプション‘アカウントは委任に対して信頼されている’にチェックします。
これは、フロントエンド・システムからバック・エンド・システムへのシングルサインオンを実行する際に必須となります。

構成手順 4: P2でネットワーク認証サービスの構成

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

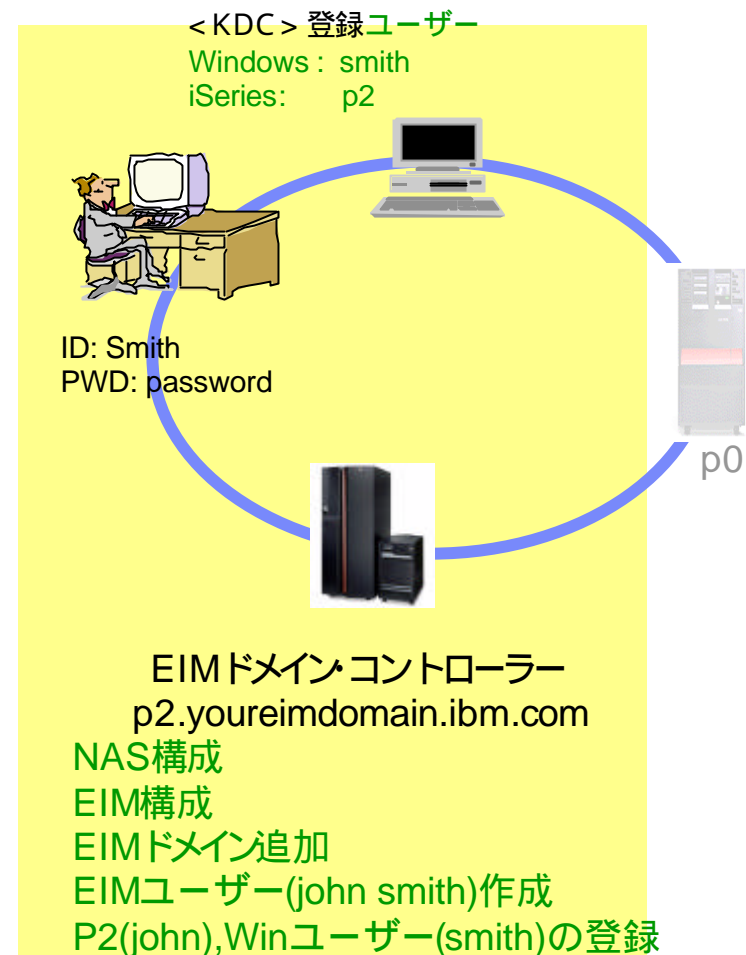
→ 4. P2 でネットワーク認証サービス(NAS)の構成

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

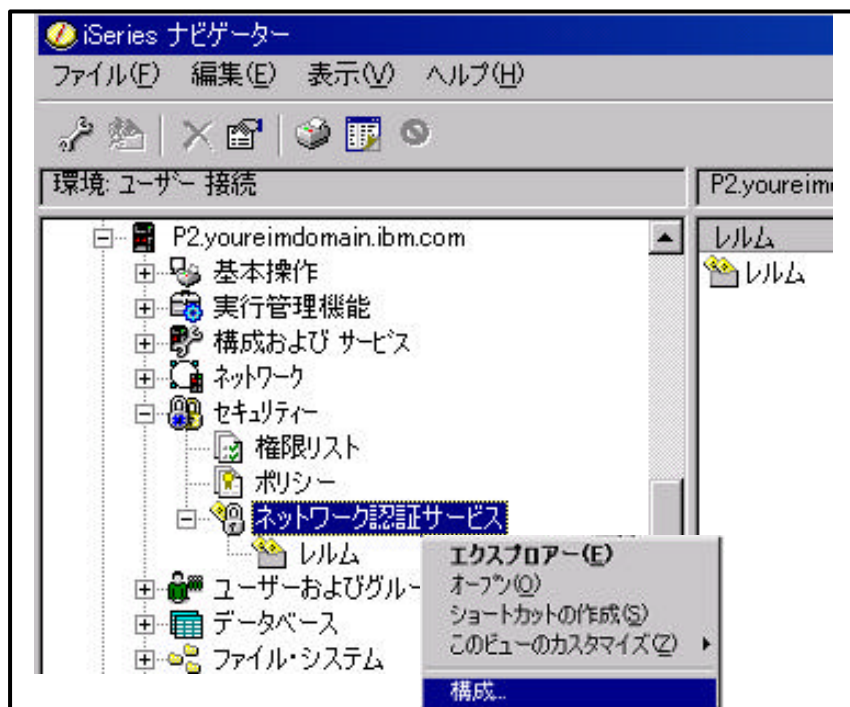
8. P2で、ユーザーのマッピング情報の登録



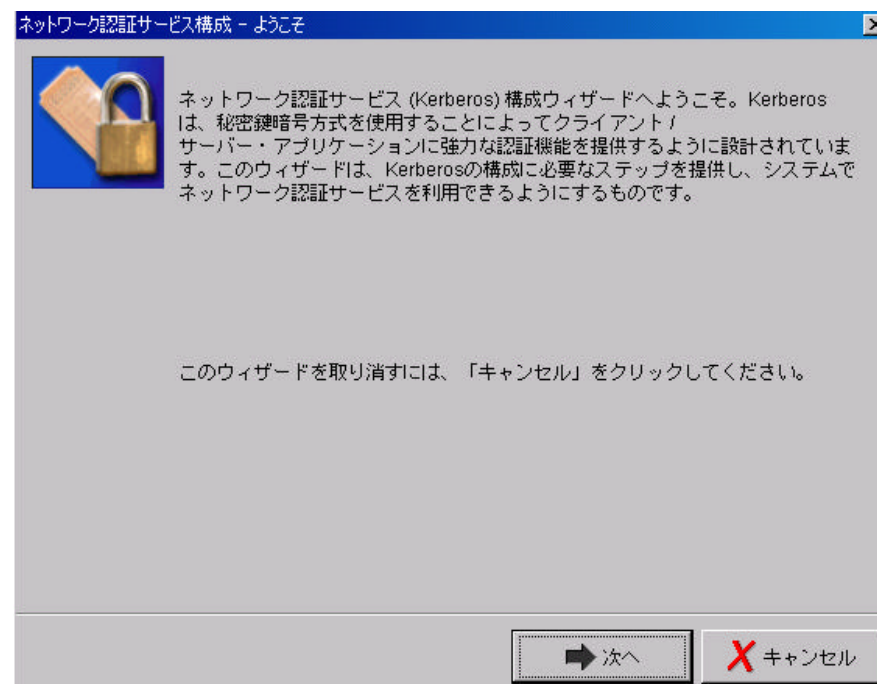
Notes: 構成手順 4

KDCで作成済みのKerberosチケットを取得するために、ネットワーク認証サービスを構成します。
ネットワーク認証サービスをSeriesナビゲーターを利用して、KDCへチケットを取得するための情報を設定します。

4. iSeriesでNASの設定 ステップ1



1. iSeriesナビゲーターより、p2 セキュリティと展開。
2. ネットワーク認証サービスを右クリックし、構成を選択。構成ウィザードが開始される。




Notes: 4. iSeriesでNASの設定 ステップ1

1. iSeriesナビゲーターより、p2 セキュリティと展開します。
2. ネットワーク認証サービスを右クリックし、構成を選択します。
構成ウィザードが開始されます。

4. iSeriesでNASの設定 ステップ2

ネットワーク認証サービス構成 - レルム情報の指定



Kerberos を使用するためには、あるシステムを少なくとも1つの Kerberos レルムの一部であるように構成しなければなりません。このレルムはそのシステムのデフォルト・レルムと呼ばれます。

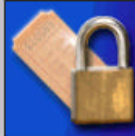
このシステムのデフォルト Kerberos レルムは？

デフォルト・レルム:

← 戻る → 次へ X キャンセル

3. レルム名を入力します。KDCのドメイン名指定。
4. KDC、ポート番号を入力します。
KDC: KDCのコンピューター名を指定
ポート: デフォルトのまま(88)

ネットワーク認証サービス構成 - KDC 情報の指定



Kerberos 鍵配布センター (KDC) には2つの機能があります。レルム内のプリンシパルを認証することと、クライアントが認証に使用するサービス・チケットを Kerberos 使用可能サービスに提供することです。

デフォルト・レルムの KDC の名前？

KDC:

ポート:


← 戻る → 次へ X キャンセル

Notes: 4. iSeriesでNASの設定 ステップ2

3. レルム名を入力します。
レルムとは、KDCが管理する対象の範囲を意味します。
今回は、KDCの範囲としてYOUREIMDOMAIN.IBM.COMというドメイン名を構成しています。
従って、ここではドメイン名を指定します。
4. KDC、ポート番号を入力します。
 - KDC: KDCのコンピューター名(kdc2000.YOUREIMDOMAIN.IBM.COM)
名前解決されることが必須となります。
 - ポートデフォルトのまま(88)

4. iSeriesでNASの設定 ステップ3

ネットワーク認証サービス構成 - パスワード・サーバー情報の指定



Kerberos パスワード・サーバーにより、クライアントは KDC 上の自身のパスワードをリモート側で変更することができます。このパスワード・サーバーは通常、KDC と同じマシン上で実行されます。

デフォルト・レルムに対してパスワード・サーバーを使用するようにこのシステムを構成しますか？

はい

パスワード・サーバー:


ポート:

いいえ

← 戻る 次へ →

5. パスワード・サーバー情報の指定画面で、
・「はい」を選択
・パスワード・サーバーには、KDCのコンピュータ名を入力
6. キータブ項目の作成では、iSeriesKerberos認証にチェックします。

ネットワーク認証サービス構成 - キータブ項目の作成



Kerberos使用可能サービスは、クライアント識別を認証するのにキー・タブ・ファイルを必要とします。キー・タブ・ファイルは、サービス・プリンシパルの長期キーの暗号化バージョンを安全に保管するために使用されます。

次のサービスのどちらについてキー・タブ項目を作成しますか？

iSeries Kerberos 認証

LDAP

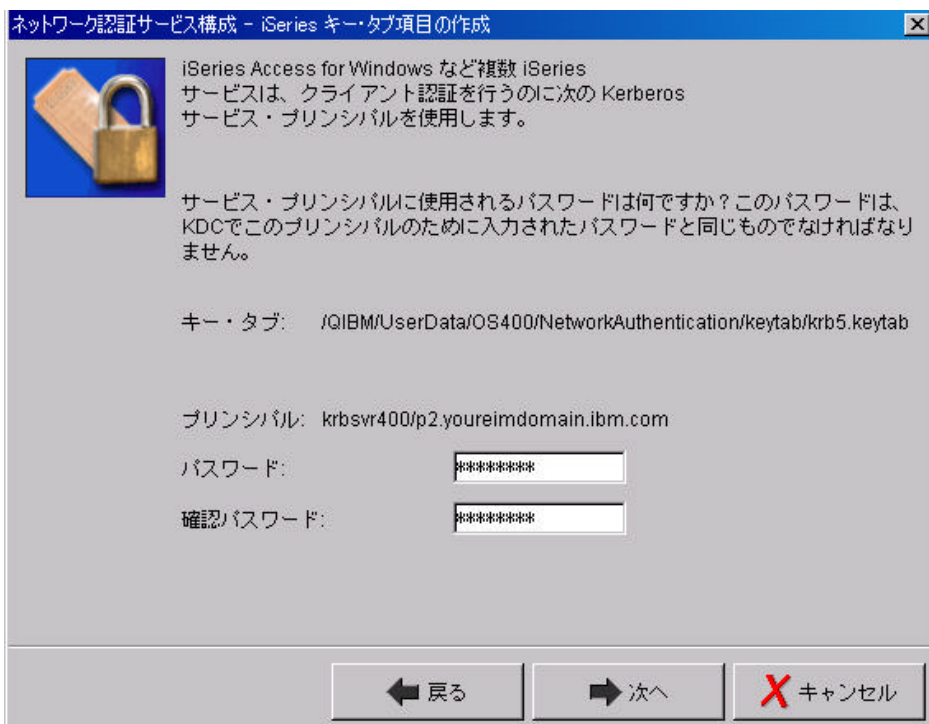
iSeries ネットサーバー

← 戻る 次へ → ✕ キャンセル

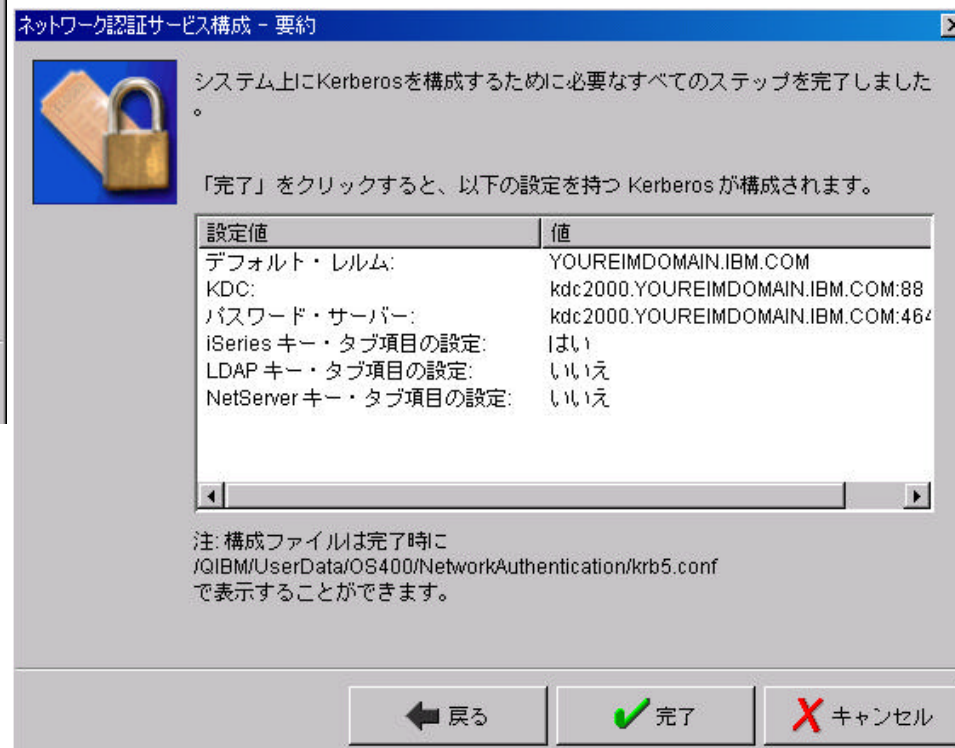
Notes: 4. iSeriesでNASの設定 ステップ3

5. パスワード・サーバー情報の指定画面が表示されます。
 - ・「はい」を選択します。
 - ・パスワード・サーバー：KDCのコンピューター名を入力します。
 - ・ポート:デフォルトのまま(464)
6. キータブ項目の作成では、iSeriesKerberos認証にチェックします。
 - iSeriesKerberos認証
複数のiSeriesサービスを利用する場合選択します。
KDCで指定すべきプリンシパル名：krbsrv400/ホスト名
 - LDAP
LDAPを利用する場合、Kerberosを使用したクライアント認証を必要とする時選択します。
KDCで指定すべきプリンシパル名：LDAP/ホスト名
 - iSeriesネットサーバー
iSeriesネットサーバーを利用する場合、Kerberosを使用したクライアント認証を行なう時選択します。
KDCで指定すべきプリンシパル名：HOST/ホスト名

4. iSeriesでNASの設定 ステップ4



7. KDCで指定したパスワードを入力
8. 要約画面で確認し、完了を選択して、NAS構成ウィザードを終了する。



ウィザードの終了と同時に、以下のオブジェクトが作成されます。

- /QIBM/ UserData/OS400/ NetworkAuthentication内
Krb5.conf(NASの構成ファイル)
- /QIBM/ UserData/OS400/ NetworkAuthentication/ keytab内
Krb5.keytab(キー情報ファイル)

Notes: 4. iSeriesでNASの設定 ステップ4

7. キータブ項目の作成画面が表示されます。
 - パスワード入力欄に、KDCで設定したパスワードを入力します。
 - プリンシパル名が、KDCで実行したktpassコマンドのパラメーターと一致することを確認してください。
一致しない場合、構成手順4 ステップ5 でエラーとなります。
8. 要約画面で確認します。完了を選択し、NAS構成ウィザードを終了します。

ウィザードの終了と同時に、以下のオブジェクトがIFS上に作成されます。

- /QIBM/UserData/OS400/NetworkAuthentication内 Krb5.conf(NASの構成ファイル)
 - /QIBM/UserData/OS400/NetworkAuthentication/keytab内 Krb5.keytab(キー情報ファイル)
- NASの構成を消去したい場合は、上記の2ファイルを削除します。

4. iSeriesでNASの設定 ステップ5

9. 5250からホーム・ディレクトリを作成
CRTDIR '/home/john'
Kinit -kコマンドを実行するOS/400ユーザーのホーム・ディレクトリを作成する。
10. QSHコマンドを実行

QSH コマンド入力

```
$
> keytab list
  キー・テーブル : /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab
  プリンシパル : krbsvr400/p2.youreimdomain.ibm.com@YOUREIMDOMAIN.IBM.COM
  キー・バージョン : 1
  鍵タイプ : 56 ビット DES
  項目タイム・スタンプ : 2003/02/21-11:53:47
```

```
プリンシパル : krbsvr400/p2.youreimdomain.ibm.com @YOUREIMDOMAIN.IBM.COM
  キー・バージョン : 1
  鍵タイプ : 鍵の導出を使用した 56 ビット DES
  項目タイム・スタンプ : 2003/02/21-11:53:47
```

```
プリンシパル : krbsvr400/p2.youreimdomain.ibm.com
  キー・バージョン : 1
  鍵タイプ : 鍵の導出を使用した 168 ビット DES
  項目タイム・スタンプ : 2003/02/21-11:53:47
```

```
$
```

QSHでは、以下を実行します。

> **Keytab list**

iSeriesで設定したNASの内容を確認。

> **kinit -k プリンシパル名**

KDCからチケットを取得する。プリンシパル名は、keytab list で確認したものを指定。

> **klist**

取得したチケットを確認。

QSH コマンド入力

```
$
> kinit -k krbsvr400/p2.youreimdomain.ibm.com @YOUREIMDOMAIN.IBM.COM
$
> klist
  チケット・キャッシュ : FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred_e55f2b60
  デフォルト・プリンシパル : krbsvr400/p2.youreimdomain.ibm.com @YOUREIMDOMAIN.IBM.COM

  サーバー : krbtgt/YOUREIMDOMAIN.IBM.COM@YOUREIMDOMAIN.IBM.COM
  有効 2003/02/21-18:34:48 - 2003/02/22-04:34:48
$
```

Notes:

> kinit -k プリンシパル名 実行時のエラーへの対処

EUVF06007E デフォルトの証明書キャッシュの名前を取得できません。

- ✓ ホーム・ディレクトリが作成済みであるか確認する。

EUVF06014E 初期証明書を取得できません。

状況 0x96c73a9a - セキュリティー・サーバーを見つけられません。

- ✓ iSeriesナビゲーターで設定したNASの構成の見直し。レルム名の太文字小文字の見直し。

EUVF06014E 初期証明書を取得できません。

状況 0x96c73a25 - 時間差が最大クロック・スキューを超えています

- ✓ KDC時刻と同期をとる。システム値QUTCOFFSETに+09:00を設定(日本時刻の場合)。その他、システム値QTIME,QDATEの見直し。デフォルト300秒差を越える場合、エラーとなる。許可範囲は、認証サービスのプロパティより変更可能。

EUVF06014E 初期証明書を取得できません。

状況 0x96c73a06 - クライアント・プリンシパルがセキュリティー・レジストリーに見つかりません。

- ✓ kdcの実行コマンドにミススペルは間違いはないか？
- ✓ iSeriesナビゲーターで設定したNASの構成の見直し。KDC名は間違っていないか？ 大文字小文字の入力は正しいか？

EUVF06016E このパスワードは krb5vr400/p2.YOUREIMDOMAIN.IBM.COM@YOUREIMDOMAI
N.IBM.COM には正しくありません。

- ✓ kdcのコマンド・プロンプトで、実行したコマンドの見直し。大文字小文字の区別。ここでは、p2.youreimdomain.ibm.com(小文字)の間違い

その他チェック・リスト:

- ✓ KDCシステムの名前解決できているか? CFGTCP op10 で、ホストテーブルにiSeriesホスト名とKDCが登録されているか? iSeriesホスト名は、プリンシパル名の/以下を一番目に登録。KDCはフル・ホスト名を登録する。
- ✓ keytab list で確認したプリンシパル名と、KDCで登録したiSeriesユーザー名が一致しているか?

構成手順 5: EIM ドメイン・コントローラーの構成

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

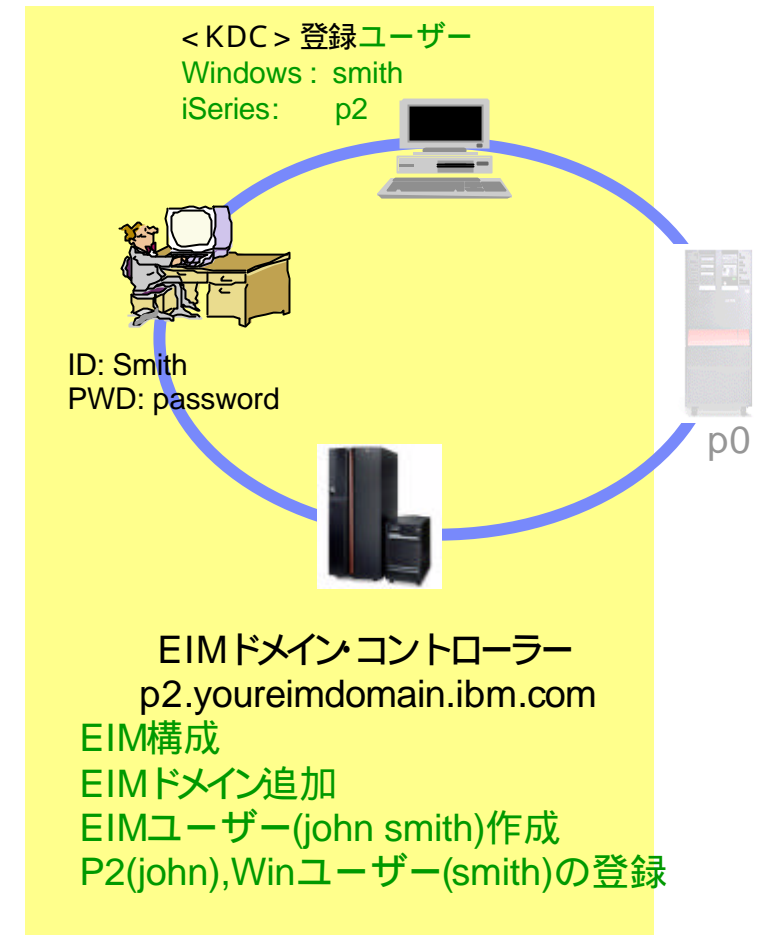
4. P2 でネットワーク認証サービス(NAS)の構成

→ 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

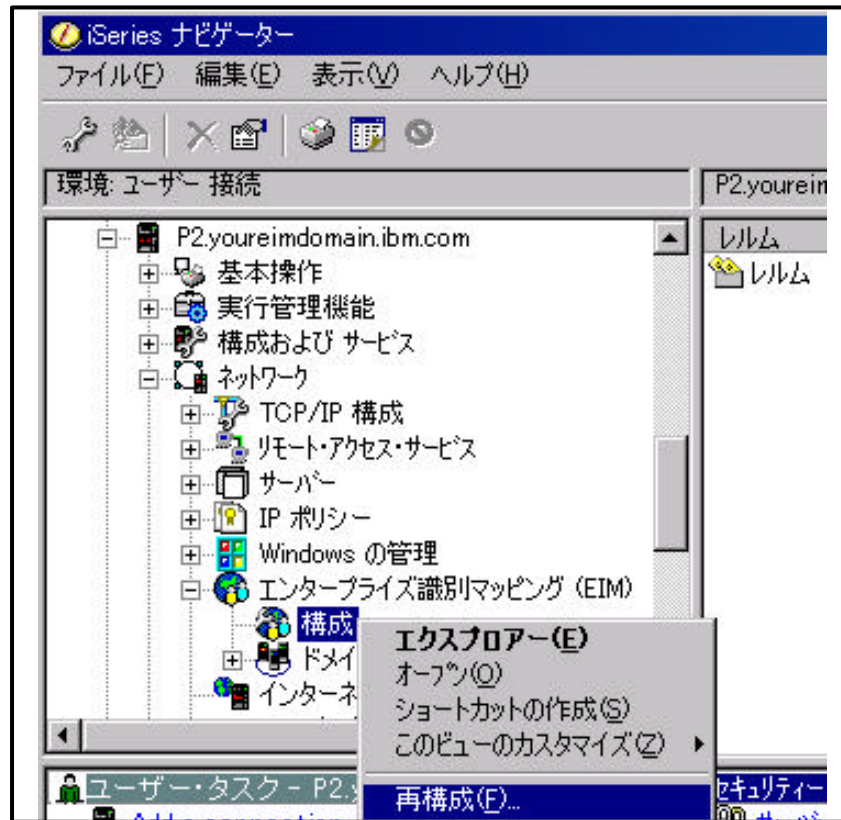


Notes:構成手順 5

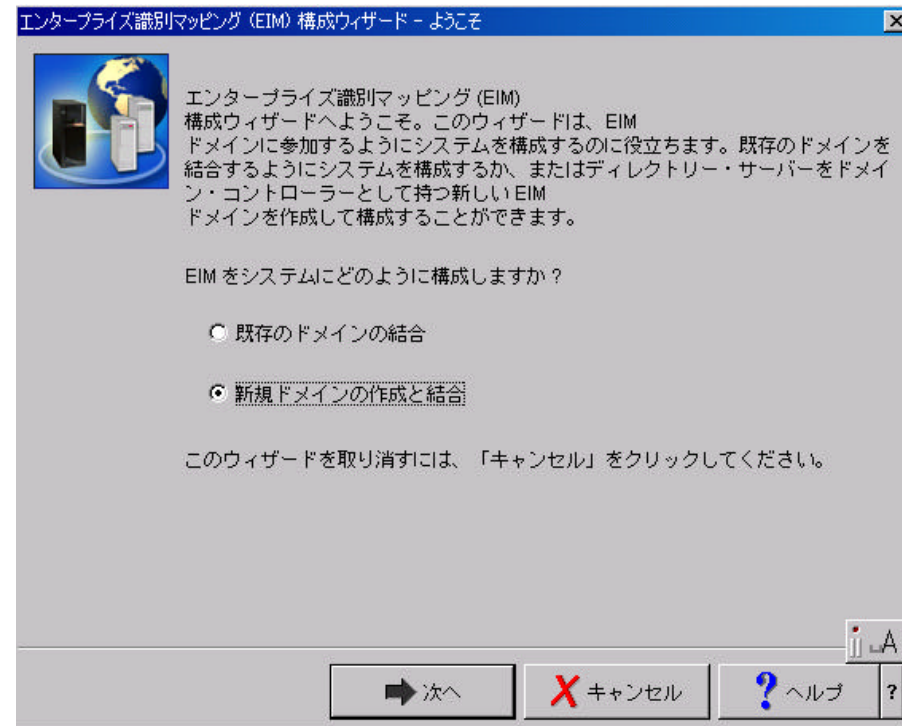
ここでは、ユーザーのマッピングを実施するEIMドメインコントローラーを構成します。

EIMドメインコントローラーの構成は、iSeriesナビゲーターを利用します。

5. EIM ドメイン・コントロールの構成 ステップ1



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と展開。
2. 構成を右クリックし、構成(または再構成)を選択。
初めて構成する場合は「構成」が、
一度構成したことがある場合は「再構成」が表示される。
3. 構成ウィザードが開始されます。新規ドメインの構成と結合を選択。



Notes: 5. EIM ドメイン・コントロールの構成

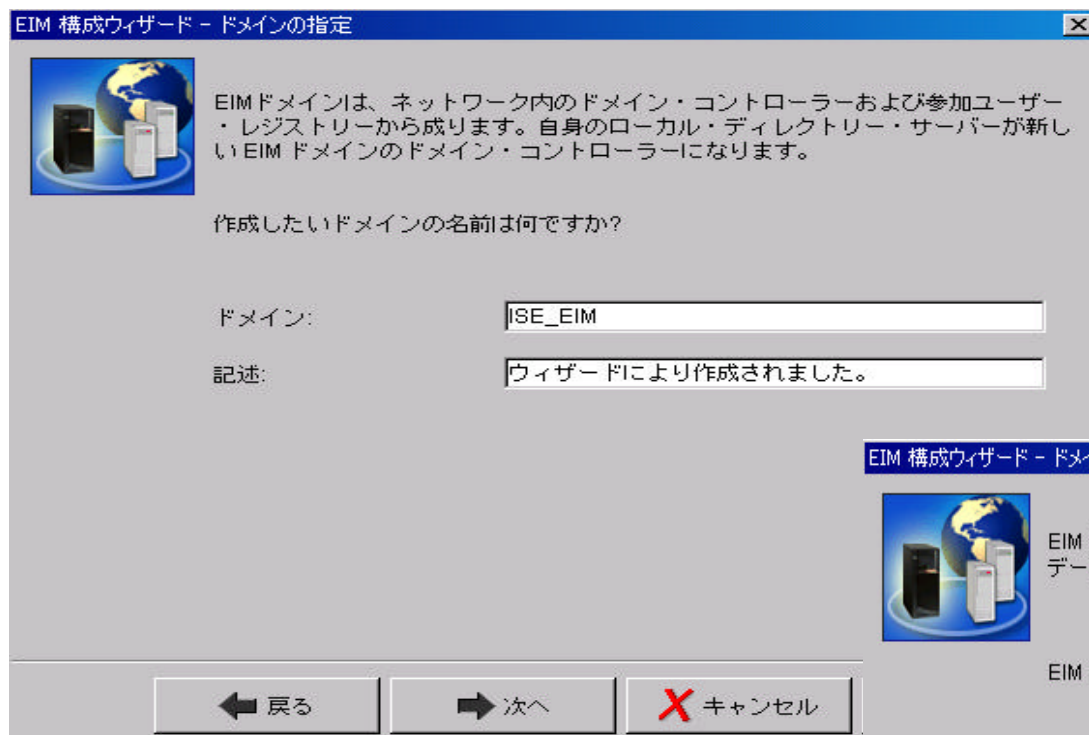
ステップ1

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と展開します。
2. 構成を右クリックし、構成(または再構成)を選択します。
システムに対して、初めてEIM構成をする場合は、「構成」が選択可能です。
一方、一度構成したことがある場合は、「再構成」が表示されます。
3. 構成ウィザードが開始されます。新規ドメインの構成と結合を選択します。

5. EIM ドメイン・コントロールの構成

ステップ2

EIM 構成ウィザード - ドメインの指定



EIM ドメインは、ネットワーク内のドメイン・コントローラーおよび参加ユーザー・レジストリーから成ります。自身のローカル・ディレクトリー・サーバーが新しい EIM ドメインのドメイン・コントローラーになります。

作成したいドメインの名前は何か？

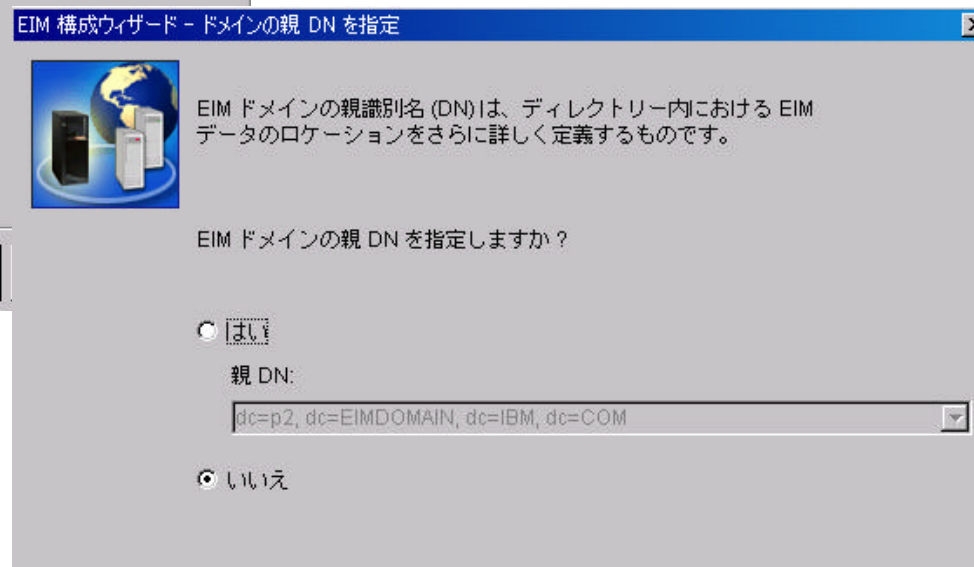
ドメイン:

記述:

← 戻る → 次へ ✖ キャンセル

4. EIM ドメイン名(ISE_EIM)と記述を入力。ドメインの親DN画面では、いいえを選択。
はい：ローカルLDAPネーム・スペースのどこにドメイン用のEIMデータを置くかを指定
いいえ：スペース内の自身の接尾部に置かれる

EIM 構成ウィザード - ドメインの親 DN を指定



EIM ドメインの親識別名 (DN) は、ディレクトリー内における EIM データのロケーションをさらに詳しく定義するものです。

EIM ドメインの親 DN を指定しますか？

はい

親 DN:

いいえ

Notes: 5. EIM ドメイン・コントロールの構成

ステップ2

4. EIMドメイン名と記述を入力します。ともに任意です。
5. ドメインの親DN画面では、いいえを選択します。
 - ◆ はい：親DNを指定します。ローカルLDAPのどこにドメイン用のEIMデータを置くかを指定することができます。
 - ◆ いいえ：自身の接尾部に置かれます。

5. EIM ドメイン・コントロールの構成

ステップ3

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 キャンセル ヘルプ

5. EIM ドメイン・コントローラーへの操作が許可されるユーザーを指定。

ユーザー・タイプ:

識別名およびパスワード - LDAP管理者
*Kerberos keytab ファイルおよびプリンシパル
*Kerberos プリンシパルとパスワード

6. レジストリーを指定。
EIMユーザーを登録するとき存在するシステムを選択します。選択対象となるシステムをレジストリーとして登録。

- ローカルOS/400 :自身のOS/400レジストリー名を入力
(p2.youreimdomain.ibm.com)
- Kerberos : KDCレジストリー名を入力
(YOUREIMDOMAIN.IBM.COM)

EIM 構成ウィザード - レジストリー情報

ユーザー・レジストリーは、特定のオペレーティング・システムまたはアプリケーションのためのユーザー定義の集合です。EIM
ドメインに追加されたユーザー・レジストリーだけが EIMに参加できます。

自身のドメインに追加したいユーザー・レジストリーは？

ローカル OS/400
P2.YOUREIMDOMAIN.IBM.COM

Kerberos
YOUREIMDOMAIN.IBM.COM

Kerberos ユーザー識別には大文字小文字の区別があります

戻る 次へ キャンセル ヘルプ

Notes: 5. EIM ドメイン・コントロールの構成

ステップ3

5. 接続のユーザーの指定画面が表示されます。
ここでは、EIM ドメイン・コントローラーへの操作が許可されるユーザーを指定します。
- | | |
|-----------|--------------------|
| ユーザー・タイプ: | 識別名およびパスワード。 |
| 識別名: | cn=administrator |
| パスワード: | LDAP管理パスワードを指定します。 |

構成ウィザードは、LDAP 管理権限をもつユーザーで実行する必要があります。

- ユーザー・タイプ:
- 識別名およびパスワード
 - Kerberos キータブ・ファイルおよびプリンシパル (プリンシパルをユーザーとして実行します。)
 - Kerberos プリンシパルおよびパスワード (プリンシパルをユーザーとして実行します。)
 - ユーザー・プロファイルとパスワード (OS/400ユーザー)
- 各ユーザーはLDAP管理者権限を与えられている必要があります。

(設定開始方法)

1. iSeriesナビゲーターより、ネットワーク ドメイン管理と展開します。
2. ドメイン名を右クリックし、権限を選択します。

6. レジストリー情報画面が表示されます。レジストリーを指定します。
レジストリーは、シングル・サインオンの対象であるユーザーが存在するシステムを示します。
ここで登録されたレジストリーは、ユーザーのマッピング情報を更新するときに選択します。
- ◆ ローカルOS/400: 自身のOS/400レジストリー名を入力
 - ◆ Kerberos: KDCレジストリー名を入力。

5. EIM ドメイン・コントロールの構成

ステップ4

EIM 構成ウィザード - EIM システム・ユーザーの指定

さまざまなオペレーティング・システム機能が EIM を使用します。オペレーティング・システムはこれらの各種機能を実行するときに、このユーザーとしてドメイン・コントローラーに接続します。EIM 機能を実行するときにオペレーティング・システムに使用させたいユーザーは？

注: このユーザーも EIM ID およびローカル EIM レジストリーに対する権限を有します。

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

7. EIMを使用するために使用されるユーザーのタイプとパスワードを入力。
8. 構成を確認し、完了をクリックし、ウィザードを終了。

EIM 構成ウィザード - 要約

新しいEIMドメインの作成と構成に必要なステップを完了しました。自身のディレクトリー・サーバーは新しいEIMドメインのドメイン・コントローラーとしても構成されました。

「完了」をクリックして、EIM を構成し、EIM ドメインを結合してください。

設定値	値
ドメイン:	ISE_EIM
ドメイン記述:	ウィザードにより作成されました。
構成のウィザード・ユーザー:	cn=administrator
ローカル OS/400 レジストリー:	P2.YOUREIMDOMAIN.IBM.COM
Kerberos レジストリー:	YOUREIMDOMAIN.IBM.COM
OS/400 EIM システム・ユーザー:	cn=administrator

← 戻る ✓ 完了 X キャンセル ? ヘルプ ?

Notes: 5. EIM ドメイン・コントロールの構成

ステップ4

7. EIMシステム・ユーザーの指定画面が表示されます。

ここでは、EIM オペレーションを実行する時にシステムが使用するユーザーを指定します。このユーザーは、

- EIM マッピング・オペレーション権限
- ローカル OS/400 ユーザー・レジストリーに対する選択したレジストリー権限の管理者

である必要があります。システムが内部的に使用するユーザーのタイプとパスワードを入力します。

上記の2つの権限を持つユーザーであれば、以下のタイプのユーザーのいずれでも指定可能です。ユーザーの権限を詳細に設定することで、EIMオペレーションの機密性を上げます。

ユーザー・タイプ:

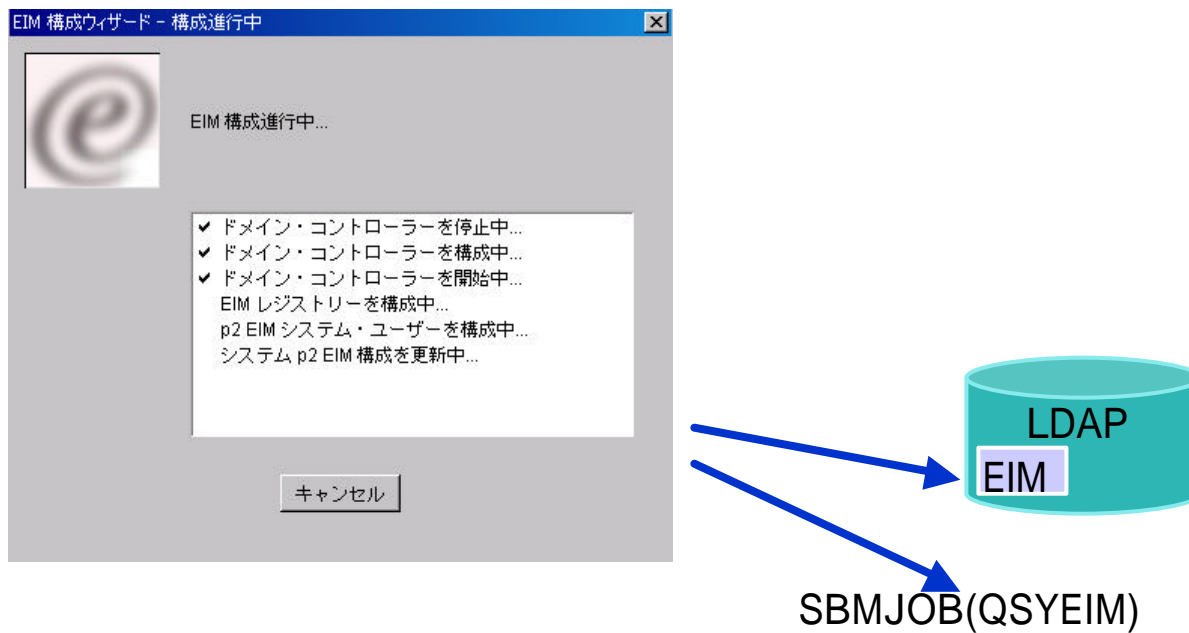
- 識別名およびパスワード
- Kerberos キータブ・ファイルおよびプリンシパル*
- Kerberos プリンシパルおよびパスワード*

(*権限が設定されたプリンシパルをユーザーとして使用できます。KDCに問い合わせ、そのユーザーの信頼性を保証します)

8. 要約画面が表示されます。構成情報を確認し、完了をクリックします。

5. EIM ドメイン・コントロールの構成

ステップ5



Notes: 5. EIM ドメイン・コントロールの構成

ステップ5

完了をクリックすれば、構成が始まります。

LDAP上に構成情報の更新します。また、EIMのサーバー・ジョブQSYEIMが開始されます。

エンタープライズ識別マッピング (EIM)関連ジョブ

- ジョブ記述: QSYS/QSYEIM
- サブシステム: QSYSWRK
- ジョブ: QTOBDNS

構成手順 6: EIM ドメインを登録

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

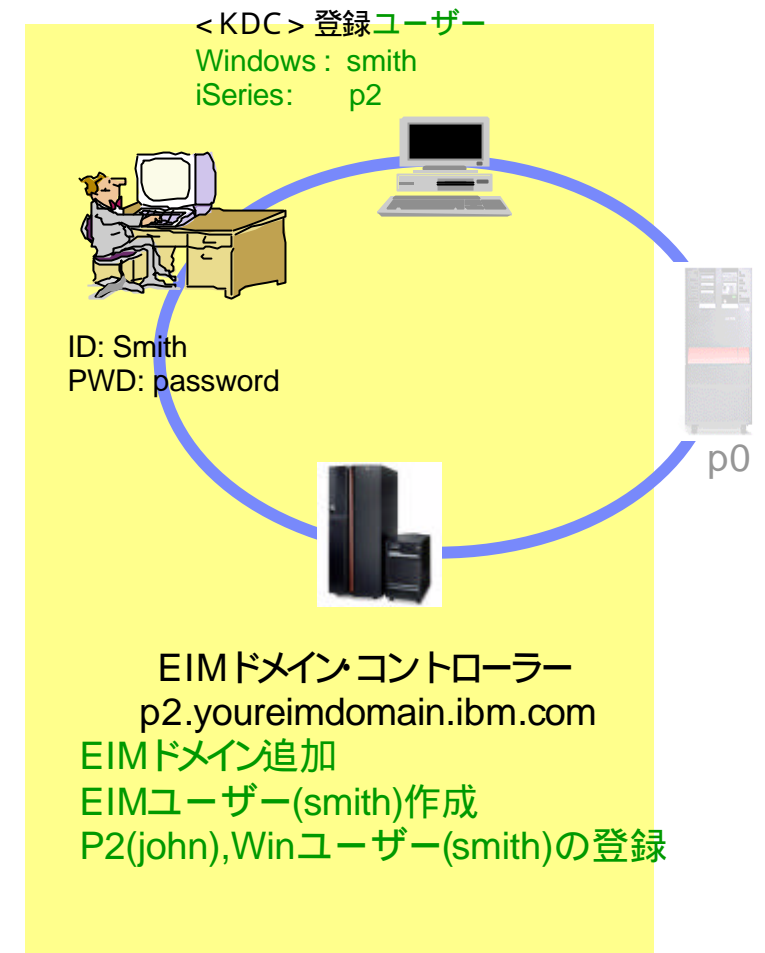
4. P2 でネットワーク認証サービス(NAS)の構成

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

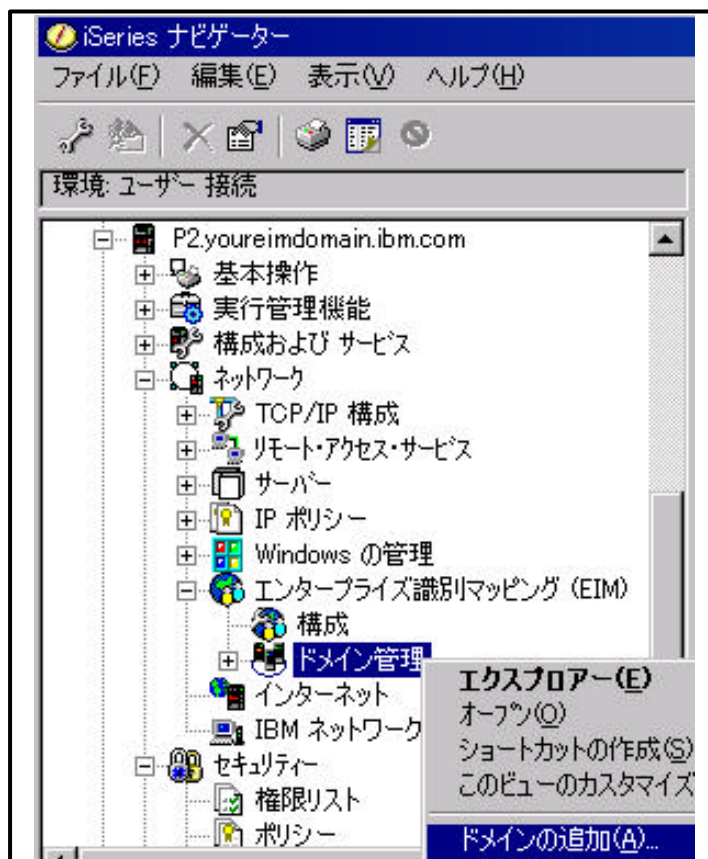
8. P2で、ユーザーのマッピング情報の登録



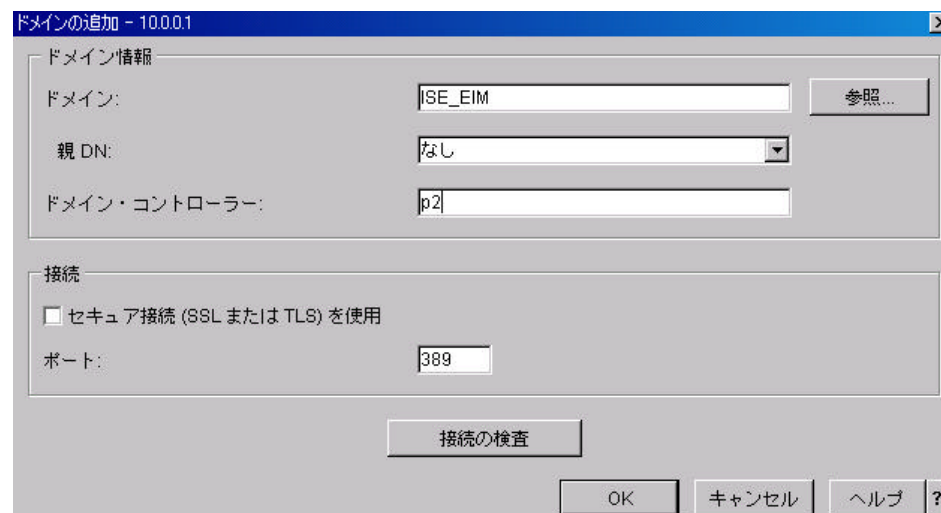
Notes:構成手順 6

ここでは、構成手順6で作成したEIMドメインコントローラーを、管理対象ドメインとして追加します。追加することで、ユーザー管理やドメイン管理が可能となります。

6. iSeriesシステムをEIM ドメインに登録 ステップ1



1. ドメイン管理を右クリックし、ドメイン追加を選択
 2. ドメイン追加画面で以下を指定
- ドメイン: 構成したドメイン名(ISE_EIM)
 ドメイン・コントローラー: EIM ドメイン・コントローラーのホスト名
 (p2.youreimdomain.ibm.com)
 ポート: デフォルトのまま(389)



Notes: 6. iSeriesシステムをEIMドメインに登録 ステップ1

1. iSeriesナビゲーターより、システム名 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. ドメイン管理を右クリックし、ドメイン追加を選択します。
3. ドメイン追加画面で以下を指定します。完了すれば、OKをクリックします。
ドメイン: 構成したドメイン名(ISE_EIM)
ドメイン・コントローラー: EIMドメイン・コントローラーのホスト名(P2.YOUREIMDOMAIN.IBM.COM)
ポート: デフォルトのまま(389)

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、追加したドメインISE_EIMが追加されていることが確認できます。