セッション L14

IBM eServer iSeries

iHOPE
iSeries Hands-On Professional Education

EM 構成

さわってみよう シングル・サインオン

特記事項

当資料で解説される項目の更に詳細な説明は、製品から提供されるマニュアル、オンライン・ヘルプ、Web上の情報を参照してください。

当資料は、2003年4月現在のIBMその他の製品情報に基づいて作成されております。この資料に含まれる情報は可能な限り正確を期しておりますが、日本アイ・ビー・エム株式会社による正式なレビューは受けておらず、当資料に記載された内容に関して日本アイ・ビー・エム株式会社および日本アイ・ビー・エム　システムズ・エンジニアリング株式会社が何ら保証をするものではありません。したがって、この情報の利用またはこれらの技法の実施はひとえに使用者の責任においてなされるものであり、当資料の内容によって受けたいかなる被害に関しても一切の保証をするものではありませんのでご了承ください。

日本IBMシステムズ・エンジニアリング株式会社
サーバー・システム部　Integrated Server グループ

商標

以下の用語は、アメリカ合衆国、あるいは他国、あるいは両国でのIBM Corporationの商標です:

- AS/400
- AS/400e
- DB2
- IBM
- MQSeries
- Operating System/400
- OS/400
- SanFrancisco
- stylized 
- WebSphere
- 400
- iSeries
- eServer

以下の用語は、アメリカ合衆国、あるいは他国、あるいは両国でのLotus Development社の商標です:

- Domino
- Domino.Doc
- LearningSpace
- Lotus
- QuickPlace
- Sametime

JavaとすべてのJavaをベースとする商標およびロゴは、アメリカ合衆国、他国、あるいは両国のサン・マイクロシステムズ社の商標または登録商標です。

Microsoft Windows, Windows NT, およびWindowsのロゴは、アメリカ合衆国、他国、あるいは両国のマイクロソフト社の商標です。

他の会社、製品、およびサービス名は、その会社の商標あるいはサービスマークかもしれません。

このプレゼンテーションに含まれるサードパーティーに関連する題材は、これらのサードパーティーから得られた情報に基づいています。これらの情報の正確さの確認のための、いかなる努力もなされていません。このプレゼンテーションは、いかなるサードパーティー製品またはサービスの、IBMによる推薦あるいは指示を表したり、ほのめかすものではありません。

目的

- EIM環境の構成要素を知る。
- シングル･サインオン環境の構築手順を知る。
- EIMを構成できる。

EIM構成要件

- システム要件
  - OS/400 V5R2
  - 5722AC3　CRYPTO ACCESS PROVIDER 128-BIT FOR AS/400
  - 5722XE1　ISERIES ACCESS FOR WINDOWS
- クライアント要件
  - iSeriesナビゲーター(コンポーネント:ネットワーク、セキュリティ)

- EIM環境の構成要素
  - クライアント
  - サーバー（シングル･サインオン先コンピューター）
  - EIMドメイン･コントローラー
  - KDC(鍵配布センター)

Notes: 構成要件

システム要件

OS/400 V5R2

5722AC3 CRYPTO ACCESS PROVIDER 128-BIT FOR AS/400

5722XE1 ISERIES ACCESS FOR WINDOWS

クライアント要件

iSeriesナビゲーター(コンポーネント:ネットワーク、セキュリティ)

EIM環境 構成要素

クライアント

サーバー (シングル・サインオン先コンピューター)

:基本的にKerberosをサポートするシステムであればEIMシングル・サインオンは実現可能です。サポート状況は、各製品のスペックを確認してください。

EIMドメイン・コントローラー

:iSeries OS/400 V5R2以降で実現可能となりました。

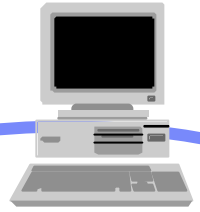
KDC(鍵配布センター)

:OS/400はKDCとして構成できません。したがって、他のオペレーティング・システムで構成する必要があります。

環境

KDC (Windows 2000 Server)
Kdc2000. YOUREIMDOMAIN.IBM.COM

Windows2000Profession
ID: Smith
PWD: password



Kerberos レルム :YOUREIMDOMAIN.IBM.COM
EIMドメイン :SE_EIM

iSeries
p0.youreimdomain.ibm.com

P0ログイン・ユーザー
ID: smith627
PWD: smith627

iSeries
p2.youreimdomain.ibm.com

P2 ログイン・ユーザー
ID: john
PWD: john

EIMドメイン・コントローラー

Eim：	john smith
Win	smith
p0	smith627
p2	john

Notes: 環境

iSeriesシステムP0, P2に対して、シングル･サインオンでアクセスする環境を構築する場合を考えます。
EIMを利用する場合、Kerberosを使用するアクセスを認可するKDC(鍵配布センター)が必要です。OS/400はKDCとし構成することはできません。したがって、OS/400以外のオペレーティング･システムをKDCとして構成する必要があります。
今回の例では、以下のシステム環境を構築する手順を見ていきます。

- クライアント： smith (Windows 2000 Proffession)
- KDC： kdc2000.YOUREIMDOMAIN.IBM.COM (Windows2000Server)
- iSeries： p0.youreimdomain.ibm.com
  p2.youreimdomain.ibm.com
- P2をEIMドメイン･コントローラーとして構成。

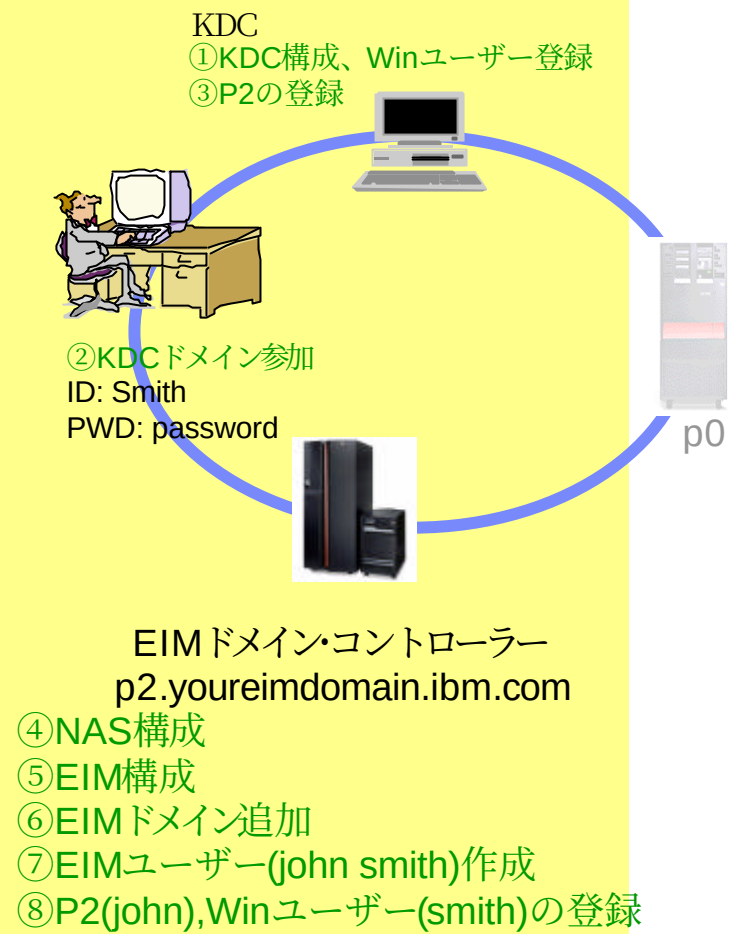
各ユーザー情報を持ちます。各ユーザー情報：

Eim：	john smith
Win	smith
p0	smith627
p2	john

- EIMドメインを、ISE_EIM とする。
- Kerberodレルムを、YOUREIMDOMAIN.IBM.COM とする。

構成手順: KDC, Winクライアント, p2

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

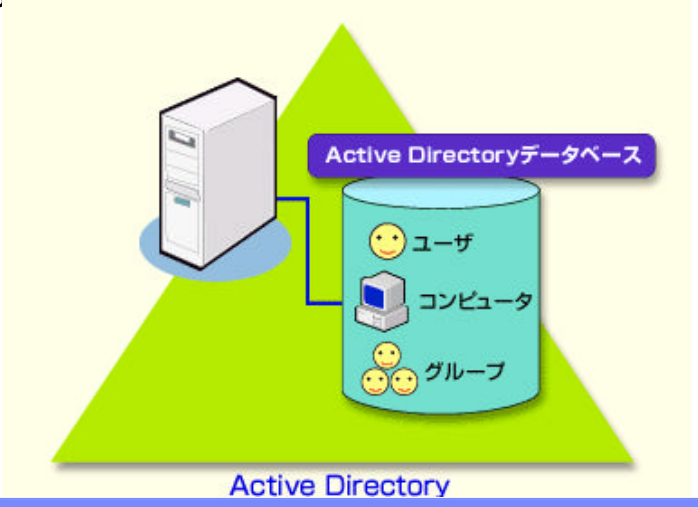
前述のシステム環境を構成する第一段階として、KDC, Win クライアント, p2のシステムを構成します。構成後、p0をEIM対象システムとして追加します。

構成手順は以下の通りです。

1. Windows2000Serverで、KDCを構成。
   ここでは、Windows2000Serverが持つActiveDirectoryを構成します。
   具体的に、ドメインを作成し、Kerberos認証を行なう対象のシステムを登録することで、管理対象としてみなします。
2. クライアントの KDC参加。
   1で作成したドメインに参加することで、KDCの管理対象として構成することができます。
3. KDCへiSeriesの参加。
   1で作成したドメインに、iSeriesP2をユーザーとして追加します。
   また、P2に対するキーを発行し、P2とのセッションを許可することになります。
   ここでは、P2のみを登録していますが、シングル・サインオン対象のシステムを追加する場合は、同様に該当システムを登録する必要があります。したがって、後ほどP0を追加します。
4. P2でネットワーク認証サービス(NAS)の構成。
   Kerberosを利用したアクセスを可能とするネットワーク認証サービスを構成します。
   構成後、構成されたKDCに対して3で作成したキーを取得します。
5. P2を、EIM ドメイン・コントローラーとして構成。
   ユーザーのマッピング管理を行なうEIM ドメイン・コントローラーを構成します。
6. 管理対象として5で作成した EIM ドメインを登録。
   EIMを管理したりEIMユーザーの追加/除去をするために、5で作成したEIM ドメイン・コントローラーをドメイン管理対象として追加します。
7. P2で、EIMユーザーの作成。
   各システムのマッピング情報を登録するためのEIMユーザーを作成します。
8. P2で、ユーザーのマッピング情報の登録。
   7で作成したEIMユーザーに該当する、各システムのユーザーIDを登録します。

1. KDC(Key Distribution Center)の構成

- KDC
  - Windows 2000 Server , Windows XP Server , Linux , AIX , zSeries　など
  - Windows 2000 Server
    - 使用コンポーネント
      - Active Directory
        - OSインストール時、デフォルトで導入される
        - Kerberos配布先ユーザー(iSeriesシステムやPCユーザー)を管理する
      - Ktpassツール(サポート・ツールに含まれる)
        - 手動で導入
        - CD-ROM 2枚目　/support/tools内　setupの実行
    - Active Directoryとは
      - ドメイン管理
      - Kerberosの配布



Notes:

iSeriesシステムは、KDC(鍵配布センター)になることはできません。したがって、他システムをKDCと構成し、シングル・サインオンを実現する必要があります。KDCを実装できるシステムには、以下があります。

- Windows 2000 Server
- Windows XP Server
- Linux
- AIX
- zSeries　など

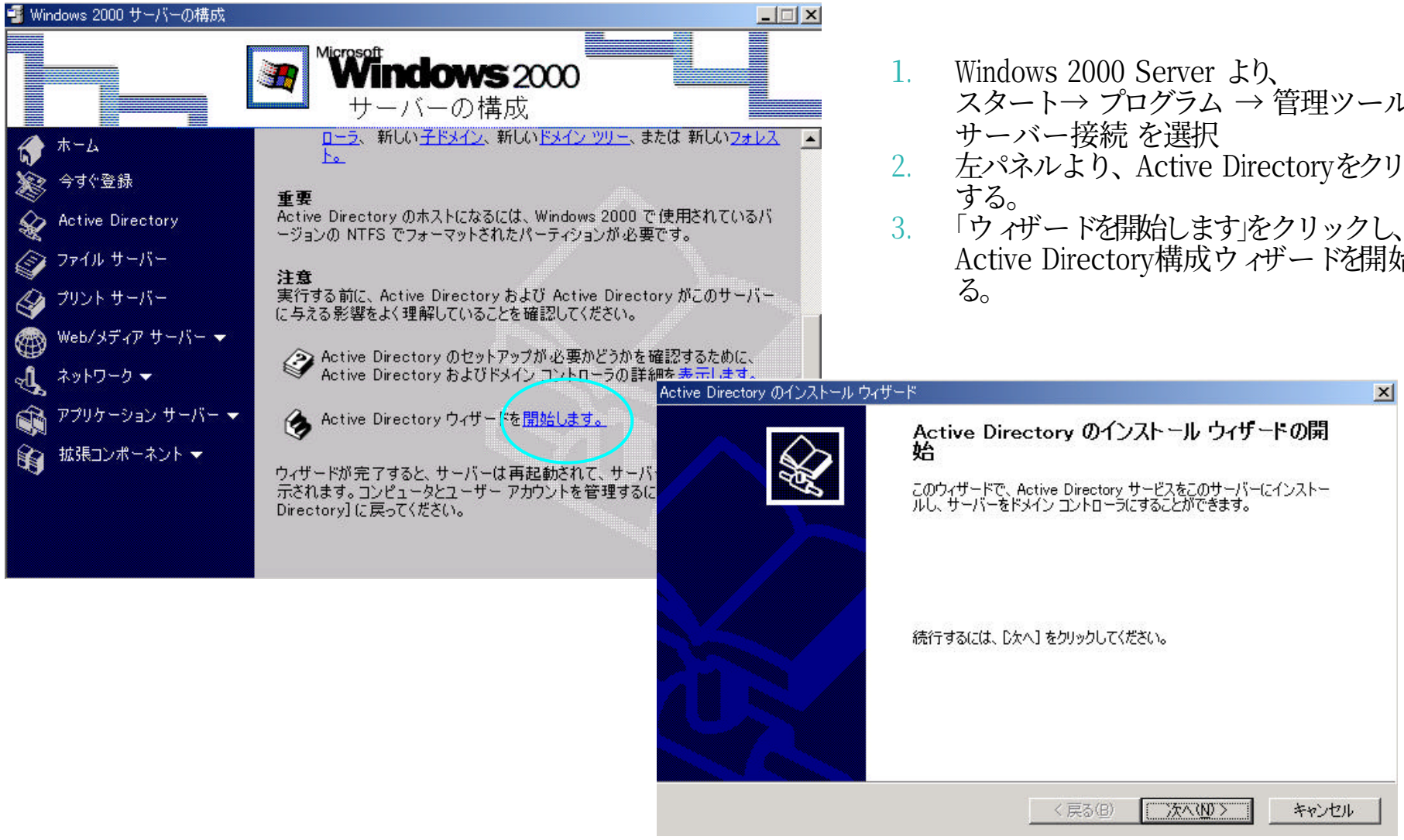
ここでは、KDC をWindows 2000 Server で実現した例を取り上げます。
Windows 2000 Server で KDC を実現するには、Windowsが、Fat32ではなくNTFSファイル・システムでインストールされていなければいけません。また、以下のコンポーネントは導入済みである必要があります。

- Active Directory
- サポート・ツール

<Active Directoryとは>
Windows 2000 Serverで提供されるディレクトリ・サービスです。Active Directoryはネットワーク上のユーザー情報やコンピュータ情報などさまざまな資源を、ドメイン単位で管理することを目的としています。ドメインを管理する際、名前解決サービスとしてDNS(Domain Name System)、情報検索用プロトコルとしてLDAP、認証プロトコルとしてKerberosを実装することが可能です。
Active Directory で、Kerberosを配布すべきシステム,、つまりシングル・サインオンの対象システムの情報が登録管理されます。

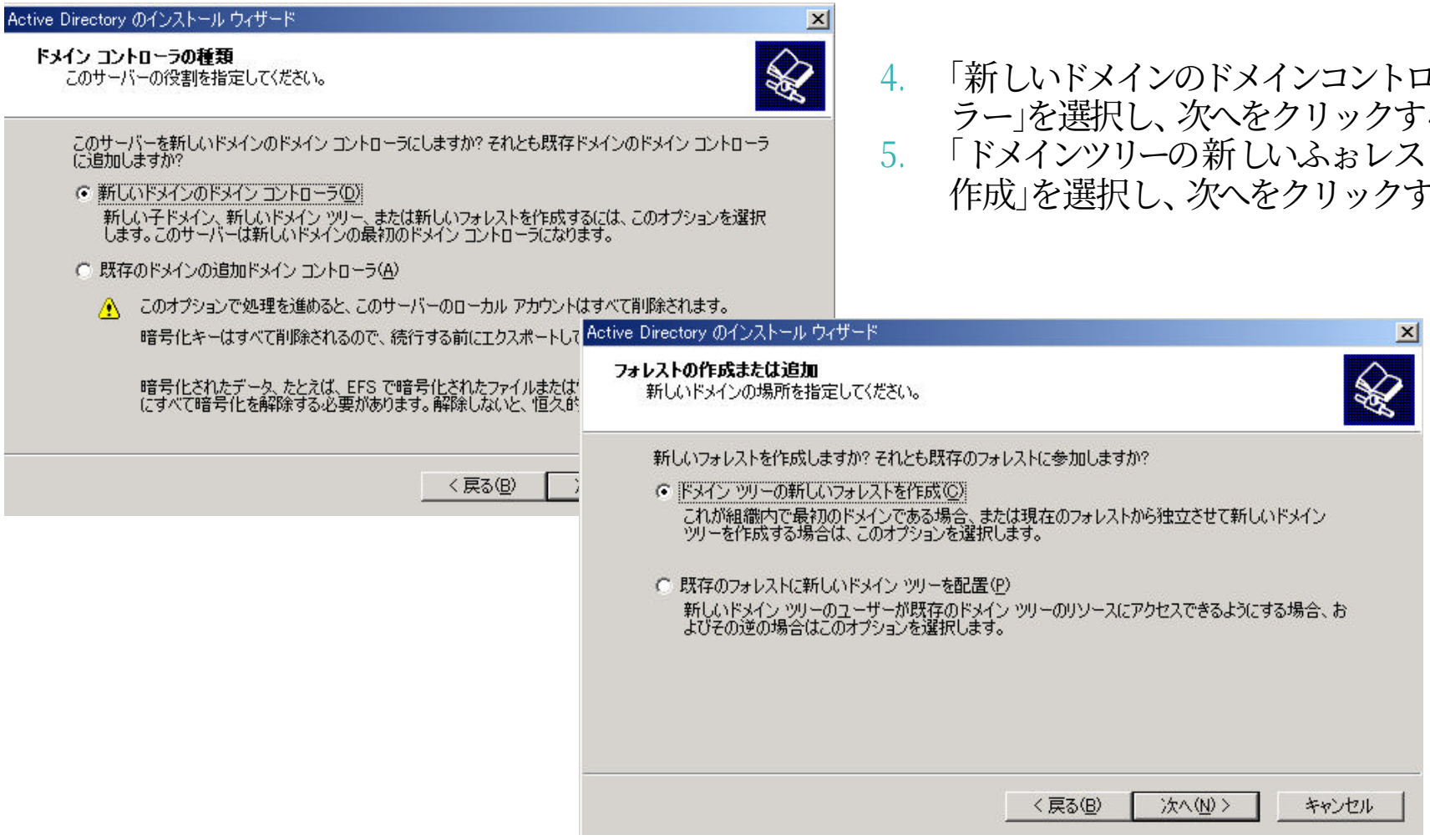
<サポート・ツールとは>
Active Directory 管理ツールです。グラフィカル・インターフェースで、対象ユーザーを登録したり編集することができます。

1. KDCの構成　ステップ1



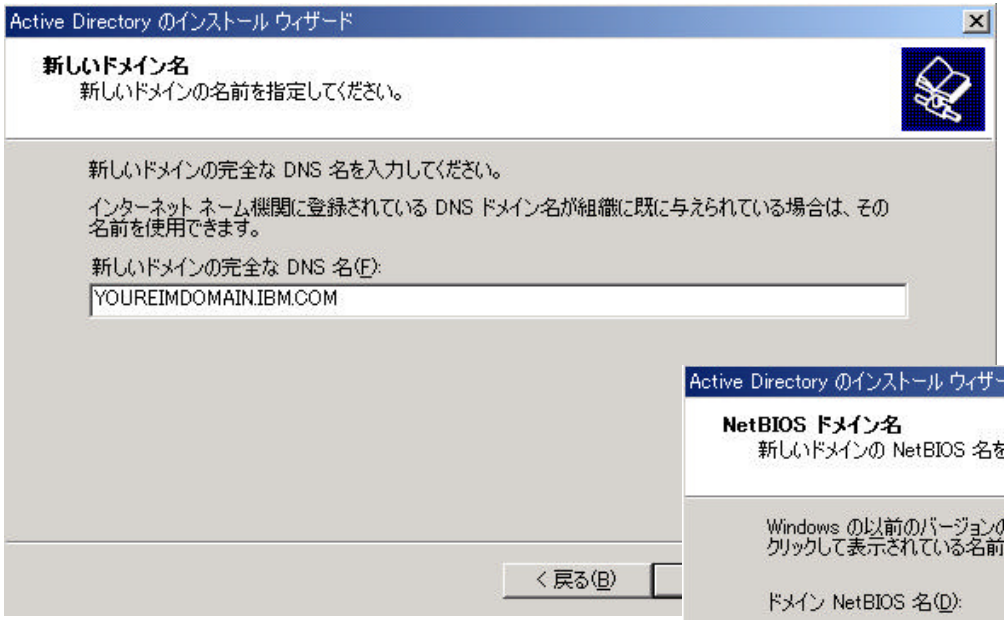
1. Windows 2000 Server より、スタート→ プログラム → 管理ツール → サーバー接続 を選択
2. 左パネルより、Active Directoryをクリックする。
3. 「ウィザードを開始します」をクリックし、Active Directory構成ウィザードを開始する。

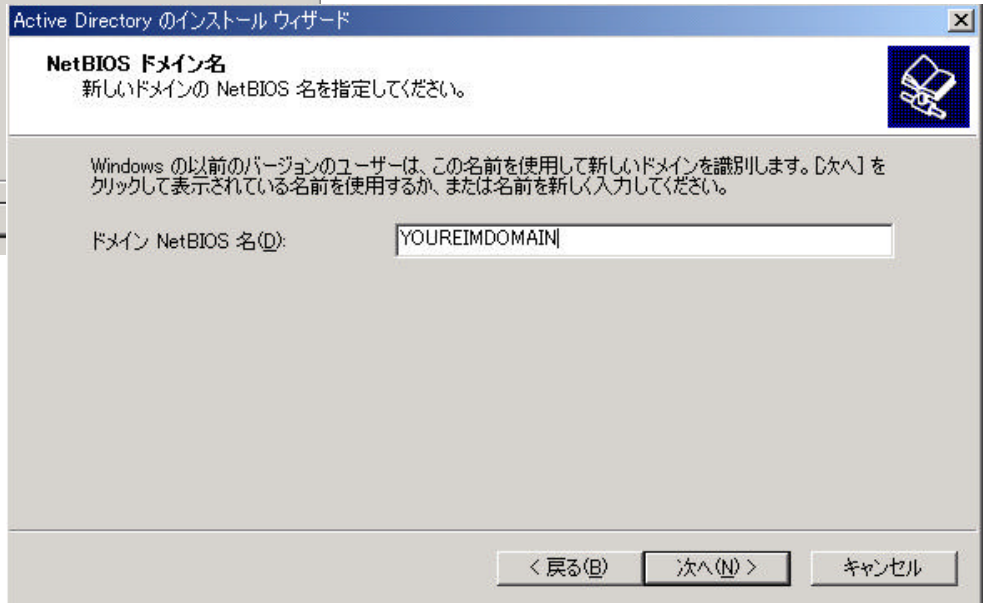
1. KDCの構成　ステップ2



4. 「新しいドメインのドメインコントローラー」を選択し、次へをクリックする。
5. 「ドメインツリーの新しいふぉレストを作成」を選択し、次へをクリックする。

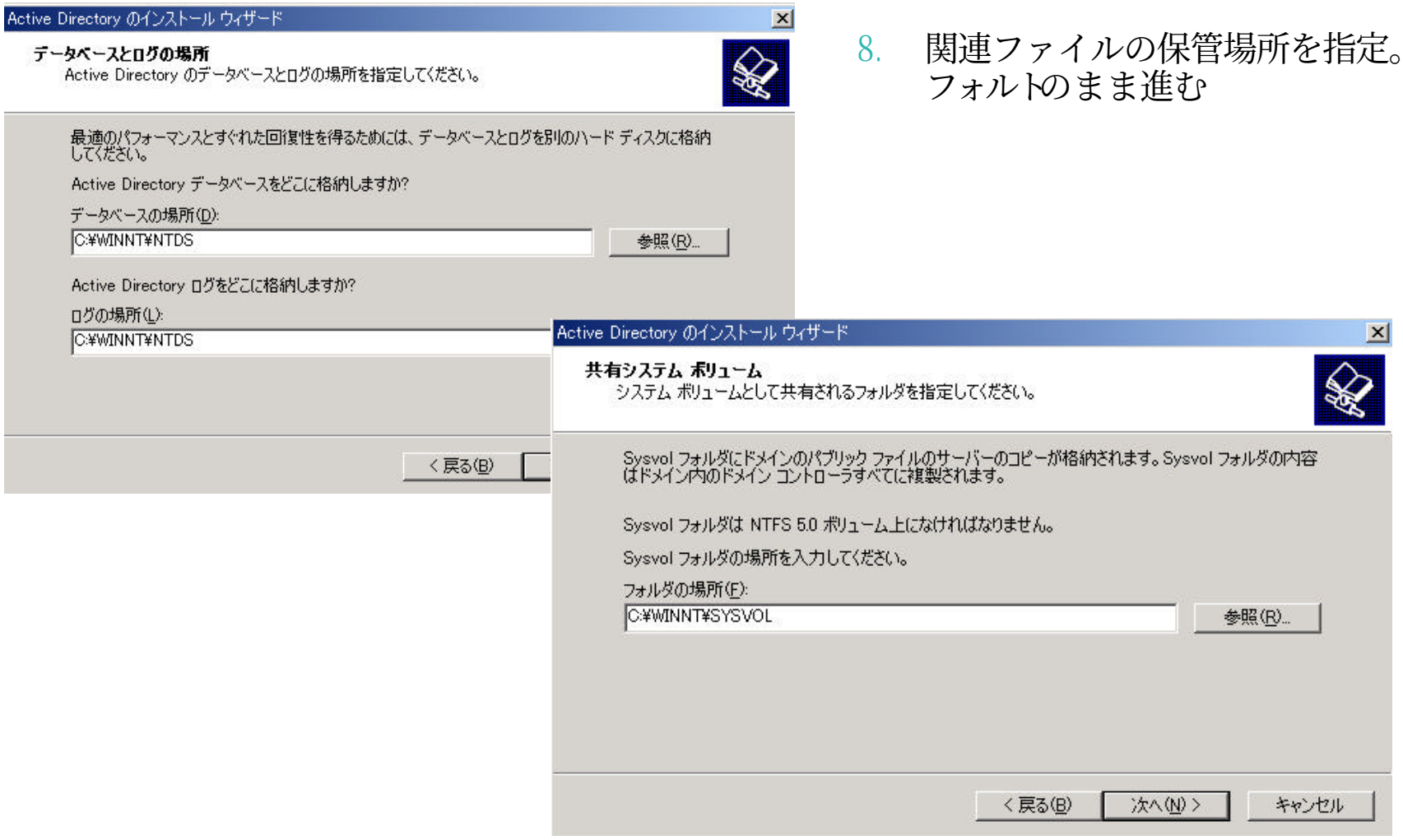
1. KDCの構成　ステップ3





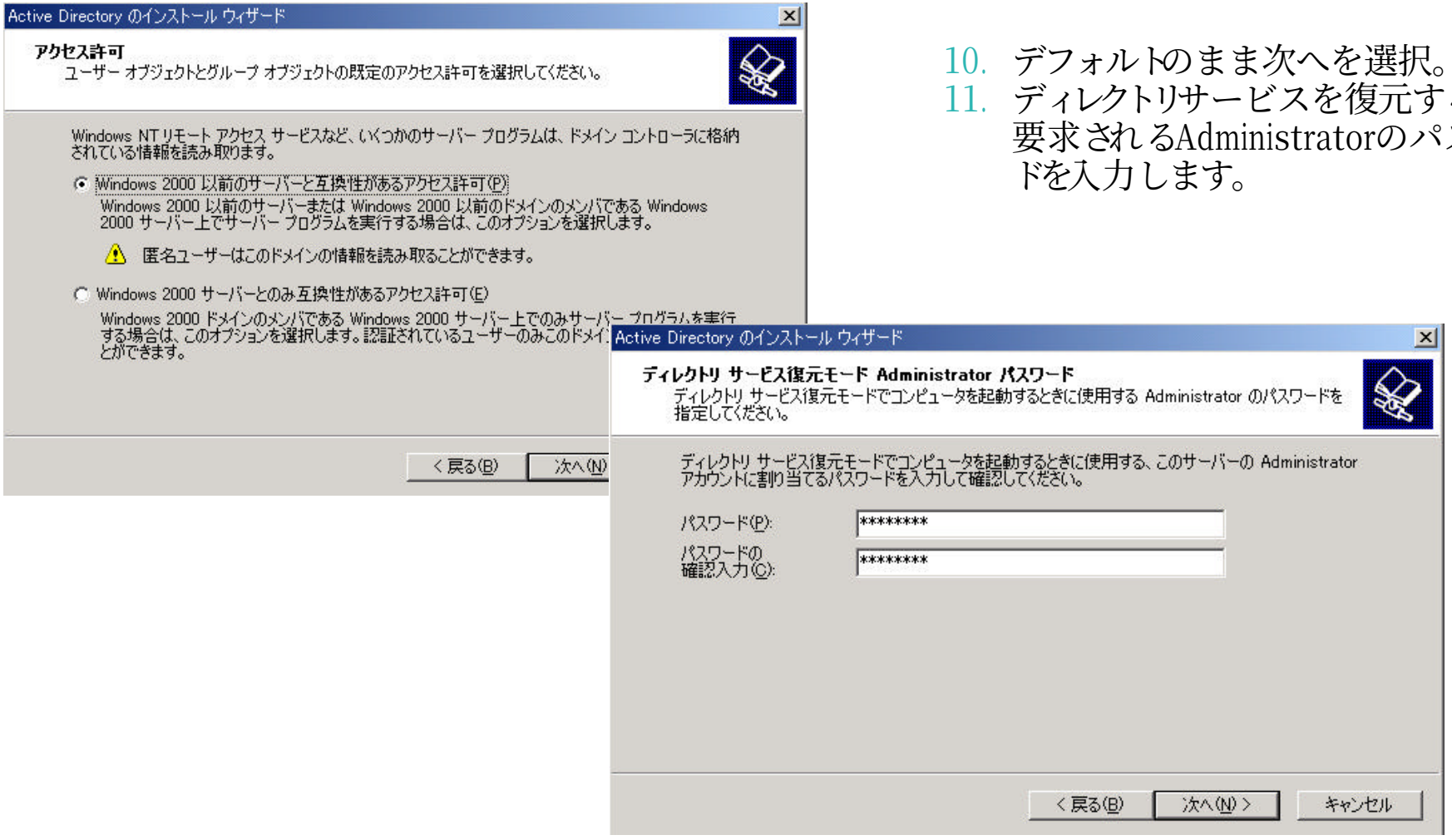
6. ドメイン名を入力。
   ここでは、
   YOUREIMDOMAIN.IBM.COM
7. NetBIOS 名を入力
   ここでは、デフォルトのまま進む。

1. KDCの構成　ステップ4



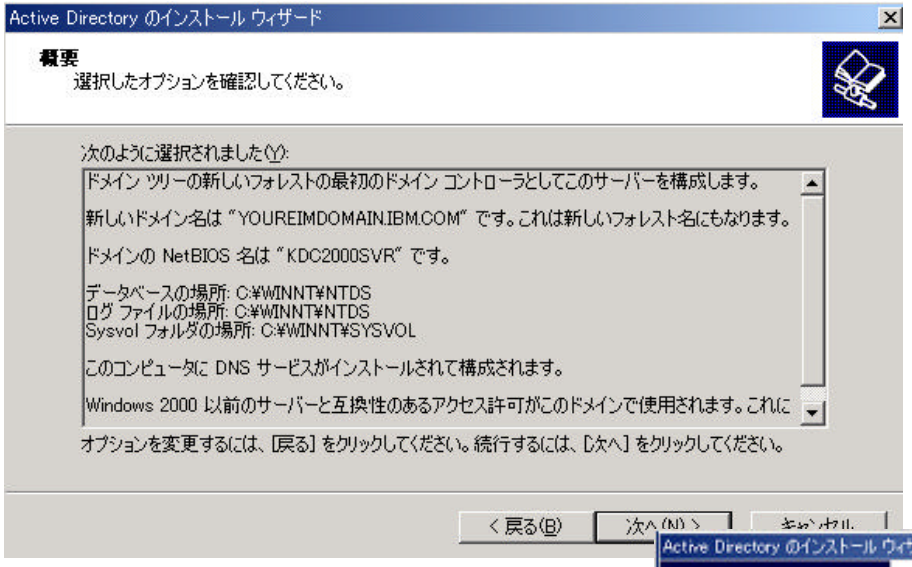
8. 関連ファイルの保管場所を指定。デフォルトのまま進む

1. KDCの構成　ステップ5

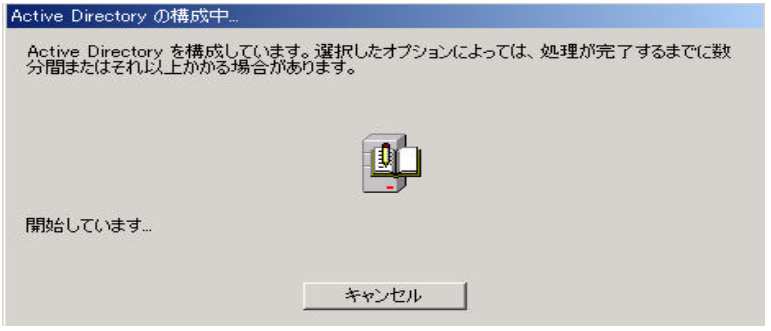


10. デフォルトのまま次へを選択。
11. ディレクトリサービスを復元する際に要求されるAdministratorのパスワードを入力します。

1. KDCの構成　ステップ6



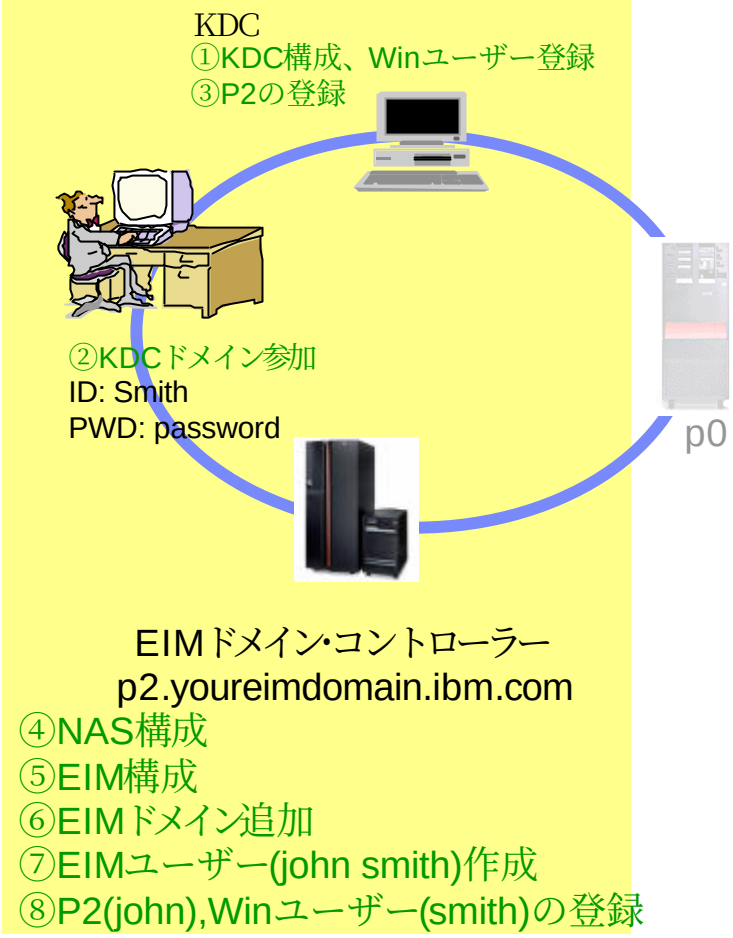
12. 構成内容を確認し、次へをクリック。
13. 構成情報が更新されます。
    数分かかります。



14. 完了をクリックします。再起動後、構成が反映されます。

構成手順 2: ユーザーのドメイン参加

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2

ここでは、手順1で作成したKDCドメインにWindowsクライアントを参加させる手順を説明します。
ドメインに参加することで、Kerberosを利用したアクセスが可能となります。

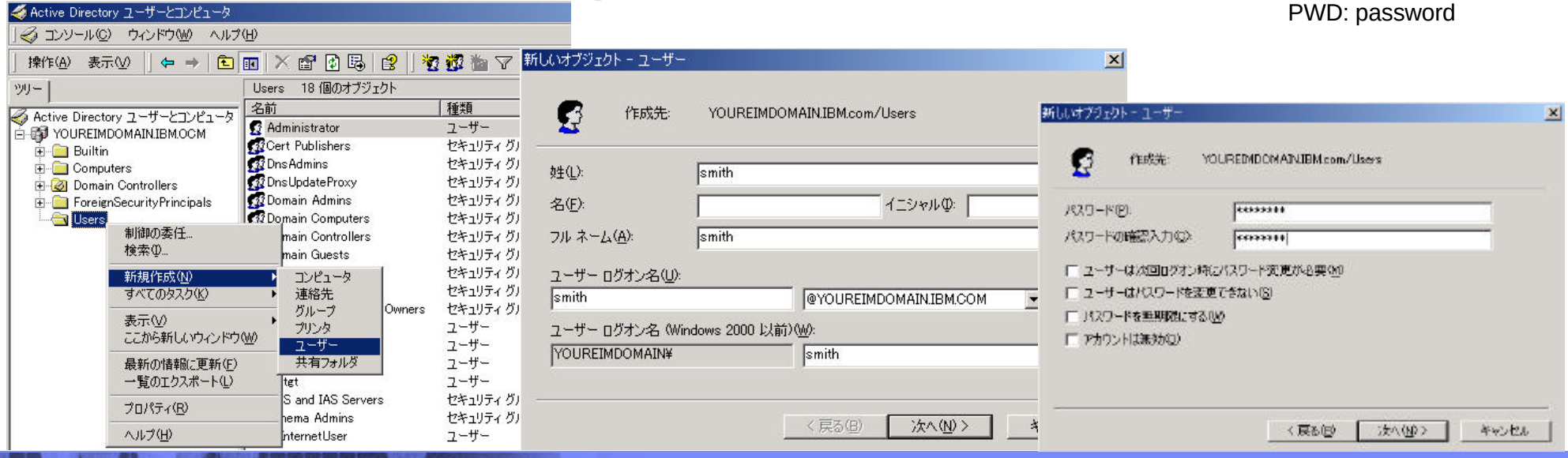
2. ユーザーのドメイン参加　ステップ1

- EIMを利用するユーザー(コンピュータ)をドメイン参加するために
  - KDC にてユーザー登録
  - ユーザーPCのドメイン参加

- KDCにおいてユーザー(smith)登録

1. KDC(ここでは、Windows 2000 Server)より、
   スタート→ プログラム → 管理ツール → ActiveDirectory ユーザーとコンピュータ　を選択。
2. Users を右クリックし、新規作成 → ユーザーを選択。
3. WindowsのサインオンID(smith)とパスワード(password)を入力し、ユーザーを作成する。

Windowsログイン
ID: Smith
PWD: password



Notes: 2. ユーザーのドメイン参加 ステップ1

ドメインに参加するために以下の設定が必要です。

- KDCにおいて、ユーザーとしてWindowsクライアントを登録する。
- PCユーザーのドメイン参加。

KDCにおいてユーザーとしてWindowsクライアント(Smith)を登録するする手順は以下の通りです。

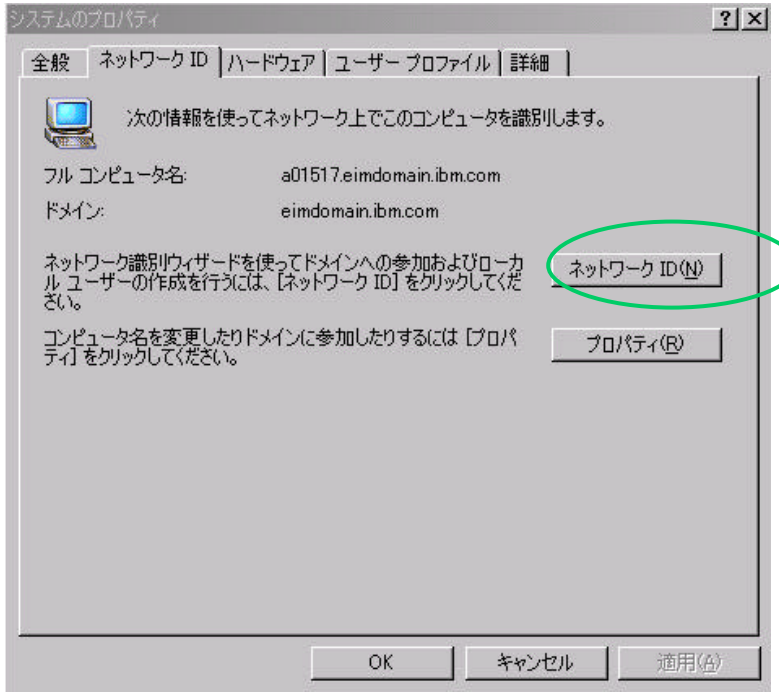
1. Windows2000Serverより、スタート→ プログラム → 管理ツール → ActiveDirectory ユーザーとコンピュータ を選択します。。
2. Users を右クリックし、新規作成 → ユーザーを選択します。
3. WindowsのサインオンIDとパスワードを入力し、ユーザーを作成します。

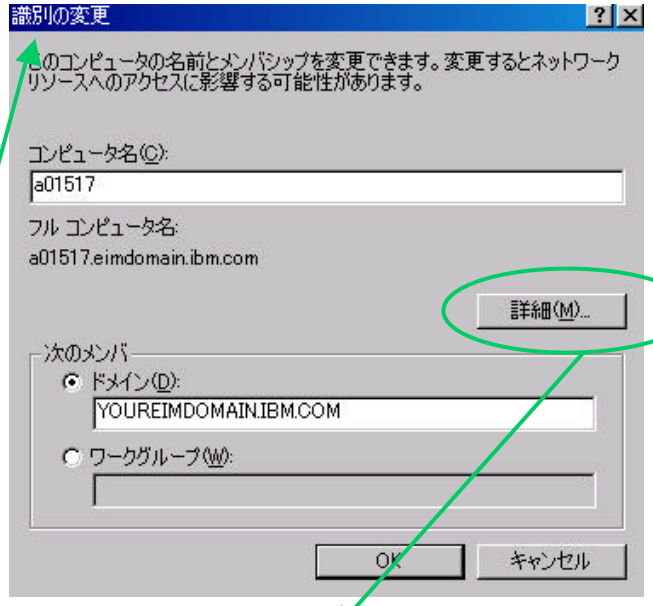
   ユーザーID: smith
   PWD: password

2. ユーザーのドメイン参加　ステップ2

- ユーザーPCのドメイン

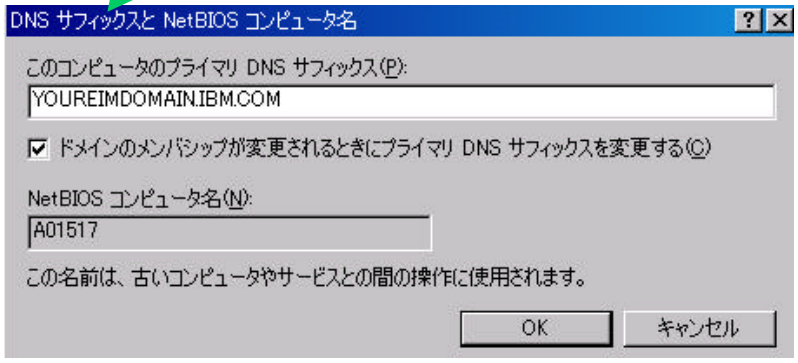
4. マイコンピュータのプロパティを開き、ネットワークIDをクリックする。





5. ドメインにチェックし、ドメイン名を入力。
6. 詳細をクリックし。DNSサフィックスを同じ名前で指定。

ドメイン名/DNSサフィックス
(YOUREIMDOMAIN.IBM.COM)



7. OKをクリックすれば、ドメインにアクセスします。
サインオン画面が表示されれば、KDCで登録したユーザーIDとパスワードでサインオンします。(ここでは、smith/password)

Notes:　2. ユーザーのドメイン参加　ステップ2

PCユーザーをドメインに参加させます。

PCのコンピューター属性 ‘ドメイン ’を変更します。

1. デスクトップ上のマイ･コンピュータを右クリックし、プロパティを選択します。
2. ネットワークIDタブを開き、ネットワークIDをクリックします。
3. ドメインをKDCで作成したドメイン名を指定します。
4. 詳細をクリックします。
5. DNSサフィックス欄に、KDCで作成したドメイン名を指定します。
6. OKをクリックすれば、ドメイン･アクセスするためのサインオンが要求されます。

KDCで設定した(手順2 ステップ2)ユーザーIDおよびパスワード(smith/password)を入力します。

8. ドメインに参加できたことを確認すれば、次回のWindowsログイン時に、ログイン先としてドメインを指定できます。

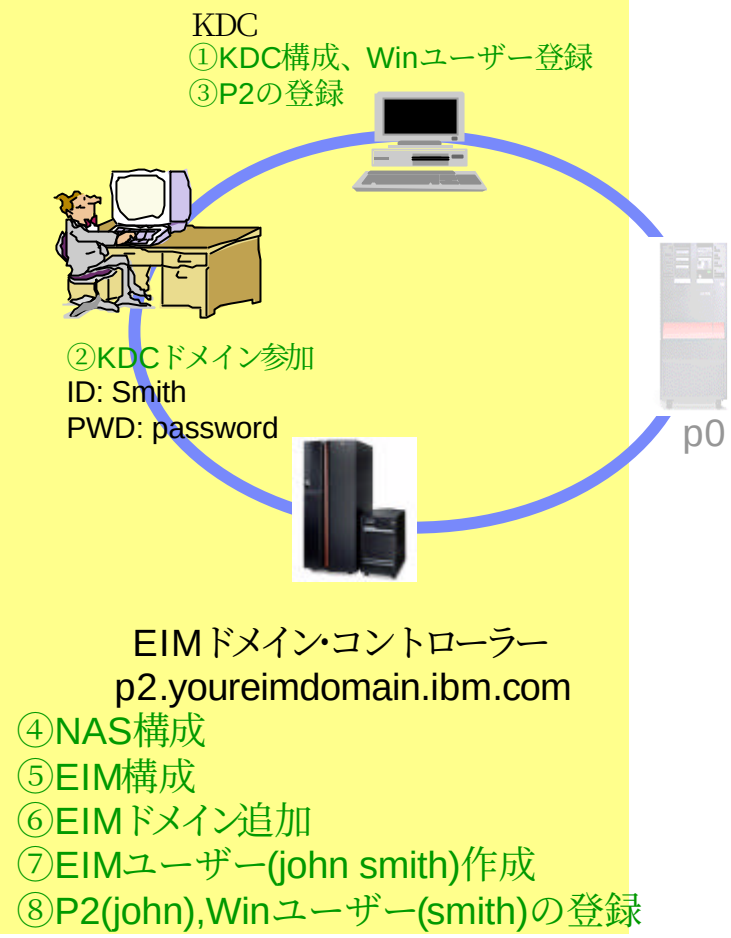
ドメイン(YOUREIMDOMAIN.IBM.COM)を選択し、smith/passwordでサインオンします。

(参考)

あらかじめ、ローカルにユーザーsmithを作成しておく必要はありません。KDCに登録されているユーザーであれば、ドメイン参加可能です。

構成手順 3:KDCへiSeriesP2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 3:KDCへiSeriesP2を登録

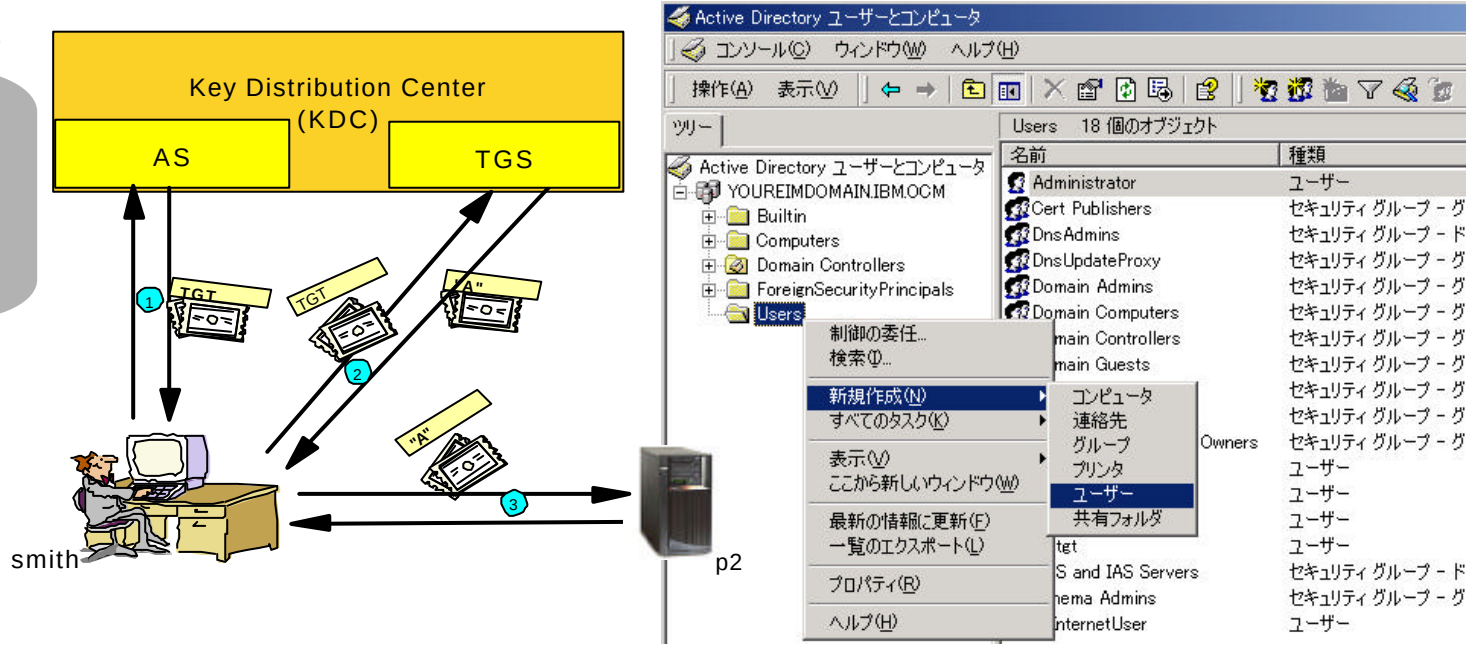
KDCの管理対象とするシステムをユーザーとして登録します。
ここでは、p2.youreimdomain.ibm.com(iSeriesシステム)を登録します。

3. KDCへiSeriesP2の追加　ステップ1

ドメインに参加する管理対象システムをユーザーとして登録します。
ここでは、p2.youreimdomain.ibm.com(iSeriesシステム)を登録します。

1. Windows 2000 Server より、
スタート→ プログラム → 管理ツール → ActiveDirectoryユーザーとコンピュータ を選択します。
2. Usersを右クリックし、新規作成からユーザーを選択します。

登録ユーザー
- Winユーザー smith
- P2.youreimdmoain.ibm.com
- P0.youreimdomain.ibm.com

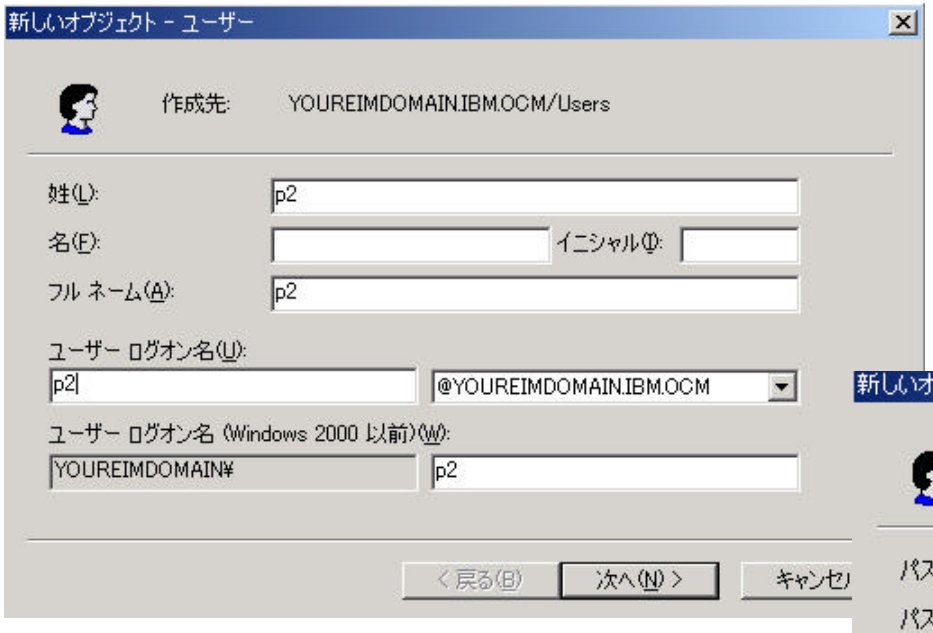


Notes: 3. KDCへiSeriesP2の追加 ステップ1

KDCの管理対象とするシステムをユーザーとして登録します。
ここでは、p2.youreimdomain.ibm.com(iSeriesシステム)を登録します。

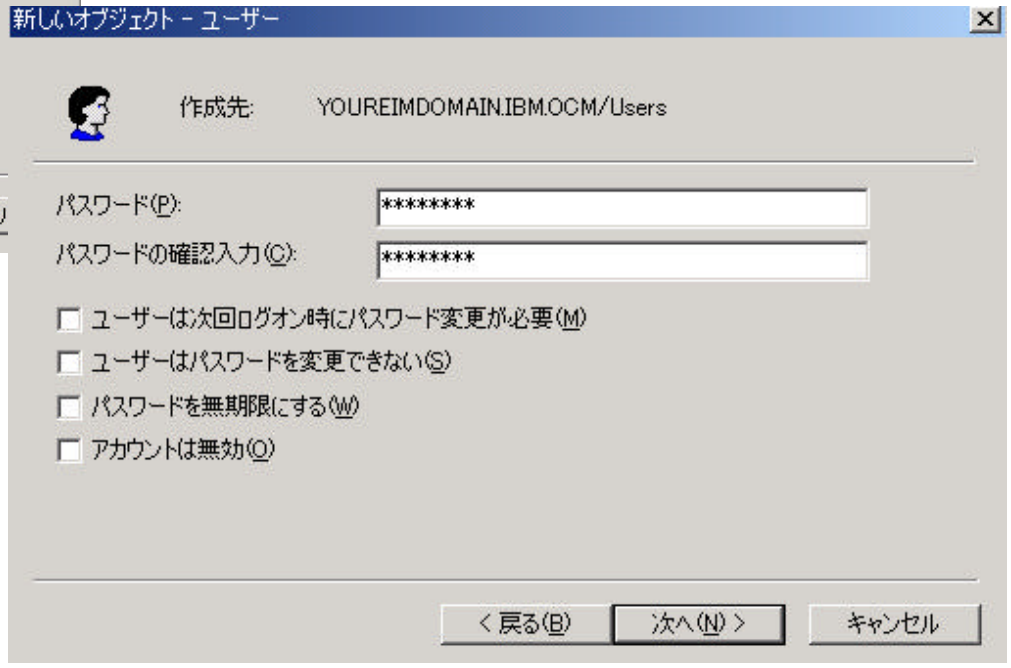
1. Windows 2000 Server より、スタート→ プログラム → 管理ツール → ActiveDirectoryユーザーとコンピュータ を選択します。
2. Usersを右クリックし、新規作成からユーザーを選択します。

3. KDCへiSeriesP2の追加　ステップ2



3. 姓名、ユーザー・ログイン名(任意)を入力します。
   ここでは、p2を入力しています。
4. パスワードを入力します。
   このパスワードは、
   - Kerberosチケット発行時(手順2ステップ2)
   - EIM構成時(手順4ステップ4)

   に使用されます。



Notes: 3. KDCへiSeriesP2の追加　ステップ2

3. 姓名、ユーザー・ログイン名(任意)を入力します。
4. パスワードを入力します。

このパスワードは、

- Kerberosチケット発行時(手順2ステップ2)
- EIM構成時(手順4ステップ4)

に使用されますので、設定したパスワードを覚えておく必要があります。

ユーザーのみが自分のパスワードを知るようにするために、次回サインオン時にパスワードを変更する場合、パスワード入力画面で、‘ユーザーは次回ログオン時にパスワード変更が必要’にチェックしてください。ユーザーが変更したパスワードはActiveDirectoryで更新されます。

ユーザーがパスワードを忘れた場合、管理者が手動でパスワードを設定する必要があります。