



IBM eServer iSeries





さわってみよう シングル・サインオン

© 2003 IBM Japan Systems Engineering Co.,Ltd.

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
- MQSeries
- AS/400e
- Operating System / 400
 OS / 400

DB2IBM

SanFrancisco

- WebSphere400
 - iSeries
 - eServer

stylized (

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

- LearningSpace
- Domino.Doc 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。





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



The next generation iSeries...simplicity in an on demand world

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 -)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。

- 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。
 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。
- 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。

 102でネットローを認知する、レスパンの構成

 102でネットローを認知する

 112 (140)の構成

 112 (140)の構成
- 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注IM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「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。
- 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。
- 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。

IBM

1. KDC(Key Distribution Center)の構成

KDC

11

- ◆ 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の宝行
 - Active Directoryとは
 - ドメイン管理
 - Kerberosの配布



Active Directory

The next generation iSeries...simplicity in an on demand world

IBM

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 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。

IEM					
LEM	_	_	_	_	_
112171			_		_
					1
				_	_
	_		_		



The next generation iSeries...simplicity in an on demand world

14



Active Directory のインストール ウィザード 新しいドメイン名 新しいドメインの名前を指定してください。	×	6.	ドメイン名を入力。 ここでは、 VOUREIMDOMAINUBM COM
新しいドメインの完全な DNS 名を入力してください。 インターネット ネーム機関に登録されている DNS ドメイン名が組織に既に与えられてい 名前を使用できます。 新しいドメインの完全な DNS 名(E): YOUREIMDOMAIN.IBM.COM	る場合は、その	7.	NetBIOS 名を入力 ここでは、デフォルトのまま進む。
Active D Netl マラス(日)	irectory のインストール ウィザード BIOS ドメイン名 新しいドメインの NetBIOS 名を指 Windows の以前のバージョンのユ クリックして表示されている名前をf ドメイン NetBIOS 名(①):	定してください ーザーは、ご 更用するか、: 「YOUF	► ► <

16

最適のパフォーマンスとすぐれた回復性を得るためには、データベースとログ してください。	を別のハードディスクに格納	
octive Directory データベースをどこ(に格納しますか?		
データベースの場所(D):		
C:¥WINNT¥NTDS	参照(<u>P</u>)	
	共有システム ボリューム システム ボリュームとして共有されるフォルダを指定してください。	\otimes
		S.
< 戻る(B) [- Sysvol フォルダにドメインのパブリック ファイルのサーバーのコピーが格納されます。Sysvol フォルダの内容 はドメイン内のドメイン コントローラすべてに複製されます。	
	Sysvol フォルダは NTFS 5.0 ボリューム上になければなりません。	
	Sysvol フォルダの場所を入力してください。	
	フォルダの場所(E):	

17

Active Directory のインストール ウィザード	×	
アクセス許可 ユーザー オブジェクトとグループ オブジェクトの既定のアクセス許可を選択してください。	Se la companya de la	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
Windows NT リモート アクセス サービスなど、いくつかのサーバー プログラムは、ドメイン されている情報を読み取ります。 ② Mindows 2000 12前のサーバーと互換性があるマクセス時間(P)	ノコントローラに格納	要求されるAdministratorのパスワー ドを入力します。
Windows 2000 以前のサーバーまたは Windows 2000 以前のドメインのメンバで 2000 サーバー上でサーバー プログラムを実行する場合は、このオプションを選択し	"ある Windows します。	
🔥 匿名ユーザーはこのドメインの情報を読み取ることができます。		
○ Windows 2000 サーバーとのみ互換性があるアクセス許可(E) Windows 2000 ドメインのメンバである Windows 2000 サーバー上でのみサーバ する場合は、このオプションを選択します。認証されているユーザーのみこのドメイ:	ー プログラム友実行 Active Directory のインスト	ル ウィザード ×
とかできます。	ディレクトリ サービス 復 ディレクトリ サービス 指定してください。	I元モード Administrator パスワード 復元モードでコンピュータを起動するときに使用する Administrator のパスワードを
< 戻る(B) 次へ(N)	ディレクトリ サービン アカウントに割り当	ス復元モードでコンピュータを起動するときに使用する、このサーバーの Administrator てるパスワードを入力して確認してください。
	パスワード(Ⴒ):	****
	パスワードの 確認入力(<u>©</u>):	*****
		< 戻る(B) 次へ(N) > キャンセル



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

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

- 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。

| 🔏 コンソール(C) ウィンドウ(W) ヘルプ(H)

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。



」 操作(A) 表示(V) 」 (中 → 配 VII-	IN I	2 💆 🛍 🟹	新しいオブジェクト - ユーザー	×
Active Directory ユーザーとコンピュータ	名前 ② Administrator	種類 ユーザー		新しいオブジェクト ニューザー 💌
Builtin Computers	Cert Publishers	セキュリティ グル セキュリティ グル セキュリティ グル	姓(L): smith	「作成先: YOUREDID DMAINIBIN com/Users
中國 Domain Controllers □-□ ForeignSecurityPrincipals □-□ Users 制御の委任	Domain Admins	セキュリティ グノ セキュリティ グノ セキュリティ グノ	名(E): イニシャル(D): 「 フル ネーム(A): 「smith	パスロード(P). 「********* パスロードの時期23入力(G3) 「*********
検索型 新規作成(<u>N</u>) すべてのタスク(K)	main Guests コンピュータ 連絡先	セキュリティ グノ セキュリティ グノ セキュリティ グノ	ユーザー ログオン名(U):	F ユーザーは次回ログオン株にバスワード変更が必要(M) F ユーザーはバスワードを変更できない(S)
表示(V) ここから新しいウィンドウ	グループ Owners プリンタ ユーザー	セキュリティ グノ ユーザー ユーザー	コーザー ログオン名(Windows 2000 以前)(W):	「「パスワードを無期税にする(<u>M</u>) 「「アカウントは無効(Q)
最新の情報に更新(E) 一覧のエクスポート(L) プロパティ(B)	共有フォルダ tet S and IAS Servers	ユーザー ユーザー セキュリティ グノ		
へルブ(<u>H</u>)	hema Admins InternetUser	セキュリティ グノ ユーザー	< 戻る(出) 次へ(い) >	

The next generation iSeries...simplicity in an on demand world

© 2003 IBM Japan Systems Engineering Co.,Ltd.



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

マイコンピュータのプロパティを開き、ネットワークDをクリックする。 識別の変更 ? X ? | X | 全般 ネットワーク ID | ハードウェア | ユーザー プロファイル | 詳細 | このコンピュータの名前とメンバシップを変更できます。変更するとネットワーク リソースへのアクセスに影響する可能性があります。 次の情報を使ってネットワーク上でこのコンピュータを識別します。 コンピュータ名(C): フル コンピュータ名: a01517.eimdomain.ibm.com a01517 ドメイン eimdomain.ibm.com ドメインにチェックし ドメ 5. フルコンピュータ名: ネットワーク識別ウィザードを使ってドメインへの参加およびローカ ル ユーザーの作成を行うには、「ネットワーク ID」をクリックしてくだ ざい。 イン名を入力。 a01517.eimdomain.ibm.com ネットワーク ID(N) 詳細をクリックし。 DNSサ 詳細(M).. フィックスを同じ名前で指 コンピュータ名を変更したりドメインに参加したりするには【プロパ ティ】をクリックしてください。 プロパティ(R) - 次のメンバー 定。 ● ドメイン(D): YOUREIMDOMAIN.IBM.COM ドメイン名/DNSサフィックス (YOUREIMDOMAIN.IBM.COM) ○ ワークグループ(W): キャンセル Ok DNS サフィックスと NetBIOS コンピュータ名 ? × OK. キャンセル 適用(品) このコンピュータのプライマリ DNS サフィックス(P): 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Dタブを開き、ネットワークD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	KDC KDC構成、Winユーザー登録 P2の登録
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	KDCドメイン参加 ID: Smith PWD: password p0
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	EIMドメインコントローラー
7. P2で、EIMユーザーの作成	p2.youreimdomain.ibm.com NAS構成 EIM構成
8. P2で、ユーザーのマッピング情報の登録	EIMドメイン追加 EIMユーザー(john smith)作成 P2(john),Winユーザー(smith)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。

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。
 Users を右クリックし、新規作成からユーザーを選択します。





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。

28

29



3. KDCへiSeriesP2の追加 ステップ2

新しいオブジェクト - ユーザー	x
	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。
教生(L): p2	このパスワードは、
名(E): イニシャルΦ:	 Kerberos チケット発行時(手順2ステップ2)
フルネーム(<u>A</u>): p2	■ EIM構成時(手順4ステップ4)
ユーザー ログオン名(山):	に使用されます。
@YOUREIMDOMAIN.IBM.OCM ▼	新しいオブジェクト - ユーザー 🔀
ユーザー ログオン名 (Windows 2000 以前)(W): YOUREIMDOMAIN¥ p2 〈 戻る(B) 次へ(N) 〉 キャンセノ	
	< 戻る(B) 次へ(N) > キャンセル

The next generation iSeries...simplicity in an on demand world



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。