Active Directory環境でのIceWallへのアクセス（信頼関係を結んでいる複数ドメイン編）

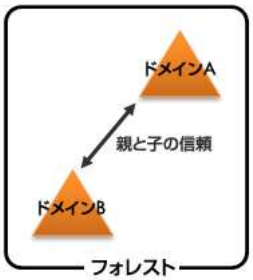
1.はじめに

複数のドメインで構成されるMicrosoft Active Directory（以下、MSAD）環境下でHP IceWall SSO Domain Gateway Option（以下、DGO）を使用する場合の注意点を記述します。

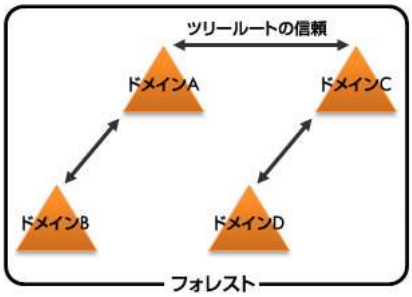
2.複数ドメインの構成

MSADは様々なドメインの構成が可能ですが、複数のドメインで構成される場合、主に以下のような構成が考えられます。

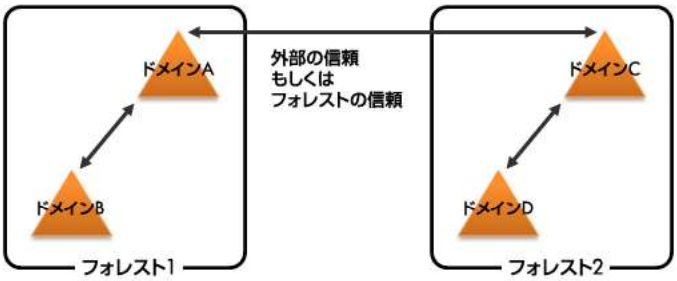
■1つのフォレスト、1つのドメイン・ツリー構成
下図のように1つのフォレスト内で1つのドメイン・ツリーが存在する構成です。
「ドメインA」と「ドメインB」では、推移的で双方向である「親と子の信頼」が確立されます。



■1つのフォレスト、複数のドメイン・ツリー構成
下図のように1つのフォレスト内で複数のドメイン・ツリーが存在する構成です。
「ドメインA」と「ドメインC」では、推移的で双方向である「ツリールートの信頼」が確立されます。



■複数のフォレスト構成
下図のように2つ以上のフォレスト間で信頼関係を確立した構成です。
フォレスト1の「ドメインA」とフォレスト2の「ドメインC」で、非推移的で一方向または、双方向である「外部の信頼」もしくは、推移的で一方向または、双方向である「フォレストの信頼」を確立します。



3.検証

3.1 検証のポイント

DGOによるSSOを実現するためには、連携対象のドメインにDGOのサービス・プリンシパル・ネーム（以下、SPN）を登録する必要があります。
1つのフォレスト、1つのドメインの環境においては、DGOのSPNを登録したドメインと、ユーザーが参加しているドメインが同じです。
この場合、ユーザーはDGOのSPNに対するチケットを取得可能なため、DGOによる統合Windows認証を利用できます。

一方、複数のドメイン環境においては、DGOのSPNを登録したドメインと、ユーザーが参加しているドメインが異なる場合が考えられます。この場合、ドメイン間の信頼の種類によっては、ユーザーはDGOのSPNに対するチケット取得が制限される場合があるので、DGOによる統合Windows認証が利用できない可能性があります。

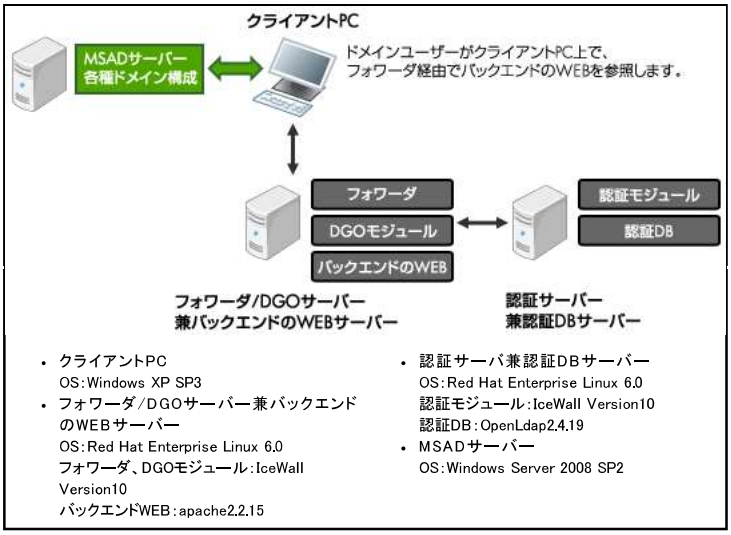
上記を考慮し、今回は、以下のドメイン構成について検証を行いました。

- 1つのフォレスト、1つのドメイン・ツリー構成
- 1つのフォレスト、複数のドメイン・ツリー構成
- 複数のフォレストが存在し、フォレスト間で双方向の「外部の信頼」を確立した構成
- 複数のフォレストが存在し、フォレスト間で双方向の「フォレストの信頼」を確立した構成

3.2 検証環境

基本構成は下図の構成とし、それぞれの検証パターンでは、ドメイン構成を変更することにより検証を実施し

ました。



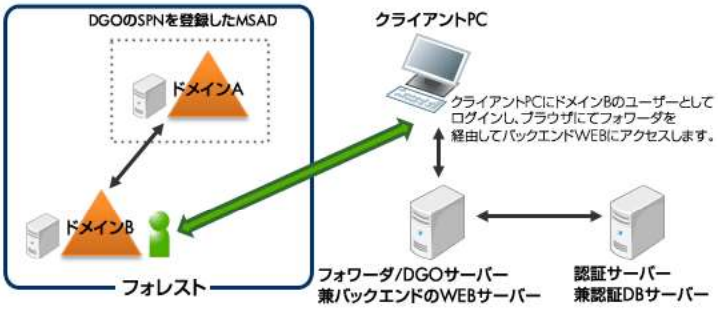
- クライアントPC
  OS：Windows XP SP3
- フォワーダ/DGOサーバー兼バックエンドのWEBサーバー
  OS：Red Hat Enterprise Linux 6.0
  フォワーダ、DGOモジュール：IceWall Version10
  バックエンドWEB：apache2.2.15
- 認証サーバ兼認証DBサーバー
  OS：Red Hat Enterprise Linux 6.0
  認証モジュール：IceWall Version10
  認証DB：OpenLdap2.4.19
- MSADサーバー
  OS：Windows Server 2008 SP2

3.3 検証パターン

検証したドメイン構成の詳細は以下の通りです。

■1つのフォレスト、1つのドメイン・ツリー構成

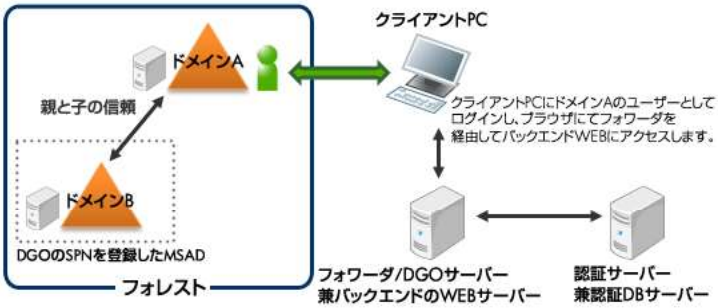
【パターン1】
DGO用のSPNを登録したドメインが親で、ユーザーを登録したドメインが子の場合ドメインAとドメインBは親と子の信頼が確立しています。



ドメインA
- フォレストの機能レベル：WindowsServer2000
- ドメインの機能レベル：WindowsServer2000
- DGO用のSPNを登録

ドメインB
- フォレストの機能レベル：WindowsServer2000
- ドメインの機能レベル：WindowsServer2000
- クライアントPCが参加
- ドメイン上に検証用ユーザーを作成

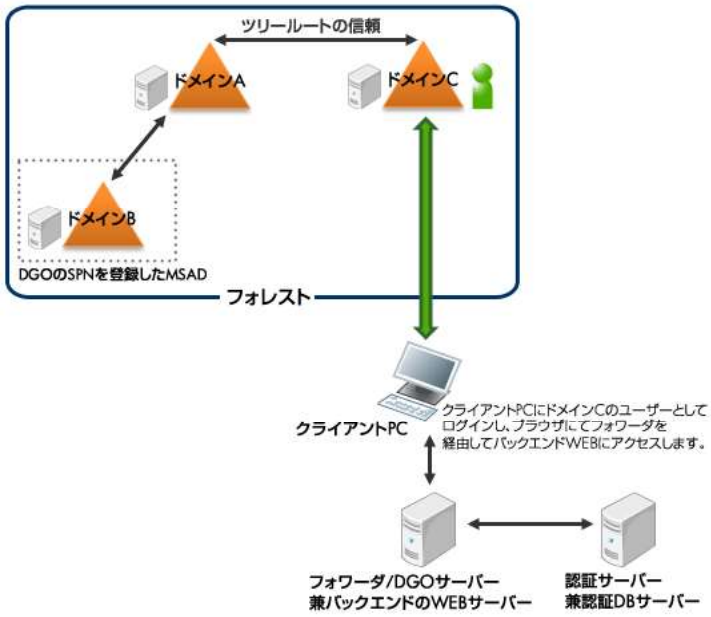
【パターン2】
DGO用のSPNを登録したドメインが子で、ユーザーを登録したドメインが親の場合ドメインAとドメインBは親と子の信頼が確立しています。



ドメインA
- フォレストの機能レベル：WindowsServer2000
- ドメインの機能レベル：WindowsServer2000
- クライアントPCが参加
- ドメイン上に検証用ユーザーを作成

ドメインB
- フォレストの機能レベル：WindowsServer2000
- ドメインの機能レベル：WindowsServer2000
- DGO用のSPNを登録

■1つのフォレスト、複数のドメイン・ツリー構成
DGO用のSPNを登録したドメインと、ユーザーが登録されているドメインが異なるドメイン・ツリーにある場合、ドメインAとドメインCは「ツリールートの信頼」が確立しています。

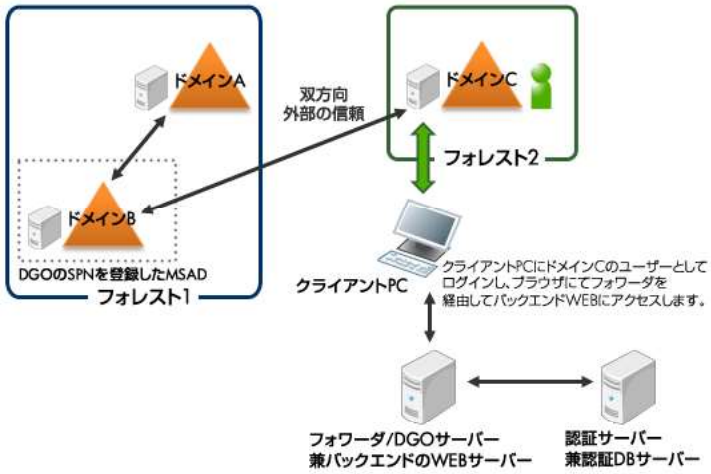


ドメインA
- フォレストの機能レベル：Windows Server 2000
- ドメインの機能レベル：Windows Server 2000

ドメインB
- フォレストの機能レベル：Windows Server 2000
- ドメインの機能レベル：Windows Server 2000
- DGO用のSPNを登録

ドメインC
- フォレストの機能レベル：Windows Server 2000
- ドメインの機能レベル：Windows Server 2000
- クライアントPCが参加
- ドメイン上に検証用ユーザーを作成

■複数のフォレストが存在し、フォレスト間で双方向の「外部の信頼」を確立した構成
DGO用のSPNを登録したドメインと、ユーザーが登録されているドメインが異なるフォレストにある場合、「外部の信頼」は推移しないため、ドメインBとドメインCに双方向の外部の信頼を確立しました。

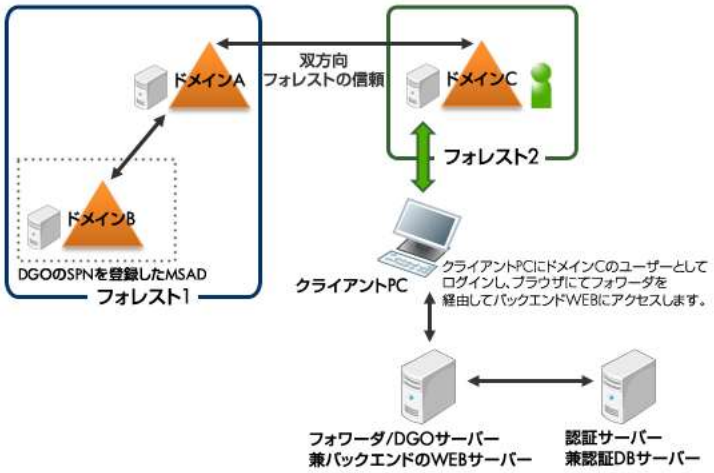


ドメインA
- フォレストの機能レベル：Windows Server 2000
- ドメインの機能レベル：Windows Server 2000

ドメインB
- フォレストの機能レベル：Windows Server 2000
- ドメインの機能レベル：Windows Server 2000
- DGO用のSPNを登録

ドメインC
- フォレストの機能レベル：Windows Server 2000
- ドメインの機能レベル：Windows Server 2000
- クライアントPCが参加
- ドメイン上に検証用ユーザーを作成

■複数のフォレストが存在し、フォレスト間で双方向の「フォレストの信頼」を確立した構成
DGO用のSPNを登録したドメインと、ユーザーが登録されているドメインが異なるフォレストにある場合、フォレスト、ドメインの機能レベルをWindows Server 2003にアップデートし、ドメインAとドメインCに双方向のフォレストの信頼を確立しました。



ドメインA
- フォレストの機能レベル：Windows Server 2003
- ドメインの機能レベル：Windows Server 2003

ドメインB
- フォレストの機能レベル：Windows Server 2003
- ドメインの機能レベル：Windows Server 2003
- DGO用のSPNを登録

ドメインC
- フォレストの機能レベル：Windows Server 2003
- ドメインの機能レベル：Windows Server 2003
- クライアントPCが参加
- ドメイン上に検証用ユーザーを作成

4.検証結果

検証結果を以下に示します。

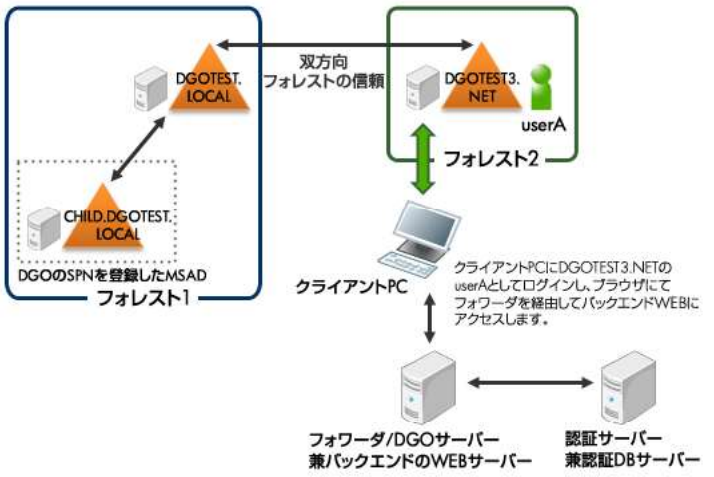
環境		統合Windows認証の可否
1つのフォレスト、1つのドメイン・ツリー構成	パターン1	可
	パターン2	可
1つのフォレスト、複数のドメイン・ツリー構成		可
複数のフォレストが存在し、フォレスト間で双方向の「外部の信頼」を確立した構成		不可
複数のフォレストが存在し、フォレスト間で双方向の「フォレストの信頼」を確立した構成		可

5.Kerberosチケット確認ユーティリティ（Kerbtray）について

Kerberosの認証要求のルーティングが出来ない等の原因によりクライアントPCがDGOのSPNに対応するKerberosチケットを取得できなければ、DGOによる統合Windows認証はできません。

Kerberosチケットの取得状況は、Windows 2000/2003のResource Kitに付属しているKerbtray ユーティリティをクライアントPC上で実行することにより確認できます。

以下は、複数のフォレストが存在し、フォレスト間で双方向の「フォレストの信頼」を確立した場合の例です。



以下のように、クライアントPCでDGO用のSPNが確認出来れば、Kerberosチケットが取得できています。

DGOによる統合Windows認証がチケットの問題でうまく動作しない場合、Kerbtrayユーティリティを使用して問題の切り分けを行うことをお勧めします。

6.まとめ

1つのフォレスト内でのドメインは、双方向の推移的な信頼である「親と子の信頼」もしくは、「ツリールートの信頼」が暗黙的に確立されます。
「親と子の信頼」、「ツリールートの信頼」は、Kerberosの認証要求のルーティングが可能なため、DGOによる統合Windows認証が可能です。

一方、複数のフォレストのドメインは「外部の信頼」もしくは、「フォレストの信頼」を明示的に確立する必要があります。
DGO用のSPNを登録したドメインと、ユーザーが登録されているドメインが異なるフォレストにある場合、「フォレストの信頼」では推移的な信頼が確立され、Kerberosの認証要求のルーティングが可能なため、DGOによる統合Windows認証が可能ですが「外部の信頼」は非推移的な信頼であり、Kerberosの認証要求のルーティングがサポートされないため、DGOによる統合Windows認証ができません。

上記より、複数ドメインの環境において、DGO用のSPNを登録したドメインと、ユーザーが参加しているドメインが異なる場合、DGOによる統合Windows認証が可能な構成は以下の通りとなります。

1つのフォレスト環境
　フォレスト及びドメインの機能レベルがWindows2000以上で親と子の信頼、ツリールートの信頼が確立されている環境

複数のフォレスト環境
　フォレスト及びドメインの機能レベルがWindows2003以上でフォレスト間で、フォレストの信頼が確立されている環境

7.おわりに

ここで述べた内容な技術的観点に基づいて検証した結果を示したもので特定の環境での動作や性能を保証するものではありません。
実際の構築に関しては、HPまたはHPパートナーへご相談ください。

関連リンク
≫ 信頼の種類とは
≫ 異なるドメインのリソースにアクセスする
≫ 異なるフォレストのリソースにアクセスする
≫ Windows 2000 Resource Kit Tool: Kerbtray.exe
≫ Windows Server 2003 Resource Kit Tools

関連技術レポート
Domain Gateway オプションの環境構築における考慮点
Active Directory環境でのIceWallへのアクセス（信頼関係を結んでいない複数ドメイン編）

2010.11.30 新規掲載
2020.6.1 記事タイトルを変更

執筆者
日本ヒューレット・パッカード　テクノロジーコンサルティング統括本部　スペシャリスト　小寺 孝一郎
日本ヒューレット・パッカード　テクノロジーコンサルティング統括本部　テクニカルコンサルタント　岩井 隆夫