第三回 IT マネジメント研究会 初心者編（東京） 議事録
日時： 2011/4/22（金）15:00～17:30 会場： クオリティ(株) 本社 6F 会議室
テーマ： Active Directory を使った PC セキュリティ設定のいろは
講師： グローバルナレッジネットワーク株式会社 取締役 技術担当　横山 哲也 氏
司会・進行： IT マネジメント研究会 初心者編 副座長 株式会社リコー IT/S 本部 IT/S 技術センター システムインフラグループリーダー 兼 IT/S 企画センター ソリューション事業支援室 中俣 幸二 氏
※当研究会の運営方針により、個人/会社名を特定できる発言、および発表者から公開の許可を得られなかった内容は 議事録より削除されています。あらかじめご了承ください。
今回は Microsoft Active Directory(以下、AD)をテーマにグローバル ナレッジ ネットワーク株式会社の横山哲也氏にご講演いただき、参加者の方々から、現在の運用に関する情報交換や自社で行っている AD の活用方法など、活発な意見交換が行われました。 以下、第二部ディスカッションでのやりとり＝＝＝＝ Q：AD というのは、全社一括で始めたほうがいいのか、または出来る範囲から始めたほうがいいのか？ A：全社導入がよいです。理由は：DNS で使われるドメイン名の矛盾をなくすためです。個々のネットワークごとに独立して AD を導入するとドメインの統合ができません。複数の AD を連携させるのは難しいため、本来は全社一括での導入が望ましいです。 Q：私の会社では、すでに AD を勝手に立ててしまっている。どうすれば解決できるのか？ A：AD を連携させることはできます。その条件は DNS の名前が違う（NT の名前）が違うことです。 名前が違えば連携できます。 Windows Server 2003 以降ですが、フォレスト信頼の設定を行うことで可能です。ただドメインコントローラの数は減りません。単一のドメインに統合する場合は、ADMT（アクティブディレクトリマイグレーションツール）を使うことで、ユーザをコピーしてくることができます。クライアント PC のドメインの付け替えも可能。再起動まで実施します。 統合後にドメイン名を変更することはできます。ただしその作業手順の数が 10 以上あるため、ドメインの変更は非常に面倒です。 Q：名前から電話番号を検索するサービスを知っている。このディレクトリサービス以外の、たとえばプリンターの設定をするような便利な機能を知りたい。 A：プリンターの設定を行う機能は AD にはありません。プリンター関連では共有プリンターの名前を登録する機能があるぐらい。これはプリンターの利用をユーザや PC に割り当てることができるものです。プリンター関連の設定は AD ではなく、プリンタサーバがドライバーを自動でインストールしてくれる

ものです。

Q：私の会社も AD が各部門ごとに入っています。ただ Mac を使う部署があり、そこはドメインに参加させていません。
しかし Windows PC と Mac でファイルを共有したいものがある。ファイルサーバは Windows 側で使っている。そのファイルサーバに Mac からアクセスできない。なぜでしょうか。

A：アクセスできます。Mac が使っているワークグループのユーザごとに AD のユーザ ID/PASS を作ることで可能になるはずです。

Q：AD は、システム管理者にとって、どのようなメリットがあるから使っているのか？
会社でも使われているが、私自身が直接 AD を操作しているわけではないので、使っていることは分かってもどんなシーンで使われているのかなど、その効果を体感できていない。

■AD を使っている方は挙手をお願いします。
＜参加者の挙手＞→AD を使っているのは 7 割。

■また AD が便利だと思う方挙手をお願いします。
＜参加者の挙手＞→AD を使っていて便利だな：4 割

＜参加者：AD が便利だと思う理由＞
■プロキシの設定を自動化できるところが便利です。またファイルやフォルダのアクセス管理も便利です。ただし自社の設定方法で正しいのかなと不安になる時もあります。
■グループポリシーを一部使っています。4 月の人事異動の時は、アクセス権の設定が簡単にできてよいで
す。AD でこういうことできないかなと思って WEB を検索してみると見つかる場合がある。しかし簡単にさがす手段がわからない。それがあるともっと便利だと思う。AD でよくわからなくなるのは、サーバ側の設定なのかユーザ側なのか混同する時がある。

＜講師から＞
■ネットワークの下の階層で、AD に関するすべての設定を見ることができます。
サポートされるバージョンもそこで把握できます。グループポリシーは増えることはあっても今後も減ることはないと思います。先ほど質問いただいた回答ですが、Windows の設定の方に、プリンターの項目があります。機能としては、サーバプリンタをデフォルトプリンタに設定するというものがあります。プリンターの項目に関しては Windows XP までは、細かな設定はできません。ただ Vista 以降で大きく変わりました。ドメインコントローラは Windows Server 2003 のままでよく、クライアントの OS をバージョンアップするだけで使えるようになります。

Q：私の会社では今現在、NT のドメインコントローラから AD に移行している最中です。
グループに NT ドメインのユーザを一括で登録しています。ローカルコンピュータのローカルグループを制御することはできるか。
A：グループポリシーの「制限されたグループ」を使えば、ドメインメンバーのローカルグループを制御できる。

Q：AD 認証ログオンに関する質問で、たまにネットワークが切れていると、ログオン出来なくて困っている。
A：ユーザのキャッシュが切れているのではないか。または持ち出し先のネットワークで、別のネットワークにつながってしまうのではないか？

Q：まれにグループポリシーが適用されない場合がある。どうしたら操作できるか？
A：Windows Vista では、ログオン途中でポリシーを適用している。一部のポリシーは完全にログインしないと適用されないものがあるため、最大では 3 回ログインしないと適用されない場合がある。それが原因ではないか？ちなみにポリシーが当たっているかどうか確認するコマンドは以下のとおり。

```
gpresult /z
```

Q：ポリシーの設定を強制したい。
A：改めて適用するコマンドを実行するしか方法はない。グループポリシーが外れたら初期設定に戻る。ちなみにプロキシの設定はグループポリシーで設定します。ユーザの設定はログオン時、PC の設定は起動時。キャッシュログオンした場合は前回の設定が適用。キャッシュはユーザローカルに残るので、クリアされることはない。

Q：2008 ドメインから 2008R2 の強化について教えてほしい。
A：一旦削除したユーザを 180 日以内であれば復元できる。コマンドで実行していたものが GUI でできるようになった。

Q：ファイル・フォルダのアクセス権について質問。フルアクセスの権限をユーザに与えると、他のユーザへの権限付与が可能になるが、フルアクセスを与える権限を与えるというのはどういうケースで起こるのか？
A：編集の権限だけなら、リード/ライトの権限で対応できる。フルアクセスの権限は、外部・部外に公開していいかどうかを決定する人にあたえる。フルコントロールはその情報をすべて変更できる。複数拠点がある場合、システム管理者が行けない。その拠点のリーダに与えればよい。

Q：まだ AD を使っていません。情報収集段階です。Windows 7 の切り替え。AD を入れるかどうか検討中。切り替えの際の工数はどれぐらいでしょうか？

A：NT ドメインから 130 名前後のユーザであれば 1 日で移行。検証は半日で終わります。100 人クラスであれば 1 日。

Q(質問者)：クライアントの移行が大変そうなイメージがあります・・・。

A：ドメインを変更するバッチファイルを作ることはできる。

Q：データの持ち込みの制御を AD で行いたい。CD-ROM を読み込ませたくない。

A：リムーバブルメディアの禁止という設定がある。

Q：プロファイル移行に時間がかかりそう。特殊な環境で 1 台につき 30 人ぐらいのプロファイルがある。

A：USMT というツールがある。現在のサポートバージョンは覚えていないが Windows XP は確実にサポートされる。Windows 7 で強化された機能を使えば、同じ PC での OS の入れ替えなら数分で移行できる。

Q：OU の使い方、関連性がはっきりしない。

A：OU とはアクティブディレクトリの中の階層構造のことで管理される物。OU にいるから管理できるものではない。

OU の目的は３つ。

【分類】（セキュリティ的意味はなし）

【管理制御】（OU の中にいる誰かに委任権限する。）

現場のマネージャーにパスワードのリセットを委任する。ユーザ登録の委任もできる。

【GPO の適用単位】グループポリシー設定の最小単位

Q：今から Windows Server 2003 と 2008 のどちらの勉強をするといいのか？

A：両方勉強するしかない。毎日コミュニケーションズの AD の本がおすすめです。

「実践 Active Directory 逆引きリファレンス」