WSUS を用いた AD による Windows Update の集中管理

藤原冨未治*、鬼頭良彦*
*工学研究科・工学部技術部 電子・情報技術系

はじめに

現在多くのユーザが使用している Windows 系 OS ではそのバージョンを問わず頻繁にセキュリティアップデートが行われている。これらの修正プログラムを OS 上に繁栄させるためには、Windows 標準機能である Windows Update を用いて修正プログラムをインストールする必要がある。この作業は、個々のコンピュータ毎に行わなければならない作業であり、修正プログラムが更新する毎に行なわなければならないことである。

電気系計算機室では、学生、教職員等電気系に所属する構成員が自由に使用できる共通の Windows 系コンピュータが配置されており、これらのコンピュータにおいても同様な作業が生じる。設置されているすべてのコンピュータに対して行わなければならない作業であるため、OS のバージョンによらず、集中的に一元管理することができれば作業時間と効率、労力の大幅な削減につながるはずである。

そこで本研鑽では Windows Server 上で Active Directory（AD）によるグループ・ポリシーを作成し、Windows Server Update Service（WSUS）をサーバ構築することにより、同一ドメイン内でのクライアントコンピュータにおける Windows Update の集中管理を行うことを目的で行った。

1. Active Directory とは

Active Directory(以下 AD)とは、Windows Server で提供されるディレクトリ・サービスのことである。ネットワーク上のユーザ情報やコンピュータ情報、グループ情報など、さまざまな資源をまとめて管理することができる。ユーザ情報では、ログイン ID、パスワード、コンピュータ情報では、ドメインに参加できるコンピュータを、またグループでは学生のグループ、職員のグループという単位として管理ができる。

この、AD の情報を元にドメイン内のクライアントコンピュータは、参加資格と、サーバへのログインの確認を行い、データベースでのデータ保持とそれを元にしたユーザ認証が行われる。

AD は「ドメイン」という単位で管理する範囲を定義している。組織で 1 つのドメインを作成すれば、組織内のユーザ、コンピュータ、グループ、サービスなどを集中して管理することができるようになる。

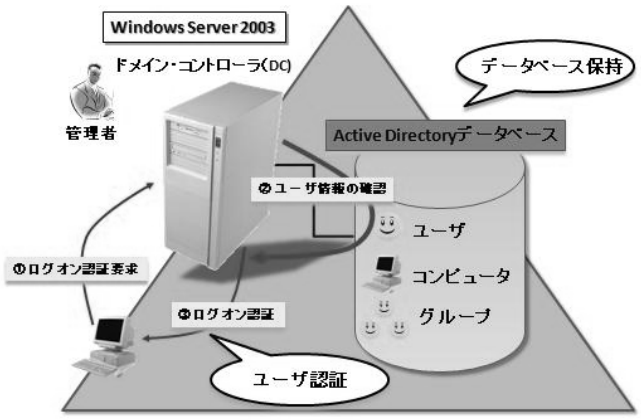

図 1. AD の概念

通常の Windows Network であるワーク・グループとの一番の違いは、認証の確認を行うかどうかという点である。

2. Windows Server Update Service とは

マイクロソフトが提供する個人ユーザ向けのパッチ管理として Windows Update がある。この Windows Update は、マイクロソフトがネットワーク上に用意したパッチダウンロードサーバに、ユーザが個々にアクセスして、パッチをダウンロードし、適用するサービスである。（図 2. ①）

しかし、この作業は管理権限を持ったものが行う必要があるため、多数のユーザが接続する環境にある場所では、この作業は現実的ではない。管理サーバを用いてクライアントを集中管理している場所で、全ユーザに対し管理権限を与えることはセキュリティ上到底できないことであるため、Windows Update をユーザ単独で実行するのは不可能となる。また、独自開発アプリケーションによっては Windows Update でのパッチ適用により不具合が発生する場合もある。

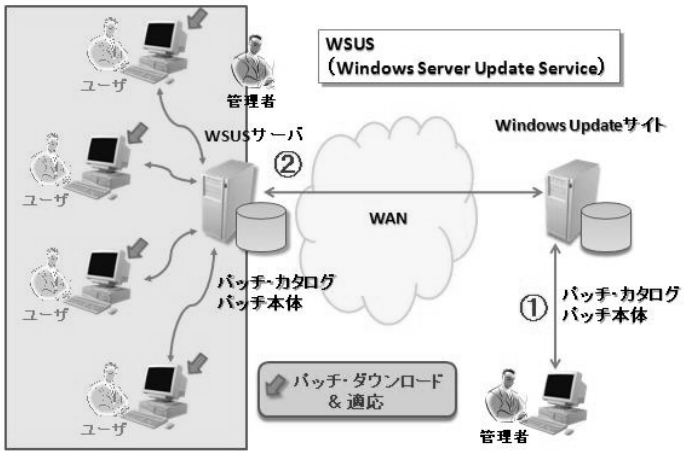

図 2. WSUS の概念

これらをマイクロソフトが事前に互換性検証を行うことは困難であるため、不具合が発生しないかどうかテスト環境で確認する必要がある。しかし、Windows Update では、パッチ適用の有無を制御することはできないため、集中管理している所に対しマイクロソフトが提供したのが Windows Server Update Service（以下 WSUS）である。（図 2. ②）

WSUS では、クライアントはインターネット上の Windows Update サイトではなく LAN 上に設置された WSUS サーバにアクセスしてパッチを適用する。WSUS サーバは、定期的に Windows Update サイトにアクセスしてパッチをダウンロードしパッチを常に最新の状態にする。また WSUS サーバは、ドメイン内のクライアントに対してパッチ適用の有無（許可/不許可）を管理でき、どのクライアントに対してどんなパッチが当たっているかということや、いつどのパッチを当てるかということも制御可能となっている。

3. システム構成

WSUS を利用するには、サーバとなるコンピュータ（以下 WSUS サーバ）に WSUS をインストールし、管理される側のコンピュータ（以下 WSUS クライアント）側に自動更新コンポーネントをインストールする必要がある。

このため、仮想ローカルネットを構築しサーバとして Windows Server 2003 をクライアントとして Windows XP、Windows 2000 を用意し、ルータを介してインターネットに接続する環境を構築した。この環境内の

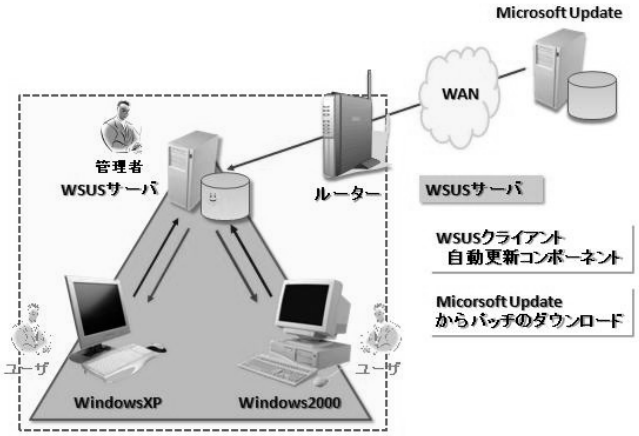

図 3. システム例

Windows Server 2003 上に WSUS をインストールし WSUS サーバにした。

AD 環境であるため、各 WSUS クライアントの設定にはグループ・ポリシーが利用でき、Windows Server 2003 側から一括管理が可能である。自動更新コンポーネント自体は Windows Update を利用する場合と同じであるが、同期先はインターネット上の Windows Update サーバではなく、LAN 内の WSUS サーバを指定する。WSUS サーバ側では、インターネット上の Windows Update サーバと同期して、新しいパッチを定期的にダウンロードするように設定する（手動での同期も可能）。

また管理者は、パッチのうちどれを WSUS クライアントに適用するか、しないかなどをあらかじめ設定しておく、各 WSUS クライアントは定期的に WSUS サーバにアクセスし、自身のパッチ適用状況を WSUS サーバ側に報告し、定められたルールと自身のパッチ適用状態を比較してどのパッチを適用するか決定する。これにより OS の違いによるパッチ適用の管理も可能となる。

4. WSUS の実施例

WSUS サーバの管理・レポート機能は、Internet Explorer を介してアクセスすることができる。ドメインに参加し、AD で管理されているクライアント情報が個別に設定、閲覧できる。図 4. は今回構築した実験用ネットワークでドメインに参加している WSUS クライアントの一覧である。各クライアントのパッチ情報は、クライアントから送られてくる適用状態と現在サーバで持っているパッチ情報が照らし合わされレポート形式で、必要の有無、すでにインストールされているのかどうかパッチの一覧として確認できるようになっている（図 5.）。これらの情報表示は、グループ単位で行うことがでるため、OS 毎のグループ設定を施せば表示形式をグループ単位でまとめることがで

図 4. WSUSークライアント一覧

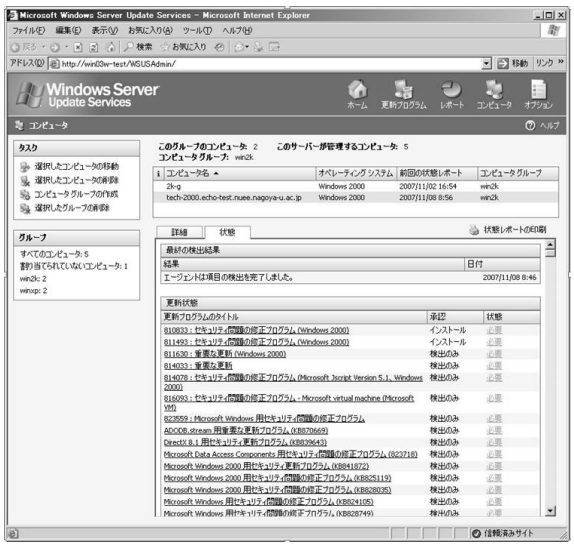

図 5. パッチ一覧（適用前）

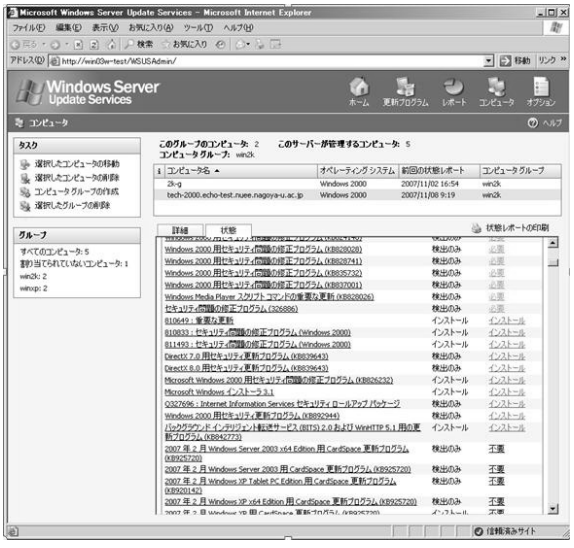

図 6. パッチ一覧（適用後）

きる。

ここで、必要なパッチでまだインストールされていないパッチに対してインストール許可を与える設定を加えると、WSUS クライアントは設定された適用時間もしくは次回起動時にそのパッチが自動的にインストールされ、それらパッチ適用情報が起動するたびごとに WSUS サーバの管理情報に反映されることになる。（図 6.）

なので、もし AD 上で独自のアプリケーション等のドメイン固有にインストールされているものがあった場合（パッチを当てることにより動作保障が難しいと思われる場合）は、まずテストクライアントに導入し、動作チェックをした後すべてのクライアントに配布するといったことが可能となる。

5. まとめ

昨年に引き続き Windows Server 2003 の設定を行い、問題なくサーバの構築を行うことが出来、AD の構築・設定、WSUS のインストール及び設定も問題なく行うことが出来た。 これにより今後 Windows Server 2003 の構築機会があった場合のノウハウを蓄積することが出来た。

AD を用い、クライアントの Windows Update サービスの自動化を行うことが出来るようになった。さらに WSUS の機能を用いてクライアントのセキュリティ・パッチ適用の有無の確認が出来るようになり、パッチの適用をクライアント毎に設定出来ることが確認できた。

また、WSUS によりクライアントである Windows 2000、Windows XP という異なる OS での Windows Update の制御が可能なことが確認できた。

これらのことにより、本研鑽での主目的であった Windows Server 上で AD によるグループ・ポリシーを作成し、WSUS をサーバ構築することで、同一ドメイン内で管理できるクライアントコンピュータの Windows Update を集中的に管理するということは十分達成できたと思われる。

今後の予定としては、クライアントとしてまだ Windows Vista での検証を行っていないため今後の普及に備え検証を行って行きたいと考えている。

参考文献

[1] 岡崎俊彦, “Windows Server 2003 サーバー構築ガイドブック R2 対応版”, ローカス

[2] 村嶋修一, “Windows Server 2003 実践ガイド”, 技術評論社

[3] 小川誉久, “Windows Server Update Services（前編）”, アットマーク・アイティ

[4] 小川誉久, “Windows Server Update Services（後編）”, アットマーク・アイティ

[5] 山近慶一, “これから始める WSUS 3.0 入門（前編）”, アットマーク・アイティ

[6] 山近慶一, “これから始める WSUS 3.0 入門（後編）”, アットマーク・アイティ