特集2

SUSはWindows管理者の救世主となるか

たかはしもとのぶ
text by TAKAHASHI, Motonobu

はじめに

本誌をお読みの方であれば、「Microsoft社はセキュリティ強化プログラムであるSTPP（Strategic Technology Protection Program）の一貫として、2002年6月24日からSUS（Microsoft Software Update Services）というプロダクトを無償でリリースしています。SUSは企業内Windows Updateサーバーともいうべきもので、企業内の各クライアントに対するホットフィックスの配布とその管理を行ないます」というような説明文[注1]を、各所のWebサイトなどでイヤというほど目にしていることでしょう。ですから、いまさら繰り返すまでもないでしょう。

このように、一見聞こえのよいセリフの並んだSUSですが、本当に使えるプロダクトなのか大いに気になるところです。筆者も早速このSUSについて検証などを行なってみましたので、以下その結果をふまえてSUSの実体について説明していきたいと思います。

注1）このレベルの情報は山ほどありますが、とりあえずMicrosoft社からのプレスリリースのページを紹介しておきます（http://www.microsoft.com/japan/presspass/releases/062402sus.asp）。

Windows Updateの概要

SUSの説明をはじめる前に、SUSのベースとなったWindows Updateについて簡単に説明しておきましょう。

ご存知のように、Windows Update（http://windowsupdate.microsoft.com/）は、セキュリティ関連のホットフィックス（HotFix）や、Microsoft社が重要だと考える製品のアップデートなどを、比較的簡単にインストールすることができるWebサイトです。

- 怪しいActive X Controlをインストールされてしまう
- セキュリティ関連のホットフィックスがWindows Updateで提供可能になるまでには、ホットフィックス自体が入手可能になってから若干のタイムラグがある
- すべてのホットフィックスがWindows Updateからインストール可能というわけではない

といった懸案事項もありますが、いままで何かと繁雑で、とても一般の人に覚

えてもらえるレベルではなかったホットフィックスなどのインストール作業を、一般の人にも何とか覚えてもらえるレベルまで簡便に行なえるようにしたという点では、Windows Updateの意義は大きいと思います。

また、Windows XPや、追加モジュールをインストールした[注2] Windows 2000では、「Windowsの自動更新」という機能を利用することで、自動的に修正モジュールをダウンロードしてインストールすることも可能となっており、その手間はさらに低減されています。

しかし、図2に示すように、Windows Updateはどちらかというと個人ユーザーをターゲットとしたサービスのため、企業内での利用を考えると以下に挙げるような問題点がありました。

問題 1

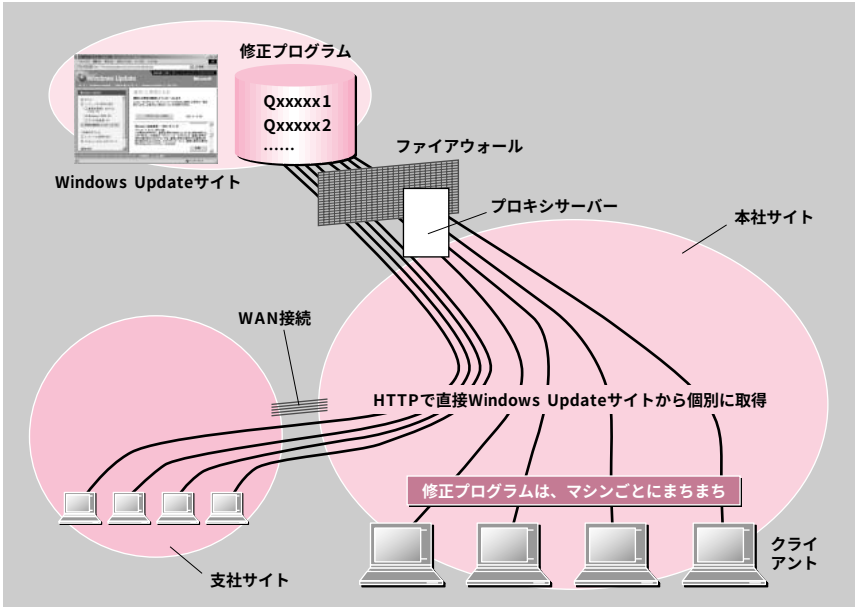
マシンにインストールするホットフィックスなどの管理ができない

企業システムでは、管理上の手間を削減するために、各マシンの環境を同一にしている場合が多いと思いますが、Windows Updateには、マシンにインストールするホットフィックスなどをシステム管理者が指定したものに限定する、あるいは指定したものについては強制的にインストールする、また各マシンにどのようなホットフィックスがインストールされているかをシステム管理者から簡単に参照できるようにするといった管理機能はまったくありません。

管理が行き届かないまま、各マシンでWindows Updateからホットフィックスや Internet Explorerの最新版などをダウンロード、インストールしてしまうと、最悪業務システムが動作しないなどの問題を引き起こしてしまうこともあります。

図1：Windows 自動更新

図2：Windows Updateの概念図



問題 2

通信量が増大する

Windows Updateを利用してホットフィックスなどをインストールしようとすると、インターネット上のWindows Updateサイトからファイルをダウンロードします。しかも、古いモジュールを

注2）Windows Updateから「Windows自動更新2002年6月」を選択して（図1）、インストールします。

インストールできないようにするという配慮のためか、キャッシュを無効にする設定が行なわれているため、途中にキャッシュサーバーなどを配置していても、毎回インターネット上からファイルのダウンロードが行なわれてしまいます。ファイルにはInternet Explorerなど数10MBに達するものもありますので、マシンの台数が多いと、インターネット回線の通信量にも無視できない影響が発生してしまいます。

問題3

インターネット接続が大前提である

プロキシ（キャッシュ）サーバー経由でもかまいませんが、とにかくHTTPプロトコルでWindows Updateサイトに接続できる環境が必要ですので、完全にクローズドなシステムでは利用できません。

こうした理由のため、企業内ではWindows Updateを無効にする、もしくは利用を禁止せざるを得ないケースが多かったのではないかと思います。

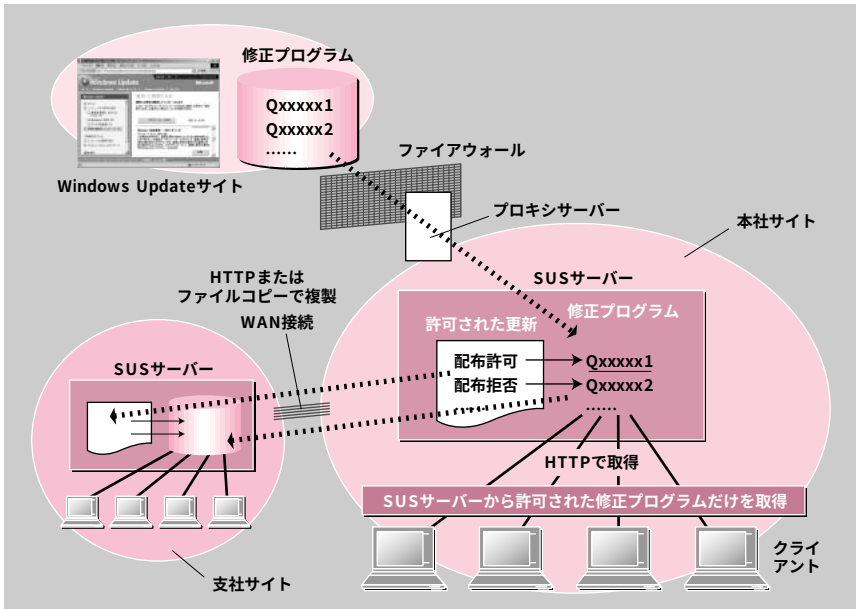
SUSの概要

SUSは、Windows Updateのこうした現状を踏まえて、企業内での利用を前提としてデザインが行なわれています。

図3のように、SUSを利用すると、各クライアントのマシンは、SUSサーバーから修正プログラムをダウンロード、インストールすることが可能になります。SUSサーバー自身はインターネット上のWindows Updateサイトや、別のSUSサーバーから修正プログラムをダウンロードします。インターネット上のWindows Updateサイトと通信する必要があるSUSサーバーは最低1台あればすむので、インターネットとの通信量を最低限に押えることが可能となり、問題2や問題3が解決します。また、具体的な方法は後述しますが、SUSサーバー間の複製は、オフラインでのファイル受け渡しで行なうことも可能なの、物理的にインターネットと接続されていない完全にクローズドなネットワークでも、SUSの恩恵を受けることが可能です。

さらに、SUSサーバーでは、Windows Updateサイトからダウンロードした修正プログラムのうち、どれをクライアントからインストール可能にするかを個別に制御できるので、問題1で指摘した修正プログラムの管理の問題もある程度解消します。ただし、クライアント側にインストールされる「Windowsの自動更新」も、指定したSUSサーバーから修正プログラムをダウンロードすることや、Active DirectoryのGPO（Group Policy Object）などを使って設定を一元的に制御できるようにバージョンアップすることが必要です。

図3：SUSの概念図



SUSとWindows UpdateやSMS

このように、SUSは、Windows Updateの問題点のいくつかを解決することにより、企業内でWindows Updateの機能を活用することを可能にするソリューションであると言えます。ただし、完全にWindows Updateを置き換えることができるものではありません。以下にSUSではできないWindows Updateの機能を示します。

サポートOS

SUSはWindows 2000/XPのみをサ

表1：SUS/SMS/Windows Updateの比較

	Windows Update	SUS	SMS
配布可能なプログラム	一部の修正プログラム、SPなど	重要な修正プログラム（Windows Updateより限定されている）	任意のプログラム（ただし基本的には要カスタマイズ）
配布対象プログラムの管理	マシンごとに管理、プログラム単位で指定	中央で一元管理、プログラム単位で指定	中央で一元管理、さまざまな条件で指定できる
配布時間などの指定	手動、簡単なスケジューリング（厳密な制御ができない）	手動、簡単なスケジューリング（厳密な制御ができない）	手動、厳密なスケジューリング
配布状況の管理	マシンごとに管理、GUIで管理できる	中央で一元管理、ログファイルベース	中央で一元管理、GUIで管理できる
管理性	一般ユーザー向けのサービスであり容易	機能が限定されているため容易	非常に難解

ポートします。一方Windows UpdateはWindows 98以降のWindows 9x系OSと、Windows NT 4.0でInternet Explorer 4.0以上が動作するWindows NT系OSからアクセスできます。

インストール可能な修正プログラム

SUSでインストールできるのは、

- Windows重要な修正プログラム
- Windows重要なセキュリティ修正プログラム
- Windowsセキュリティロールアップ

だけです。

また、従来からMicrosoft社が企業内でのファイル配布用途などに用いる製品として販売しているSMS（Systems Management Server）と競合しないようにという意図があってか、前述した特定の修正プログラム以外の配布は行なえない仕様になっているほか、スケジューリング機能や、配布状況の管理機能などが意図的に中途半端なものになっているという感じがします。

要点を表1に簡単にまとめましたので、参照してみてください。

SMS（またその他のファイル配布プロダクト）をすでに使って修正プログラムの配布を行なっているのであれば、あえてSUSを使う必要はないでしょう。

なお、管理性については特に説明していませんが、これについては以下具体的なインストールや設定方法について説明しますので、そちらを参照してください。機能が限定されていることもあって、設定や管理は非常にシンプルです。

SUSのインストール

それでは、以下具体的なインストール方法について説明していきましょう。といっても、SUSのインストールは非常に簡単ですので、迷うことはないと思います。

ただし、SUSサーバーになれるのは、Internet Explorer 5.5以上を搭載しており、IIS 5.0がインストールされたWindows 2000 Server SP2以降のみとなっています。しかも、FAQのページ[注3]に記載していますが、ドメインコントローラはSUSサーバーになることができませんので、SUSをインストールできるのは、メンバサーバーかスタンドアロンサーバーのいずれかに限定されます。また、インストール先のパーティション（またはボリューム）は、NTFSでフォーマットされている必要があります。ただしFAQのページにある

「x86または互換P700レベルプロセッサ、512メガバイト（MB）のRAM、および6ギガバイト（GB）のディスク空き容量が必要です。」

という最低限必要なハードウェアについての記述については、あまり気にする必要はないようです。実際筆者の手元では、

「Celeron 566/256MB/空き容量5GB（インストール時）」

というマシンで問題なく検証などが行なえています。

バイナリの取得とインストールの開始

まずは、SUSのバイナリをダウンロードしてください。MSI形式のバイナ

注3）http://www.microsoft.com/japan/windows2000/windowsupdate/sus/susfaq.asp

図４：「ファイルの場所の選択」画面

図５：言語の設定

リがSUSのホームページ[注4]から取得できます。ファイルの容量が47MBありますので、回線が細い場合には注意してください。

ダウンロードが完了したら、インストールを行なう前に「インターネットインフォメーションサービス」から、動作中のIISのWebサイト[注5]をすべて停止しておくことをお勧めします。

SUSの実体は、大きく分けると各種の管理を行なうためのWebアプリケーション、クライアントに修正プログラムを配布するためのWebサイト、およびSoftware Update Serviceというサービスから成りたっています。

Webアプリケーションの部分は、デフォルトで「既定のWebサイト」にインストールされますが、その際、Webサイトのディレクトリ直下にいくつかのファイルを置いてしまうので別のWebサイトとして分離するに越したことはないでしょう。動作しているIISのサイトがなければ、インストール過程でSUSというWebサイトが自動的に生成され、SUSを構成するファイルもそこに置かれます。

IISの設定を終えたら、早速アイコンをクリックしてインストールを開始しましょう。

ウィザードにしたがって、インストールを行なっていくとセットアップの種類として「標準」と「カスタム」を指定する画面が現れます。ここで「標準」を選択した場合、以下で説明する設定がデフォルトの値に設定されます。設定自体は後で変更できますが、SUSのWebサイトを構成するファイルの位置を後から変更するのは面倒ですので、「カスタム」でのインストールをお勧めします。以下「カスタム」を選択した場合を例にとって説明します。

「カスタム」インストールの設定

「カスタム」を選択すると、図4のように「ファイルの場所の選択」画面が現われるので、適切なフォルダを選択してください。特に「更新の保管場所」で、「更新を次のローカルフォルダに保存する」を指定すると、そのフォルダ以下にダウンロードしてきた修正プログラムが格納されます。初期ダウンロードで150MB程度[注6]の容量が必要とありますが、その後ホットフィックスなどがリリースされるたびにどんどん増加していくことを考えると、数GBの容量を確保しておいた方がよいでしょう。

図5に示す「言語の設定」では、Windows Updateサイトからダウンロードする修正プログラムの言語を指定します。大半の方は「日本語のみ」でよいのではないかと思いますので、そのように変更しておきましょう。その次の「以前に許可された更新の新しいバージョンの処理」は、デフォルトのままでかま

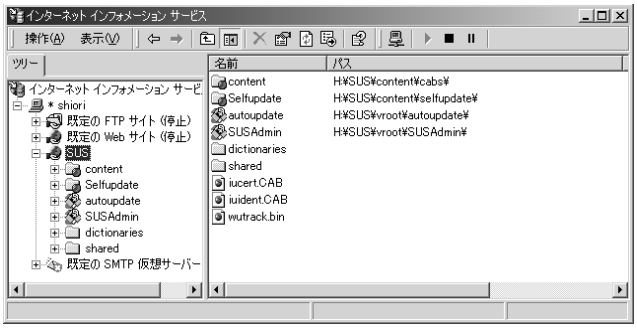
注4）http://www.microsoft.com/japan/windows2000/windowsupdate/sus/default.asp

注5）この「Webサイト」は、IIS用語のWebサイトを意味します。

注6）これは1言語の場合で、すべての言語の場合は600MB程度必要とドキュメントにあります。なお、筆者の環境では、日本語のみ（PC-98xxシリーズ用の日本語NECは含めません）の初期ダウンロード状態で120MB程度でした。

図6：IIS Lockdownの実行。強制的に実行される

図7：SUSサイト



contentという仮想ディレクトリや、SUSAdminというディレクトリなどが確認できる

いません。最終的に「インストールの準備完了」という確認画面が現れますので、「インストール」ボタンを押すとインストールがはじまります。

なおNECのPC-98xxシリーズ用の修正プログラムが必要な場合は、「特定の言語」ボタンを押して、明示的に「日本語NEC」を選択する必要がありますので注意してください。

IIS Lockdownの実行

インストールの過程で図6のようにIIS Lockdownが実行されます。これは強制的に実行され、回避することはできません。IIS Lockdownが実行されると、表2のようにASP以外の動的コンテンツが禁止され、サンプルや管理サイトなどが削除されますので、ある意味セキュアにはなります。しかしIISを他の用途にも使っている場合や試験用サーバーなどの場合は、勝手に設定を変更されてしまい迷惑でもあります。

Microsoftが推奨するように、専用サーバーにしてしまえばよいのでしょうが、小規模なサイトではそうもいかないのが現実だと思いますので、この仕様は筆者としてはちょっと乱暴過ぎるように思います。セキュリティ強化を促す意味で、IIS Lockdownが自動起動されるところまではよいと思うのですが。

IISサイトの生成

最終的にインストールが完了すると、図7のようにSUSというWebサイトが作成されます[注7]。SUS関連のファイルやフォルダについては図8のようにACLが設定され、基本的にはAdministratorsローカルグループのアカウント以外が利用できないように設定されています。逆に言えば、Administratorsグループのアカウントであれば、別マシンから管理することも可能です。

SUSクライアントのインストール

SUSを利用するには、クライアント側にもSUSに対応した「Windows自動

注7）前述したように、デフォルトの状態でインストールを行なった場合は、「既定のWebサイト」に対してファイルが追加されます。

表2：IIS Lockdownにより行なわれる設定の変更

スクリプト マッピングの削除：ASP	.ASPファイルの有効化
スクリプト マッピングの削除：IDQ	無効化
スクリプト マッピングの削除：SHTML、SHTM、STM	無効化
スクリプト マッピングの削除：IDC	無効化
スクリプト マッピングの削除：printer	無効化
スクリプト マッピングの削除：HTR	無効化
サンプルWebファイルの削除	ファイルの削除
スクリプ仮想ディレクトリの削除	ディレクトリの削除
MSDAC仮想ディレクトリの削除	ディレクトリの削除
WebDAVの無効化	WebDavの無効化
IIS匿名ユーザーによるシステムユーティリティの実行阻止	阻止
IIS匿名ユーザーアカウントによるWebコンテンツの書き込み阻止	阻止

詳細は、「Microsoft Software Update Servicesの展開」の「付録A：Software Update Services Setupを理解する」を参照

図8：SUSAdminディレクトリのセキュリティ

Administrators と SYSTEM はフルコントロールだが、それ以外の 2 つのアカウントには書き込み拒否という特殊なアクセス権のみが設定されているので、基本的にはまったくアクセス権はない。また、Everyone など、ACL のないアカウントについても、当然アクセス権はない

更新」をインストールする必要があります[注8]。ドキュメントなどには明記されていませんが、これはWindows Updateなどからインストール可能な「Windows自動更新2002年6月」と同じものですので、既にこれをインストールしている場合は、改めてインストールする必要はありません。新規にインストールする場合は、Windows Updateから行なってもかまいませんし、SUSのホームページ[注9]の下の方にあるリンクから行なってもかまいません。インストール時には特にオプションなどはありません。

このファイルはMSI形式のファイルになっていますので、Active DirectoryのGPOを利用するなどして一括して自動的にインストールすることも可能です。

注8）Windows 2000 SP3やWindows XP SP1からはSUS対応のWindows自動更新がデフォルトでインストールされる予定です。

注9）http://www.microsoft.com/japan/windows2000/windowsupdate/sus/default.asp

図9：SUSの管理画面

SUSの初期設定

インストールが完了すると、「http://localhost/SUSAdmin/」にアクセスすることで、図9のようなSUSの管理画面が表示されます。SUSの設定や管理は、すべてここから行ないます。

実環境で設定を行なう上では、あらかじめ運用のポリシーを決めておく必要がありますが、まずは機能説明を兼ねて、一通り各メニューを紹介しておきます。

最初に行なうことは、「オプションの設定」からSUSサーバーの設定を確認することです。「オプションの設定」メニューを表示すると、右側のペインに現れる設定項目を図10に示します。見てのとおり、設定項目はたったこれだけです。

以下個々の項目について説明します。

①プロキシサーバーの構成を選択します

Windows Updateサイトへの接続にプロキシサーバーを経由する必要がある場合は、ここで設定を行ないます。

②この更新サーバーを見つけるためにクライアントが使用する名前を指定してください

文字どおり、クライアントマシンがSUSサーバーにアクセスする際に使う名前を指定します。

③コンテンツを同期するサーバーを選択します

修正プログラムのダウンロード元を指定します。

SUSサーバーを選択した場合に、「許可された項目の一覧を同期する（置換モード）」のチェックボックスをチェックすると、クライアントにどの修正プログラムを配布するかという「許可された項目」情報も、ダウンロード元のSUSサーバーから取得するようになります。この場合、このサーバー上では情報を

図10：「オプションの設定」メニュー

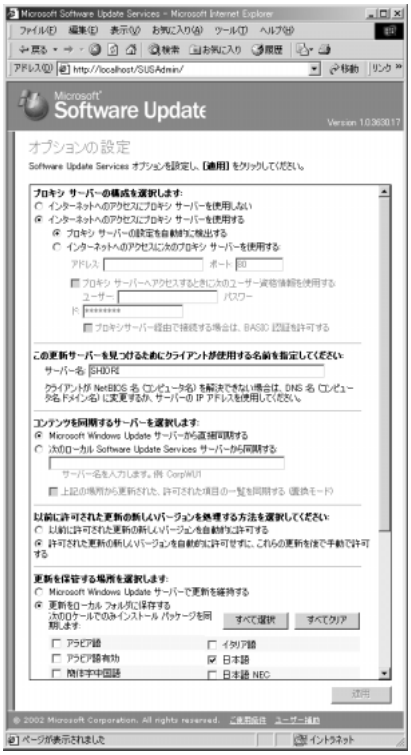


図11：「サーバーの同期」メニュー

変更できません。

④以前に許可された更新の新しいバージョンを処理する方法を選択してください

一度「許可された項目」に追加した修正プログラムが更新された時に、自動的に「許可された項目」に追加するかどうかを決定します。デフォルトでは追加しません。

⑤更新を保管する場所を選択します

修正プログラムをローカルに保管するかどうか、また保管する場合にどの言語のものを保管するかを設定します。

ここで「Microsoft Windows Updates サーバーで更新を維持する」を選択した場合は、クライアントマシンはSUSサーバーからではなく、Windows Updateサイトから修正プログラムをダウンロードしますが、クライアントマシンは「許可された項目」の情報をSUSサーバーから取得します。

この設定は、クライアントマシンに適用する修正プログラムは管理したいが、修正プログラム自体はSUSサーバーから配布したくないという状況で使いますが、通常この設定にする必要はないと思いますので、本記事でもこれ以上は触れません。保管する言語については、インストール時に行なった設定が反映されているはずです。

このうち、設定を変更する必要があるのは、①と②だけでしょう。④と⑤の設定は、インストール後で変更することはあまりないと思います。③については後で説明しますが、1台目のSUSサーバーの場合は設定を変更する必要はありません。

設定が一通りすんだら、図11の「サーバーの同期」メニューから「今すぐ同期」を選択してください。しばらく時間がかかりますが、Windows Updateサイトから修正プログラムが一式ダウンロードされます。定常運用にはいったら「同期スケジュール」から設定を行なって、夜間などにダウンロードを行なうようにするとよいでしょう。

ダウンロードが完了したら、図12のような「更新の許可」メニューを開いてください。このようにSUSサーバーにダウンロードされたクライアントに配布可能な修正プログラムが一覧になっ

図12：「更新の許可」メニュー（初期状態）

図13：「更新の許可」メニュー（許可の設定後）

て表示されていますので、実際に配布を行ないたいものにチェックボックスをつけ、「許可」ボタンを押してください。配布可能となったものは、通常は図13のように、各修正プログラムの右に「(許可済み)」と表示されています。なお、一括で許可という機能はありませんが、右側のペインのスクロールバーで囲まれた「利用可能な更新」にフォーカスを合わせれば、後はTABキーで移動しながらスペースを押してチェックボックスをチェックしていくことで、比較的素早く多数の修正プログラムを「許可」することが可能です。

これで、SUSサーバーについては、初期設定が完了です。

なお、ここで説明した以外のメニューのうち「関連項目」にある各種メニューは、見てのとおりドキュメントや外部のWebサイトへのリンクです。「ログの表示」と「サーバーの管理」については、SUSサーバーの管理に利用するものですので、後で説明します。

SUSクライアントの設定

SUSでは、冒頭で説明したように各クライアントマシンがSUSサーバー（またはWindows Updateサイト）から修正プログラムを取得するというプル型のモデルですので、クライアント側でもSUSサーバーを利用するため、先ほどインストールした「Windows自動更新」の設定が必要になります。

設定は基本的にレジストリを修正することで行ないます。もちろんローカルポリシー（コラム1）、GPOやシステムポリシーを使ったり、スタートアップスクリプトでREGファイルを自動的に読み込ませるなどの方法で自動的に設定することが可能です。ローカルポリシーやGPOを利用する場合のポリシーテンプレートとしてwuau.admというファイルがあらかじめ用意されています。なお各方式の具体的な方法はSUSとははずれますのでここでは説明しません。以下にレジストリとその意味について説明します。

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU

- REG_DWORD: NoAutoUpdate
  0＝自動更新を行ないます
  1＝自動更新を行ないません
- REG_DWORD: UseWUServer
  0＝WUServerで指定されたSUSサーバーを使いません
  1＝WUServerで指定されたSUSサーバーを使います
- REG_DWORD: AUOption
  2＝更新をダウンロードする前、およびインストールする前に通知する
  3＝更新を自動的にダウンロードし、インストールの準備ができたら通知します
  4＝更新を自動的にダウンロードし、ScheduledInstallDayとScheduledInstallTimeで指定されたスケジュールでインストールします
- REG_DWORD: ScheduledInstallDay
  0＝毎日
  1～7＝日曜日（1）から土曜日（7）の曜日

コラム1　ローカルポリシーによる「Windows自動更新」の設定

とりあえず手軽に設定する方法として、ローカルポリシーによる設定方法について説明しておきましょう。

まずは、「スタート」メニューの「ファイル名を指定して実行」からgpedit.mscを実行して、ローカルコンピュータポリシーのMMCスナップインを起動します。ついで図14のように管理用テンプレートのコンテキストメニューから「テンプレートの追加と削除」を選択して、本文でも説明したwuau.admを追加します。

これで、「管理用テンプレート」-「Windows コンポーネント」の下に「Windows Update」というフォルダが現れ、なかにポリシーが2つ現れますので、適宜設定してください。設定項目自体は、本文で説明したレジストリと同じです。

図14：「テンプレートの追加と削除」メニューの選択

AUOption＝4の時に、自動インストールが行なわれる曜日を指定します。

・REG_DWORD: ScheduledInstallTime

0～23＝24時間形式の時刻。AUOption＝4の時に、自動インストールが行なわれる時刻を指定します。

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

・REG_SZ: WUServer

SUSサーバーのURLを指定します。たとえばSUSサーバーがSHIORIという名前で参照可能な場合、「http://shiori」のように指定します。なお、値が設定されていない場合は、Windows Updateサイトから修正プログラムのダウンロードが行なわれます。

・REG_SZ: WUStatusServer

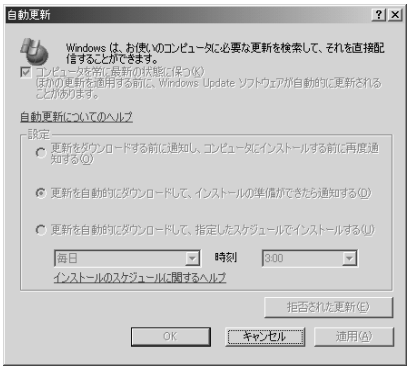
後述するステータスサーバーのURLを指定します。よくわからない場合はSUSサーバーと同じ値を設定してください。

通常は、自動更新を有効にするには、NoAutpUpdate=0、UseWUServer=1に設定して、WUServerとWUStatusServerにSUSサーバーのURLを指定したうえで、ポリシーに応じてAUOptionを3か4に設定することになるでしょう。いずれにしても、上記レジストリを設定すると、各マシンのGUIによる設定画面は図15のようにグレーアウトして設定できなくなります。

自動更新が有効になっている各マシンは、1日に1回定期的にSUSサーバーに接続して、SUSサーバーが「許可された更新」に含めた修正プログラムをダウンロードし（AUOption＝2の時は、ダウンロードをしてよいか通知します）、ダウンロード完了後に、ユーザーに通知、もしくは指定された時刻に自動的にインストールを行ないます。なお、SUSサーバーに接続する時間は制御することができませんので、厳密なトラフィック管理ができません。このあたりも、SMSを意識して故意に機能を落しているような感じがします。

インストール後再起動が必要な修正プログラムを自動でインストールすると、インストール完了後に自動で再起動が行なわれますので、自動でインストールする（AUOption＝4）場合は、自動的な再起動で編集中のファイルが破棄されるなどの問題が発生しないように運用に注意する必要があります。また、SMSとは違い、SUSでは一度クライアントがインストールした修正プログラムをアンインストールする機能は提供されていません。どうしてもアンインストールが必要になった場合は、SUS以外の方法で行なう必要があります。

図15：グレーアウトした「自動更新」の設定画面



SUSの管理

一度インストールして運用を開始してしまえば、これ以降行なうことは、新規修正プログラムがダウンロードされるたびにそれを「許可された更新」に含めるかどうかを判断して設定すること以外、基本的にログの監視になります。

SUSサーバーのログ監視は、基本的に前述した図9のSUSの管理画面にある図16のような「同期ログの表示」と

図16：「同期ログの表示」メニュー

Windows Updateサイトや別のSUSサーバとの同期に関するログになる

図17：「許可ログの表示」メニュー

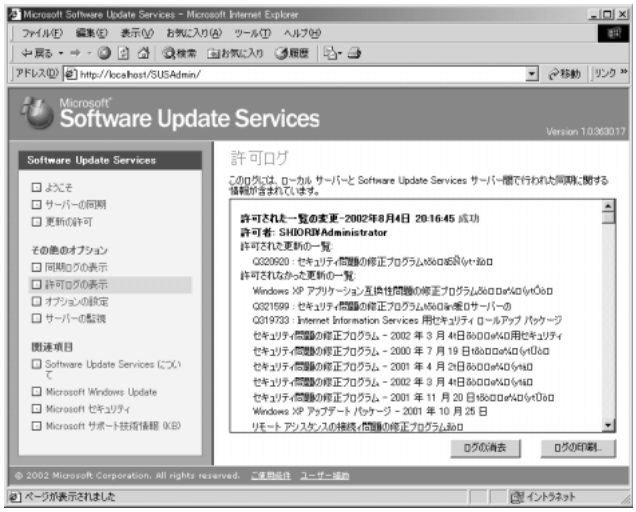
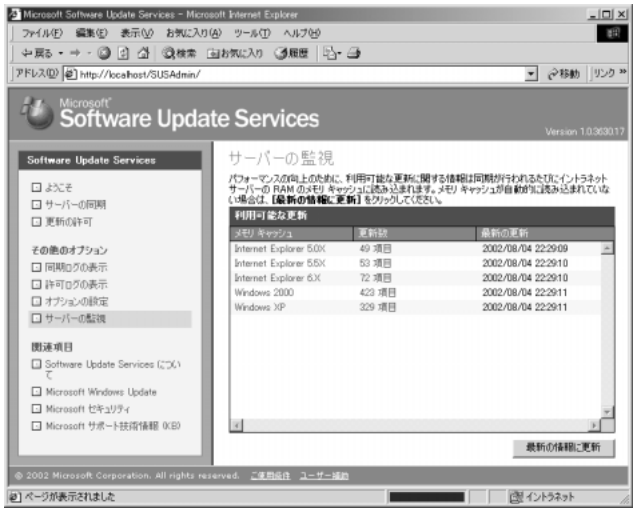


図18：「サーバーの監視」



「許可された更新」の操作に関するログになる

図17のような「許可ログの表示」画面から行ないます。なおこれらのファイルはSUSのWebサイト以下の\AUtoupdate\Administrationフォルダ以下に、おのおのhistory-sync.xmlとhistory-approve.xmlという名前のXML形式のファイルとして保管されていますので、スクリプトなどでログの解析を行なうことも可能です。

また、図18の「サーバーの監視」では、メモリ中に格納されている最新の修正プログラムに関する情報を参照することが可能です。

実際にトラブルが発生した場合の対応方法や、発生しそうなトラブルの一覧については、「Microsoft Software Update Servicesの展開」の「トラブルシューティング」（P64）などに詳細な情報がありますので、そちらを参照してください。

ステータスサーバーによるクライアントの状態の管理

SUSを管理していくうえで、各クライアントへの修正プログラムの配布状況などは把握しておきたいことでしょう。SUSではちょっとトリッキーな方法でIISのログファイルを活用することで、こうした情報を収集しています。

SUSのクライアントは、何らかのアクションを行なうと、ステータスを示すさまざまな引数を指定してステータスサーバーとして指定されたサーバー上の/wutrack.binというダミーのファイルをGETします。これにより、IISのログに/wutrack.binファイルへのアクセスというかたちで記録が行なわれ、ログファイルを解析することでSUSクライアントの状態を把握できるようになっています[注10]。ここまでやるなら、ログファイルを解析する画面（またはツール）もつけてくれてもよさそうなところですが、SMSとの競合を避けるためか、そうしたツールはついていません。

SUSクライアントが記録するログの例をリスト1に示します。

/wutrack.binをGETする際に、さまざまな変数が指定されていますが、これがSUSクライアントのステータスを意味するものになります。変数部分を模式化すると

注10：SUSクライアントの設定にあるステータスサーバーとは、この目的で接続するサーバーを指定する設定項目です。

リスト1：SUSクライアントが記録したログの例

```
2002-08-03 10:55:44 192.168.10.107 - 192.168.10.107 80 GET /wutrack.bin
U=71f2dcb0975a1c4087f346cf28faaf69&C=iu&A=n&I=&D=&P=5.0.893.2.110.3.0&L=
ja-JP&S=s&E=00000000&M=&X=020803105544673 200 Industry+Update+Control
```

*）上記は、デフォルトのW3C拡張ログファイル形式になっています。
*）実際は改行なし

```
/wutrack.bin?U=<ping_ID>&C=<client>
&A=<activity>&I=<item>&D=<device>&P
=<platform>&L=<language>&S=<status>
&E=<error>&M=<message>&X=<proxy>
```

＊）実際は改行なし

のようになります。それぞれの意味は表3のとおりです。

実際に運用を行なう際には何らかの解析ツールを作成して統計情報を収集した方がよいでしょう。

SUSクライアントの動作ログファイル

そもそもSUSクライアントからサーバーへの接続自体が行なわれていないといったトラブル時に参照できるログとして、SUSクライアント（Windows自動更新）の自体のログが%WinDir%\Windows Update.logというファイルに自動的に出力されています。SUSクライアント自体の動作に問題が発生した時は、このログを参照するようにしましょう。ログの一部をリスト2に示します。

ここでは、3行目で、iuident.capファイルのダウンロードに失敗したことや、8行目で更新すべき修正プログラムの有無をSUSサーバーに問い合わせたことなどが確認できます。

SUSの展開と運用

ここまで、SUSサーバーおよびクライアントの設定方法について説明してきました。以下では、実際に導入を検討する上での考慮点などについて説明していきましょう。

表3：SUSクライアントのログの意味

activity	動作に関する情報を示します n：初期化 s：セルフアップデート d：検出 w：ダウンロード。成功および失敗、また該当する場合は取り消しと拒否が記録されます i：インストール。再起動のない失敗と成功、再起動を伴う成功、該当する場合は拒否が記録されます
item	activityで指定された処理が行なわれるコンポーネント（もしあれば）を示します
device	処理対象のデバイスID（もしあれば）を示します
platform	クライアントマシンのシステムに関する情報を示します このフィールドには、“.”区切りでOS関連の情報が記録されています <maj_os_ver>.<min_os_ver>.<build_num>.<plat_id>.<suite_mask>.<prod_type>.<processor_arch>
plat_id	システムの系列を示します 1：Windows 9x系OS（Windows 95/98/Me） 2：Windows NT系OS（Windows NT/2000/XP）
suite_mask	インストールされている製品に関する情報を示します このフィールドはビットマスクになっていますが、以下よく使われるであろうビットのみ記載します[注11] たとえば、リスト1の110という値は、0x10+0x100で、ターミナルサーバーがインストールされていることを示します
prod_type	システムに関する情報を示します
processor_arch	プロセッサアーキテクチャを示しますが、32ビットマシンの場合、この値は0です
language	ja-JP（日本語/日本）といったISO形式でクライアントOSの言語／地域を示します
status	処理のステータスを示します。以下値を示します S（成功）：処理は、完全かつ無事に実行されました R（成功－再起動が必要）：ここまでの処理の実行は成功しました。再起動して続行する必要があります F（失敗）：ユーザーによる取り消し以外の理由で、処理の実行が失敗しました C（取り消し）：ユーザーによって、実行中に処理が取り消されました D（拒否）：ユーザーによって、処理が拒否されました N（項目なし）：処理を実行できる更新項目がありません P（保留）：（おそらく）想定されていない状態です[注12]
error	処理の結果を8桁の16信数で示します[注13]。使用されない場合、値は0になります
message	発生したエラーの説明が含まれます
proxy	状態メッセージのタイムスタンプを格納します。タイムスタンプの形式は、YYMMDDHHMMSSmmmです

注11、13）詳細は、「Microsoft Software Update Servicesの展開」を参照してください。

注12）マニュアルをみると、「返される情報はすべて、開発者および顧客の問題を解決するサポートによって使用されます」と記述されています。

そもそもSUSを導入する必要があるか？

当たり前ですが、メリットもないのにやみくもに導入しても仕方ありません。

冒頭で説明したように、SUSの恩恵を受けられるのはWindows 2000/XPのみですので、これ以外のクライアントしかないのであれば、導入するメリットは

リスト2：Windows Update.logの内容（一部）

```
 1:   2002-08-04 18:01:25  09:01:25   Success   IUCTL          Starting
 2:   2002-08-04 18:01:27  09:01:27   Error     IUCTL          Library download error. Will retry. (Error
0x801901F7)
 3:   2002-08-04 18:01:27  09:01:27   Error     IUCTL          Failed to download iuident.cab from http://shiori
to H:\Program Files\WindowsUpdate\V4 (Error 0x801901F7)
 4:   2002-08-04 18:01:27  09:01:27   Success   IUCTL          Ignore above error, use local copy of iuident.cab
from H:\Program Files\WindowsUpdate\V4
 5:   2002-08-04 18:01:27  09:01:27   Success   IUCTL          Checking to see if new version of Windows Update
software available
 6:   2002-08-04 18:01:27  09:01:27   Success   IUENGINE       Starting
 7:   2002-08-04 18:01:28  09:01:28   Success   IUENGINE       Determining machine configuration
 8:   2002-08-04 18:01:30  09:01:30   Success   IUENGINE       Querying software update catalog from
http://shiori/autoupdate/getmanifest.asp
 9:   2002-08-04 18:01:32  09:01:32   Success   IUENGINE       Shutting down
10:   2002-08-04 18:01:32  09:01:32   Success   IUCTL          Shutting down
```

ありません。またSUSが配布できるのは、セキュリティ修正モジュールなどを中心とした修正プログラムに限られますので、すでにこうした修正プログラムを配布する体制が整っているのであれば、やはりSUS導入のメリットはないでしょう。逆に考えると

- Windows 2000/XPクライアントが存在している
- セキュリティ修正モジュールなどを随時インストールする必要がある
- 現在クライアントに一括して修正プログラムを配布する体制がない。もしくは各マシンが個々にWindows Updateサイトを使っているので、インターネット接続回線の帯域を圧迫している

ような状態であれば、管理コストが非常に低いSUSは導入の価値があると言えるでしょう。

各クライアントへの「Windowsの自動更新」の配布

導入を決定したら、対象となる各クライアントに対して更新された「Windowsの自動更新」を配布する必要があります。

自動的に行なうには、さまざまな方法が考えられます。Active Directoryを導入していれば簡単ですが、導入していない場合でも、クライアントマシンの管理者権限があれば、タスクを配布してそのなかでインストールを実行するなどいくつか方法が考えられます。

SUSサーバーの配置と構成

最後にSUSサーバー自身をどこにどのように配置するかを考える必要があります。考慮するうえでのポイントとしては、以下の4つがあげられます。

SUSサーバーの台数と場所

Microsoftのドキュメントによると、最小ハードウェア[注14]の構成でも15000台のクライアントをサポートできるとありますので、SUSサーバーのパフォーマンス面が問題となることはないでしょう。後はWAN越しの各サイトにSUSサーバーを配置するかどうかを、ネットワークトラフィックとサーバー導入コスト的な観点から決定することになります。

「許可された更新」の設定を行なう場所

組織のポリシーにもよりますが、大半の組織では、中央のSUSサーバーで行なった設定を各SUSサーバー（もしあれば）に配布するのが管理の一元化の観点でよいでしょう。

SUSサーバー間の修正プログラムの複製方法

これは、組織のネットワーク構成やポリシーに依存します。主にトラフィックの観点からいうと、各拠点間がインターネット経由で結ばれているのであれば、各拠点のSUSサーバーが独自にWindows Updateサイトから取得する設定にした方がよいでしょうが、インタ

注14）前掲しましたが、CPUがP3-700/メモリ512MB/ディスクの空き6GBです。

ーネット接続が1箇所の場合や、「許可された更新」の設定を一元管理したい場合は、マスタのSUSサーバーがWindows Updateサイトから取得した修正プログラムをさらに組織内の別のSUSサーバーが取得する設定にした方がよいでしょう。

なお、通常SUSサーバー間の複製は、直接HTTPで通信することによって行ないますが、物理的な接続が許可されないようなクローズドなネットワークの場合でも、オフラインでのファイル（および設定）の複製により、SUSサーバーの構築が可能です。

各クライアントの「Windowsの自動更新」の設定

考慮のポイントは、AUOptionを3（インストール前に通知）にするか、4（自動インストール）にするかだと思います。各ユーザーに管理者権限を与えず、全クライアントを一元管理しているような組織であれば、4の選択もあると思いますが[注15]、各クライアントの管理はクライアントマシンの利用者に任せているような環境では、勝手に再起動しては困る場合もあると思いますので、3が無難ではないかと思います。

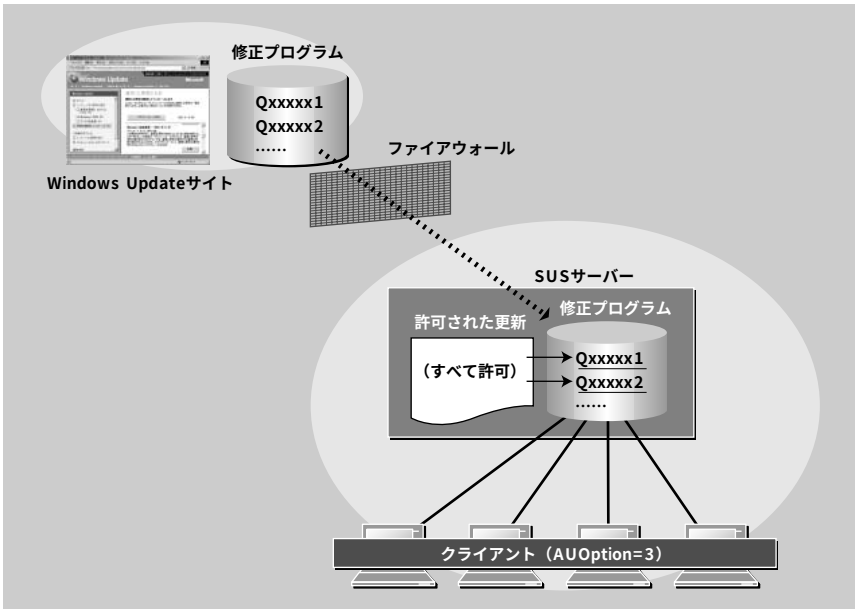
これらを考慮した、典型的と思われる導入形態をいくつか示します。

SOHOや小規模な組織

事務所が1箇所の場合は、図19のように単純にSUSサーバーも1台、冗長化とバックアップを考慮しても2台配置しておけばよいでしょう。

SUSサーバーはWindows Updateサイトから修正プログラムをダウンロードし、サーバー内に蓄積します。これにより、クライアントのWindows Updateのトラフィックがインターネットに流れることを防ぎます。クライアント側を厳密に管理していないのであれば、「許可された更新」では、すべての修正プログラムを許可して、どれをインストールするかはクライアント側にまかせてしまえばよいでしょう。クライアント側では、「AUOption＝3」に設定して、各クライアントマシンの管理者が必要な時に必要な修正プログラムをインストールできるようにしておきます。

図19：SOHOや小規模な組織の導入例



WANで複数サイトに分割されている組織

事務所が複数あって、間がWANで接続されている場合は、WANの帯域と各拠点のクライアントマシンの台数にもよりますが、ある程度以上の規模であれば図20のような多段構成を検討するとよいと思います。

この場合、クライアントに配布する修正プログラムは、本社側のサーバーで一元管理できるように、支社側のサーバーでは、コンテンツを同期するサーバーとして、本社のSUSサーバーを指定するとともに、「許可された項目の一覧を同期する（置換モード）」のチェックボックスをチェックしておきましょう。

完全にクローズドなネットワークな組織

この場合は、Windows Updateサイトから修正プログラムをダウンロードして蓄積するインターネットに接続した環境にあるSUSサーバーと、手動による複製を行ない、クローズドなネットワ

注15）ただ、こうした厳格な管理を行なっている組織では、すでに何らかのファイル配布のしくみを構築している場合が多いようですので、そもそもSUSを導入する必要がないように思います。

図２０：複数サイトがある組織の導入例

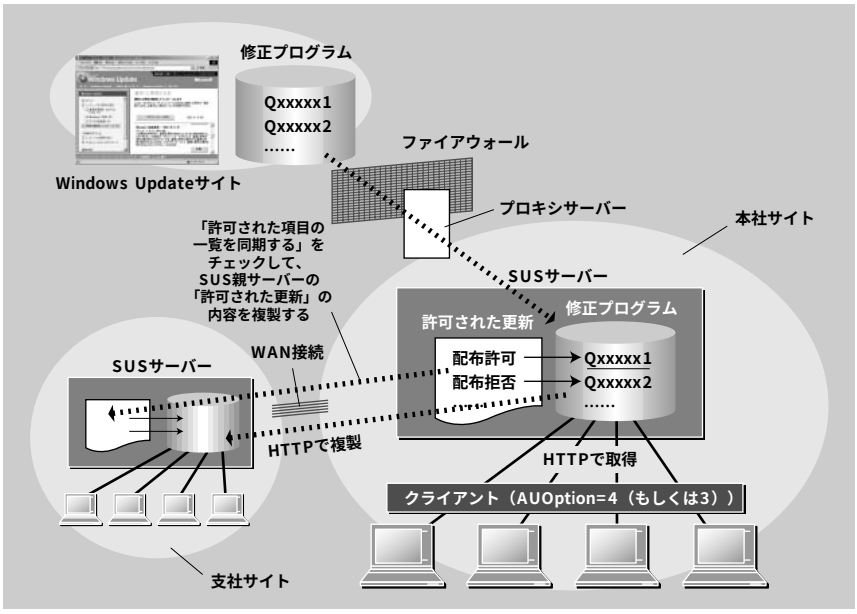
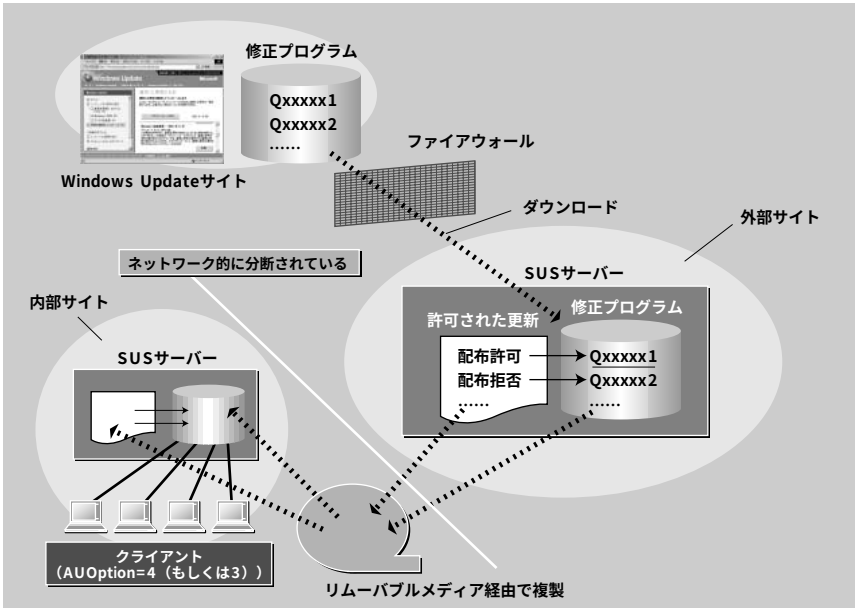


図２１：完全にクローズドなネットワーク環境への導入例



ーク内でSUSサーバーとして機能させる内部SUSサーバーの最低2台のSUSサーバーが必要となります。

具体的な複製の方法は、コラム2を参照してください。クローズドなネットワーク内の各クライアントは、内部SUSサーバーから、自動的に修正プログラムをダウンロードして、インストールすることが可能となります（図21）。

とりあえずの評価

ここまで、SUSについて一通り説明しました。筆者自身、まだ使い込むというところまではいっていないので、今後予想外の問題点が出てくるかもしれませんが、とりあえずの評価としては「可もあり不可もあり」といったところでしょうか。

操作性に関しては、非常にシンプルで評価できます。いままでWindows Updateに頼ってきた組織にとっては、ネットワークトラフィックの低減という点だけでも導入する価値があるのではないでしょうか？

一方各クライアントを厳格に管理して運営しているような組織にとっては、スケジューリング機能の低さがネックになって、いまひとつ導入しづらいと思います。特にSUSクライアントがいつSUSサーバーに接続できるかを制御できない点は、問題となるケースも多いと思います。

こうした点から考えると、SUSは主にあまり厳格な管理の必要でない、OA系ネットワークにWindows Updateの代替として導入するのが一番似合っているように思います。ネットワークトラフィックが制御できない点を除けば、ある程度厳格な管理もできますが、ほかのプロダクトとの連携機能がないなど、厳格な管理を行なうにははがゆい点が多いので、導入は注意深く行なうことが必要でしょう。

もっとも、ある程度機能や目的を限定しているからこそ、最近の多機能指向のMicrosoft社製品のなかにあって非

コラム 2

オフラインでの複製

高度なセキュリティを保つために、完全に切り離されているネットワーク間でも、以下のようにすることでSUSサーバーの情報を複製することができます。

複製先のサーバーは、IIS 5.0が稼働していることが必要です。複製は、ファイルを手動で複製することで行ないます。

①配布元サーバーの/(トップディレクトリ)直下にある以下の3つのファイルを複製先WebサーバーのSUS用Webサイトのトップディレクトリに複製します。

- Aucatalog.cab
- Aurtf.cab
- approveditems.txt

②配布元サーバーの/Content/cabs以下にあるすべてのファイルおよびフォルダを任意のフォルダ（たとえばc:\SUS\content\cabs）に複製します。

③②で複製したフォルダに対して、/contentでアクセスが可能なように、仮想フォルダを設定します。

複製自体に必要な設定はこれだけです。

要は、上記ファイルについて、複製元のSUSサーバーと同じURLで同じ設定でアクセスできるようにすればOKということです。この機能により、リムーバブルメディアなどを使った複製によるSUSサーバー間の複製が実現しますので、物理的に切り離されているネットワーク間でも複製を行なうことが可能になります。

常にシンプルな操作性が実現されているわけです。SUSだけですべてが解決できるわけではないですが、SUSをうまく既存のシステムに取り込めば、役立ってくれるのも確かでしょう。こうしたツールをどう使うか、生かすも殺すも後はわれわれ管理者の腕にかかっているといったところでしょうか。

最後になりましたが、SUSの導入にあたっては、事前にSUSのホームページ[注16]から参照、ダウンロードできる各種ドキュメント、なかでも特に本文中でも何度か紹介した「Microsoft Software Update Servicesの展開[注17]」に目を通しておくことを強く推奨します。90ページ以上あるのでちょっと読みこなすのは骨ですが、これを読み通せばSUSの設定、運用を行なううえで十分な知識が身につくと思います。

注16）http://www.microsoft.com/japan/windows2000/windowsupdate/sus/default.asp

注17）http://www.microsoft.com/japan/windows2000/windowsupdate/sus/susdeployment.asp

Microsoft Software Update Services構築の実際