Windowsクライアント管理の重要性と工数削減のテクニック

株式会社デジタルアドバンテージ
代表取締役 小川誉久

Windowsクライアントは何を使うか？

- 16bit Windows＝**個人向け**OS
  ユーザー認証がない
  ファイルシステムはアクセス制限機能を持たないFAT**のみ**

  – Windows 95　ーWindows 98
  – Windows 98 SE　ーWindows Me

- **フル**32bit Windows＝**企業クライアント向け**OS
  ユーザー認証が可能
  アクセス制限機能を持つNTFS**を利用可能**

  – Windows NT　ーWindows 2000
  – Windows XP Professional

Windows 9x／Me
クライアントの問題点（1）

- よくも悪くもパソコン。ユーザーが自由に何でもできる
  - ESCキーでログオンを無視できる（匿名ユーザーで自由にコンピュータにアクセス可能）
  - ユーザーが自由に共有設定を行える
  - パスワード・ベースのアクセス制限をユーザーが自由に設定可能
  - システム・ポリシーを組み込めば、ある程度の制御（ログオンの強制、パスワード・キャッシュの無効化など）は可能だが、完全とはいえない

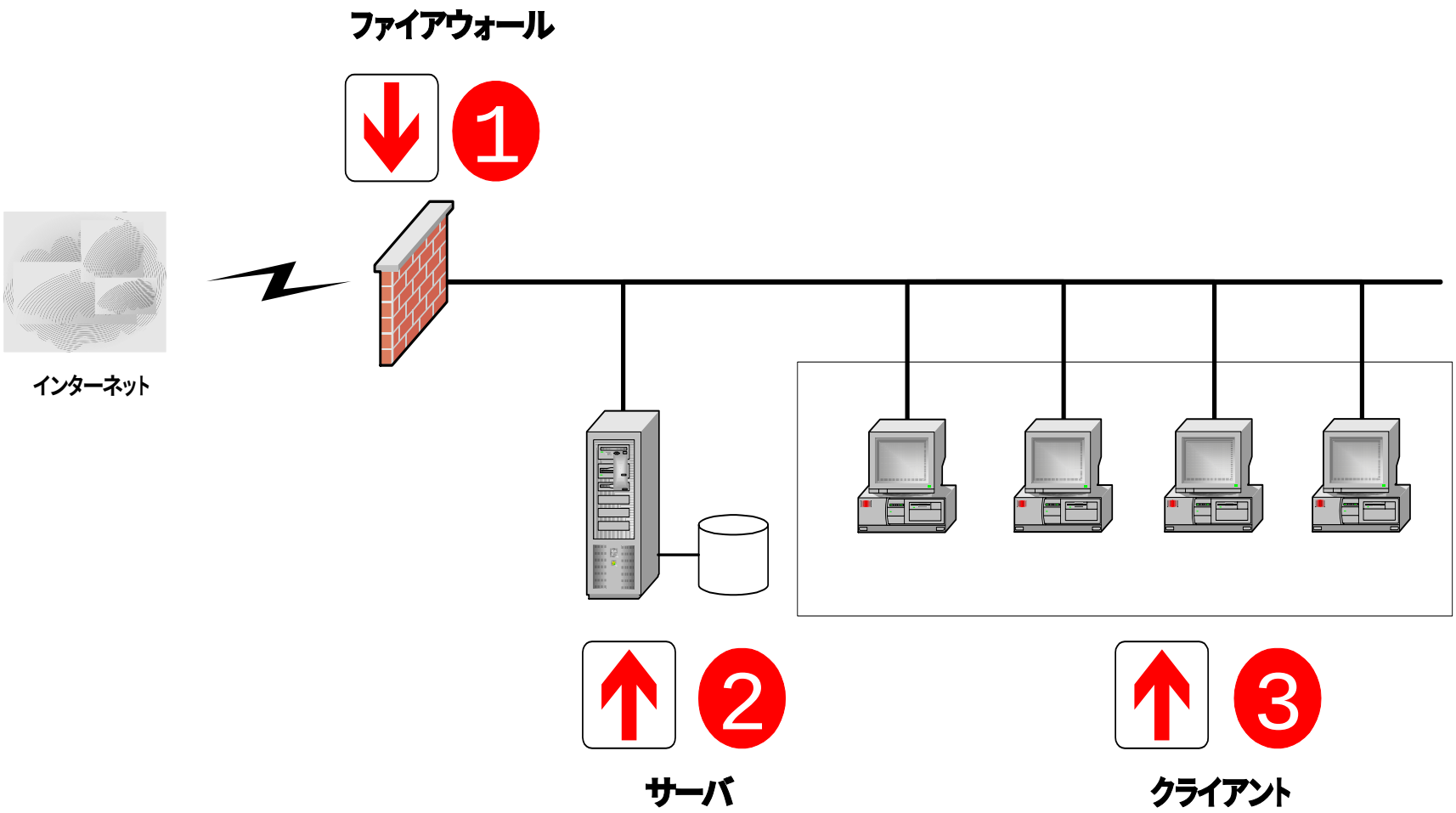
Windows 9x／Me
クライアントの問題点（2）

- ドメインでの一括管理不能
  - GPでの集中管理不可
  - ユーザーが自由にアプリケーションをインストール可能
  - 自由に設定変更できる
  - ファイルの消去なども自由。アクセス管理もできないのでデータ・セキュリティ機能はない（ACLがない）
  - リモート管理が困難

Windows 9x／Meは排除するしかない

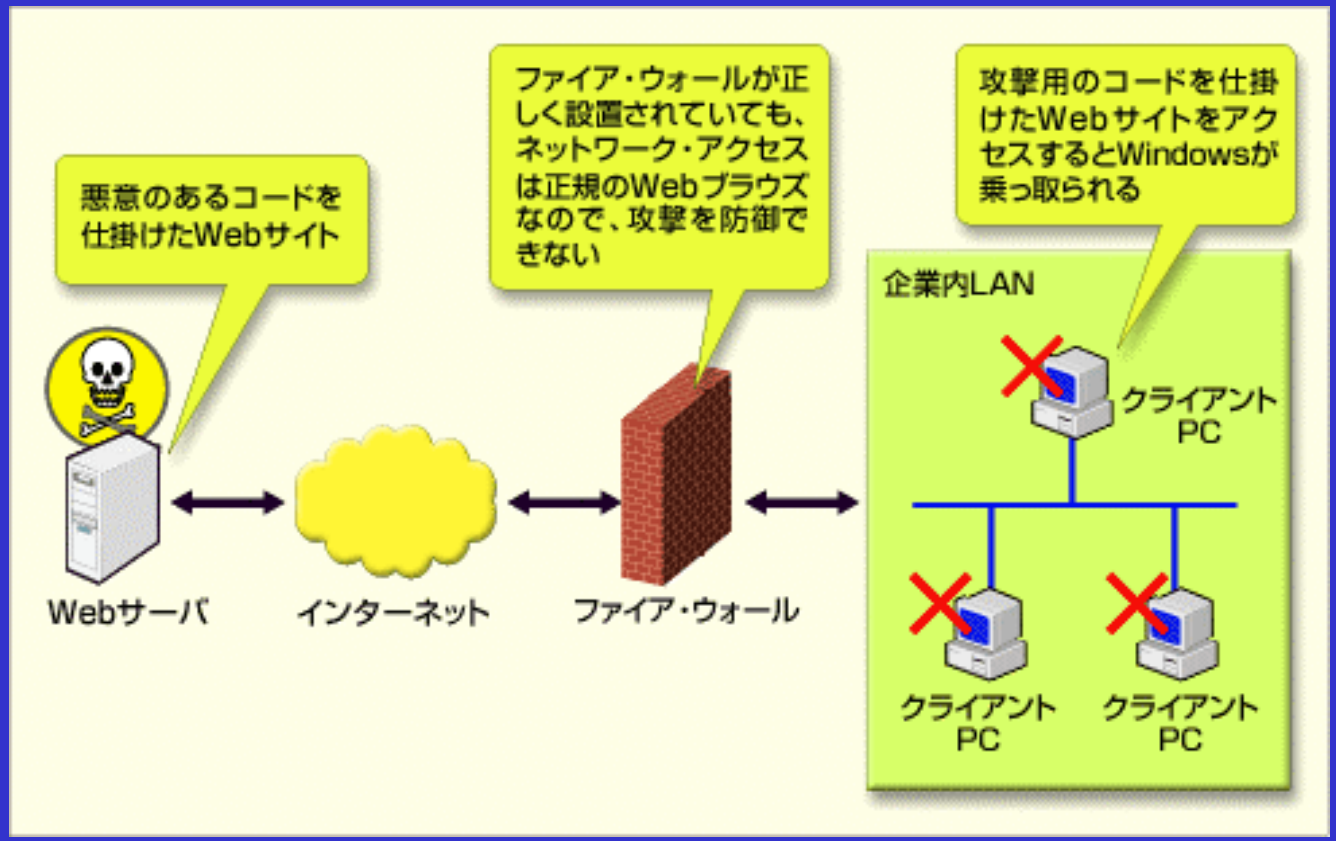
- Windows 9x／Meを排除しなければ、集中管理はできない。セキュリティをうんぬんする以前の問題
- 少なからぬ出費、既存アプリケーションの移行などの問題はあるが、管理コストや、管理不十分な状態がもたらすリスクを評価する必要がある。
- 急な完全移行が困難なら、部署やグループなどの単位で移行し、移行したものからActive Directoryなどを利用した集中管理体制に移行する

Windowsセキュリティのポイント



クライアントのセキュリティ・ホールを放置すると

- ファイアウォールやサーバ側の管理では防止できない攻撃を受ける可能性がある
  [例] MS03-008 Windows スクリプト エンジンの問題により、コードが実行される



セキュリティ管理はトータルで

- ファイアウォール
  - 外部からの侵入阻止
- サーバ管理
  - 外部からのアクセスがあるものは、攻撃の矢面に立つ
  - 共有資源をつかさどるサーバで万一の事故があると影響が大きい
  - 高可用性が求められるため、リセットなどを伴うメンテナンスは容易でない
- クライアント管理
  - OS、ソフトウェア構成などがまちまち
  - 数が多い
  - 1台1台の管理リスクは大きくないが、HotFixの配布を組織的に実施した場合、問題が起こると被害が広範囲に及ぶ

混迷極める修正プログラム事情
—— 複雑な提供方法 ——

- ServicePack：複数のHotFixをまとめたものが定期的に提供される
- Security Rollup Package：いくつかのセキュリティFixをひとまとめにしたもの
- HotFix
  - 重要な更新：主にセキュリティFix
  - 推奨される更新：その他（.NET Framework、DirectX9など）
  - ドライバの更新：新しいデバイス・ドライバ
  - QFE（Quick Fix Engineering）：スポット対応
- Microsoftダウンロード・センター：基本的にすべての修正プログラムを提供。拡張機能モジュールなども提供（日本向けで約1700種類）

混迷極める修正プログラム事情
—— 適用による副作用 ——

- HotFixの適用では、システム・ファイルが置き換わる
- 場合によっては、副作用によって障害が発生する可能性がある
- 新しいHotFixを右から左に適用すればよいというわけではない
- 修正プログラムの内容を吟味し、適用計画を立てる (適用の有無、テスティングなど)

[例]

MS03-004 Internet Explorer 用の累積的な修正プログラム (2003 年 2 月)

→適用でOutlook Expressがページ違反を発生するようになる

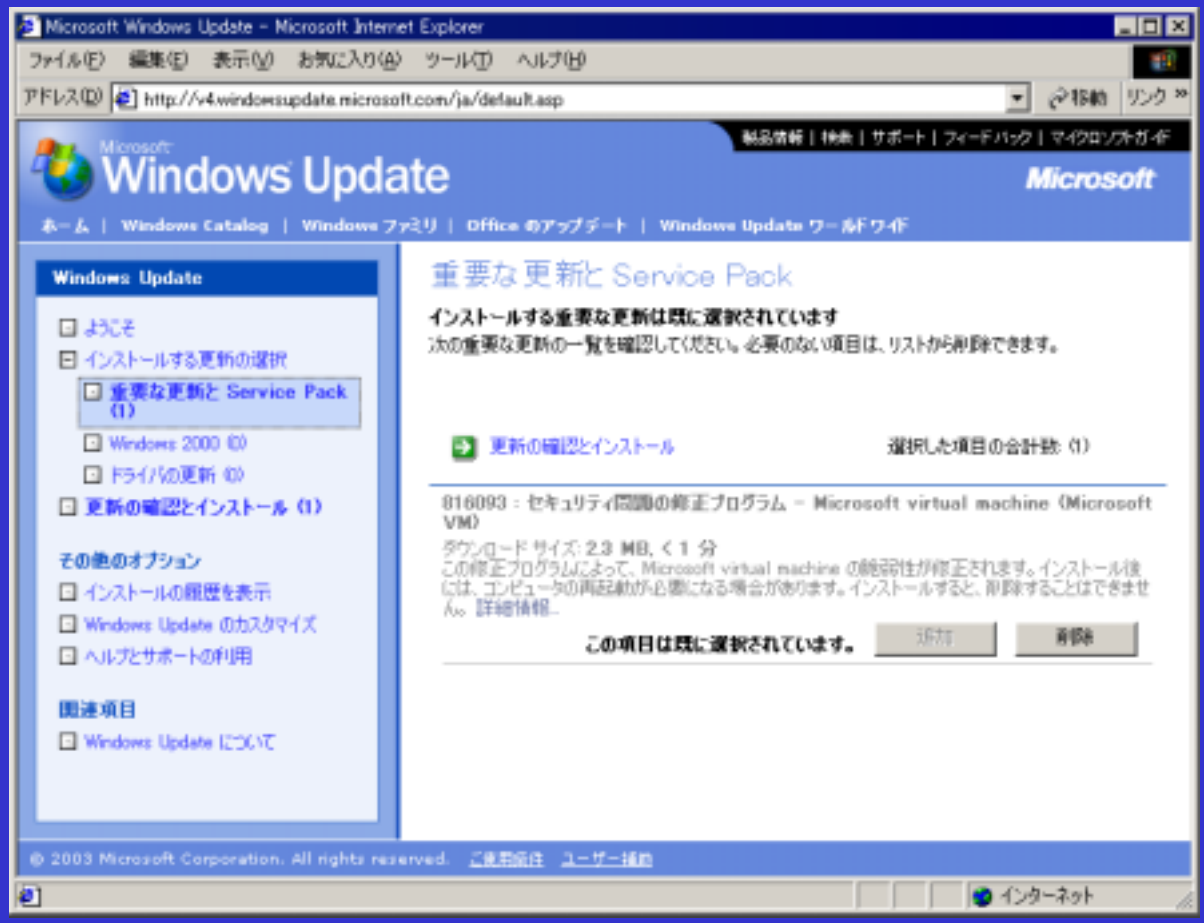
混迷極める修正プログラム事情
—— 要調査ポイント ——

- ファイルに依存関係はないか？　前提となるSPやHotFixはないか？
- どのファイルが置き換わるのか？
- 再起動が必要か？
- 指定すべきインストール･オプションは？
  - 無人インストール用のオプション設定など

マイクロソフトの無償提供ツール

- Windows Update (Web版)
- Windows Update (自動更新)
- SUS (Microsoft Software Update Services)
- MBSA (Microsoft Baseline Security Analyzer)
- **コマンドライン・ツール**
  - HFNetChk
  - QChain

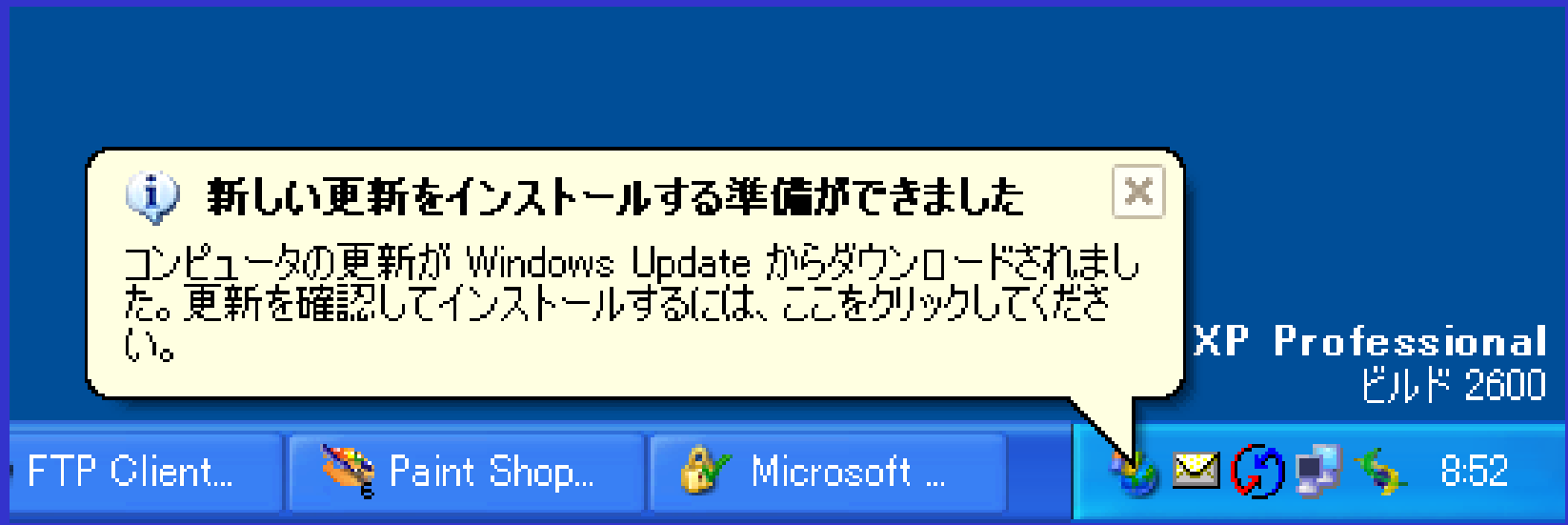
Windows Update (Web版)



Windows Update (Web版)

- ActiveXコントロールを使ってローカル・コンピュータの状態を調べ、未適用の修正プログラムだけを表示して適用を可能にする
- ServicePackも適用可能
- セキュリティFix以外の更新も適用可能
- ただし、利用するユーザーにはローカル・コンピュータの管理者権限が必要
- サポートされるのはOS、IE、IISなど。サーバ製品の修正プログラムは提供されない

Windows Update (**自動更新**)



Windows Update (自動更新)

- Windows 2000 SP3、Windows XPから対応
- 新しいHotFixが公開されると自動的にダウンロードし、ユーザーに通知する (デフォルト時)
- ユーザーが適用を指示すると、インストールが開始される
- 利用するユーザーにはローカル・コンピュータの管理者権限が必要
- 適用できるのはセキュリティFixを含む「重要な更新」のみ。ServicePackや、推奨される更新などは適用できない

SUS
(Microsoft Software Update Services)

- Windows Update (自動更新) を企業内で利用可能にする
- HotFixの配布サーバを社内に設置 (大規模システムでは、配布サーバの階層管理が可能)
- クライアント側にはSUS用の自動更新クライアントをインストール (Win2K SP3、XP SP1に同梱されるWindows Update用の自動更新クライアントと同じもの)
- グループ・ポリシーを使い、クライアント側からHotFixをプルする
- 制限ユーザーでもHotFixの適用が可能
- 配布するHotFixは管理者が設定可能

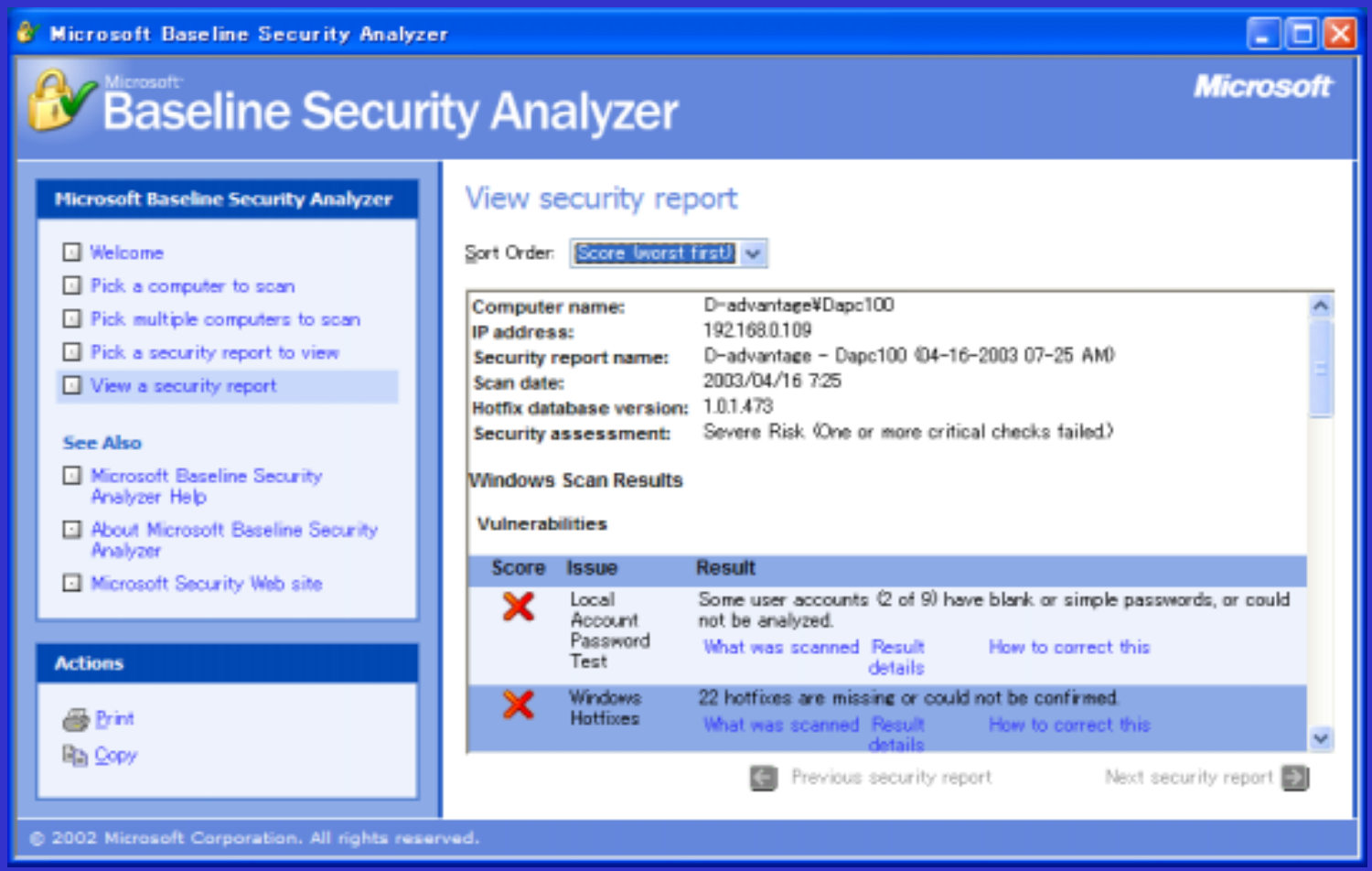
SUS
(Microsoft Software Update Services)

- **グループ単位で適用できる**HotFix**がオール・オア・ナッシング**
- HotFix**の適用が正常に完了したか、簡単には確認できない**
- **適用可能な**HotFix**は**Windows Update (**自動更新**) **と基本的に同じ。したがって**ServicePack**は適用不可。サーバ向け**HotFix**も適用できない**
- **適用可能クライアントは**Win2k SP2**以上、**IE 5.5**以上**
- **詳細は**Windows Server Insider**の記事を参照**
  - http://www.atmarkit.co.jp/fwin2k/operation/sus1/sus1_01.html

Windows Update／SUSで適用可能な修正プログラム

	Windows Update（Web版）	Windows Update（自動更新）／SUS
ServicePack	○	×
Security Rollup Package	○	○
重要な更新	○	○
推奨される更新	○	×
ドライバの更新	○	×

MBSA
(Microsoft Baseline Security Analyzer)



MBSA
(Microsoft Baseline Security Analyzer)

- コンピュータを走査し、未適用のHotFixなどを一覧する (リモートからも実行可能)
- HotFix情報だけでなく、さまざまなセキュリティ項目をチェックし、警告する
- GUIツール
- Win2K、XPにインストール可能。走査対象としては、NT4、Win2K、XPを指定可能 (Win9xは対象外)
- 正式な日本語版は提供されていない (制限はあるが、英語版を日本語環境で利用可能)
  - http://www.microsoft.com/japan/technet/security/tools/tools/mbsahome.asp

HFNetChk

- HotFixの適用状況をチェックできる（リモート実行して集中的に情報収集することが可能）
  - http://www.microsoft.com/japan/technet/security/tools/tools/hfnetchk.asp
- コマンド・ライン・ツール
- 日本語版データベース・ファイルも提供される
- 走査対象はNT4、Win2K、XP

- データベースはタイムリーには更新されない（緊急の更新があったときに更新されている模様）

QChain

- **複数のHotFixの適用を指定した場合、同じファイルが更新されるときは、最新のファイルを適用するようにする**
  - http://support.microsoft.com/default.aspx?kbid=296861
- **再起動も1回ですむ**
- **コマンド・ライン・ツール**

- **特定のインストーラ (hotfix.exe) にのみ対応。すべてのHotFixに対して有効というわけではない**

システム管理ツール

- SMS（マイクロソフト）、QND（クオリティ）などのネットワーク管理ツールの中には、ソフトウェアの配布機能を持つものがある。こうした配布機能を使ってHotFixを適用することができる
- インベントリ（構成情報）の取得が可能

- 配布するパッケージは管理者が作る必要がある（HotFixの依存関係やインストール・オプションなどは管理者が調査して配布パッケージを作成する）
- 資産管理に重点を置いて開発されているものが多い

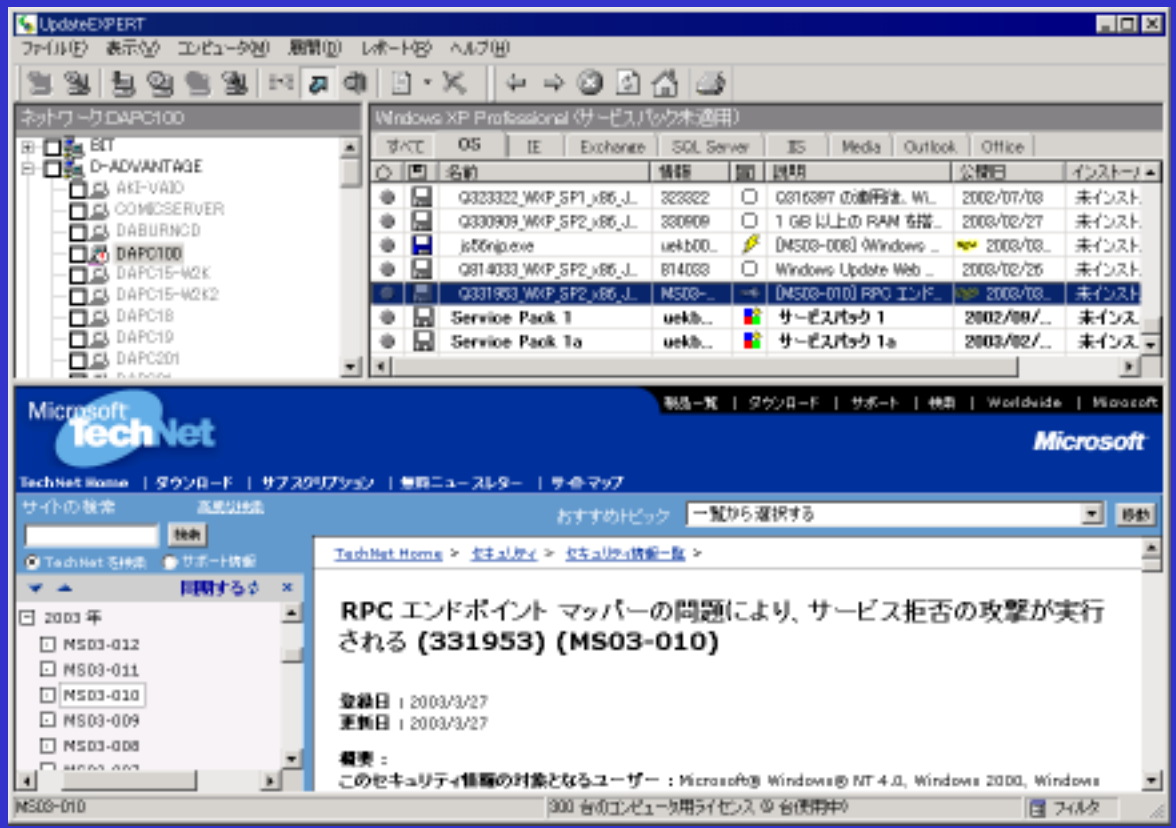
HotFix専用管理ツール

- HotFixの適用状態の確認、リモート適用が可能。HotFix間の依存関係やインストールオプション指定などを自動化してくれる
- 専用ツールなので小回りが効く
- 米国では複数のツールが販売され、マーケットが確立されている

製品名	開発元	URL
PatchLinlk Update	PatchLink	http://www.patchlink.com/
BigFix Enterprise Suite	BigFix	http://www.bigfix.com/website/
UpdateExpert	St. Bernard Softwre	http://www.stbernard.com/products/updateexpert/products_updateexpert.asp/
HFNetChkPro	Shavlik	http://www.shavlik.com/

HotFix専用管理ツール

- このうちSt. Bernard社のUpdateEXPERTの日本語対応版がアップデートテクノロジー社から発売された
- 今後は他製品の日本語版も発売されるものと思われる



UpdateEXPERT日本語版

まとめ

- セキュリティ管理はトータルで対応。クライアント管理も避けて通れない
- しかしクライアント向けのHotFix管理作業はあまりに複雑。管理するクライアントの台数が多ければ多いほど作業工数は増大する
- マイクロソフトの無償ツールを活用できるが、現実問題としては制限が大きい
- システム管理ツールのソフトウェア配布機能をHotFix配布に応用できる場合があるが、配布するための情報収集やパッケージ作成は簡略化されない
- HotFixの大量配布に特化した製品が登場し始めた。目的を限定する代わり、HotFix管理を前提とする各種作業（依存関係の処理、インストール・オプションの設定）が自動化される


DIGITAL
ADVANTAGE