Active Directoryの運用管理とセキュリティ

山近慶一, 創報
kyama@mountain.jp

本チュートリアルの概要

- 目的
  - Active Directoryドメインにおける、Windowsネットワークのセキュリティ維持に必要なシステムの構築運用について習得する
- 内容
  - Active Directoryの概要
  - Windowsネットワークの運用管理
  - Windows XP SP2 & Windows Server 2003 SP1
  - Software Update Servicesの概要

自己紹介

- 生業
  - テクニカルライター
    - IDG『Windows Server World』
  - 講師
    - 高度ポリテクセンター（幕張）
    - ポリテクセンター関西（大阪）
- 所属
  - NT-Committee2
  - MSMVP（Shell/User）

アンケートとディスカッション

- Q1：現在Windows NTドメインを運用していますか？
  - また、その規模（ユーザー数、コンピュータ数など）はどのくらいですか？
  - Windows 9x/Meも使っていますか？
- Q2：現在Active Directoryドメインを運用していますか？
  - また、その規模はどのくらいですか？
  - 導入時に苦労したことはありますか？
- Q3：Active Directoryドメインの導入を検討していますか？
  - いつ頃導入しようと考えていますか？
- Q4：検討中の方に伺います。
  - 今まで導入しなかった、できなかったのはなぜですか？
- Q5：検討していない方に伺います。
  - 導入しない理由は何でしょうか？
- Q6：本チュートリアルで、どんな成果を期待しますか？

Windows NTドメインの概要 (1)

- PDCとBDCの役割
  - レジストリのSAM (Security Account Manager) データベースの管理
  - PDCはSAMの原本を管理し、BDCはSAMの完全なコピーを持つ
  - 新規インストール中に役割を決定する
    - [サーバーマネージャ]で降格／昇格が可能
    - メンバサーバとドメインコントローラの降格／昇格は不可能
- ユーザー認証をどこで行うか
  - ワークグループ環境
    - コンピュータごとに認証
  - NTドメイン環境
    - ドメインコントローラに外部委託 (アウトソーシング)
    - コンピュータごとの認証も併用＝ドメインはワークグループを内包する
    - セキュリティ保護チャネルによる通信
- 「ドメインに参加する」とは
  - コンピュータアカウントをSAMに登録する
  - ドメインコントローラはメンバコンピュータを認証する
  - メンバコンピュータはドメインコントローラを信頼する

Windows NTドメインの概要 (2)

- 認証方式とセキュリティ
  - 認証方式
    - Lan Manager (LM) 認証：Lan Manager, Windows 9x/Me
    - NTLM認証：WindowsNT 4.0 SP3以前
    - NTLMv2認証：Windows NT 4.0 SP4以降, Windows 2000/XP, Windows Server 2003
  - セキュリティ
    - SMB (Server Message Block)：ファイル共有などの通信プロトコル
    - SMB署名 (SMBデジタル署名)：Windows NT 4.0 SP3以降で使用可能
- ドメイン構成の特徴
  - フルフラット構成＝すべてのドメインが対等
    - ユーザーが意図的に使い分ける
  - 信頼関係の複雑化
    - 2ドメインで2本、3ドメインで6本、4ドメインで12本…n× (n-1) 個の信頼関係が必要

Windows NTドメインの概要 (3)

- ドメインの管理
  - システムポリシー
    - レジストリ操作でシステムに制限をかける
    - “刷り込み”効果がある
- コンピュータ名 (NetBIOS名) とホスト名
  - コンピュータ名とNTドメイン名の名前解決
    - LMHOSTSファイル
    - WINS (Windows Internet Name Service) サーバ
    - 通信可能な範囲に、重複するコンピュータ名やNTドメイン名があってはならない
  - ホスト名とインターネットの利用
    - HOSTSファイル
    - DNSサーバ
  - 問題点
    - NTドメイン名 (NetBIOSドメイン名) とDNSドメイン名に関連がない
    - コンピュータ名とホスト名の2重管理

Active Directoryドメインの概要 (1)

- ディレクトリサービスとは
  - ユーザーやグループに関する総合カタログ
    - メールアドレスや役職情報などを提供する
  - アプリケーション用に拡張可能
    - アプリケーションディレクトリパーティション
    - DNSサーバ (Active Directory統合ゾーン)
- ドメイン、フォレスト、サイト
  - ドメイン
    - 1台以上のDCを持つコンピュータの集合
  - フォレスト
    - 1つ以上のドメインを持つドメインの集合
    - ドメインツリー：同じDNSドメイン名の下に作るドメイン群
    - フォレストが2つ以上のツリーに分かれていてもよい
  - サイト
    - 異なるネットワーク
    - 1つのドメインが複数のサイトにまたがっていてもよい
    - 1つのサイトに複数のドメインがあってもよい

Active Directoryドメインの概要 (2)

- DCの役割
  - ディレクトリデータベースの管理
  - マルチマスタ複製
  - インストール中およびインストール後に役割を決定する
    - コマンドで役割を変更可能
- DNSドメインとActive Directoryドメインの関係
  - DNSのしくみ
    - 前方参照ゾーン：ホスト名＋ドメイン名から、IPアドレスを取得
      - example.co.jp
        ルートーjpドメインーcoドメインーexampleという組織
    - 逆引き参照ゾーン：IPアドレスからホスト名＋ドメイン名を取得
      - 192.168.1.1
        ルートーarpaーin-addrー192ー168ー1ー1というIPアドレス
  - 名前解決
    - ゾーン名＝Active Directoryドメイン名
      - example.co.jp
    - SRVリソースレコードを使ってDCを特定
      - _msdcs.example.co.jp
  - DNSドメインの名前階層＝フォレストのツリー構造
    - 前方参照ゾーンの階層構造が、ドメインツリーを決定する

Active Directoryドメインの概要 (3)

- ドメインの管理
  - グループポリシー
    - “刷り込み”効果がない
    - 再起動なしに適用可能
      - [Secedit]コマンドや[Gpupdate]コマンドで更新も可能
    - 最終的にはレジストリに書き込まれる
      - HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies
      - HKEY_CURRENT_USER¥Software¥Policies
  - 組織単位
    - ユーザーやコンピュータを分類する
- Kerberos認証
  - 鍵交換方式
  - 時刻同期
    - 5分以内のズレを許容
    - メンバコンピュータはDCと自動的に同期
    - DCは自分自身、または外部のNTPサーバを参照して同期
- 下位互換性
  - NetBIOSサポート
    - 通信可能な範囲に、重複するコンピュータ名やNetBIOSドメイン名があってはならない
  - セキュリティ：NTLMv2認証、SMB署名

DCの役割

- FSMO (Flexible Single Master Operations)
  - スキーママスタ (フォレスト全体で1台)
    - ディレクトリデータベースの変更を管理する
  - ドメイン名前付けマスタ (フォレスト全体で1台)
    - フォレスト内のドメインの追加／削除を管理する
  - RIDマスタ (ドメインごとに1台)
    - ユーザーの内部IDである、セキュリティIDを管理する
  - PDCエミュレータ (ドメインごとに1台)
    - Windows NTドメインのPDCをエミュレートする
  - インフラストラクチャマスタ (ドメインごとに1台)
    - ディレクトリデータベースの複製を管理する
- グローバルカタログ (GC)
  - ユーザーが所属するグループの確認や、オブジェクトの検索
  - 重い電話帳のかわりの、携帯可能なアドレス帳
  - ログオン時に参照

Active Directoryドメインの導入方法

- 1. 新規導入
  - 制約のない環境に、Active Directoryドメインを構築する
- 2. アップグレード
  - 既存のWindows NTドメインコントローラをWindows Server 2003にアップグレードして、直接Active Directoryドメインに変更する
- 3. マイグレーション
  - 新規にActive Directoryドメインを構築し、ツールを使って移行する
  - a) 併呑
    - Windows NTドメインを最終的に消滅させる
  - b) 共存
    - アプリケーションなどの都合で、Windows NTドメインも使い続ける

Active Directory導入前の検討項目

- フォレストとドメインの設計
  - DNSの名前階層
    - Webサイトやメールアドレスとの統一性
  - DNSサーバの設置
    - 外向きDNSサーバと内向きDNSサーバ
    - Active Directory用のDNSサーバをインターネットに公開しない
      - 全コンピュータの情報をインターネットに晒すことになる
  - サブドメイン、別のツリー、サイト
- 互換性
  - Windows 9x/Me/NTとの接続
  - アプリケーション
- ライセンス
  - クライアントアクセスライセンス (CAL)
  - ターミナルサービス (TS)

運用管理

- グループポリシーの設定
  - システムポリシーとグループポリシー
  - OUとグループポリシーの利用方法
  - 適用状況の監視
- システム管理ツール
  - イベントビューア
  - ドメインとフォレストの機能レベル
- バックアップ
  - システム状態 (System State)
  - ディレクトリサービス復元モード

グループポリシーでできること

- できること
  - セキュリティの設定
    - ユーザーアカウントとパスワードの管理
    - システム監査
    - サービスの動作状態
    - ソフトウェアの制限
    - ワイヤレスネットワーク
  - Windowsコンポーネント
    - Windowsファイアウォール
    - Internet Explorer
    - Windows Update
    - NetMeeting, Windows Messenger, Windows Media Player
  - デスクトップなどのカスタマイズ、変更禁止
  - アプリケーションの配布と割り当て
- 制限事項
  - コンテナには適用できない
  - グループには適用されない

グループポリシーの適用順序

- 適用順序＝LSD-OU
  - 1. ローカルグループポリシー
  - 2. サイトにリンクされたグループポリシー
  - 3. ドメインにリンクされたグループポリシー
  - 4. OUにリンクされたグループポリシー
- 同一レベルに複数のグループポリシーがある場合は、並び順の下から
- ポリシーの上書き
  - 同一ポリシー項目は、後から適用されるポリシーの設定で上書きされる
- ドメインレベルでのみ有効なポリシー
  - アカウントポリシー
  - セキュリティオプション
    - ネットワークセキュリティ：ログオン時間を経過した場合はユーザーを強制的にログオフさせる
    - アカウント：Administratorアカウント名の変更
    - アカウント：Guestアカウント名の変更
- 更新
  - 90分ごと（0～30分のランダムオフセット付き）
  - 更新間隔もグループポリシーで設定可能

特殊なグループポリシーと管理

- 特殊なグループポリシー
  - ローカルセキュリティポリシー
    - ローカルグループポリシーから、セキュリティ関連のポリシーを切り出したもの
  - ドメインセキュリティポリシー
    - ドメイングループポリシー (Default Domain Policy) から、セキュリティ関連のポリシーを切り出したもの
  - ドメインコントローラセキュリティポリシー
    - Domain Controllers OUにリンクされたグループポリシー (Default Domain Controllers Policy) から、セキュリティ関連のポリシーを切り出したもの
- グループポリシーの管理
  - グループポリシー管理コンソール (GPMC)

パスワードのポリシー

- [パスワードは要求する複雑さを満たす]
  - 次の4群から3つ以上を組み合わせる
    - アルファベット大文字 (A～Z)
    - アルファベット小文字 (a～z)
    - 数字 (0～9)
    - 記号 (!、$、#、%)
  - ユーザー名の一部を含まない
- パスワードの長さ
  - 最大127文字、15文字以上はWindows 9xが認識不能
  - 8文字～14文字を推奨
- 変更の頻度
  - 短期間で変更するべき
  - ユーザーが覚えられない
    - メモする、貼る
    - 同じパスワードを繰り返し使う

役割の移動と負荷分散

- 管理ツールでFSMOとGCを移動する
  - スキーママスタ
    - [Active Directoryスキーマ]
  - ドメイン名前付けマスタ（ドメインネーミングマスタ）
    - [Active Directoryドメインと信頼関係]
  - RIDマスタ
    - [Active Directoryユーザーとコンピュータ]
  - PDCエミュレータ
    - [Active Directoryユーザーとコンピュータ]
  - インフラストラクチャマスタ
    - [Active Directoryユーザーとコンピュータ]
  - GC
    - [Active Directoryサイトとサービス]
- 成功のポイント
  - 移動先のDCで管理ツールを操作する

[Active Directoryスキーマ] 管理ツールの使用

- レジストリに登録する
  - 1. コマンドプロンプトを開く
  - 2. 次のコマンドを実行する
    Regsvr32 %SystemRoot%¥System32¥Schmmgmt.dll
- スナップインを開く
  - 1. [スタート]－[ファイル名を指定して実行]を開く
  - 2. [mmc]と入力して、管理コンソールを開く
  - 3. [ファイル]－[スナップインの追加と削除]を実行する
  - 4. [Active Directoryスキーマ]スナップインを追加する

FSMOの強制移動（占有）

- Ntdsutilコマンド
  - ntdsutil: roles
  - fsmo maintenance: connections
  - server connections: connect to server <自DCのFQDN>
  - server connections: quit
  - fsmo maintenance: seize RID master
    - seizeサブコマンドを実行するごとに、最新の操作マスタが列挙される
  - fsmo maintenance: seize PDC
  - fsmo maintenance: seize infrastructure master
  - fsmo maintenance: seize domain naming master
  - fsmo maintenance: seize schema master
  - fsmo maintenance: quit
  - ntdsutil: quit
- 注意
  - seizeを実行しても、最初にtransferが試みられる
  - 強制移動後は、移動元DCを稼働状態に戻してはならない

情報と使用ツールなど

- マイクロソフト ヘルプとサポート
  - http://support.microsoft.com/
  - サポート技術情報を直接参照するには
    - http://support.microsoft.com/default.aspx?scid=kb;ja;＜文書番号＞
- Active Directoryクライアント for Windows NT 4.0
  - http://www.microsoft.com/japan/windows2000/server/evaluation/news/bulletins/adextension.asp
  - Windows 9x用はWindows 2000 Serverのインストール CD-ROMに同梱
- グループポリシー管理コンソール SP1 日本語版
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=c355b04f-50ce-42c7-a401-30be1ef647ea&DisplayLang=ja
  - GPMCのFAQ http://www.microsoft.com/japan/windowsserver2003/gpmc/gpmcfaq.mspx

Windowsの通信ポート

- DNS
  - TCP/UDP 53
- Kerberos
  - TCP/UDP 88
  - TCP/UDP 464
- NTP
  - UDP 123
- NetBIOS系
  - TCP/UDP 137～139
- LDAP
  - TCP/UDP 389
  - SSL使用時はTCP/UDP 636
- Macintoshサービス
  - TCP 548
- SMB
  - TCP/UDP 445
- GC
  - TCP/UDP 3268
  - SSL使用時はTCP/UDP 3269
- その他
  - %SystemRoot%¥System32¥drivers¥etc¥services
  - KB：832017

Windowsのノードタイプ

- bノード：
  - ブロードキャストノード
  - ①NetBIOSネームキャッシュ
  - ②ブロードキャスト
  - ③LMHOSTS
- hノード
  - Hybridノード
  - ①NetBIOSネームキャッシュ
  - ②WINS
  - ③ブロードキャスト
  - ④LMHOSTS
- mノード
  - Mixedノード
  - ①NetBIOSネームキャッシュ
  - ②ブロードキャスト
  - ③WINS
  - ④LMHOSTS
- pノード
  - Point-to-Pointノード
  - ①NetBIOSネームキャッシュ
  - ②WINS
  - ③LMHOSTS

Tea Break 1

Service Packs for Windows XP and Windows Server 2003

概要

- Windows XP SP2の新機能
- Windows XP SP2の強化変更点
- Windows Server 2003 SP1の新機能
- Windows Server 2003 SP1の強化変更点
- SPの機能比較
- SPの配布

Windows XP SP2の概要 (1)

- 新機能
  - セキュリティセンター
  - データ実行防止
  - ワイヤレスネットワークセットアップウィザード
  - Post-Setup Security Updates
- 強化変更
  - Windowsファイアウォール
  - 自動更新
  - Internet Explorer 6.0 SP2
  - Outlook Express 6.0 SP2

Windows XP SP2の概要 (2)

- 強化変更 (続き)
  - 「プログラムの追加と削除」のフィルタ
  - Windows Installer 3.0
  - Background Intelligent Transfer Service 2.0
  - RPCのセキュリティ強化
  - DCOMのセキュリティ強化
  - WebDAVと基本認証の使用制限
  - Windows Update Version 5
  - Windows Updateからドライバをインストール

Windows XP SP2の概要 (3)

- 強化変更 (続き)
  - NAT Traversal
  - Bluetoothデバイスのサポート
  - Alerter/Messengerサービスの無効化
  - Windows Messenger 4.7
  - Windows Media Player 9
  - Windowsムービーメーカー2.1
  - DirectX 9.0c
  - NetScheduleとタスクスケジューラAPI
  - タブレットPC用の文字認識能力改善

Windows Server 2003 SP1の概要 (1)

- 新機能
  - セキュリティ構成ウィザード
  - データ実行防止
  - ワイヤレスネットワークセットアップウィザード
  - ワイヤレスプロビジョニングサービス
  - Post-Setup Security Updates

Windows Server 2003 SP1の概要 (2)

- 強化変更
  - Windowsファイアウォール
  - 自動更新
  - Internet Explorer 6.0 SP2
  - Outlook Express 6.0 SP2
  - 「プログラムの追加と削除」のフィルタ
  - Windows Installer 3.01
  - Background Intelligent Transfer Service 2.0
  - RPCのセキュリティ強化
  - DCOMのセキュリティ強化

Windows Server 2003 SP1の概要 (3)

- 強化変更
  - WebDAVと基本認証の使用制限
  - Windows Update Version 5
  - Windows Updateからドライバをインストール
  - TCP/IPプロトコルスタックの強化
  - ポータブルメディアデバイスのサポート
  - Windows Media Player 10
  - DirectX 9.0c
  - 「タスク」の「隠しタスクを表示」オプション

SPの機能比較 (1)

- Windows XP SP2のみの機能
  - セキュリティセンター
  - NAT Traversal
  - Alerter/Messengerサービスの無効化
  - Windows Messenger4.7
  - Windowsムービーメーカー2.1
  - タブレットPC用の文字認識能力改善
- Windows Server 2003 SP1のみの機能 (暫定)
  - セキュリティ構成ウィザード
  - ワイヤレスプロビジョニングサービス
  - TCP/IPプロトコルスタックの強化
  - ポータブルメディアデバイスのサポート
  - 「タスク」の「隠しタスクを表示」オプション

SPの機能比較 (2)

- 共通機能 (暫定)
  - データ実行防止
  - Post-Setup Security Updates
  - ワイヤレスネットワークセットアップウィザード
  - 自動更新
  - Internet Explorer 6.0 SP2
  - Outlook Express 6.0 SP2
  - 「プログラムの追加と削除」のフィルタ
  - Background Intelligent Transfer Service 2.0
  - DCOMのセキュリティ強化
  - WebDAVと基本認証の使用制限

SPの機能比較 (3)

- 共通機能 (暫定)
  - Windows Update Version 5
  - Windows Updateからドライバをインストール
  - DirectX 9.0c
- Windows Server 2003 SP1で変更された機能 (暫定)
  - Windowsファイアウォール
  - Windows Installer 3.01
  - RPCのセキュリティ強化
  - Windows Media Player10

Windowsファイアウォール (1)

- 差違
  - Windows XP SP2：Windowsファイアウォールは常に有効
  - Windows Server 2003 SP1：新規インストール時のみ有効
    - 既存Windows Server 2003にSP1をインストールしても、有効にならない
- 例外の許可と構成
  - 有効、有効＋例外を許可しない、無効
  - 例外
    - プログラムの追加
      - Svchost.exeは登録不可
    - ポートの追加
  - 構成オプション
    - グローバル構成オプション＝「例外」タブ
    - ローカル構成オプション＝「詳細設定」タブ
  - スコープ
    - 任意のコンピュータ（インターネット上のコンピュータを含む）
    - ユーザーのネットワーク（サブネット）のみ
    - カスタムの一覧

Windowsファイアウォール (2)

- コンピュータ起動時の保護
  - 起動時ポリシー
- デフォルト設定のリストア
  - 「詳細設定」タブの「既定値に戻す」ボタン
- プロファイル
  - 「標準プロファイル」と「ドメインプロファイル」
  - モバイル環境で使い分け
- リモート管理
  - 管理ツールの接続エラー
    - コンピュータ＜コンピュータ名＞にアクセスできません
    - ネットワークパスが見つかりませんでした
  - Netshコマンドの拡張
    - Netsh firewall set portopening TCP 445 enable
    - 「ファイルとプリンタの共有」に含まれる
  - ポリシー
    - Windowsファイアウォール：リモート管理の例外を許可する
    - Windowsファイアウォール：ファイルとプリンタの共有の例外を許可する

Windowsファイアウォール (3)

- IPv6用ICFの統合
  - Advanced Networking Pack for WindowsXP
- RPCのフィルタリング
  - RPCの待ち受け側は例外に登録
- マルチキャストとブロードキャスト
  - 3秒以内の応答を選択受信
  - 「Windowsファイアウォール：マルチキャストまたはブロードキャスト要求に対するユニキャスト応答を禁止する」ポリシー
  - Netshコマンドの拡張
    - Netsh firewall show multicastbroadcastresponse
    - Netsh firewall set multicastbroadcastresponse ENABLE (またはDISABLE)
- カスタマイズ
  - %SystemRoot%¥inf¥Netfw.inf
  - 「Using the Windows Firewall INF File in Microsoft Windows XP Service Pack2」 (http://www.microsoft.com/downloads/details.aspx?FamilyID=cb307a1d-2f97-4e63-a581-bf25685b4c43&displaylang=en)

セキュリティセンター

- 3本の柱
  - ファイアウォール
    - サードパーティ製品との衝突に注意
  - 自動更新
    - 「ようこそ」画面やログオン画面が表示される前
    - SUS/WUS使用時は常に「設定を確認してください」
  - ウイルス対策
    - Windows Management Instrumentation (WMI)で監視
- ドメインとワークグループ
  - デフォルトではワークグループ環境でのみ動作
    - このコンピュータはドメイン (ネットワーク上のコンピュータのグループ) に属するため、このコンピュータのセキュリティの設定は、ネットワーク管理者によって管理されています
  - 「セキュリティセンターを有効にする (ドメイン上のコンピュータのみ) 」ポリシー

セキュリティ構成ウィザード

- オプションコンポーネント
- 作成できるセキュリティポリシー
  - 不要なサービスの停止
  - 不要なインターネットインフォメーションサービス (IIS) Web拡張の停止
  - 未使用の通信ポートの閉鎖やIPSecの使用
  - 「LAN Manager認証レベル」「LDAP署名」「SMB署名」などによる通信のセキュリティ強化
  - 監査ポリシーの設定
- ウィザードの機能
  - ローカルまたはリモートコンピュータのセキュリティポリシーの新規作成、編集、適用
  - 適用済みのセキュリティポリシーを以前の状態に戻す「ロールバック」
  - セキュリティポリシーを作成したり分析したりするだけで、適用しないオプション
  - 「Scwcmd.exe」コマンドによる、作成、分析、適用などのコマンド実行
  - 作成したセキュリティポリシーを、グループポリシーで配布する
  - XMLファイルにセキュリティポリシーを保存して、配布したり再編集したりする
    - デフォルトの保存先フォルダは、「%SystemRoot%¥security¥msscw¥Policies」
  - 従来のセキュリティテンプレートファイルをインポートして利用する

自動更新とBITS 2.0

- SUS/WUSサポート
  - Software Update Services/Windows Update Services
    - 「イントラネットのMicrosoft更新サービスの場所を指定する」ポリシー
- ポリシーテンプレートファイル
  - %SystemRoot%¥inf¥wuau.adm
    - Windows Server 2003 SP1が最新版
- Background Intelligent Transfer Service (BITS) 2.0と協調
  - BITS 2.0の特長
    - 「WinHTTP」コンポーネントを使ってファイル転送を実行する
    - 優先度を指定して複数のファイルを転送できる
    - ファイルの転送を実行する時間帯を指定できる
    - ファイルの変更差分だけを転送できる
    - フォアグラウンドで全帯域を使用したファイル転送と、バックグラウンドでアイドル帯域を使用したファイル転送ができる
    - 転送中に接続が切れても、中断したところから転送を再開できる
  - 自動更新のプロキシ対応
    - BITS 2.0自体はプロキシに対応しているが、自動更新が非対応
    - Local Systemアカウントにレジストリ値を設定
      - HKEY_USERS¥S-1-5-18¥Software¥Microsoft¥Windows¥CurrentVersion¥Internet Settings
      - ProxyEnable、ProxyServer、ProxyOverride

データ実行防止

- 例外エラー
  - ユーザーモードのDEP例外：STATUS_ACCESS_VIOLATION (0xc0000005)
  - カーネルモードのDEP例外：ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY (0xFC)
- ソフトウェアDEP
  - Boot.iniの「/NoExecute＝<レベル>」オプション
    - OptIn (デフォルト)：「重要なWindowsのプログラムおよびサービスについてのみ有効にする」オプションと同じ。
      - 「/NoExecute＝<レベル>」オプションが記述されていなければ、「OptIn」であると解釈される
    - OptOut：「次に選択するものを除くすべてのプログラムおよびサービスについてDEPを有効にする」オプションに相当
      - 例外アプリケーションを手動で登録できる
    - AlwaysOn：システム全体でDEPを有効にする。すべてのプロセスがDEPの保護対象になる
    - AlwaysOff：システム全体でDEPを無効にする
- ハードウェアDEP
  - No eXecute (NX) / Execute Disable bit (XD)
    - AMD：Opteron、Athlon64、Sempron
    - インテル：Itanium、Pentium4、Celeron
    - トランスメタ：Efficeon
  - Physical Address Extension (PAE)モード

Post-Setup Security Updates

- Post-Setup Security Updates
  - Out-of-Box Experience
- 差違
  - Windows XP
    - ログオン前に「コンピュータを保護してください」で自動更新を設定
    - ログオン後にセキュリティセンターが起動
  - Windows Server 2003
    - 新規インストール時にWindowsファイアウォールの設定とWindows Updateによるシステムの更新を実行
    - SP1適用済みのWindows Server 2003を新規インストールしたときのみ実行
  - 以下のケースでは実行されない
    - 既存のWindows Server 2003にSP1をインストールした場合
    - Windows 2000 ServerからSP1適用済みのWindows Server2003にアップグレードしたとき
    - 無人インストールで、明示的にWindowsファイアウォールを有効または無効に設定したとき
    - グループポリシーで、明示的にWindowsファイアウォールを有効または無効に設定したとき

IE 6.0 SP2の新機能 (1)

- 情報バー
  - 表示条件
    - アドオン (ActiveXコントロール) のインストール時と実行時
    - ポップアップのブロック時
    - ファイルのダウンロード時
- ポップアップブロック
  - ブロック条件
    - DHTMLのwindow.openメソッドやwindow.showHelpメソッドなどで、ユーザーのクリック操作なしでウィンドウを開こうとしたとき
    - デスクトップの表示領域より大きいウィンドウや、表示領域外にウィンドウを描画しようとしたとき
  - 例外
    - 「信頼済みサイト」ゾーンや「イントラネット」ゾーンに登録されたWebサイト
    - 「許可されたサイト」に登録されたWebサイト
    - ユーザーが意図的にリンクをクリックして開いたWebページ
    - 「Ctrl」キーを押しながらクリックして開いたWebページ
    - ローカルコンピュータにインストールして実行中のアプリケーションが開くウィンドウ
    - インストールされたActiveXコントロールが開くウィンドウ
    - Webページに重ねて表示するDHTML要素

IE 6.0 SP2の新機能 (2)

- ウィンドウの制限
  - 一般の制限
    - ウィンドウのステータスバーを無効にできない
    - ウィンドウタイトル、ツールバー、アドレスバー、ステータスバーを、表示領域外に隠したウィンドウを作成できない
    - デスクトップの表示領域より大きいウィンドウを作成できない
    - デスクトップの表示領域外にウィンドウを作成できない
  - ポップアップウィンドウの表示制限
    - ウィンドウサイズが親ウィンドウの上端または下端を超えない
    - ウィンドウの幅は、親のウィンドウより狭い
    - ウィンドウの表示位置は、親ウィンドウと水平方向で重なる
    - ウィンドウは、親ウィンドウと一緒に移動する
    - ウィンドウは、ダイアログボックスなどのウィンドウを隠さないように、親ウィンドウに重ねて表示する
- 発行者のデジタル署名の確認
  - 「信頼された発行元」と「信頼されない発行元」

IE 6.0 SP2の新機能 (3)

- アドオンの管理
  - 有効/無効、ActiveXの更新
- アドオンのクラッシュ検出
  - 「クラッシュの検出を無効にする」ポリシー
- ビヘイビアの制限とロックダウン
  - バイナリビヘイビアとスクリプトビヘイビアの制限
  - 影響
    - ActiveXコントロールやスクリプトがエラーになる
    - 画像が表示されない
    - Javaアプレットが実行されない
- BindToObject実行時のセキュリティチェック処理負荷の軽減
  - URLをソースとするすべてのオブジェクトの初期化について、「ActiveXセキュリティモデル」が適用される

IE 6.0 SP2の新機能 (4)

- ローカルコンピュータゾーンのロックダウン
  - オプション
    - マイコンピュータでの、CDのアクティブコンテンツの実行を許可する
    - マイコンピュータのファイルでのアクティブコンテンツの実行を許可する
- MIMEハンドリングのセキュリティ強化
  - MIMEハンドラのProgIDと、拡張子に関連づけられたアプリケーションのCLSIDをチェック
- ネットワークプロトコルのロックダウン
  - 「file:」「shell:」などを個別に制限できる
- 「UrlAction」の制限ポリシー
  - 「未署名のActiveXコントロールのダウンロード」「ActiveXコントロールとプラグインの実行」「異なるドメイン間のサブフレームの移動」などのゾーン別制限
- ゾーン昇格ブロック
  - 「より権限の少ないWebコンテンツゾーンのWebサイトがこのゾーンに移動できる」オプション
- オブジェクトキャッシュのアクセス禁止
  - クロスドメインアクセスを防止

OE 6.0 SP2の新機能

- メッセージのプレーンテキスト表示
  - MSHTMLコントロールからリッチエディットコントロールに変更
  - 文字のサイズを変更したり、メッセージ内のテキストを検索したりする機能が使用できない
- 迷惑メール対策
  - 「HTML電子メールにある画像および外部コンテンツをブロックする」オプション
- 添付ファイルブロック
  - 「ウイルスの可能性がある添付ファイルを保存したり開いたりしない」オプション

RPCのセキュリティ強化

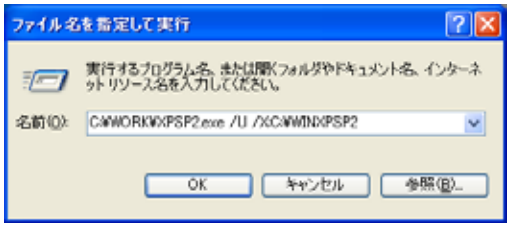
- レジストリ
  - キーの場所:
    HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows NT¥RPC
  - 「認証されていないRPCクライアントの制限」ポリシー
    - RestrictRemoteClients (DWORD値)
      - 0＝RPCの匿名アクセスを許可する (デフォルト)
      - 1＝従来のWindowsと同じレベルの拒否
      - 2＝RPCによるリモート匿名呼び出しを完全に禁止する。管理ツールやWMI (Windows Management Instrumentation) などは利用不能になる
    - WindowsXP SP1ではデフォルト値は「1」だったが、Windows Server2003 SP1のデフォルト値は「0」に変更されている
  - 「RPCエンドポイントマッパクライアント認証」ポリシー
    - EnableAuthEpResolution (DWORD値)
      - 0＝エンドポイントマッパにアクセスする際にNTLM認証を必要としない (デフォルト)
      - 1＝NTLM認証を使用する

SPのインストールオプション (1)

- 新しいインストールオプション
  - 確認方法
    - XPSP2.exe /?
    - SRSP1.exe /?
    - update.exe /help

SPのインストールオプション (2)

- 自動展開
  - XPSP2.exe /U
  - SRSP1.exe /U
- 展開フォルダ指定
  - XPSP2.exe /X:**パス**
  - SRSP1.exe /X:**パス**



SPのアンインストール

- プログラムの追加と削除
- コマンド
  - ＜SP2のアンインストールフォルダ＞¥spuninst¥spuninst.exe
- 回復コンソール
  - CHDIR $NtServicePackUninstall$¥spuninst
    BATCH spuninst.txt
    EXIT

SPの配布

- 配布ポイント
  - ＜保存フォルダ＞¥XPSP2.exe /U /X:E:¥WINXPSP2
  - E:¥WINXPSP2を共有
  - Everyone 読み取り
- グループポリシー
  - パッケージの割り当て
- 統合インストール
  - XCOPY ＜CD-ROMドライブ＞¥ ＜コピー先ドライブ＞¥XPPROSP2 /E
  - ＜配布ポイント＞¥I386¥Update¥Update.exe /integrate:＜統合先ドライブ＞¥XPPROSP2
  - Everyone 読み取り
- リモートインストールサービス
  - システム準備ツール
  - セットアップマネージャ
  - Riprep.exeでイメージ作成
- ツール
  - SUS/WUS/SMS

参考情報 (1)

- セキュリティセンター
  - WindowsXP SP2の新機能 [セキュリティセンター] の概要 (883739)
  - Windowsセキュリティセンターを使用して自動更新の設定を変更する方法 (875349)
  - WindowsXP SP2でドメインに参加すると、セキュリティセンターが既定で無効にされる (883763)
  - 他社製ファイアウォールソフトが認識されない場合 (884154)
  - 他社製ファイアウォールソフトを使う場合 (884156)
  - [セキュリティセンター] でウイルス対策ソフトが認識されない場合の対処方法 (883879)
- データ実行防止
  - WindowsXP Service Pack2で“データ実行防止”というエラーメッセージが表示される (875351)

参考情報 (2)

- Windowsファイアウォール
  - WindowsXP Service Pack2のWindowsファイアウォール機能について (843090)
  - WindowsXP Service Pack2でWindowsファイアウォール機能を構成する方法 (875356)
  - Windowsファイアウォールの設定項目の詳細 (883590)
  - WindowsXP Service Pack2でセキュリティの警告ダイアログボックスを使用する方法 (875353)
  - Windowsファイアウォールの設定を既定値に戻す方法 (883697)
  - WindowsXP SP2のクライアント管理ツールでの既知の問題 (870703)
  - Windowsファイアウォールを設定したまま、リモートデスクトップを有効にする方法 (883874)
  - Windowsファイアウォールを有効にした状態でファイルとプリンタの共有を行うには (883876)
  - Windowsファイアウォールを設定したまま、IISのサービス提供を有効にする方法 (883877)
  - WindowsXP Service Pack2でWindows NetMeetingのリモートデスクトップ共有機能を有効にする方法 (878451)
  - Advanced Networking Pack for WindowsXPの概要 (817778)

参考情報 (3)

- 自動更新
  - 自動更新機能の使用方法 (833627)
  - 自動更新中に [コンピュータの電源を切る] を選択した時の動作について (884157)
- IE 6.0 SP2
  - WindowsXP Service Pack2への対応に向けたWebサイトの最適化
    - http://www.microsoft.com/japan/msdn/windows/windowsxp/xpsp2web.asp
  - WindowsXP SP2のInternet Explorerの情報バーについて (843017)
  - [Windowsセキュリティの重要な警告] 画面について (875399)
  - ローカルディスクやCD-ROMに保存されているHTMLファイルが期待通りに動作しない (875396)
  - Internet Explorerのポップアップブロックを構成する方法 (843016)
  - ポップアップブロックの設定を変更する方法 (884223)
  - WindowsXP Service Pack2でポップアップブロックを有効にしても、ポップアップウィンドウが表示される (843015)
  - Internet Explorer6の安全でないファイル (Unsafe File) 一覧に関する情報 (291369)

参考情報 (4)

- OE 6.0 SP2
  - WindowsXP Service Pack2のOutlook Expressのテキスト形式モードについて (883257)
  - 添付ファイルのブロックの設定をカスタマイズする方法 (883764)
  - Outlook Expressの添付ファイルブロック機能について (883873)
- BITS 2.0
  - WindowsXP用のバックグラウンドインテリジェント転送サービス (BITS) 2.0およびWinHTTP5.1を含む更新プログラムパッケージ (842773)
  - WindowsXPのバックグラウンドインテリジェント転送サービス (BITS) 2.0用の更新プログラム (842309)
- その他
  - The Task Scheduler API
    - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/taskschd/taskschd/the_task_scheduler_api.asp

参考情報 (5)

- Windows XP SP2
  - **パソコンの安全対策**
    - http://www.microsoft.com/japan/windowsxp/sp2/booklet/default.mspx
  - WindowsXP Service Pack2**の**CD-ROM**ご注文**
    - http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/ja/default.mspx
  - IT**プロフェッショナルおよび開発者用**WindowsXP Service Pack2**ネットワークインストールパッケージ**
    - http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=049C9DBE-3B8E-4F30-8245-9E368D3CDB5A
  - 「WindowsXP Service Pack2**セキュリティ強化機能搭載**」**を入手する方法** (885012)
  - WindowsXP Service Pack2**に必要なハードディスクの空き領域** (837783)
  - **詳細な**WindowsXP Service Pack2**インストールチュートリアル** (875364)
  - WindowsXP Service Pack2**リリースノート** (835935)
  - WindowsXP SP2**をインストールする方法** (884514)

参考情報 (6)

- Windows XP SP2
  - WindowsXP**互換性情報－各メーカー別**WindowsXP Service Pack2**関連情報**
    - http://www.microsoft.com/japan/windowsxp/compatible/sp2/
  - WindowsXP SP2**をインストールする前に推奨する事前準備** (884473)
  - WindowsXP SP2**のインストールが正常にできているか確認する方法** (884227)
  - **プログラムや更新プログラムをインストールできない** (822798)
  - **コンピュータから**WindowsXP Service Pack2**を削除する方法** (875350)
  - WindowsXP Service Pack2**を削除する場合にコンピュータを保護する方法** (878454)
  - WindowsXP Service Pack2**展開に関する情報**
    - http://www.microsoft.com/japan/technet/prodtechnol/winxppro/deploy/xpsp2dep.mspx
  - WindowsXP Service Pack2**適用済みインストールイメージの作成方法** (884746)
  - WindowsXP Service Pack2**適用済みインストールイメージは**WindowsXP**以外で作成できない** (884737)
  - WindowsXP Service Pack2**展開ツール**
    - http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=3E90DC91-AC56-4665-949B-BEDA3080E0F6

参考情報 (7)

- Windows XP SP2
  - Systems Management Serverを使用してWindowsXP Service Pack2 (SP2) をインストールする方法 (842844)
  - WindowsXP Service Pack2 SMS Files
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=938f3fec-9e63-40c2-83a6-fc97a239ddd5&DisplayLang=en
  - WindowsXP SP2の配布と、WindowsXP2クライアントでの運用について
    - http://www.microsoft.com/japan/smserver/techinfo/sms2003xp.mspx
  - Using the Windows Firewall INF File in Microsoft Windows XP Service Pack2
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=cb307a1d-2f97-4e63-a581-bf25685b4c43&displaylang=en
- 配布禁止
  - Windows Updateおよび自動更新によるWindowsXP Service Pack2の配布を一時的に無効にする
    - http://www.microsoft.com/japan/technet/prodtechnol/winxppro/maintain/sp2aumng.mspx
  - Toolkit to Temporarily Block Delivery of WindowsXP SP2 to a PC Through Automatic Updates and Windows
    - http://www.microsoft.com/downloads/details.aspx?FamilyId=8BCE6BBA-EA5D-4425-89C1-C1CB1CCD463C&displaylang=en

Tea Break 2

Software Update Services

修正プログラム (HotFix) の配布

- 直接配布
  - グループポリシー
  - ログオンスクリプト
  - スタートアップスクリプト
  - バッチファイル
- 間接配布、自動配布
  - Systems Management Server
  - ネットワーク管理システム製品
  - Software Update Services

修正プログラム適用時の問題

- 適用漏れ
  - 何を適用できているか分からない
- 適用権限
  - ほとんどがAdministrator権限を要する
- ネットワークトラフィック
  - ゲートウェイやルータが落ちるかも
- 適用による不具合
  - トラブル・メンテナンス速報
    http://www.microsoft.com/japan/support/sokuho/

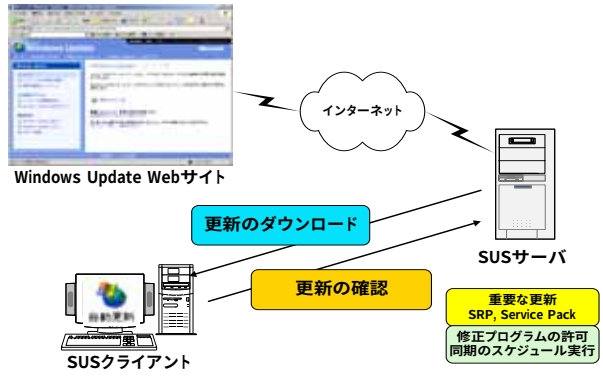
SMSとネットワーク管理システム

- アプリケーションの配布
  - アプリケーション、Service Pack、HotFix
  - 配布対象を細かく指定できる
  - PUSH風（専用クライアントが必要）
- 資産管理（インベントリ）
  - ハード＆ソフトの現状を各種条件で取り出せる
- デメリット
  - SQL Serverが必要など、大がかり

SUS Overview

- 修正プログラムの配布専用
  - HotFix（セキュリティ中心）、Service Pack、SRPのみ
  - インベントリ不可（IISのアクセスログのみ）
  - 配布対象の指定不可
  - PULL風（SP適用で自動的にクライアントがインストールされる）
- システム要件
  - SUSサーバ
    - OS：Windows 2000 Server SP2 / Windows Server 2003
    - IIS、Internet Explorer 5.5以降、NTFSでフォーマット済みのドライブ
    - カスケード可能
  - SUSクライアント
    - OS：Windows 2000 SP2以降 / XP / Windows Server 2003
    - Windows 2000 SP3 / Windows XP SP1でSUSクライアントが自動的にインストールされる
  - ドメインは必須ではない

SUSのシステム構成と基本動作



SUSサーバの構築手順

- 1. IISをインストールする
  - [サーバの役割管理→[役割を追加または削除する]
    →[アプリケーションサーバ (IIS、ASP.NET)]
  - [アプリケーションサーバのオプション]
    - [FrontPageサーバ拡張]
      [ASP.NETの有効化]
- 2. Windowsに修正プログラムを適用する
  - 最低限の修正プログラムはIISのインストール前に適用しておく
- 3. SUSサーバをインストールする
  - ポリシーテンプレートファイルのデグレードに注意！
- 4. オプションを設定する
- 5. コンテンツを同期する
- 6. 適用を許可する
- 7. グループポリシー (ローカルまたはドメイン) を設定する
  - レジストリを編集してもよい

SUSサーバインストールオプション

No.	オプション	デフォルト値
1	SUS Webサイトのファイルを保存するフォルダ	C:\SUS ※NTFSファイルシステムでフォーマットされたドライブの中で、最大の空き容量を持つフォルダ
2	更新の保管場所	更新を次のローカルフォルダに保存する C:\SUS\content\
3	サポートされている言語	利用可能な言語すべて
4	更新の許可の設定	許可された更新の新しいバージョンを自分で手動で許可する
5	ダウンロードURLの指定	http://＜SUSサーバのコンピュータ名＞

グループポリシーの設定

ポリシー名	説明	注意
自動更新を構成する	このポリシーを有効にすると、「自動更新」の機能が利用可能になる。 インストールの実行日時は、「4=自動的にダウンロードし、インストールのスケジュールをたてる」を選択した場合のみ有効になる。	このポリシーを有効にしただけでは、SUSクライアントとしては機能していない。
イントラネットのMicrosoftの更新サービスの場所を指定する	「自動更新を構成する」ポリシーを有効にしたうえで、このポリシーを有効にするとSUSクライアントが機能する。	
自動更新のインストールの予定を変更する	実行されなかった修正プログラムのインストール処理が残っている場合、次回起動時にこのポリシーで指定した時間を経過してから、インストール処理が再開される。	「4=自動的にダウンロードし、インストールのスケジュールをたてる」を選択したときのみ
自動更新のインストールで、システムを自動的に再起動しない	再起動が必要な修正プログラムを適用すると、ログオン中のユーザーのデスクトップにシャットダウンまでのカウントダウンが表示され、残り時間が0になると再起動が行われる。 このポリシーを有効にすると、ログオン中のユーザーが再起動を先送りすることができる。 再起動の権限を持たないユーザーがログオンしている場合は効果なし（先送り不可で強制的に再起動される）。	「4=自動的にダウンロードし、インストールのスケジュールをたてる」を選択したときのみ

SUSのよくある間違い

- 間違い1
  - SUSは修正プログラムを配布する
- 間違い2
  - 修正プログラムは指定時刻に適用される
- 間違い3
  - 修正プログラムの適用には管理者権限が必要
- 間違い4
  - SUSはWindows Updateを置き換える
- 間違い5
  - SUSを使えば運用管理の作業から解放される

SUSクライアントのレジストリ (1)

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU			
値の名前	設定値 (範囲、すべてREG_DWORD型)	デフォルト値	動作
NoAutoUpdate	0:自動更新を有効にする 1:自動更新を無効にする	0 (有効)	自動更新 (SUSクライアント) を無効にする。
AUOptions	1:無効 2:更新をダウンロードする前に通知し、コンピュータにインストールする前に再度通知する 3:更新を自動的にダウンロードして、インストールの準備ができたら通知する 4:更新を自動的にダウンロードして、指定したスケジュールでインストールする	3	自動更新の実行スケジュールを設定する。 4を指定したときのみ、ScheduledInstallDayとScheduledInstallTimeもあわせて設定する。
ScheduledInstallDay	0:毎日、1:日曜、2:月曜…7:土曜	0 (毎日)	スケジュール実行時の曜日を指定する。
ScheduledInstallTime	0～23 (10進数)	3 (午前3時)	スケジュール実行時の時刻を、0:00から23:00の1時間刻みで設定する。
UseWUServer	0:SUSサーバを使用しない 1:SUSサーバを使用する	なし	SUSサーバを使用する。
RescheduleWaitTime	1～60 (単位:分)	なし	自動更新のインストールの予定を変更する。 値を設定しない場合は、「RescheduleWaitTime」そのものを削除する。
NoAutoRebootWithLoggedOnUsers	0:自動再起動を有効にする 1:自動再起動を無効にする	なし	再起動が必要な修正プログラムの適用時にユーザーがログオンしている場合、自動的に再起動しない。

SUSクライアントのレジストリ (2)

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate			
値の名前	設定値 (範囲、すべてREG_SZ型)	デフォルト値	動作
WUServer	http://<SUSサーバのコンピュータ名>	なし	SUSサーバのURLを指定する。
WUStatusServer	http://<統計サーバのコンピュータ名>	なし	SUSの統計情報を収集するサーバのURLを指定する。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update			
値の名前	設定値 (範囲)	デフォルト値	動作
AUOptions	前述	1 (無効)	前述
AUState	0:最初の24時間のタイムアウト待ち (注) 1:自動更新ウィザードの実行待ち 2:自動更新の実行待ち 3:ダウンロード待ち (ユーザーが許可するまで) 4:ダウンロード中 5:インストール待ち (ユーザーが許可するまで) 6:インストール完了 7:無効 8:再起動待ち	7 (無効)	注:自動更新は、コンピュータがインターネットに接続されてから24時間を経過しないと「自動更新ウィザード」を表示しない。
LastWaitTimeout	最終チェック日時	なし	新しい更新がなければ、この時間から22時間～ランダムな時間後に次回のチェックを実行する。
DetectionStartTime	チェック開始日時	なし	今回のチェック開始時刻。

ログのフィールド情報 (1)

フィールド	値の意味	
&U=<Ping ID>	SUSクライアントを識別する固有IDで、SUSクライアントの参照数を把握できる。	
&C=<クライアント>	SUSクライアントの大まかな状態を示す。	
	IU	初期化
	AU	ダウンロードと実行
	IU_Site	Windows Update Webサイトへの接続
&A=<アクティビティ>	処理内容として、以下のアルファベットのいずれかが記録される。	
	N	初期化
	S	セルフアップデート
	D	検出
	W	ダウンロード
	I	インストール
&I=<アイテム>	修正プログラムの識別名があれば記入される。	
&D=<デバイス>	デバイスIDがあれば記入される。	
&P=<プラットフォーム>	OSのバージョン番号、ドメインコントローラの区別、CPUのアーキテクチャが記録される。	
&L=<言語>	言語（日本語：ja-JP、英語：en-US）が記録される。	

ログのフィールド情報 (2)

フィールド	値の意味	
&S=<ステータス>	処理結果として、以下のアルファベットのいずれかが記録される。	
	S	インストール成功
	R	インストール成功（再起動が必要）
	C	ユーザーによる取り消し
	D	ユーザーによるインストール拒否
	F	cやd以外の理由によるインストール失敗
	N	インストール可能な更新モジュールがない
	P	保留中（インストール待ち）
&E=<エラー番号>	Win32エラーステータス番号が、8桁の16進数で記録される。正常終了時は「00000000」。 エラーコードの一覧と詳細は「Microsoft Software Update Services の展開」を参照。	
&M=<メッセージ>	エラーメッセージがあれば記入される。	
&X=<タイムスタンプ>	状態メッセージのタイムスタンプが、「YYMMDDhhmmss+mmm」形式でミリ秒単位まで記録される。	

クライアントアクセスライセンス

- IISの匿名利用に関するCAL
  - SUSサーバがWindows 2000の場合：不要
  - SUSサーバがWindows Server 2003の場合：必要
    - インターネットからのアクセスの場合のみCALは不要
- モードの選択とCALの必要数
  - 同時使用ユーザー数モード
    - 同時にWindows Server 2003に接続するユーザーの数だけ
  - 接続デバイス数
    - SUSクライアント（自動更新）を設定したPCの中で、そのサーバにアクセスする台数分
  - 接続ユーザー数
    - SUSクライアントをインストールしたPCを使う人の数
    - サーバやクライアントに登録されたアカウント数ではない
- 声をあげれば改善されるかも（期待）

資料

- SUSホームページ
  - http://www.microsoft.com/japan/windowsserversystem/sus/
- SUSserver.com
  - http://www.susserver.com/
- eXperts Connection
  - http://www.exconn.net/
- Microsoft Baseline Security Analyzer 日本語版
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=8b7a580d-0c91-45b7-91ba-fc47f7c3d6ad&DisplayLang=ja
- proxy 環境下での自動更新 from セキュリティホールmemo
  - http://damedame.monyo.com/?date=20040303#p02