Windows サーバ運用での
アカウント、セキュリティ管理

Admintech.jp #15

永尾幸夫

2009年01月24日

自己紹介

- こんな人です m(_ _)m
  - 永尾幸夫 (ながお ゆきお：ynagao)
    - 年齢詐称疑惑あり？ (^^;
  - 某 SIer 関西会社に所属。。。でも関東勤務 orz
    - 某お客様システムの保守、運用、監視などなど
      - 以前はグループ内サポート業務に従事。
    - 得意分野はプラットフォーム系
      - いまは UNIX (Linux) 系がメイン。NW 系も見れなくはない。
      - DB 周りは素人同然で、開発は全くダメ orz
      - 以前は Windows 基盤系、Exchange Server, ISA Server を担当
  - IT 系の記事執筆
    - 日経 BP 社など雑誌や、 ITpro, @IT など Web にも寄稿
  - その他、コミュニティ系活動など
    - 神戸セキュメロのスタッフしてます。3 月に京都で (!?)

Agenda

1. Windows Server でのアカウント設計、管理
   - Builtin アカウントの保護
   - ユーザアカウント設定指針
2. Windows Server のセキュリティ強化
   - 不要サービスの停止、無効化
   - セキュリティテンプレートの適用
3. SQL Server 導入でのセキュリティ強化
   - アカウント管理指針
   - 必要サービス、監査の設定

- Appendix
  - PC での起動サービス例、ウィルス対策ソフト動作概要

攻撃への防御

- 多層防御 (Defense-in-depth) で複数の手段を設ける
  - 各レイヤにおける適切なレベルの防御を実装
    - ポリシー：ユーザ向けセキュリティ教育、意識改善
    - 物理セキュリティ：警備員、サーバルーム、施錠、追跡装置、サーバルームの隔離、リムーバブルメディアの無効化、起動時パスワード設定、電源・リセットボタンの保護
    - 境界セキュリティ：ファイアウォール、IDS
    - 内部ネットワーク：ネットワークセグメントの整備、フィルタ (IPsec、Windows ファイアウォール等)、ネットワーク型 IDS
    - ホスト：サーバ・クライアント強化、更新プログラム管理、認証方式、ウィルス対策ソフト、ホスト型 IDS
    - アプリケーション：認証方式、セキュアコーディング、設定での強化、ウィルス対策ソフト
    - データ：アクセス制御リスト (ACL) 、暗号化

1. Windows Server での アカウント設計、管理

1. アカウント設計、管理

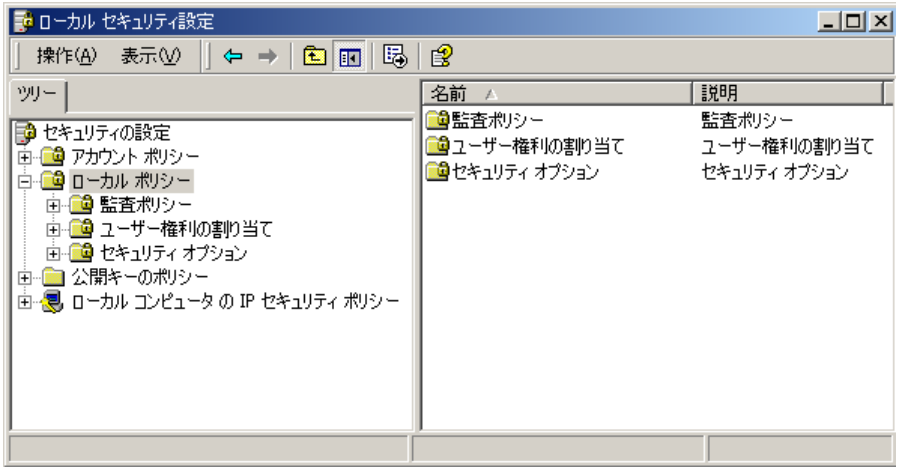
- Builtin アカウントの保護
- ポリシー (アカウント、監査)
- アカウント構成の指針

Builtin アカウントの保護

- Administrator、Guest の名前を変更、無効化
  - おとり用に “Administrator” という一般ユーザを作成
  - Administrator 無効化 (Windows Server 2003 以降で可能)
- ユーザ権利の割り当て (ポリシーでの設定)
  - Builtin アカウント、システムサービスアカウント
    - ネットワークを経由したアクセス、ターミナルサービスでのログオンを禁止
  - Support_388945a0 および Guest
    - Support_388945a0 は Windows XP 以降での Builtin ユーザ
    - バッチジョブでのログオンも禁止
  - サービスの構成
    - ドメインアカウントを使用してログオンさせない
    - “Local System” にも注意！！ (管理者と同等権限でアクセス)

ポリシー (アカウント、監査)

- アカウントポリシー
  - パスワードのポリシー
    - 「パスワードの長さ」「パスワードは要求する複雑さを満たす」など
  - アカウントロックアウト
    - 「アカウントロックアウトのしきい値」など
- 監査ポリシー
  - イベントログ (セキュリティ) へ記録するための設定



アカウント構成の指針

- 基本方針
  - 「必要なユーザに必要な権限 (ロール) を」が鉄則
    - システム特権は安易に付与せず、必要性を考慮
    - 必要に応じて、runas (Secondary Logon を利用) を用いた、別ユーザでの作業を行うことも検討材料に？
  - 登録したユーザと権限は、アカウント管理簿に登録
- ローカルアカウントのみの場合
  - 上記の基本方針を遵守
  - コンピュータだけでなく、各アプリケーションのアカウントも、忘れずに管理対象とする
- ドメインでの管理を行っている場合
  - 権限の有効範囲は、より慎重に決定
  - PC のローカル管理者アカウントとの住み分けも考慮に

2. Windows Server のセキュリティ強化

2. Windows Server の強化

- 不要サービスの停止
- 不要リソースの無効化
- フォルダ・ファイル、レジストリ
- レジストリの監視
- ファイアウォール、フィルタ
  - ファイアウォールの動作
  - サービスに必要なポートの調査
- セキュリティログ収集
- セキュリティテンプレートの設定、適用
- バックアップ (システム)
- バックアップ (データベース)

不要サービスの停止

- サーバの役割に必要なサービス以外はすべて停止
  - 例) Web サーバの運用に最低限必要なサービス
    - Event Log
    - Protected Storage
    - Remote Procedure Call (RPC)
    - World Wide Web Publishing Service
  - Server サービス、Workstation サービス
    - ファイル共有、リモート管理機能のため必要
    - 使用しない場合は、NetBIOS も無効とする
    - SQL Server では、Enterprise Manager での接続で必要となる。
  - DFS (分散ファイルシステム)
  - FRS (ファイル複製サービス)
    - 必要な場合を除き、ファイルサーバでは無効とする

不要リソースの無効化

- 不要プロトコル (NetBIOS) の無効化
  - ファイル共有を必要としない場合、無効化する
    - [NetBIOS over TCP/IP を無効化する]
    - [Microsoft ネットワーク用ファイルとプリンタ共有] の削除
    - NetBIOS over TCP/IP ドライバの削除
  - 無効化の際、イベントログにエラーメッセージが出力されることも
- 不要サブシステムの停止
  - POSIX サブシステムを停止
    - 普通は使わない。
    - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Session Manager¥SubSystems の Optional を 0000 と設定し、POSIX を削除。

フォルダ・ファイル、レジストリ

- NTFS アクセス許可
  - ルートフォルダの設定
    - 既定は「Everyone – 読み取りと実行」、一般ユーザにフォルダの作成許可あり
- レジストリのアクセス許可
  - ローカルアクセスとリモートアクセス
    - ローカルアクセス (既定)
      - 「Administrators - フルコントロール」
      - 「Authenticated Users - 読み取り」
    - リモートアクセス (既定)
      - 「Administrators - フルコントロール」
      - 「Backup Operators - 読み取り」
      - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurePipeServers¥winreg で設定

レジストリの監視

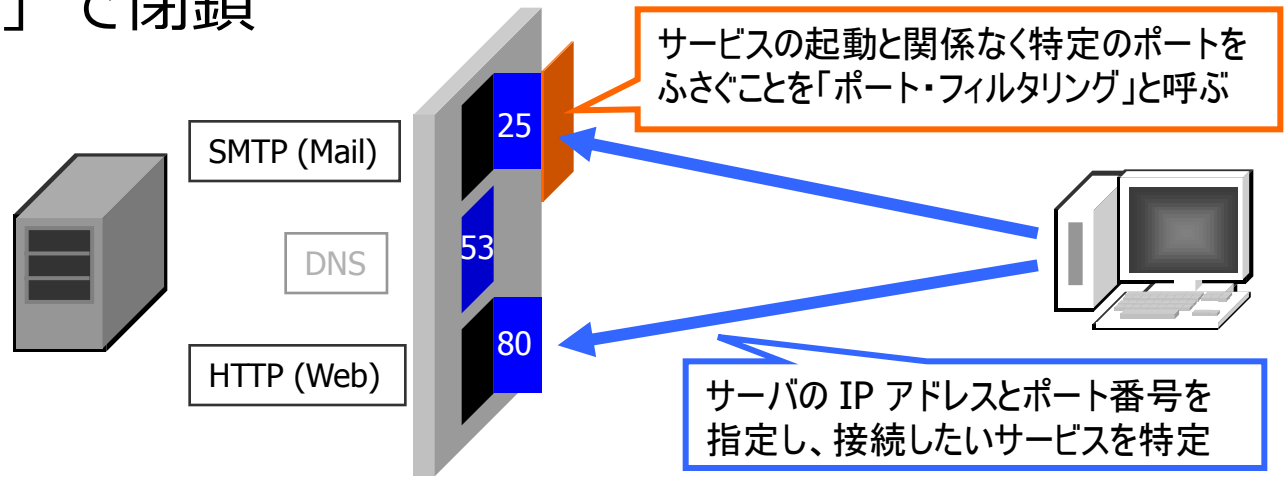
- 「例外パス」と「自動起動」に注意
  - 「例外パス」は匿名でアクセスできるレジストリ
    - HKLM¥SYSTEM¥CCS¥Control¥SecurePipeServers¥winreg¥AllowPath に登録
  - 「自動起動」はユーザログオンのタイミングで起動
    - 以下の順で登録内容が確認される (Windows 2000)
      1. HKLM¥SOFTWARE¥MS¥Windows¥CV¥RunOnce
      2. HKLM¥SOFTWARE¥MS¥Windows¥CV¥Run
      3. HKCS¥SOFTWARE¥MS¥Windows¥CV¥Run
      4. スタートアップフォルダ
      5. HKCS¥SOFTWARE¥MS¥Windows¥CV¥RunOnce
      - HKLM = HKEY_LOCAL_MACHINE (全ユーザに有効)
      - HKCS = HKEY_CURRENT_USER (ログオンユーザに有効)
    - HKLM¥SOFTWARE¥MS¥Windows¥CV¥RunOnceEX もある

ファイアウォール、フィルタ

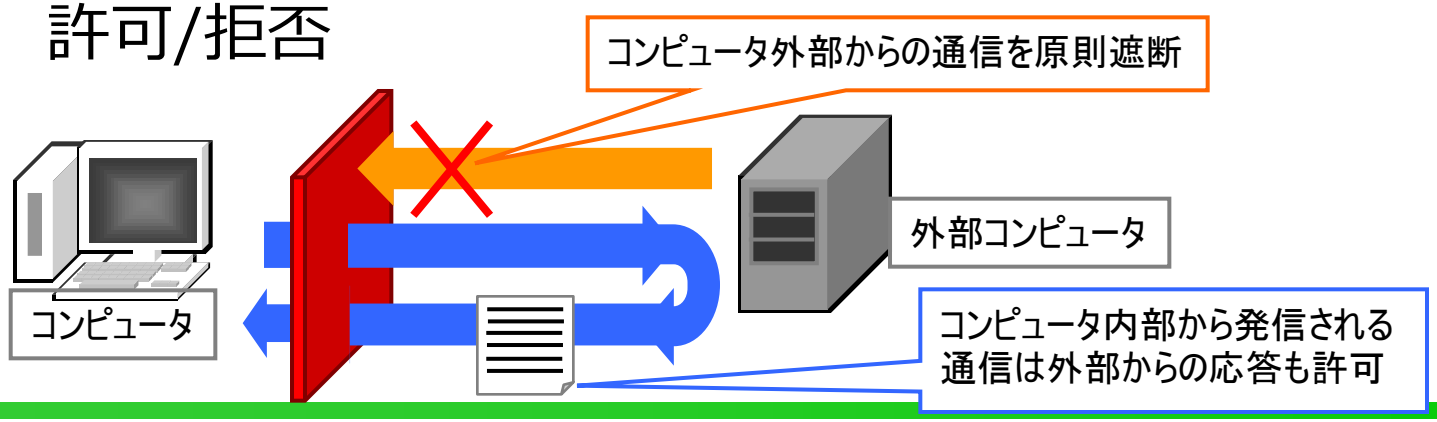
- Windows ファイアフォール
  - Windows XP SP2、Windows Server 2003 SP1 より
    - Windows Server 2003 までは、着信方向フィルタのみ有効
    - Windows Vista や Windows Server 2008 では、発信方向もフィルタの対象
  - GUI の他、netsh (firewall コンテキスト) でも制御可能
- TCP/IP フィルタで着信・発信の制御
  - Routing and Remote Access Service (RRAS)
    - IP アドレス、ポート、プロトコルを基準
  - IP security (IPsec)
    - 「通信のブロック」でフィルタを設定
  - netsh (filter コンテキスト)
    - 例：netsh routing ip add filter ****

ファイアウォールの動作

- 「ポート」単位で通信の許可/拒否を実施
  - サービス受付窓口の「扉」 となる「ポート」を「フィルタ」で閉鎖



  - ステートフル型は、接続方向、プロトコル/ポートで許可/拒否



サービスに必要なポートの調査

- tasklist /svc、netstat –ano の実行結果より確認
  - 例：SQL Server のリモート利用に必要なポートの調査

コマンド プロンプト

```
C:¥>tasklist /svc

イメージ名                     PID サービス
========================= ====== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       388 N/A
csrss.exe                      568 N/A
winlogon.exe                   592 N/A
services.exe                   648 Eventlog, PlugPlay
lsass.exe                      664 Netlogon, PolicyAgent, ProtectedStorage,
                                   SamSs
svchost.exe                    872 DcomLaunch, TermService
svchost.exe                    960 RpcSs
svchost.exe                   1044 AudioSrv, Browser, CryptSvc, Dhcp, dmserver
                                   ERSvc, EventSystem, helpsvc, lanmanserver,
                                   lanmanworkstation, Netman, Nla, Schedule,
                                                                        TrkWks
svchost
svchost                                                                 bClient
spoolsv.exe                    1364 Spoole
inetinfo.exe                   1540 IISADMIN, MSFtpsvc, SMTPSVC, W3SVC
sqlservr.exe                   1572 MSSQLSERVER
alg.exe                         484 ALG
explorer.exe                   1040 N/A
VMwareUser.exe                  740 N/A
ctfmon.exe                     1224 N/A
sqlmangr.exe                   1372 N/A
svchost.exe                    2272 HTTPFilter
conime.exe                     3256 N/A
svchost.exe                    3428 stisvc
mmc.exe                        3696 N/A
cmd.exe                         832 N/A
tasklist.exe                    340 N/A
```

サービス「MSSQLSERVER」はプロセスID 1572 で動作する sqlservr.exe である

コマンド プロンプト

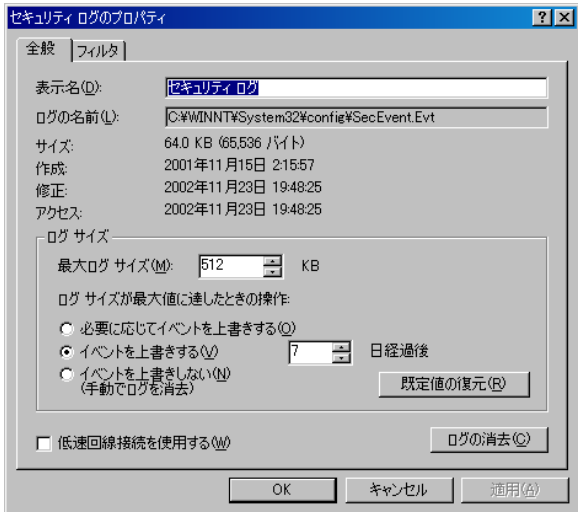
```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       1540
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING       1540
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1540
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       960
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       1540
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING       1540
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       1572
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       1196
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       872
  TCP    127.0.0.1:1033         0.0.0.0:0              LISTENING       484
  TC
  U
  U
  U
  U
  UDP    0.0.0.0:1029           *:*                                    1100
  UDP    0.0.0.0:1030           *:*                                    1100
  UDP    0.0.0.0:1031           *:*                                    1100
  UDP    0.0.0.0:1032           *:*                                    1100
  UDP    0.0.0.0:1434           *:*                                    1572
  UDP    0.0.0.0:3456           *:*                                    1540
  UDP    0.0.0.0:4500           *:*                                    664
```

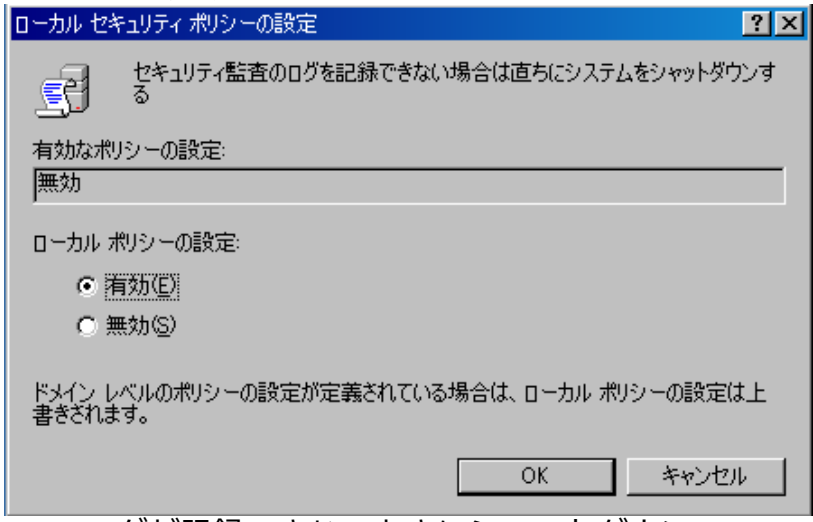
プロセスID 1572 のプログラムが TCP ポート 1433 と UDP ポート 1434 で待ち構えている

セキュリティログ収集

- セキュリティログの有効化 (既定では無効)
  - セキュリティログサイズの設定
    - 最大ログサイズ設定、ログサイズが最大値に達したときの操作
  - セキュリティログが記録できないときの動作
    - ポリシーで設定
- 監査項目の選択
  - 必要な項目のみを監査。ポリシーで設定



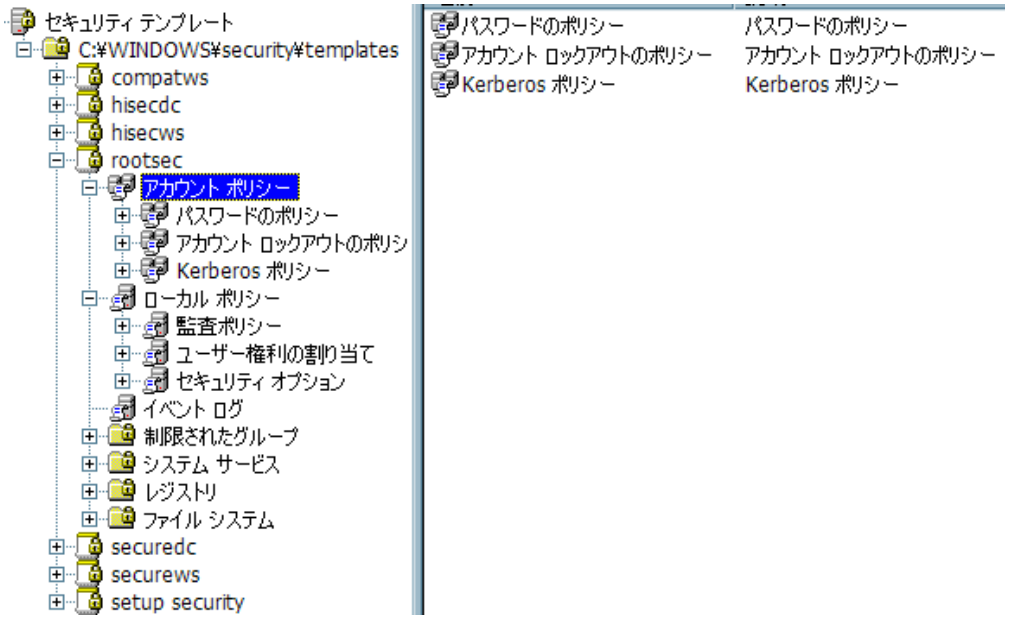
ログサイズ、最大値に達したときの操作



ログが記録できないときにシャットダウン

セキュリティテンプレートの設定

- アカウントポリシー、サービスファイルシステム
  - 用途ごとに、定義済みのテンプレートが用意されている
    - %SystemRoot%¥security¥templates
  - マイクロソフト Web ページからもダウンロード可能
- セキュリティテンプレートのカスタマイズ
  - MMC スナップイン「セキュリティテンプレート」で設定可能



セキュリティテンプレートの適用

- ローカルコンピュータでの設定
  - セキュリティデータベースを作成して設定反映
  - MMC スナップイン「セキュリティの構成と分析」
  - Secedit コマンド
    - secedit /import /db *db-path* /cfg *template-name* で、セキュリティテンプレートからデータベースを作成
      - db-path : c:¥security.sdb など
    - secedit /configure /db *db-path* で設定を反映
- Active Directory のグループポリシー
  - グループポリシーオブジェクトにセキュリティテンプレートをインポートする

バックアップ (システム)

- システムイメージ (ゴールデンイメージ) 取得
  - サーバの運用を開始する前に
    - 構築時のイメージを一旦取得し、障害発生した際の復旧用に
- 運用時のバックアップ取得タイミング
  - Service Pack、修正プログラム適用、パラメータ変更前
- 運用イメージの定期的なバックアップ
- 復元方法の確立は必須
  - 復元環境で新規インストールを行う場合は特に注意
    - Service Pack や修正プログラムのバージョンをバックアップ元環境と合わせる
- 代替機の検討
  - 代替環境構築の時間短縮、リスクの低減

バックアップ (データベース他)

- 業務での利用状況により、取得頻度を決める
  - 「データベースは毎日取得」の場合が多い
  - ファイルサーバでも、作業リカバリに用いることが
- バックアップデータ保存先の検討
  - テープなどのメディア、別サーバのディスク上、など
- バックアップデータ正当性の検証
  - データ復元可否は、システムイメージより重要度が高い
  - 本番環境の取得データを試験環境に復元、のケースも
- 代替機の検討
  - 試験環境を代替機として定義付けることも
- 「バックアップ不要」とは、絶対にならない！！

3. SQL Server 導入でのセキュリティ強化

3. SQL Server での強化

- アカウントの構成
- Windows 側の設定
- 不要なサービスの無効化
- SQL Server の監査
- データベースオブジェクトの保護

アカウントの構成

- sa (システム管理者) には強力なパスワードを使用
  - SQL Server 管理用ロール (グループ) sysadmin メンバ
  - SQL の認証を Windows 認証とした場合でも sa は有効
  - レプリケーション使用では distributor_admin にも注意
- BUILTIN¥Administrators サーバログインを削除
  - 自動的に sysadmin ロールへ追加される
- SQL の Guest アカウントを削除
  - Windows の Guest が有効な場合、自動的に作成される
- public ロールにアクセス許可を割り当てない
  - Windows の Everyone グループ相当
  - public ロールは削除できない

Windows 側の設定

- アカウント構成
  - SQL Server サービスアカウント
    - User グループから削除、強力なパスワードの使用
  - 使用されていない Windows アカウントは無効に
- 認証トラフィックに関する設定
  - NTLMv2 のみを有効にする
- フォルダ、レジストリのアクセス許可
  - SQL Server インストールフォルダなどが対象
  - Everyone にアクセス許可のないよう設定
- 不要リソースの削除
  - ログファイルからパスワードのインスタンスを削除
  - 共有資源や、SDK やリソースキットなどのツールを削除

不要なサービスの無効化

- データベースエンジンのみ必須
  - MSSQLSERVER (必須)
    - データベースエンジンで、稼動に必要
    - 名前付きインスタンスの場合 MSSQL$*InstanceName*
  - SQLSERVERAGENT
    - コマンドのスケジュール実行、エラー発生時の通知
    - 名前付きインスタンスの場合 SQLAgent$*InstanceName*
  - MSSQLServerADHelper
    - Active Directory の統合サービス
    - データベースインスタンスの登録など
  - Microsoft Search
    - 全文検索機能を提供
  - Microsoft DTC
    - 分散トランザクションで使用

SQL Server の監査

- ログイン監査
  - SQL Server Enterprise Manager で設定
  - [監査レベル] を [すべて] または [失敗] に設定
- SQL プロファイラを使用した監査
  - エンドユーザ、管理者のアクティビティ、セキュリティ、ユーティリティ、サーバ、監査イベント
- ストアドプロシージャの設定
  - サーバ起動時に監査を開始する場合に必要
  - 監査スクリプトをストアドプロシージャでラップし、AutoStart を指定

データベースオブジェクトの保護

- サンプルデータベースの削除
  - Pubs、Northwind などを Enterprise Manager で削除
- ストアドプロシージャの保護
  - 認証と権限の設定で、必要なユーザだけに実行許可
- オブジェクトの暗号化
  - ストアドプロシージャ、ユーザー定義関数、トリガ、ビューを暗号化
  - オブジェクト定義 TSQL に「WITH ENCRYPTION」を
- sysadmin ロールへの cmdExec アクセスを制限
  - sysadmin ユーザのみジョブスケジュールを可能に
- ビュー、ストアドプロシージャの使用
  - SQL クエリでの直接アクセスはできるだけ避ける

Appendix

[例] PC の起動サービス (A-P)

OS：Windows XP Professional SP2

“net start” を実行した結果から。
BITS (Background Intelligent Transfer Service) と Windows Installer が、停止しているため、自動更新もままならない状態。。。

Application Layer Gateway Service
Automatic Updates
AVG E-mail Scanner
AVG7 Alert Manager Server
AVG7 Update Service
COM+ Event System
Cryptographic Services
DHCP Client
DNS Client
Error Reporting Service
Event Log
Help and Support
HID Input Service
IPSEC Services
Logical Disk Manager
MGABGEXE
Network Connections
Network Location Awareness (NLA)
Plug and Play
Protected Storage

自動更新 (Automatic Update)

AVG (無料ウィルス対策ソフト) 関連

暗号化の実行

DNS クライアントとしての動作に必要

ネットワーク接続 (マイネットワーク) 関連

秘密鍵などの保護

[例] PC の起動サービス (R-W)

Remote Access Connection Manager
Remote Procedure Call (RPC)
Secondary Logon
Security Accounts Manager
Security Center
Shell Hardware Detection
SSDP Discovery Service
System Event Notification
System Restore Service
Task Scheduler
Telephony
Terminal Services
VMware Authorization Service
VMware DHCP Service
VMware NAT Service
VMware Registration Service
VMware Virtual Mount Manager Extended
Windows Audio
Windows Defender
Windows Firewall/Internet Connection Sharing (ICS)
Windows Management Instrumentation
Windows Time

は、停止してよいと思われるサービス

Dial Up 利用の名残。。。

ユーザアカウント、グループ管理と Runas (他のユーザで実行)

VMware Server 関連

Windows ファイアウォール

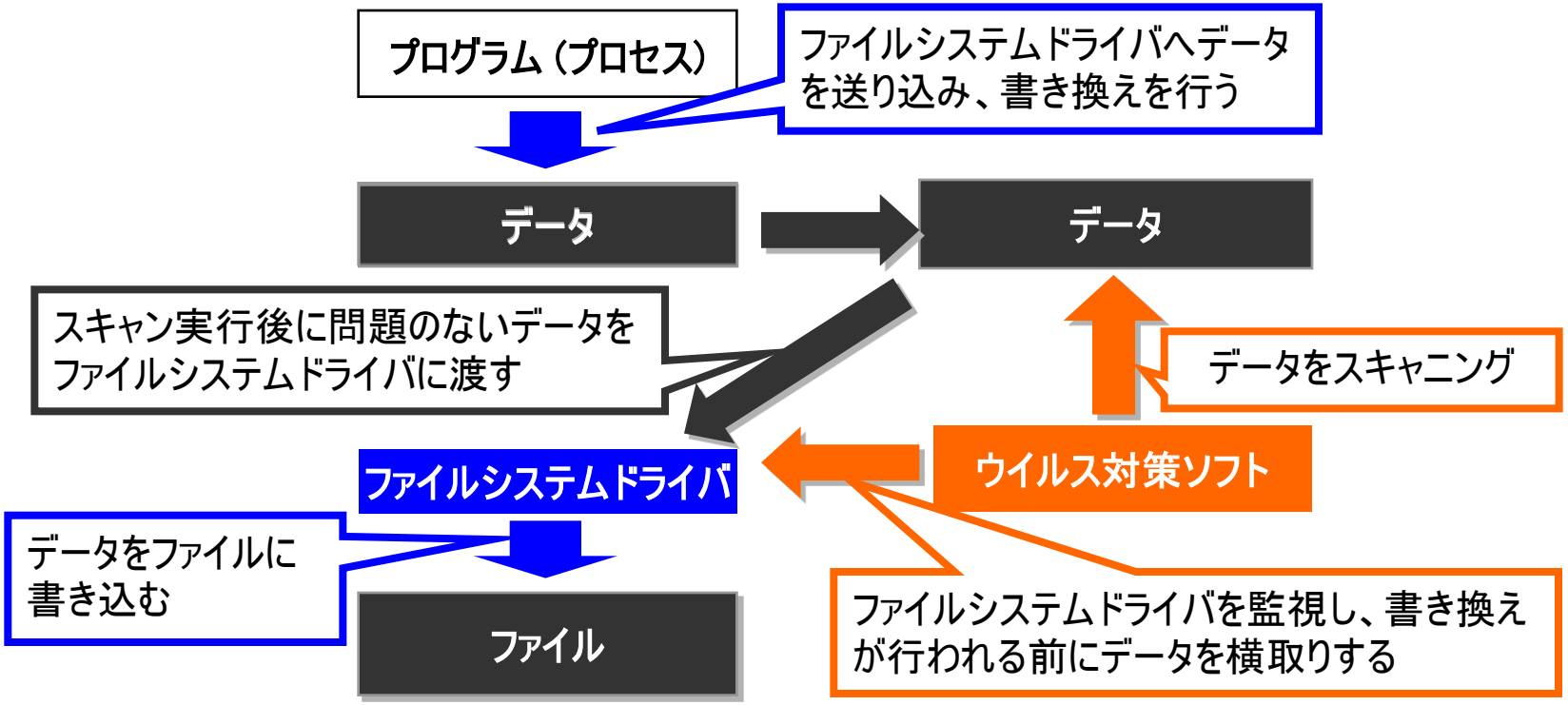
Windows の管理サービス

ウィルス対策ソフトの動作概要

- スキャンによる検知
  - ファイルベースでパターンマッチングを行う
    - マッチングに用いる情報は「ウィルスそのもの」ではない
    - データベース、独自フォーマットデータに対しては効力がない
      - 例：Lotus Notes/Domino, Exchange Server
    - ファイル読み書きに介入するリアルタイムスキャン 検疫と削除
  - 検知されたファイルなどを隔離する
  - 無害化などの処理も実施されることがある
    - 例：ファイル中より検知されたスクリプトコードのみ削除
  - 隔離されたファイルより、削除や復元などの操作を行う
    - 基本的に、自動で削除されることはない
    - 復元は、スパイウェアなどを前提とする

リアルタイムスキャン動作概要

- ファイルシステムドライバの動作を監視
- データの読み書きに介入してスキャンを実施
- データベースの動作などに悪影響
  - 専用のアドオンなどを実装している場合は別

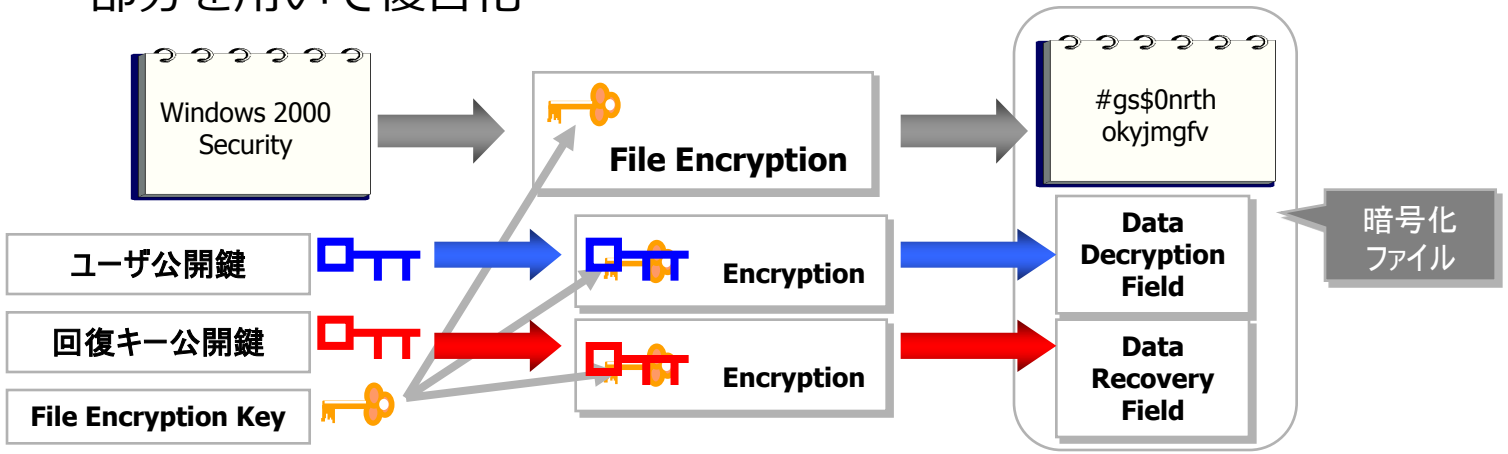


ウィルス対策ソフトの影響

- スキャン動作における問題
  - パターン (定義) ファイルの品質によって、深刻な影響
    - いわゆる「誤検知」の問題
    - 例：定義ファイル適用後に実行されるスキャンでフリーズ状態
  - リアルタイムスキャン動作がもたらす問題
    - ファイル読み書きに遅延が発生することがある
    - アプリケーションによっては、データの不整合と判断する
      - スキャン効果のないソフトウェアで顕在化する傾向
- 検疫および削除のもたらす問題
  - 検知されたファイルの管理
    - 例：「無害化」の過程で必要データが削除されてしまう

ファイル暗号化 (EFS)

- NTFS ボリューム上での EFS 暗号化
  - 公開鍵と複合鍵 (秘密鍵) の組み合わせで実現
    - FEK (File Encryption Key) ファイル暗号化キー
      - ランダムに生成
    - DDF (Data Decryption Field) データ復号化フィールド
      - ユーザ公開鍵で暗号化された FEK を格納。ユーザ秘密鍵を用い復号
    - DRF (Data Recovery Field) データ回復フィールド
      - 回復キー公開鍵部分で暗号化された FEK を格納。回復キー秘密鍵部分を用いて複合化



最後に

- 場当たり的に設定を施すだけでは、セキュリティ対策を施したとはいえない
- 日頃の維持・運用をきちんと継続できるかがカギ
- 運用管理体制を整え、常に情報をウォッチして、必要な対策を検討・実施する必要がある