IPSecの新機能

管理

- IP セキュリティ モニタ
- Netshでのコマンド ライン管理
- ローカル IP の構成のための論理アドレス

セキュリティ

- より強固な暗号マスターキ (Diffie-Hellman)
- コンピュータ起動時セキュリティ
- セキュリティ強化の継続的なポリシー
- 証明書の要求から CA の名前を排除する機能
- 向上した既定の例外処理

相互運用性

- ネットワーク アドレス変換 (NAT) の IPSec 機能
- ネットワーク負荷分散での IPSec 統合の向上

起動時のセキュリティー強化

- IPSec ポリシーが適用される前の通信を保護
  - IPSec 適応前は該当マシンからの outbound トラフィックは許可
  - IPSec 適応前は outbound への応答 inbound トラフィックは許可
  - IPSec 適応前はそれ以外のトラフィックをフィルタ
  - Netsh IPSec コマンドにより設定可能

IPSec の既定の例外ルール

レジストリ値に保存

HKLM¥SYSTEM¥CurrentControlSet¥Services¥IPSEC¥NoDefaultExempt

NoDefaultExempt values	0	1	2	3
Windows Server 2003	• RSVP • IKE • Kerberos • Multicast • Broadcast	• IKE • Multicast • Broadcast	• RSVP • IKE • Kerberos	• IKE
Windows 2000 Server	• RSVP • IKE • Kerberos • Multicast • Broadcast	• IKE • Multicast • Broadcast	X	X

IPSec の NAT への対応

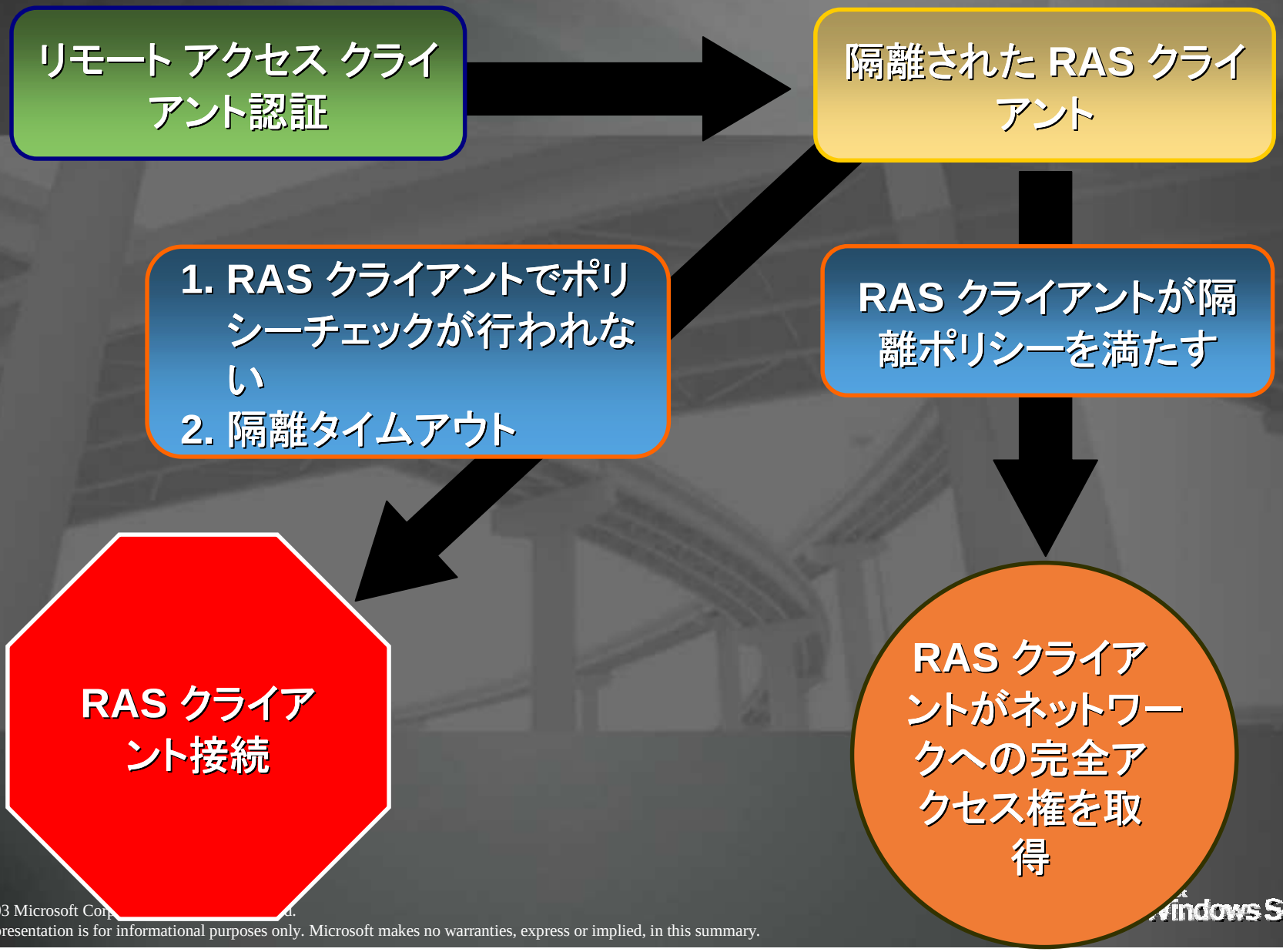
- Windows .NET 2003 での IPSec 実装
  - IPSec NAT Traversal
    - ESP パケットを UDP でカプセル化
    - 受信側、送信側とも IPSec 機器の対応が必要

Windows Server 2003

RRAS のネットワーク アクセス隔離

Windows Server 2003

ネットワーク アクセスの隔離とは?

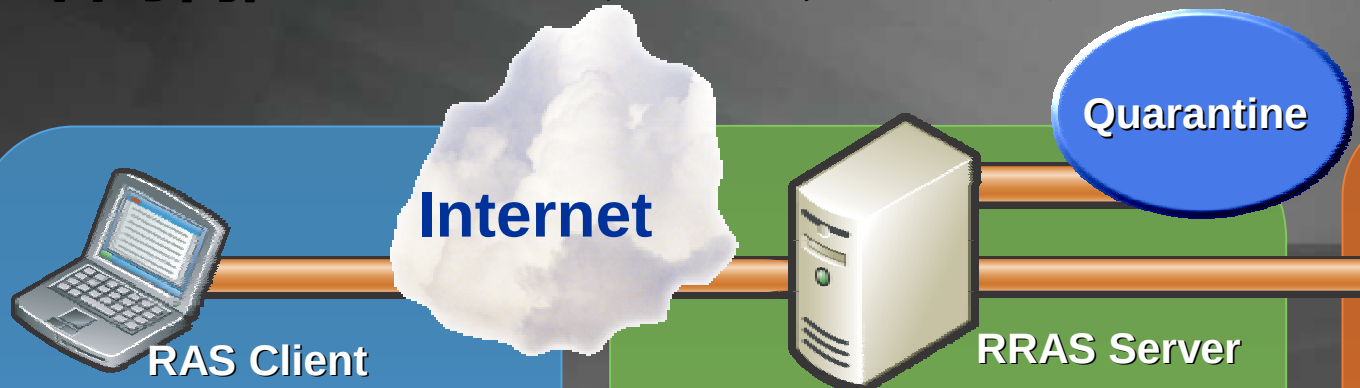


ポリシールールとは?

隔離ポリシールールは、設定が可能で、通常のポリシールールには以下のものが含まれる場合があります

- サービスパックまたは最新の修正プログラムのインストール
- アンチウイルスソフトウェアのインストール
- アンチウイルス署名ファイルのアップデート
- RAS クライアントのルーティングの無効
- インターネット接続ファイアウォールの設定
- パスワード保護のスクリーンセーバーの設定

隔離アーキテクチャ



CM プロファイル
- カスタマイズ可能なポスト接続スクリプト
- スクリプトの”結果文字列”をRQC notifierで送信

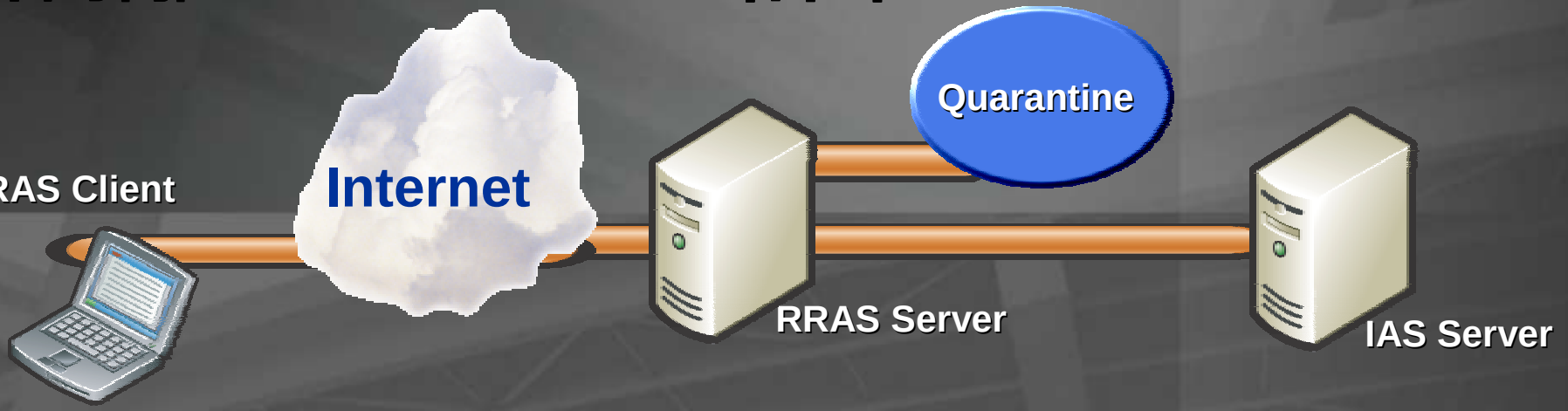
リスナ
- RQS がNotifier の “結果文字列” を受信
- ルールと結果を比較
- 応答が受け取れたが、クライアントが最新でない場合、タイムアウトを解除
- クライアントが最新の状態である場合、隔離フィルタを解除

隔離 VSA
- タイマーが時間ウインドウを制限し、自動切断の前に通知を受け取る
- 隔離フィルタが一時ルート フィルタを設定し、アクセスを制限

RQC.exe および RQS.exeはWindows Server 2003 Resource Kitに含まれています

Windows Server 2003

隔離プロセスの詳細



接続

認証

許可

隔離 VSA および
一般のフィルタ

アクセスの隔離

ポリシー チェックの結果

隔離の停止

フル アクセス

Windows Server 2003

ソフトウェア制限ポリシー

Windows Server 2003

ソフトウェア制限ポリシー

- 2つのモード:無効、無制限
- 実行可能コードの管理
  - .ADE
  - .ADP
  - .BAS
  - .BAT
  - .CHM
  - .CMD
  - .CPL
  - .CRT
  - .EXE
  - .HLP
  - .HTA
  - .INF
  - .INS
  - .ISP
  - .JS
  - .JSE
  - .LNK
  - .MDB
  - .MDE
  - .MSC
  - .MSI
  - .MSP
  - .MST
  - .PCD
  - .PIF
  - .REG
  - .SCR
  - .SCT
  - .SHS
  - .URL
  - .VB
  - .VBE
  - .VBS
  - .WSC
  - .WSF
  - .WSH

SRP が保護されない場合

- ドライバまたはカーネル モードのソフトウェア
  - SYSTEM から保護されない
- SYSTEM アカウントによって実行されるプログラム
  - SYSTEM からは保護されない
- Microsoft Office の文書内のマクロ
  - マクロセキュリティ設定を使用
- 共通言語 ランタイム 用に記述されたプログラム
  - コード アクセス セキュリティを使用

SRP ルールの種類

ハッシュ ルール

- ファイルの MD5 ハッシュまたは SHA1 ハッシュと実行しようとしたファイルを比較
- ファイルの特定のバージョンが実行する許可/禁止する必要がある場合に使用

証明書ルール

- アプリケーション
  例:Authenticode のデジタル署名をチェック
- win32 アプリケーションおよび ActiveX コンテンツの両方を制限する場合に使用

パス ルール

- 実行されるファイルのパスと有効なパスのリストを比較
- 同じアプリケーションで多くのフォルダを使用する場合にこのルールを使用
- SRP の対象が厳密な場合に必要

インターネット ゾーン ルール

- インターネットゾーンにアクセスする方法を制御
- 高度なセキュリティ環境で、Web アプリケーションへのアクセスを管理する際に使用

Microsoft Windows Server 2003

ルールの優先順位

- 複数のルールが設定されている場合
  - Windows Calculatorの実行

c:¥winnt	Unrestricted
A6A44A0E8A76C7B2174DE68C5B0F724D:114688:32771	Disallowed
c:¥winnt¥system32¥calc.exe	Disallowed

- より限定された一致ルールを優先
  1. ハッシュルール
  2. 証明書ルール
  3. パスルール
  4. ゾーンルール

ポリシーの作成方法

- 有効なアプリケーションのリストの作成
  - アプリケーションの起動
  - システム情報を確認 (msinfo32.exe)
    - ソフトウェア環境→ 実行中のタスク
    - ソフトウェア環境→ 読み込み済みのモジュール
    - ソフトウェア環境→スタートアップ プログラム
  - ルールの作成
  - ルールの一般化
    - C:¥winnt → %WINDIR%
    - C:¥app¥dir1, c:¥app¥dir2 → c:¥app

ポリシー作成に関する考慮点

- 以下の点を必ず考慮に入れる
  - 複数の EXE で構成されるものがある
    - Powerpnt.exe
      (クリップアートにより起動する mstore.exe)
  - ログインスクリプト
  - スタートアップフォルダおよびレジストリキー
  - アンチウイルス
  - プログラムアドイン
- 許可しすぎていないか?
- ACL をチェック
  - 特にパスルールを使用する場合

EFS: Encrypting File System

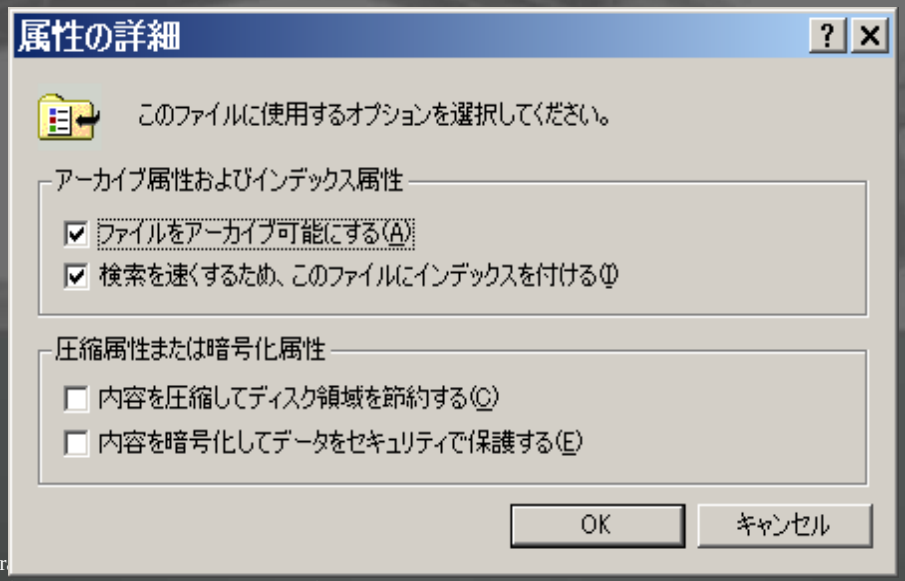
Windows Server 2003

暗号化ファイルシステム
(EFS: Encrypting File System)

- セキュリティ機能の拡張
  - 暗号化をファイルシステムレベルで実装
    - ファイルシステムのアクセス権に加えて、ファイル自身を暗号化することで更に高度なセキュリティを実現
    - NTFS に統合された機能で、ユーザには特別な操作を必要としない
  - デスクトップ及びラップトップでの使用が効果的
    - 記憶媒体が PC本体から外された場合の保護
- ACL (Access Control List) との違いは
  - OS が ACE を用いて管理するセキュリティー制御
  - EFS は削除からファイルを保護はしない

暗号化ファイルシステム
(EFS: Encrypting File System)

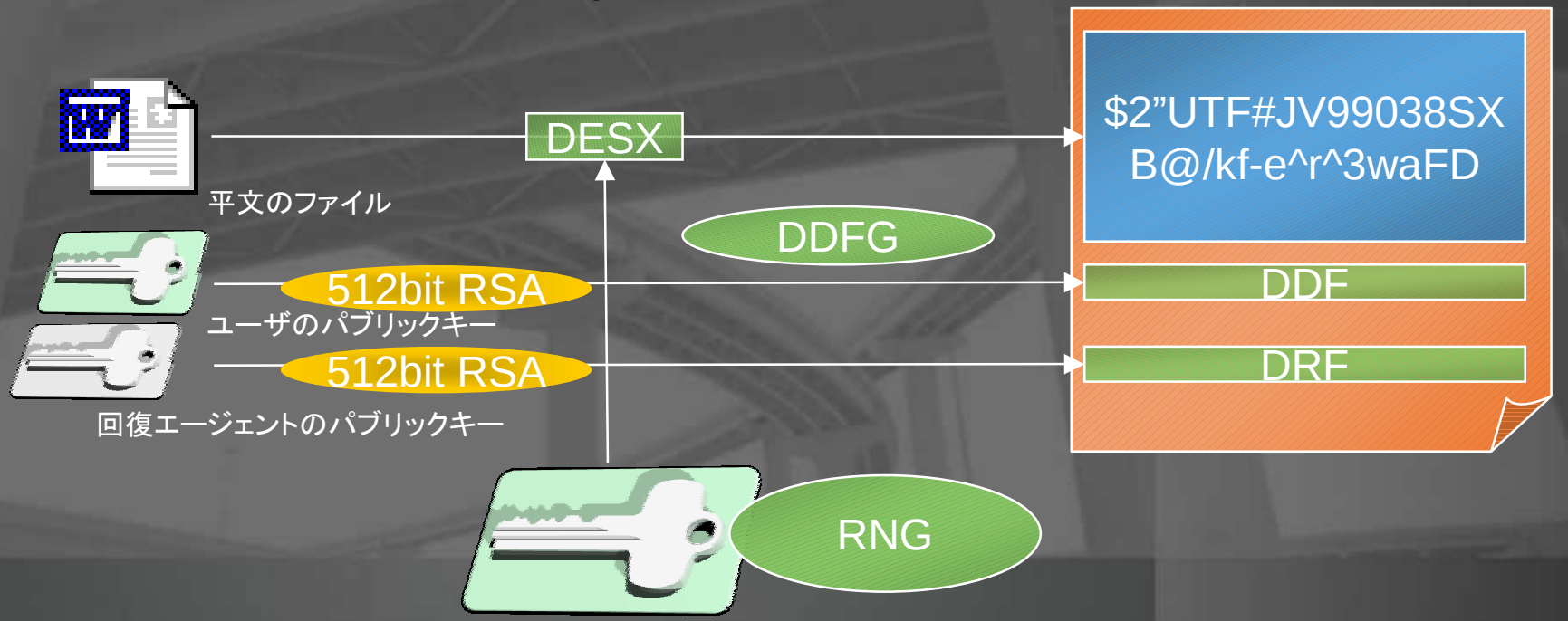
- 暗号化はファイル/フォルダ単位で設定
  - 暗号キー：ドメイン ユーザーごとに実装
  - 回復キー：管理者がパスワードを忘れた場合など、暗号化データを回復できるように生成される
    （*回復キーは、ファイルとしてFDなどに別途保管可能）



Windows Server 2003

EFS のアーキテクチャ

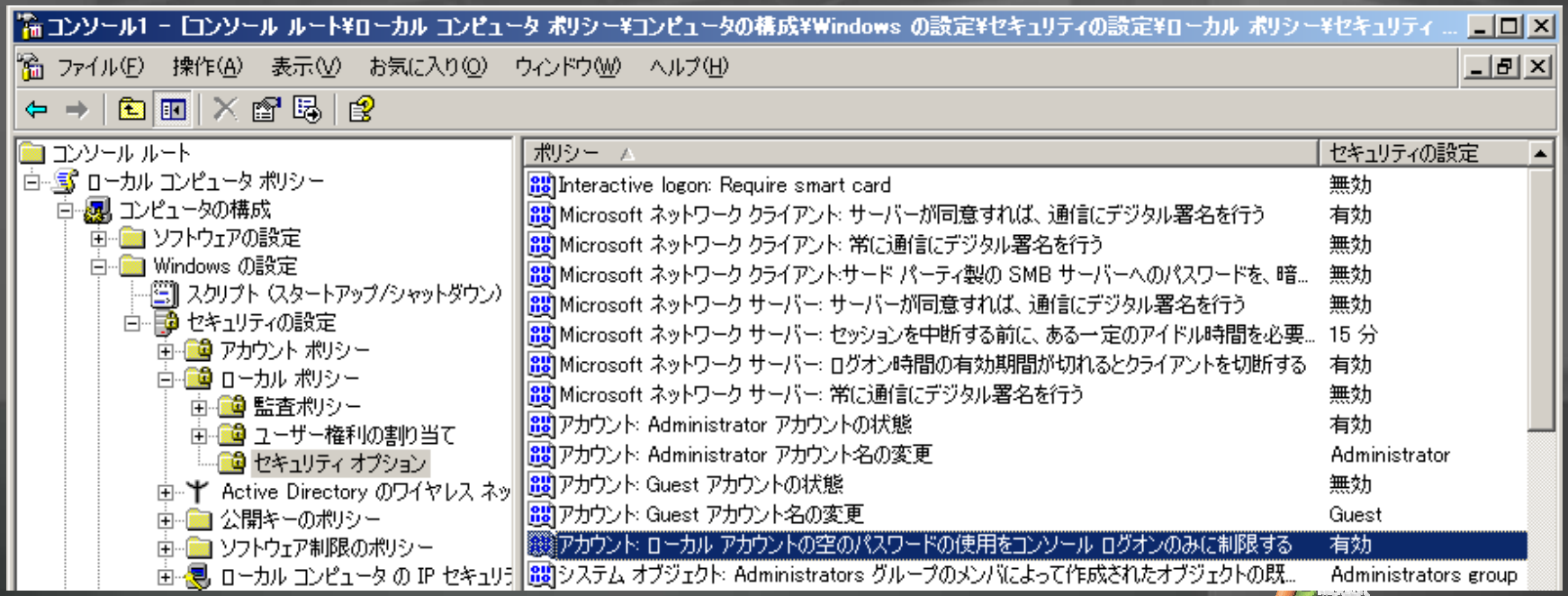
- ファイル暗号化のメカニズム
  - DESX がドキュメント自体の暗号化に用いられる
  - RSA が FEK の暗号化に用いられる



Windows Server 2003

空白パスワードを持つアカウントの使用を制限

- 空白パスワードを持つアカウントを制限
  - ローカルアカウントのみ
  - ドメインアカウントには適用されない
  - DefaultでON



Windows Server 2003

その他の強化ポイント

NoLmHash

- Lan Manager (LM) Hash を保存しない設定が可能
  - セキュリティレベルの向上
  - LM Hash は、下位レベルのOSからの認証やパスワード変更に必要とするもの
  - Windows NT/2000 は NTLM v1/v2 を使用可能
  - 設定方法 :
    - HKLM¥System¥CurrentControlSet¥Control¥Lsa
      Key : NoLmHash を追加
    - Reboot
    - ユーザ全てのパスワード変更を強制する

そのほかの強化ポイント

- DLL の検索優先が作業ディレクトリから ¥windows¥system32 に変更
- AES-256-bit の暗号が EFS で有効
- Everyone グループから匿名ユーザー（anonymous/guest）を除外
- EAP（PEAP) の保護
- 詳細なセキュリティ監査
- アカウントログオン監査が既定で有効
- RRAS 基本ファイアウォール

そのほかの強化ポイント

- IIS 6.0 ロックダウンモード
- IIS 再構築
- 承認マネージャ (AuthMan)
- 資格情報マネージャ (CredMan)
- 強制委任
- .Net Framework 1.1 の
  コードアクセスセキュリティ

そのほかの強化ポイント

- 匿名アクセスが以下の場合にのみに有効となるように制限
  - SAM
  - 名前付きパイプ
  - 共有
- サーバーサービスからリモートレジストリを分離
- IE ロックダウン
- ターミナルサーバーへのアクセス権限の制御
- DPAPI 統合
- *セキュリティ向け*にヘルプ ファイルを大幅に改善