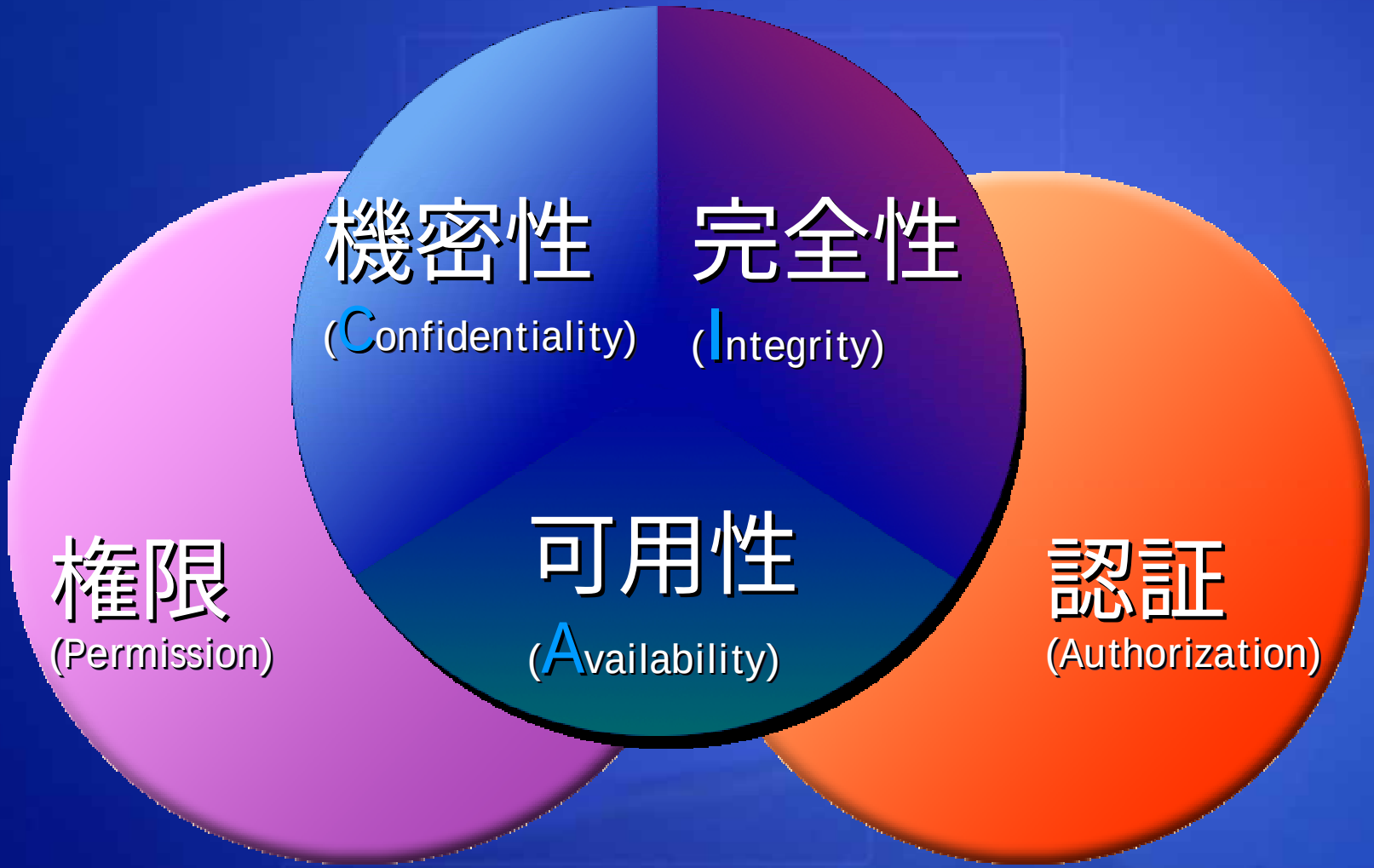
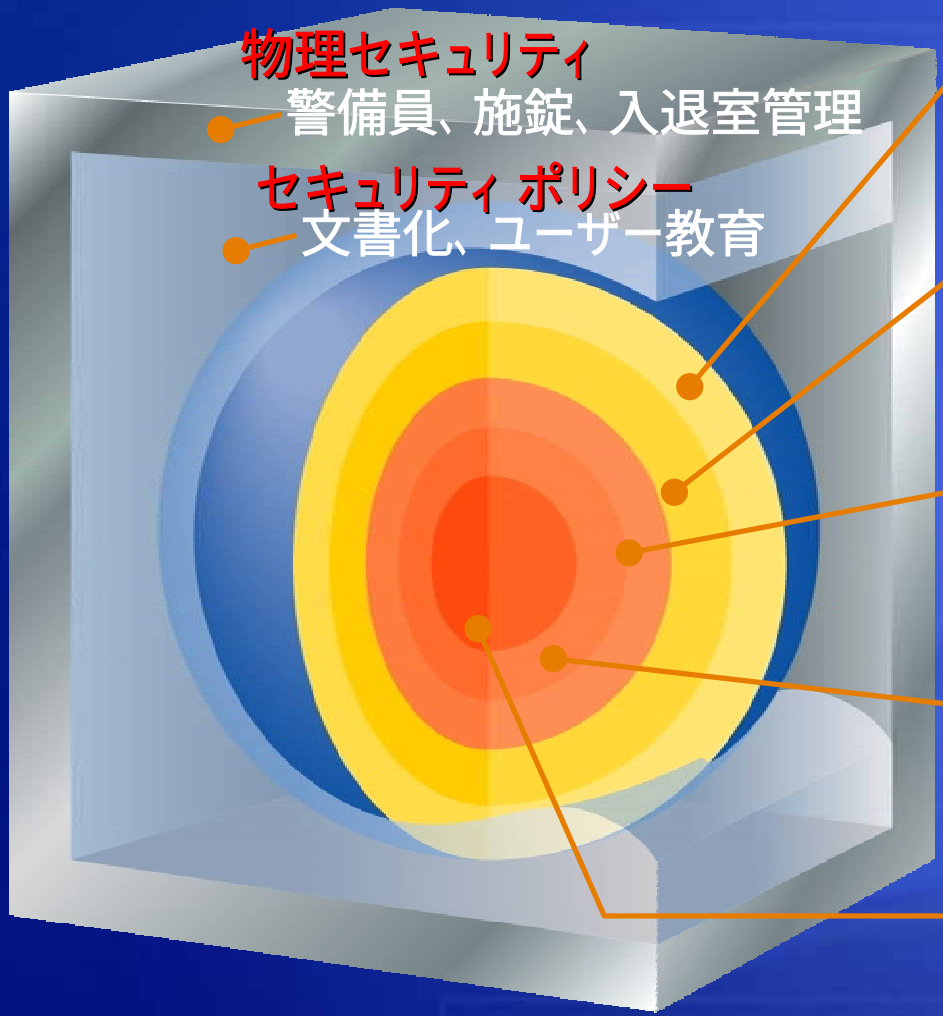
Windows Server のセキュリティ概要

マイクロソフト株式会社
セキュリティレスポンスチーム
小野寺 匠

セキュリティ(安全性)とは



多層防御 (Defense-in-depth)



物理セキュリティ
警備員、施錠、入退室管理

セキュリティ ポリシー
文書化、ユーザー教育

ネットワーク境界部
ファイアウォール、VPN、 侵入検知

内部ネットワーク
ネットワーク ポート、IPSec、
無線LANセキュリティ、検疫

ホスト
OS の設定、更新プログラム管理
ネットワーク認証、侵入検知

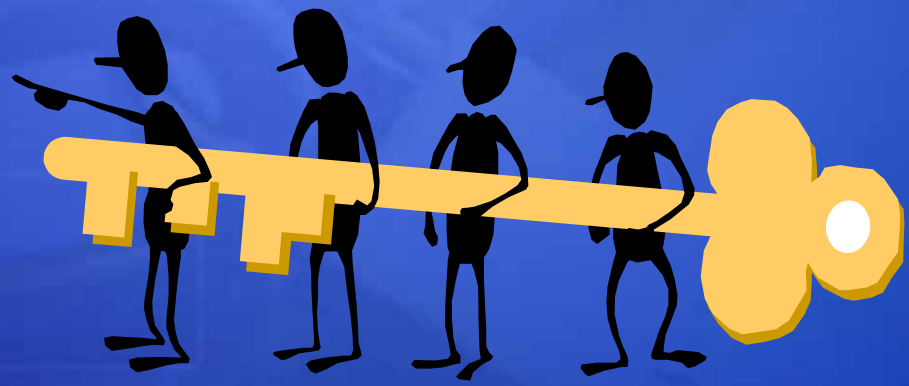
アプリケーション
セキュアなコーディング、
ウイルス対策、ユーザー認証

データ
ACL、暗号化

安全な運用のためのポイント

- 安全なインストール
  - 安全なインストールソース
  - インストール直後の更新の適用
- 安全な構成
  - サービス、機能の適切な設定
  - ネットワークの安全性
- 適切な更新と検査
  - セキュリティ更新の適用
  - 監査と異常の検出

インストールと起動時のセキュリティ



インストール時のセキュリティ

- インストール中は無防備な状態
  - セキュリティ更新が適用されていない
    - 社内のネットワークが「安全」とは限らない
    - ワーム感染、ツールによる攻撃
  - 一切の攻撃の記録が残せない
    - もし、攻撃されても確認できない
  - もし、侵害されれば・・・
    - 以降のセキュリティ対策はすべて無意味
    - バックアップも侵害された状態となる

安全なインストール方法と環境

- インストール方法

インストール方法	信頼性	注意点
正規のCD	高	
スリップストリーム CD	中高	CDの作成者と保管の管理
ネットワーク共有	中	経路の安全性の確保
Remote Install Server (RIS)	中低	専用のネットワークが必要

- ネットワーク
  - クリーンな専用のネットワークが望ましい
    - CD インストールの場合は、切断する
- セキュリティ更新/サービスパックの適用
  - CD/DVD に準備
  - 専用ネットワーク上のファイル共有
  - Microsoft Update (条件付)

ネットワーク上の更新の適用

- Windows Server 2003 SP1
  - セット アップ後のセキュリティ更新
    - Windows Firewall により自動的に着信接続を拒否
    - ファイル共有の利用、Microsoft Update の利用が可能
- Windows Server 2003
  - Internet Connection Firewall を有効に設定
- Windows 2000 Server
  - Firewall 機能は標準ではない
  - TCP/IP フィルタを使用する (お勧めできない)
    - TCP: 一部許可する (80/443)
    - 再起動が必要

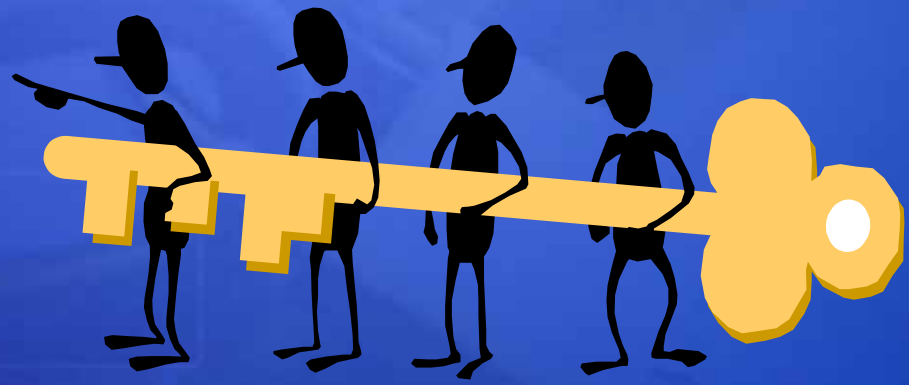
起動時のセキュリティ

- 起動/シャットダウン時の隙間
  - スタックの起動後にファイアウォールが起動
    - ファイアウォールの起動まで数秒～十数秒の隙間
    - その間に攻撃される可能性
  - IPSec も同様
- 対応策
  - Windows Server 2003 SP1
    - 全接続の拒否がスタックのデフォルトルール
    - ファイアウォール起動によりルールを解除
  - Windows Server 2003 以前
    - 実質的な対応策はない
    - 他のネットワーク境界でリスクを緩和させる

起動時の他の注意点

- Network Boot Protocol
  - RIS 等を使用した場合は、 Disable に設定
    - PXE (BootP/DHCP) による起動を禁止する
  - 再起動時に別の PXE を読み込む危険性
- CD/DVD-ROM
  - CD-ROM による別システムの起動
    - ファイルシステムのアクセス権をすべて無視できる
    - CD-ROM からの起動を禁止する
  - 物理的な侵入が前提
- BIOS パスワード
  - 上記設定の保護のためのパスワード

攻撃面を最小化するための構成



安全な構成

- セキュリティの構成ウィザード
  - Windows Server 2003 SP1 の新機能
  - 安全な構成の分析と選択
    - 必要な役割 (roll) 別のサービス選定
    - ネットワークポートの詳細な確認とブロック
    - 認証、署名通信に関するレジストリの調整
    - 監査ポリシーの設定
    - IIS の設定
  - 設定は、XML で保存可能
    - 他の同種サーバーに展開可能
    - GPO による展開、定期的なポリシー検査が可能

サービス最小化の意味

- 攻撃可能なポイントを減らす
  - Firewall等でも同様に可能
- サービスを減らす意味
  - 踏台にされた内部からの攻撃の防御
  - 侵入した不正なソフトの追加の攻撃の防御
  - 更新プログラムの適用数の削減
    - 再起動の抑止
    - 必要な互換性検証作業の抑制
- 停止と無効の違い
  - 停止(手動): 他のサービスの要求により起動可能
  - 無効: 一切の起動要求を拒否

最小サービス

- **必要最小限 = 要塞ホスト**
  - Cryptographic Services
  - DNS Client
  - Event Log
  - IPSEC Policy Agent (IPSec Service)
  - Netlogon
  - Plug and Play
  - Protected Storage
  - Remote Procedure Call (RPC)
  - Security Accounts Manager
  - System Event Notification
  - Windows Management Instrumentation
  - Windows Time
  - Workstation
- **一般的なサーバーには不都合が多すぎる**
  - DMZ **または境界面に配置するサーバー向けの構成**

現実的な最小サービス

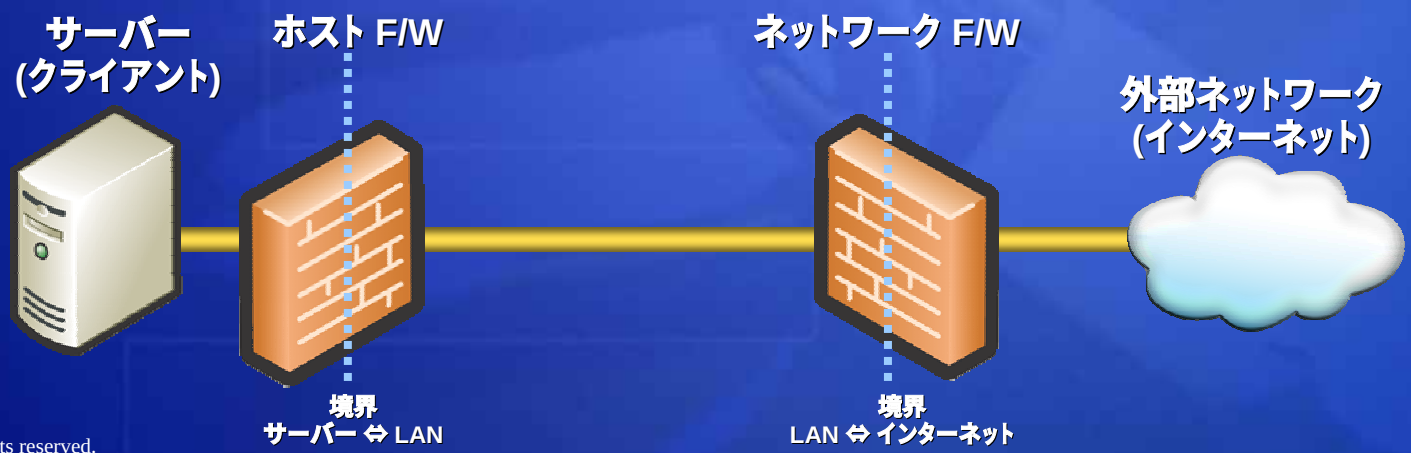
- Automatic Updates
- Computer Browser
- Cryptographic Services
- DHCP Client
- DNS Client
- Event Log
- IPSEC Policy Agent (IPSec Service)
- Netlogon
- NTLM Security Support Provider
- Plug and Play
- Protected Storage
- Remote Procedure Call (RPC)
- Remote Registry Service
- Security Accounts Manager
- Server
- System Event Notification
- TCP/IP NetBIOS Helper Service
- Terminal Services
- Windows Installer
- Windows Management Instrumentation
- Windows Time
- Workstation

サービスの状態の変更

- 互換性に注意
  - サービスの停止による機能不全の可能性
  - 月末、期末のみ動作する機能に注意
- 変更時の注意
  - 変更前のサービスの一覧を保存
    - GPO の保存
    - wmic service list
  - 変更点の記録
    - トラブル時は、速やかに元の設定に戻す
    - GPO の適用を解除

ホストファイアウォール

- ネットワークファイアウォール
  - インターネットからの不正アクセスを防ぐ
  - 社内からのウイルス蔓延には無力
- ホストファイアウォール
  - 各サーバー毎のファイアウォール
  - 社内からの不正アクセスにも対処



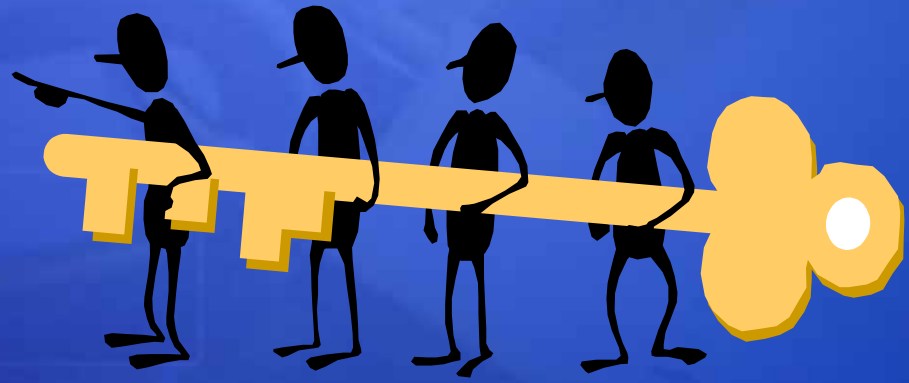
IPSec によるパケット フィルタ

- IPSecとファイアウォールの違い
  - IPSec
    - 認証、暗号化が可能
    - 通信元先の細かな指定が可能
  - ファイアウォール
    - 設定が容易
    - IPSec に比べて高負荷時のスループットが良い
- 適応範囲
  - 高いレベルのセキュリティが要求される場合
  - 開発環境
    - 一般に危険なポートを特定の PC に対してのみ開放

IPSec によるフィルタ例

サービス	プロトコル	送信元ポート	宛先ポート	送信元アドレス	宛先アドレス	操作	ミラー
メンバサーバー共通							
CIFS/SMB	TCP/UDP	任意	445	任意	このコンピュータ	許可	可
RPC	TCP/UDP	任意	135	任意	このコンピュータ	許可	可
NetBIOS	TCP/UDP	任意	137	任意	このコンピュータ	許可	可
	UDP	任意	138	任意	このコンピュータ	許可	可
	TCP	任意	139	任意	このコンピュータ	許可	可
Terminal Service	TCP	任意	3389	任意	このコンピュータ	許可	可
ICMP	ICMP	任意	任意	このコンピュータ	任意	許可	可
(既定の動作)	任意	任意	任意	任意	このコンピュータ	ブロック	可
Active Directory (ドメインコントローラ)							
DNS	TCP/UDP	任意	53	任意	このコンピュータ	許可	可
Global Catalog	TCP	任意	3268	任意	このコンピュータ	許可	可
	TCP	任意	3269	任意	このコンピュータ	許可	可
Kerberos	TCP/UDP	任意	88	任意	このコンピュータ	許可	可
LDAP	TCP/UDP	任意	389	任意	このコンピュータ	許可	可
	TCP/UDP	任意	636	任意	このコンピュータ	許可	可
NTP	TCP/UDP	任意	123	任意	このコンピュータ	許可	可
Static AD Replication	TCP	任意	57952	任意	このコンピュータ	許可	可
DC Comms	任意	任意	任意	このコンピュータ	他の DC	許可	可

攻撃に耐えるための構成



管理者アカウントの保護

- 管理者アカウントの変更
  - Administrator から任意の名前に変更
    - 一般ユーザーと区別がつかないのが理想
  - “Administrator”のアカウントを別途作成
    - 無効でグループに属さないアカウントとして作成
    - ログオンの失敗を監視することで攻撃の兆候がわかる
- 最終ログオンアカウントの表示の禁止
  - 表示されていては、名前を変更した意味が薄れる
  - [対話型ログオン：最後のユーザー名を表示しない]
    - 推奨値: 有効

アカウントの保護 (パスワード)

- 十分な強度のパスワード
  - 長ければ長いほど良い
    - ただし、記憶できる範囲で・・・
  - 多くの文字種を組み合わせが必要
    - アルファベット(大文字、小文字)、数字、記号
- 推奨設定
  - グループポリシー
    - [コンピュータの構成] - [Windowsの設定] - [パスワードポリシー]
    - パスワードの履歴を記録する: 24
    - パスワードの有効期間: 42 日
    - パスワードの変更禁止期間: 2 日
    - パスワードの長さ: 12 文字
    - パスワードは、複雑さの要件を満たす必要がある: 有効
    - 暗号化を元に戻せる状態でパスワードを保存する: 無効

アカウントの保護 (ロックアウト)

- アカウントロックアウトの調整
  - しきい値が小さすぎる
    - ヘルプデスク担当者への負担
    - 故意のロックによる DoS 攻撃
  - しきい値が大きすぎる
    - パスワード推測攻撃を行いやすくする
- 推奨設定
  - グループポリシー
    - [コンピュータの構成] - [Windowsの設定] - [アカウントポリシー]
    - アカウントのロックアウトのしきい値: 10 回
    - ロックアウト期間: 30 分
    - ロックアウト カウンタのリセット: 15 分

認証方式と強度

- Kerberos
  - 現状選択可能な最大強度
  - Windows 2000 以降が対応
- NYLMv2
  - Challenge – Response 方式
    - NTLM に nonce を追加し対タンパ性を強化
- NTLM (NT Hash)
  - LM Hashの 約4×10^{54} 倍の有効なHash空間
  - Challenge – Response 方式
- LM (LanMan) Hash
  - 大文字、小文字を区別しない
  - 使用するには、危険な強度
    - 互換性のためだけに存在

LMCompatibilityLevel

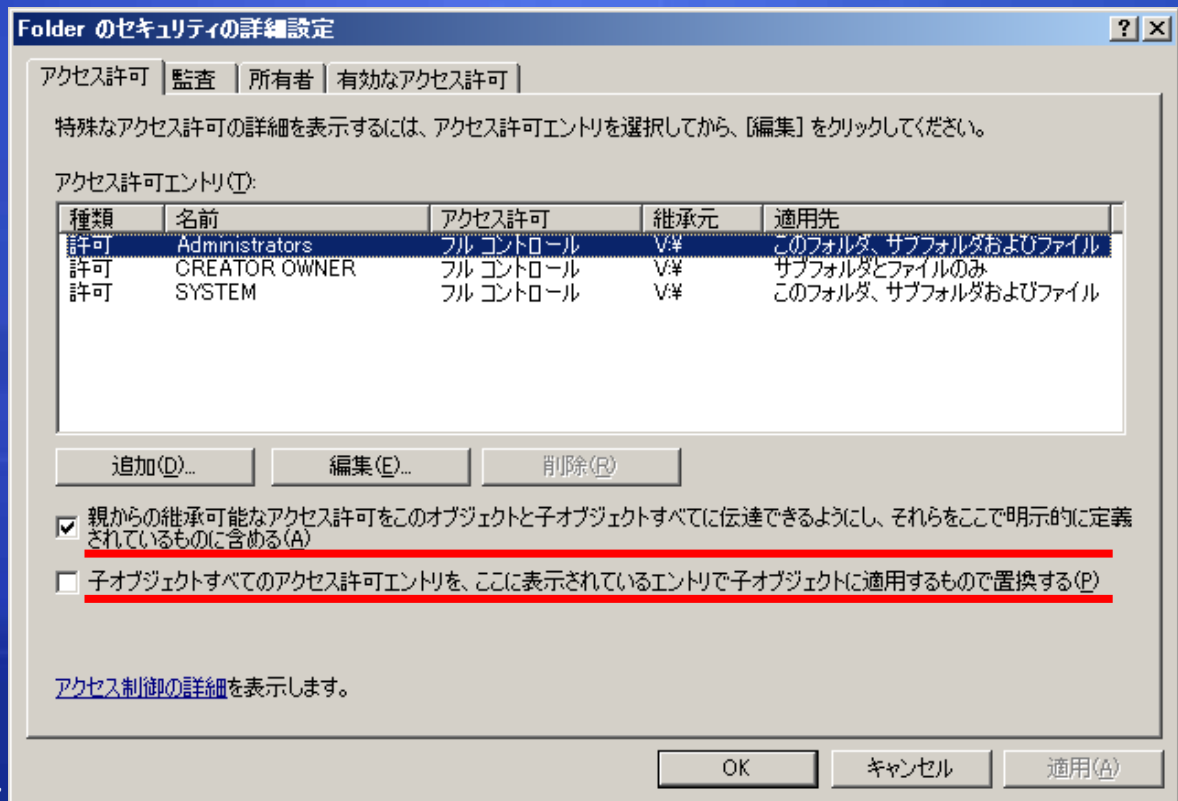
- ネットワークセキュリティ: LAN Manager 認証レベル
  - HKLM¥System¥CurrentControlSet¥control¥LSA¥LMCompatibilityLevel
  - 互換性情報: サポート技術情報 823659, 239869

レベル	送信	受信	備考
0	LM, NTLM,	LM, NTLM, NTLMv2	
1	LM, NTLM, Session security	LM, NTLM, NTLMv2	
2	NTLM, Session security	LM, NTLM, NTLMv2	
3	NTLMv2, Session security	LM, NTLM, NTLMv2	
4	NTLMv2, Session security	NTLM, NTLMv2	「ルーティングとリモートアクセス」を使う場合の推奨値
5 (推奨)	NTLMv2, Session security	NTLMv2	GPO: [NTLMv2 応答のみ送信¥LMとNTLMを拒否する]

- ネットワーク セキュリティ:
  次のパスワードの変更でLAN Managerのハッシュの値を保存しない
  - 推奨値: 無効
  - パスワードデータベース上の LM ハッシュを削除する

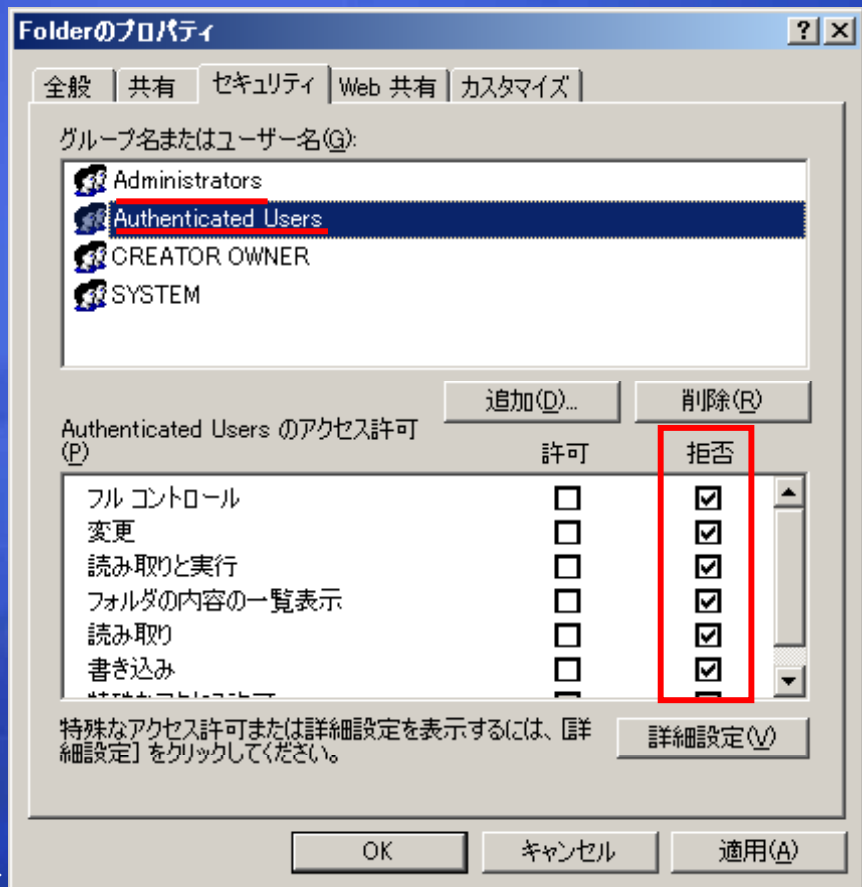
NTFS アクセス権 (継承)

- 継承されるアクセス権
  - アクセス権を深い階層に設定しない
  - 深い階層ほどアクセス権を拡大する
  - ファイルに対して特定のアクセス権を設定しない



NTFS アクセス権 (許可と拒否)

- 許可と拒否
  - アクセス許可: アクセスを許す
  - アクセス拒否: アクセスを拒む
  - 両方を設定した場合は、**拒否が優先される**
    - 不要なアカウントについて積極的に“拒否”を設定する



NTFS アクセス権 (権限)

- 最小限の権限
  - 可能な限り小さなグループに対して設定する
    - ただし、細かくしすぎない
  - 必要な権限のみ与える
    - ただし、特殊なアクセス権を可能な限り用いない
  - Everyone に権限を与えない
    - Authenticated Users を利用する

	一覧	読み取り	書き込み	削除	実行	権限の変更
フォルダ内容の一覧表示	○	–	–	–	–	–
読み取り	○	○	–	–	–	–
書き込み	–	–	○	–	–	–
読み取りと実行	○	○	–	–	○	–
変更	○	○	○	○	○	–
フルコントロール	○	○	○	○	○	○

共有のアクセス権

- ネットワーク経由のアクセス制限
  - NTFS と権限の範囲が違う
  - NTFS で許可していない操作は行えない
    - NTFS アクセス権が優先される
  - フルコントロールは、設定しない
    - ネットワーク経由の権限の変更は推奨されない
  - 用途別に共有することを検討する
    - 読み取り専用: share_RO, 変更可能: share_RW

	一覧	読み取り	書き込み	削除	実行	権限の変更
読み取り	○	○	–	–	○	–
変更	○	○	○	○	○	–
フルコントロール	○	○	○	○	○	○

TCP/IP: DoS 攻撃耐性

キー	推奨値	目的	備考
HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters			
SynAttackProtect	1	SYN Attack	
EnablePMTUDiscovery	0	SYN Attack	
KeepAliveTime	300,000	SYN Attack	(5 分)
TcpMaxConnectResponseRetransmissions	2	SYN Attack	
TcpMaxDataRetransmissions	2	SYN Attack	
TCPMaxPortsExhausted	5	SYN Attack	
EnableICMPRedirect	0	ICMP Attack	
EnableDeadGWDetect	0	SNMP Attack	
DisableIPSourceRouting	2	-	
PerformRouterDiscovery	0	-	
TcpMaxHalfOpen	500	SYN Attack	Windows 2000 のみ
TcpMaxHalfOpenRetried	400	SYN Attack	Windows 2000 のみ
NoNameReleaseOnDemand	1	-	
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥AFD¥Parameters¥			
DynamicBacklogGrowthDelta	10		
EnableDynamicBacklog	1		
MinimumDynamicBacklog	20		
MaximumDynamicBacklog	20,000		

SafeDllSearchMode

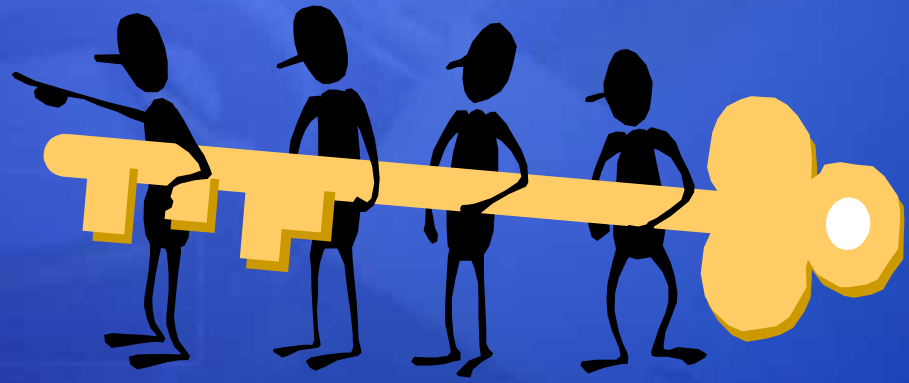
- DLL の検索順序 (Safe DLL Search Mode)
  - Enable:
    - システムパス → プロセスの作業ディレクトリ
  - Disable:
    - プロセスの作業ディレクトリ→システムパス

キー	推奨値
HKLM¥SYSTEM¥CurrentControlSet¥Control¥Session Manager	
SafeDllSearchMode	1

AntiVirus 使用時の注意

- Exchange Server
  - [XADM] Exchange とウイルス対策ソフトウェア
    - http://support.microsoft.com/kb/328841
  - Exchange Server 2003 とウイルス対策ソフトウェアの概要
    - http://support.microsoft.com/kb/823166
- IIS
  - PRB: Antivirus software causes FileSystemObject calls to hang IIS
    - http://support.microsoft.com/kb/295375
  - IIS 6.0: Antivirus Scanning of IIS Compression Directory May Result in 0-Byte File
    - http://support.microsoft.com/kb/817442
  - PRB: Exceptions Occur When You Run ASP.NET Applications and Inoculan Antivirus Software
    - http://support.microsoft.com/kb/309337
- Index Server
  - Backup and Recovery Guidelines for Index Server Catalog
  - http://support.microsoft.com/kb/247093
- File Replication
  - FRS Encounters "ERROR_SHARING_VIOLATION" Errors When It Tries to Replicate Data That Is Still in Use
  - http://support.microsoft.com/KB/822300

安全性を維持するための運用



セキュリティ更新

- 更新の提供サイクル
  - 通常: 毎月第2火曜日の翌日
    - 第2水曜日ではない
  - 緊急: 随時
    - 更新の提供前にワーム化し被害が拡大している場合など
    - 更新の互換性テストとのバランス
- 即時適用の必要性
  - 脆弱性情報の公開後・・・
    - Exploit の公開: 即日
    - ワーム化: 1週未満～数週間

セキュリティ情報の見つけ方

- TechNet Security Center (**無償**)
  - **セキュリティ情報検索**
    - **製品とサービスパックによる絞込み**
    - **包括された更新の除外が可能**
    - http://www.microsoft.com/japan/technet/security/current.aspx
  - **メール配信**
    - **情報の更新も受け取れるサービス**
    - **事前告知、アドバイザリ情報も配信**
    - http://www.microsoft.com/japan/technet/security/bulletin/notify.mspx
  - RSS **配信**
    - **公開したセキュリティ情報の一覧**
- MSN Alert (**無償**)
  - **コンピュータ・アラート**
    - Windows/MSN Messenger **で公開をお知らせ**
    - http://alerts.msn.co.jp/computer/Signup.aspx

適用の時期・期限

- ルールを持つことが大切
  - 一定の検証が可能な期間を設定
  - 危険度の上昇により、緊急適用可能な体制
    - 互換性よりも、侵害のリスクを回避する
    - 危険性情報は、ニュース、アドバイザリを参照
  - 未検証適用もひとつの方法
    - トラブル時はロールバックし、調査

深刻度評価	適用期限		備考
	推奨	最大	
緊急	24 時間	2 週間	
重要	1ヶ月	2ヶ月	
警告	4ヶ月	6ヶ月	期間内の定期メンテナンス時
注意	1 年	適用しない	サービスパック、ロールアップによる適用

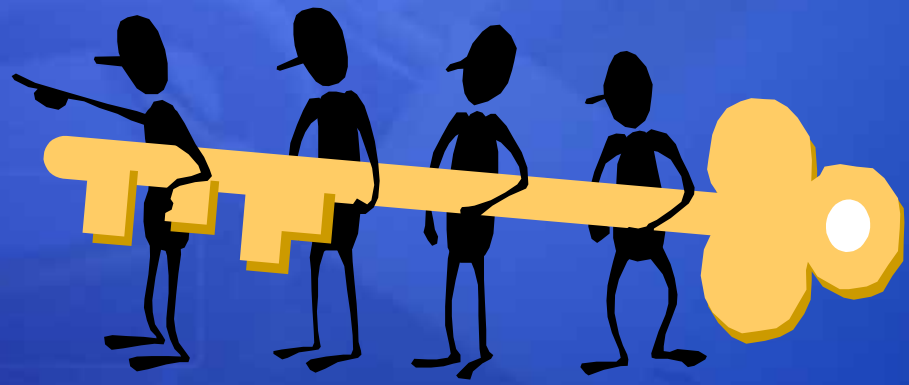
サービス・再起動の削減

- 更新の一括適用
  - xxxxxx.exe /passive /promptrestart
    - バージョンの新旧は自動的に調整
    - qchain の実行は不要
- 適用後再起動の要不要
  - レジストリ UpdateExeVolatile
    - 1 以上は、再起動の保留中
    - 0, 存在しない場合は、再起動不要
    - Reg Query "HKLM¥SOFTWARE¥Microsoft¥Updates¥UpdateExeVolatile" /v Flags
- 運用による削減
  - ロードバランス (NLB)、クラスター

更新の展開方法

- Windows Software Update Service (WSUS)
  - サーバーのグループ化
  - グループ毎の展開する更新の制御 (選択)
  - 展開状況のレポート
- 手動 (スクリプトの利用)
  - ダウンロードセンターから入手した個別の更新
  - 適用手順をスクリプト化
    - TechNet スクリプトセンターにサンプル多数
- 自動更新 (Auto Update)
  - ダウンロードまでは自動を推奨
    - 「更新を自動的にダウンロードするが、インストールは手動で実行する」
  - ダウンロード済み更新の適用を選択可能
- Microsoft Update
  - サーバー毎の手動操作
  - 「カスタム」モードによる適用する更新は選択可能

監査と事故対応



監査の目的

- 監査の目的
  - 操作の記録を残す
    - 事故が起きてから取得はできない
  - 監査記録を分析する
    - 見ないログに意味は無い
- 監査設定の影響
  - 設定により膨大なイベントログが出力される
  - ログを適切に保管する運用負荷が増大する
  - 過剰な監査はパフォーマンスに影響する
- 成功と失敗の違い
  - 成功: 被害の事実
  - 失敗: 攻撃の兆候

主な監査項目

- アカウント監査
  - アカウント ログオン イベントの監査
  - アカウント管理の監査
- システム監査
  - システム イベントの監査
  - ログオン イベントの監査
  - プロセス追跡の監査
  - ポリシーの変更の監査
  - 特権使用の監査
- オブジェクト監査
  - オブジェクト アクセスの監査
  - ディレクトリ サービスの監査

サーバーの監査設定

推奨する監査

	成功	失敗
アカウント ログオン イベントの監査	○	○
アカウント管理の監査	○	○
ディレクトリ サービスのアクセスの監査	○	○
ログオン イベントの監査	○	○
オブジェクト アクセスの監査	○	○
ポリシーの変更の監査	○	○
特権使用の監査		○
システム イベントの監査	○	

イベントログのサイズ

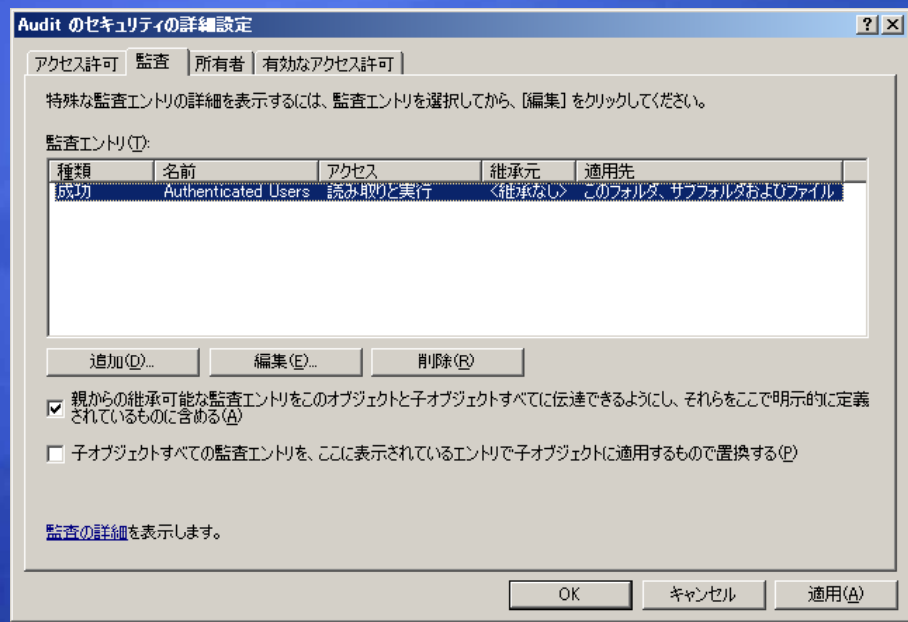
	推奨	最大
アプリケーション ログ	16,384 KB	4 GB
セキュリティ ログ	81,920 KB	4 GB
システム ログ	16,384 KB	4 GB

- オブジェクト アクセス監査をとる場合は、セキュリティログのサイズの拡張を検討

ファイル操作の監視

- 必要な監査
  - オブジェクト アクセスの監査
  - 別途監査設定が必要
    - 監査対象のユーザー (グループ)
    - 監査する操作 (読み取り、書き込み、削除、etc...)
- 確認するべきイベント

イベント ID	内容
560	ファイルへのアクセス
564	ファイルの削除



ログオンの監視

- 必要な監査
  - ログオン イベントの監査
- 確認するべきイベント

イベント ID	内容
529	不明なユーザー名によるログオン パスワード間違え
534	許可されていないログオン方法の使用
539	アカウント ロックアウト

- 注意点
  - 大量の 529 の発生はパスワード推測攻撃
  - 大量の 534 は、広範囲のパスワード推測攻撃
    - まれに社内のアカウント ロック DoS

システムの監視

- 必要な監査
  - システム イベントの監査
- 確認するべきイベント

イベント ID	内容
516	記録できなかったイベントがある
517	イベントが消去された

- 注意点
  - 516 が連続して発生する場合は、ログの消去を狙った不正行為を疑う
  - 517 の記録と運用記録が合わない場合は、管理者権限でシステムが侵害されている可能性がある

効率的なイベントの監視

- 自動化ツールの利用
  - Microsoft Operation Manager (MOM) [有償]
    - イベントログの収集と分析の自動化
    - 異常な傾向があった場合の警告
  - Log Parser [無償]
    - 構造化照会言語 (SQL) に似たクエリを使用した Log の抽出
    - 表計算、RDBMS による分析
    - Syslog サーバーに送信することも可能

インシデントレスポンス

- 復旧と調査は二律背反
  - 復旧 = 調査対象の変更/削除
  - Mirror している場合は、Secondly を調査用に保護
- 再起動前に情報を取得
  - Tasklist /svc
  - Tasklist /v
  - Tasklist /M
  - reg export HKLM c:¥hklm.txt
- 法的な調査
  - 専門企業への依頼を推奨
  - 専門的な知識と、少しだけ特殊な機器が必要
- 原因、再発防止策の簡易調査
  - ディスクイメージツールによるバックアップ
    - イメージを専用のブラウザで参照
  - Virtual PC の利用
    - Link disk をつかった、Virtual 環境での検証、観察

Appendix

- TechNet セキュリティ センター
  - http://www.microsoft.com/japan/technet/security/
- Windows Server 2003 をセキュリティ保護する
  - http://www.microsoft.com/japan/technet/security/guidance/secmod119.mspx
  - Windows Server 2003 ドメイン コントローラのセキュリティを強化する
    - http://www.microsoft.com/japan/technet/security/guidance/secmod120.mspx
  - Windows Server 2003 要塞ホストのセキュリティを強化する
    - http://www.microsoft.com/japan/technet/security/guidance/secmod127.mspx
  - Windows Server 2003 環境のドメイン インフラストラクチャを構成する
    - http://www.microsoft.com/japan/technet/security/guidance/secmod118.mspx
- 脅威とその対策-Windows Server 2003とWindows XPのセキュリティ設定
  - http://www.microsoft.com/japan/technet/security/guidance/secmod48.mspx
- Windows 2000 セキュリティ強化ガイド
  - http://www.microsoft.com/japan/technet/security/prodtech/windows2000/win2khg/01intro.mspx
- Windows 2000 Server セキュリティ運用ガイド
  - http://www.microsoft.com/japan/technet/security/prodtech/windows2000/staysecure/default.mspx

Appendix: Tools

- Microsoft Baseline Security Analyzer (MBSA)
  - http://www.microsoft.com/japan/technet/security/tools/mbsahome.mspx
- Log Parser 2.2 **日本語版**
  - http://www.microsoft.com/japan/technet/scriptcenter/tools/logparser/default.mspx
  - Professor Windows ‐ 2005 **年** 5 **月** - Log Parser 2.2 **の動作方法**
    - http://www.microsoft.com/japan/technet/community/columns/profwin/pw0505.mspx
  - Tales from the Script -**ログこそすべて**
    - http://www.microsoft.com/japan/technet/community/columns/scripts/sg0105.mspx
- TechNet **スクリプト センター**
  - http://www.microsoft.com/japan/technet/scriptcenter/default.mspx
- **中規模企業のためのセキュリティ リスク自己診断ツール**
  - http://www.microsoft.com/japan/technet/security/tools/self-assessment.mspx
- Microsoft Operations Manager 2005
  - http://www.microsoft.com/japan/mom/default.mspx

Appendix: Knowledge Base

- Windows 2000 で TCP/IP フィルタリングを構成する方法
  - http://support.microsoft.com/kb/309798
- セキュリティ設定およびユーザー権利の割り当てを変更すると、クライアント、サービス、およびプログラムとの互換性がなくなる
  - http://support.microsoft.com/kb/823659
- NTLM 2 認証を有効にする方法
  - http://support.microsoft.com/kb/239869
- Microsoft Windows サーバー システムのポート要件
  - http://support.microsoft.com/kb/832017

Microsoft®

Your potential. Our passion.™