Windows環境における セキュリティ強化のポイント

小野寺 匠
GTSC Security Response Team
Microsoft Asia Limited,.

管理者誰もが・・・

- Confidentiality (機密性)
- Integrity (完全性)
- Availability (可用性)

= 信頼できるシステム

を望んでいる

実際には・・・

- 毎月多くのサイトが改竄されている
  - 有名無名は関係ない！
- 個人情報・機密情報が頻繁に漏洩
  - 設定ミス
  - アプリケーションの問題
- 意図せず他のサーバーの攻撃に加担
  - DNS Root ServerへのDDOS Attack
  - SQL Slammer ワーム

しかし・・・

- 自分だけは安全
- パッチを適用したから安全
- ファイアウォールがあるから安全
- ウイルスチェックをしているから安全

という幻想を抱いている

対策を行うために

システムを
よく知る

構成・必要な機能・問題点

脅威と対策
を知る

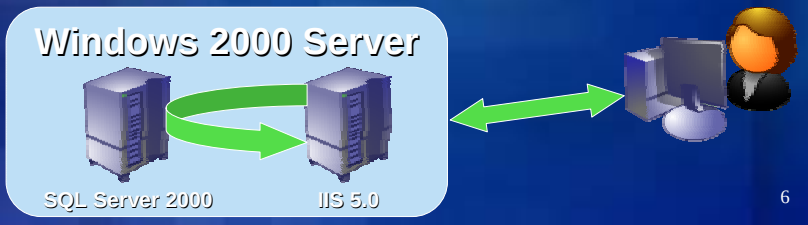
脅威の把握と、対策方法
の把握

対策の確実な実施

信頼できるシステム

想定

- 不特定多数向けサーバー
- 利用する製品
  - Windows 2000 Server
  - Internet Information Services (IIS) 5.0
  - SQL Server 2000



アジェンダ

- **Secure Windows 2000**
- Secure IIS 5.0
- Secure SQL Server 2000

Windows 2000 Server

- **すべての基礎**
  - Server Application**はOSに依存**
- Windows 2000 Server
  ベースライン セキュリティ チェックリスト
  - http://www.microsoft.com/japan/technet/security/tools/chklist/w2ksvrcl.asp

ポイント

- 1 パスワード
- 2 管理者アカウント
- 3 ファイルシステムの安全性
- 4 匿名アクセスを拒否
- 5 最小限のサービス
- 6 不要なファイル共有の削除

パスワード

- すべての基本
  - 多くは、パスワードで保護されている
  - 知っていれば、すべてが行える
  - 安易なパスワードは設定しない
- 最低限
  - 最低 9 文字以上
  - 最初の 7 文字にアルファベット、数字、記号のすべてが含まれる
  - 辞書にある単語は使用しない

管理者アカウント

- アカウント名
  - デフォルトは Administrator
  - すべてのユーザーに知られている
    - 攻撃されやすい
  - わかりにくい名前に
    - 目立たない
    - 他のユーザーと区別のつかない名前
- さらに
  - ロックアウトを有効に

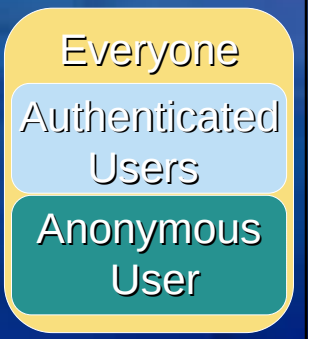
ファイルシステムの安全性

- ポイント
  - すべてのパーティションでNTFSを利用
- なぜ？
  - NTFSには、セキュリティ機能がある

ファイル システム	アクセス制御	暗号化	信頼性
NTFS	◎	◎	◎
FAT/FAT32	×	×	△

ファイルとディレクトリ

- アクセス権は最小限に
- 特定のユーザーは明示的に拒否
  - サービス用アカウント
    - IUSER_, IWAM_, etc…
  - Guest
- 安易に Everyone を使わない
  - Authenticated Usersを利用



適切な ACL を適用する

- Windows 2000 Default
  - http://www.microsoft.com/japan/technet/prodtechnol/windows2000serv/maintain/featusability/secdefs.asp
- Common Criteria
  - http://www.microsoft.com/technet/security/issues/w2kccscg/w2kscgc3.asp
- + MS02-064
  - http://www.microsoft.com/japan/technet/security/bulletin/ms02-064.asp

匿名アクセスを拒否

- 匿名ユーザー (Anonymous User)
  - ＝信頼できないユーザー
  - ＝システムにアクセスする必要がない
- レジストリ
- LSA/SAM
  - 共有の一覧とアクセス権
  - アカウント／グループの一覧

不要なファイル共有の削除

- あらゆる被害の入り口に・・・
  - 情報漏洩
  - ワーム／ウイルスの侵入経路
  - ローカル システムへの入口
- 管理共有
  - Admin$, <drive>$

最小限のサービス

- 必要のないサービスはすべて無効に
  - 停止では不十分 (無効と停止は違う)
- 何が必要で何が不要か？
  - Case By Case
  - サービスの意味を知る必要がある

必要なサービス

- Event Log
- Logical Disk Manager
- Network Connections
- Plug and Play
- Protected Storage
- Remote Procedure Call
- Security Account Manager
- Windows Management Instrumentation
- Windows Management Instrumentation Driver Extensions

アジェンダ

- Secure Windows 2000
- **Secure IIS 5.0**
- Secure SQL Server 2000

IISのセキュリティ

- 1 IISのアクセス権
- 2 不要な機能の停止
- 3 Lockdown/URLScan
- 4 Web Application
  - XSS
  - Cookie
- 5 ログの記録

IIS のアクセス権

- 2段階のアクセス制御
  - IIS
  - OS (NTFS)

IIS のアクセス権 (IIS)

- 通常は・・・
  - “読み取り”のアクセス権のみ必要
- スクリプトは・・・
  - 実行アクセス権を”スクリプトのみ”に設定
- CGIは・・・
  - 他のコンテンツと分離して管理
  - 実行アクセス権を”スクリプトと実行”に設定

IIS のアクセス権 (NTFS)

- NTFS
  - 静的コンテンツ・スクリプト
    - “読み取り”アクセス権のみが必要
  - CGI
    - “読み取りと実行”アクセス権が必要

他のアクセス権は不要！

コンテンツ種別	読み取り	実行	書き込み
静的コンテンツ	必要	不要	不要
スクリプト	必要	不要	不要
CGI	必要	必要	不要

不要な機能の停止/削除

- サンプル アプリケーション
  - IISSamples
  - IISHelp
  - MSADC
  - IISADMPWD
- WebDAV
- スクリプトマッピング
  - .htr (Web ベースのパスワード リセット)
  - .idc (インターネット データベース コネクタ
  - .stm, .shtm, .shtml (サーバー側のインクルード)
  - .printer (インターネット印刷)
  - .htw, .ida, .idq (インデックス サービス)

IIS Lockdown/URLScan

- IIS Lockdown
  - サンプル、不要な機能の削除・無効化
  - ログファイルの保護
  - 匿名ユーザーのアクセス制限
    - システムファイルへのアクセス拒否
- URLScan
  - URLをIISの手前でフィルタ
    - ISAPIフィルタで実現
    - 設定は慎重に行う必要がある

Web Application

- クロスサイトスクリプティング (XSS)
  - サニタイジングが必要
    - Response.HTMLEncode (ASP)
    - 特定文字の削除・エスケープ
  - HTML 生成直前が最適のタイミング
    - 埋め込まれるデータはすべて対象
- Cookie
  - HTTPSのサイトは、secure フラグを利用
  - セッション管理をCookieのみに頼らない
    - セッション・ハイジャックの危険
  - 個人情報・機密情報は扱わない

ログの記録

- ログの記録が必要
  - 不正アクセスの調査に必要
  - W3C 拡張ログ ファイル形式
- 取得項目が重要
  - ユーザー名 [cs-username]
  - メソッド [cs-method]
  - URI Stem [cs-uri-stem]
  - URI クエリ [cs-uri-query]
  - プロトコルの状態 [sc-status]
  - Win32 の状態 [sc-win32-status]
  - ユーザー エージェント [cs (User-Agent)]
  - サーバー IP アドレス [s-ip]
  - サーバー ポート [s-port]

アジェンダ

- Secure Windows 2000
- Secure IIS 5.0
- **Secure SQL Server 2000**

SQL Server 2000

- 1 sa パスワード
- 2 システムSPの制限
- 3 サービス実行アカウント
- 4 SQL Injection

sa パスワード

- sa は、完全な権限 (sysadmin) を持つ
- パスワードは、必ずつける
- SQL 認証 (sa) を使用しないことを推奨
  - Windows統合認証を使用
- ブランク パスワードを狙うワーム
  - SQLSPIDA
  - CBLAD

システムSPの制限

- 非常に強力なシステムSP
  - デフォルトでは、sysadmin ロールが必要
  - public ロールで実行可能なものも
- 明示的に実行権限 (EXEC) を拒否
  - public
    - すべてのユーザー (ロール) に影響
    - sysadmin のみ例外
  - guest
- 拒否はすべての権限に優先

システムSPのデフォルト設定

	SP	sysadmin	public	guest
コマンドシェル	xp_cmdshell	○		
アカウントの操作	sp_addlogin	○	○	
	sp_adduser	○	○	
	sp_addrolemember	○	○	
	sp_addsrvrolemember	○	○	
権限の許可	sp_grantlogin	○	○	
	sp_grantdbaccess	○	○	

サービス実行アカウント

- 強力なアカウントは使用しない
  - Local System, Administrator
- 専用のアカウントの作成
  - 最小限の権限
    - Books Online :
      Windows サービス アカウントの設定
  - 他のリソースへのアクセスを明示的に拒否
    - SQL Serverを経由した攻撃の予防

SQL Injection

- Adhoc クエリ
  - 実行時に別のクエリが混入する可能性

select password from table
where user='mary'

where user='' or user is not NULL or user=''

SQL Injection

- Adhoc クエリ
  - 実行時に別のクエリが混入する可能性
- 外部データーをそのまま挿入しない
  - 文字のエスケープ
  - 禁止文字の検出
- ストアドプロシージャ (SP)
  - 特定の SP のみ実行を許可

まとめ

- 安全な設定が必要
  - デフォルト設定は危険
- パスワード
  - すべての要
  - 破られれば、全てが奪われる
- アクセス権
  - 必要最小限を与える
  - 重要なリソースは、明示的な拒否を利用する

まとめ

- サニタイジング
  - クロスサイトスクリプティング
  - SQL Injection
- Cookieの取り扱い
  - secure フラグ
  - セッション・ハイジャック

まとめ

- 運用が最後の要
  - セキュリティポリシー
  - オペレーターの啓蒙
  - 経営者がそのことを認識すること
- どんなに設定を施しても・・・

人間が一番の脆弱性であり脅威

参考資料 – 共通基準認定

- 概要 : Windows 2000 の Common Criteria (共通基準) 認定
  - http://www.microsoft.com/japan/technet/security/issues/w2kccwp.asp
- Windows 2000 評価された構成 管理者ガイド
  - http://www.microsoft.com/japan/technet/security/issues/w2kccadm/default.asp

参考資料 – チェックリスト

- Windows 2000 Server ベースライン セキュリティ チェックリスト
  - http://www.microsoft.com/japan/technet/security/tools/chklist/w2ksvrcl.asp
- **Windows 2000 Professional ベースライン セキュリティ チェックリスト**
  - http://www.microsoft.com/japan/technet/security/tools/chklist/w2kprocl.asp
- Windows NT 4.0 Server ベースライン セキュリティ チェックリスト
  - http://www.microsoft.com/japan/technet/security/tools/chklist/nt4svrcl.asp
- IIS 5.0 ベースライン セキュリティ チェックリスト
  - http://www.microsoft.com/japan/technet/security/tools/chklist/iis5cl.asp
- Internet Information Services 5 セキュリティ保護チェックリスト
  - http://www.microsoft.com/japan/technet/security/tools/chklist/iis5chk.asp
- IIS 4 ベースライン セキュリティ チェックリスト
  - http://www.microsoft.com/japan/technet/security/tools/chklist/iis4cl.asp

参考資料 – コラム

- セキュリティに関する 10 の鉄則
  - http://www.microsoft.com/japan/technet/columns/security/essays/10imlaws.asp
- セキュリティ管理に関する 10 の鉄則
  - http://www.microsoft.com/japan/technet/columns/security/essays/10salaws.asp
- Microsoft Security Response Center のツアー
  - http://www.microsoft.com/japan/technet/columns/security/essays/sectour.asp
- セキュリティ対応の第 3 の波を目指して
  - http://www.microsoft.com/japan/technet/columns/security/essays/thrdwave.asp
- パッチより Service Pack が優れている理由
  - http://www.microsoft.com/japan/technet/columns/security/essays/srvpatch.asp
- 「セキュリティの脆弱性」の定義
  - http://www.microsoft.com/japan/technet/columns/security/essays/vulnrbl.asp

参考資料 – ベストプラクティス

- 企業セキュリティのベスト プラクティス
  - http://www.microsoft.com/japan/technet/security/bestprac/bpent/bpentsec.asp
- DoS (サービス拒否) 攻撃防止のためのベスト プラクティス
  - http://www.microsoft.com/japan/technet/security/bestprac/dosatack.asp
- 分散サービス拒否攻撃への対処
  - http://www.microsoft.com/japan/technet/security/bestprac/ddosatku.asp
- Windows IIS Web サービスのセキュリティ管理
  - http://www.microsoft.com/japan/technet/security/bestprac/mcswebbp.asp
- Code Red ワームを阻止するための ISA Server の設定方法
  - http://www.microsoft.com/japan/technet/security/bestprac/isacored.asp
- ネットワーク攻撃の認識と対応
  - http://www.microsoft.com/japan/technet/security/bestprac/netdefnd.asp
- Microsoft テクノロジによるモバイル コードの管理
  - http://www.microsoft.com/japan/technet/security/bestprac/mblcode.asp

参考資料 – オペレーションガイド

- Microsoft Exchange 2000 Server
  セキュリティ運用ガイド
  - http://www.microsoft.com/japan/technet/security/prodtech/mailexch/opsguide/default.asp
- Microsoft Windows 2000 Server
  セキュリティ運用ガイド
  - http://www.microsoft.com/japan/technet/security/prodtech/windows/windows2000/staysecure/default.asp

参考資料 - ポリシー

- Microsoft Security Response Center
  セキュリティ情報の深刻度評価システム
  (改訂版 2002 年 11 月)
  - http://www.microsoft.com/japan/technet/security/policy/rating.asp
- **深刻度評価システムについてよく寄せられる質問**
  - http://www.microsoft.com/japan/technet/security/policy/ratefaq.asp
- **マイクロソフト社 Web サイトとお客様のプライバシーに関して**
  - http://www.microsoft.com/japan/info/privacy.htm
- **ソフトウェアの配布に関するマイクロソフトの方針**
  - http://www.microsoft.com/japan/technet/security/policy/swdist.asp