Windows を使用したシステムの運用ポリシーとセキュリティ管理

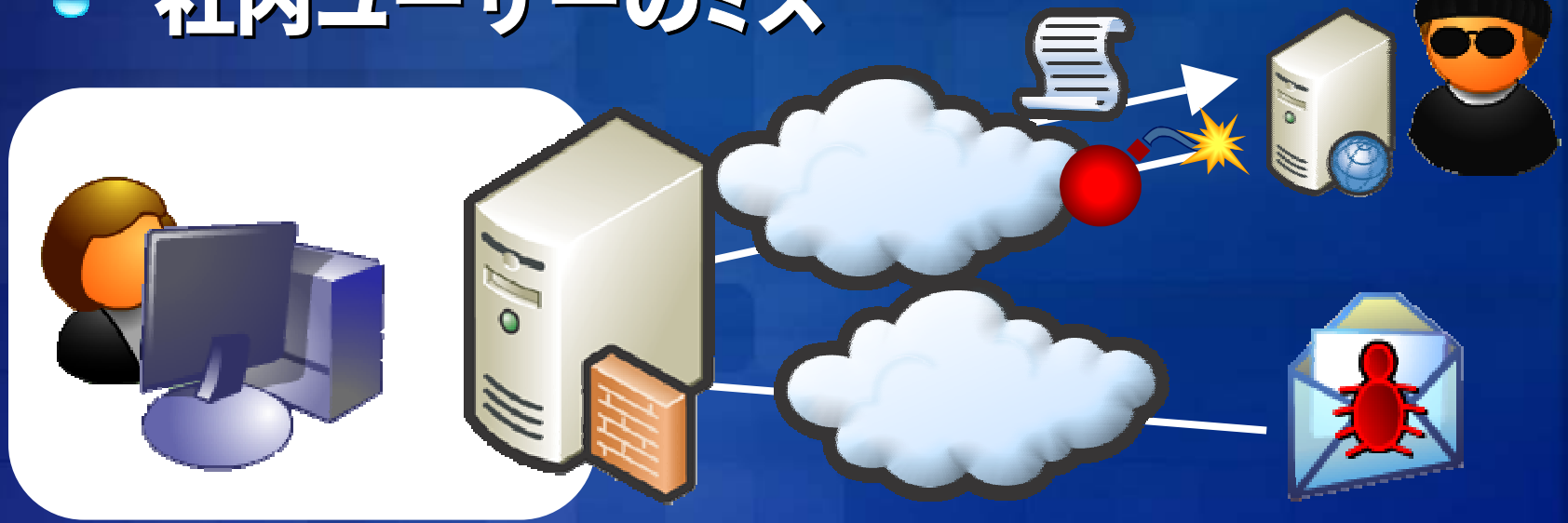
Masaki Yamazaki

GTSC Security Response Team
Microsoft Asia Limited

Client PC を取り巻く環境

- ウイルス、ワーム
- ハッキング行為
- 情報漏えい
- グレーウェア
- 社内ユーザーのミス

巧妙な手口
新しいタイプのウイルス



管理者の抱える問題

- セキュリティへの認識が低く、重要さが理解されない！
- ウイルスメールを開き実行してしまう！
- 外部に社内の情報を流してしまう！
- 不明なプログラムを使用されたくない！
- 脆弱性をそのままシステムに残したくない！
- 修正プログラムを配布するのが大変！
- パスワードがあまりに簡単なものでこまる！

Client PCのセキュリティ対策

運用ルールにより得られる事

- 目的
  - 情報資産を守る
  - 責任範囲の明確化
- 効果
  - 管理者の負担の低減
  - セキュリティ モラルの向上

運用ルールの内訳

- コンピューターの利用ポリシー
- アプリケーションの利用ポリシー
- コンピュータインシデント対策のポリシー
- システム維持のポリシー

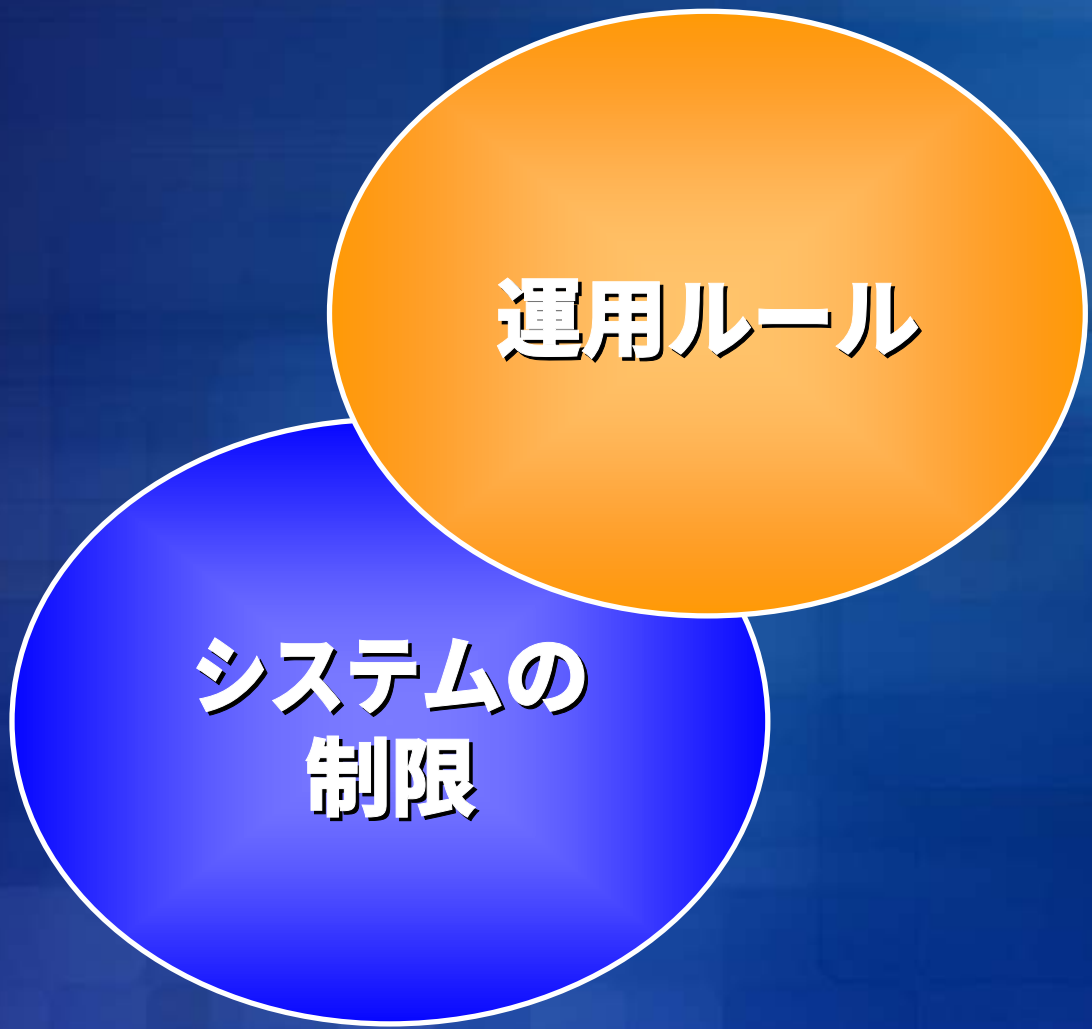
運用ルールに大切な事は

- 社員全員のモラルが最も大切
- なぜなら
  - 人間 (ユーザー) が最も脆弱であり、脅威
  - 技術だけではセキュリティを保てない
- その為にも
  - なぜセキュリティが大切なのか
  - セキュリティの教育が大切

ルールを作るうえでの考慮点

- ユーザーの利便性
  - 厳しすぎるルールはユーザーの反発を招く
  - ユーザーとのコミュニケーション
- なぜ必要なのかユーザーへ説明が大切
- 経営者の同意

Client PCのセキュリティ対策



システムの管理

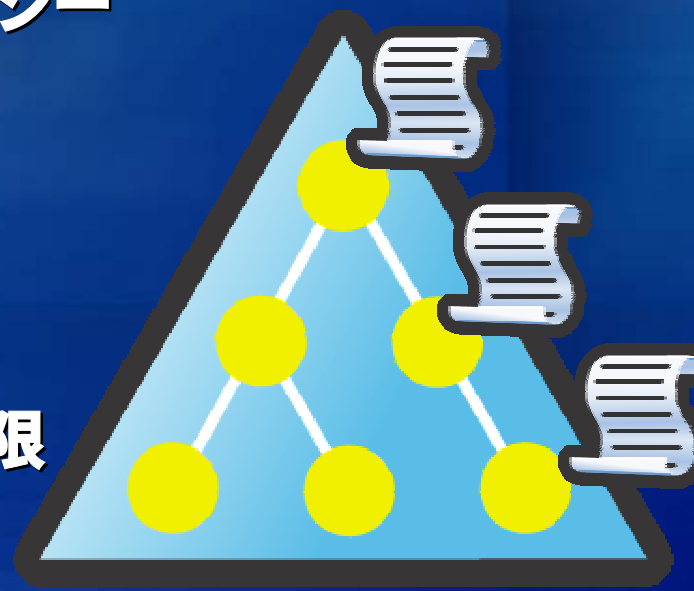
- 目的
  - 確実な対処（人的ミスの防止）
  - 即時対応（情報伝達の省略化）
  - 管理者の負担を低減
- 効果
  - セキュリティ リスクの抑制
  - 責任所在の明確化

システム制限の内訳

- 強度なパスワード
- 適切なアクセス制御
- 最低限の機能
- 各種アプリケーションの管理
  - Internet Explorer の管理
  - Outlook の管理
- 不審なプログラムの実行制限

WindowsならGroup Policyがある!

- 管理の軽減
- コストを抑える
- 多種多様なセキュリティ設定を展開可能
  - セキュリティの設定
    - パスワードのポリシー設定
    - アカウントのロックアウトのポリシー
    - 監査のポリシー
    - ユーザー権利の割り当て
  - 機能の制限
    - サービスの無効化
    - ユーザーインターフェイスの制限
    - プログラムの制限



アプリケーションの実行制限

- メールの添付ファイルを実行しない
  - ウイルスの感染原因 No1
- 不審なプログラムを実行しない
- ソフトウェア制限ポリシーの利用
  - 識別方法は3種類
    - 証明書の規則
    - パスの規則
    - ハッシュの規則
- Windows XP, Windows Server 2003 から実装

Group Policy

demo

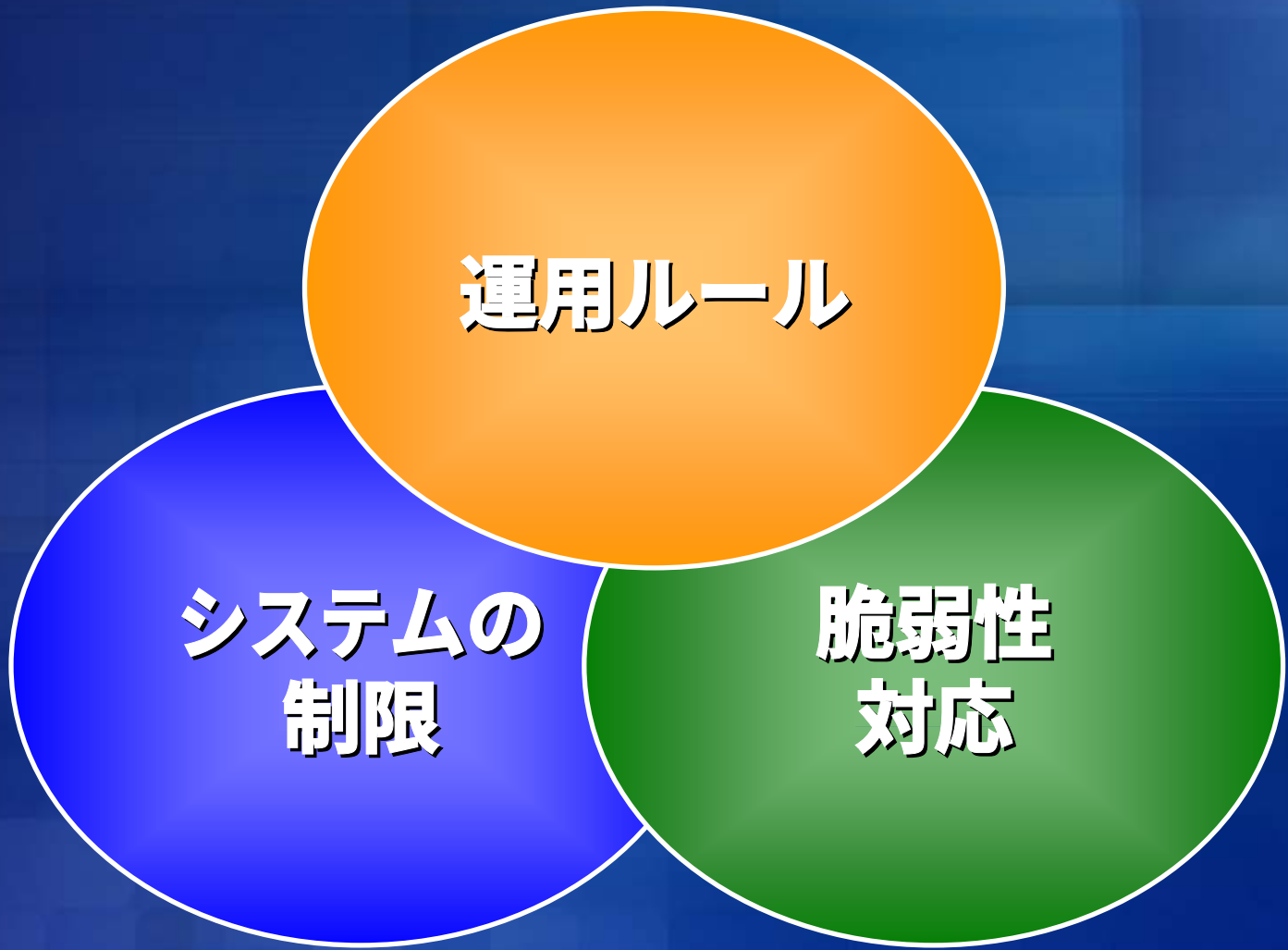
管理を行う上での注意点

- 問題点の見直し
  - 自由に使用できる範囲
- 状況変化への対応
- ユーザーのフィードバック
- 定期的な見直し
  - 問題を改善し、セキュリティ レベルを向上

混在環境でのセキュリティ管理

- 個別の対応が必要
- 可能な限りソフトウェアを統一する
- 古い OS (Windows 98 、NT4.0) は バージョンアップを検討
  - Windows 9x はセキュリティの機能不足
  - サポート期間が残りわずか
    - サポート ライフサイクル
    - http://www.microsoft.com/japan/windows/lifecycle.asp

Client PCのセキュリティ対策



脆弱性対策の必要性

- 一般的なセキュリティ対策では対処不可能
- 脆弱性の存在が社内全体に影響を与えることがある
- 脆弱性の公表が行われた時点で、公知の事実となる
- ほとんどの場合明確な対処方法が存在する

脆弱性対策の具体的な方法

- 脆弱性の対応フローの明確化
- セキュリティ修正プログラムの適用
- 回避策の導入
- IDS や対策ツールにより脆弱性を悪用した攻撃を検出、無効化

修正プログラム展開計画

- 配布方法には様々な方法があり、環境に合わせた手段を選択

	負荷	コスト	Win 9x	制限ユーザー
手動	×	○	○	×
ログオン スクリプト	△	○	○	×
Windows Update	△	○	○	×
Group Policy	○	○	×	○
System Management Server (SMS)	○	△	○	○
Microsoft Software Update Services (SUS)	○	○	×	○

脆弱性の対策の注意点

- 修正プログラムの互換性問題による問題
  - セキュリティ情報の再確認
  - ロールバックプロセスの検討
- 適用漏れの確認
  - Microsoft Baseline Security Analyzer
- 脆弱性の深刻度の把握
  - システムの把握
  - セキュリティ情報の把握

まとめ

- クライアントのセキュリティ対策で重要なのは、利用者全員がセキュリティへの意識を持つことです
- 不必要な機能を制限することにより、リスクとコストを抑えることができます
- 脆弱性は、システムのアキレス腱なので、何らかの対策を行うことが大切です
- 修正プログラムの配布は、システムの共通性が進むにつれ対応し易くなります

Appendix
- システム制限の具体例

- パスワード
- 管理者アカウント
- ファイルシステムの安全性
- 適切なACL
- 不要なファイル共有の削除
- 最小限のサービス
- Internet Explorer の制限

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
  - 知られれば、すべてが行える
  - 安易なパスワードは設定しない
  - メモなどに残さない
- 最低限
  - 長さが 8 文字以上
  - 大文字、小文字、数字、記号を含む
  - 2 ～ 6 番目の位置に、少なくとも 1 つの記号を含む
  - 少なくとも 4 種類の文字を含め繰り返さない

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付かない名前

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	×	×	△

適切な ACL を適用する

- Windows 2000 のアクセス制御のデフォルト設定
  - http://www.microsoft.com/japan/technet/prodtechnol/windows2000serv/maintain/featusability/secdefs.asp
- Common Criteria
  - http://www.microsoft.com/japan/technet/security/issues/w2kccscg/w2kscgc3.asp
- + MS02-064
  - http://www.microsoft.com/japan/technet/security/bulletin/ms02-064.asp

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)
- なに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

- Windows の起動に最低限必要なサービス
  - 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
- 用途や管理に合わせて必要なサービスを追加

Internet Explorer の制限

- 最新のブラウザを利用
- 不必要な機能を制限
  - 受動的攻撃からの防御
- セキュリティゾーンの利用
  - インターネットゾーンの設定を強化
    - Active X：無効
    - Microsoft VM：無効
    - スクリプト関連：無効
  - 安心できるサイトは「信頼済みサイト」に登録

Appendix

- Microsoft Security
  http://www.microsoft.com/japan/security/
- TechNet Security
  http://www.microsoft.com/japan/technet/security/
- セキュリティ 警告サービス 日本語版
  http://www.microsoft.com/japan/technet/security/bulletin/notify.asp
- セキュリティ ツール、チェックリスト
  http://www.microsoft.com/japan/technet/security/tools/tools.asp
- Microsoft Solution for Securing Windows 2000 Server (英語情報)
  http://www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.asp