セキュリティ修正プログラムを効果的に管理するベストプラクティス

山崎雅樹
GTSC Security Response Team
Microsoft Asia Limited

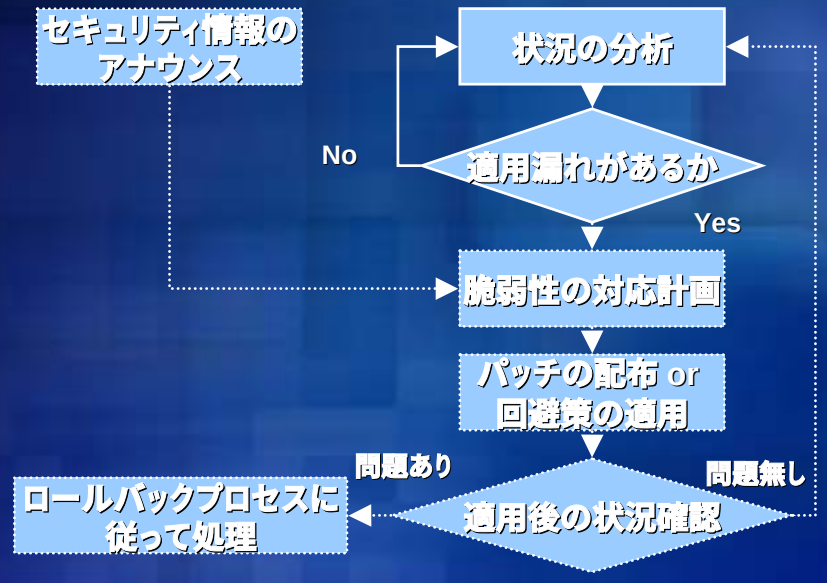
セキュリティ担当者(管理者)の不満

- 制限ユーザで利用している端末への効果的なパッチ配布
- どの修正プログラムが必要か判断できない
- セキュリティ情報の内容が分かりにくい
- パッチ適用に伴う運用管理コストの増大

Agenda

- 適用状況の分析
- セキュリティ情報の確認
- 脆弱性の対応計画
- 修正プログラム配布、状況確認

修正プログラム管理プロセス



修正プログラムの適用状況を分析

準備事項

- 環境の把握
  - OS、サービス、アプリケーション、所有者、etc
  - 資産価値、脅威、脆弱性の把握

- **修正プログラムの適用状況をチェックするツールの利用**
  - **HFNetChk**
  - **Microsoft Baseline Security Analyzer (MBSA)**

HFNetChk

- **ネットワーク上のコンピュータのセキュリティ修正プログラムの適用状況を確認**
- **コマンド ライン ツール**
- **開発元の shavlik のサイトでは、最新のバージョンが入手可能**
  - **マイクロソフトからの HFNetChk の提供は終了する予定**
- **無償**

HFNetChk 管理スクリプト

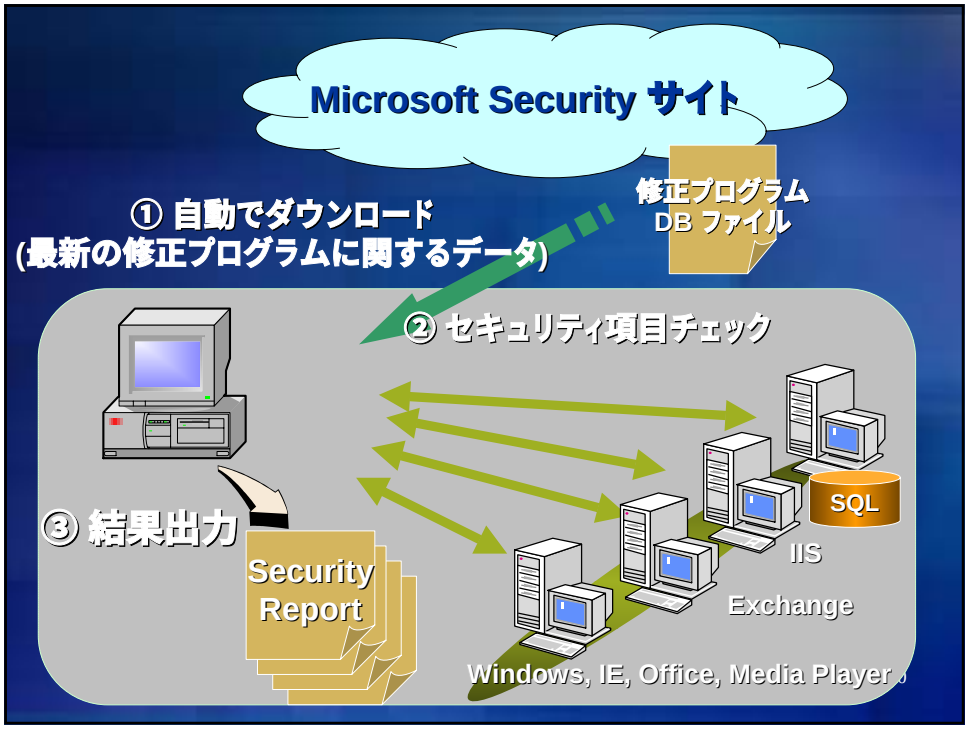
- セキュリティ運用ガイドに HFNetChk 用の管理スクリプトが付属
- 複数のサーバーに対して修正プログラムの適用漏れがないかどうかをチェックし、日付ごとのフォルダに保存される
- 日本語版 XML DB ファイルを利用するためには スクリプトに修正が必要
  - 日本語版 XML DB ファイル
    http://download.microsoft.com/download/xml/security/1.0/NT5/JA/mssecure.cab

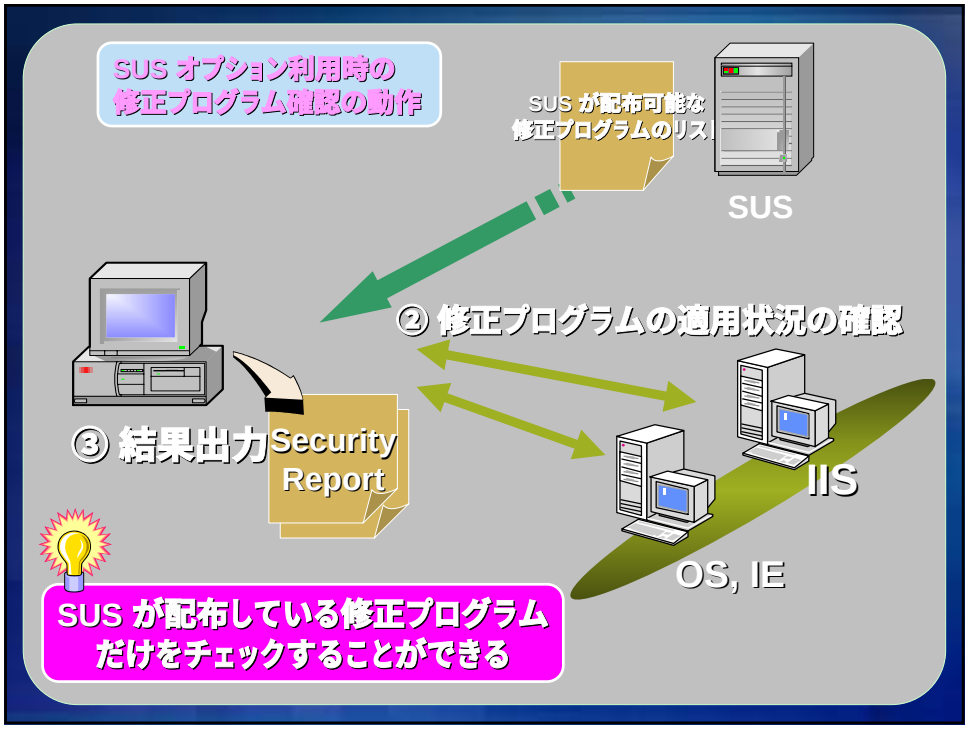
Microsoft Baseline Security Analyzer 1.1（MBSA）

- 様々なセキュリティ項目を確認
  - パスワードの設定
  - サービスの起動状況
  - アプリケーションの設定
- SUS との連携
- HFNetChk の機能を包括
- 無償

HFNetChk と MBSA の違い

- HFNetChk のメリット
  - 日本語版 XML DB ファイルによる正確な状況の把握
- MBSA のメリット
  - 様々なセキュリティ設定の確認
  - GUI ツール
  - SUS との連携

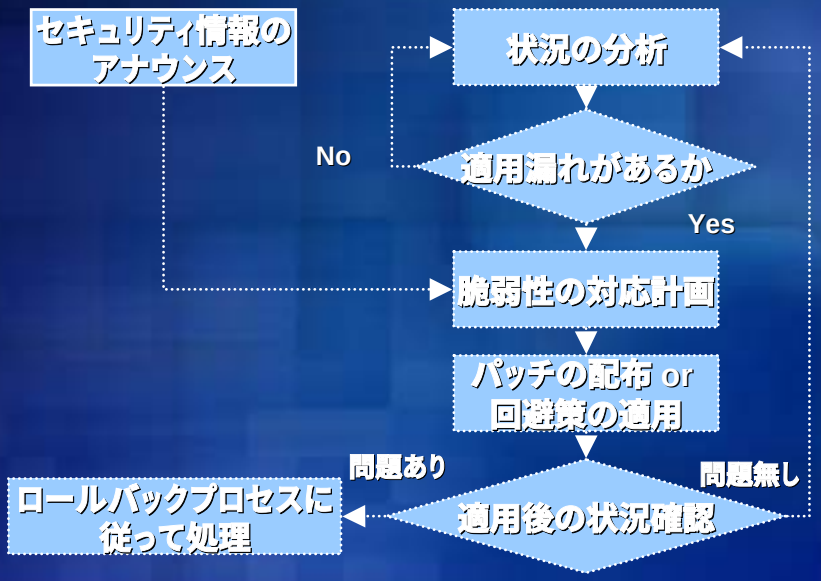




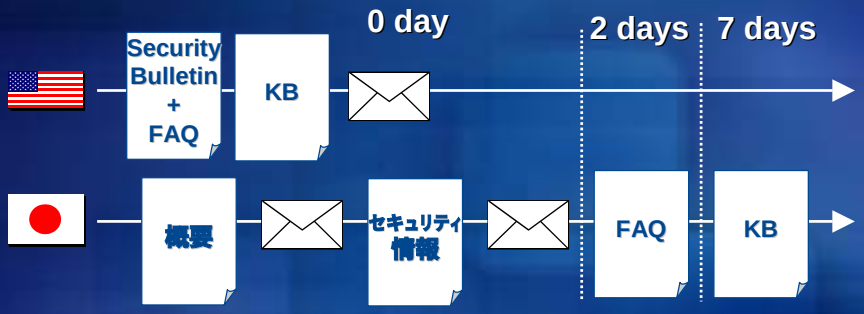
HFNetChk and MBSA

demo

修正プログラム管理プロセス



セキュリティ情報のアナウンス



- 概要情報
  - US 公開後、午前中までに公開
- セキュリティ警告サービス-日本語版
  - セキュリティ情報の新着および更新情報を電子メールでお知らせするもの
- セキュリティ情報 (Security Bulletin)
  - 脆弱性に関する全般的な情報
- セキュリティ情報 - よく寄せられる質問 (FAQ)
  - 脆弱性を把握するのに有効
- 技術情報 (KB)
  - 修正プログラム、製品に関する情報、セキュリティ以外の問題に関する情報

セキュリティ情報の確認 - 1

1. 「概要」を確認
   - 該当製品
   - 深刻度
   - 推奨する対応策
2. 「問題を緩和する要素」を確認
   - 回避策で対応できるか、その他に対応方法がないか確認
3. 「問題」、「よく寄せられる質問」を確認
   - どのような問題か
   - 脅威の影響
   - 仕様変更の情報

セキュリティ情報の確認 - 2

4. 修正プログラムに関する情報
   - 対象プラットフォーム
   - 再起動の必要性
   - 修正プログラムのアンインストール
   - 修正プログラムに含まれる過去の修正

セキュリティ情報の確認 - 3

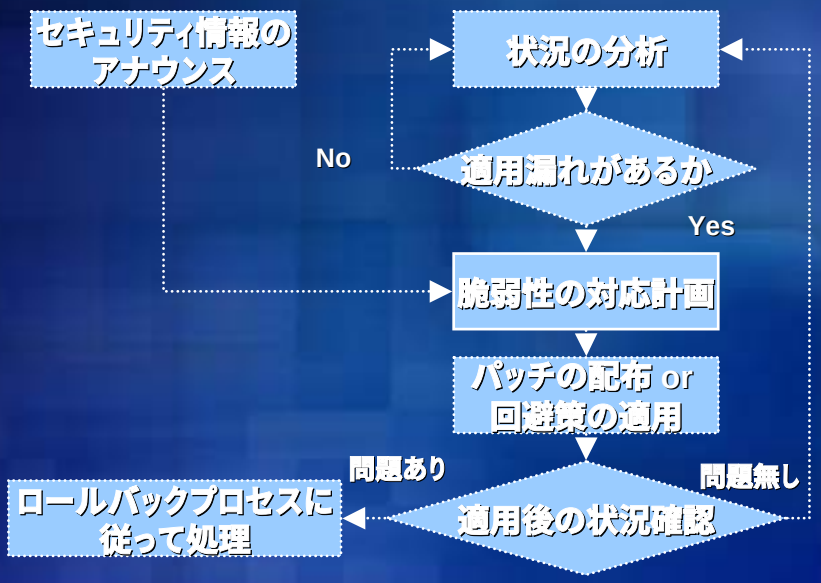
5. サポート技術情報(KB)の確認
   - 修正プログラムに関する情報が記載
   - 修正プログラムを適用することにより本稼働環境に悪影響を与えないか(仕様の変更点があるか確認)
   - Internet Explorer または Windows のアップデート適用後の問題 (325192)
     http://support.microsoft.com/default.aspx?scid=kb;ja;325192
6. 更新情報の確認
   - 「マイクロソフト セキュリティ情報一覧」の更新日を確認
     http://www.microsoft.com/japan/technet/security/current.asp

外部セキュリティ情報

- 海外
  - Bugtraq
  - CERT/CC
- 国内
  - IPA/ISEC
  - JPCERT/CC
- Virus 対策ベンダー
  - トレンドマイクロ株式会社
  - 株式会社シマンテック
  - 日本ネットワークアソシエイツ株式会社
- セキュリティ関連企業
  - 株式会社 ラック
  - インターネット セキュリティ システムズ株式会社

外部サイトからの情報入手が不可欠

修正プログラム管理プロセス



脆弱性の対応計画

セキュリティ対策の重要点

- 脆弱性の対策はコストとリスクのバランスが大切
- 脆弱性によるリスクは時間とともに増加

対策方法の検討

回避策による対応

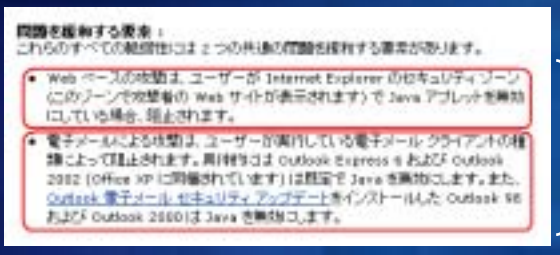
- 回避策による対応が必要な場合
  - 修正プログラムによる問題
  - 修正プログラムの適用のコストが高い
  - 不必要な機能、サービスが立ち上がっている
- 「セキュリティ情報」、「よく寄せられる質問」、「サポート技術情報」を確認し回避方法を検討
- ご不明な点は

セキュリティ情報センター

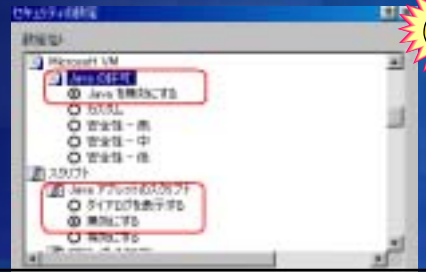
http://www.microsoft.com/japan/security/sicinfo.asp
電話番号 :0120-69-0196
営業時間 :平日9:30～12:00/13:00～19:00

回避策による対応 - 例

MS02-069 Microsoft VM の問題により、システムが侵害される (810030)



対策を行うことにより、リスクを緩和できる



回避策を対策を行うことにより、Microsoft VM に関係する問題に今後対応しなくてもすむ

修正プログラム適用時の考慮点

計画の立案

担当オーナーの明確化

暫定的な対策の必要性を検討

バックアップの検討

適用にかかるコストを検討

テスト項目を検討

テスト実施

修正プログラム管理プロセス

セキュリティ情報のアナウンス

状況の分析

No

適用漏れがあるか

Yes

脆弱性の対応計画

パッチの配布 or 回避策の適用

問題あり

問題無し

ロールバックプロセスに従って処理

適用後の状況確認

修正プログラム配布計画

	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	△	○	○	×
System Management Server (SMS)	○	×	○	○
Microsoft Software Update Services (SUS)	○	○	×	○

Software Update Services（SUS）

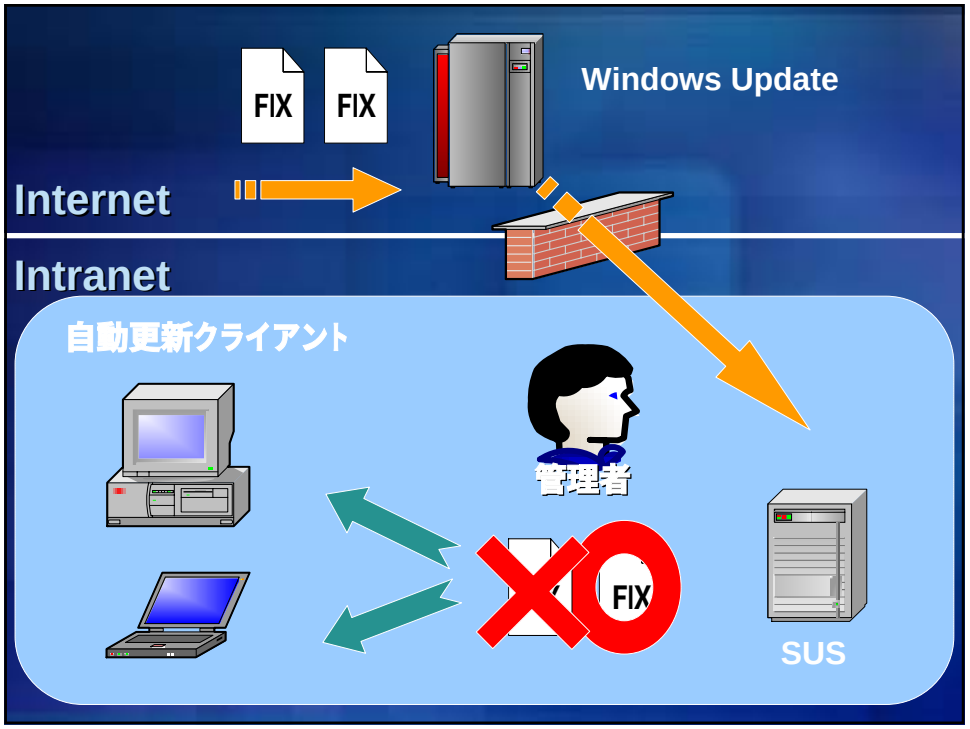
- Windows Update を企業内に構築
  - 必要な修正プログラムを簡単に適用可能
  - 配布する修正プログラムを管理者が設定可能
  - セキュリティ修正プログラムを含む「重要な更新」が配布可能
  - システム要件
    - Windows 2000 Server SP2 以上
    - Internet Explorer 5.5 以上

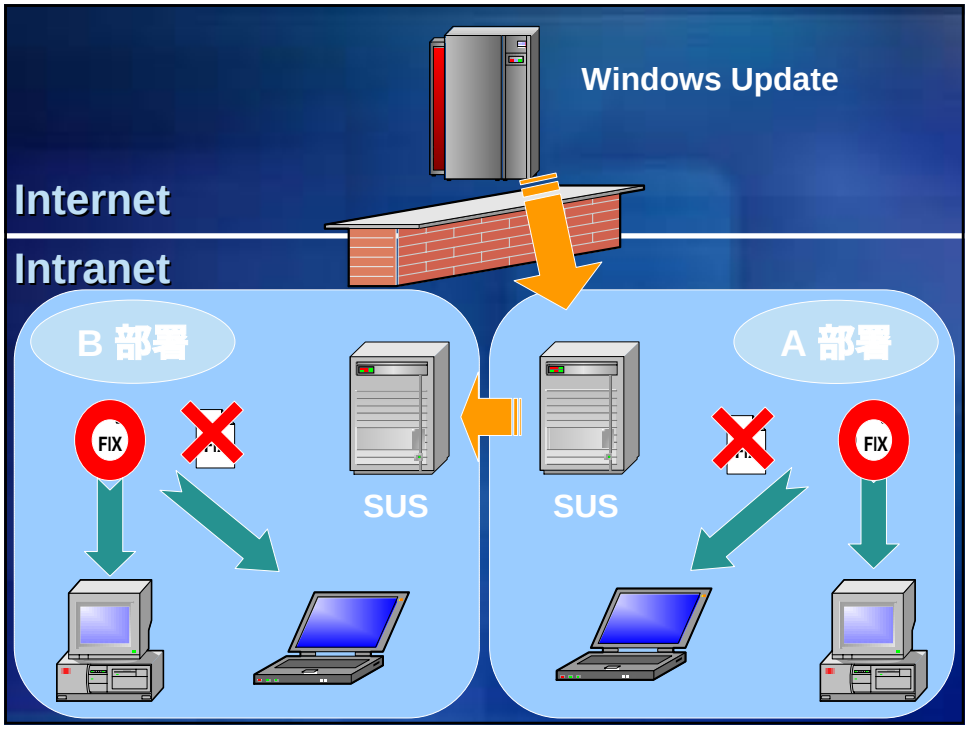
自動更新クライアント

- SUS を利用するためには自動更新クライアント（Ver2.2 以上）が必要
- Windows 2000 SP3 、Windows XP SP1 に含まれる
- 制限ユーザーでも修正プログラムのインストールが可能

Software Update Services SP1

- Server 改良点
  - Windows 2000 ドメイン コントローラおよび Small Business Server 上でも稼動
  - IIS Lockdown ツールとの統合性を向上
  - ソフトウェア更新パッケージの [詳細] リンク
- Client 改良点
  - 次回の予定インストール実行時間を指定する機能を提供
  - ユーザーのログオン中の自動リブートの可否


FIX
FIX
Windows Update
Internet
Intranet
自動更新クライアント
管理者
FIX
SUS


Windows Update
Internet
Intranet
B 部署
A 部署
FIX
FIX
SUS
SUS

Security Update Service

demo

対策後の監視、確認

- 修正プログラムの適用漏れがないか確認
- 対策実施後、一定期間の監視が必要
  - 各種ログファイル
  - パフォーマンスモニタ
  - ユーザーからのフィードバック
- 問題が確認された場合
  - セキュリティ情報の再確認
  - 修正プログラムのアンインストール、および回避策による脆弱性の対策

まとめ

- 修正プログラムの管理はセキュリティ リスクを抑える有効な手段です
- セキュリティ ホールの対策は、セキュリティの被害で発生するコストに比べ大幅に軽減されます
- セキュリティ対策は継続が重要です

Microsoft®

Appendix

- Microsoft Security
  http://www.microsoft.com/japan/security/
- TechNet Security
  http://www.microsoft.com/japan/technet/security/
- 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
- Best Practices for Applying Service Packs, Hotfixes and Security Patches（英語情報）
  http://www.microsoft.com/technet/security/bestprac/bpsp.asp
- 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
- 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
- マイクロソフト セキュリティ情報一覧（スライド 17）
  http://www.microsoft.com/japan/technet/security/current.asp

Appendix

- Internet Explorer または Windows のアップデート適用後の問題 (325192)（スライド 17）
  http://support.microsoft.com/default.aspx?scid=kb;JA;325192
- Microsoft Baseline Security Analyzer 1.1（MBSA）（スライド 8）
  http://www.microsoft.com/japan/technet/security/tools/tools/mbsahome.asp
- HfNetChk（スライド 6）
  http://www.microsoft.com/japan/technet/security/tools/tools/hfnetchk.asp
- Software Update Services（SUS）（スライド 27）
  http://www.microsoft.com/japan/windows2000/windowsupdate/sus/
- セキュリティ 警告サービス 日本語版（スライド 14）
  http://www.microsoft.com/japan/technet/security/bulletin/notify.asp
- HFNetChk 管理スクリプト (スライド7、36)
  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9989D151-5C55-4BD3-A9D2-B95A15C73E92

セキュリティ運用ガイド

- TechNet サイトに公開
  - Windows 2000 Server
  - Exchange 2000 Server
- CD に含まれるファイルは適宜更新