セキュリティ脅威の傾向と対策のポイント

2004年2月4日

中央大学 研究開発機構 専任研究員

塩月誠人<shio@st.rim.or.jp>

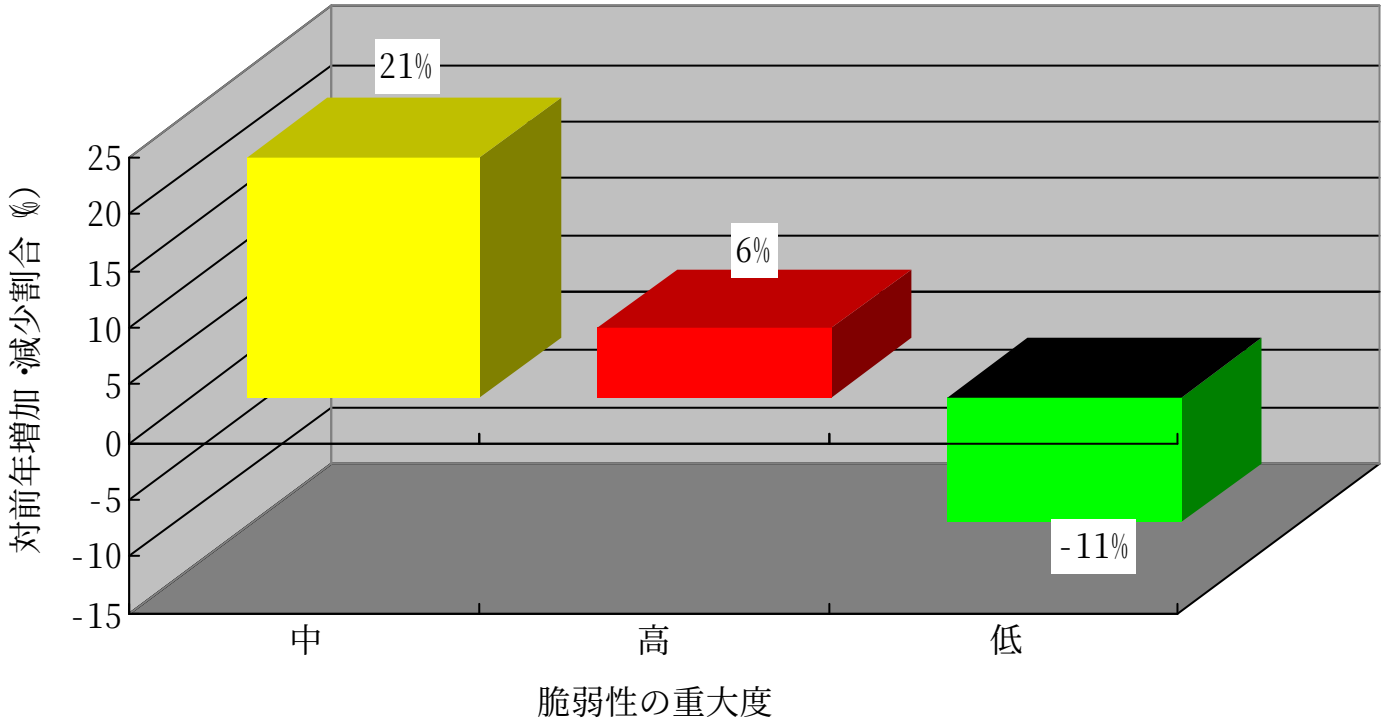
Agenda

- セキュリティ脅威の傾向
  - セキュリティホールの傾向
  - ネットワーク攻撃の傾向
  - 内的要因によるセキュリティ侵害
  - 注目すべきセキュリティ脅威
- セキュリティ対策のポイント
  - OSのセキュリティ基本設定
  - パッチマネージメント
  - クライアントPCセキュリティ
  - アプリケーションセキュリティ
  - セキュリティテスト

セキュリティ脅威の傾向

セキュリティホールの傾向　(その1)

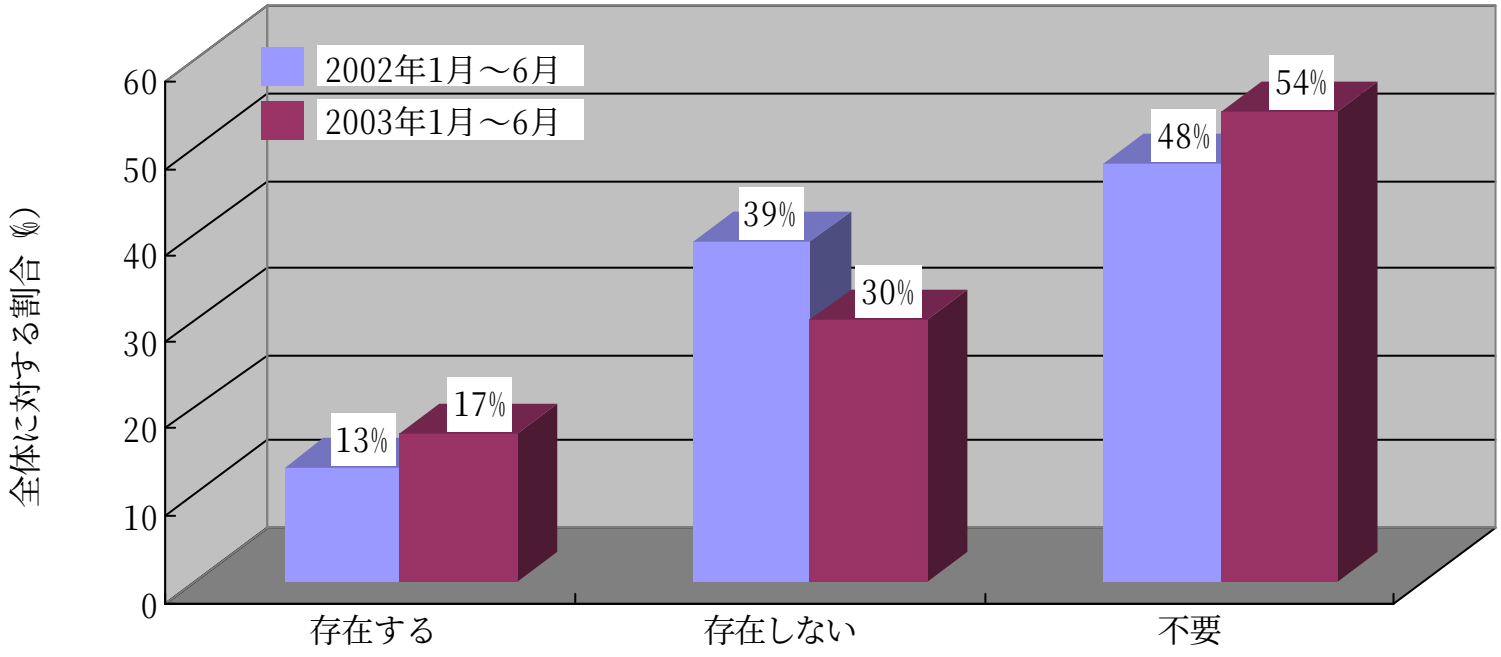
- 危険度の高いセキュリティホールの増加



（Symantec Internet Security Threat Report　September 2003）」より）

セキュリティホールの傾向 (その2)

- 攻撃に利用されやすいセキュリティホールの増加



(「Symantec Internet Security Threat Report September 2003)」より)

セキュリティホールの傾向 (その3)

- クライアントマシンがターゲットとなるセキュリティホールの増加

Windows OSにおける最近のクライアントセキュリティホール	
Microsoft WordおよびMicrosoft Excelの脆弱性 (MS03-050)	Microsoft Access Snapshot Viewerの未チェックのバッファ (MS03-038)
Workstationサービスのバッファ オーバーラン (MS03-049)	Visual Basic for Applicationsの問題 (MS03-037)
Internet Explorer用の累積的なセキュリティ更新 (MS03-048)	WordPerfectコンバータのバッファオーバーラン (MS03-036)
リストボックスおよびコンボボックスのコントロールのバッファオーバーラン (MS03-045)	Microsoft Wordの問題によりマクロが自動実行 (MS03-035)
Windowsの「ヘルプとサポート」のバッファオーバーラン (MS03-044)	MDAC機能の未チェックのバッファ (MS03-033)
メッセンジャサービスのバッファオーバーラン (MS03-043)	Internet Explorer用の累積的な修正プログラム (MS03-032)
Windowsトラブルシュータ ActiveXコントロールのバッファ オーバーフロー (MS03-042)	DirectXの未チェックのバッファ (MS03-030)
Authenticodeの検証の問題 (MS03-041)	Windowsシェルの未チェックのバッファる (MS03-027)
Internet Explorer用の累積的な修正プログラム (MS03-040)	RPCインターフェイスのバッファオーバーラン (MS03-026)
RPCSSサービスのバッファオーバーラン (MS03-039)	ユーティリティマネージャによるWindowsメッセージ処理の問題 (MS03-025)

(「マイクロソフトセキュリティ情報一覧」より、昨年7月以降)

セキュリティホールの傾向 (その4)

- 種の尽きないWebブラウザのセキュリティホール

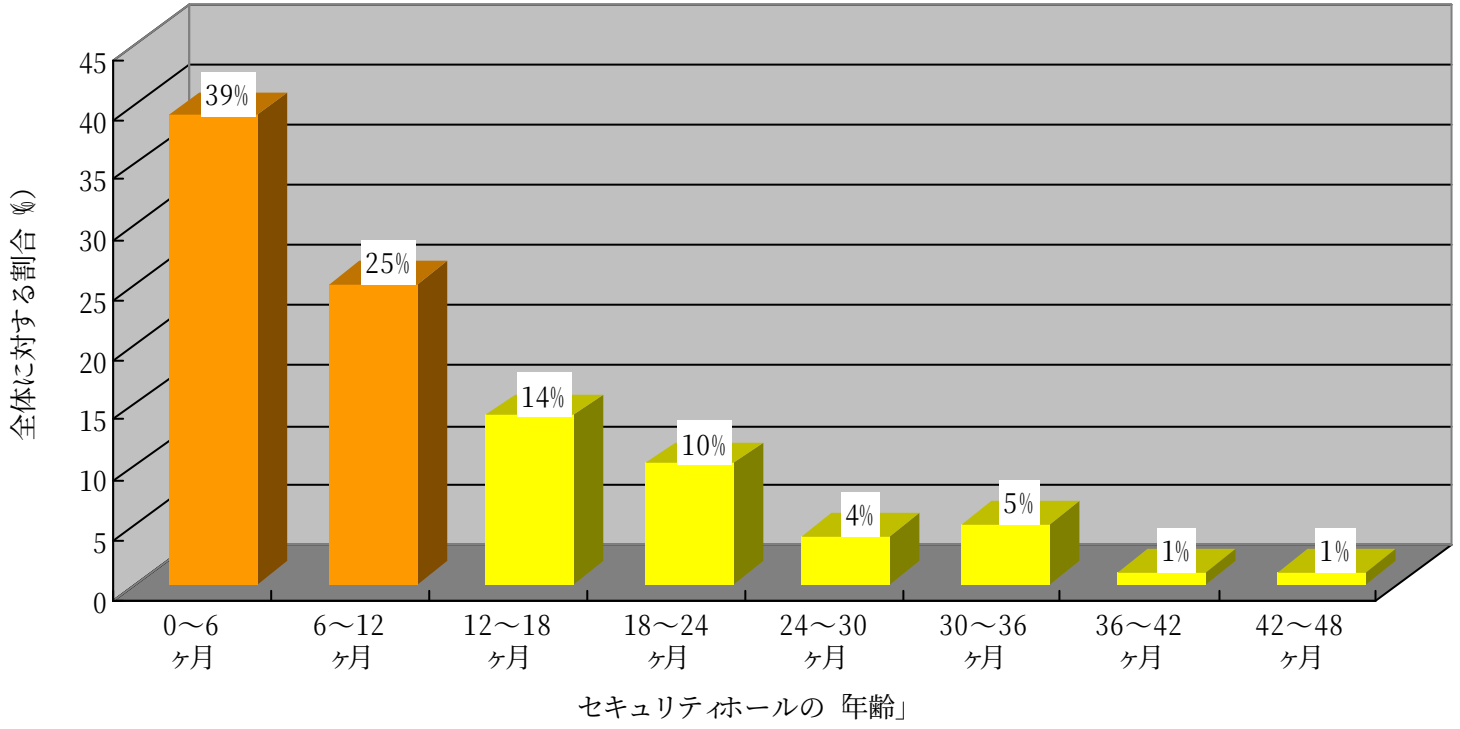
パッチのないInternet Explorerのセキュリティホール (主要なもの)	
Shell.Application ActiveXによるLNKファイル作成と実行	クロスドメインスクリプティング
ShowHelpディレクトリトラバーサルによるCHMファイルの実行	CODEBASEを利用したローカルファイルの実行
%01記号によるサイトスプーフィング	ADODB.Streamによるローカルファイル書き込み
不正なContentTypeによるキャッシュディレクトリパスの暴露	NOTEPAD.EXE書き換えによるview-sourceでの任意プログラム実行
MHTMLリダイレクションによる任意ファイルのダウンロードと実行	IEキャッシュディレクトリにおけるローカルゾーン適用
MHTMLリダイレクションによるローカルファイルのパース	RedirectionとRefreshによるローカルファイルのパース

(「Unpatched Internet Explorer Bugs」より

- ✓ 実行系はローカルゾーンに限られる
- ✓ しかしこれらを組み合わせることで、Webアクセスによるプログラム起動攻撃が可能

ネットワーク攻撃の傾向 (その1)

- 攻撃対象の64%は過去一年以内に見つかったセキュリティホール



（「Symantec Internet Security Threat Report　September 2003」より）

ネットワーク攻撃の傾向 (その2)

- 迅速な攻撃プログラムの公開
  - 「Windows RPC/DCOM」セキュリティホール
    - 7月17日、情報およびパッチ公開 (MS03-026)
    - 7月26日、攻撃プログラム公開 (dcom.c)
    - 8月12日頃、ブラスターワーム発生
  - 「Cisco IOSサービス妨害」セキュリティホール
    - 7月16日、情報およびパッチ公開
    - 7月18日、攻撃プログラム公開 (shadowcode)
  - 「Windows Workstationサービス」セキュリティホール
    - 11月11日、情報およびパッチ公開 (MS03-049)
    - 11月12日、攻撃プログラム公開 (0349.cpp等)

ネットワーク攻撃の傾向 (その3)

- 感染性能に優れたワーム/ウィルスによる攻撃
  - クライアントPCのセキュリティホールを攻撃
    - ブラスター、ウェルチア (RPC/DCOMセキュリティホールを利用)
  - クライアントPCから社内ネットワークへ感染
    - 自宅等で感染したPCを持ち込む
    - VPN/RASで社内にアクセス
    - 社内クライアントPCからインターネットへダイアルアップ
    - 規模の大きな企業ほど感染 (全体平均で18.6%、IPA調べ)
  - 複合的なセキュリティ脅威
    - 感染したPC自体の被害
    - 感染行為によるネットワーク障害
    - 情報漏洩、情報削除
    - ...

内的要因によるセキュリティ侵害（その1）

- 最近の個人情報流失事例

組織名	流出規模	流出情報	流出経路・原因
NTTデータ	4312件（紛失）	サービス利用者の依頼情報	業務委託先社員のノートPC紛失
ファミリーマート	18万2780件	会員の個人情報	調査中
コンピュータソフトウェア著作権協会	1184件	Webサイトの質問者の個人情報	WebサイトCGIプログラムの不備
ローソン	約56万件	カード会員の個人情報	調査中（業務委託先から漏洩?）
近畿日本ツーリスト	2600件	顧客メールアドレス	ウィルス駆除通知メール
アプラス	7万9110名	顧客個人情報	調査中（業務委託先から漏洩?）
リコー/帯広市役所	6万2433件（紛失）	除籍簿情報	調査中（磁気テープ宅配過程にて紛失?）

（各組織のプレスリリースおよびメディア報道より）

内的要因によるセキュリティ侵害（その2）

- 情報流失の内的要因
  - 過失による情報漏洩（誤掲示、誤送信）
  - PCやフロッピーディスク等の盗難・紛失
  - システム設定の不備（Webアクセス許可の設定ミス等）
  - Webアプリケーションの不備（一定の操作をすればデータにアクセス）
  - 内部者（業務委託先）による故意の流出
    - アクセス権を持つ者が行う場合
    - アクセス権を持たない者が行う場合

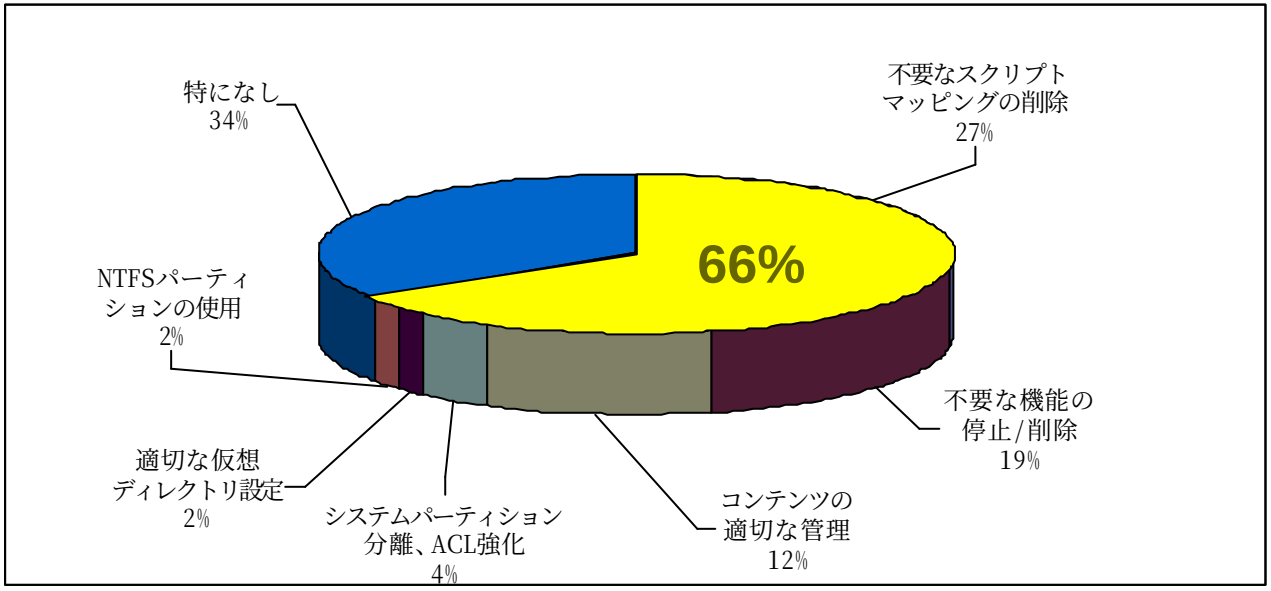
注目すべきセキュリティ脅威

- ワームやウィルス
  - 出現が早く強力に感染 → パッチが間に合わない
  - クライアントPCにより社内に感染、複合的に影響
- 内部者の故意・過失
  - 技術的/管理的コントロールが未整備
  - 対外的なダメージが非常に大きい
- Webアプリケーションの不備
  - サイト固有の問題であるため実態の把握が困難
  - しかし現実に多く存在する

セキュリティ対策のポイント

OSのセキュリティ基本設定（その1）

- （一般的に）デフォルト状態はセキュアでない
- 基本設定を施すことで未然に防げる場合が多い



（2000年から昨年3月までのIISセキュリティホール、独自調べ）

- システム設計時におけるセキュリティ設定の標準化

OSのセキュリティ基本設定（その2）

- Windows 2000における一般的脅威と対策
  - Nullセッションによる情報取得
    - 「匿名接続の追加を制限する」-> 「SAMのアカウントと共有の列挙を許可しない」もしくは「明示的な匿名アクセス権がない場合アクセスを許可しない」
  - パスワードクラック
    - 各種アカウント設定（長さ、文字種制限、ロックアウト設定、等）
    - NoLMHash設定
  - SMBリレー等によるMan-in-the-Middle攻撃
    - SMB署名、IPSec通信
  - ソースルーティングによるIPアドレス詐称
    - ソースルーティング禁止設定（DisableIPSourceRouting＝2）
  - 各種物理攻撃
    - EFSの使用、SYSKEYを2以上に設定
  - その他
    - 不要サービスの停止（メッセンジャー、サーバサービス、…）、監査の有効化

パッチマネージメント（その1）

- セキュリティパッチにはタイムラグがある
  - 発見者が脆弱性情報をどのように取り扱うかに依存
  - 攻撃ツール（Worm等）の蓄積 → 新たな脆弱性にすばやく対応
  - 日本語版ゆえのパッチの遅れ … 最近はあまりない？
- セキュリティパッチは必ずしも完全ではない
  - パッチは緊急的に作成（早期提供が優先）
  - ベンダー側での検証・テストが十分でない
- セキュリティパッチ適用のインパクト
  - 実運用環境に適用する前にテストが必要
  - パッチ自体の問題、動作環境やアプリケーションとの関係

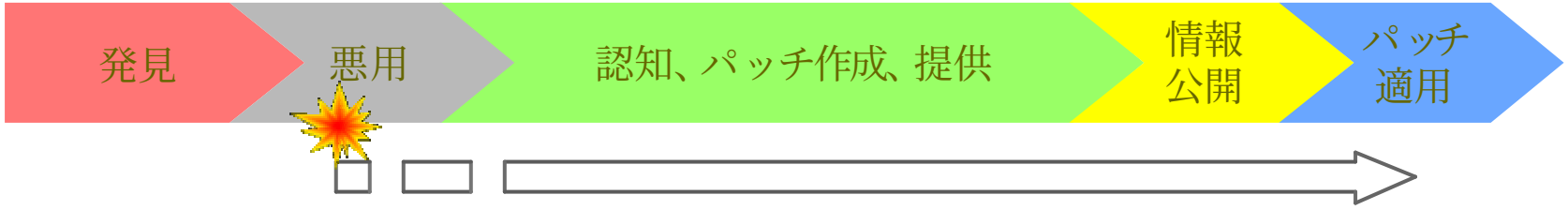
パッチマネージメント (その2)

- パッチのタイムラグ

パッチ提供後、脆弱性の詳細が公開

発見者がベンダーに通知せず詳細を公開

発見者が脆弱性を悪用して攻撃プログラムを作成

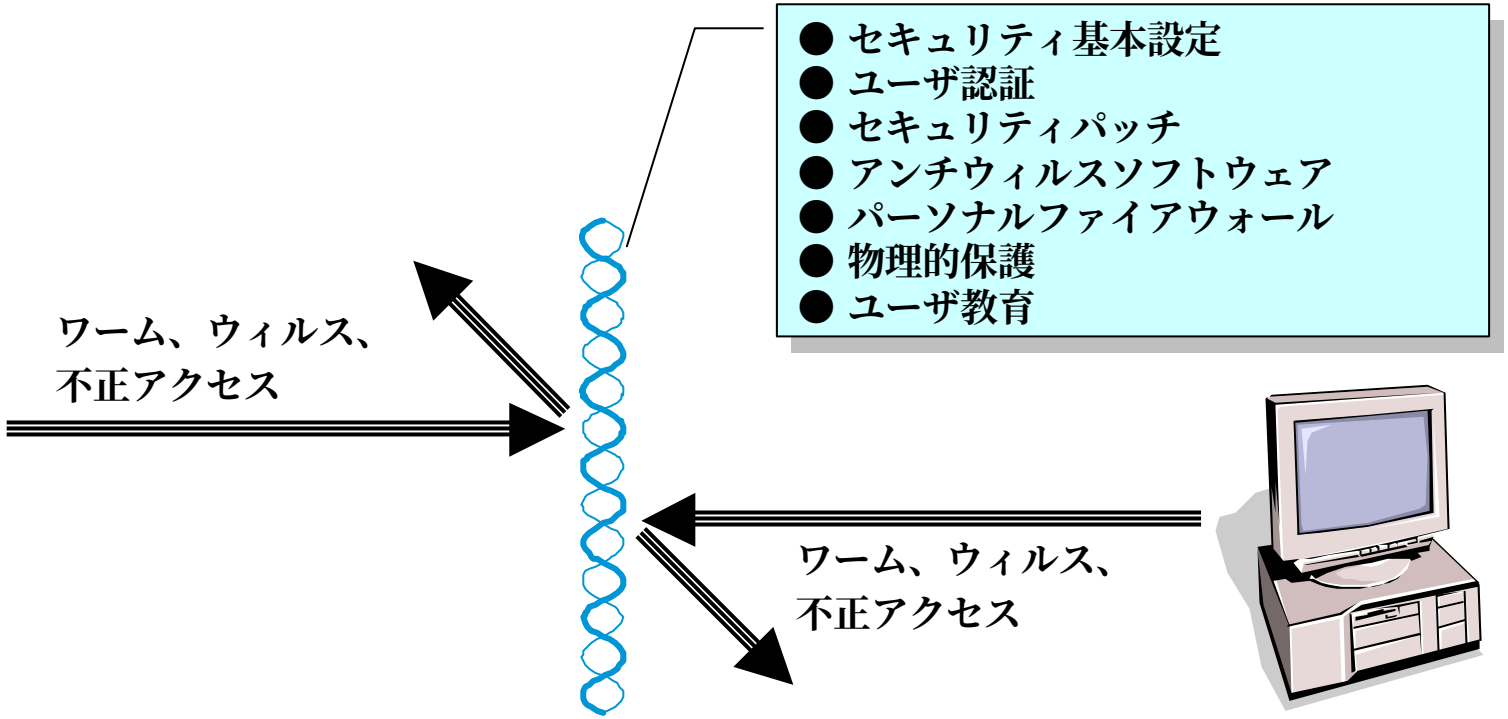


パッチマネージメント (その3)

- パッチ適用の判断
  - すぐに適用すべきか、定期メンテナンス時でもよいか
  - セキュリティホールおよびパッチ適用のリスクを知る
  - リスクが許容できるかどうかを判断する
  - 判断材料 … セキュリティホールの情報と自己の状況
- パッチのテストと実環境への適用
- パッチ適用を前提としたシステム設計・構築
- クライアントPCに対するパッチ適用
- パッチマネージメントシステムの導入

クライアントPCセキュリティ（その1）

- クライアントPC自体を保護する
- クライアントPCからの攻撃を防ぐ

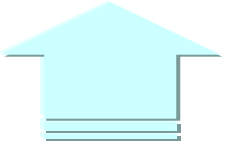


クライアントPCセキュリティ（その2）

- Windowsクライアント PCを安全に使うには（特にモバイル）
  - Windows 2000もしくはWindows XP Proを使用する
  - 一般ユーザでログオンして使用する
  - BIOSパスワードやHDパスワードを利用する
  - SYSKEYを2（パスワード入力）に設定する
  - 暗号化機能を正しく使う
  - ホストファイアウォール機能を利用する
  - IEのゾーンセキュリティ設定を強化する
  - 「ソフトウェア制限のポリシー」を有効に使う（XPの場合）
  - アンチウイルス、Windows Update、データバックアップ、…

クライアントPCセキュリティ（その3）

- エンドユーザ自身の不正な行動を制限する
  - 不正プログラム、攻撃プログラムのインストール・実行
  - アクセス許可のない情報へのアクセス
  - 機密情報の外部への持ち出し



  - ユーザ操作権限を限定
  - 不正プログラムの検査・削除
  - ユーザの行動の監視
  - リムーバブルメディアの制限
  - 非正規PCの接続の拒否
  - 統合クライアント管理システムの導入

アプリケーションセキュリティ

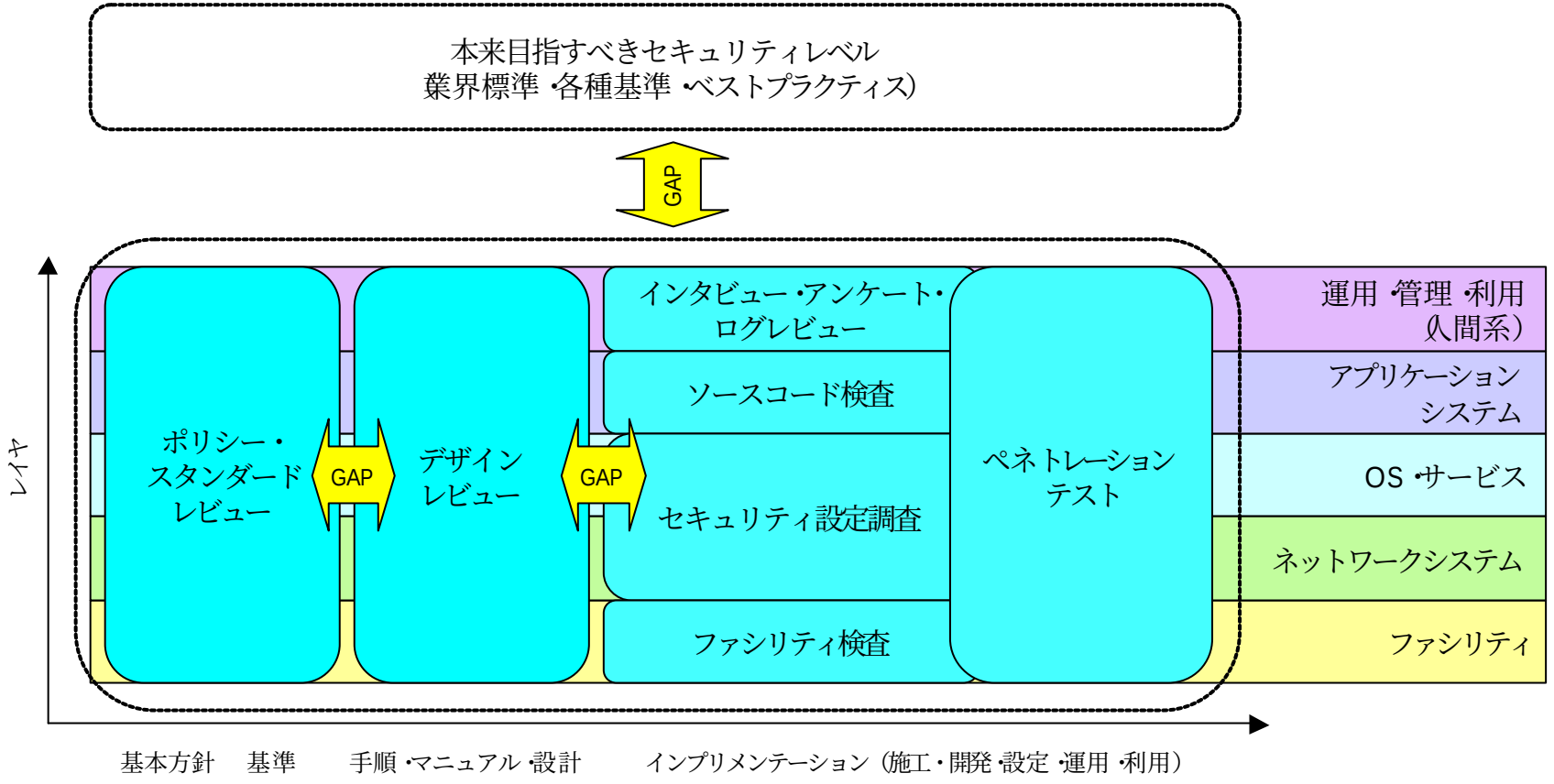
- 特にWebアプリケーション（CGI等）
  - クロスサイトスクリプティング
  - プログラム実行、ファイル内容表示、ディレクトリトラバーサル
  - アカウント推測、セッションID再利用、認証ロジック回避
  - バッファオーバーフロー、フォーマットストリング攻撃
  - SQLインジェクション
- 基本的にはアプリケーションの設計・プログラミングミス
- Webシステムにおける非常に大きな脅威
- セキュアプログラミング
- アプリケーションファイアウォール

セキュリティテスト（その1）

- セキュリティテストの目的
  - 組織が自ら定めたセキュリティレベルに達しているか?
  - 本来目指すべきセキュリティレベルに達しているか?
- セキュリティテストの実施時期
  - システム導入時の実施（システム開発、システム購買）
  - システム改変時の実施（機能追加、改良）
  - 定期的な実施（毎月、半年おき、一年おき、等）
- さまざまなセキュリティテスト
  - ポリシーレビュー、スタンダードレビュー、デザインレビュー
  - ファシリティ検査
  - セキュリティ設定調査、アプリケーションソースコード検査
  - 管理者や利用者へのインタビュー、アンケート、ログ（記録）のレビュー
  - ペネトレーションテスト

セキュリティテスト（その2）

- 各種セキュリティテストの守備範囲



セキュリティテスト（その3）

- ペネトレーションテストの特徴
  - 【長所】:侵入者と同じ思考、手口、ツールで、不正侵入の可能性を実証
    - → 実際に利用されうる脆弱性を、具体的に明らかにできる
    - → インパクトのある結果を提示することができる
    - → 非正規のサーバ、アクセスポイント等、隠れた問題を明らかにできる
    - → 単体ではなくシステムとしての問題点を明らかにできる
    - → 侵入の検知やハンドリングをテストすることができる
  - 【短所】:限られた期間内および侵入経路による、実装に対するテスト
    - → 問題の根本原因を解き明かすことはできない
    - → 問題を網羅的に明らかにすることはできない
    - → 潜在的な問題を明らかにすることはできない
    - → 相応のリスクを伴う

まとめ

- 事後対応型（Reactive）から事前予防型（Proactive）へ
  - セキュリティ基本設定を含むセキュアなシステム構築
  - セキュリティテストによる目標との乖離状況チェック
  - 侵入や情報漏洩を未然に防ぐためのセキュリティ監視
- 外部防御から内部防御へ
  - クライアントPCのセキュリティ対策
  - クライアントPCを網羅したパッチマネージメントシステム
  - エンドユーザの行動をいかに制限するか
- 下位レイヤーから上位レイヤーへ
  - ネットワークやOS層からアプリケーション層や人間系へ
  - セキュアプログラミング、アプリケーションファイアウォール
  - 教育、教育、教育、…

参考

- Symantec Internet Security Threat Report Volume IV
  https://enterprisesecurity.symantec.com/Content/displaypdf.cfm?SSL=YES&EID=0&PDFID=551&promocode=ITR
- マイクロソフトセキュリティ情報一覧
  http://www.microsoft.com/japan/technet/security/current.asp
- Unpatched Internet Explorer Bugs
  http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/index.html
- W32/MSBlaster及びW32/Welchiウイルス被害に関する企業アンケート調査の結果について（IPA）
  http://www.ipa.go.jp/ipa/press/img/030918Press.pdf
- セキュリティ基本設定の重要性（NT-Committee2 緊急コンピュータセキュリティ研究会）
  http://impress.tv/im/article/kcs.htm
- Windows Server World誌 特集 「社内不正ユーザ撃退法」
  http://www.st.rim.or.jp/~shio/wsvworld/maluser/
- IPA ISEC セキュア・プログラミング講座
  http://www.ipa.go.jp/security/awareness/vendor/programming/index.html
- Intrusion Prevention Systems: the Next Step in the Evolution of IDS
  http://www.securityfocus.com/infocus/1670