

攻撃手法別にみる一歩踏み込んだWindowsセキュリティ対策

— マルウェア対策編 —

2012年12月19日（水）

塩月 誠人 <mshio@Sec-Pro.Net>
合同会社セキュリティ・プロフェッショナルズ・ネットワーク

セキュリティ・プロフェッショナルズ・ネットワークとは

□ 合同会社セキュリティ・プロフェッショナルズ・ネットワーク

- 設立 . . . 2008年5月26日
- 役員 . . . 塩月誠人、吉田英二

□ 情報セキュリティ人材育成活動を行う事業主体として設立

□ 三つの事業活動

- 実務に役立つセキュリティ技術の実践トレーニングの提供
- 情報セキュリティに関するさまざまな技術セミナーの企画
- セキュリティ技術者同士のヒューマンネットワークの構築

本セミナーの概要

- 昨今の標的型攻撃に代表される脅威から組織の情報資産を守るためには、もはや一般的なセキュリティ対策では限界があります。本セミナーではWindowsシステムを取り巻くさまざまな「脅威」すなわち攻撃手法を整理するとともに、それらの攻撃手法ごとにどのような追加的セキュリティ対策が有効であるかについて、Windows OSが本来備えているセキュリティ機能を中心にデモを交えながら解説します。

Windowsシステムにおけるセキュリティ脅威

□ 三つの主要なセキュリティ脅威

- マルウェア感染

- ネットワーク不正アクセス

- 物理的な不正アクセス

← 本セミナーはここにフォーカス

□ 攻撃者の主たる目的

- 情報の取得 (= 金銭、スパイ活動)

- 踏み台としての利用 (ボット化、攻撃元の詐称、隠れ蓑、中継地点)

マルウェアの侵入経路

□ 外部記憶媒体を経由

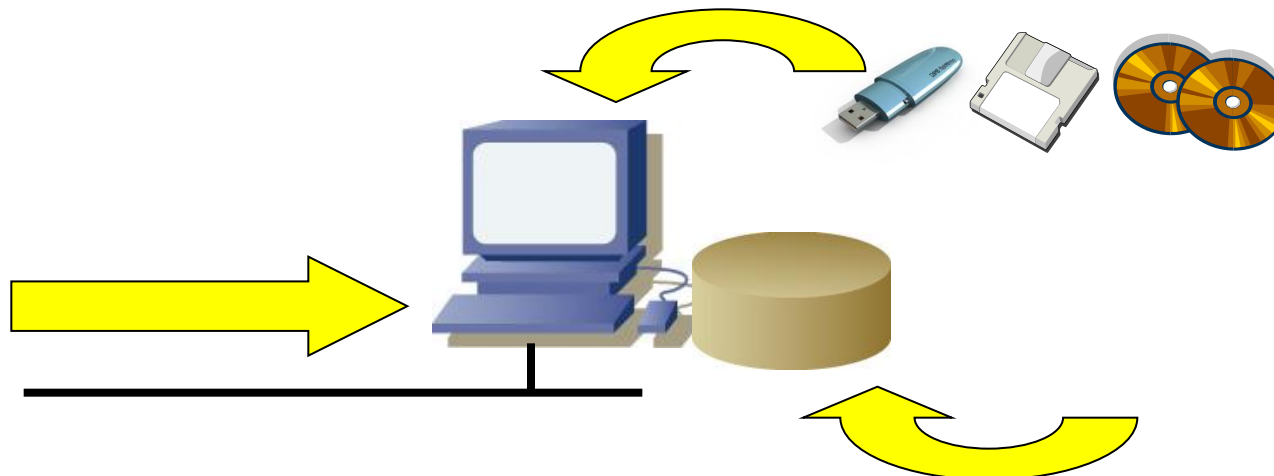
- USBメモリ、SDメモリカード、フロッピーディスク、CD/DVD、・・・

□ ネットワークを経由

- Webアクセス、ファイル共有、電子メール、ネットワーク攻撃、・・・

□ ハードディスクへの直接導入

- ハードディスクの物理的アクセスによるファイルの書き換えや設置



マルウェアの感染手法

- ユーザを利用する（ユーザが自ら実行してしまう）ことで感染
 - 不用意にプログラムを実行／インストールしてしまった
 - アイコンやファイル拡張子が偽装されていた
 - 知り合いや関係者（らしき人）から送られてきたので信用してしまった
 - 正規のプログラムファイルが置き換えられていた

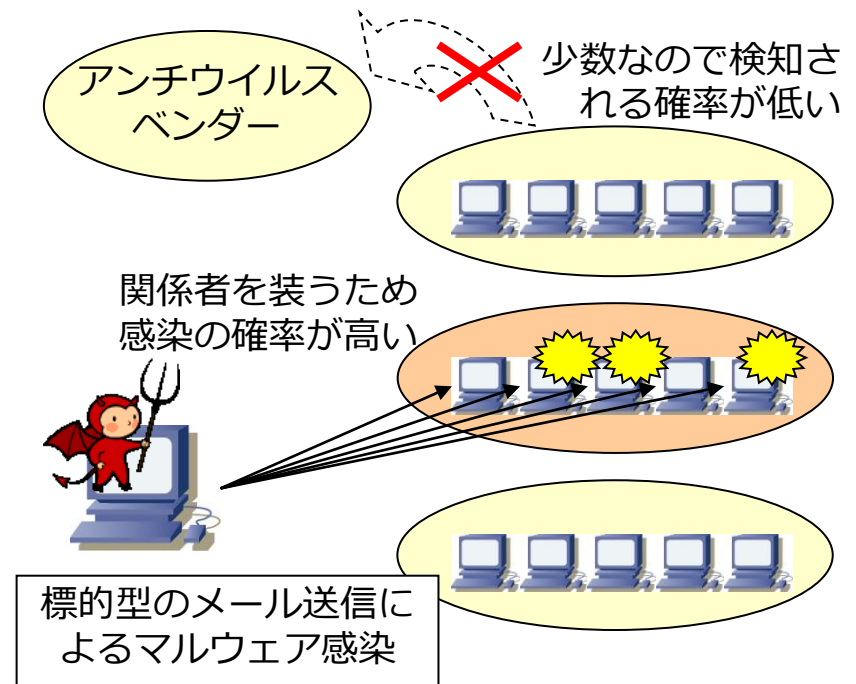
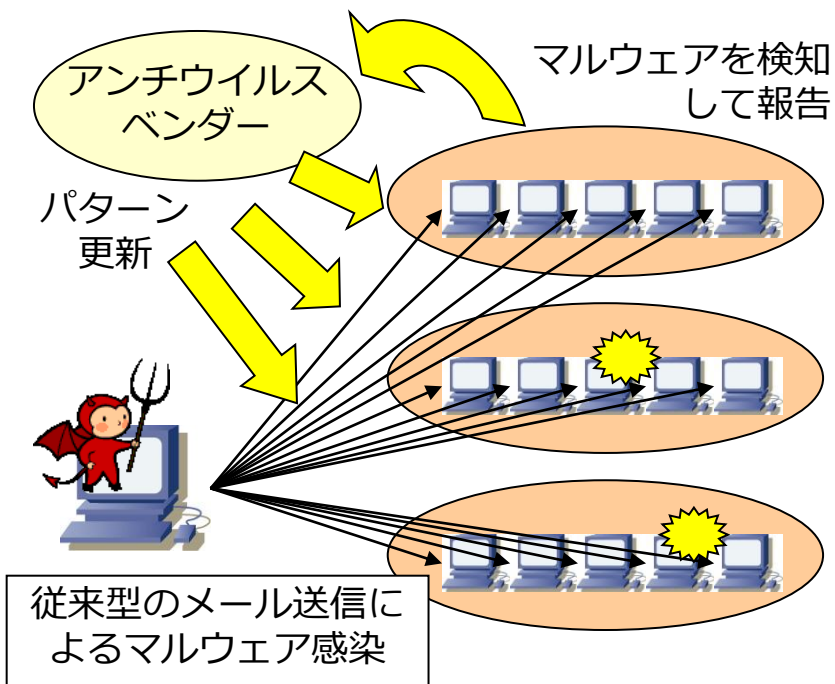
- 脆弱性を利用することで感染
 - ネットワーク経由での脆弱性の利用
 - Webアクセス → ブラウザの脆弱性の利用
 - 電子メール閲覧 → メールソフトの脆弱性の利用
 - 文書／画像／圧縮ファイルオープン → ビューアソフト等の脆弱性の利用

- OSの機能を利用することで感染
 - ブート情報を書き換えることで自動的に実行して感染（Bootkit）
 - USBメモリやCD／DVDの自動実行（Autorun）により感染

標的型攻撃

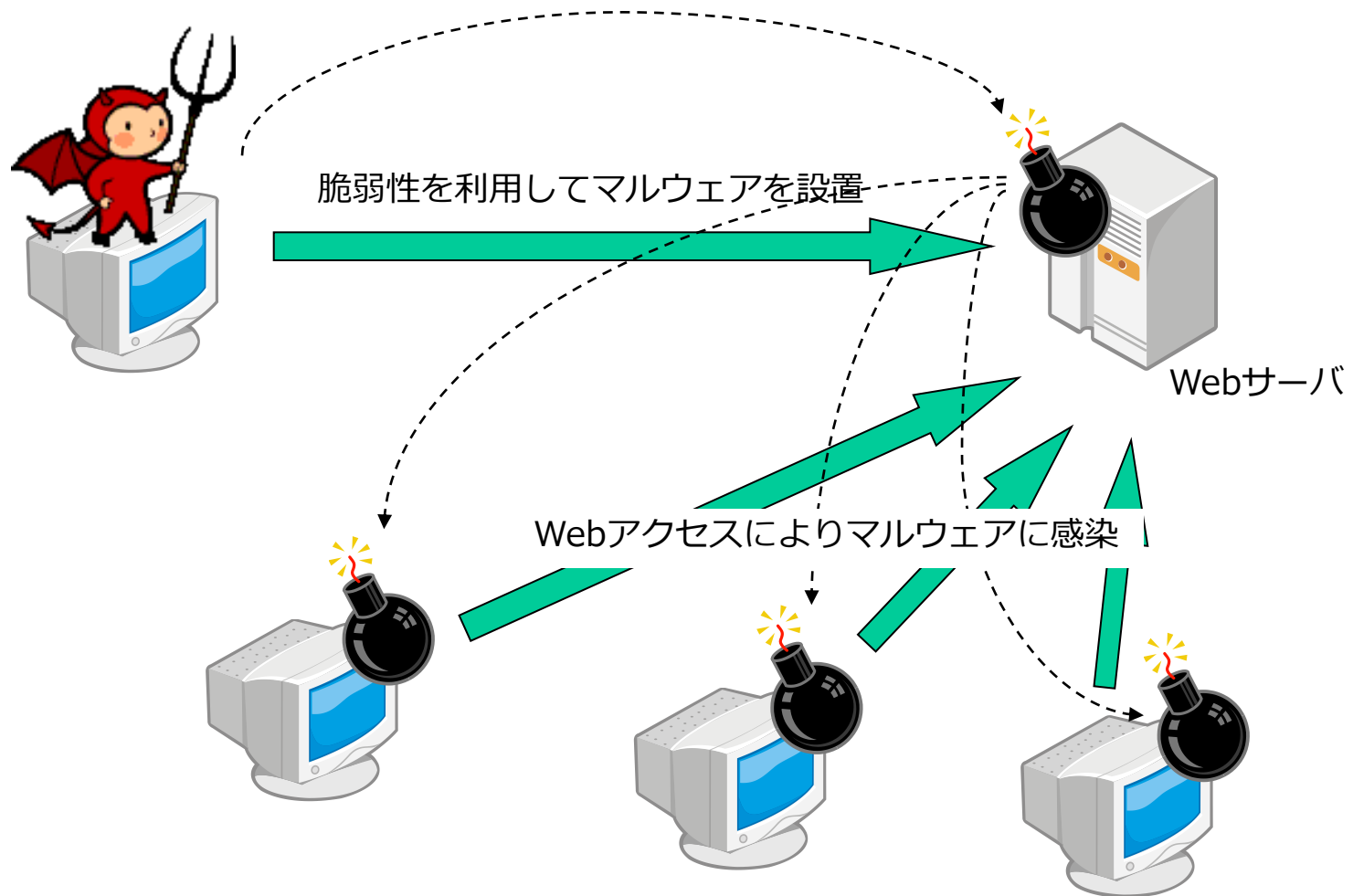
□ 特定組織や特定のユーザ群にターゲットを絞って攻撃

- 関係者を装って電子メールを送信し、添付ファイルを開かせたり、不正サイトへのリンクをクリックさせたりしてセキュリティ侵害を引き起こす
- ターゲットを絞ることで検知される確率が低くなるとともに、攻撃成功の確率を高めることが可能



Webアクセスによるマルウェア感染

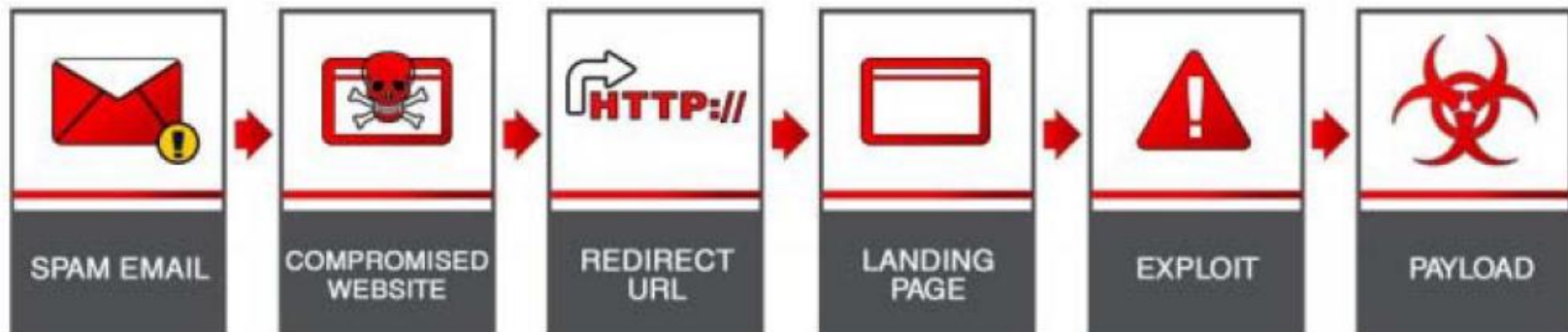
□ Webアクセスによるマルウェア感染のイメージ



Webアクセスによるマルウェア感染 (つづき)

□ クライアントPCの脆弱性を利用して感染

- Blackhole Exploit Kit . . . マルウェア感染の仕組みを提供
- 複数の脆弱性をサポートし、効果的なマルウェア感染を実現
 - Windows/IE/Adobe Reader/Flash Player/Java



(「Blackhole Exploit Kit: A Spam Campaign, Not a Series of Individual Spam Runs」のFigure 1より引用、
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf)

□ ユーザにソフトウェアをインストールさせることで感染

- 偽セキュリティ対策ソフト、偽フリーソフト、海賊版キー生成ツール、等

Webアクセスによるマルウェア感染 (つづき)

□ Webアクセス → 偽のセキュリティチェック実行 → マルウェア感染



The screenshot shows a Windows XP desktop environment. On the left is the Start menu with 'System Tasks' and 'Other Places'. The main area shows 'System folders' (Shared Documents, My Documents), 'Hard drive' (C:), and 'Security' (Microsoft Secure Kit). A progress bar indicates 'Checking: DBLSPACE.BAT' at 75%. A red banner at the bottom states 'Your Computer is infected' with a list of detected malware: Trojan Horse IRC, Adware.Win32.Look2me, Trojan.Qoologic - Key Logger, Trojan.Fakealert, and Trojan virtumonde. A 'Windows Security Alert' dialog box is open, displaying a list of detected spyware and adware with their filenames and severity levels.

Detected spyware and adware on your computer:	Filename:
Adware.Win32.Winad	noise.dat
W32.Yaha.B@mm	emptyregdb.dat
Magic DVD Ripper	mpr.dll
Trojan-PSW.Win32.LdPinch.abm	ieakui.dll
Trojan virtumonde	SET3.tmp
Trojan.Fakealert.355	country.sys

Spyware	Critical
Spyware	High
Spyware	Medium
Spyware	Critical

0-day (ゼロデイ) 攻撃

□ 防御が困難な「0-day攻撃」

- パッチが提供されていない脆弱性 . . . 0-day脆弱性
- 攻撃に利用できる0-day脆弱性はアンダーグラウンドで高値で売買

□ IEの0-day脆弱性 (CVE-2012-4969)

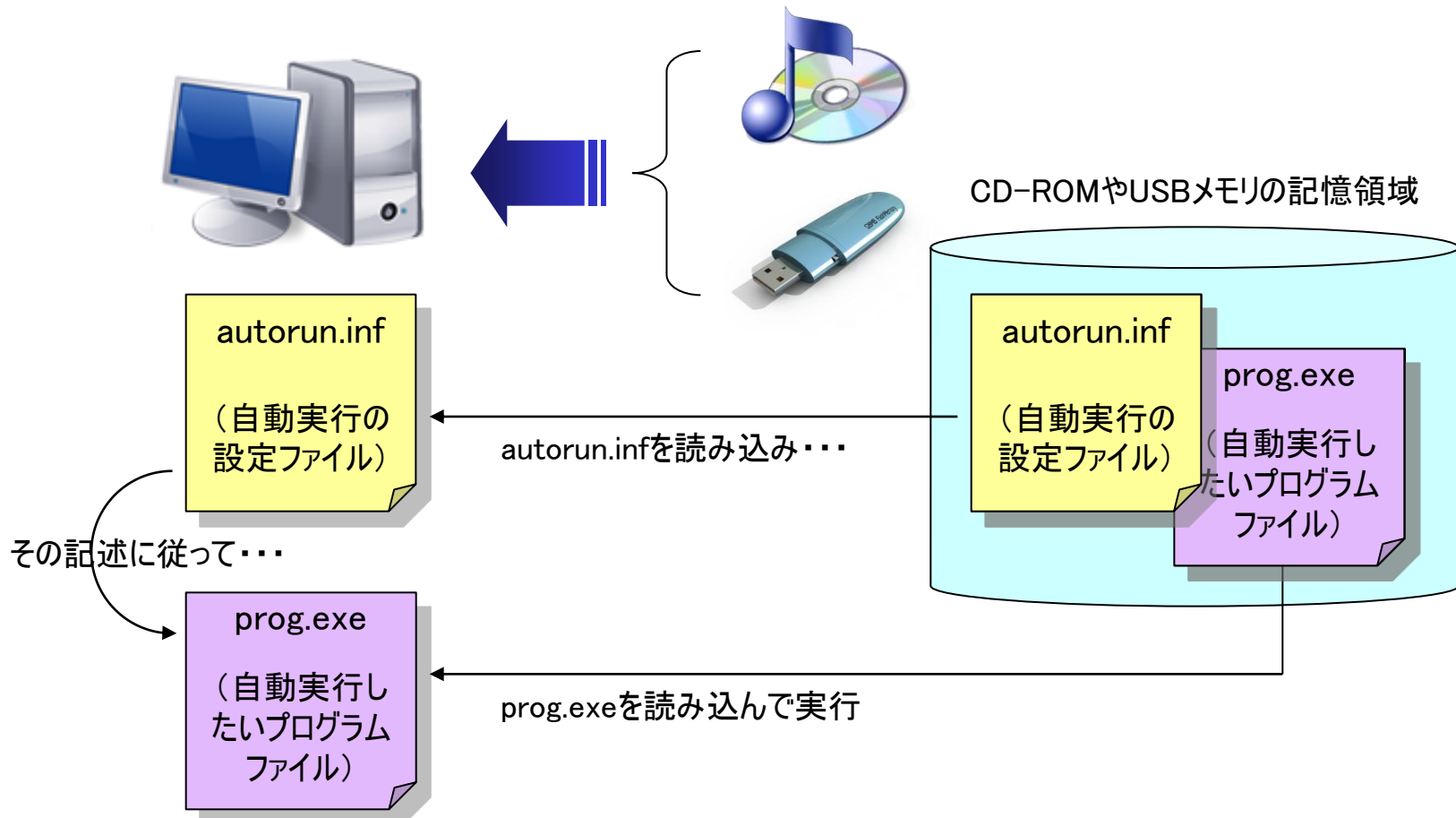
- マイクロソフト セキュリティ アドバイザリ (2757760)
 - <http://technet.microsoft.com/ja-jp/security/advisory/2757760>
- 解放したメモリを再利用するバグ (Use-After-Free) が脆弱性として存在
- MS12-063にてフィックス (2012年9月)
- IEで不正なWebページにアクセスすることによりシェルコードが実行

□ Java7の0-day脆弱性 (CVE-2012-4681)

- 不正なJavaアプレットを読み込むことで任意のコードが実行
- Java7 update7で修正 (2012年8月)
- 各種ブラウザ経由で各種OS (Windows/Linux/OS X等) を攻撃可能

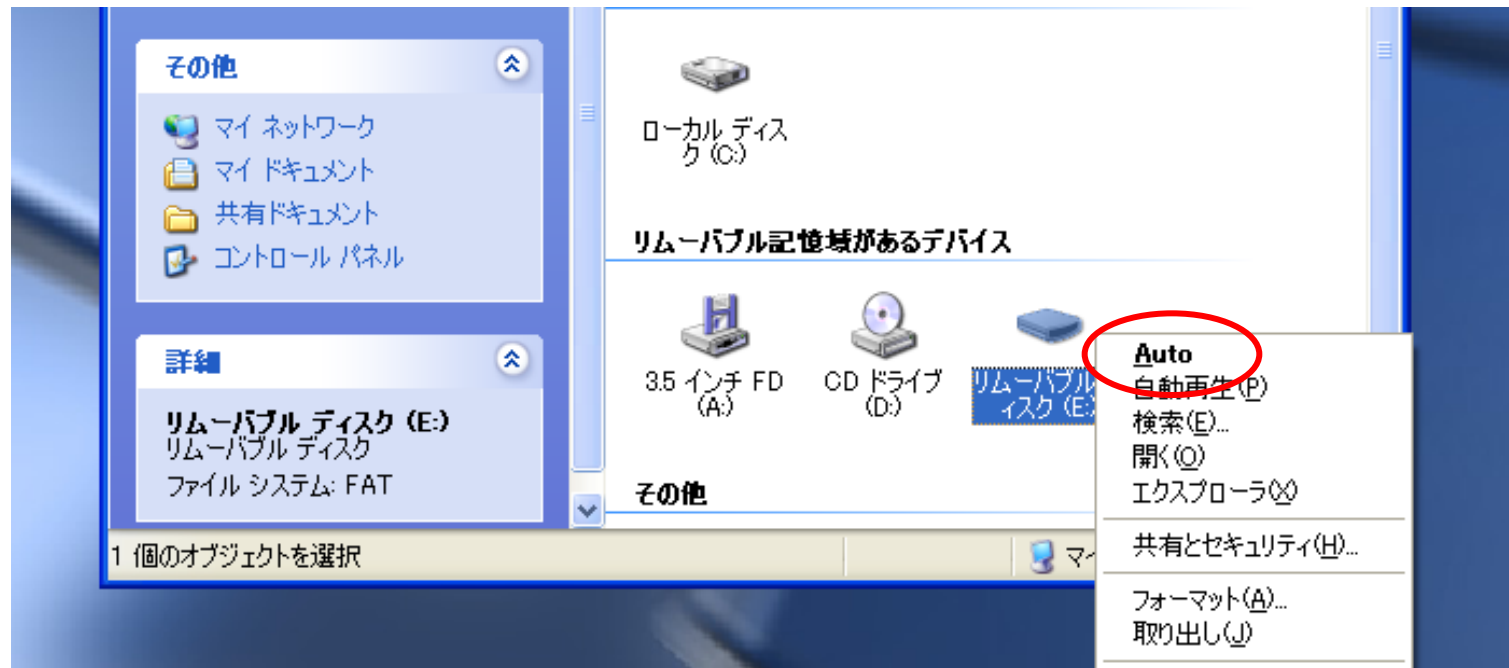
USBメモリのAutorunによるマルウェア感染

□ Autorunの仕組み



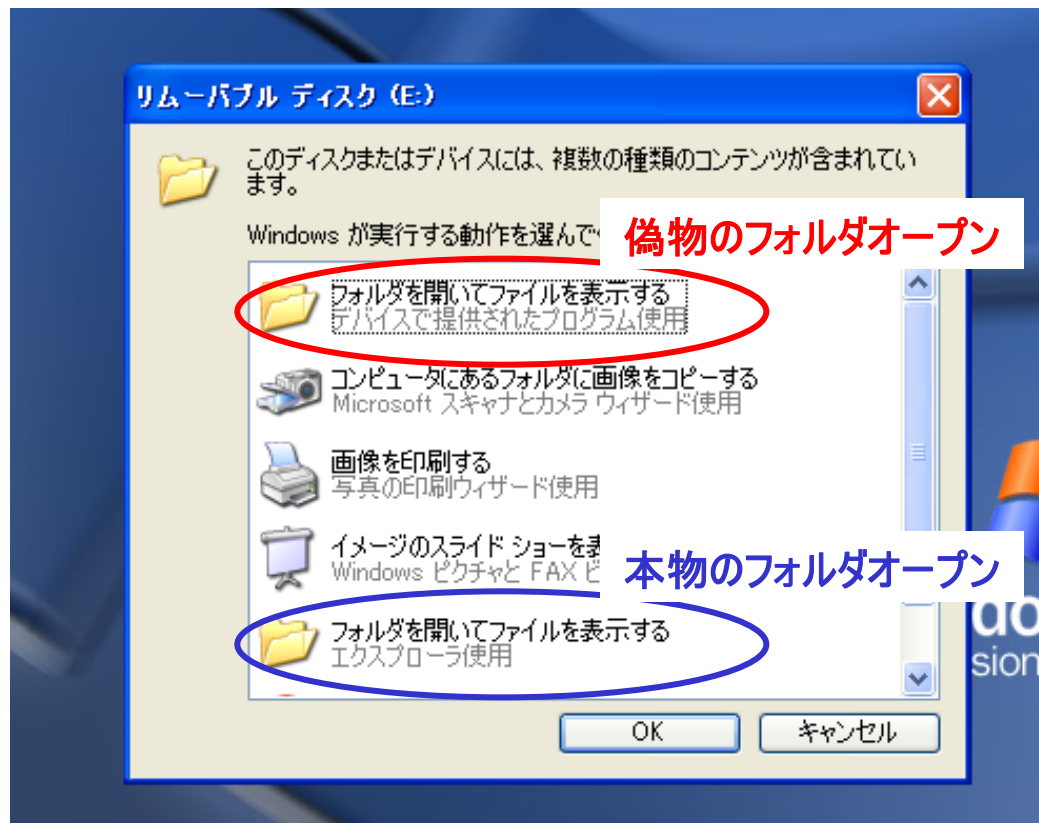
USBメモリのAutorunによるマルウェア感染 (つづき)

- USBメモリのドライブアイコンをダブルクリックすることで感染



USBメモリのAutorunによるマルウェア感染 (つづき)

- 自動再生ダイアログで偽のフォルダオープンを選択することで感染

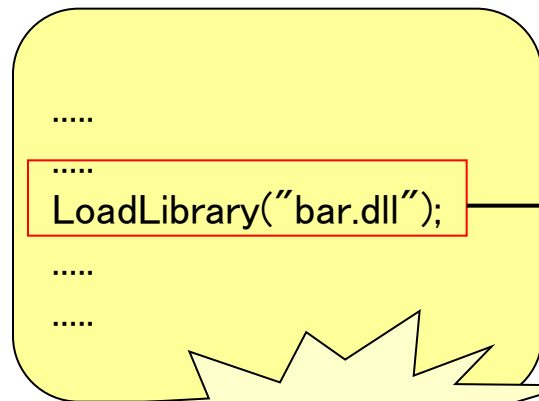


- 最新状態のWindowsは、USBメモリではAutorunしないように改善

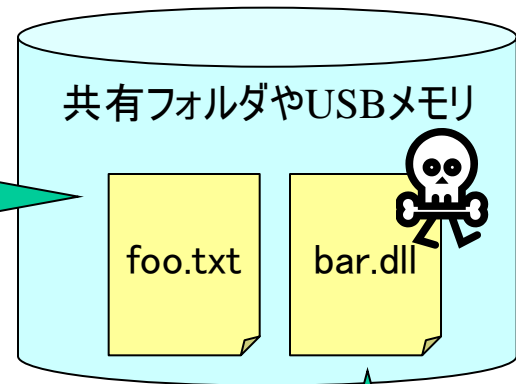
バイナリ・プランティング攻撃

□ バイナリ・プランティング攻撃の例

脆弱なソフトウェア(例:テキストエディタ)



① ダブルクリックして起動



② bar.dllのサーチ

アプリケーション起動ディレクトリ ... Not Found

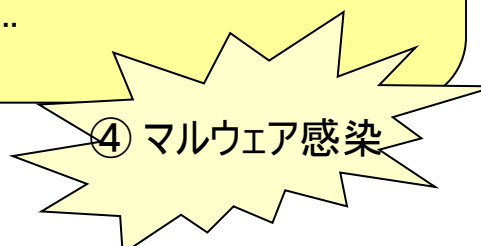
System32ディレクトリ ... Not Found

Systemディレクトリ ... Not Found

Windowsディレクトリ ... Not Found

カレントディレクトリ ... Found !!

③ DLLファイルをロード



バイナリ・プランティング攻撃 (つづき)

□ LoadLibraryのサーチパス (DLLファイルのロード)

1. アプリケーションの起動ディレクトリ
2. System32ディレクトリ
3. Systemディレクトリ
4. Windowsディレクトリ
5. カレントディレクトリ
6. PATHに指定されたディレクトリ



□ WinExecのサーチパス (EXEファイルの起動)

1. アプリケーションがロードされたディレクトリ
2. カレントディレクトリ
3. Windows のシステムディレクトリ
4. Windows ディレクトリ
5. 環境変数 PATH に記述されている各ディレクトリ



バイナリ・プランティング攻撃 (つづき)

□ さまざまなバイナリ・プランティングの脆弱性

ID	タイトル	公表日
JVNDB-2010-001999	WindowsプログラムのDLL読み込みに脆弱性	2010/08/26
JVNDB-2010-000037	LhaplusにおけるDLL読み込みに関する脆弱性	2010/10/12
JVNDB-2010-000045	TeraPadにおけるDLL読み込みに関する脆弱性	2010/10/21
JVNDB-2010-000047	SleipnirおよびGraniにおけるDLL読み込みに関する脆弱性	2010/10/22
JVNDB-2011-000010	Operaにおける実行ファイル読み込みに関する脆弱性	2011/02/02
JVNDB-2011-000022	Picasaにおける実行ファイル読み込みに関する脆弱性	2011/03/25
JVNDB-2011-000060	WindowsのURLプロトコルハンドラにおける実行ファイル読み込みに関する脆弱性	2011/08/10
JVNDB-2012-000034	複数のジャストシステム製品におけるDLL読み込みに関する脆弱性	2012/04/24

(JVN脆弱性対策情報データベースより、<http://jvndb.jvn.jp/index.html>)

バイナリ・プランティング攻撃 (つづき)

□ バイナリ・プランティング攻撃の防御の難しさ

- 一般的なプログラミングにより脆弱性が発生
 - 多数のソフトウェアが潜在的に脆弱
- 利用者が少ないソフトウェアの脆弱性は誰も指摘しない
 - 0-day攻撃になる可能性が高い
- 特定の環境で使用される特定のソフトウェアの脆弱性 (制御システム等)
 - 標的型攻撃のターゲットとして利用 (Stuxnetで実際に発生)

□ レジストリ設定によるカレントディレクトリパスの無効化

- 「DLL検索パス アルゴリズムを制御する新しいCWDIllegalInDllSearchレジストリ エントリについて」
 - <http://support.microsoft.com/kb/2264107/ja>
- ただしEXEのカレントディレクトリパスは無効化されない

権限の昇格

□ Windowsにおける主要な二つのユーザグループ

■ 一般ユーザ . . . Usersグループ所属

- システム領域への書き込み権限がない
- システムに関わる設定変更ができない

■ 管理者ユーザ . . . Administratorsグループ所属

- システムを完全に制御することが可能
- ただし、Vista/7ではUAC（ユーザアカウント制御）によって権限が削除
- 権限昇格することにより、管理者としての権限が付与

□ マルウェアがシステムを完全に制圧するためには、管理者権限やシステム権限が必要 → 権限昇格攻撃

UAC（ユーザアカウント制御）とは

- 管理者権限がなくても日常的な操作を可能
 - タイムゾーンの設定、電源管理、フォントのインストール、プリンタの追加、VPNの構成、無線LAN設定、・・・

- 必要に応じてダイアログを表示し、管理者に権限昇格
 - 一般ユーザ・・・管理者のパスワード入力（資格情報を求める）
 - 管理者ユーザ・・・実行の確認（同意を求める）

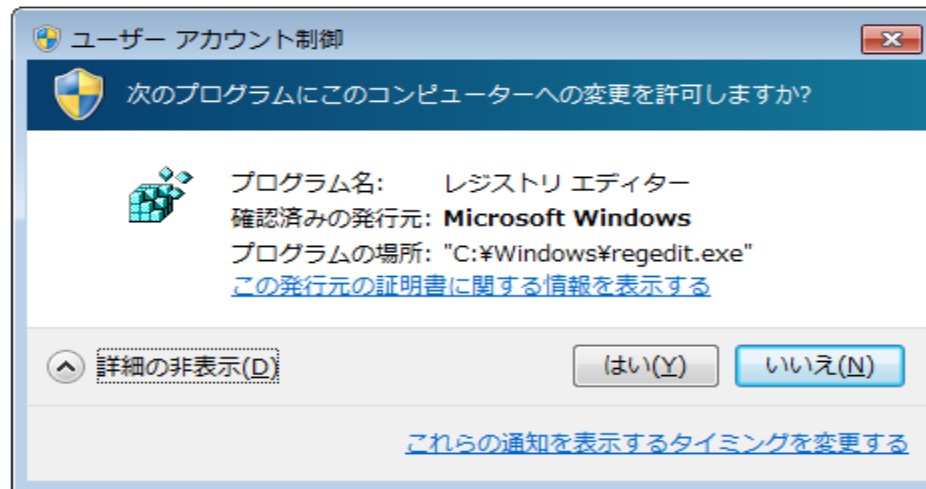
- 整合性レベルによるアクセス制御 → プロセス等のオブジェクトをレベル分けすることで、低レベルプロセスからのアクセスを制限

- ファイルシステムとレジストリの仮想化 → 一般ユーザによるレガシーアプリケーションの実行を支援

UACのバイパス攻撃 – その1

□ Metasploit Frameworkの「BypassUAC」

- UACにより、管理者ユーザでも通常は一般ユーザ並みの権限しかない
- つまりシステム領域への書き込みには権限昇格が必要
- 権限昇格時には通常「権限昇格ダイアログウィンドウ」が表示



- BypassUACはUACの例外措置である「自動昇格（ダイアログを出さずに権限昇格）」するプログラムを悪用し、ダイアログウィンドウを表示させずに権限昇格を実行

UACのバイパス攻撃 – その2

□ バイナリ・プランティングを利用した権限昇格

- マルウェア「ZeroAccess」にて実装
- Flash Playerのインストールプログラム「InstallFlashPlayer.exe」を利用
- 一時フォルダに正規のInstallFlashPlayer.exeおよび不正なDLLファイルを設置し、InstallFlashPlayer.exeを起動 → 不正なDLLが自動的にロード
- ユーザがAdobeのFlash Playerだと勘違いして「Yes」を押すことを期待



(「ZACCESS/SIREFEEF Arrives with New Infection Technique」のfigure2およびfigure3より引用、
<http://blog.trendmicro.com/trendlabs-security-intelligence/zaccesssirefef-arrives-with-new-infection-technique/>)

一般的なセキュリティ対策の限界

- パッチ適用の限界
 - 0-dayの脆弱性・・・そもそもパッチが存在しない
 - 運用上の問題でパッチが適用できないケース（互換性問題、隔離環境）

- ウィルス対策ソフトの限界
 - 「シグネチャ方式」では新種や亜種への対応が困難

- ファイアウォールの限界
 - Webアクセス、メール添付、USBメモリ、共有フォルダ、・・・

- 危険なWebサイトへはアクセスしない！？？？
 - 普通のWebサイトがマルウェア配布サイトに

- 不審な添付ファイルは開かない！？？？
 - 巧妙化かつ一般化する標的型攻撃

マルウェア感染において防止すべき三つのポイント

□ シェルコードの実行

- メモリ破壊系の脆弱性を利用（バッファオーバーフロー等）
- ネットワーク・ワーム、Webアクセス、メール添付ファイル、・・・

□ 不正なプログラムファイルの実行

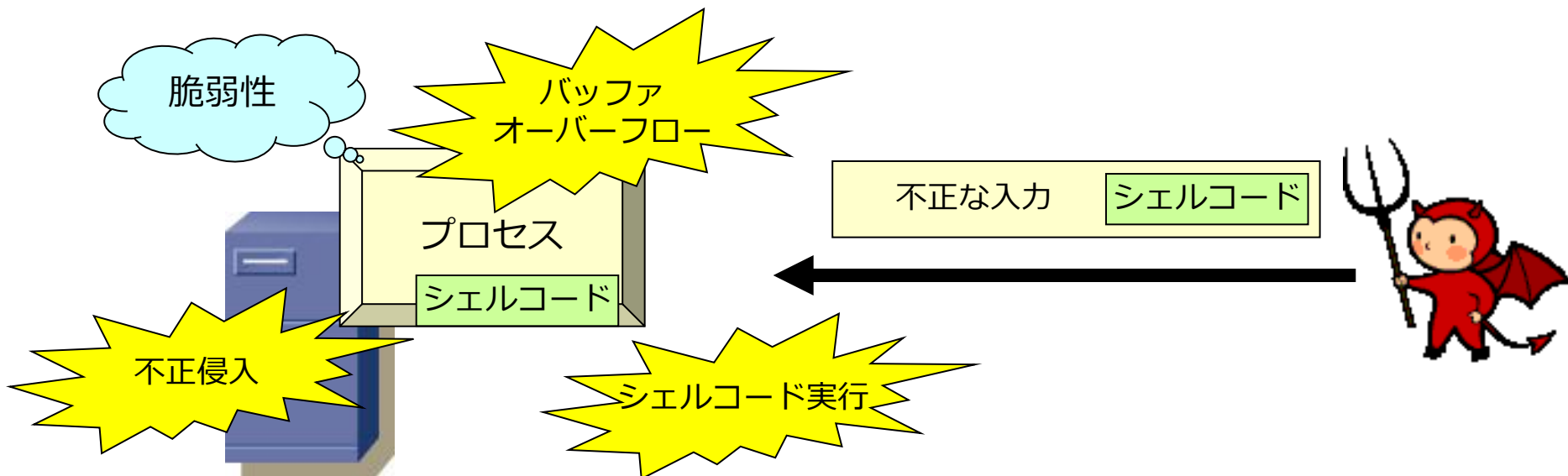
- 脆弱性を利用する（ドライブ・バイ・ダウンロード等）
- ユーザを欺いて実行させる（偽のマルウェア検査実行等）
- OSの機能を悪用する（Autorunによる実行等）
- Webアクセス、メール添付ファイル、USBメモリ、共有フォルダ、・・・

□ 管理者権限やシステム権限の取得

- 特定の利用者権限を不正に取得 → 管理者権限に昇格
- そもそも管理者権限でマルウェアに感染

シェルコードとは

- バッファオーバーフロー攻撃などで用いられる、不正行為を行う実行コード
- 「shellを実行させるコード」が語源
- ターゲットプロセスのメモリ中に挿入し、プロセスの処理をシェルコードに移すことで実行



Windowsにおけるシェルコード実行の防御機能

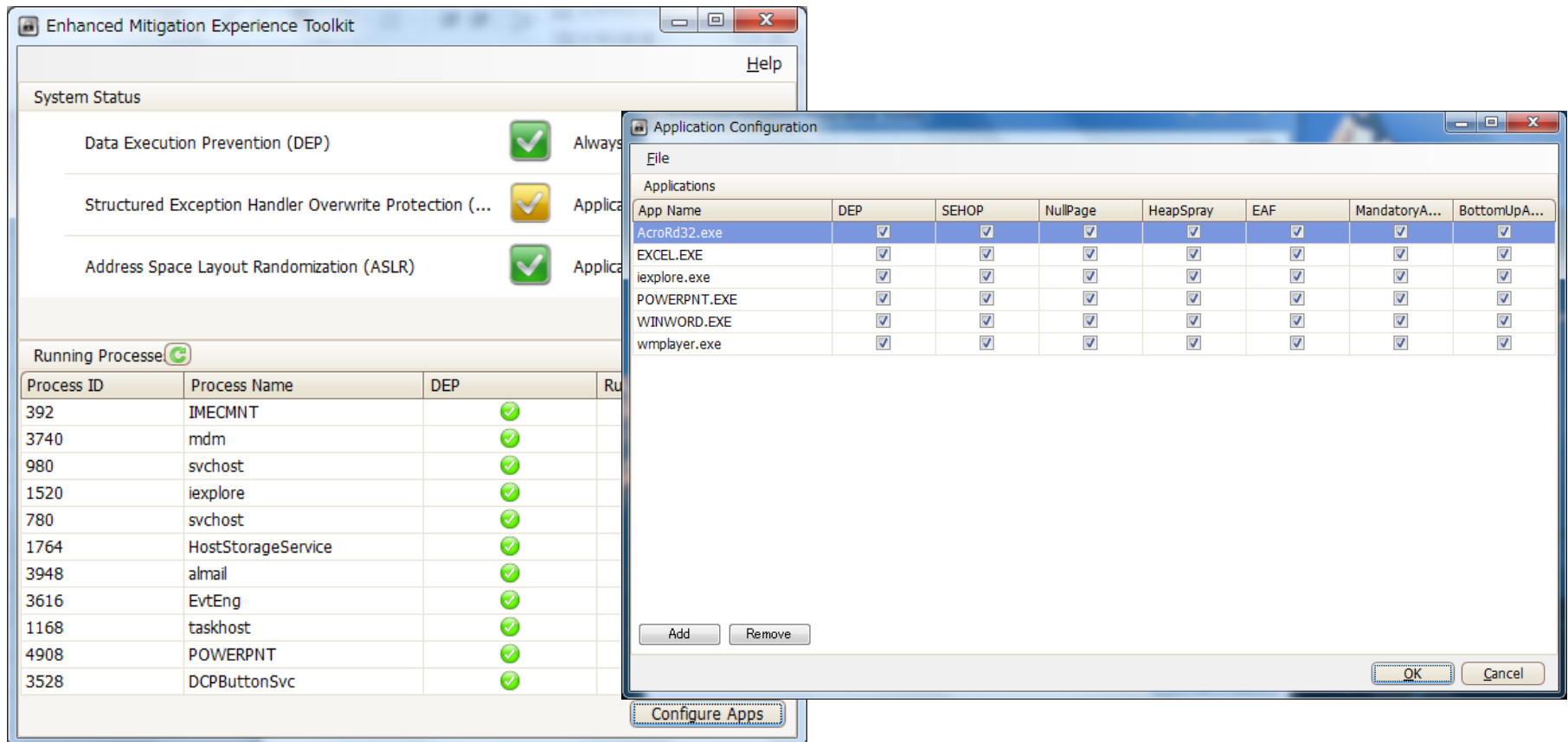
- DEP (Data Execution Prevention : データ実行防止)
 - Windows XP SP2から実装
 - メモリ中のデータ領域でのコード実行を防止 (ハードウェアDEP)
 - XPやWin7のデフォルトは特定のプロセスのみが保護 (オプトイン設定)
 - 既知のコードアドレスを利用することで比較的容易に回避することが可能 (Return-to-libc、ROP攻撃)
- ASLR (Address Space Layout Randomization)
 - Vistaから実装 (一部機能はXPSP2より)
 - メモリ中のプログラムコードやスタック/ヒープのベースアドレスをランダム化
 - アドレス位置を不定にすることで攻撃をやりにくくする
 - すべてのプログラムやDLLについてASLRが有効になっているわけではない
 - 攻撃者はASLRが無効状態のコードを利用 (Java6のmsvcr71.dll等)
- その他
 - スタック保護、ヒープ保護、例外ハンドラ保護 (SafeSEH、SEHOP) 、 等

EMET : Enhanced Mitigation Experience Toolkit

- マイクロソフトが公開しているシェルコード実行防止ツール
- Windows標準のシェルコード防御機能を補強
 - ダイナミックDEP
 - SEHOP拡張
 - 強制ASLR
 - ヒープスプレイ・アロケーション
 - Nullページ・アロケーション
 - EAT (Export Address Table) フィルタリング
 - ボトムアップASLR
 - ROP攻撃対策 (v3.5 Tech Preview版)
 - ロードライブラリ・チェック
 - メモリ保護チェック
 - 呼び出し元チェック
 - 実行フロー・シミュレーション
 - スタック・ピボットの検知

EMET : Enhanced Mitigation Experience Toolkit (つづき)

- プロファイルによる構成、グループポリシー対応、レポート機能
- EMETを導入し、アプリケーションごとに設定することで安心感UP！



System Status

- Data Execution Prevention (DEP) Always
- Structured Exception Handler Overwrite Protection (SEHOP) Application
- Address Space Layout Randomization (ASLR) Application

Running Processes

Process ID	Process Name	DEP	Run
392	IMECMNT	<input checked="" type="checkbox"/>	
3740	mdm	<input checked="" type="checkbox"/>	
980	svchost	<input checked="" type="checkbox"/>	
1520	iexplore	<input checked="" type="checkbox"/>	
780	svchost	<input checked="" type="checkbox"/>	
1764	HostStorageService	<input checked="" type="checkbox"/>	
3948	almail	<input checked="" type="checkbox"/>	
3616	EvtEng	<input checked="" type="checkbox"/>	
1168	taskhost	<input checked="" type="checkbox"/>	
4908	POWERPNT	<input checked="" type="checkbox"/>	
3528	DCPButtonSvc	<input checked="" type="checkbox"/>	

Application Configuration

App Name	DEP	SEHOP	NullPage	HeapSpray	EAF	MandatoryA...	BottomUpA...
AcroRd32.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EXCEL.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
iexplore.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
POWERPNT.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WINWORD.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
wmplayer.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Add, Remove, OK, Cancel

SRP : ソフトウェア制限ポリシー

- XPから導入されたプログラムの実行を制限する機能（Homeエディションは除く）

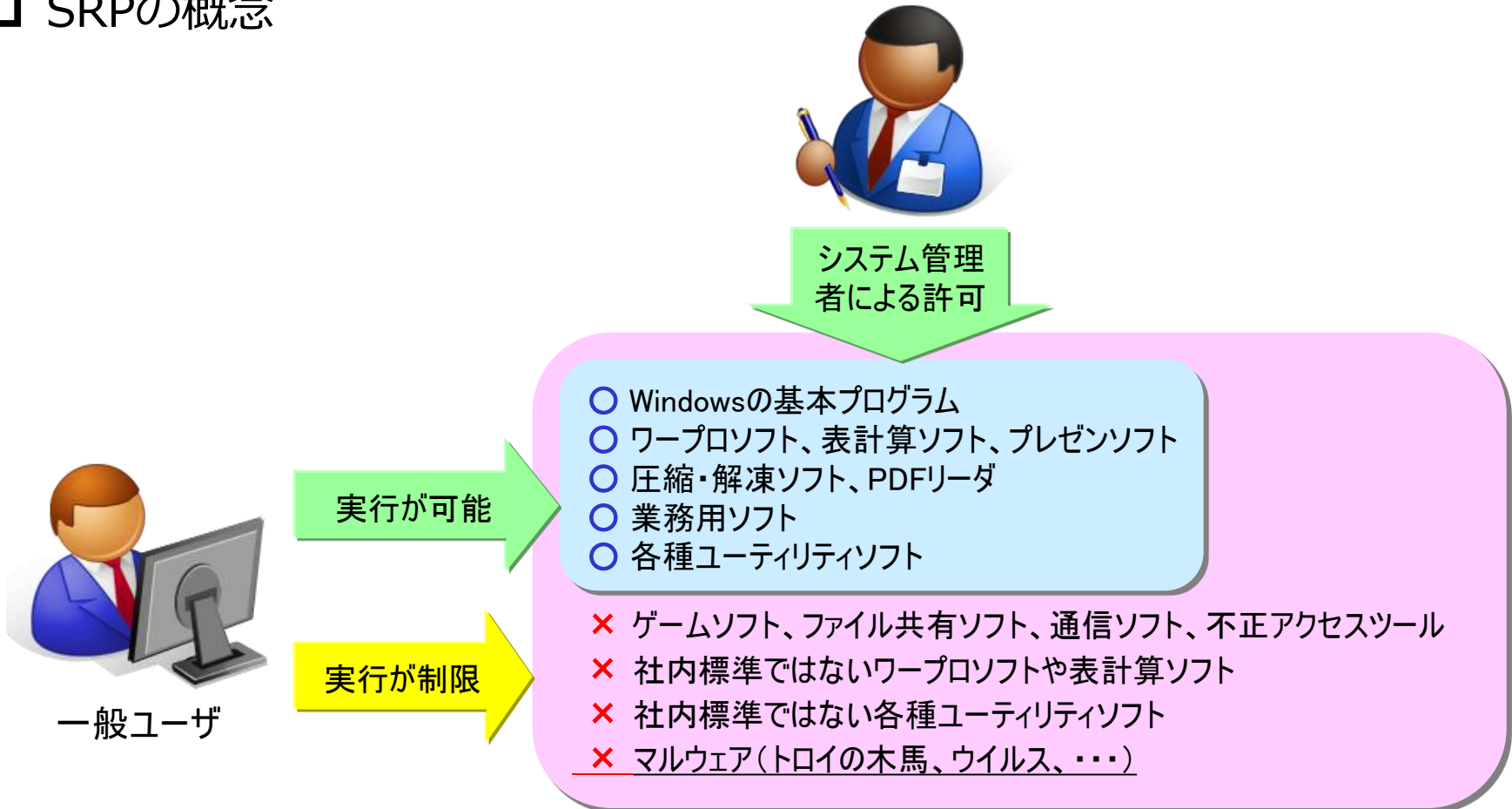
- 次の4種類の方法で規制
 - ハッシュの規則
 - 証明書の規則
 - パスの規則
 - インターネットゾーンの規則

- 一般ユーザに対して規則を適用することにより、一般ユーザ権限では指定されたプログラム以外は実行できなくなる

- 有害なプログラムがユーザの意図に反して実行されることを防ぐ効果

SRP : ソフトウェア制限ポリシー (つづき)

□ SRPの概念



(「ソフトウェア制限ポリシーによるマルウェア対策」より引用、<http://www.st.rim.or.jp/~shio/winsec/srp/>)

AppLocker

- Windows 7 (Ultimate/Enterprise) およびWindows Server 2008 R2で導入されたソフトウェア制限ポリシー (SRP) の後継機能
 - 発行元、パス、ハッシュの規則で制限
 - 実行可能ファイル、Windowsインストーラ、スクリプトに対する設定
 - ユーザやグループに対する制限
 - 監査モードによる規則のテスト
 - 複数規則を一度に作成するウィザード
 - ポリシーのインポート/エクスポート
 - PowerShellによるAppLockerポリシーの管理

UACを過信しない！！

- Vista . . . UACが厳密に設定
 - すべての権限昇格でダイアログウィンドウが表示
 - 利便性が損なわれたため、利用者には不評（ダイアログがうざい！）

- Windows 7 . . . UACのデフォルト設定がやや緩め
 - 管理者ユーザが特定のプログラムで権限昇格する場合、ダイアログを表示しない
 - 利便性は向上したが、 BypassUAC（前述）のような攻撃を可能に . . .

- 管理者ユーザであっても常に一般ユーザアカウントでログオンして使用するか、UAC設定をMAXにして運用することが推奨

- XPの場合は？？？ . . . がんばって一般ユーザで使いましょう！

Catch, Patch, Match

- オーストラリア国防信号局（DSD）が提唱するスローガン
 - Catch . . . ホワイトリストによるプログラム実行制限
 - Patch . . . OSやアプリケーションソフトのパッチ適用
 - Match . . . ユーザに適した権限でのコンピュータの使用



(「Catch, Patch, Match video」より引用、<http://dsd.gov.au/videos/catch-patch-match.htm>)

まとめ：マルウェア感染を効果的に防ぐには・・・

- まずは一般的なセキュリティ対策を確実に

- さらに追加的対策として、
 - シェルコードの実行を阻止する
→ EMETの導入および利用が効果的

 - 不正なプログラムファイルの実行を阻止する
→ 意図しないプログラム起動を防ぐためSRP/AppLockerで自身を束縛

 - 不正な管理者権限の取得を阻止する
→ 一般ユーザでの使用を心がける or UACの設定を強化

ご清聴ありがとうございました。

Any Questions ?