

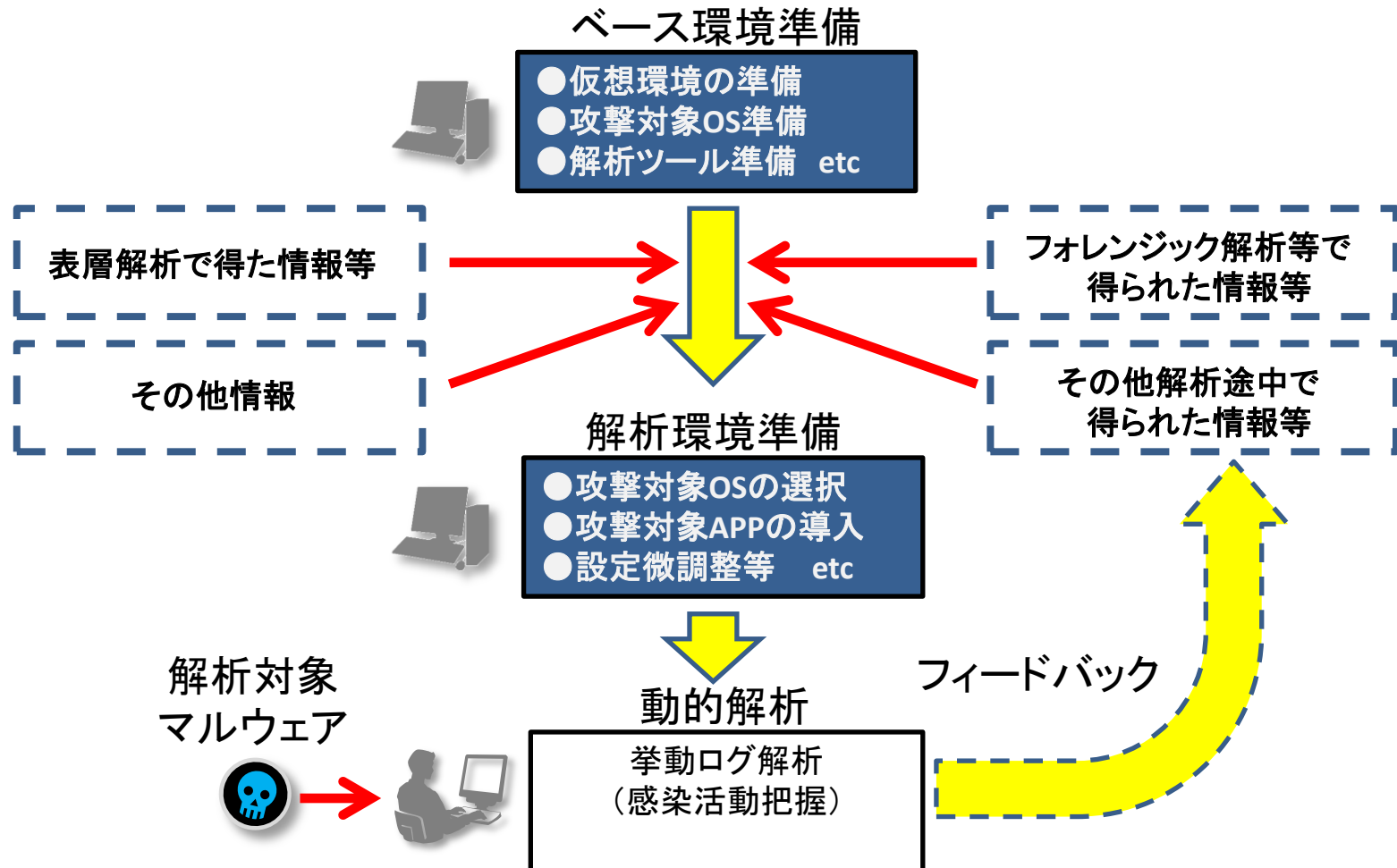
動的解析準備訓練 座学

訓練概要

- 目的
 - 表層解析等で得られた情報等を元に、マルウェアが挙動を示し動的解析が行える環境が構築できる様にする
- 種別
 - マルウェア動的解析
- 事前知識
 - 表層解析の基礎、Windows及びLinuxのネットワーク設定
 - 模擬サーバ(INetSim、NetCat、FakeDNS等)
- 習得技術
 - 動的解析環境の構築
- 対象
 - 一般隊員

動的解析環境の準備

・ 環境準備の流れ



ベース環境の準備

• 仮想環境

- 感染からの復旧・解析リトライの容易性 ⇒ 仮想環境の利用が基本
- 仮想環境を検知するマルウェアの台頭 ⇒ 物理端末の利用や設定見直しが必要



• 攻撃対象OS

- 組織内の守るべきシステム環境の存在 ⇒ 使われているOSが基本
- 感染による挙動のし易さ(脆弱な環境) ⇒ 脆弱性緩和策の無効化
- 64bit OSに特化したマルウェアの台頭 ⇒ 64bit OSの利用が必要



• 模擬サーバ

- C&C等接続による情報漏えい等懸念 ⇒ 模擬サーバの利用推奨



ベース環境の準備

• 動的解析ツール

- ファイルアクセス監視 ⇒ Capture-BAT, Process Monitor 等
- プロセス・タスク監視 ⇒ Process Explorer, Process Monitor 等
- レジストリ監視 ⇒ Autoruns, Regshot, Regedit等
- ネットワーク監視 ⇒ Wireshark, Capture-BAT
- API呼び出し監視 ⇒ API Monitor 等

※各ツールの詳細は「動的解析実践訓練(初級)」にて示す。

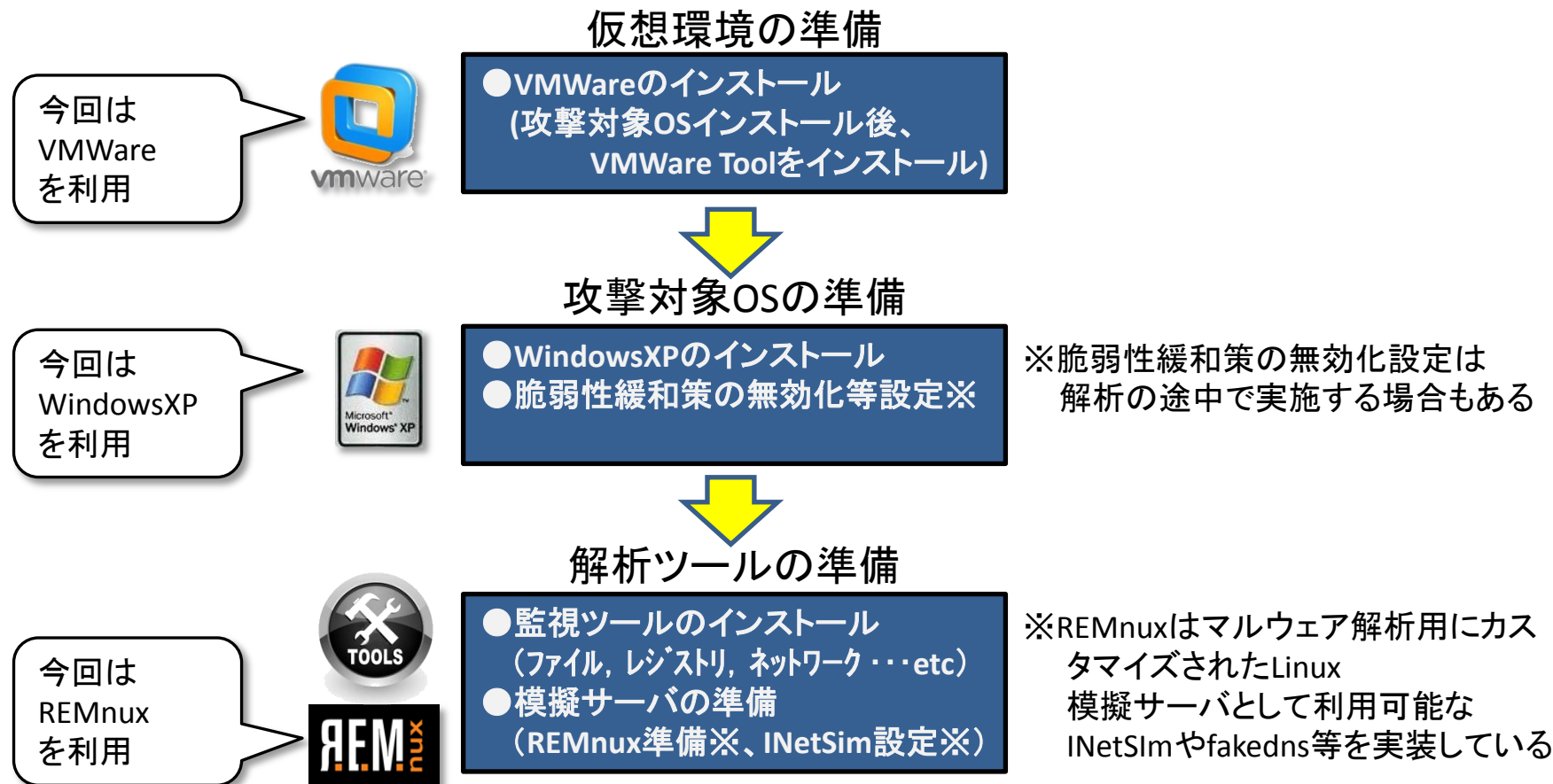
ベース環境の準備

・ ベース環境のイメージ(例)



ベース環境の準備

・ベース環境準備の流れ(例)



補足：脆弱性緩和策

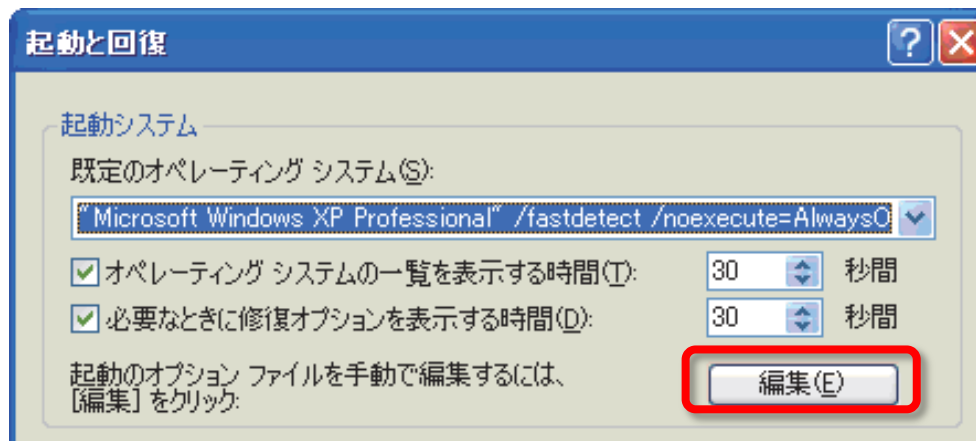
- **Windows XP における脆弱性緩和策 (SP2以降)**
 - DEP (Data Execution Prevention)
 - 実行不可能なメモリ領域からコードを実行することを防止。
 - 例えばバッファオーバーフローを経由してコードを格納し、そのコードを実行しようとする攻撃に効果がある
- **Windows Vista 以降の脆弱性緩和策**
 - ASLR (Address Space Layout Randomization)
 - 重要なデータ領域 の位置を無作為に配置する技術。
 - 攻撃者が標的のアドレスを予測することをより困難にすることによって、その種の攻撃を妨害する
 - UAC (User Account Control)
 - 管理者権限を持つユーザに普段は一般ユーザ権限しか与えず、管理者権限の必要な処理を実行しようとした際に警告ダイアログを表示して本当に実行してよいかユーザに確認する機能

補足：脆弱性緩和策

【参考】

• DEPの無効化(Windows XP)

- Administrator権限で、以下の操作を実施
- ① [スタート]－[コントロールパネル]を選択
- ② “作業する分野を選びます”の“パフォーマンスとメンテナンス”を選択
- ③ “コントロールパネルを選んで実行します”の“システム”を選択
- ④ <<詳細設定>>タブの“起動と回復”の 設定 ボタンをクリック
- ⑤ “起動システム”の 編集 ボタンをクリック

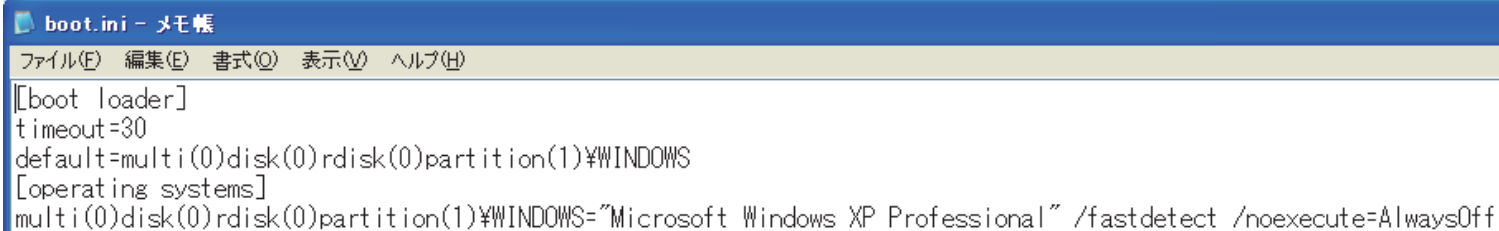


補足：脆弱性緩和策

【参考】

• DEPの無効化(Windows XP)

- ⑥ boot.iniファイルの[operating systems]の次の行を参照



```
boot.ini - メモ帳
ファイル(F)  編集(E)  書式(O)  表示(V)  ヘルプ(H)
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /fastdetect /noexecute=AlwaysOff
```

- ⑦「multi...」の行の記述内容からDEPの状態を調べ、以下の表の最下行と同じ状態になっていない場合には、最下行の記述に修正

boot.iniの記述	DEPの状態
「/noexecute=」の記述がない場合	OptIn（重要なWindowsプログラム等のみ有効）
「/noexecute=OptIn」の場合	OptIn（重要なWindowsプログラム等のみ有効）
「/noexecute=OptOut」の場合	OptOut（例外を除く全てのプロセスでDEP有効）
「/noexecute=AlwaysOn」の場合	AlwaysOn（例外無く全てのプロセスでDEP有効）
「/noexecute=AlwaysOff」の場合	AlwaysOff（DEP無効）

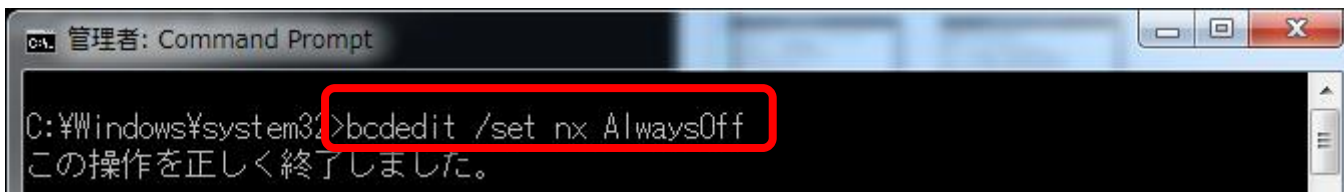
- ⑧PCを再起動

補足：脆弱性緩和策

【参考】

• DEPの無効化（Windows Vista /7）

- Administrator権限で、以下の操作を実施
- ① [スタート]－[すべてのプログラム]－[アクセサリ]を選択
- ② [コマンドプロンプト]で右クリックし、[管理者として実行]を選択
- ③以下の表の最下行のコマンドを実行



設定するDEPの状態	実行コマンド
OptIn に設定する場合	bcdedit /set nx OptIn
OptOut に設定する場合	bcdedit /set nx OptOut
AlwaysOn に設定する場合	bcdedit /set nx AlwaysOn
AlwaysOff に設定する場合	bcdedit /set nx AlwaysOff

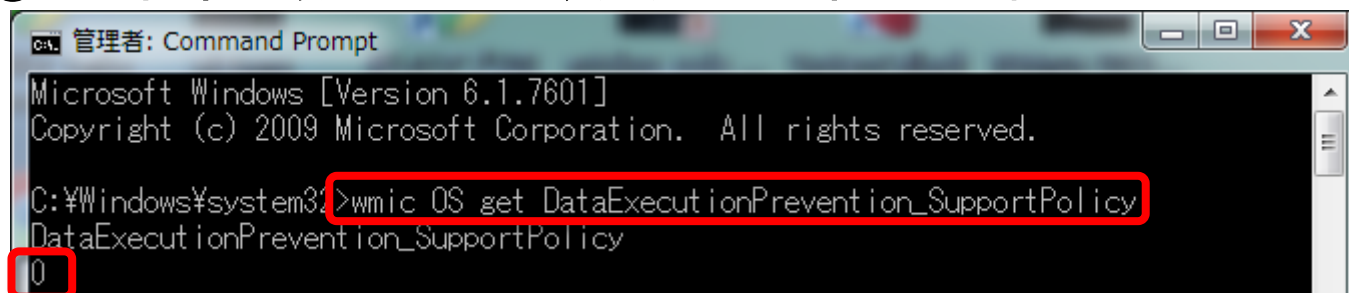
- ④PCを再起動

補足：脆弱性緩和策

【参考】

• DEP状態の確認 (Windows XP / Vista / 7)

- Administrator権限で、以下の操作を実施
- ① [スタート]－[すべてのプログラム]－[アクセサリ]を選択
- ② [コマンドプロンプト]で右クリックし、[管理者として実行]を選択
- ③ コマンド[wmic OS get DataExecutionPrevention_SupportPolicy]を実行
- ④ 出力結果の数値と以下の表を照らし合わせて確認



```
管理者: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic OS get DataExecutionPrevention_SupportPolicy
DataExecutionPrevention_SupportPolicy
0
```

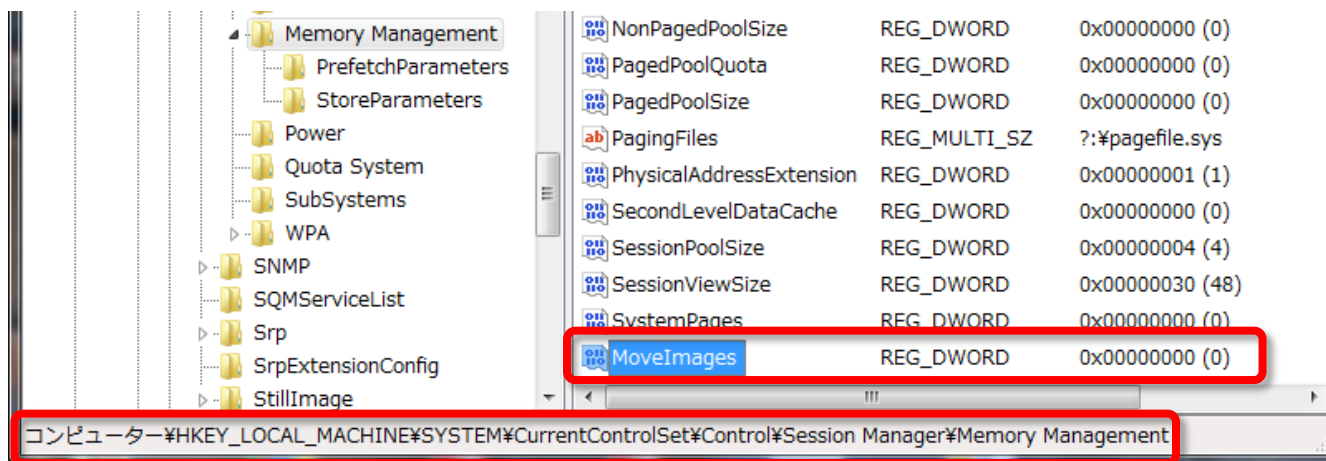
数値	ポリシーレベル	概要
0	AlwaysOff	DEP無効
1	AlwaysOn	例外なく全てのプロセスでDEP有効
2	OptIn	重要なWindowsプログラム・サービスのみ有効
3	OptOut	例外なく全てのプロセスでDEP有効

補足：脆弱性緩和策

【参考】

• ASLRの無効化 (Windows Vista /7)

- Administrator権限で、以下の操作を実施
- ① [スタート]－[プログラムとファイルの検索]枠に[regedit]と入力し実行
- ② サブキー[HKLM¥SYSTEM¥CurrentControlSet¥Control¥Session Manager¥Memory Management]へ移動
- ③値 "MoveImages" に [dword:00000000]を設定

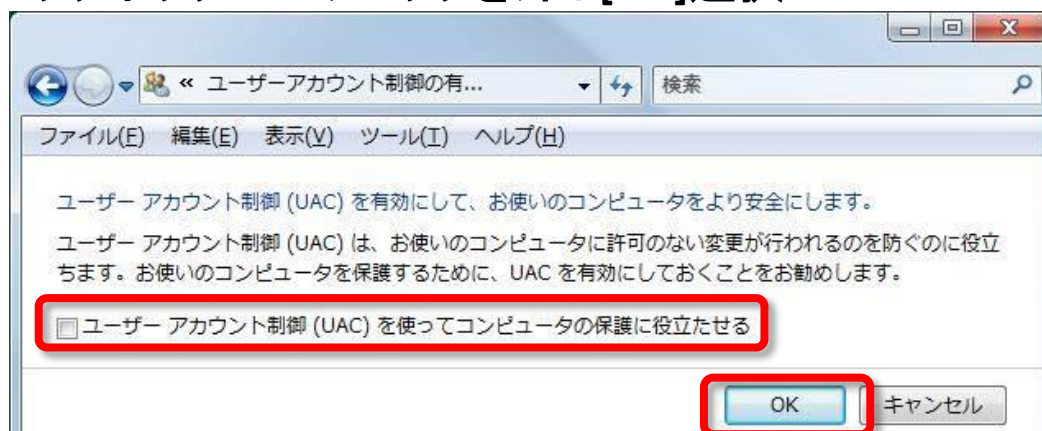


補足：脆弱性緩和策

【参考】

• UACの無効化(Windows Vista)

- Administrator権限で、以下の操作を実施
- ① [スタート]－[コントロールパネル]－[ユーザーアカウントと家族のための安全設定]－[ユーザアカウント制御の有効化または無効化]を選択
- ② [ユーザーアカウント制御]画面で[継続]を選択
- ③ [ユーザーアカウント制御(UAC)を使ってコンピュータの保護に役立たせる]チェックボックスのチェックを外し[OK]選択



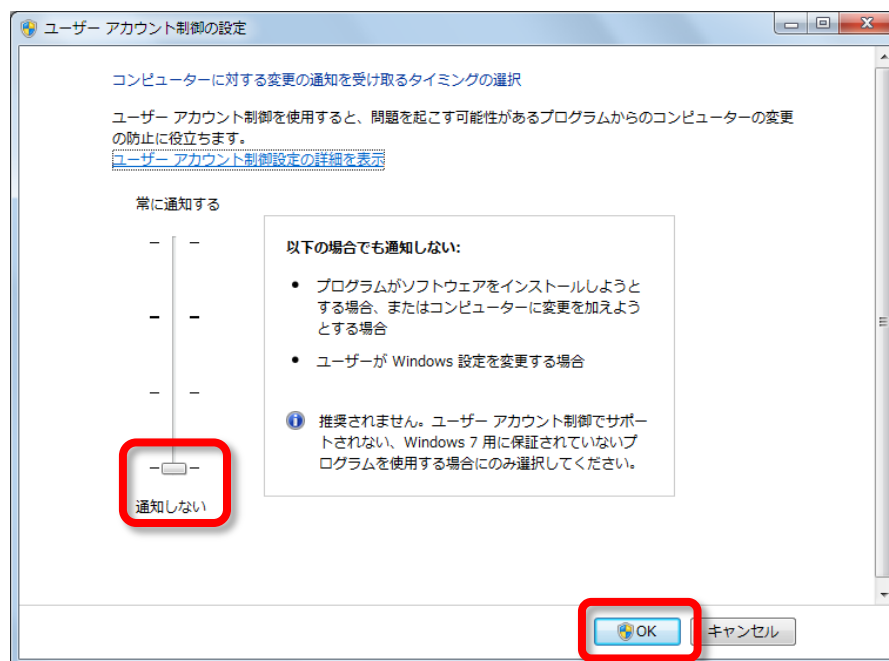
- ④ PCを再起動

補足：脆弱性緩和策

【参考】

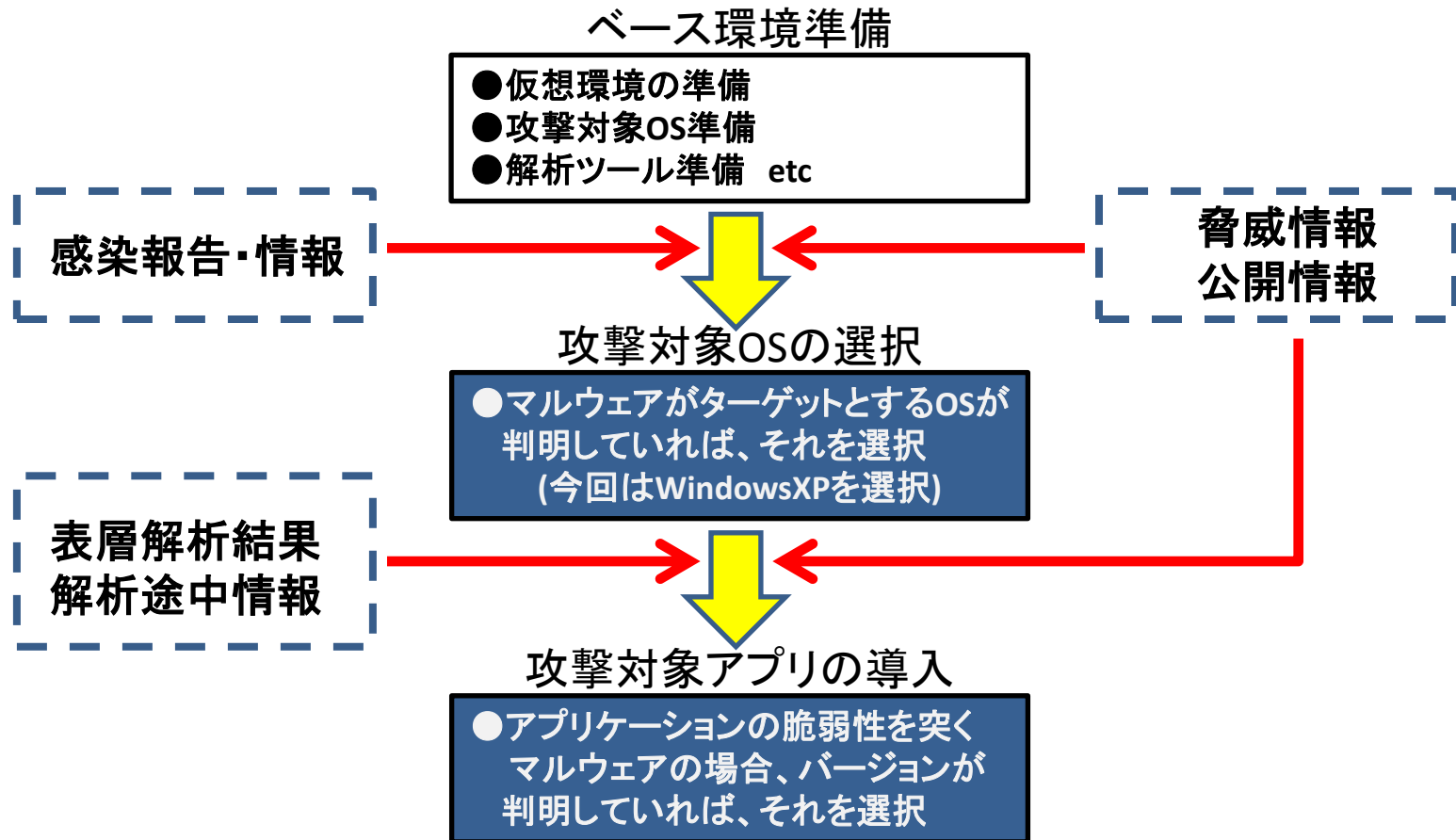
• UACの無効化(Windows 7)

- Administrator権限で、以下の操作を実施
- ① [スタート]ー[コントロールパネル]ー[ユーザーアカウントと家族のための安全設定]ー[ユーザアカウント]ー[ユーザーアカウント制御設定の変更]を選択
- ② 通知の制御レベルを最低の「通知しない」に設定し[OK]選択



マルウェアに合った解析環境

・ 解析環境準備の流れ

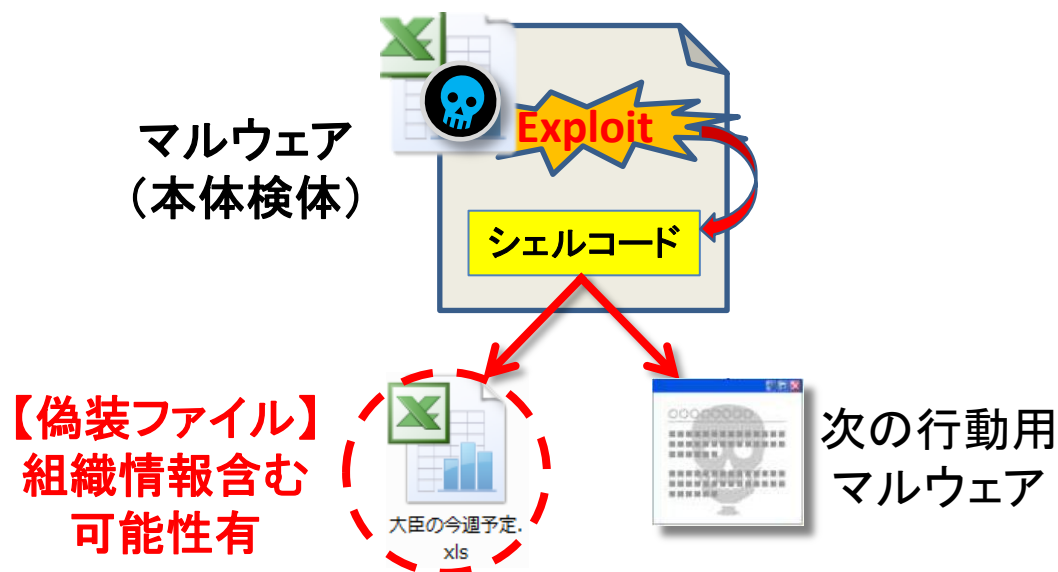


公開情報等利用上の注意

・ オンライン解析サイトの利用

－ 組織情報等の有無

- ・ マルウェアの中には、偽装ファイルとして防衛省やその他省庁等の組織情報を含むファイルを使用する場合がある
⇒ 気付かずに組織情報を外部へ漏えいさせている。
- ・ まずはハッシュ値 (MD5, SHA-1, SHA-256) での検索を推奨



補足：公開情報の一例

【参考】オンライン解析サイト

- **VirusTotal** (<https://www.virustotal.com/ja/>)

- 多数のアンチウイルスエンジンによるオンライン解析
- ハッシュによる検索が可能



- **ThreatExpert** (<http://www.threatexpert.com/>)

- 複数のアンチウイルスエンジンによるオンライン解析
- 地域やカテゴリ等による検索が可能



補足：公開情報の一例

【参考】脆弱性情報データベース

- **CVE - Common Vulnerabilities and Exposures**
(<http://cve.mitre.org/>)

- MITRE社が採番・管理している脆弱性情報DB
- 脆弱性管理製品の多くが利用



- **JVN - Japan Vulnerability Note** (<http://jvn.jp/>)

- JPCERT/CCとIPAが管理している脆弱性情報DB
- 日本の脆弱性情報に焦点が置かれている

