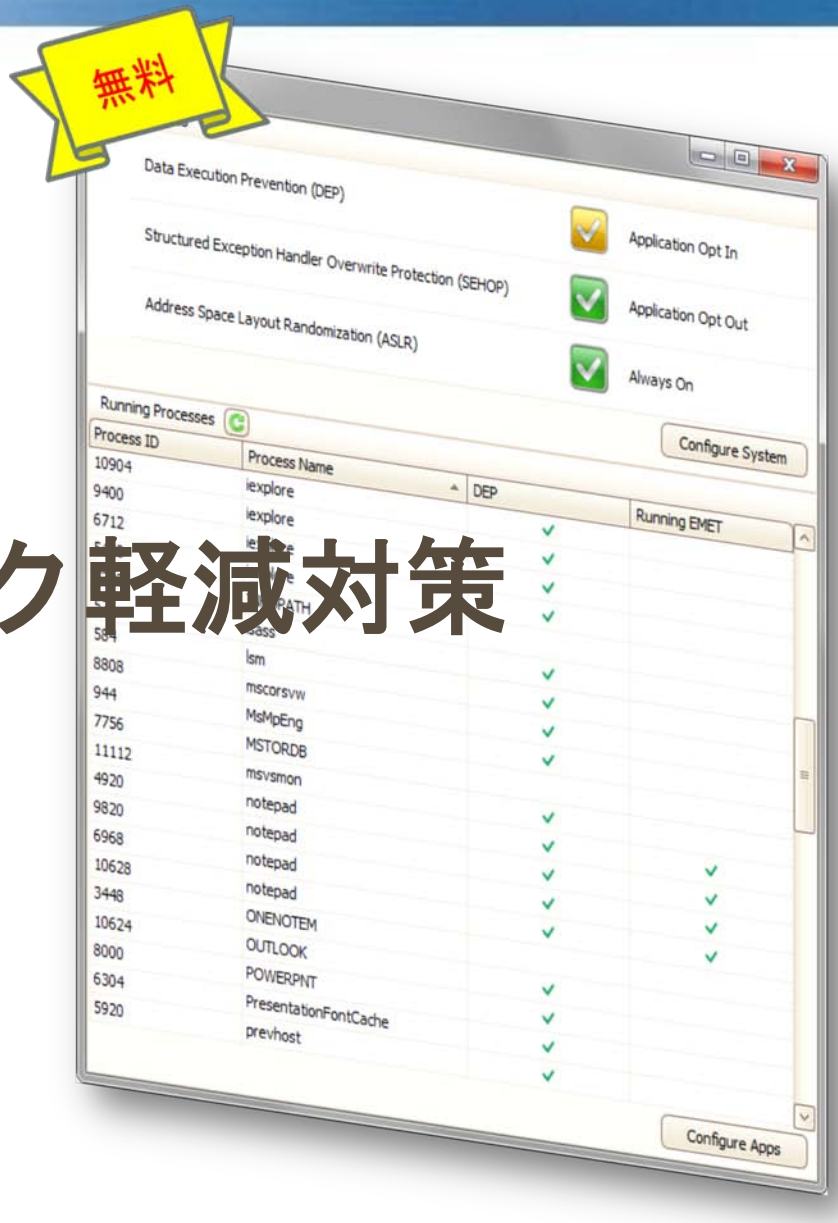
Microsoft Security



制御システムのセキュリティ リスク軽減対策 ～ EMET のご紹介 ～

日本マイクロソフト株式会社
田村 紀恵

2011/2/10

現実化した脅威への対策…課題

- 制御システム防御のための実践的なセキュリティ対策が必要
- 制御システムを狙ったマルウェア Stuxnet
- セキュリティ更新の適用は容易ではない
- ネットワーク境界での防御だけでは不完全
- 最新の防御製品の導入は予算オーバー
- セキュア コーディングのための開発コストはかけられない
- 古いアプリケーションの対策手段がない




Microsoft Security

アジェンダ

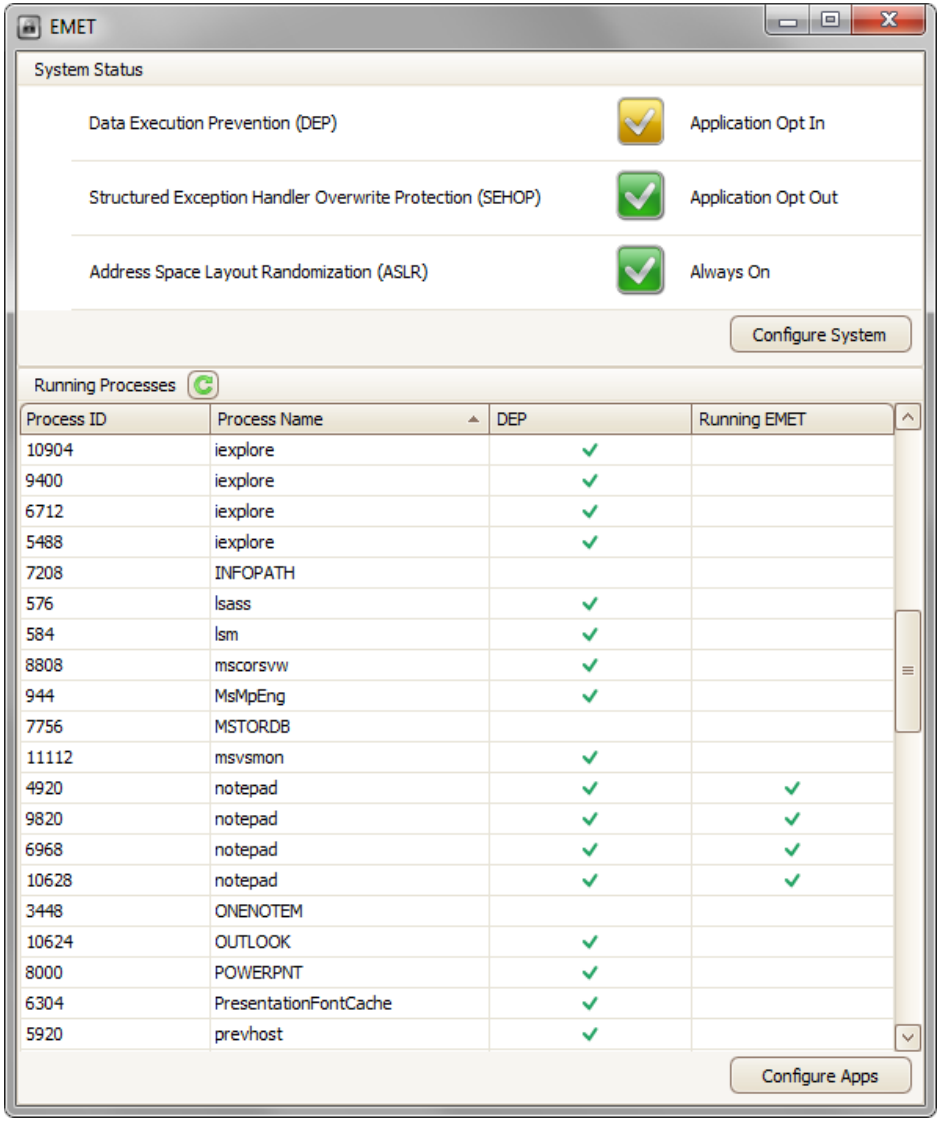
- EMET とは？ (+デモ)
- 各緩和技術の説明
- 事例紹介

Microsoft
Security

Enhanced Mitigation Experience Toolkit

EMET =
脆弱性緩和技術導入ツール

- 6 つのセキュリティ緩和技術
- あらゆるアプリケーションに対応
  - 基幹業務アプリケーション
  - 他社アプリケーション
  - 古いアプリケーション
  - ソース コードが利用不可のアプリケーション
- プロセス単位で設定
- 更新プログラム インストール前の緩和策



EMET の緩和技術

緩和技術	保護内容
Structured Exception Handler Overwrite Protection (SEHOP) ★	Final Handler を置くことで、バッファ オーバーフロー発生時の例外処理 (SEH) の際の脆弱性を緩和
Dynamic Data Execution Prevention (DEP) ★	プロセスのメモリの一部を “実行不可能” とマークすることで、メモリ上からシェルコードが実行されるのを防ぐ
Heap Spray Allocation	幾つかのメモリを予め割り当てることで Heapspray の攻撃手法を緩和 (成功率を下げる) *Heapspray: ASLR 回避などの目的で、シェルコードのコピーを可能な限り多くのヒープ領域上に置くことで、メモリの割り当てが動的に変化しても、最終的にコード実行の確率を上げる手法
Null Page Allocation	メモリの Null ページを予め割り当てることで、ユーザーモードにおける Null 逆参照のリスクを緩和 *多層防御保護
Mandatory Address Space Layout Randomization (ASLR) ★	OS ブート時に各モジュールがロードされるアドレスを予測不可能なようにランダム化する技術 *EMET ではすべてのモジュールに対しオプトインなしで ASLR を強制できる
Export Address Table Filtering (EAF)	EAT の読み書きを制限することでシェルコードが Windows API のアドレスを取得するのをブロック

★ 特定のバージョン以降の Windows OS で標準搭載されている緩和技術

デモ

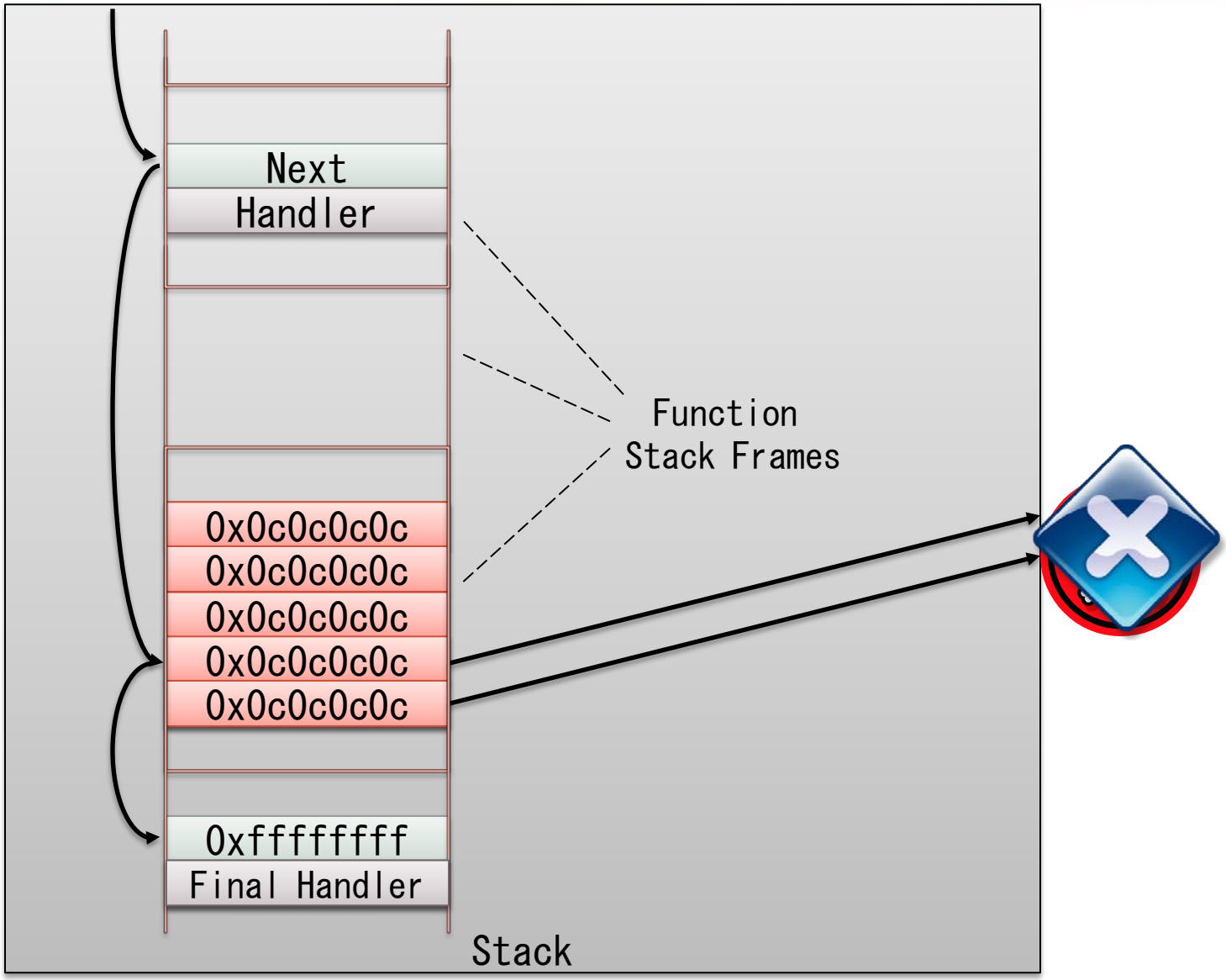
Microsoft
Security

EMET の各緩和技術

Microsoft
Security

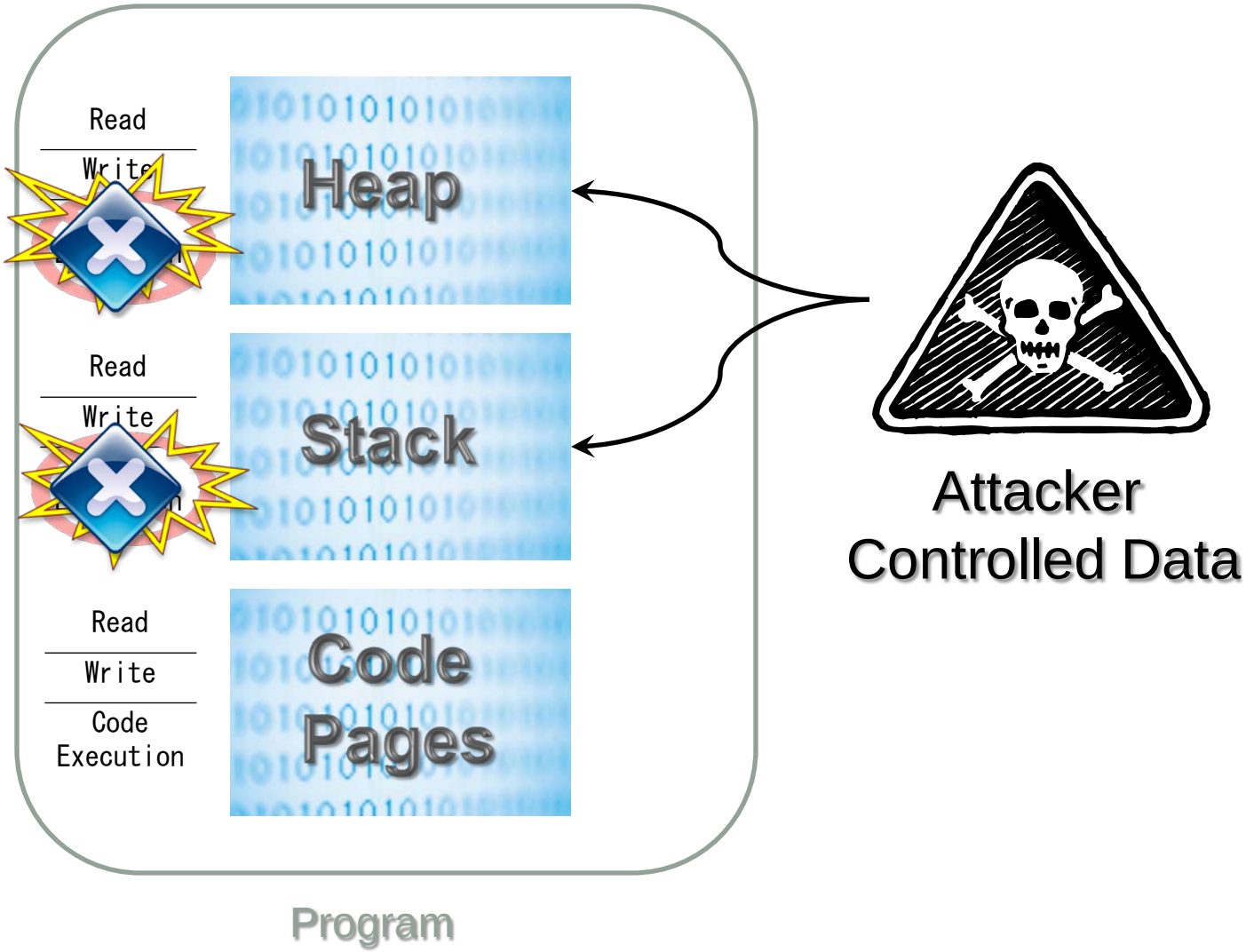
Structured Exception Handler Overwrite Protection

EMET On



Dynamic Data Execution Prevention

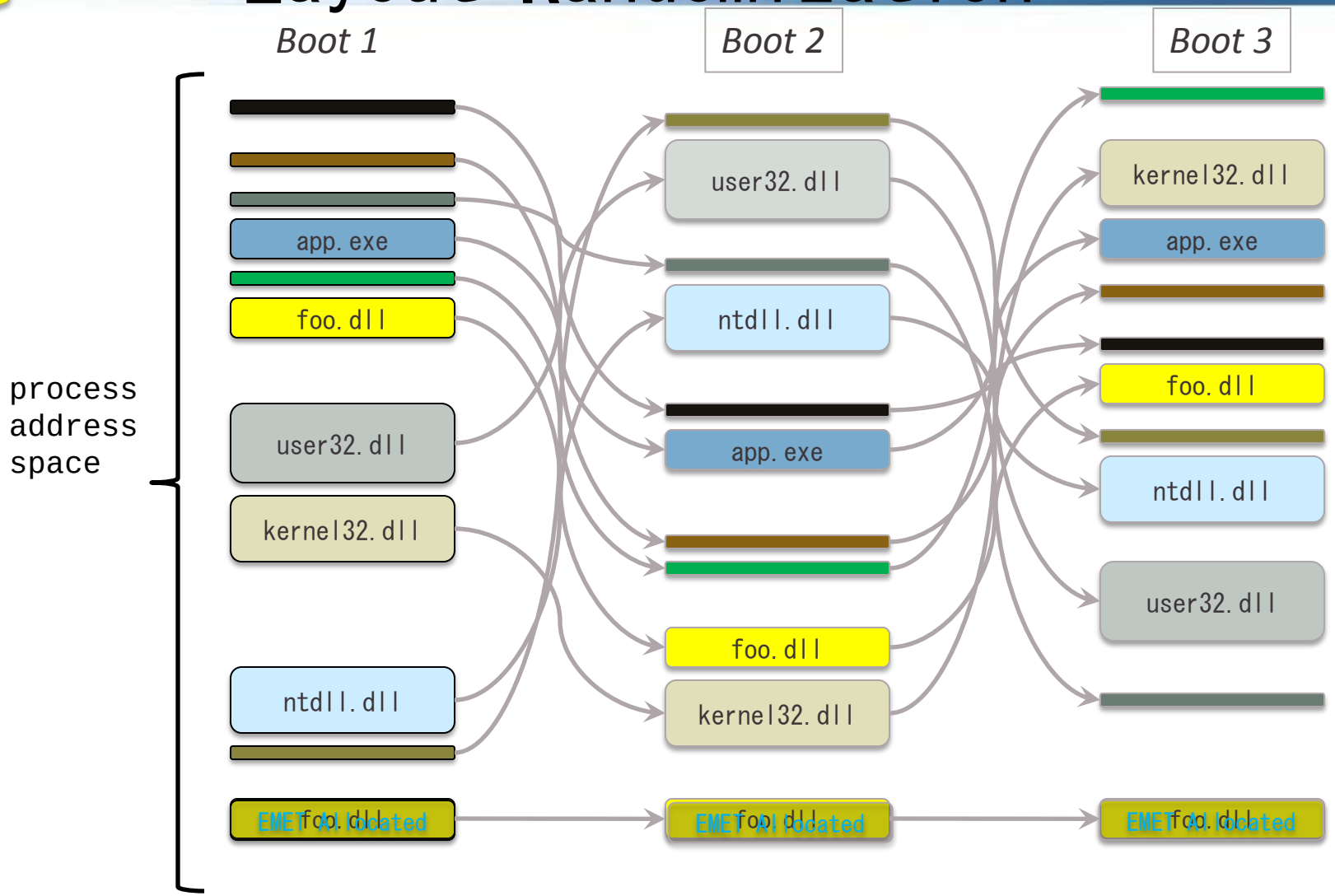
EMET On



V2 New!

Mandatory Address Space Layout Randomization

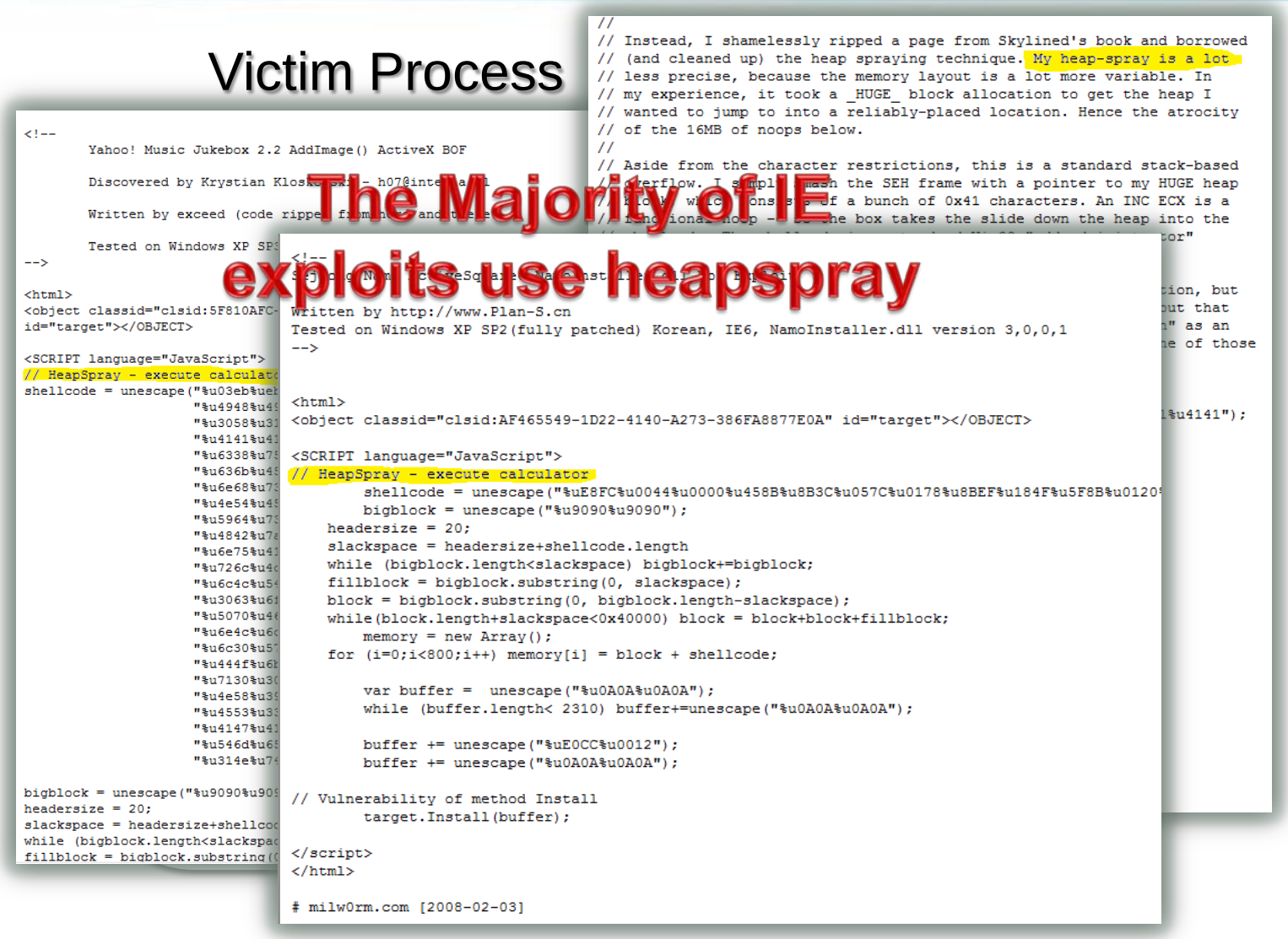
EMET On



Heapspray Allocation

EMET On

Victim Process



その他の緩和技術

- Null Page Allocation
  - Heapspray allocation に類似
  - メモリの最初のページ（Null page）を予め割り当てることで、ユーザー モードにおける Null 逆参照のリスクを緩和
  - 現時点ではこの攻撃手法は確立されておらず、多層防御の観点での緩和技術

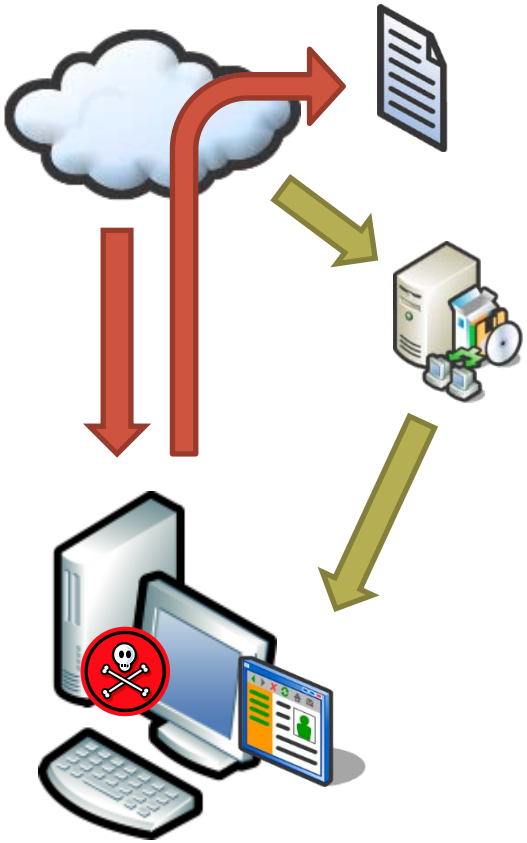
- Export Address Table Filtering (EAF)
  - EAT にブレークポイントを置き読み書きを制限することで、シェルコードが Windows API のアドレスを取得するのをブロック
  - 実質的に、現在あるすべてのシェルコード技術に対し有効

EMET 導入事例

#1 サムヒューストン州立大学

環境

- 数百のサーバー/数千のクライアントを強力な IT で中央管理
- 100 以上のアプリケーションを含む標準化デスクトップ環境
- ソフトウェア展開などは SCCM
- セキュリティ更新は WSUS
- 生徒数約 18,000人 / 教員数約 2,000人



現在…

- リスクの高いアプリケーション（※）を含むワークステーション 3,750 台に EMET を必須展開

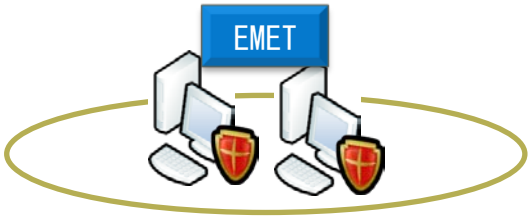
  ※ Adobe Acrobat、Mozilla Firefox、Microsoft Internet Explorer、Oracle Java、Apple QuickTime および Real Network’s Real Player

- システム パフォーマンスや使用感への影響はほとんど感じられない

EMET 導入背景

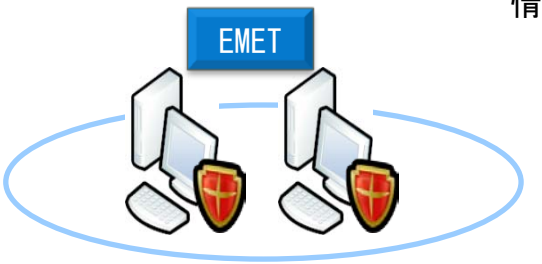
- 更新は年 3 回
- 特定のアプリケーション経由で悪用
- 悪用により IT に作業負荷
- ホストベースの IPS を検討したが、高価で管理コストも高い
- コストを抑え、アプリケーションの安全を保つため EMET を導入

#1 サムヒューストン州立大学

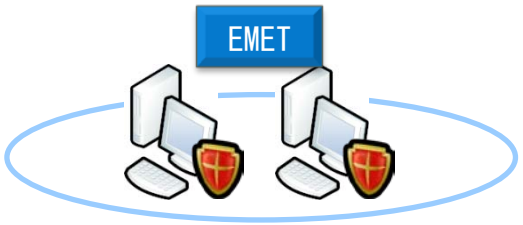


情報セキュリティ部門

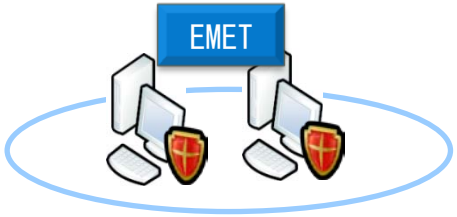
サーバー



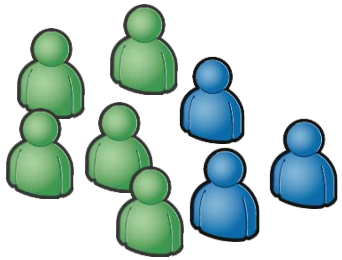
コンピューターラボ A

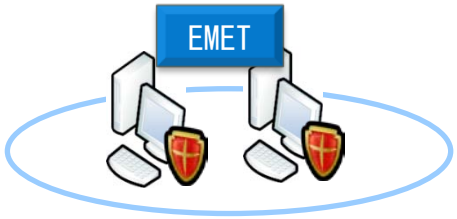


コンピューターラボ B



コンピューターラボ C





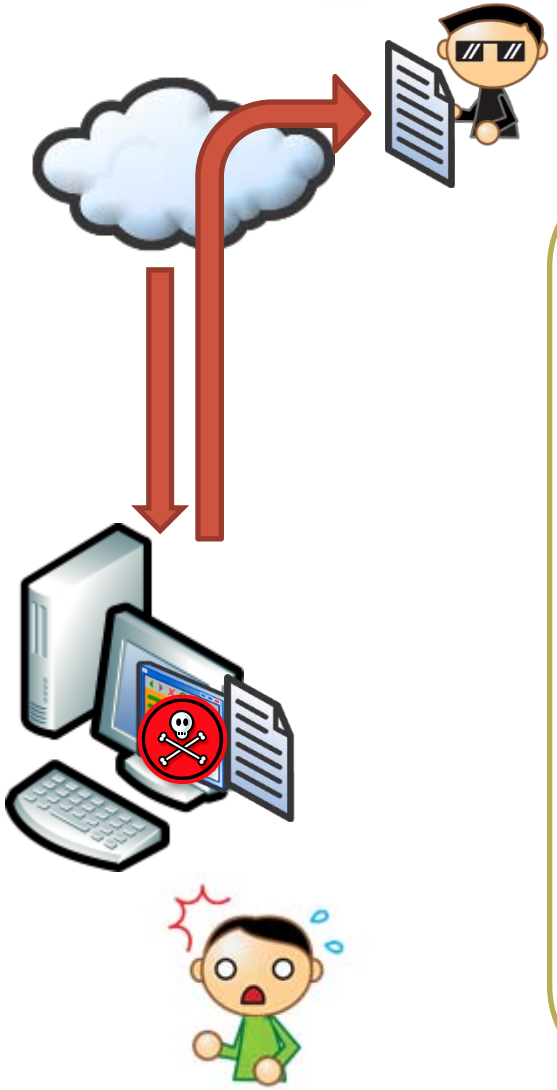
コンピューターラボ D

※わかりやすくするため構成を簡略化しています。

#2 米国大手エネルギー会社

EMET 導入背景

- 脅威に対するセキュリティ意識が高く、多層防御を推進
- 頻繁に使用するソフトウェア（ブラウザ、ドキュメントリーダー、ブラウザープラグイン、ランタイム等）で、リンクをクリックしたことで乗っ取られる悪用が増加
- 外部要因により必ずしも最新のソフトウェアを使用できるわけではない
- 企業セキュリティの弱点となる “ユーザー” に頼らない対策を模索
- 悪用を防ぐひとつの手段として EMET を導入



現在…

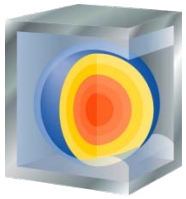
- 50 台のコンピューターに EMET を導入し初期テスト中（1 月 12 日時点）
- 0 day に対してや、パッチのない脆弱なバージョンの製品を使用している時でも安心

今後…

- 数か月かけてテストを拡大
- 最終的に全コンピューター約 75,000 台に導入予定
- 展開は SCCM を利用
- 新規コンピューターは EMET 構成済み展開用ディスク イメージを使用

EMET の活用

- 多層防御の一環
  - 既存のセキュリティ対策と併用



- ビジネス リスクが高いアプリケーション
  - 基幹業務アプリケーション
  - 重役の Web ブラウザー

- 1 台はみんなのために
  - リスク管理の観点

Microsoft Security

リソース

- EMET v2.0 ダウンロード: 無料
  http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c6f0a6ee-05ac-4eb6-acd0-362559fd2f04

- EMET 紹介 Web キャスト
  http://technet.microsoft.com/ja-jp/security/gg443928

- サポート技術情報 2458544
  http://support.microsoft.com/kb/2458544/ja

- EMET のフィードバック
  switech@microsoft.com までお寄せください（英語）

Microsoft
Security

参考情報 – サムヒューストン州立大学

環境
- 大半が Windows ベースの数百のサーバーと数千のクライアントを強力な IT で中央管理
- 100 以上のアプリケーションを含む標準化されたデスクトップ環境
- ソフトウェア展開、サードパーティ製品の更新は System Center Configuration Manager (SCCM) を利用
- マイクロソフト製品のセキュリティ更新は Windows Server Update Services (WSUS) を利用
- 生徒数約 18,000人、教員数約 2,000人

導入背景・導入目的
- サードパーティ アプリケーションの更新は、年 3 回の休暇シーズンに実施していた
- インターネットから直接情報を取るアプリケーションもあり、悪用のリスクも高く、有事の際余分な作業負荷もかかる
- 現在あるネットワークベース IPS と ホストベースのウイルス対策ソフトを補完するため、ホストベースの IPS の導入を検討したが、高価かつ管理コストも高いため採用不可
- コストを抑えつつ、リスクの高いアプリケーション (※) の安全を保つソリューションとして EMET を検討・導入

※ Adobe Acrobat、Mozilla Firefox、Microsoft Internet Explorer、Oracle Java、Apple QuickTime および Real Network’s Real Player

展開
- 2010 年 12 月までに、リスクの高いアプリケーションを含むワークステーション 3,750 台に EMET を展開
- 互換のためのトランスフォーム ファイルおよび設定ファイルをパッケージ化した MSI を SCCM で展開

展開詳細
1. 情報セキュリティ部門のクライアント数台に導入し数人で EMET の機能をテスト。その後、高いトラブルシュート能力を持つ 10 人の IT スタッフ、30 人の IT サポート スタッフへと拡大
2. 数か月のテストを経て、使用頻度の高いコンピューターラボの 100 ノードのうち半数に展開
3. 1 ケ月のエンドユーザーテストを経て、トラフィックの高いコンピューターラボの約 120 台のクライアントに展開
4. 特に問題もなかったため、2010 年 12 月 23 日に校内すべてのクライアントに必須ソフトウェアとして展開

困難・フィードバック
- １つのアプリケーションで互換性の問題があった
- 現バージョンの EMET では、設定変更したい場合中央管理する方法がなく、MSI の再適用が必要となる
- Active Directory やグループ ポリシーと連携して容易に展開・管理できるとよい
- EMET の導入には 100% 肯定的。企業における脆弱性を軽減するのに非常に有効
- システムのパフォーマンスや使用感への影響はほとんど感じられない

コメント
- 設定するアプリケーションのすべての機能が問題なく動作するか、出来る限りの検証を
- EMET は、ファイアウォールやウイルス対策製品などと同様で、多層防御のためのひとつの補助ツールと捉え、既存のセキュリティ対策と併用すると良い

参考情報 – 米国大手エネルギー会社

導入背景
- 企業として脅威に対するセキュリティ意識が高く、多層防御を推進
- 頻繁に使用するソフトウェア（ブラウザ、ドキュメントリーダー、ブラウザープラグイン、ランタイム等）でリンクをクリックしたことで乗っ取られる悪用が増加
- 外部要因により必ずしも最新のソフトウェアを使用できるわけではない
- 企業セキュリティの弱点となる “ユーザーの判断” に依存しない対策を模索
- 悪用を防ぐためのひとつの手段として EMET を導入。0-day に対してや、パッチのない脆弱なバージョンの製品を使用している時でも安心して実行できる

展開
- 現在 50 台のコンピューターに導入し初期テスト中（2011 年 1 月 12 日時点）
- 数か月かけてテスト対象コンピューターを拡大
- 最終的には全てのコンピューター約 75,000 台に導入予定
- EMET の展開は SCCM を利用し、MSI と設定ファイルを配布
- 新規コンピューターについては、EMET 構成済みの展開用ディスク イメージを使用

困難
- “すべて” のプロセスに DEP を展開したかったが、Office 2010 など一部のプロセスで互換がないものもあった
- 組織で新しいアプリケーションやプロセスが追加された際、それを検知して EMET を自動適用するための既存の方法は用意されていないため、それを行うための専用ツールの開発が必要となった

フィードバック
- ほとんどのプログラムは問題なく動作中
- EMET の導入には、導入部員のある程度の作業負荷が必要となる
- EMET プリインストール版であるとか、容易な配布方法を検討してほしい。IT にとって導入は少し負荷と捉えられる

コメント
- 新たにインストールされたアプリケーションをどう保守するかを考える必要がある
- 周到なテスト プランを立て、IT サポートがトラブルシュートできる手段（ガイドライン、ツール）を用意しておくこと
- 一般ユーザーがトラブルシュートできるための方法（電話サポート、ガイドライン、ツール）も用意できると可

Microsoft®
Security

Microsoft®

Be what's next.™