Enhanced Mitigation Experience Toolkit 5.5

ユーザー ガイド

2016 年 1 月

www.microsoft.com/emet

目次

導入

脆弱性緩和ツール、Enhanced Mitigation Experience Toolkit (EMET) は、攻撃者がコンピューター システムへのアクセスを得るのを防ぐ目的で設計されました。EMET は、攻撃者がコンピューター システム内の脆弱性を悪用するために使用する可能性のある最も一般的なテクニックを予測し、それらのアクション、およびテクニックを回避、ブロック、および無効にすることで保護を助けます。EMET は、新しい、および未発見の脅威をセキュリティ更新プログラム、およびマルウェア対策ソフトウェアによって解決される前でさえ、コンピューターを保護します。EMET は、ビジネスや日常生活を混乱させる可能性のあるセキュリティの脅威、およびプライバシーの侵害から保護することで企業や、すべての PC ユーザーを支援しています。

ソフトウェアの脆弱性、およびその悪用は日常生活の一部となってきました。事実上、すべての製品が、それらに対処しなければならず、結果として、ユーザーは絶え間なくセキュリティ更新プログラムと向き合っています。最新の更新プログラムが展開される前に攻撃を受けたユーザー、あるいは、ゼロデイ攻撃のケースのように更新プログラム利用可能になる以前に攻撃を受けたユーザーについては、マルウェア感染、Personally Identifiable Information [個人情報] (PII) の損失、ビジネス データの損失などの甚大な被害を招く可能性があります。

セキュリティ緩和技術は、与えられたソフトウェア内で、攻撃者が脆弱性を悪用するのを、より困難にするために設計されました。EMET は、お客様がこれらのセキュリティ緩和策技術を彼らのシステム上で活用でき、結果としていくつかの優れた利益をもたらします。

ソースコードは不必要: 利用可能ないくつかの緩和策（例えば、データ実行防止など）は、アプリケーションを手動で展開し、そして再コンパイルされることを必須としています。EMET では、ユーザーが再コンパイルなしにアプリケーションを展開できるように変更されます。これは、緩和策が展開される、また、ソースコードの利用可能以前に書かれたソフトウェアに対し、緩和策を展開する場合に有用です。

高度に設定が可能: EMET は、各プロセス ベースに対し個別に緩和策が適用されるようにすることで、より高い精度を提供します。製品全体、あるいはアプリケーション一式を有効にする必要はありません。これは、特定の緩和技術とプロセスの互換性がない場合に役立ちます。そのような場合、ユーザーは、そのプロセスについてただ、緩和策を無効にするだけです。

レガシ アプリケーションの強化を支援する: 簡単に書き換えができず、段階的にゆっくりと停止していく必要のある古いレガシ ソフトウェアに対して強い依存度を持つことはめずらしいことではありません。残念ながら、レガシ ソフトウェアが、セキュリティ脆弱性を持っていることはよく知られているために、このことが、簡単にセキュリティ リスクをもたらします。これに対する実際の解決策は、レガシ ソフトウェアから移行することですが、EMET は、移行を行っている最中に、ハッカーがレガシ ソフトウェアの脆弱性を悪用するのをより困難にすることで、リスクを管理する手助けをしてくれます。

Web サイトをサーフィンする際に SSL 証明書の信頼度を確認してくれる: 証明機関に関する事故が、不正な SSL 証明書を作成可能にして、中間者攻撃を実行する問題が頻発しているため、EMET は発行を行ったルート CA (設定可能な証明書ピン設定) に対し、特定のドメインの SSL 証明書を認証できる、ピン設定ルールを実行できる可能性を提供します。

アプリケーション内のグラニュラー プラグイン ブラックリストを許可する: モジュール、およびプラグインはアプリケーションを読み込むと、脆弱性、そしてその結果として起こりうる攻撃にさらされる機会が増えます。EMET で、アプリケーション内にロードされるモジュール、およびプラグインをブラックリストに掲載できます。

使いやすさ: システム規模の緩和策に関するポリシーは、EMET のグラフィカル ユーザー インターフェース、コマンドライン ツール、もしくはグループ ポリシーを介して、確認と設定ができます。レジストリキーを探す、または判読する、あるいは、プラットフォーム依存のユーティリティを実行する必要はありません。EMET で、基本的にプラットフォームに関係なく、インターフェースにあわせて、設定を調整することができます。

継続的な改善: EMET は、新しい緩和技術が利用可能になる度に更新されるよう設計された、ライブ ツールです。これは、最先端の緩和策を試し、利益を受ける機会を与えます。また、EMET のリリース サイクルはどの製品とも関連がありません。

機能

EMET は、緩和策に対するシステム ポリシーを設定するだけでなく、それを実行可能かどうかに応じて設定が可能です。さらに、EMET は、設定可能な「ピン設定」ルールに対して SSL 証明書を認証し不正なものについて検出する機能を提供します。

システム緩和策ポリシーは、システムがサポートする緩和策を、ユーザーが既定で設定できるものです。例えば、緩和策をすべてのプロセスに対して有効にする必要があるのか、選択したものについてのみ有効にすべきか、あるいは完全に無効にするのかを選択します。

実行可能な緩和策オプションは、ユーザーがアプリケーションに対して EMET がサポートする緩和策を有効にできます。サポートされている緩和策はいずれも、システムに存在するあらゆるアプリケーションに対して、個別に有効/無効可能です。次に設定されたアプリケーションが実行された場合、規定の緩和策が展開されます。これらの二つのオプションを兼ね備えることで、ユーザーに、システム上で利用可能な緩和策、および、それらがどう使用されるかに対して、より高いレベルのコントロール権を与えます。

証明書信頼機能で、ブラウズしている最中に、デジタルで署名された証明書 (SSL 証明書)に対して一連のピン設定ルールを設定できます。これらのルールは、特定のドメインの SSL 証明書と通信する、証明書を発行したルート証明機関(ルート CA) とを結びつけるよう設計されています。EMET が特定のドメイン用に設定された SSL 証明書を発行するルート CA の変動について検出した場合、この変動を、進行中の中間者攻撃が起こりうる症状であるとして、報告します。

EMET 緩和策モジュールは、サービスとしては実行されず、デバッガーのようにアプリケーションに付随されません。その代わり、裏側では、アプリケーションに対して緩和策を有効にするために、EMET は、Windows 内のアプリケーション互換性フレームワークと呼ばれるインフラストラクチャを活用しています。このインフラストラクチャに付随するツール キットの詳細な概要は、このブログで参照することができます。

注: 次に進む前に、いくつかのセキュリティ緩和技術は、いずれかのアプリケーションを実行した場合、互換性の問題が生じる場合もあることを念頭においてください。プロダクション環境で実行する前に、すべてのターゲット使用シナリオで十分に EMET をテストすることが重要です。

緩和策

EMET は、多様な緩和技術をサポートしています。このセクションでは、異なる緩和策の概要、および、それら緩和策が提供する保護策について説明します。

Structured Exception Handler Overwrite Protection (SEHOP)

この緩和策は、現在最も一般的な Windows のスタック・オーバーフローを悪用する手法から保護します。この緩和策は、Windows Vista SP1 から、Windows では標準装備されています。Windows 7 および Windows のその後のバージョンでは、これを有効・無効にできる機能が追加されました。EMET では、Windows XP まで遡る、あらゆるプラットフォームのバージョンに対して、最新の Windows と同じ機能を提供しています。詳しくは、SEHOP 概要 (英語情報) および Windows 7 SEHOP 変更点 (英語情報) を参照してください。

EMET が実行されていない場合、攻撃者は、スタック上の例外レコードのハンドラー ポインターを任意の値で上書きすることができます。一度、例外が起こると OS が例外レコードのチェーンを渡り歩き、それぞれの例外レコードのハンドラーを呼び出します。攻撃者が、そのレコードの一つを管理しているため OS は、どこであろうと攻撃者が望む場所に移動し、攻撃者が実行の流れを管理できるようになります。この解説は図 1 を参照してください。

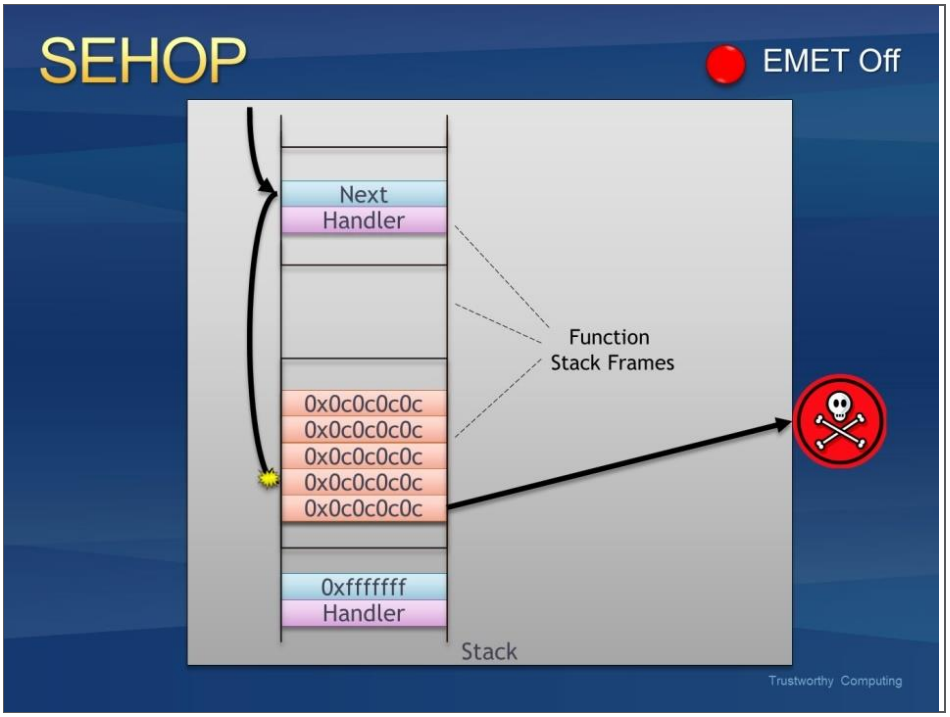

図 *1:* 例外ハンドラーの乗っ取り

EMET を実行している場合、OS があらゆる例外ハンドラーを呼びだす前に、例外レコード チェーンの検証を行います。最終の例外が定義済みのものを含むかどうかについても確認を行います。チェーンが破損していれば、EMET はいずれのハンドラーも呼び出すことなくプロセスを終了します。図 2 で、これがどのように起こるのか解説しています。

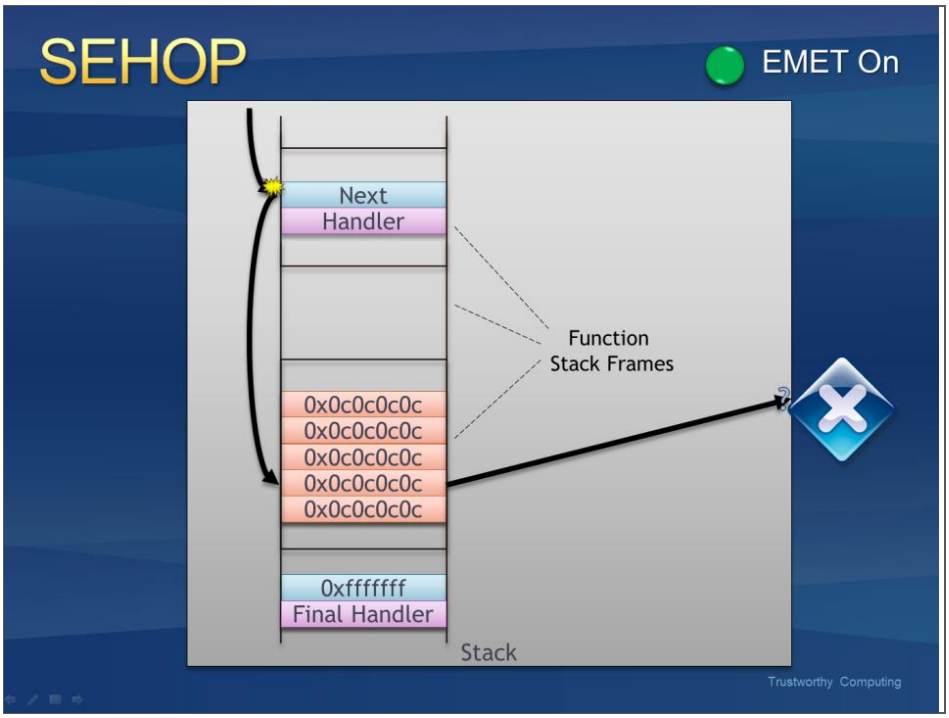

図 *2: EMET* が例外ハンドラーの乗っ取りを止める

注意: Windows 7 以降の新しいバージョンの Windows については、選択されたアプリケーション用にオペレーティング システムが提供する本来の SEHOP を EMET が設定します。

データ実行防止 (DEP)

DEP は、Windows XP から利用可能です。しかしながら、現在の設定オプションでは、特別なフラグでまとめられていなければ、アプリケーションを個別に選択することができません。EMET の利用で、フラグがまとめられていないアプリケーションを個別に選択することができません。EMET を利用することで、フラグでまとめられていないアプリケーションも選択することができます。DEP が何か、そしてどのように機能するかについての詳細は 2 部構成になっている Microsoft Security Research & Defense (SRD) のブログ投稿のパート 1 (英語情報)、およびパート 2 （英語情報）を参照してください。

EMET を実施していない場合、攻撃者は、ヒープあるいはスタックなど、攻撃者がコントロールするデータが存在するメモリ ロケーション内のシェルコードに移動することで、脆弱性を悪用しようと試みる可能性があります。これらの領域においては、実行可能と認識されているため、悪意のあるコードが実行可能です。

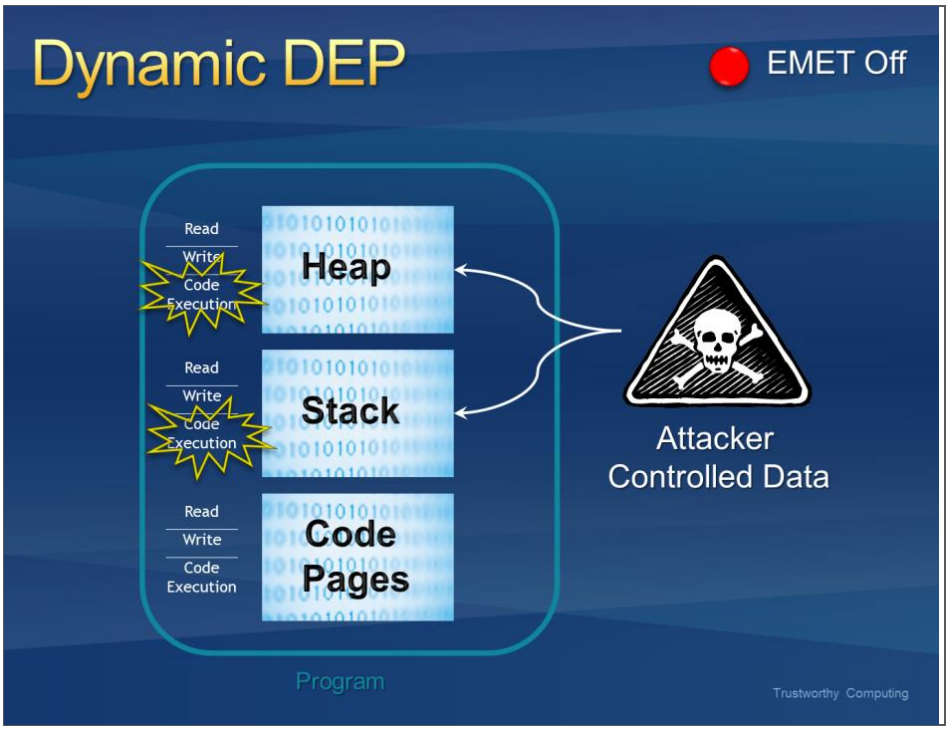

図 *3:* 攻撃者が管理する領域でシェルコードを実行する

EMET を実行することで、プロセスに対しデータ実行防止が有効化されます。有効後は、スタックおよびヒープはコードが実行不可能と認識され、これらの領域から悪意のあるコードを実行しようとする、あらゆる試みがプロセッサ レベルで拒否されます。

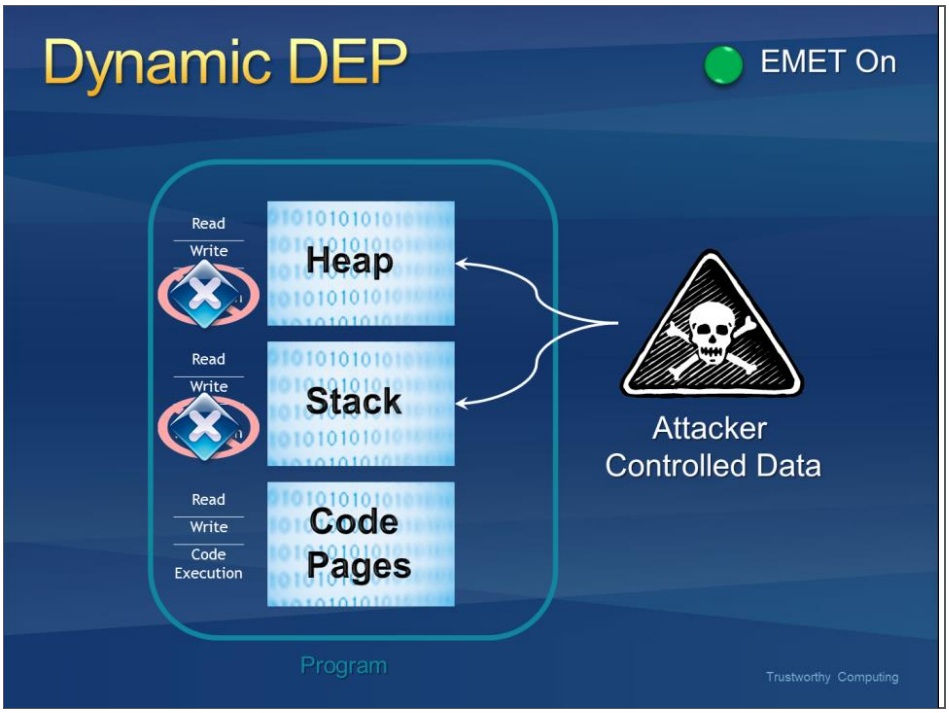

図 *4:* データ実行防止でシェルコードの実行を阻止する

ヒープスプレー アロケーション

悪用が実行されているとき、シェルコードが存在するアドレスが定かでない場合も多く、インストラクション ポインターをいつ、コントロールするのか推測しなければなりません。成功の確率を上げるために、悪用が行われる場合はほとんど、可能な限りメモリ ロケーションにシェルコードのコピーを置くというヒープスプレー手法が使用されています。図 5 では、被害者のプロセスにおいてこれがどのように行われるかについて解説しています。

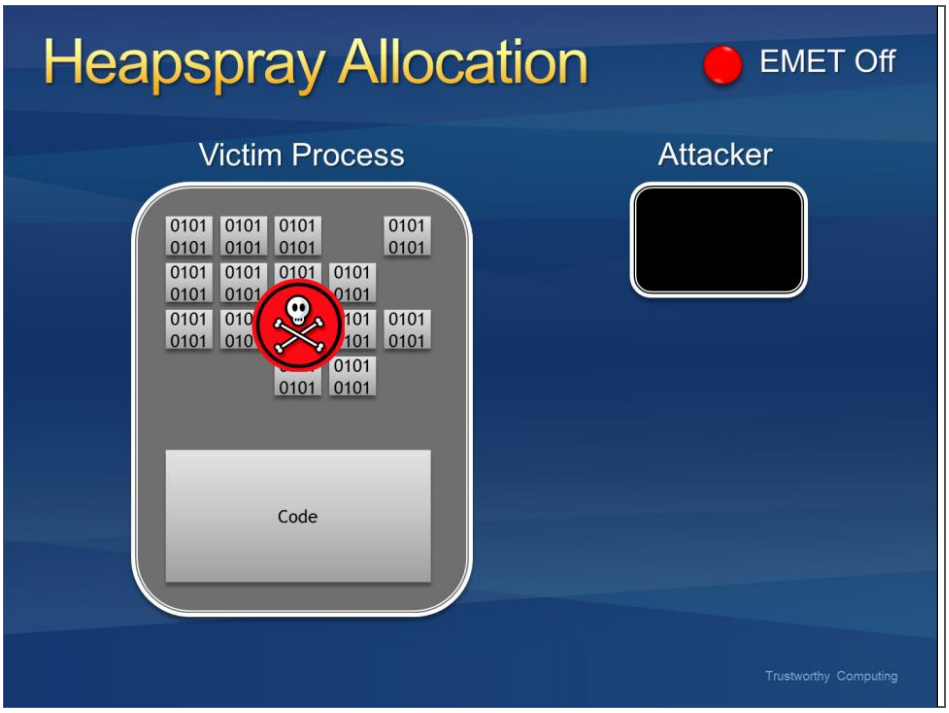

図 *5* 悪用におけるヒープスプレーの使用

EMET を実行している場合、一般によく使用されるメモリ ページは事前に割り当てられていることがあります。これらのページのコントロール（その後、該当ページに移動する）を前提としている悪用は成功しません。

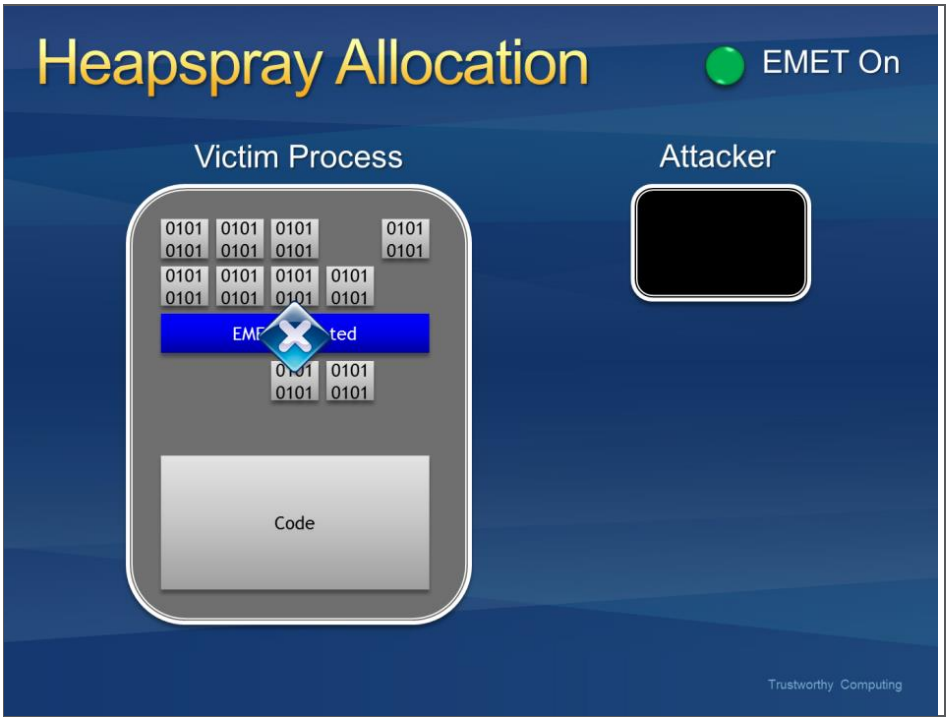

図 *6:* ヒープスプレーを使用する攻撃を阻止する

これは現在の悪用手法を失敗させるために設計された、疑似緩和策である点にご注意ください。将来起こりうる悪用をも防ぐために設計されたものではありません。悪用手法の発達にともない、EMET も進化します。

Null ページ アロケーション

これはヒープスプレー アロケーションに似た技術ですが、ユーザー モードで起こりうる NULL 逆参照を防ぐために設計されています。現在、これらを悪用する既知の方法はないため、これが徹底した防御の緩和技術なのです。

強制 Address Space Layout Randomization (ASLR)

ASLR は、攻撃者が予測可能なロケーションにあるデータを悪用しようとするのを防ぐために、モジュールがロードされるアドレスをランダム化します。問題点は、すべてのモジュールが、これを選択するために、コンパイル タイムグラフを使用しなければならないことです。EMET を実行していない場合、攻撃者が DLL の予測可能なマッピングを巧みに利用し、Returned Oriented Programming (ROP) と呼ばれる既知の手法を通じて DEP をバイパスするためにそれらを使用する可能性があります。

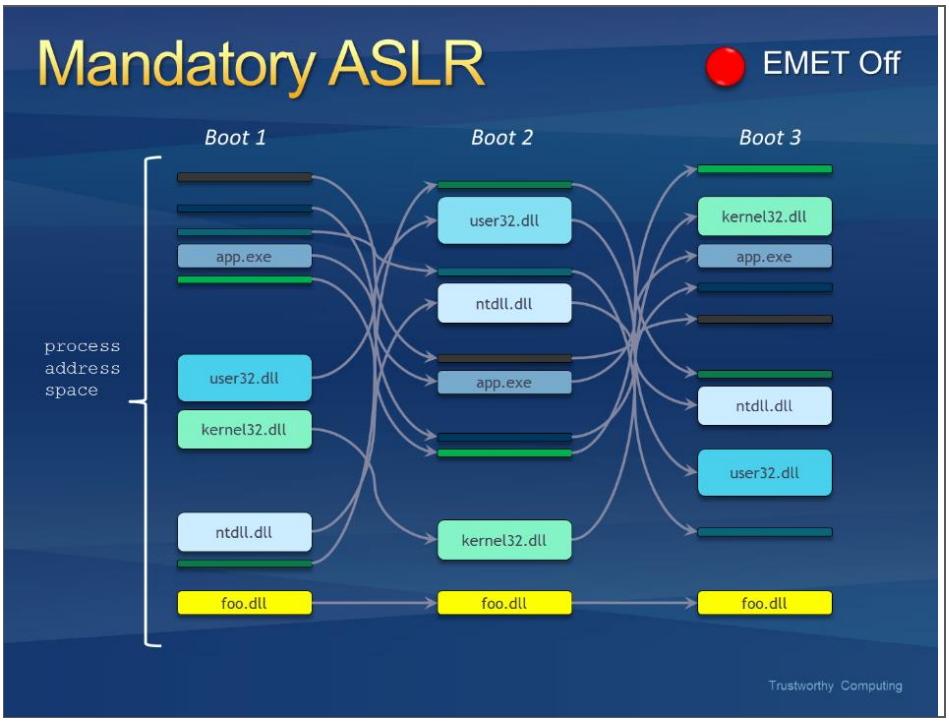

図 7: 予測可能なロケーションに、あるモジュールがロードされる

EMET を実行していると、まとめられているフラグに関係なく、標的とするプロセスのためにランダム化されたアドレスに強制的にモジュールがロードされます。ROP を利用する悪用、そして予測可能なマッピングを当てにしている悪用は成功しません。

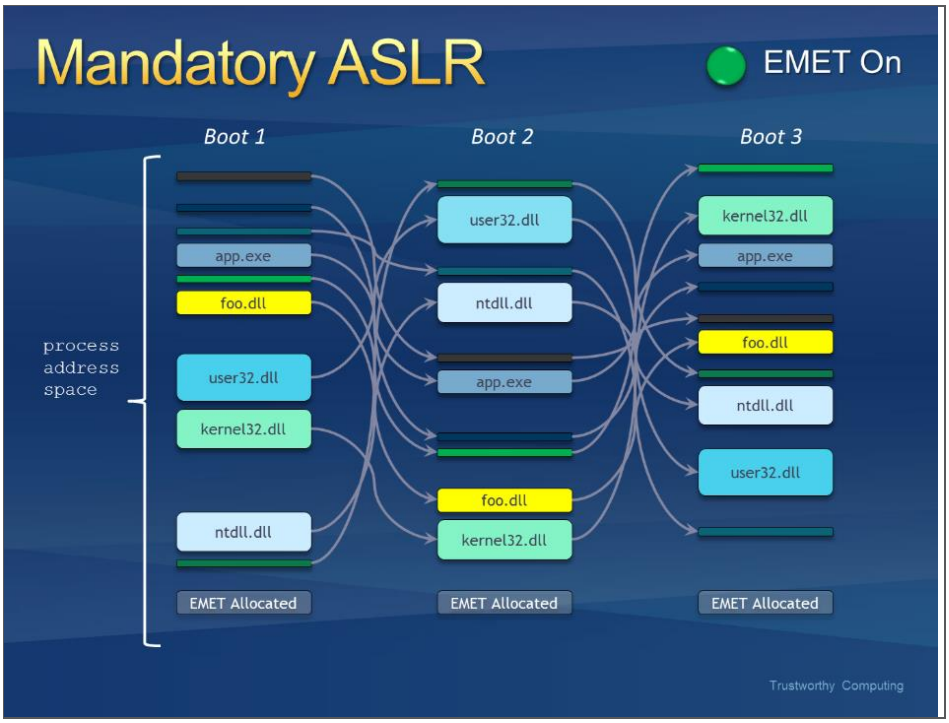

図 *8:* ランダムなアドレスに強制的にロードされる、あるモジュール

注意: Windows 8 以降の新しいバージョンの Windows については、アプリケーション用にオペレーティング システムが提供する本来の強制 ASLR が既に有効になっている場合は、EMET はこの緩和策は利用しません。

Export Address Table Access Filtering (EAF)

何か「有益な」ことを行うために、シェルコードは一般に Windows API を呼び出す必要があります。API を呼び出すために、シェルコードはまず、API がロードされているアドレスを見つけなければなりません。これを行うために、多くのシェルコードは、すべてのロードされているモジュールの Export Address Table を検索し、有用な API を含むモジュールを探します。通常、これには kernel32.dll、ntdll.dll あるいは kernelbase.dll が関与します。有用なモジュールが見つかると、シェルコードは、そのモジュールの API が存在するアドレスを探し出すことができます。

この緩和策は、Export Address Table (EAT) への閲覧アクセスをフィルタリングし、シェルコード由来の呼び出しコードか否かに基づいて、読み取り/書き込みのアクセス許可、拒否を行います。EMET を実行していると、データに必要な API を検索しようとした場合、現在出回っている大抵のシェルコードが阻止されます。

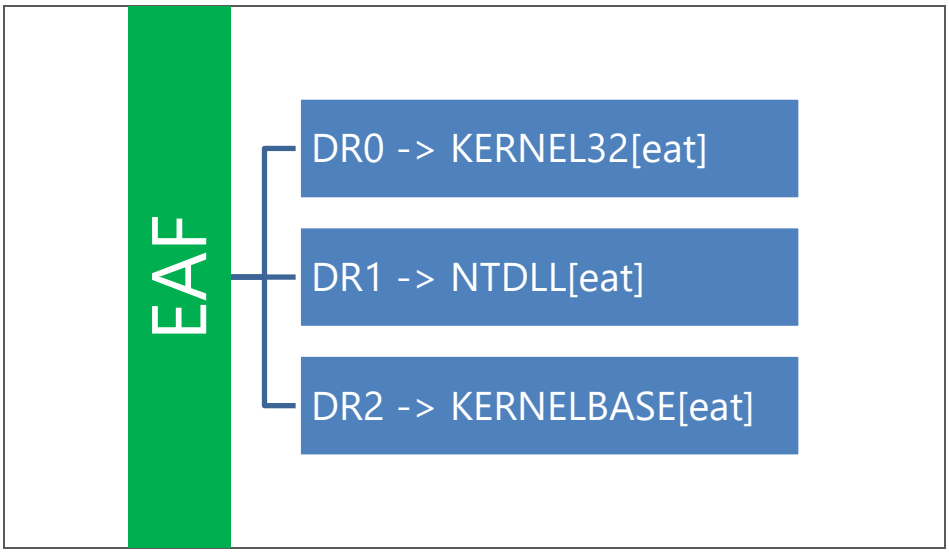

図 *9:* 旧バージョンの *EMET* で *EAF* がどのようにして重要なモジュールのエクスポート アドレス テーブルへのアクセスを監視しているか; 新バージョンの *EMET* は、保護の実装に異なる仕組みを用いる場合があります。

この緩和策は、デバッガーのようなソフトウェア、デバッガーのように機能するソフトウェア、もしくはデバッグ対策手法を使用するソフトウェアとの間に互換性の問題がある可能性があります。例えば、ビデオゲーム、サンドボックス ソリューション用の保護構造、DRM、デバッグ/トレーシング ツール、そしてアンパッカーなどがそうです。

これは現在の悪用手法を失敗させるために設計された、疑似緩和策である点にご注意ください。将来起こりうる悪用を防ぐために設計されたものではありません。悪用手法が発達するにともない、EMET も進化します。

Export Address Table Access Filtering Plus (EAF+)

EAF+ 緩和策は、EAF の拡張版で、EAF+ 単独、または EAF との併用で利用できます。以下が、この緩和策が実行するアクションです:

- スタック レジスタが許可されたバウンダリーの範囲外にある場合に検出する
- スタック、およびフレーム ポインター レジスタの不一致を検出する
- 特定のモジュール由来の KERNEL32、NTDLL、および KERNELBASE のテーブル ポインターをエクスポートしようとするメモリ読み取りアクセスを検出する (一般に、メモリ破損の脆弱性悪用の最中に利用される)
- 特定モジュールの MZ/PE ヘッダーへのメモリ読み取りアクセスを検出する (一般に、メモリ破損の脆弱性悪用の最中に利用される)

箇所書きの最後の 2 点については、検証に使用される一連のモジュールをユーザーが特定するのが必須です。モジュールが特定されないと、これらのアクションは無視されます。

ボトムアップ ランダム化

この緩和策は、一度 EMET がこの緩和策を有効にすると、ボトムアップ型の割り当て（ヒープ、スタック、およびその他のメモリ アロケーション）のベース アドレスをランダム化します （8 ビットのエントロピ）。有効にする以前の割り当てについてはランダム化されません。

ROP 緩和策

EMETは、ROP に依存する悪用をブロックすることを目的とする、複数の実験的な Return Oriented Programming (ROP) 回避緩和策を提供します。ROP 悪用は、データ実行防御などの緩和策が実施されている場合にコード実行を促す手法です。ROP 悪用では、既に攻撃を受けたアプリケーションのメモリ－領域に存在するコードの断片を利用します。

ROP 緩和策はすべて、32 ビットプロセス、そして一部の 64 ビットプロセスに対してのみ利用可能であることに注意してください。

以下は、ROP 緩和策の詳細説明です:

ロード ライブラリ チェック (Load library checks): EMET は LoadLibrary API へのコールをすべて監視し、UNC パス (例： ¥¥evilsite¥bad.dll) からライブラリへロードされるのを阻止します。プログラムが意図的に UNC パス、あるいはリモート サーバーから DLL をロードする場合には、このオプションを無効にできます。この緩和策は 32、および 64 ビットプロセスで利用可能です。

メモリ 保護チェック (Memory protection checks): EMET は、スタック領域を実行可能にすることを認めません。大抵、シェルコード、あるいは ROP ガジェットがこのような活動を利用します。この緩和策は 32、および 64 ビットプロセスで利用可能です。

呼び出し元チェック (Caller checks): EMET は、クリティカルな関数が呼び出された場合、「RET」ではなくコール命令を介して呼び出されたか、必ず確かめます。これは、大変便利な緩和策で多くの ROP ガジェットを破ります。この緩和策はいくつかのアプリケーションと互換性がない可能性があります。この緩和策は 32 ビットプロセスで利用可能です。

実行フローのシミュレート (Simulate execution flow): クリティカルな関数に対する呼び出しを受けて、この機能は ROP ガジェットを検出しようと試みます。「呼び出し元チェック」のように、この機能はいくつかのアプリケーションと互換性がない可能性があります。この緩和策は 32 ビットプロセスで利用可能です。

スタック ピボット (Stack pivot): スタックが変更された場合に、それを検出するために利用される緩和策です。この緩和策は、特定の API のコンテクスト構造に存在するスタック レジスタも有効にしま

す。大抵のプログラムと互換性があります。この緩和策は 32、および 64 ビットプロセスで利用可能です。

攻撃表面の縮小 (ASR)

攻撃面の縮小 (ASR) は、特定のモジュール、もしくは対象のアプリケーション内のプラグインの使用を禁止することで、アプリケーションが攻撃のリスクに晒されるのを軽減します。例えば、EMET は Microsoft Word が Flash のプラグインをロードしようとするのを禁止するよう設定できます。もしくは、セキュリティ ゾーン (英語情報) によって、イントラネット ゾーンの Web サイトでは Java を許可しながらも、インターネット ゾーンの Web サイト上に Oracle Java プラグインがロードされるのを禁止するのに利用することができです。この仕組みは、単純に、プロセス毎に DLL のロードを禁止し、特定のアプリケーションの「Killbit」に特化したモジュールに対してより効果をもたらせます。

ROP の高度な緩和策

EMET は、すべての設定ソフトウェアに適用できる追加の緩和策オプションを備えています。追加の緩和策は ROP 緩和策、および EAF で現在、利用可能で、有効、あるいは無効にした場合、EMET で構成された ROP、もしくは EAF 緩和策を最低一つでも持つプログラムすべてに影響します。

以下はこれら詳細な緩和策の概要です:

ROP 要件	**ディープ フック (Deep hooks):** EMET は、クリティカルな API、およびこれに続く高いレベルの API が利用する低レベルの API を保護します。例えば、EMET は *kernel32!VirtualAlloc* だけではなく、*kernelbase!VirtualAlloc* および *ntdll!NtAllocateVirtualMemory* などの関連するレベルの低い関数もフック、および保護します。 **迂回回避 (Anti detours):** フック関数のプロローグをコピーすることで、フックを回避しようと試みる悪用があり、悪用後にプロロール以前の関数に飛びます。「迂回回避」オプションを有効にすることで、この技術を利用する一般的なシェルコードは無効です。 **禁止された機能 (Banned functions):** このオプションを有効にすることで、EMET は API を侵害する可能性のある悪用を緩和するため ntdll!LdrHotPatchRoutine への呼び出しを遮断します。

証明書信頼 (設定可能な証明書ピン)

EMET は、暗号化されたチャンネル上での中間者攻撃を検出するという目的で、証明書チェーンの信頼検証動作の最中に追加でチェックする機能も備えています。HTTPS Web サイトを閲覧している際に、SSL 証明書のために、Internet Explorer が証明書チェーンを構築する度に、EMET は、エンド エンティティ SSL 証明書を認証し、それがそのサイト用に設定されたピン ルールで指定されたルート証明機関にチェーンするかを検証します。 特定のドメイン向けに設定されたルールによって、EMET がピン ルールで指定された証明書とは異なるルート証明書にチェーンするサーバー認証証明書を検出した場合、EMET は単にユーザーへ警告して接続は許可、あるいは完全に接続をブロックすることができます。既定では、EMET はタスク バーの通知領域近くの “トースト” 通知でユーザーへ警告し、接続を停止しません。このルールをブロック ルールに変更するためのチェック ボックスがあります。ピン ルールは、ルート証明機関の証明書の拇印 (指紋とも呼ばれる) の観点から実装されています。ユーザーまたは IT 管理者は、構成しているコンピューターのルート証明書ストアから 1 つ以上のルート証明書を選択することでピン ルールを定義します。ピン ルールが立証されると、サーバーのルート証明機関の証明書の拇印は、ピン ルールと紐づいている拇印の 1 つと一致する必要があります。(これは、証明書のサブジェクト名とシリアル番号、または公開キーのハッシュと一致という以前のバージョンの EMET からの変更点ですので、ご注意ください。) また、EMET は、ピン ルールで設定された Web サイト名に対し、利用可能なサブジェクトの別名も含め、 SSL 証明書のサブジェクト名 (CN) とも一致します。Windows の信頼済みルート証明機関ストアから、証明書をインポートすることで信頼済みルート証明機関の一覧を明示することができます。既定では、ルート ストアはすべての信頼済みのルート証明機関の一部のみを含みます。このコマンド: **certutil -SyncWithWU *directory*** を実行すると、完全な信頼済みのルート証明機関の一覧をダウンロードできます。続いて、**ertutil -addStore** コマンドで、任意またはすべての証明書をローカルのルートストアへインポートすることができます。ルールが適用されないように、一時的に特定のドメイン用のピン ルールを非アクティブとしてマークすることもできます。 キーサイズ、ハッシング アルゴリズム、または発行国に基づいて以前のバージョンの EMET で提供された例外のピン ルールは、設定 UI に表示されていても今後 EMET では実装されませんのでご注意ください。

信頼されていないフォントの緩和策

Windows 10 は、信頼されていないフォントをブロックする機能を追加し、信頼されていない、または攻撃者によって制御されたフォントファイルから発生する攻撃からユーザーを保護します(

この機能の詳細については、Technet の記事、「エンタープライズ内の信頼されていないフォントのブロック」を参照してください）。

EMET は、システム全体の信頼されていないフォント保護を有効にし、この保護から特定のアプリケーションを除外する機能を備えます。

信頼されていないフォントは、%windir%/Fonts ディレクトリ外にインストールされているすべてのフォントです。信頼されていないフォントをブロックすると、リモート (web ベースまたは Email ベース) およびフォント ファイルの解析処理中に起こりうるローカル EOP 攻撃の両方を阻止します。

レポート

EMET は、「Microsoft EMET Service」と呼ばれる Windows Service を通じて、レポートを提供する機能を備えています。一旦 EMET をインストールすると、このサービスは自動的に Windows でスタートするよう設定されます。EMET Service は、EMET アイコンでタスクバーのシステム トレイ領域に現れる EMET エージェントを配信する役割を担っています。トレイ領域での EMET エージェントの表示はグループ ポリシー、またはコマンドライン ツールを通じて設定可能です。

EMET Service は、以下のタスクを実行します:

Windows イベント ログにイベントを書き込む: EMET イベントは、EMET と呼ばれるイベント ソースを介してログをとります。これらログは、アプリケーション ログで見つけることができます。ログは、3 段階別で存在しています。情報、警告、そして、エラーです。情報メッセージは、EMET エージェントが開始した通常のオペレーションなどのログをとるために利用されます。警告メッセージは、EMET の設定が変更される、あるいは、例外ルールによって SSL 証明書の証明書信頼の検出をレポートするために利用されます。エラー メッセージは、信頼できない SSL 証明書が検出された場合、あるいは、EMET がその緩和策の一つで悪用を停止した場合 (これは起こり得る積極的な攻撃が防御されたことを意味する) などのログをとるケースに利用されます。 EMET レポートと関連する可能性のあるイベント ID のリストは下記に掲載されています。ユーザーは、いくつかの緩和策がシステム緩和策として設定されている場合、およびオペレーティング システムの提供するものであった場合に EMET によって完全にログされない可能性があることに注意しなければなりません。

表 1: イベント ID フォーマット

イベント レベル	イベント ID
情報	[S]0
警告	[S]1
エラー	[S]2

[S] は、ログ イベントを送信するサブシステムを特定するために使用される番号です *(利用可能な値: 0-4)*

表 *2:* 予想されるイベント *ID*

イベント レベル	緩和策	GUI	コマンド ライン	エージェント	証明書信頼
情報	00	10	20	30	40
警告	01	11	21	31	41
エラー	02	12	22	32	42

表 *3:* イベント ログに利用可能な *EMET* 緩和策

強制 ASLR	DEP	SEHOP	EAF	EAF+	ヒープ スプレー	ボトムアップ	Null ページ	ロード ライブラリ	メモリ保護	強制フローのシミュレーション	スタック ピボット	ASR
✔ *	✔ *	✔ *	✔	✔	✔	✘	✘	✔	✔	✔	✔	✔

(*) システム緩和策として設定された場合、ログ エントリを生成しない場合がある

タスクバー通知領域にあるヒントを通じて重要なイベントを表示する: Windows イベント ログに書かれたエラー メッセージと深刻度は似ており、EMET が緩和策の一つで悪用を停止する、あるいは、信頼できない SSL 証明書を検出した場合に、ユーザーに向けて、どのアプリケーションが停止しているのか、そして悪用を停止するためにどの緩和策が使用されたのかが表示されます。証明書信頼の違反があった場合は、現在の HTTPS 接続上の信頼できない SSL 証明書に関する詳細が表示されます。

証明書信頼検証タスクを実行する: SSL 証明書、ルート CA 証明書、およびピン設定ルールは、EMET Service が有効で実行されている場合のみ実行され、検証が行われます。

早期警告プログラムについてレポートを送信する: EMET は、「Early Warning Program (早期警告プログラム)」レポート機能を提供します。EMET によって悪用の試みが検出、およびブロックされた際、攻撃に関わる一連の情報が、標準の Windows Error Reporting 機能を通じてマイクロソフトに送信されます。この情報は、マイクロソフトがゼロ デイ悪用に関連する情報を得る際に役立ち、より大きな脅

威となる前に問題の改善が促されます。もし、脆弱性がサード パーティ ベンダーが提供するソフトウェアと関連している場合は、マイクロソフトは Microsoft Vulnerability Research (マイクロソフト脆弱性調査) プログラムを通じて、影響を受けるベンダーと協力して、問題の改善に努めます。 また、早期警告プログラム レポート機能は、マイクロソフト オンライン サービスに関わる、疑わしい SSL 証明書に関連する情報もマイクロソフトに送信します。マイクロソフトに対して送信されるデータの種類に関する詳細については、EMET GUI 内の [Help] リボン、または http://aka.ms/EMETps からも利用可能な「Privacy Statement.rtf」ファイルを参照してください。

注: EMET のレポート機能は、デスクトップ アプリケーション上でのみ利用可能です。モダン アプリケーションはこの機能を活用することはできません。

サポートされているオペレーティング システム、およびソフトウェア要件

サポートされているオペレーティング システム、およびアプリケーション

EMET 5.5 は、以下のオペレーティング システム、およびサービス パック レベルをサポートします: (または最新、Windows サポート ライフサイクルの範囲内に限る):

クライアント オペレーティング システム

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 Service Pack 1
- Windows Vista Service Pack 2

サーバー オペレーティング システム

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 Service Pack 1
- Windows Server 2008 Service Pack 2

すべてのオペレーティング システムに対し、すべての緩和策がサポートされているわけではないことに注意してください。

表 *4:* システム緩和策互換性マトリックス

緩和策の種類	緩和策	Vista、Windows 8、8.1/Server 2008 および以降のバージョン	Windows 10
システム規模	DEP	✔	✔
	SEHOP	✔	✔
	ASLR	✔	✔
	信頼されていないフォント	✘	✔
アプリケーション	DEP	✔	✔
	SEHOP	✔	✔
	NULL ページ	✔	✔
	ヒープ スプレー	✔	✔
	強制 ASLR	✔	✔
	EAF	✔	✔
	EAF+	✔	✔
	ボトムアップ ASLR	✔	✔
	ロード ライブラリ	✔	✔
	メモリ保護	✔	✔
	実行フローのシミュレーション	✔	✔
	スタック ピボット	✔	✔
	コーラー チェック	✔	✔
	ASR	✔	✔
	信頼されていないフォント	✘	✔

さらに、64 ビットシステム上では、あるアプリケーションの特定の緩和策については、32 ビット プロセスで実行している場合にのみ適用可能なものがあります。詳細については、以下の表を参照してください:

表 *5:* アプリケーション緩和策互換性マトリックス

緩和策の種類	緩和策	32 ビット プロセス	64 ビット プロセス
アプリケーション	DEP	✔	✔
	SEHOP	✔	✘
	NULL ページ	✔	✔
	ヒープ スプレー	✔	✔
	強制 ASLR	✔	✔
	EAF	✔	✔
	EAF+	✔	✔
	ボトムアップ ASLR	✔	✔
	ロード ライブラリ	✔	✔
	メモリ保護	✔	✔
	実行フローのシミュレーション	✔	✘
	スタック ピボット	✔	✔
	コーラー チェック	✔	✘
	ASR	✔	✔
	信頼されていないフォント	✔	✔

EMET は、仮想マシンにインストールし、利用可能ですが Microsoft App-V、あるいは VMware ThinApp™ などの仮想化されたアプリケーションについてはサポートしていません。

証明書信頼機能は Internet Explorer のみサポートされていますが、実験的設定で他のブラウザー用に設定することも可能です。サード パーティ ブラウザーに関する詳細情報は、証明書信頼機能の設定の項目を参照してください。

ソフトウェア要件

EMET は、Microsoft .NET Framework 4 が必須です。また、EMET が Windows 8、および Windows Server 2012 上で適切に稼働するために、マイクロソフト サポート技術情報 2790907 – Windows 8 および Windows Server 2012 用の互換性更新プログラムをご利用いただけます、またはより最新の互換性更新プログラムのインストールが必須です。

EMET の設定

セキュリティ緩和策を有効にするためには EMET をインストール後 EMET の設定をしなくてはなりません。EMET を構成するためには、以下の設定を指定しなくてはいけません:

- どの緩和策を有効にすべきか
- どのアプリケーションが、どの緩和策で保護されるべきか
- どの SSL/TLS 証明書ピン設定ルールを導入するのか

システム、およびアプリケーションの双方の緩和策についても、EMET グラフィカル ユーザー インターフェース、あるいは EMET コマンド ライン ツールを通じて設定可能です。SSL/TLS 接続向けの証明書信頼機能については、EMET グラフィカル ユーザー インターフェースを通じてのみ設定可能です。設定を完了するために、これらインターフェースをどのように利用すれば良いかについては、このガイドの EMET グラフィカル ユーザー インターフェース、および EMET コマンド ライン ツールの項目を参照してください。

EMET のシステム、および、アプリケーション緩和策の設定をするには、グループ ポリシーを利用することも可能です。グループ ポリシー サポートについては、グループ ポリシーの項目で解説しています。

その他の EMET を設定するオプションには、保護プロファイルを利用する方法があります。これら保護プロファイルには何が含まれているのか、その詳細についてはセクション 2.1 を参照してください。

EMET を設定する最も簡単な別の方法として、設定ウィザードを利用する方法があります。インストールの最後に、設定ウィザードから一連の推奨する設定を展開するよう尋ねてきます。手動の設定が好ましい場合は、設定ウィザードを無視することも可能です。設定ウィザードに関する詳細情報は、設定ウィザードの項目 を参照してください。

通常の EMET 設定は、レジストリ サブ キー *HKLM¥SOFTWARE¥Microsoft¥EMET* に保存され、制限的なユーザー固有の設定は *HKCU¥SOFTWARE¥Microsoft¥EMET* に保存されます。グループポリシー

を介して構成された EMET 設定は、レジストリ サブ キー HKLM¥SOFTWARE¥Policies¥Microsoft¥EMET に保存されます。一部のアプリケーションごとの設定は、HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Image File Execution Options にある場合もあります。64 ビット プラットフォームでは、設定はレジストリ内の 64 ビット ハイブおよび 32 ビット対応の両方に保存されている場合があります (例: Wow6432Node) 。

EMET 保護プロファイル

EMET には、既定でアプリケーション用の保護プロファイル、および、証明書信頼向けの保護プロファイルが 1 点、既定で付いてきます。保護プロファイルは、一般的なマイクロソフト、およびサード パーティ アプリケーション用に事前に設定された EMET 設定を含みます。EMET インストール ディレクトリでは、これらのファイルは展開/保護プロファイル フォルダーに保存されています。現状のままで有効、修正可能で、新しい保護プロファイルの作成に利用することもできます。

EMET に含まれるプロファイルは

Recommended Software.xml: Microsoft Internet Explorer、WordPad、Microsoft Office スイートに含まれるアプリケーション、Adobe Acrobat、Adobe Reader、そして Oracle Java に対する緩和策を有効にします。

Popular Software.xml: その他一般的なアプリケーションに対する緩和策を有効にします。

CertTrust.xml: Microsoft アカウント、Microsoft Office 365、および、Skype、そして Twitter、Facebook、および Yahoo などのログイン サービス用の証明書ピン設定ルールを有効にします。

注: EMET の保護プロファイルは、いくつかのアプリケーションに対する既知の互換性の問題を考慮に入れて、最適構成で更新されました。EMET で利用可能な既定の証明書信頼ルールは、保護されている SSL 証明書の満了前に、個別の満了日別にそれぞれのルールを無効にするよう設定されています。

Popular Software.xml からいくつかのルールを見てみましょう。

```
<App Name="Word" Path="*¥OFFICE1*¥WINWORD.EXE">
<Mitigation Enabled="true" Name="ASR">
<asr_modules>flash*.ocx</asr_modules>
</Mitigation>
</App>
```

このルールが EMET に利用可能なすべての既定のメモリー緩和策で Microsoft Word を保護するように知らせます。そして、“flash*.ocx” と一致する任意のモジュールの読み込みをブロックする ASR を追加します。特定のアプリケーションの設定を必要とする ASR、および EAF+ を除き、既定で保護プロファイル内のすべてのアプリケーション用に、すべての緩和策が有効化されます。これは、プロファイルファイル内の DefaultConfig ノードを編集することで変更できます。

<Product Name="Windows Media player">

<Version Path="*¥Windows Media Player¥wmplayer.exe">

<Mitigation Enabled="false" Name="MandatoryASLR"/>

<Mitigation Enabled="false" Name="EAF"/>

<Mitigation Enabled="false" Name="SEHOP"/>

</Version> </Product>

このルールで、強制 ASLR、EAF、そして SEHOP を除く、Windows Media Player 向けのすべての緩和策を有効にします。もう一つの重要な情報はパスです。“*¥Windows Media Player¥wmplayer.exe” というパスがあります。パスは、アプリケーション用に緩和策を登録するために EMET が利用するものです。緩和策が実施されるためには、ターゲットのアプリケーションのパスと合致していなければなりません。

アプリケーションのパスのフルネームを指定する必要があります。* あるいは ? などのワイルドカードを使用することも可能です。もう一つのオプションは、wmplayer.exe などのように、パスなしで実施可能な名前を使用する方法です。

ワイルドカードは、パスについてのみ承認され、実行可能な名前では承認されないことをご承知ください。例えば、“wmplayer.exe” または “*¥wmplayer.exe” は有効なパスですが、“*wmplayer.exe” は無効です。これは、EMET が依存する Windows 内のアプリケーション互換性フレームワークの制約によるものです。

新規開始のプロセスが複数の特定のパスと一致した場合、EMET は長いパス指定子を持つルールを選択します。これは、最も明確な一致を選んで概算します。

保護ファイルは、プログラムの注釈がしっかりしています。コメント欄を読むのは、この機能について学ぶ良い方法です。保護プロファイルは、EMET グラフィカル ユーザー インターフェース、EMET コマンド ライン ツール、あるいはグループ ポリシーを通じて有効化できます。

EMET グラフィカル ユーザー インターフェース

EMET と情報をやりとりする方法の 1 つが、グラフィカル ユーザー インターフェース (GUI) を利用するものです。EMET をインストールする際に、スタートメニュー/ウィンドウ アイコンから起動することができます。このセクションでは、多様なウィンドウ、およびセクションについて説明します。EMET GUI を起動すると、以下のウィンドウが表示されます。

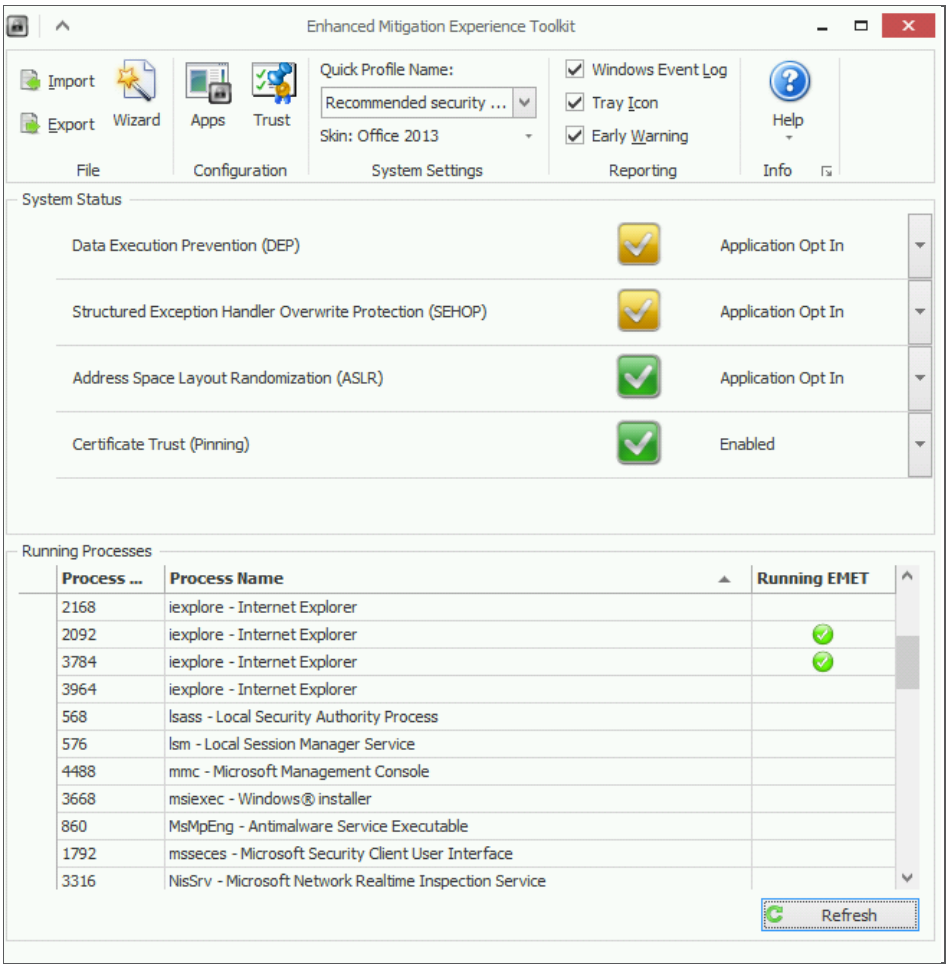

図 10: EMET GUI メイン ウィンドウ

EMET GUI は 3 つのセクションにわかれています。上から下まで順に:

リボン:

- **File (ファイル):** このグループは、EMET の設定の [Import (*Ctrl*+*Shift*+*I*)]、または [Export (*Ctrl*+*Shift*+*E*)]、そして EMET Configuration Wizard (*Ctrl*+*Shift*+*W*) の実行を許可します。その他の詳細については設定ウィザードを参照してください。このグループは、レジストリ設定の代わりにグループ ポリシーで設定を有効にすることもできます。ローカルまたは Active

Directory のグループ ポリシーを設定するには、リモート サーバー 管理ツール (RSAT) をインストールする必要があります。

- **Configuration (設定):** このグループは、[Apps] (*Ctrl+Shift+A*) をクリックすることで [Application Configuration (アプリケーション設定)] ウィンドウ、そして [Trust] (*Ctrl+Shift+T*) をクリックすることで「Certificate Trust Configuration (証明書信頼設定)] ウィンドウへのアクセスを許可します。その他の詳細についてはアプリケーション用の緩和策を設定する、および証明書信頼の設定（ピン設定ルール）を参照してください。
- **System Settings (システムの設定):** このグループは、システムにクイック プロファイルを適用するだけではなく、EMET GUI の外観を選択できます。その他の詳細については、システム規模の設定を構成するを参照してください。
- **Reporting (レポート):** このグループはレポート オプションが切り替えられます。その他の詳細については、レポートを設定するを参照してください。
- **Help (ヘルプ):** このグループは、サポート フォーラム、およびユーザー ガイド (*Ctrl+Shift+F1*) などのヘルプ リソース、そして EMET プライバシー声明へアクセスできます。

System Status (システムのステータス): このセクションは、システム緩和策 (DEP、SEHOP、および ASLR) の現在のステータス、および証明書信頼機能のステータスを表示します。これらの設定は、このセクションから直接変更可能です。

Running Processes (稼働プロセス): このセクションでは、現在稼働しているアプリケーションのリスト、および、EMET で保護されているアプリケーションを表示します。アプリケーションのリストは 30 秒毎に更新され、[Refresh (更新)] ボタンをクリックすることで手動更新も可能です。また、キーボードとの組み合わせ *CTRL + F* でリスト内の特定のアプリケーションを検索することもできます。

設定ウィザード

設定ウィザードは、EMET インストールの最後に表示され、公正な EMET インストールのために、推奨される設定を適用するか、あるいは、手動で EMET を設定する、のいずれかを行うことができます。前バージョンの EMET から更新する場合、現在の設定を残せます。

設定ウィザードは、システムに 既に EMET が設定されているかを自動的に検出し、それに準じて異なるオプションを提案してきます。

私たちは、新規のインストール、および更新のシナリオの双方について常に推奨される設定を適用し、必要に応じて EMET の設定を切り替えることを強くお奨めします。

ウィザード オプション

Use Recommended Settings (推奨設定を使用): このオプションでは、あらゆる既存の設定を削除し、推奨される設定を適用します:

- **Application Configuration (アプリケーションの設定):**
  - Internet Explorer、WordPad、Microsoft Office、Adobe Acrobat および Reader そして Oracle Java 向けの保護を追加します。
  - EAF+ を Internet Explorer、Microsoft Trident Engine、Adobe Flash プラグイン、Microsoft VML プラグイン、Microsoft VBScript エンジン、および Microsoft JavaScript エンジンと設定します。Adobe Acrobat、および Adobe Reader を Lotus Notes Filed Exchange Module for Adobe Acrobat、Adobe Reader エンジン、および Adobe Acrobat フォームと設定します。
  - Adobe Flash プラグインが Microsoft Excel、PowerPoint、および Word で実行されるのを阻止し、Oracle Java、Microsoft VML、Microsoft MSXML 4.0、Windows Script Host Runtime、および Microsoft Scripting Runtime プラインが信用済みサイト、あるいはイントラネット ゾーンに属していない Internet Explorer の Web サイトで実行されるのを阻止します。
- **Certificate Trust (証明書信頼):** Microsoft、およびその他サード パーティのオンライン サービス向けのルールを追加します。
- **Reporting (レポート):** すべてのレポート機能 (Windows イベント ログ、トレイ アイコン、および早期警告プログラム) を有効にします。

(新規のインストール) 後で設定を手動で行う: このオプションでは、EMET の設定は行われません。

(以前のバージョンからアップグレードする) Keep Existing Settings (既存の設定を残す): このオプションは、既存の EMET の設定を残します。EMET の新機能に関連する 2 件のオプション設定は自動的に設定可能です:

- Certificate Trust (証明書信頼): Microsoft、およびその他サード パーティのオンラインサービス向けのルールを追加します。
- Reporting (レポート): 早期警告プログラムを有効にします。

システム規模の設定を構成する

システムの設定を構成する方法は 2 つあります。[System Settings] リボン グループから 2 つのシステム緩和策プロファイルの内、1 つを選択する、あるいは個別に緩和策の設定をするといういずれかの選択肢があります。

システムの再起動が必須な設定変更もあることに注意してください。 EMET GUI は、必要に応じて、通知を行います。

利用可能なシステム緩和策のリストは、利用する Windows のバージョンによって異なります。これは、すべてのシステム緩和策は、すべてのバージョンの Windows では利用可能でないためです。Windows バージョン別におけるシステム緩和策サポートに関する詳細情報はサポートされているオペレーティング システム、およびソフトウェア要件に記載されています。

証明書信頼機能は、関連するエントリを変更することで、有効にも無効にもできます。さらに、[Application Configuration] に Internet Explorer を追加しなければなりません。

アプリケーション用の緩和策を設定する

EMET が提供する緩和策を適用するために、具体的なアプリケーションを設定することができます。更に、緩和策は個別にアプリケーション単位で有効、もしくは無効にすることができます。

例えば、すべての EMET 緩和策を適用するために iexplore.exe を設定でき、それと同時に、SEHOP、および強制 ASLR のみに winword.exe を適用できます。

アプリケーションを適用外にするフォント チェックボックスにチェックを入れると、Windows 10 の信頼されていないフォントの緩和策からそのアプリケーションが適用外になりますのでご注意ください。この設定は推奨していませんが、標準フォントのディレクトリにインストールされていないフォントを使用している特定のアプリケーションをお持ちの場合は有効です。

対応するボタンをクリックすることで、リストからアプリケーションを追加 (*Ctrl* + *Shift* + 正符号 *(+)* キー)、および削除 (*Ctrl*+ マイナス記号 *(-)* キー) できます。アプリケーションを追加する際は、ユーザーには通常の「ファイルを開く」というダイアログが表示されます。その後、アプリケーションを選択でき、リストに追加可能です。 [Add Wildcard (ワイルドカードを追加する)] (*Ctrl*+ *Shift* + アスタリスク *(*)* キー) ボタンは、ワイルドカードをそのパスに追加することでアプリケーションの設定を可能にします。

緩和策名列、あるいはアプリケーション行を右クリックすると、多数の緩和策を有効/無効にできます。

「OK」ボタンをクリックした場合のみ設定が適用されます。

追加の緩和策設定

EMET 緩和策に対し、追加の設定を行うことが可能です。これらの設定は、[Application Configuration] ウィンドウからアクセスできます。

[Default Action (既定のアクション)] リボンは、悪用が検出された場合に EMET がどのようなアクションを実行するのか定義します:

- **Stop on exploit (悪用を止める):** EMET は、悪用の試みを報告し、プロセスを終了します。
- **Audit only (監査のみ):** EMET は、悪用の試みを報告しますが、プロセスは終了しません。このモードは、すべての緩和策に対し適用可能ではありません。なぜなら、悪用の試みが検出された場合、プロセスが既に実行されているため修復できない場合があるからです。この機能をサポートする緩和策は下記です:
    - EAF
    - EAF+
    - ROP 緩和策: LoadLib、MemProt、Caller、 StackPivot, SimExecFlow
    - SEHOP (Windows Vista、および Windows Server 2008 のみ)
    - ASR

[Options (オプション)]リボン内の [Show All Settings (すべての設定を表示する)] ボタンは、一部の緩和策の、追加の強制特質を微調整、あるいは設定を許可します。現在、このパネル経由で設定可能な緩和策は下記の通りです:

- **Heap Spray (ヒープ スプレー):** この緩和策用に事前に割り当てるために、メモリ アドレスの設定ができます。
- **Simulate Exec Flow (実行フローをシミュレートする):** シミュレートされた指示の数を特定し、チェックできます。
- **EAF+:** 保護アプリケーションのインポート/エクスポート テーブルを評価して、どのモジュールが阻止されたか特定できます。この設定に既定値はありません。

  [Modules (モジュール)] フィールドは、保護アプリケーションのエクスポート、およびインポート テーブル アドレスへのアクセスを制限されているモジュールがどれか特定します。ここで特定されるべきモジュールは、悪用の最中に API を解決するのに活用されるものである可能性があり、アプリケーション毎に異なります。既定設定は、保護アプリケーションの悪用の最中に

使用されたと確認されている、あるいは今後使用される可能性のあるモジュールのリストを含みます。ユーザーは、モジュール名にワイルドカードを使用でき、セミコロン (;) で区切ることで複数のモジュールを特定できます。例をあげると module1.dll; module2.ocx; module3*.dll などです。

- **ASR:** 保護アプリケーションにロードされるのを阻止されるモジュール/プラグインの一覧を特定できます。この設定には規定値はなく、強制で緩和策を有効にします。

  [Molules (モジュール)] フィールドは、保護アプリケーションにロードされるのを阻止されるのがどのモジュールか特定できます。ユーザーは、モジュール名にワイルドカードを使用でき、セミコロン (;) で区切ることで複数のモジュールを特定できます。例をあげると module1.dll; module2.ocx; module3*.dll などです。

  [Internet Xone Exeptions (インターネット ゾーン除外)] ドロップダウンは、どのインターネット セキュリティ ゾーンに対して ASR が適用されないか (除外) を特定します。この設定は、インターネット セキュリティ ゾーン (例： トライデント エンジン) をサポートするアプリケーションのみで有効です。例えば、「ローカル インターネット」および「信頼済みサイト」を選択すると、これら 2 つのゾーンに定義されたモジュールがロードされます。

証明書信頼 (ピン設定) の設定

この機能、「証明書信頼 (ピン設定)」を有効にするには、「システム規模の設定を構成する」の項目で説明されているように有効にすることが必須で、「アプリケーション用の緩和策を構成する」の項目で説明されているように、iexplore.exe プロセスは保護されているアプリケーションに追加されなければなりません。証明書信頼機能を利用するために、有効にしなければならない緩和策は他にはありません。

EMET GUI ウィンドウのメイン画面にある、リボン グループ [Configuration] の [Trust] (*Ctrl* + *Shift* + *T* キー) ボタンをクリックすることで、SSL/TLS 証明書ピン設定ルールを構成することが可能です。[Certificate Trust Configuration] ウィンドウからは、保護されている Web サイト (SSL 証明書の項目名)を追加、あるいは列挙することが可能で、個別の Web サイトに対し、既存のルールを指定することができます。[Add / Remove] リボン内の、 [Add Website] (*Ctrl* + *Shift* + 正符号 *(+)* キー) をクリックした後、SSL 証明書に記されている通りに、Web サイトの完全修飾ドメイン名を入力します。
(注：ワイルドカード、あるいはその他の記号は利用できず、名前はリスト内で固有のものでなければなりません)

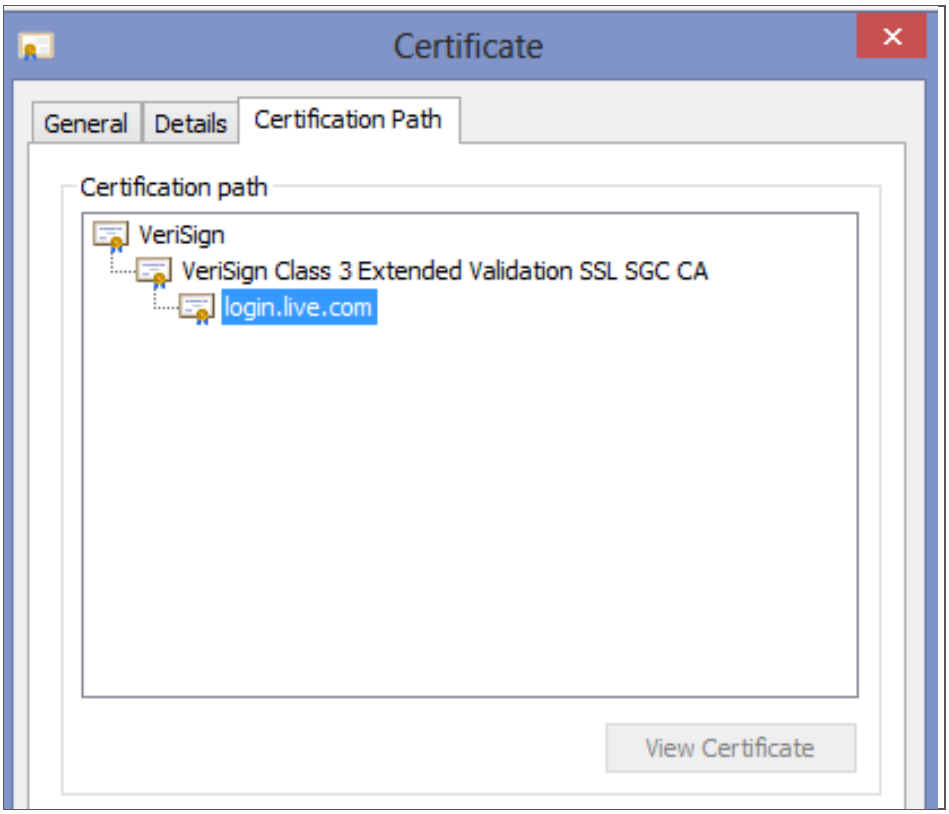

図 *11: login.live.com* の証明書信頼チェーン

次のステップでは、Web サイトに「ピン設定」を割り当てます。ルールがない場合は、 [Pining Rules] タブをクリックします。適用可能なルールのリストがウィンドウに表示されます。

このウィンドウでは、Web サイトに割り当てることのできる証明書ピン設定ルールを明確にできます。新しいルールを作成するには、[Add / Remove] リボン グループの [Add Rule] (*Ctrl* + *Shift* + 正符号 *(+)* キー) をクリックし、テーブルに適切な数値の、最低 3 つのパラメーターを入力します:

Name (名前): ルール用の独自の識別子で、後で、[Protected Websites] タブからアクセスできます。

Certificates (証明書): ユーザー証明書ストア (certmgr.msc) 内の信頼済みルート証明書フォルダーの定義、およびインポートを許可するためにウィンドウを開きます。このリストから、1 つ以上の信頼済みルート証明機関 を選択することができます。もし、リスト内にルート CA がなければ、事前にインポートする必要があります。

Rule Expiration (ルールの終了): ルールがいつ終了するのか、設定します。ルールが終了すると、これは無視されるようになり、ルールが終了したことを通知するために、EMET エージェントにログ イベントが書き込まれます。

Blocking Rule (ブロックの設定): 有効化されると、ルールの不一致が検出された場合に EMET が接続を停止します。

EMET の証明書信頼設定ダイアログ ボックスに、最小キー サイズ、許可されている国、ブロックされるハッシュ、および公開キーの照合が表示されていても、今後 EMET はこれらを使用しませんのでご注意ください。

一旦、ルールが定義されたら、[Protected Websites] タブをクリックし、希望の Web サイトにそのルールを付与します。ピン設定ルールは複数の Web サイトに付与することができますが、1 つの Web サイトに付与できるピン設定ルールは 1 件のみです。

[Protected Websites]、および [Pinning Rules] のエントリは、テーブルのエントリをクリック、または、後で、リボン グループの [Add / Remove] の [Remove Website]、あるいは [Remove Rule] (*Ctrl* + マイナス記号 *(-)* キー) をクリックすることで削除の必要があるものを削除できます。いずれの Web サイトでも使用されていない場合のみ、ピン設定ルールを削除できます。特定の [Protected Websites] 向けの保護は、[Active] 列のチェックボックスをはずすことで一時的に無効とすることができます。

一旦設定が行われると、もし、ブラウズしている最中にピン設定の 1 つが引き起こされた場合、EMET は設定されたルールと合致しない SSL 証明書を検出し、レポートの設定 (早期警告レポート機能は、証明書信頼機能では利用できません)、および引き起こされた設定がブロックの設定であるかどうかに準じて対応します。

EMET グラフィカル ユーザー インターフェース (EMET_GUI.exe) は、「Certificate Trust (証明書信頼)」エントリを設定するインターフェースを提供します。しかしながら、 EMET_GUI もしくは EMET_CONF のいずれかを利用して、以前にエクスポートしたピン設定構成をインポートすることも可能です。

証明書信頼ピン設定を作成する方法の例は、Security Research & Defense Blog の、このブログ投稿 (英語情報) で確認することができます。

設定レポート

EMET 警告のレポートの精度を細かく、設定することができます。EMET が悪用の試み、あるいはピン設定を侵害する SSL 証明書を検出した場合、EMET エージェントがアクションを実行します。このアクションは、Windows イベントログに書き込む、警告を表示する、または両方ともの、いずれも定義することができます。早期警告プログラム悪用の検出のみに利用可能です。

EMET GUI メイン ウィンドウから直接、攻撃を検出している際に、EMET がどのアクションを実行するか設定することが可能です。[Reporting] リボン グループには 3 つのエントリ、Windows Event Log、Tray Icon、そして Early Warning があります。

Windows Event Log: EMET が Windows イベント ログに書き込みます。

Tray Icon: EMET エージェントが攻撃の詳細を含む、ポップ アップを表示します (検出、および攻撃を止めるために利用される対象プロセス、および緩和策)。

Early Warning: EMET は、メモリ ダンプ、および検出、そして攻撃を停止するために利用された緩和策の種類を含む、攻撃に関する一連の情報を生成し、標準のマイクロソフト エラー レポート チャンネルを介してこの情報をマイクロソフトに送信します。ユーザーは、マイクロソフトに送信される情報を送信が発生する前にレビューできる機会を持つことができます。

注:カスタムの [Tray Icon] メッセージの詳細設定向けの詳細オプションについては、詳細設定の項目を参照してください。

設定の外観

EMET では、EMET GUI、および EMET GUI、そして EMET エージェント双方の多様なグラフィカル コンポーネントの概観とイメージを設定することができます。EMET のテーマは、リボン グループの [System Settings] の [Skin] をクリックすることで、EMET GUI ウィンドウから変更することができます。

ユーザー補助

EMET GUI では Windows の提供するユーザー補助機能により忠実に準拠するようにユーザー補助機能を提供しています:

- キーボード ナビゲーションを全支援
- ハイコントラスト支援を全支援
- 異なるテキスト サイズ、既定より最大で 200% 拡大までフルサポート
- ナレーターによるサポート

EMET コマンドライン ツール

EMET を設定する代替的な方法として、EMET_Conf.exe を利用する方法があります。このコマンドライン ユーティリティは EMET がインストールされたロケーションで見つけることができます。 一方、EMET 5.5 には、以下の新たなサブ オプションが追加されました。

EMET コマンドライン ツールを引数なしで実行すると、すべての、現在サポートされているアプリケーションに特化した緩和策だけでなく、すべてのサポートされているシステム緩和策を含む、使用状況が

表示されます。現在、コマンドライン ツールはすべての EMET 機能の設定を許可するわけではありません。

以下は、EMET コマンドライン ツールがサポートしている設定に関わるオプションです。

サブ オプション

以下の構成ができます:

- ASR モジュールおよびゾーン
- EAF モジュール
- シミュレートされた命令の ROP シミュレート実行手順の数

複数のコマンドを同時に実行

一行に複数のコマンドがあります。同じ行に任意のコマンドを追加することが可能になりました。構文の検証が完全かつ正常に完了すると、コマンドは左から右へ順番に実行されます。

使用例:

EMET_Conf.exe --set prog1.exe +DEP -SEHOP --set prog2.exe -DEP +StackPoint –list

上記のコマンドは 2 つのプログラムの設定を変更し、新規のアプリケーションの構成を表示します。

プレフィックスオプションで、 “-- “ (オリジナル EMET スタイル)、“-“ (Unix スタイル) または “/” (Windows スタイル) を頭に付けることができます。異なるプレフィックスを同じコマンドで使用できます。

出力と戻り値

成功した場合、EMET_conf.exe は既定で呼び出しプロセスに対して 0 を返し、何も表示しません。

標準出力は、具体的に表示を要求するすべてのコマンドで使用されています (例: command “list)。

エラー出力 (stderr) は、その他すべて、主にエラーで使用されます。

以下は、EMET コマンドライン ツールがサポートする構成に関わるオプションです。

ヘルプを表示する

EMET_Conf --help

EMET_Conf /?

すべてのサポートされているシステムの緩和策だけでなく、現在サポートされているアプリケーションの特定の緩和策の利用状況の画面を表示します。

引数なしで EMET コマンドライン ツールを実行すると、コマンド ヘルプと同等の効果があります。

使用例:

“EMET_Conf --help

解析のみ (実行なし)

EMET_Conf -- parseonly

実行なしで構文を検証します。オプションとそれに依存するサブオプションの間を除いて、コマンドのどこにでも設定できます。

使用例:

“EMET_Conf -set myprog.exe +DEP -SEHOP -parseonly

EMET にアプリケーションを追加または修正する

EMET_Conf --set [--force] <実行ファイルのパス> [(+|-)緩和策…[modules|zones|number] …]

<実行ファイルのパス> は、アプリケーションへのフル パス名となる場合があります。* もしくは、? などワイルカードを利用することも可能です。

その他のオプションは、パスなしで実行可能な名前、例えば wmplayer.exe などを利用する方法です。

ワイルドカードは、パス部分でのみ承認され、実行可能なイメージ名では無効となることに注意してください。例えば、 “wmplayer.exe” あるいは “*¥wmplayer.exe” は有効なパスですが、“*player.exe” もしくは “*wmplayer.exe” は無効です。これは、EMET が依存する、Windows 内のアプリケーション互換性フレームワークの制限によるものです。

--force オプションは、現在システム上にインストールされていないアプリケーション用に、EMET を設定するために利用されます。

サブ オプション:

- オプション “(+|-)ASR は 2 つのサブ オプション：-- modules と – zones

  使用例: *“EMET_Conf /set prog.exe +EAF -modules malware.dll -zones "1;2" +DEP*

- オプション “(+|-)EAF は 1 つのサブ オプション：-- modules

使用例: *“EMET_Conf /set prog.exe +ASR -modules suspicious.dll*

- オプション “(+|-)SimExecFlow は 1 つのサブ オプション：-- number (シミュレートされた命令数)

  使用例: *“EMET_Conf /set prog.exe +SimExecFlow -number 12*

その他使用例:

“EMET_Conf /set program.exe” は program.exe 向けのすべての緩和策を有効にします。

“EMET_Conf --set program.exe --DEP” は、program.exe 用の DEP を除くすべての緩和策を有効にします。

どのアプリケーションで EMET が有効になっているかリストする

EMET_Conf --list

初めに、ローカルで構成された設定 (EMET_GUI あるいは、EMET_CONF) を表示し、続いて、グループ ポリシー を介して構成された設定と、EMET 用のすべてのアプリケーション緩和策を表示します。

どのシステム緩和策が、EMET によって有効になっているかリストする

EMET_Conf --list_system

初めに、ローカルで構成された設定 (EMET_GUI あるいは、EMET_CONF) を表示し、続いて、グループ ポリシー を介して構成された設定と、すべてのシステム緩和策を表示します。

証明書信頼設定をリストする

EMET_Conf --list_certtrust

ローカルで構成された (EMET_GUI あるいは EMET_CONF) 、すべての証明書信頼 Web サイト、およびピン設定を表示します。

EMET からアプリケーションを削除する

EMET_Conf --delete <実行ファイルのパス>

<実行ファイルのパス> は、フルパス、ワイルドカードを含むパス、または、実行可能な名前のみの場合があります。それは、EMET にアプリケーションを追加する際に使用された

<実行ファイルのパス> と合致しなければなりません。

EMET からすべてのアプリケーションを削除する

EMET_Conf --delete_apps

これは、すべての EMET アプリケーション緩和策設定を削除します。グループ ポリシー を介して構成されたアプリケーション緩和策設定については削除されないことに注意してください。

すべての証明書信頼設定を削除する

EMET_Conf --delete_certtrust

これは、EMET からすべての証明書信頼設定を削除します。

すべての EMET 設定を削除する

EMET_Conf --delete_all

これは、すべての EMET アプリケーション緩和策設定、および、証明書信頼設定を削除します。

“--delete_apps” と “--delete_certtrust” を同時に稼働するのと同等です。

システム緩和策を修正する

EMET_Conf --system [--force] <SysMitigation=State> [SysMitigation=State …]

--force オプションは、緩和策を不安定な状態に設定するために必要です。この詳細情報は、詳細オプションの項目を参照してください。不安全なオプションは既定で、コマンドライン ユーティリティ、もしくは UI のいずれでも非表示です。--force オプションは、システム規模の DEP 緩和策の設定が変更され、BitLocker がインストールされた際にも必要です。

強化緩和策オプションを修正する

EMET_Conf --deephooks (enabled|disabled)

EMET_Conf --antidetours (enabled|disabled)

EMET_Conf -- eafplus (enabled|disabled)

Xml ファイルからアプリケーション設定をインポート/エクスポートする

EMET_Conf --import [--force] <xml ファイル>

以前にエクスポートされた設定をインポートします。このコマンドは、保護されたプロファイル、あるいは証明書信頼機能に対するすべての設定、例えば、EMET_Conf --import “Deployment¥Protection Profiles¥Popular Software.xml” などをインポートし、有効にすることも可能です。

--force オプションは、緩和策を安全ではない状態に設定する Xml ファイルをインポートするのに必要です。この詳細情報は、詳細設定の項目を参照してください。--force オプションは、システム規模の DEP 緩和策の設定が変更され、BitLocker がインストールされた際にも必要です。

EMET_Conf --export <xml ファイル>

現在の設定を特定の xml ファイルにエクスポートします。

レポート設定を構成する

EMET_Conf --reporting (+|-)(telemetry|eventlog|trayicon)

このスイッチは、レポートが発生する方法を構成します。このコマンドと切り替わる設定は下記です:

- **eventlog:** このキーワードは、Windows イベントシステム内の攻撃の記録を有効、または無効にします。
- **trayicon:** このキーワードは、ユーザーに対する目に見える通知を有効、または無効にします。
- **telemetry:** このキーワードは、早期警告プログラム機能を、有効、または無効にします。 このコマンドの使用法の例は下記のとおりです:

EMET_Conf --reporting -telemetry +eventlog +trayicon

悪用に対するアクション設定を構成する

EMET_Conf --exploitaction (audit|stop)

このスイッチは、悪用が発生した場合に EMET がどのように反応すべきか設定します:

- **audit (監査):** 適用できる場合に、プロセスを停止はせずに、ただ悪用の試みを記録します。
- **stop (停止):** 悪用の試みが検出された場合に、プログラムを停止します。

トレイ領域の EMET エージェント アイコンの表示を設定する

EMET_Conf --agentstarthidden (enabled|disabled)

このスイッチは、トレイ領域の EMET エージェント アイコンの表示を設定します。

EMET を適用する

EMET では、企業が適用に際して、既存の管理基盤を生かすことができ、広域的に EMET を設定することが可能です。このセクションでは、企業のネットワーク上で EMET を適用、そして管理するために、System Center Configuration Manager、および グループ ポリシーをどのように使用すれば良いか、ご説明します。

Microsoft System Center Configuration Manager

EMET は、適用および設定目的で、簡単に Microsoft System Configuration Manager に組み込むことができます。

クライアントに EMET を適用するために、アプリケーションを作成する

EMET を適用する第一段階は、EMET インストーラー をダウンロードすることです。MSI パッケージを準備したら、以下のステップに従わなければなりません。この例では、私たちは Configuration Manager 2012 にアプリケーションを構築する例に言及しますが、同様のことが Configuration Manager 2007 を利用して、パッケージ、プログラムおよび提供情報でも達成可能です。

1. [ソフトウェア ライブラリ] – [アプリケーション管理] – [アプリケーション] から、[アプリケーションの作成] を選択します。
2. 既定の種類である Windows インストーラー (ネイティブ) を維持し、以前にダウンロードした (*) EMET セットアップ MST ファイルを検索するために、ソース UNC パスをブラウズします。
3. アプリケーションの詳細は、(インポート情報ページにある) MSI 製品コードと一緒に、自動的に MSI から抽出されます。
4. 概要のページでは、このアプリケーションについて、あらゆる詳細情報を追加することができ、インストール プログラムに続いて、MSI に基づく EMET インストールの詳細を持つ、あらかじめ用意されたコマンドが表示されます。**msiexec /i "EMET Setup.msi" /qn /norestart** を読み込むために、インストール ラインを編集します。
5. インストールの動作を、**Install for system (システム用にインストール)** に変更します。
6. ウィザードを完了します。
7. 作成したばかりのアプリケーションから、展開を選択します。
8. ターゲットにするために、コレクションを閲覧します。
9. コンテンツ ページで、配布ポイントを選択します。
10. 展開設定のページで、対象とするインストール設定を選択します (大抵、これは必須ですが、そうでない場合、ただのテスト展開です)。
11. 展開のスケジュール、ユーザー側の表示と操作、および、アラートを設定し、その後、ウィザードを完了します。

12. すべての対象とするクライアントに対し、サイレントで EMET クライアントを展開するプロセスが開始されました。そのプロセスは、レポート|展開で監視することができます。

EMET 設定のために、パッケージ、およびプログラムを作成する

EMET が展開されたので、環境内でアプリケーションを保護するために設定しなくてはなりません。EMET の設定なく、ベース クライアントはスタンドアローンではアプリケーション防護の強化する試みを何も行いません。ここでは、EMET クライアントをインストールしたと報告する、クライアントのコレクションを作成し、設定パッケージでそれらを対象とします。

EMET 設定ターゲット コレクションを作成します

1. [資産とコンプライアンス] – [デバイス コレクション]、から [デバイス コレクションの作成] を選択します。
2. デバイス コレクション (インストールされた EMET とクライアント) に名前をつけ、限定コレクションを選択します。
3. メンバーシップの規則ページで、[規則の追加] をクリックし、[クエリ規則] を選択します。
4. クエリに名前を付け、クエリ ステートメントの編集を選択します。
5. [条件] タブないの、黄色の星をクリックします。
6. [条件] プロパティ内で、条件の種類を単純な値のままにし、選択をクリックします。
7. 属性クラスとして、インストールされたアプリケーションを選択します。
8. 属性として、表示名を選択します。
9. OK をクリックした後、[値] ボタンをクリックします。
10. 値のリストから EMET を選択します。少なくと も 1 つのシステムは、この値を、EMET クライアントのインストール後にハードウェアのインベントリのアップを報告する必要があります。リストにない場合は、単純な値と入力します。
11. クエリ規則を完了した後、このコレクションをどのくらいの頻度で評価するか、選択します。私たちは、このコレクションに対し EMET 設定を対象とするので、随時、評価を行います。また、このコレクションが追加されるのは、クライアント (EMET がインストールされた) のインベントリ情報がサーバーに送信された場合のみであることに注意してください。既定で、インベントリは 7 日毎に送信されます。

EMET 設定パッケージ、およびプログラムを作成する

1. EMET 設定パッケージのソースとして使用される、以下の 4 ファイルをソース ディレクトリに置きます。これらのファイルは、システムにインストール後、EMET クライアントのソース ディレクトリから収集できます。すべてのファイルが揃わないと、EMET 設定は稼働しません。
   a. Popular Software.XML (アプリケーション フォルダー ¥EMET¥Deployment¥Protection Profiles から)
   b. EMET_Conf.exe (アプリケーション フォルダー ¥EMET から)
   c. HelperLib.dll (アプリケーション フォルダー ¥EMET から)
   d. MitigationInterface.dll (アプリケーション フォルダー ¥EMET から)
   e. PKIPinningSubsystem.dll (アプリケーション フォルダー ¥EMET から)
   f. SdbHelper.dll (アプリケーション フォルダー ¥EMET から)
2. ソフトウェア ライブラリ | パッケージ から、パッケージの作成を選択します。
3. パッケージに名前を付け、ソース ファイルを含む、このパッケージを選択してください。ステップ 1 で言及された、4 つのファイルについてパスを提供します。
4. スタンダード プログラムを選択します。
5. プログラムに名前を付け、EMET_Conf.exe –import ”Popular Software.xml” となるようコマンド ラインを設定します。これは、EMET チームが提供する「Popular Software (人気のあるソフトウェア)」 保護ファイルを使用する一例です。このプロファイルを修正、もしくは EMET の提供するその他の保護ファイルを利用することも可能です。インポートされるファイルは、レファレンス付きで EMET 設定パッケージに含まれなければなりません。
6. ユーザーがログオンしているか否かに関わらず、サイレントでプログラムが稼働するよう設定します。
7. ウィザードを完了します。
8. パッケージ、およびプログラムが完了したら、展開を選択します。
9. 作成されたばかりのコレクションを対象とするコレクションとして選択し、希望する設定でウィザードを完了します。

グループ ポリシー

グループ ポリシーを通じて、EMET インストーラーを展開するには、マイクロソフト サポート技術情報 816102 で説明されている手順に従ってください。

グループ ポリシー 管理者は、EMET GUI および標準のグループ ポリシー 編集ツールを使用してグループ ポリシーで EMET の設定を構成できます。EMET GUI の方が使いやすいですが、どちらも使用できます。グループ ポリシーで構成した設定は、ローカル レジストリで構成された設定を上書きします。

EMET GUI を使用してグループ ポリシーを設定するには、Group Policy ボタンをクリックして設定するポリシー ストアを選択するか、新規作成の New をクリックしてください。EMET GUI のメイン画面とよく似たグループ ポリシーの EMET 設定ダイアログ ボックスが開きます。主な違いは、構成する設定がローカル レジストリではなくグループ ポリシー オブジェクトに書き込まれることです。Import および Export ボタンは、XML ファイルを使用してグループ ポリシーと通常のレジストリ構成間で設定一式を “転送” することができます。また、以下を使用して構成できる機能がいくつかあります。

EMET GUI のグループ ポリシー設定 GUI に表示されていない Windows のグループ ポリシー エディターを使用しているグループ ポリシー

いったん、EMET が展開されると、ユーザーは設定用に提供されたテンプレート ファイルを使用できます。”Deployment¥Group Policy Files” フォルダーに EMET.admx および EMET.adml ファイルが置かれます。これらのファイルは、インストール後に必ず、それぞれ¥Windows¥PolicyDefinitions および ¥Windows¥PolicyDefinitions¥en-US フォルダーにコピーします。一旦この作業が完了すると、EMET の設定はグループ ポリシー経由で構成可能です。

これら複数のポリシーのセットは、 EMET が公開しているものです。以下が、それぞれの概要です。 各ポリシーに関してはポリシー エディターで詳細情報を入手できます。

システム緩和策: System ASLR、System DEP、および System SEHOP と命名されたこれらポリシーはシステム緩和策を設定するために使用されます。システム緩和策の修正を有効にするために再起動が必要な場合があることに注意してください。

既定保護: これらは、アプリケーションのグループ向けに予め定義された保護設定のセットです。これら 3 つのプロファイルは互いに組み合わさっているわけではないため、予め定義されたアプリケーション保護の一覧を有効にするためには、3 つのプロファイルをすべて有効にしなくてはなりません。Internet Explorer および 推奨されるソフトウェアを有効にするのは、EMET がインストールされるとき、設定ウィザードが適用される設定に対応しています。

- **Internet Explorer:** Internet Explorer 用の既定で推奨された保護を有効にする。
- **推奨されるソフトウェア:** WordPad、Microsoft Office スイート、Adobe Acrobat、Adobe Reader、および Oracle Java の一部であるアプリケーション用の既定で推奨された保護を有効にする。

- **人気のソフトウェア:** その他の人気ソフトウェア用の既定で推奨された保護を有効にする。

既定の保護オプションは、EMET GUI グループ ポリシーの設定ダイアログには表示されませんのでご注意ください。既定の保護オプションで予め構成された設定は、一般的な Software.xml および推奨された Software.xml 保護プロファイルにある設定と同じです。EMET GUI のグループ ポリシー設定のアプリケーション保護プロファイルをインポートすると、これらは次に記載されているアプリケーションの構成に追加されます。アプリケーションの構成および既定のプロファイルの 1 つで同じアプリケーションが構成されている場合、アプリケーションの構成設定が優先されます。

アプリケーション設定: ここから、既定の保護プロファイルに含まれない、追加のアプリケーションの設定ができ、2 列のテキストエディターに移動できます。左の列はアプリケーション用の照合パスルール、右の列は既定以外の構成オプションを指定します。右の列を空白にすると、すべての既定の緩和策が適用されます。Windows のグループ ポリシー エディターに表示されるヘルプ テキストに記載されている構文を使用して、ASR や EAF+ 用に個々の緩和策および供給パラメーターを有効または無効にすることができます。

EMET GUI グループ ポリシー設定ダイアログの保護プロファイルをインポートすると、EMET はプロファイルの設定をアプリケーションの構成に追加します。EMET GUI または Windows のグループ ポリシー エディターでこれらの設定の詳細を変更できますが、EMET GUI の方が変更しやすいです。アプリケーションの構成設定は、レポーティングとコンプライアンス チェックができるグループ ポリシー定義スキーマ (ADMX) と互換性があります。

既定 アクション、および緩和策の設定: これらの設定は、ROP 緩和策の詳細設定の項目で説明されている ROP 緩和策の詳細設定、および悪用が検出された場合の既定のアクション (監査のみ、もしくは停止) と関連しています。

証明書ピンの構成: この設定は、2 つに分かれた 2 列のテキスト エディターを使用して EMET 証明書ピンの構成を構成します。最初のテキスト エディターは、固定するサイトおよび各サイトに関連づけるルールの名前を指定します。2 番目のテキスト エディターは、各ルールの詳細とルール名を関連付けます。各構文は、Windows のグループ ポリシー エディターに表示されるヘルプ テキストに記載されています。EMET GUI の方が使用しやすいため、証明書の構成には Windows のグループ ポリシー エディターよりも EMET GUI のご利用を強く推奨します。証明書ピンの構成設定は、レポーティングとコンプライアンス チェックができるグループ ポリシー定義スキーマ (ADMX) と互換性があります。

EMET エージェント可視性: この設定で、タスクバーのトレイ領域にある EMET エージェントアイコンを自動的に隠すことができます。

EMET エージェント カスタム メッセージ: このエントリでは、EMET が攻撃を検出した際に表示される警告にディスプレイされる特別仕様のメッセージを定義することができます。メッセージを表示するには、トレイ アイコンレポート設定をオンにしておかなければなりません。

レポート: このエントリで、Windows イベント ログ、トレイ アイコン、および早期警告プログラム用のレポート設定を切り替えることができます。

一旦、EMET グループ ポリシーが有効になると、*HKLM¥SOFTWARE¥Policies¥Microsoft¥EMET* のレジストリに書き込まれます。このレジストリ キーは EMET Service が監視しており、ローカルで自動的に設定を適用します。

グループ ポリシーで制御された EMET 設定を閲覧するためには、EMET コマンド ライン ツールを使用して下記コマンドを実行します。

EMET_Conf --list

グループ ポリシーを介して構成された設定は、EMET GUI もしくは、EMET コマンド ライン ツールを使用してローカルで構成された設定より優先されることに注意しなくてはなりません。また、グループ ポリシーで制御された設定は、グループ ポリシーを介してしか、修正および削除ができません。例えば、以下を実行すると、

EMET_Conf --delete_all

EMET GUI、あるいは EMET_Conf を介して定義された緩和策、および SSL 証明書ピン設定のみが削除されます。GPO 経由で定義された緩和策設定、および SSL 証明書ピン設定は残ります。

その他オプション

System Center Configuration Manager、もしくは グループ ポリシーのいずれにも頼らずに、別の管理ソリューションを使用する場合は、EMET 保護プロファイルの項目で紹介されている保護プロファイル機能を活用することを推奨します。

詳細オプション

安全でない設定を有効にする

既定で、EMET は安全でないと思われる設定オプションを隠します。これらのオプションは、一般使用のシナリオでシステムに不安定な状態を起こすことが分かっています。しかしながら、レジストリ キーを追加設定することで、これらのオプションを設定することが可能です。追加設定が適用されると、EMET が安全でないオプションを表示しますが、その内のいずれかが選択された場合にユーザーに警告します。

追加設定は、*HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥EMET* のレジストリで確認できます。このキーが存在しない場合は、EMET GUI を稼働し、レジストリの表示を更新してください。キー内に、*EnableUnsafeSettings* と呼ばれる、DWORD 値があります。既定で、値が 0 になっています。そちらを、1 に設定し EMET GUI を再起動すると、安全でないオプションが選択できます。

EMET では、現在、安全でないオプションが 1 つあります。これは、System ASLR 設定用の「Always On」を指します。オペレーティング システムの構成によって、System ASLR 設定を「Always On」に設定することで、オペレーティング システムがブート時にクラッシュする可能性があります。これを回復するためには、システムをセーフ モードで起動し、System ASLR を [Opt In] (推奨) もしくは [Disable] に設定する必要があります。

ユーザー レポートに使用するカスタム メッセージの設定

攻撃が検出された際に出る、レポート ポップアップ用のカスタム メッセージを設定することが可能です。EMET 4.0 では、この設定は グループ ポリシーを介して、もしくはレジストリ キーを作成することで設定することができます。

ハイブ内の *HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥EMET* で *TrayIconMsg* という名前の新しい文字列値を作成します。ここで指定された文字列は、既定の通知に代わって EMET が攻撃を検出、そして阻止した場合にユーザーに表示されます。

証明書信頼機能をサード パーティ ブラウザー用に設定

上級ユーザーは、証明書信頼機能が提供する緩和策を有効利用するために、サード パーティ ブラウザーの設定をすることができます。ブラウザーは、Windows CryptoAPI を使用しなければならず、CAPI 拡張を支援しなければなりません。さらに、サード パーティ ブラウザーは保護されているアプリケーショ

ン (緩和策がなくても) に追加されなければなりません。最終的に、サード パーティ ブラウザーの実行可能な名前を、“;” で分けて、レジストリ ハイブ *HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥EMET* のレジストリ数値 “EMET_CE” に追加しなくてはなりません。

例えば、 “iexplore.exe;third_party_browser.exe” です。

注: このシナリオは、サポートされておらず、実験的なものです。厳密に言うと、SSL チェーン信頼検証のために、Microsoft CryptoAPI を使用しているあらゆるプログラムを、 EMET 証明書信頼機能と連携するように、レジストリ値に入れることができます。

ローカル テレメトリの設定

トラブルシューティング目的で、マイクロソフトは、「ローカル テレメトリ」モードを追加しました。このモードが有効になっている場合は、「早期警告」を通じて送信される情報は、ユーザー定義フォルダーに保存される代わりにローカルで保存されます。このモードを有効にするには、*HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥EMET* レジストリ ハイブに 2 つのエントリを作成する必要があります:

- LocalTelemetryPath (文字列): 情報を保存するパス (例: c:¥emet_local_telemetry)

任意で、どのような MiniDump ファイルを作成するかをコントロールするためのレジストリ キーが作成可能です:

- MiniDumpFlags (DWORD): 0x1ff (既定値)

フラグの候補に関する詳細情報については MSDN の記事に掲載されています。

EMET エージェント アイコンの表示設定

ユーザーは、レジストリ ハイブ *HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥EMET* に DWORD レジストリ キー AgentStartHidden を追加することで、トレイ領域の EMET エージェント アイコンの表示を設定できます。候補の値は、非表示が「1」で、表示が「0」です。

緩和策考慮事項

EMET を通じて利用できる多用な緩和策を設定するときに、いくつか考慮しなくてはならない事柄があります。次のセクションでは、システム設定、およびアプリケーションの特定の設定によって、破損される警告についてお話します。

システム設定

DEP

- DEP 用にシステム設定を構成することで、Windows の起動オプションが変更されます。BitLocker を使用しているシステムでは、この変更で、BitLocker がシステム起動情報が変更されたと検出し、次の再起動で回復キーを入力することになります。 BitLocker が有効になっているシステムで、DEP 用のシステム構成設定を変更する前に、回復キーを控えておくことを強くお奨めします。
- 仮想マシンを含め、すべてのシステムが DEP をサポートしているわけではありません。しかしながら、サポートされていないマシン上で EMET を稼働している場合においても、このオプションは有効です。このオプションをそれらのシステムに設定することで、影響はありません。DEP を設定する際には、システムの制約に注意してください。

SEHOP

- Windows 7 以降のバージョンでは、SEHOP (システム全体およびアプリケーション単位の両方) がオペレーティング システム (OS) に導入されています。このため、この緩和策が有効になっていて検出された場合、EMET は、SEHOP が検出されたという情報を入手し、それを通知することはできません。代わりに、OS はプロセスを終了し、アプリケーションのイベント ログにイベントを書き込みます。

ASLR

- ASLR 設定には、”Always On (常時有効)” と呼ばれる安全ではないオプションがあります。この設定は、特にそれをサポートしていないバイナリに対して、強制的に ASLR を行います。この設定は、システムの不安定性を紹介するリスクを考慮して、既定で非表示になっています。

テストで、ASLR を ”Always On (常時有効)” にする一般的に使用されるシナリオは、起動の最中にシステムがブルー スクリーンになる可能性がある、という問題に遭遇しました。これは、あるサード パーティのビデオ ドライバ用のアドレス スペースがランダム化されたために発生しました。これらのドライバは、このランダム化をサポートするよう構築されてはいなく、その後ドライバだけでなく、システム全体も破損しました。この問題から回復するには、保護されたモードで起動する、そして System ASLR 設定を [Opt in] あるいは [Disabled] に切り替えることが必須です。

安全でない ASLR 設定を有効にする方法の詳細情報は、詳細オプションの項目を参照してください。

アプリケーション別の設定

DEP

- 仮想マシンを含め、すべてのシステムが DEP をサポートしているわけではありません。しかしながら、サポートされていないマシン上で EMET を稼働している場合においても、このオプションは有効です。このオプションをそれらのシステムに設定することで、影響はありません。DEP を設定する際には、システムの制約に注意してください。

SEHOP

- Windows Vista 上、およびそれ以前の多用なアプリケーションは、EMET の SEHOP と互換性がなく、このような場合、EMET から SEHOP を無効にして、システム緩和策の SEHOP を使用することが望ましいです。システム緩和策 SEHOP をアプリケーション オプトアウトに設定してください。

EAF

- degug 起動オプションで、システムを設定した場合は、EAF が有効になっているアプリケーションを稼働する際にデバッガーをアタッチする必要があります。/degub 起動オプションが有効になっているのにデバッガーがアタッチされていない場合、EAF 有効のアプリケーションがスタートした際に、反応しなくなります。これは、EAF 緩和策がデバッグ レジストリに依存しているために起こります。もし、Windows がカーネル デバッガーを使用するよう設定されたのであれば、Windows は、幾つかある内のメモリ アドレスの 1 つにアクセスがあった場合はいつでも、デバッガーに通知しようと試みます。Windows はその後、デバッガーからのレスポンスを待ちます。デバッガーからレスポンスがなかった場合、システムは反応しません。
- デバッグ レジスタ (結果、EAF も) をサポートしない仮想マシンがあります。しかしながら、EAF オプションは、EMET がデバッグ レジスタをサポートしないマシン上で稼働しない場合でさえも、利用可能です。それらのマシンに、このオプションを設定することで影響はありません。EAF を設定する際には、この制約に注意してください。
- EAF 緩和策は、パッカーあるいはコンプレッサーを使用する保護されたプログラムおよびライブラリ、DRM もしくはデバッグ対策コード、デバッガー付きのソフトウェア、そしてウイルス対策、サンドボックス、ファイアウォールなどのセキュリティ ソフトウェアに適用してはいけません。

強制 ASLR

- Windows 8、およびそれ以降のバージョン上、いくつかのプログラム (例: Internet Explorer 11 または Office 2013) では、オペレーティング システムが元々提供している強制 ASLR で実行されるよう構成されています。このため、本来の Windows 由来の ASLR がアプリケーションで有効になっていると、この緩和策に通知、およびレポートを提供できません。その代わりに、OS がプロセスを終了し、アプリケーションのイベント ログにイベントを書き込みます。
- EMET の緩和策は、コア プロセスのアドレス スペース、そして静的リンクが設定された後で有効になります。Mandatory ASLR は、これらのいずれに対してもアドレス スペース ランダム化を強制しません。Mandatory ASLR の主な焦点は、プラグインなどの動的リンクのモジュールを保護することです。

よく寄せられる質問

ライフサイクル ポリシー

古いバージョンもサポートされますか？

EMET 5.5 の時点で、EMET 4 あるいはそれ以前のバージョンをサポートしません。EMET 5.5 は 2017 年 1 月までサポートされます。EMET 4 に関する質問

EMET 4 および EMET 5.2 の設定は、EMET 5.5 と互換性がありますか？

いいえ。EMET 5.5 では、管理を容易にするためにレジストリはリファクターされました。以前のバージョンの EMET (EMET 5.5 Beta を含む) から設定を変換するには、エクスポート機能を使用して以前のバージョンの設定を保存してください。そして、PowerShell スクリプト コンバーターを使用して保存した設定をインポートし直してください。EMET 4 をインストールしています。新しいバージョンをインストールする前に、アンインストールする必要がありますか？

EMET 5.5 をインストールする前に、EMET 4 をアンインストールする必要はありません。EMET 5.5 インストーラーは自動的に EMET 4 をアンインストールし、EMET 5.5 をインストールします。アップグレードの際、現在の設定を保持するために、エクスポート機能を使用して以前のバージョンの EMET 設定を保存してください。そして、PowerShell スクリプト コンバーターを使用して保存した設定をインポートし直してください。

一般的な緩和策に関する質問

Process Explorer では、EMET がアプリケーションとともに使用するために設定されているにも関わらず、プロセス用の ASLR 列が空欄になっています。

EMET は、ASLR の OS 導入については考慮していません。Process Explorer は、ASLR の OS 導入のみをクエリするため、Process Explorer は ASLR が有効になっている状態でも、Process Explorer には表示されません。

どのアプリケーションに対し、EMET 緩和策を適用すれば良いでしょうか?

信頼できないソースから入ってくるファイル、あるいはファイルを扱い、一般に悪用の標的になるアプリケーションに対し EMET 緩和策を適用するよう提案しています。該当例にはウェブ ブラウザー、ドキュメント リーダー、などが挙げられます。デバッガーなどの特定のアプリケーション、もしくは DRM ファイルを扱うアプリケーションは EMET に大いに適合性があります。もしも、これらの種類のアプリケーションに EMET 緩和策を適用したい場合は、いくつかの緩和策が制御されると予測してください。EMET 緩和策に関するガイドラインはサポート技術情報 2909257 に掲載されています。

緩和策の問題を修復する

私は、DEP 用のシステム設定を修復し、再起動しました。現在、BitLocker が回復キーを要求してきます。なぜ、聞かれるのでしょうか、またどうやったら要求を止めることができますか？

DEP 用のシステム設定を修正すると、オペレーティング システムの起動オプションが変更されます。BitLocker は攻撃者がこれらのオプションを改ざんすることを阻止できないので、その代わりに変更を監視します。変更されると、BitLocker はその変更が正当であるか保証するために、回復キーを要求します。

BitLocker が何度も回復キーを要求するのを防ぐためには、BitLocker を一時停止し、変更を適用してマシンを再起動します。再起動後、再開できます。この結果、BitLocker は新しい起動オプションを記録します。

Export Address Filtering (EAF) 緩和策が有効になると、システムが中断します。

これが発生するのは、システムがデバッグ モード (/debug 起動オプションが指定されています) で稼働している場合です。アプリケーションの実行を続ける前に、システムはデバッガーからのレスポンスを待つので、EAF 緩和策の特性 (デバッグ レジスタ、およびシングル ステップ イベントが関わる) によって中断が発生します。
この発生を防ぐには、以下の内いずれか 1 つを実行してください。

- /debug 起動オプションを削除し、システムを再起動します。
- デバッガーをアタッチし、システムを反応させます。

EMET を設定したアプリケーションが、起動時に常に異常終了します。

大抵、この現象が起こるのは、アプリケーションが EMET の緩和策の 1 つと互換性がないためです。どの緩和策がこの現象を引き起こしているのか突き止める方法の 1 つは、アプリケーションが異常終了せずに起動を行うようになるまで、すべての有効になっている緩和策を 1 つずつ無効にして確認していくことです。一旦、問題となっている緩和策が判断できたら、その緩和策を無効にし、残りの緩和策を有効にします。

上記の質問内の “常に” の強調に注意してください。ユーザー インプットが、アプリケーションの互換性の問題である可能性が高いにも関わらず、もし、アプリケーションが、あなたが信頼済みと判断しているベンダー経由のものである場合、異常終了は 常に起こります。

時折、起こる異常終了、または、特定のドキュメントをリーダーで開くなど、外部入力で起こる異常終了、あるいは、信頼できないソース経由のアプリケーションはそれぞれ、違った対処をしなければなりません。これらのアプリケーションについて、EMET 緩和策は、セキュリティ事故を避けるため、異常終了の根本的原因が分かるまで、意図的に無効にしてはいけません。

EAF 緩和策を有効にした後で、アプリケーションを起動すると、いつもアプリケーションが異常終了します。

一つ前の質問と同様ですが、EAF 緩和策と連動しない可能性のあるアプリケーションがあります。これは、アプリケーションが知的財産を保護しようと実行する防御によって、頻繁に起こります。私たちはそのアプローチをビデオ プレーヤー、コンバーター、 VOIP プログラムなどで時折目にします。アプリケーションが起動されている最中に、そのアプリケーション内で、EMET の EAF 緩和策が原因で常に異常終了を目にする場合、EAF 緩和策を無効にすることが可能で、なおかつ、そのアプリケーションに対して残りの緩和策は保持することができます。

一般的な質問

グラフィカル ユーザー インターフェースを起動しようと試みると、「app failed to initialize properly (アプリケーションを適切に初期化できませんでした)」というエラーが出ます。これをどうやったら改善できますか？

GUI は、.NET 4.0 がシステムにインストールされていることが必須です。もし、他のマシンからバイナリをコピーした後で、このエラーが出ているのならローカルマシンでインストーラーを稼働してみてください。再配布可能な .NET 4.0 をダウンロードできるロケーションに誘導してくれます。

64 ビット版アプリケーションで EMET は動作しますか？32 ビットプログラム ファイル ディレクトリにインストールされています。

はい、EMET は 64 ビットアプリケーションをサポートしています。インストーラーは、64 ビットシステム、および 32 ビットシステムの両方で動くようデザインされています。このことがもたらす好ましくない影響は、バイナリが 32 ビット ディレクトリにあることです。

しかしながら、64 ビットアプリケーションで利用できない、あるいは適用できない緩和策があることに注意してください。詳細情報は、サポートされているオペレーティング システム、およびソフトウェア要件の項目を参照してください。

古いバージョンの EMET をインストールしています。EMET 5.5 のアップグレードはどうやるのですか？

EMET 3 よりも古いバージョンをお持ちの方には、はじめに、Windows コントロール パネルで古いバージョンの EMET をアンインストールし、その後、手動で HKLM¥Software¥Microsoft¥EMET および HKLM¥Software¥Policies¥Microsoft¥EMET キーを削除することを推奨しています。

EMET 3、あるいは EMET 4 をお持ちで、EMET 5.5 にアップグレードしたい場合は、インストール パッケージを実行し、古い設定を維持する、あるいは推奨される設定を適用する、のいずれについても、指示に従います。

自分のアプリケーションが EMET と互換性があるかどうか、どうやったら分かりますか？

テストは、既定保護プロファイルに含まれるアプリケーションのみに対して、既定の設定で行いました。その他のアプリケーション、あるいは標準ではない設定についてはプロダクション システム上のそれらのアプリケーション に EMET 保護を適用する前に、専用の環境で徹底的にテストすることを推奨します。

アプリケーションを保護した場合、プラグインも同様に保護されますか？

はい。EMET 保護プロセスにロードされる ActiveX コントロール、あるいはその他のサード パーティ アドインなどのプラグインにも緩和策は適用されます。

サポート

プレミア、あるいはプロフェッショナル サポート契約をしているお客様は、サポートを受けるためにこれらのチャンネルを活用することができます。

ユーザーは、フィードバックおよび提案を emet_feedback@microsoft.com (英語) にメールを送ることができます。サポートに関するリクエストについてはこの電子メールは使用せず、TechNet フォーラム、もしくはオフィシャル サポート チャンネルを利用してください。

付録 A：EMET 互換性

EMET の互換性について考えるのは、適用プロセスにおいて重要な部分です。この文脈における互換性は、「機能性を失わずに、すべての EMET 緩和策を有効にした状態で、アプリケーションを稼働することができる」、ことを意味します。

EMET は有害なことを一切行いませんし、極めて大きな非互換性を引き起こすであろう、あらゆる事柄を避けます。つまり、大抵のアプリケーションは互換性があるということを意味します。ですが、アプリケーションに EMET 保護を適用する前に、アプリケーション上で互換性のテストを行うことを強く推奨します。

EMET では、アプリケーションの互換性テストは、すべてのサポートされているプラットフォームの EMET 保護プロファイルの一部である、すべての Microsoft、およびサード パーティアプリケーションに対して行いました。

特定のアプリケーションに対して EMET 緩和策の一部が持っている既知の互換性の問題についてはサポート技術情報 2905257 の「アプリケーションの互換性一覧」の項目に記載されています。この一覧は、定期的に更新されていますが、この更新は EMET の最新の利用可能なバージョンに基づいています。

非互換性が発見された場合、次のステップは、どの緩和策がそれを引き起こしているのか判断することです。この問題を再現するために、すべての EMET 緩和策を有効にして、アプリケーションを稼働することで判断可能です。その後、この問題が再現されなくなるまで 1 つずつ緩和策を無効にしていきます。一旦、このテストプロセスを通じて、問題を引き起こす緩和策が特定されたら、可能な限り EMET 保護を活用するために、適用時間内に問題を引き起こさない緩和策を引き続き有効にします。

遭遇したあらゆる非互換性については、サポートの情報の項目経由で遠慮なくお問い合わせください。

付録 B：EMET 5.5 リリース注釈

EMET 5.5 の主な変更点

- 全機能を備えた GPO 管理、レポーティングおよびコンプライアンス要件に対応
- コマンドライン: 新規構文とオプション
- ルート証明機関の拇印に基づく証明書ピンの実装と例外ロジックの削除
- エクスポートおよびインポートのパス記憶
- EMET のレジストリのリファクタリング。以前のバージョンの EMET (EMET 5.5 Beta を含む) から設定を変換するには、ファイルにレジストリの値を保存する必要がります。そして、EMET5.5 をインポート後、PowerShell スクリプト コンバーターを使用して保存した設定をインポートし直してください。手順は以下の通りです：

  a. 設定をエクスポートします。管理者特権の PowerShell で以下のコマンドを実行します：

     .¥Migrate-EmetSettings.ps1 -RegFile .¥NewEmetSettings.reg -MissingCertCsv .¥MissingCerts.csv

     EMET 5.5 RTM は PowerShell スクリプト Migrate-EmetSettings.ps1 を備えています。これには、使用法についての説明書が含まれています。

  b. 以前のバージョンの EMET をアンインストールします。

  c. EMET 5.5 RTM をインストールします。”Use recommended settings (推奨の設定を使用する)“ または “あとで手動で設定する” のどちらかの選択を要求された場合、“Configure manually later (あとで手動で設定する)” を選択します。

  d. 設定をインポートします。管理者特権の PowerShell で以下のコマンドを実行します:

     reg.exe import .¥NewEmetSettings.reg

このソフトウェアおよびマニュアルは、本製品の使用許諾契約書のもとでのみ使用することができます。このソフトウェアおよびマニュアルのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。

マイクロソフトは、このマニュアルに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。このマニュアルはこれらの特許、商標、著作権、またはその他の無体財産権に関する権利をお客様に許諾するものではありません。

© 2016 Microsoft Corporation. All rights reserved.

ホワイトペーパーでアルファベット順に使用されている Microsoft の商標一覧は、米国 Microsoft Corporation およびその他の国における登録商標または商標です。