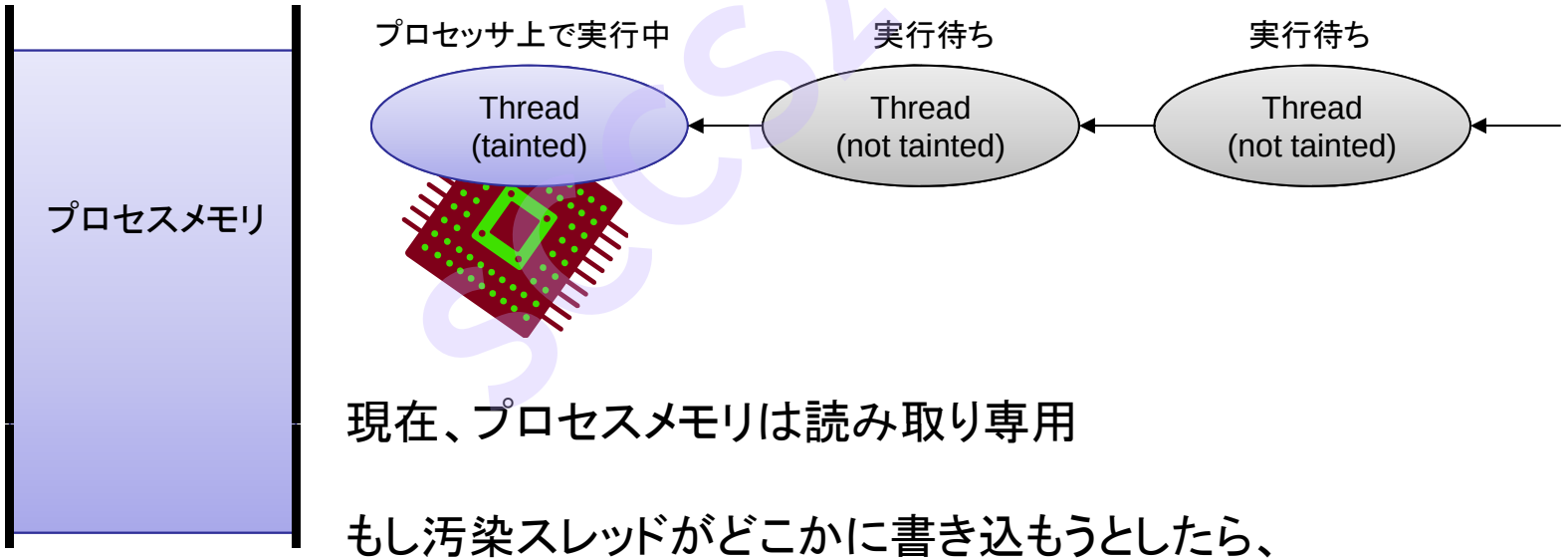
Ring-0における汚染追跡の実装

- 汚染スレッドがアクティブになったとき、
  eggはすべてのプロセスメモリを読み取り専用に変更する

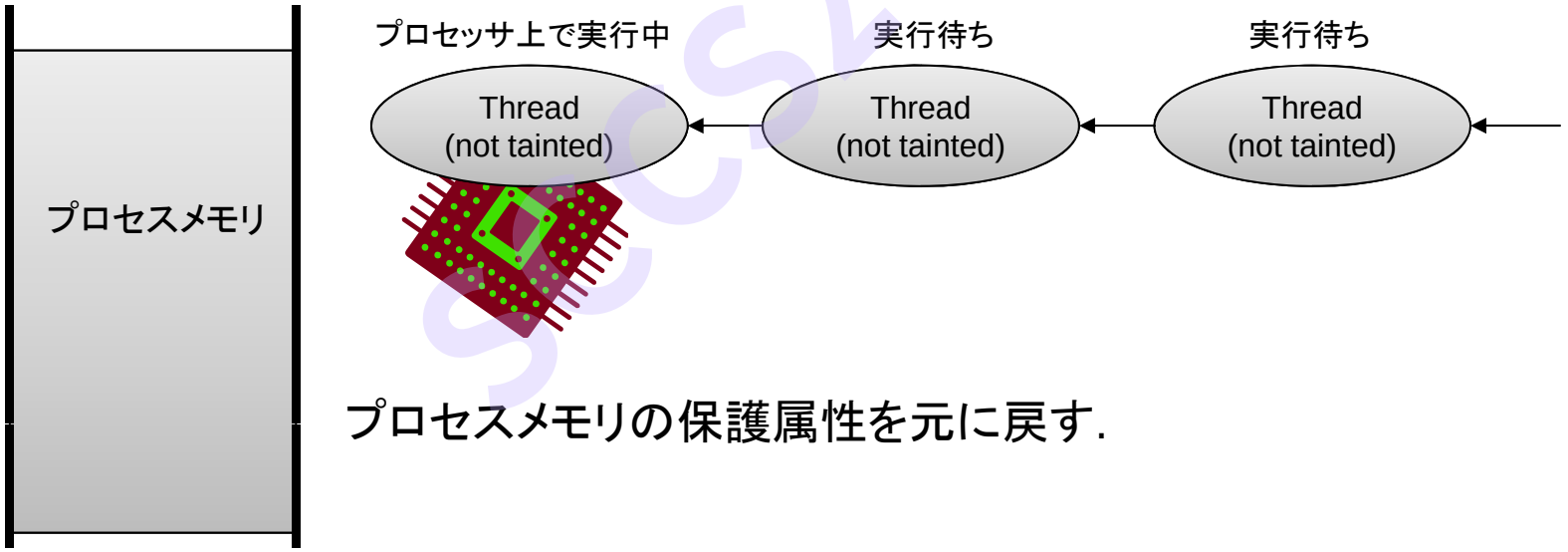


現在、プロセスメモリは読み取り専用

もし汚染スレッドがどこかに書き込もうとしたら、
プロセッサは例外を発生させる。
egg はこの例外を汚染イベントとしてキャッチする。

Ring-0における汚染追跡の実装

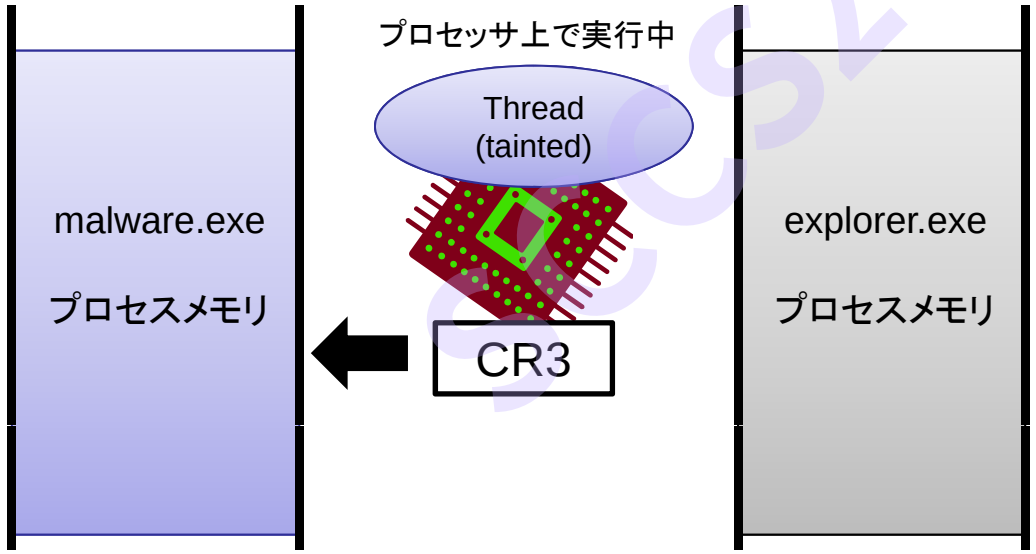
- 汚染スレッドがアクティブではなくなったとき、
  eggはすべてのプロセスメモリの保護属性を元に戻す



プロセスメモリの保護属性を元に戻す.

プロセス間メモリ操作の追跡

- プロセス間メモリ操作を追跡するために、eggはプロセスメモリ空間の切り替え関数(KiSwapProcess)をフックする
- これによりeggはプロセス間のメモリ操作を知ることができる

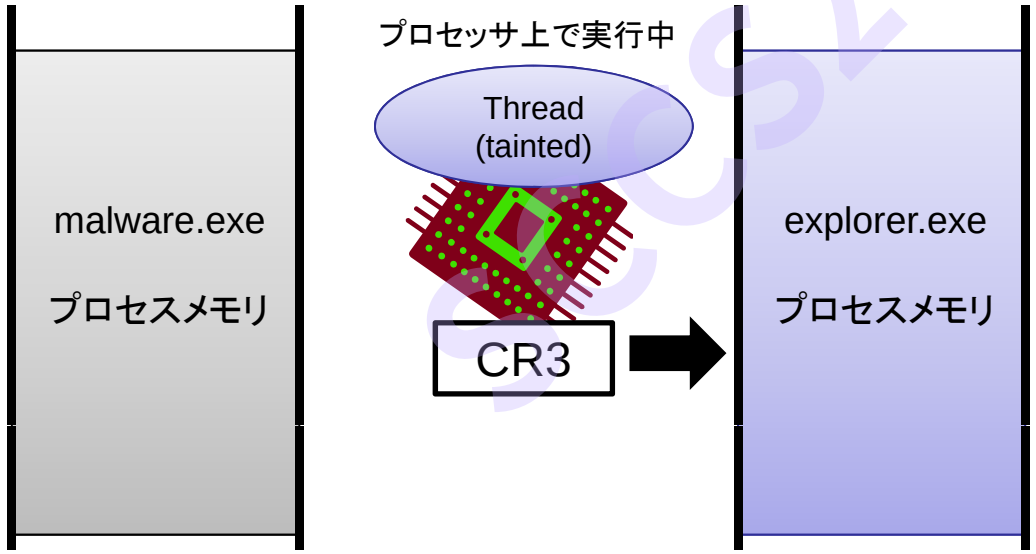


読み取り専用

保護属性はまだ変更されていない

プロセス間メモリ操作の追跡

- 汚染スレッドが別のプロセスメモリで実行されたとき、eggはそのプロセスメモリを読み取り専用に変更する



eggは他のプロセスメモリに対する操作（例：WriteProcessMemory）でも追跡することができる。

デモ：汚染追跡

- サンプルマルウェアはスレッドインジェクションを行う

- サンプルマルウェアは“injector.exe”
- VirtualAllocEx、WriteProcessMemory、CreateRemoteThreadを用いてnotepad.exeにスレッドをインジェクトする
- インジェクトされたスレッドはAllocConsoleとWriteConsoleをループの中で呼び出す
- eggはこのインジェクトされたスレッドも解析する

同レベル特権の問題

- egg はカーネルモードの解析について制限を持つ
  - カーネルモードマルウェアからeggは可視であり、破壊可能
- この制限は仮想マシン検知技術の影響を回避するための
  トレードオフ

まとめ

動的解析システムの種類	Egg	従来システム	先進的システム
有用な情報の取得	良い	不十分	良い
カーネルモードコードの解析	可	不十分	良い
拡散するマルウェアの解析	良い	不十分	良い
仮想マシン検知技術への耐性 （影響のなさ）	良い （影響を受けない）	良い （影響を受けない）	不十分 （影響を受ける）

- eggを使用することで解析の所要時間を抑えることができる
- 将来のバージョンでは、より高速かつ安定した動作を目指す.

ありがとうございました

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp