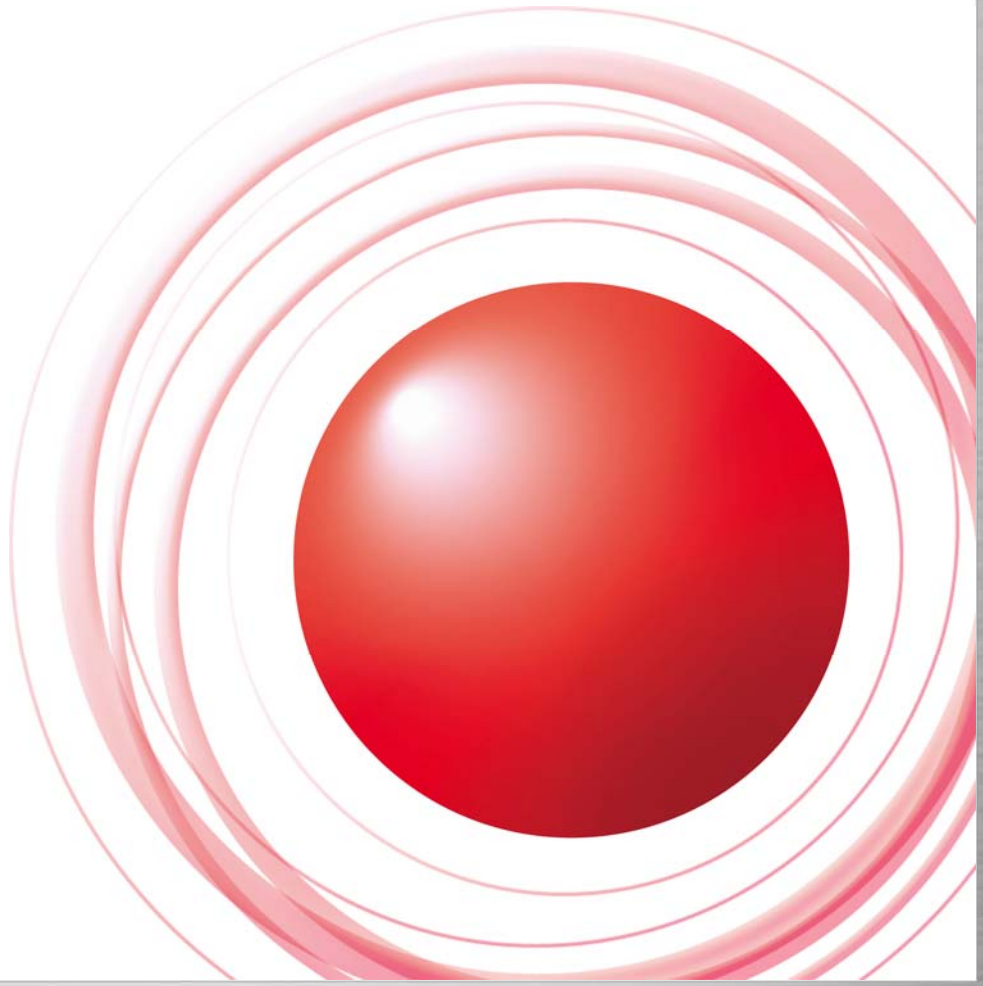
セキュリティ動向2010（2）
デジタルフォレンジックに関する取り組み

IIJ Internet Initiative Japan



2010/11/19

株式会社インターネットイニシアティブ
サービス本部　セキュリティ情報統括室
春山敬宏

Ongoing Innovation

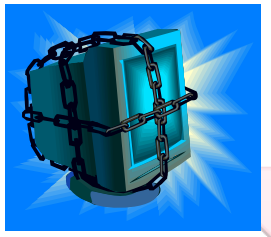
Overview

- デジタルフォレンジック概要
- インシデント対応例
- 起こりうる問題と技術的な取り組み

デジタルフォレンジック概要

デジタルフォレンジックとは

- インシデントレスポンス時や訴訟に必要なデータ提出時等に電子データを分析して情報を得るための調査手法



保全

報告

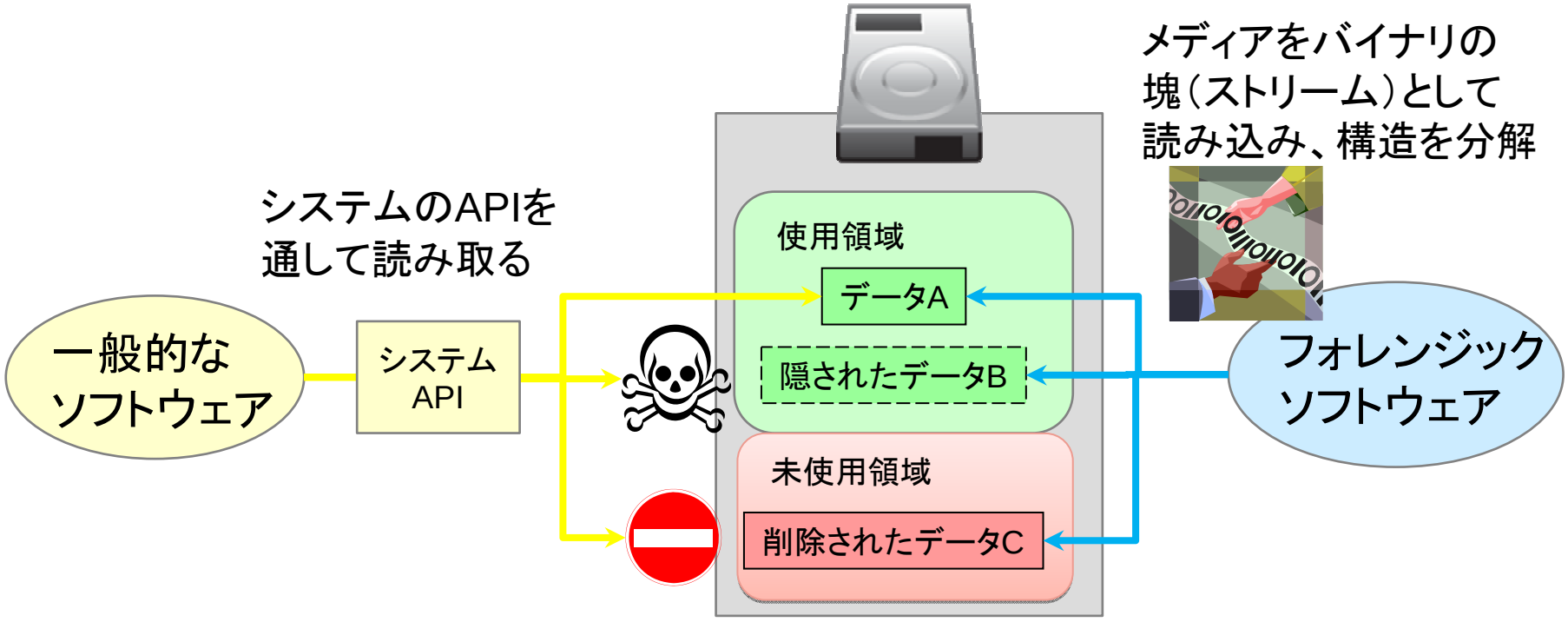
解析

保全の推奨事項

- 保全が実施されるまでは、端末の状態維持に努める
- 保全対象はメディア全体
  - 未使用領域も含む
- 揮発性のオーダーで保全
  - 実際には揮発性のデータは取れないことが多い‥
- 書き込み禁止で実施
  - 保全操作でデータを変えない
  - 専用のハードウェアやBoot CDを使う

フォレンジックツールによる解析

- システムのAPIに頼らず、独自にメディアの構造を0からパース(分解)する
  - マルウェア、ルートキット等による隠蔽を受けにくい
  - 削除されたデータやその断片を抽出可能

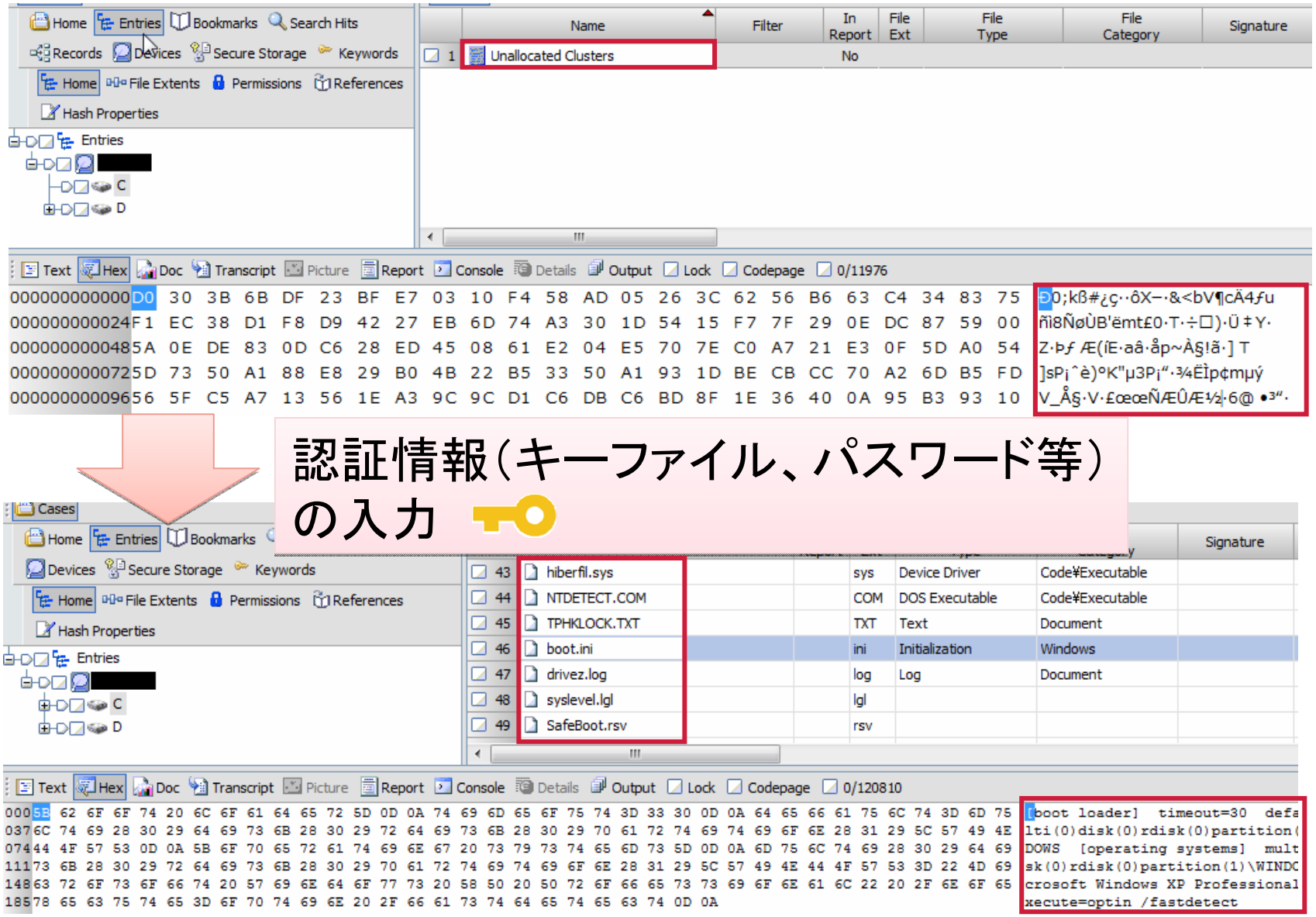


インシデント対応例

インシデント対応例

- シナリオ例：Web Proxyのログから、Drive by Downloadによってマルウェアに感染したノートPCが判明
  - 既にオフラインの状態
  - ディスクは暗号化されている
- ディスク内をプレビュー（簡易解析）
  - ディスクの暗号化を解除
  - 検体の取得
  - 特徴的なファイルやレジストリの変化を検出
- ディスクの保全を実施（イメージを作成）
- イメージを解析
  - 削除ファイルの復元
  - ファイル、レジストリ、ブラウザ履歴のタイムライン調査
  - プログラム実行痕跡、自動起動プログラム等のチェック
  - etc…

ディスク暗号化の解除



保全されたメディアのイメージ

名前	更新日時	種類	サイズ
[redacted]E01	2010/10/29 20:24	EnCase Evidence File	2,047,985 KB
[redacted]E02	2010/10/29 20:26	E02 ファイル	2,047,984 KB
[redacted]E03	2010/10/29 20:28	E03 ファイル	2,047,984 KB
[redacted]E04	2010/10/29 20:29	E04 ファイル	2,047,984 KB
[redacted]E05	2010/10/29 20:31	E05 ファイル	2,047,984 KB
[redacted]E06	2010/10/29 20:33	E06 ファイル	2,047,984 KB

2GBで分割保存されたディスクのイメージ

Device

Name	[redacted]
Actual Date	2010/10/29 20:22:57
Target Date	2010/10/30 05:22:58
File Path	[redacted]E01
Case Number	[redacted]
Evidence Number	[redacted]
Examiner Name	th
Notes	[redacted] SafeBoot
Label	/dev/sda
Model	[redacted]
Serial Number	[redacted]
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	9554815648e364a5f6a27dc80f3c6bc2
Verification MD5	9554815648e364a5f6a27dc80f3c6bc2
GUID	[redacted]

イメージの整合性チェックにより、証拠が変更されていないことが保証される
（保全の時に読み取ったデータのハッシュ値と読み取り後のイメージのハッシュ値を比較）

解析例：タイムライン調査

Web履歴

どこにアクセスしていて
ここに転送されたか？
（原因の特定）

Last Accessed	Url Name
2010/10/05 09:16:33	
2010/10/05 09:16:33	
2010/10/05 09:16:33	
2010/10/05 09:16:34	
2010/10/05 09:16:34	
2010/10/05 09:16:34	
2010/10/05 09:16:51	PrivacIE:64.27.25.224/1/*/
2010/10/05 09:16:55	
2010/10/05 09:22:58	
2010/10/05 09:22:58	
2010/10/05 09:22:58	
2010/10/05 09:22:58	
2010/10/05 09:22:58	

exploit site!

ファイルシステム・レジストリ

exploitの結果、ファイルシステムやレジストリに
どのような改変が行われたか？（影響範囲の特定）

95	132B7A3[redacted]\C\Program Files\Trend Micro\OfficeScan Client\Suspect\jar_cache8558493207611998067.tmp	File	6542	2010/10/05 09:17:11	2010/10/27 16:30:58	2010/10/05 09:17:12
96	132B7A3[redacted]\C\Program Files\Trend Micro\OfficeScan Client\Suspect\0.1690712346834503.swf	File, Archive	25335	2010/10/05 09:17:14	2010/10/27 16:30:41	2010/10/05 09:17:14
97	132B7A3[redacted]C\Program Files\Trend Micro\OfficeScan Client\Suspect\0.1690712346834503.swf	File, Archive	25335	2010/10/05 09:17:14	2010/10/27 16:30:41	2010/10/05 09:17:14
98	132B7A3[redacted]\C\Documents and Settings\[redacted]\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat	File, Hidden, Archive	262144	2008/05/23 11:40:32	2010/10/27 16:35:03	2010/10/27 16:35:03
99	132B7A3[redacted]\C\Program Files\Trend Micro\OfficeScan Client\Suspect\mstmp	File, Archive	22263	2010/10/05 09:17:22	2010/10/27 16:30:59	2010/10/05 09:17:22

起こりうる問題と技術的な取り組み

起こりうる問題

- マルウェアによるアンチフォレンジック
  - e.g., タイムスタンプの変更
- 感染した疑いのあるPCが多数存在
  - 全てやろうとすると解析が追いつかない
- 感染したPCが遠隔地に存在
  - 解析に時間がかかる

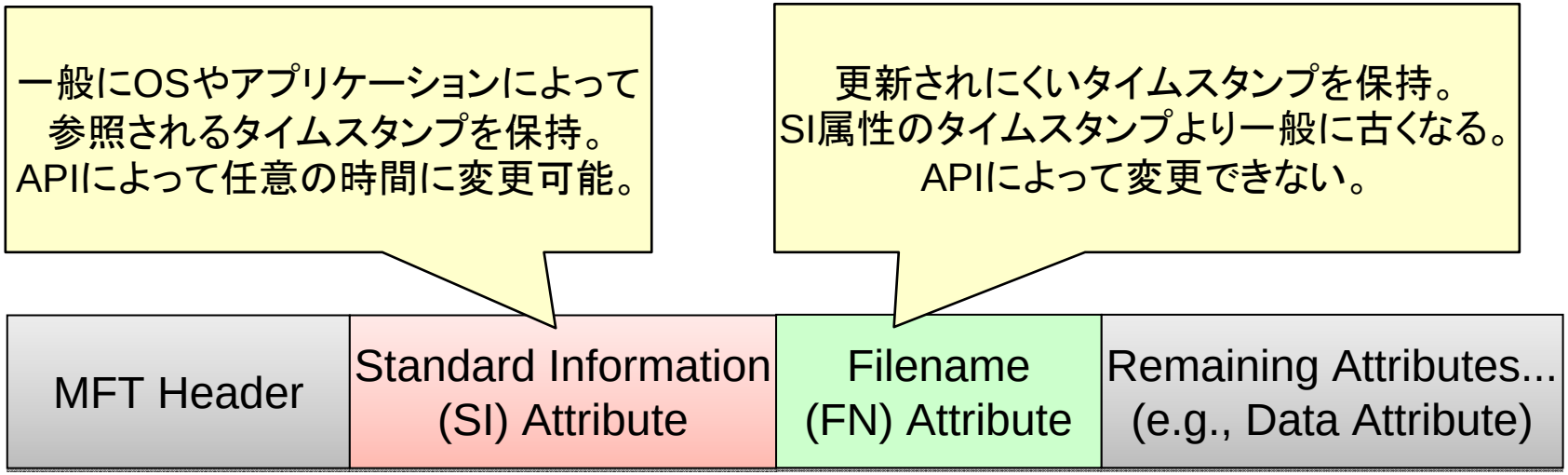
起こりうる問題

タイムライン調査による見逃しを防止する取り組み

- マルウェアによるアンチフォレンジック
  - e.g., タイムスタンプの変更
- 感染した疑いのあるPCが多数存在
  - 全てやろうとすると解析が追いつかない
- 感染したPCが遠隔地に存在
  - 解析に時間がかかる

ファイルシステムのタイムスタンプ

- NTFSファイルシステムはMaster File Table (MFT)にファイルのメタデータを保存
- MFTレコードは**2種類のタイムスタンプセット**を持つ
  - MACE（更新/最終アクセス/生成/エントリ更新）のセットが2つの属性データに含まれる



FN属性を考慮したタイムライン作成機能の実装

SI属性のタイムスタンプ

Create Date

[SI] 132B7A3-2\C\Program Files (x86)\Windows NT\TableTextService\ TableTextServiceSimplifiedZhengMa.txt	File, Archive, Hard Linked	1810352	2009/07/14 06:38:37	2009/07/14 06:38:37	20
[SI] 132B7A3-2\C\Program Files (x86)\Windows NT\TableTextService\ TableTextServiceYi.txt	File, Archive, Hard Linked	44968	2009/07/14 06:38:38	2009/07/14 06:38:38	20
[SI] 132B7A3-2\C\Program Files (x86)\DOSDROP\dosdrop.exe	File, Archive	4096	2009/06/12 12:29:17	2009/06/12 12:29:17	20
[SI] 132B7A3-2\C\Program Files (x86)\DOSDROP\dosdrop.exe	File, Archive	40960	2009/06/12 12:29:17	2009/06/12 12:29:17	20

FN属性のタイムスタンプ

[FN] 132B7A3-2\C\Program Files (x86)\Common Files\System\Ole DB\ oledb32.dll	File, Archive, Hard Linked	864256	2010/04/15 20:57:58	2010/04/15 20:57:58	20
[FN] 132B7A3-2\C\Program Files (x86)\DOSDROP\dosdrop.exe	File, Archive	4096	2010/04/15 20:59:49	2010/04/15 20:59:49	20
[FN] 132B7A3-2\C\Program Files (x86)\DOSDROP\dosdrop.exe	File, Archive	40960	2010/04/15 20:59:49	2010/04/15 20:59:49	20
[FN] 132B7A3-2\C\Program Files (x86)\DOSDROP\dosdrop.exe	File, Archive	40960	2010/04/15 20:59:49	2010/04/15 20:59:49	20
[FN] 132B7A3-2\C\Program Files (x86)\DOSDROP\dosdrop.exe	File, Archive	40960	2010/04/15 20:59:49	2010/04/15 20:59:49	20
[FN] 132B7A3-2\C\Program Files (x86)\DOSDROP\readme.txt	File, Archive	211	2010/04/15 20:59:49	2010/04/15 20:59:49	20

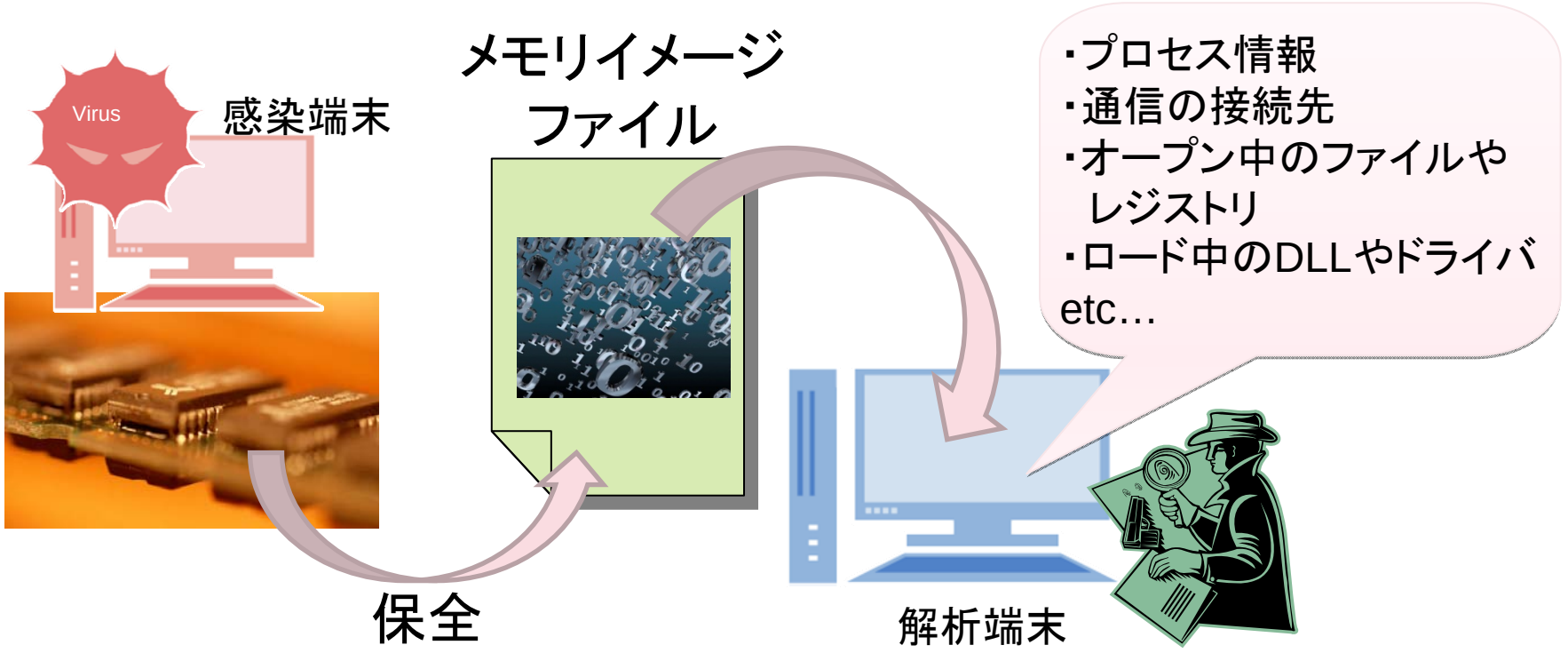
起こりうる問題

- マルウェアによるアンチフォレンジック
  - e.g., タイムスタンプの変更
- 感染した疑いのあるPCが多数存在
  - 全てやろうとすると解析が追いつかない
- 感染したPCが遠隔地に存在
  - 解析に時間がかかる

対応スピードを上げる技術的な取り組み

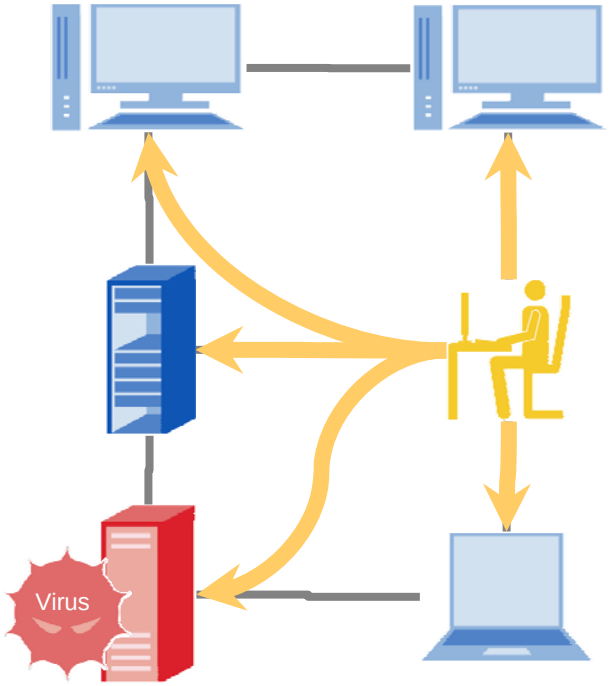
メモリフォレンジックツールの実装・調査

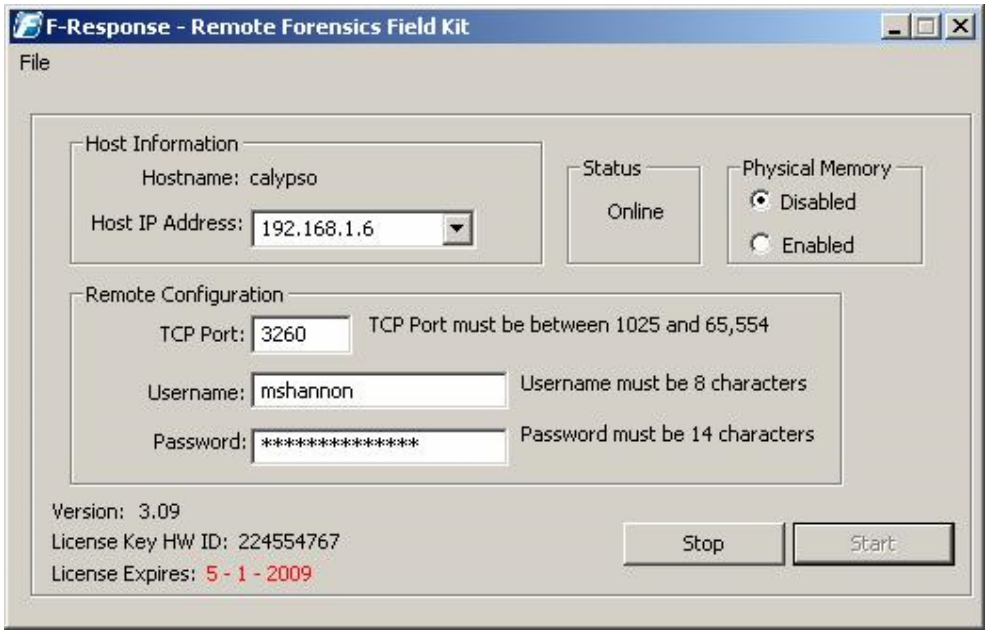
- 数百GBのディスクを調べる前に数GBのメモリを調べる
- 終了したプロセスやクローズした通信を調べることが可能
- 2つの手法で解析
  - Tree & list traversal： 仮想アドレスを変換してポインタを解決
  - Object “fingerprint” searches： カーネルオブジェクトをcarving



参考：リモートプレビュー技術の紹介

- エージェントを介した遠隔プレビュー・保全
  - 感染有無がグレーなマシンを迅速にチェック可能
  - 副次的な効果：ディスク暗号化の解除が不要

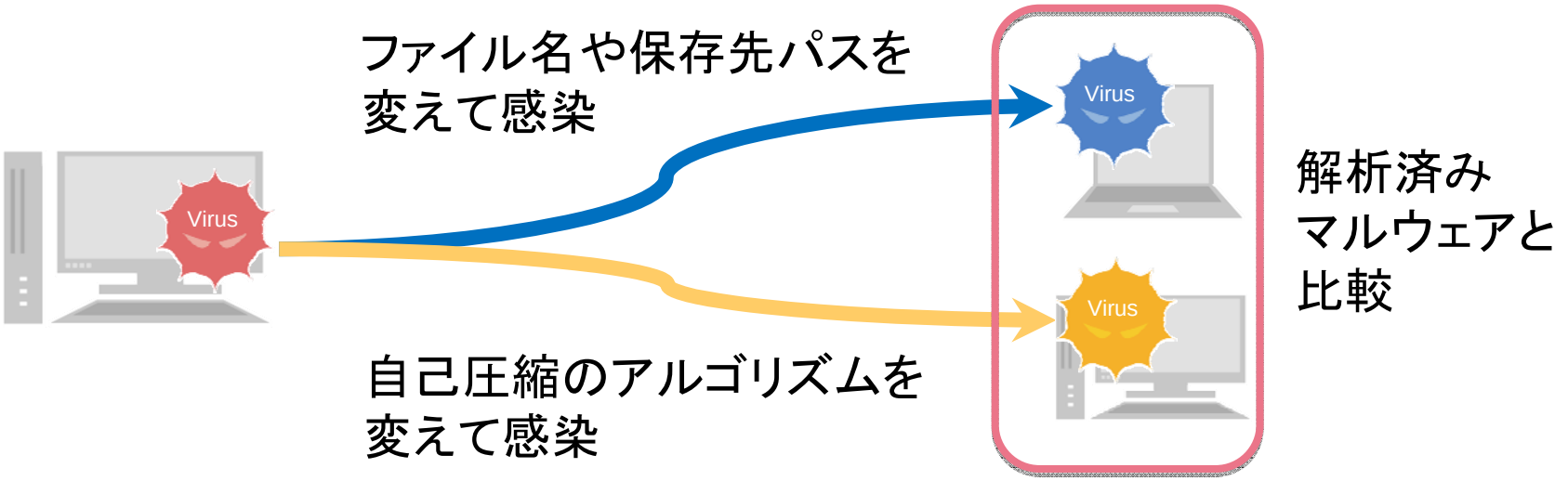




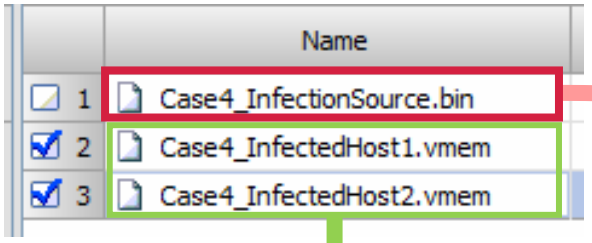
対応スピードを上げる手法の例

- 遠隔からメモリ上に展開されたプロセスやDLLの特徴量（エントロピー）を計算して既存マルウェアにマッチするものを検出
  - 各PCやその中のバイナリを個別に調べていく手間を省く

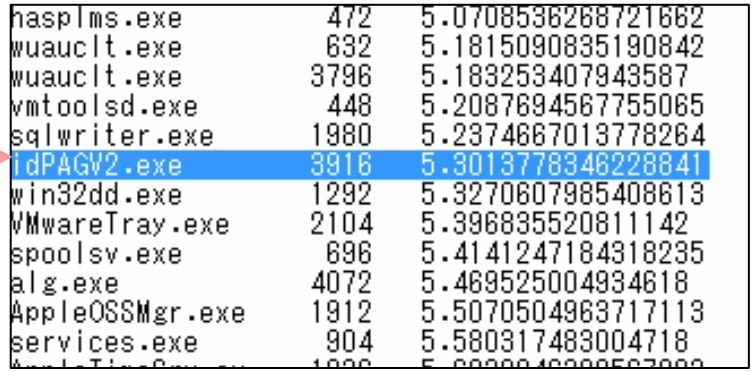
  →日単位でかかる対応を分単位で可能にする



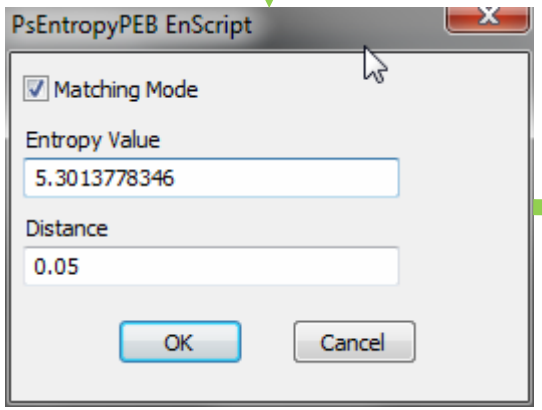
実装

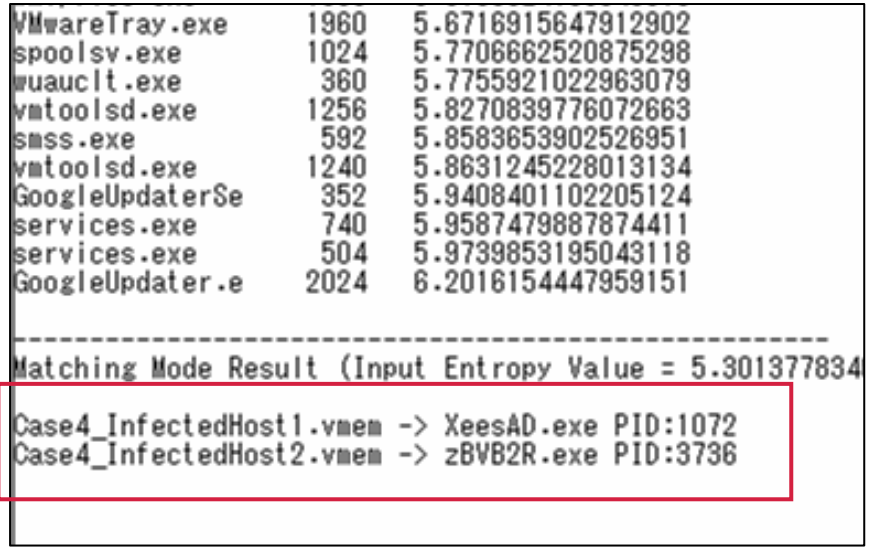


①既知マルウェアの
エントロピーを計算



②既知マルウェアのエントロピーに
近いプロセスを検出





Appendix

参考：仮想化システムのフォレンジック

- ハイパーバイザーベースの仮想化システムにおいて、ゲストOSのメモリ情報をホストOSからプレビュー・保全・解析

```
C:¥Program Files¥Debugging Tools for Windows (x64)>LiveCloudKd.exe
     LiveCloudKd - 1.0.20100813
     Microsoft Hyper-V Virtual Machine Live Kernel Debugger
     Microsoft Hyper-V Virtual Machine Physical Memory Dumper
     Copyright (C) 2010, MoonSols SARL <http://www.moonsols.com>
     Copyright (C) 2010, Matthieu Suiche
     All rights reserved.

  Virtual Machines:
   --> [0] Windows7 Pro Office

  Please select the ID of the virtual machine you want to play with
  > 0
  You selected the following virtual machine : Windows7 Pro Office

  Action List:
   --> [0] Live kernel debugger
   --> [1] Linear physical memory dump
   --> [2] Microsoft crash memory dump

  Please select the Action ID
  > 2

  Destination path for the virtual machine physical memory dump
  > C:¥test.dmp

  Total Size: 1024 MB
  Starting... Done.
```

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation