

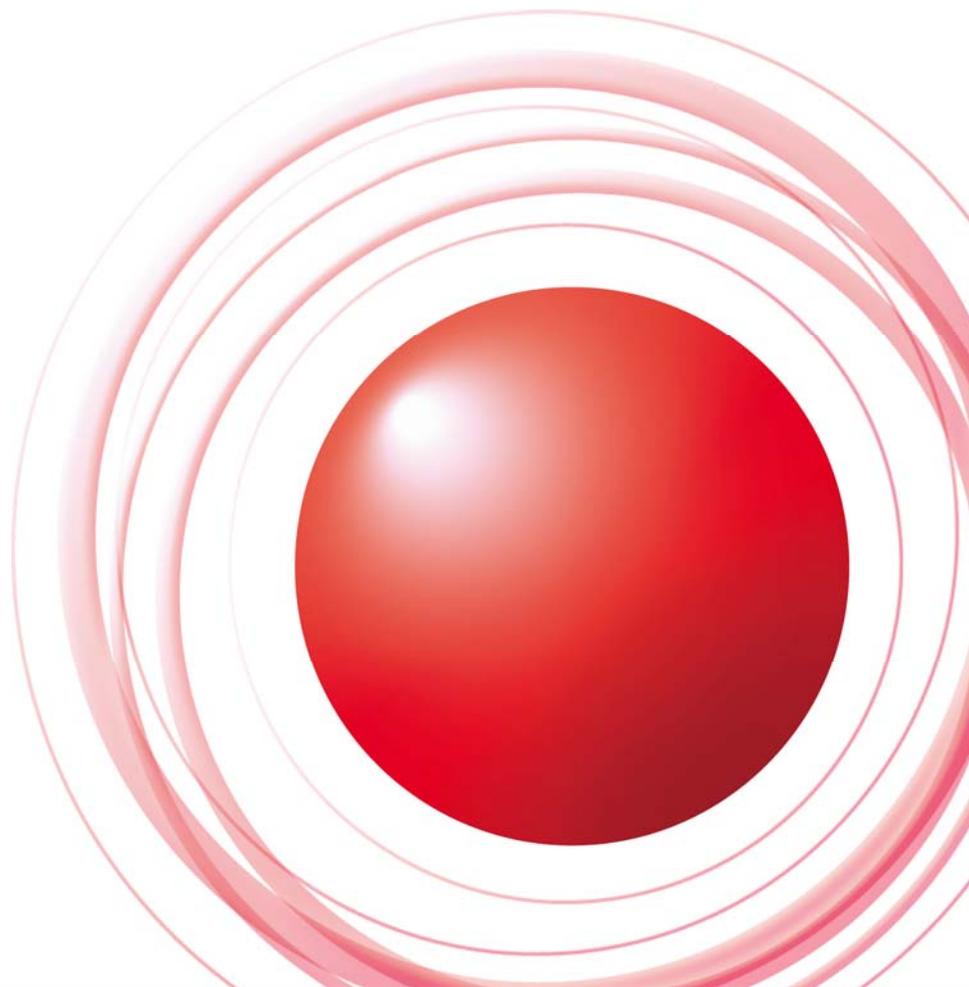
セキュリティ動向2010(2) デジタルフォレンジックに関する取り組み



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



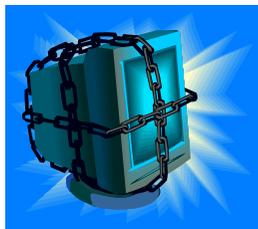
Overview

- 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

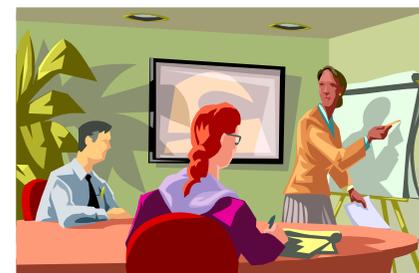
デジタルフォレンジックとは

- 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



CPUレジスタ



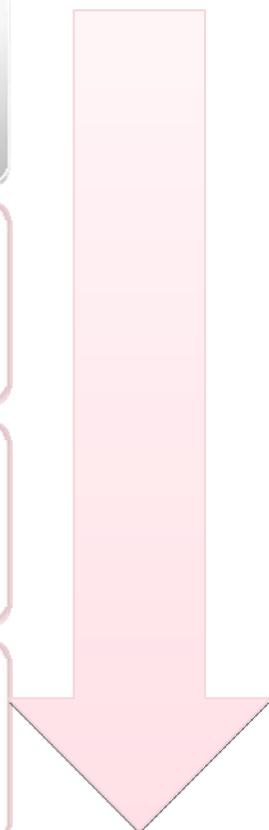
メモリ



ディスク



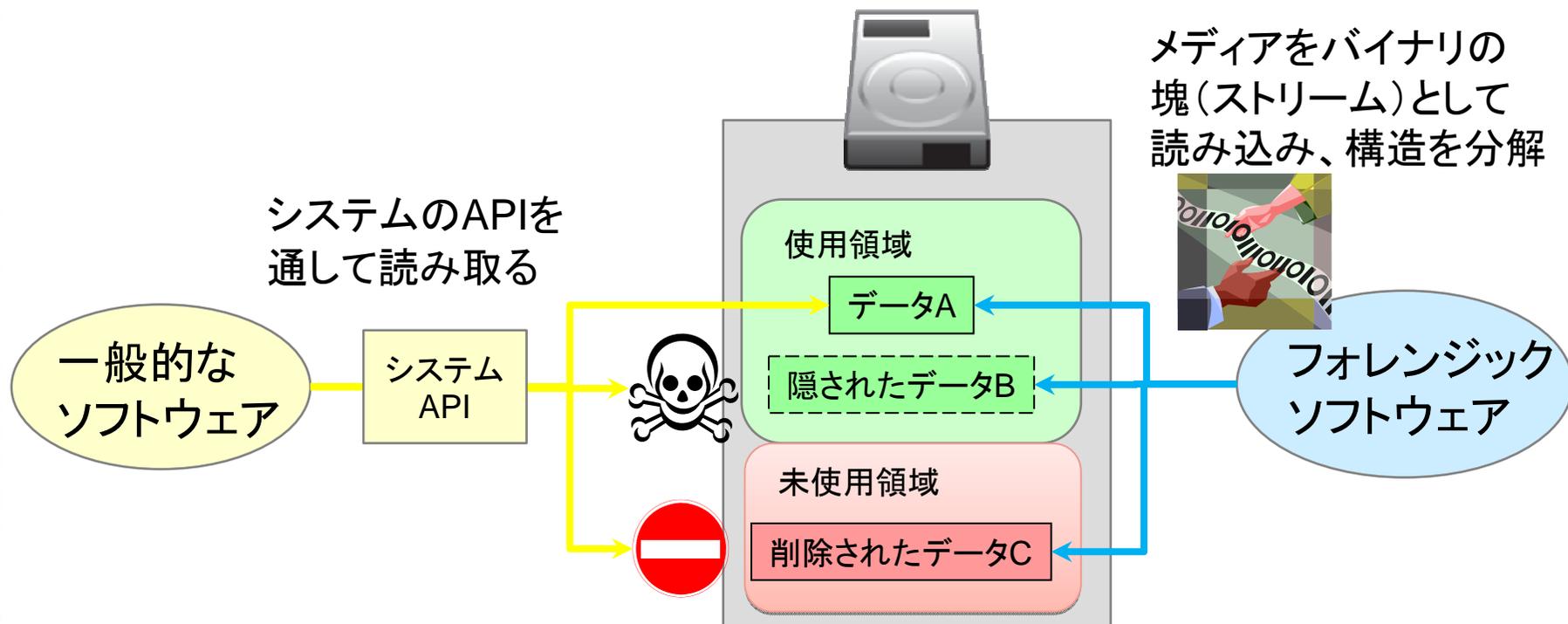
CD-ROM等の
バックアップメディア



- 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

Name	Filter	In Report	File Ext	File Type	File Category	Signature
1 Unallocated Clusters		No				

```

000000000000D0 30 3B 6B DF 23 BF E7 03 10 F4 58 AD 05 26 3C 62 56 B6 63 C4 34 83 75
000000000024F1 EC 38 D1 F8 D9 42 27 EB 6D 74 A3 30 1D 54 15 F7 7F 29 0E DC 87 59 00
0000000000485A 0E DE 83 0D C6 28 ED 45 08 61 E2 04 E5 70 7E C0 A7 21 E3 0F 5D A0 54
0000000000725D 73 50 A1 88 E8 29 B0 4B 22 B5 33 50 A1 93 1D BE CB CC 70 A2 6D B5 FD
00000000009656 5F C5 A7 13 56 1E A3 9C 9C D1 C6 DB C6 BD 8F 1E 36 40 0A 95 B3 93 10
    
```

0;kb#zG·ôX--&<bV¶cÄ4fu
ñ18ÑøÙB'ëmt£0·T·÷□)·Ü±Y·
Z·bf Æ((IE·aâ·âp~À\$!ã·] T
]sPj^è)°K"µ3Pj"·¾EÏpçmý
V_À\$·V·£ceceÑÆÙÆ½¼·6@ ·³"



認証情報(キーファイル、パスワード等)の入力 

Name	Filter	In Report	File Ext	File Type	File Category	Signature
43 hiberfil.sys			sys	Device Driver	Code\$Executable	
44 NTDETECT.COM			COM	DOS Executable	Code\$Executable	
45 TPHKLOCK.TXT			TXT	Text	Document	
46 boot.ini			ini	Initialization	Windows	
47 drivez.log			log	Log	Document	
48 syslevel.lgl			lgl			
49 SafeBoot.rsv			rsv			

```

0005B 62 6F 6F 74 20 6C 6F 61 64 65 72 5D 0D 0A 74 69 6D 65 6F 75 74 3D 33 30 0D 0A 64 65 66 61 75 6C 74 3D 6D 75
0376C 74 69 28 30 29 64 69 73 6B 28 30 29 72 64 69 73 6B 28 30 29 70 61 72 74 69 74 69 6F 6E 28 31 29 5C 57 49 4E
07444 4F 57 53 0D 0A 5B 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 73 5D 0D 0A 6D 75 6C 74 69 28 30 29 64 69
11173 6B 28 30 29 72 64 69 73 6B 28 30 29 70 61 72 74 69 74 69 6F 6E 28 31 29 5C 57 49 4E 44 4F 57 53 3D 22 4D 69
14863 72 6F 73 6F 66 74 20 57 69 6E 64 6F 77 73 20 58 50 20 50 72 6F 66 65 73 73 69 6F 6E 61 6C 22 20 2F 6E 6F 65
18578 65 63 75 74 65 3D 6F 70 74 69 6E 20 2F 66 61 73 74 64 65 74 65 63 74 0D 0A
    
```

[boot loader] timeout=30 defa
lti(0)disk(0)rdisk(0)partition(0)
DOWS [operating systems] mult
sk(0)rdisk(0)partition(1)\WINDC
crosoft Windows XP Professional
xecute=optin /fastdetect

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
📁 E01	2010/10/29 20:24	EnCase Evidence File	2,047,985 KB
📁 E02	2010/10/29 20:26	E02 ファイル	2,047,984 KB
📁 E03	2010/10/29 20:28	E03 ファイル	2,047,984 KB
📁 E04	2010/10/29 20:29	E04 ファイル	2,047,984 KB
📁 E05	2010/10/29 20:31	E05 ファイル	2,047,984 KB
📁 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	██████████
Actual Date	2010/10/29 20:22:57
Target Date	2010/10/30 05:22:58
File Path	██████████.E01
Case Number	██████████
Evidence Number	██████████
Examiner Name	th
Notes	██████████ SafeBoot
Label	/dev/sda
Model	██████████
Serial Number	██████████
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	9554815648e364a5f6a27dc80f3c6bc2
Verification MD5	9554815648e364a5f6a27dc80f3c6bc2
GUID	██████████

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	[Redacted]
2010/10/05 09:16:33	[Redacted]
2010/10/05 09:16:33	[Redacted]
2010/10/05 09:16:34	[Redacted]
2010/10/05 09:16:34	[Redacted]
2010/10/05 09:16:34	[Redacted]
2010/10/05 09:16:51	PrivacIE:64.27.25.224/1/*/
2010/10/05 09:16:55	[Redacted]
2010/10/05 09:22:58	[Redacted]

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)

ID	Path	Type	Size	Created	Modified	Accessed
95	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	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	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	C:\Documents and Settings\...\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	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

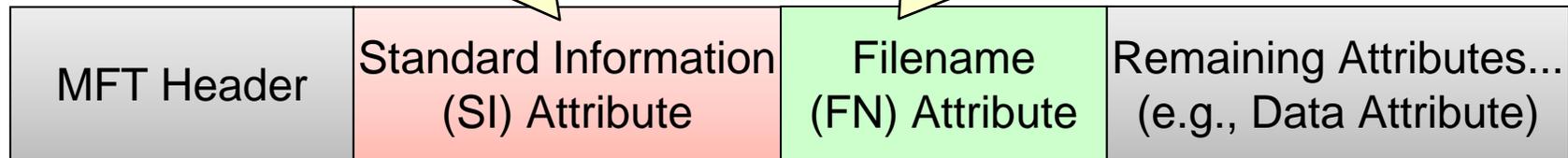
- マルウェアによるアンチフォレンジック
 - e.g., タイムスタンプの変更
- 感染した疑いのあるPCが多数存在
 - 全てやろうとすると解析が追いつかない
- 感染したPCが遠隔地に存在
 - 解析に時間がかかる

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

一般にOSやアプリケーションによって参照されるタイムスタンプを保持。APIによって任意の時間に変更可能。

更新されにくいタイムスタンプを保持。SI属性のタイムスタンプより一般に古くなる。APIによって変更できない。



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	40960	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	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\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

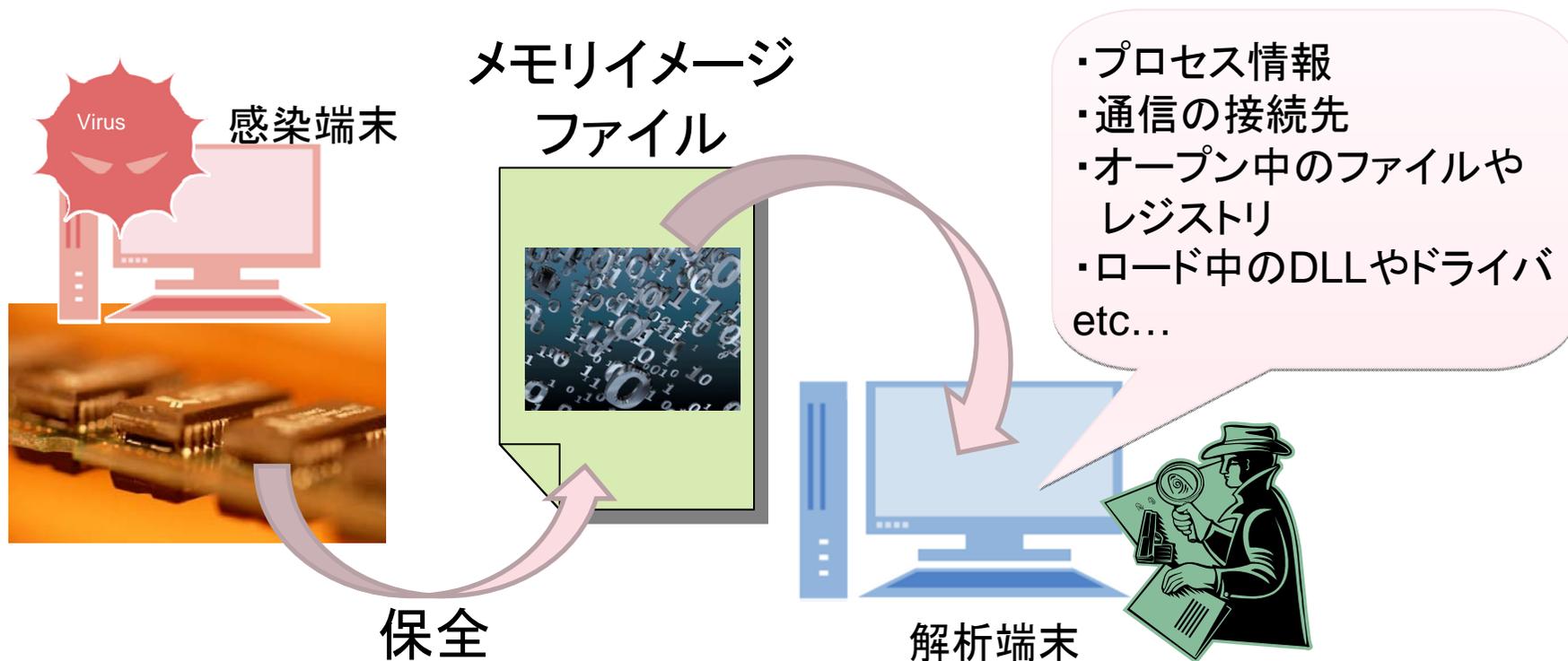
起こりうる問題

- 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

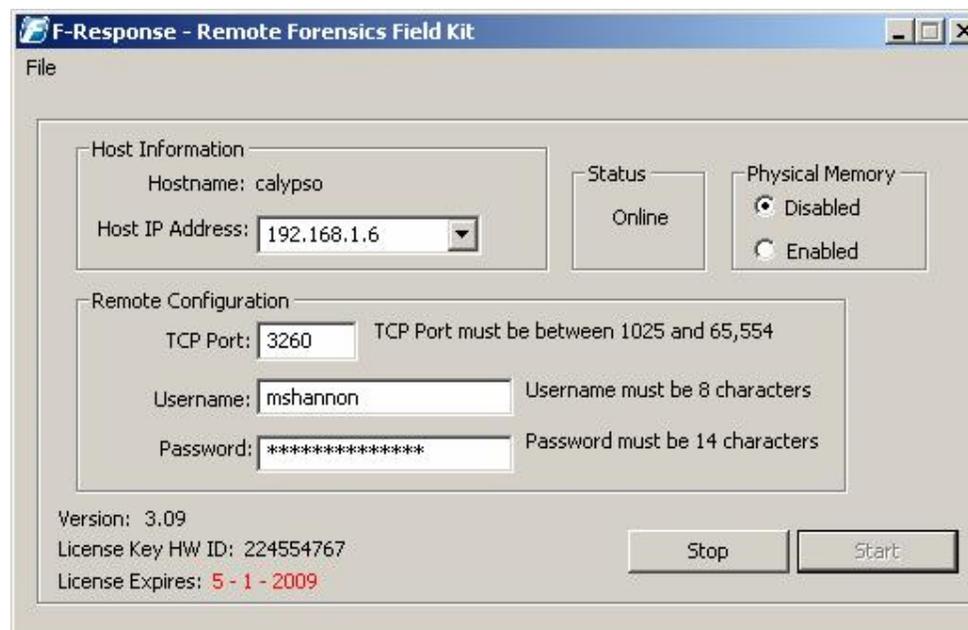
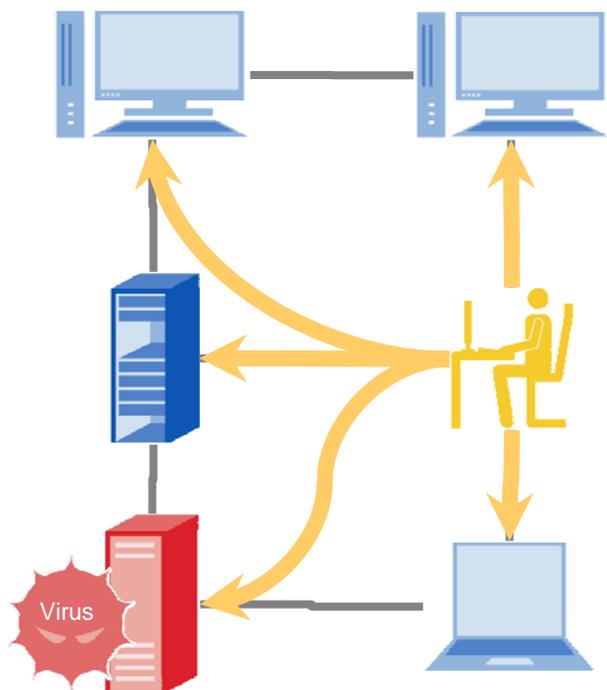
メモリフォレンジックツールの実装・調査

- 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事が可能
- 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



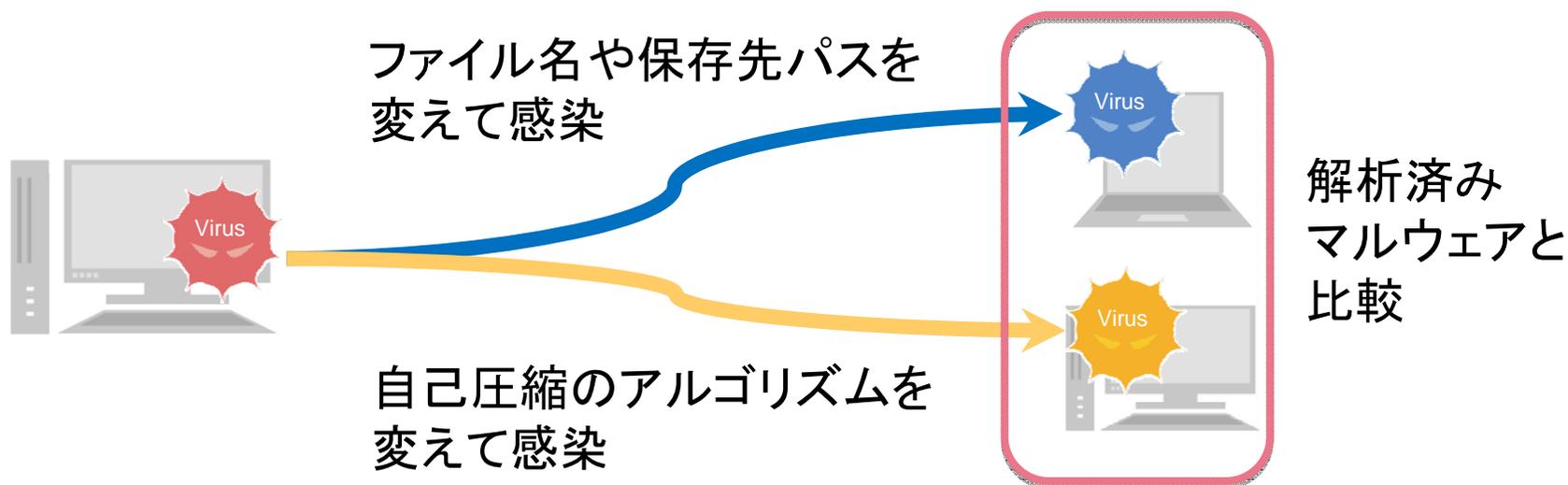
参考：リモートプレビュー技術の紹介

- 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

	Name
<input type="checkbox"/>	1 Case4_InfectionSource.bin
<input checked="" type="checkbox"/>	2 Case4_InfectedHost1.vmem
<input checked="" type="checkbox"/>	3 Case4_InfectedHost2.vmem

hasplms.exe	472	5.0708536268721662
wuauclt.exe	632	5.1815090835190842
wuauclt.exe	3796	5.183253407943587
vmtoolsd.exe	448	5.2087694567755065
sqlwriter.exe	1980	5.2374667013778264
idPAGV2.exe	3916	5.3013778346228841
win32dd.exe	1292	5.3270607985408613
VMwareTray.exe	2104	5.396835520811142
spoolsv.exe	696	5.4141247184318235
alg.exe	4072	5.469525004934618
AppleOSSMgr.exe	1912	5.5070504963717113
services.exe	904	5.580317483004718
...

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

PsEntropyPEB EnScript

Matching Mode

Entropy Value
5.3013778346

Distance
0.05

OK Cancel

VMwareTray.exe	1960	5.6716915647912902
spoolsv.exe	1024	5.7706662520875298
wuauclt.exe	360	5.7755921022963079
vmtoolsd.exe	1256	5.8270839776072663
smss.exe	592	5.8583653902526951
vmtoolsd.exe	1240	5.8631245228013134
GoogleUpdaterSe	352	5.9408401102205124
services.exe	740	5.9587479887874411
services.exe	504	5.9739853195043118
GoogleUpdater.e	2024	6.2016154447959151

Matching Mode Result (Input Entropy Value = 5.301377834)

Case4_InfectedHost1.vmem	->	XeesAD.exe	PID:1072
Case4_InfectedHost2.vmem	->	zBV82R.exe	PID:3736

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.
```



ご清聴ありがとうございました

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ, Internet Initiative Japan は、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示しておりません。©2010 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事例は、将来予告なしに変更することがあります。