初動対応とファスト・フォレンジック

デジタル・フォレンジック研究会「技術」分科会

2018/03/19

株式会社 サイバーディフェンス研究所　山崎 輝

CyberDefense

目次

CyberDefense

1. ファスト・フォレンジック導入の背景と経緯
2. 保全／収集（CDIR-C）
3. 解析（CDIR-A）
4. ファスト・フォレンジック適用事例と得られた教訓

1. ファスト・フォレンジック
導入の背景と経緯

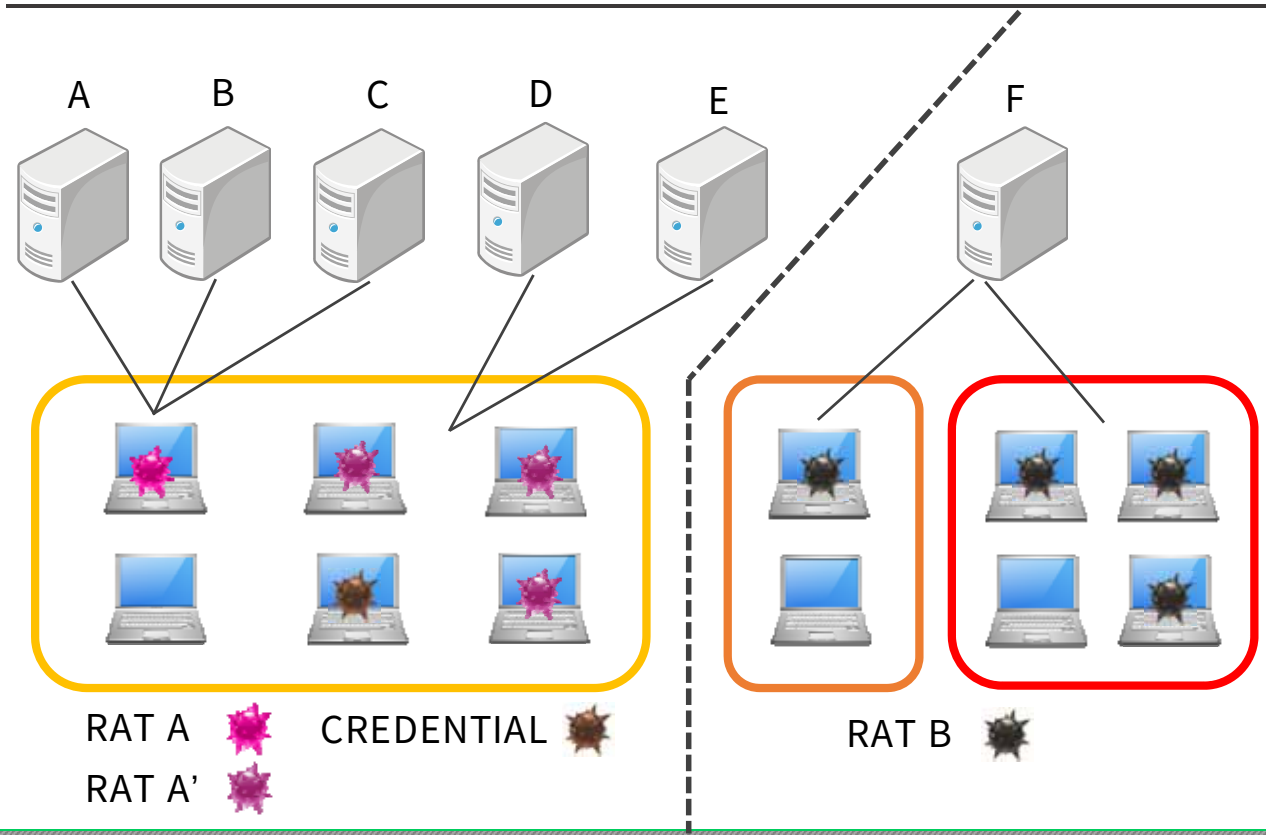
CyberDefense

インシデント事例

CyberDefense

- 2015年の標的型攻撃
- 外部通報により発覚
- 不審な通信は半年以上前から発生
- 攻撃者による情報窃取活動の可能性
- 感染台数・規模は不明

侵害状況



フォレンジック調査の特徴

- メリット
  - 未知の被害対象を発見
  - 未知のマルウェア、C2を発見
  - 調査対象の被害有無を高精度に判定
- デメリット
  - ディスクの保全・解析に時間（コスト）がかかる
  - 結果的に深く調査する必要が無かった場合の損失が大きい
  - 被組織システム全体（全端末）のチェックは困難

情報共有のトライアングル

“早さと正確性、網羅性はいずれか2つしか満たせない”

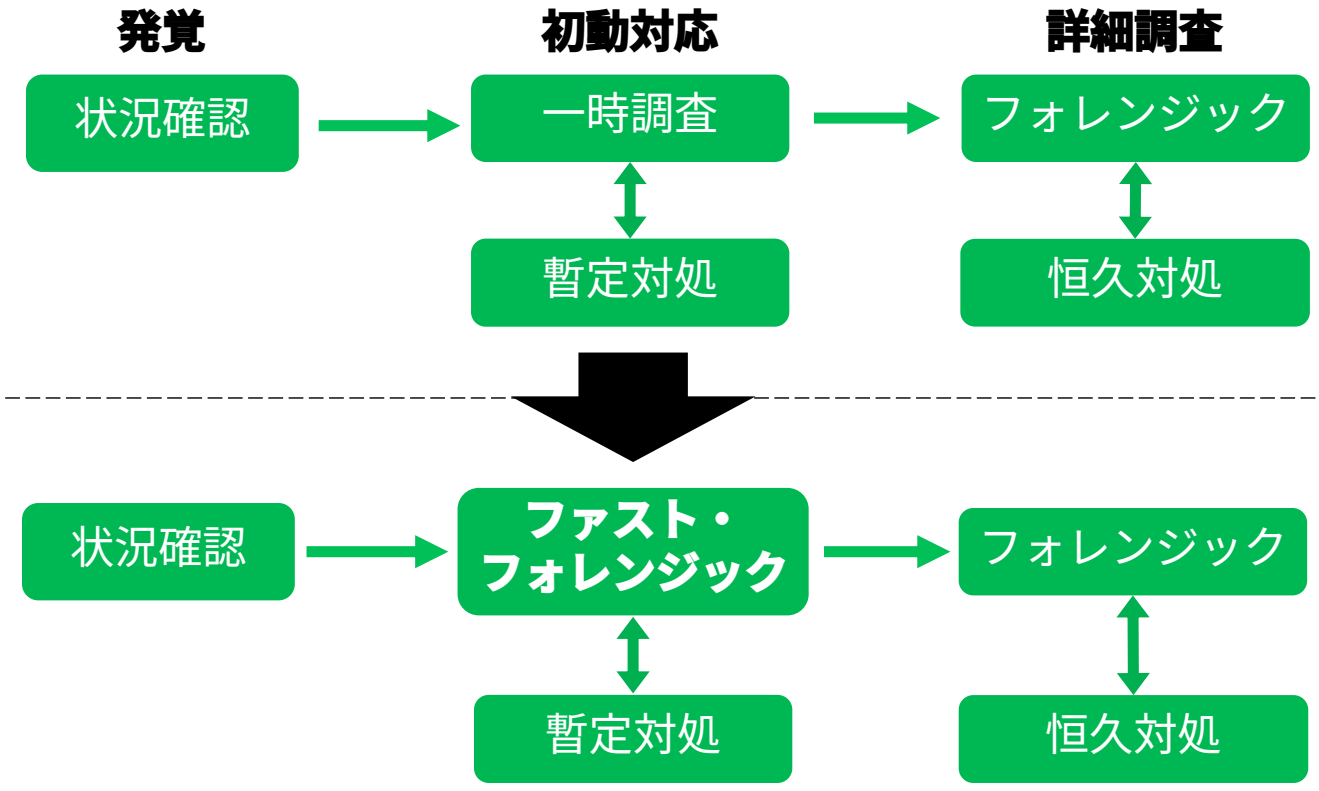
（参照）セキュリティ対応組織(SOC/CSIRT)強化に向けた サイバーセキュリティ情報共有の「5W1H」（P.15）
http://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.0.pdf

- インシデント対応における情報共有を考えると…
  - 初動対応では**早さ**を重視
  - フォレンジック調査は**正確性**と**網羅性**を確保

ファスト・フォレンジックの検討

- 初動対応にフォレンジック要素を盛り込む
- 網羅性を犠牲にして**早さ**を確保
- 目的はインシデント発覚後の被害範囲／深刻度の早期判断
- EDRが導入されていない環境を想定

インシデント対応フロー



ファスト・フォレンジックツール CDIR

2016年5月リリース
https://www.cyberdefense.jp/products/cdir.html

CSIRTのインシデント対応能力を強化

CDIRは適切な初動対応を支援することを目的としたツールです。調査対象端末の汚染や業務への影響を最小限に抑えながら調査対象データを安全に収集し、インシデントの影響範囲と被害内容を迅速に把握することが出来ます。フォレンジック調査の一部を内製化できるだけでなく、社外のフォレンジック専門チームとの連携を円滑にすることが出来ます。

CDIRの現状構成

	オープンソース	プロトタイプ
保全／収集	**CDIR-C**	CDIR Cloud
解析	**CDIR-A**	CDIR-A Wrapper CDIR-V

2. 保全／収集（CDIR-C）

保全／収集ツールのコンセプト

CyberDefense

- インシデント発覚後、現場での利用を想定
  ⇒ 日本語対応や使いやすさを重視
- 対象はWindows
  ⇒ ログだけでなく他のアーティファクトやメモリも取得
- 保全／収集時に加工しない
  ⇒ 解析時に様々なツールが使える
- インシデント発覚時に制限なく使える
  ⇒ オープンソース（無償利用可）

CDIR-C 概要

CyberDefense

- https://github.com/CyberDefenseInstitute/CDIR
- NTFS内部ファイルや使用中ファイルを取得
- オープンソースのツール／ライブラリを活用

データ種別	ツール／ライブラリ
メモリ	winpmem
メタデータ	NTFSParserDLL
ジャーナル	
イベントログ	
プリフェッチ	
レジストリ	
ブラウザ	

CDIR-C メモリ取得処理

CyberDefense

- winpmem-2.1.post4.exe
  （https://github.com/google/rekall/releases）
  - CDIR-Cでコマンドライン実行を自動化
- 既知の問題
  - VSM（Virtual Secure Mode）が有効な環境でBSoD
  - 大容量メモリ（64GB以上）搭載環境でBSoD
- 対応
  - メモリ取得をOFF設定にしてCDIR-Cを実行する
  - メモリの保全は別のツールを活用する

CDIR-C メイン処理

CyberDefense

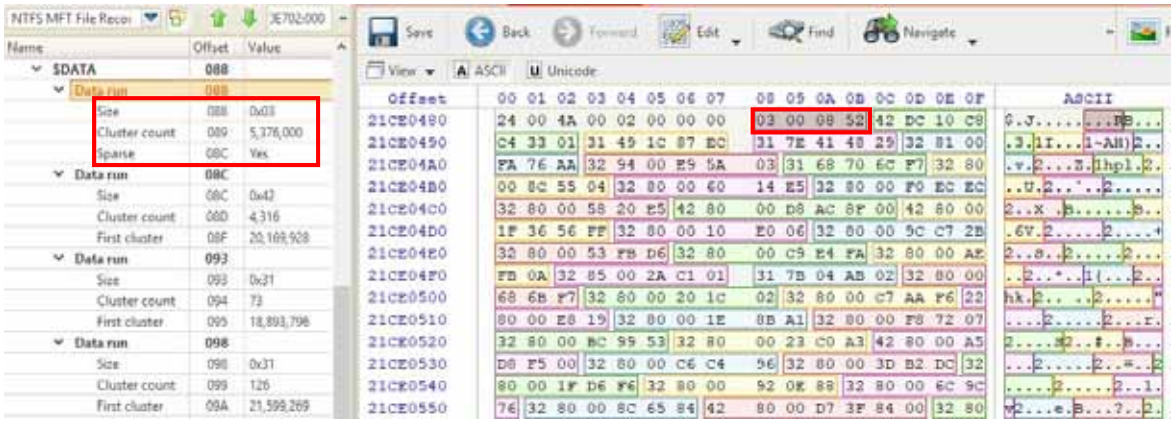
- NTFSParserDLL
- NTFS上のファイルのOpen/Read/Close
- NTFSの構造を解釈し各データの保存位置を直接参照
  - MFT
  - FileRecord
  - Attribute
  - DataRun
  - Stream

  …
- 既知の問題（2018/3時点のバージョン 1.2.2）
  - Windows 10の一部環境でファイル取得エラー
  - ユーザプロファイルが別ドライブの場合にエラー

CDIR-C USNジャーナルのスパーススキップ

CyberDefense

- USNジャーナルはスパースを使った特徴的な保存



- スパース領域を0x00で扱うと無駄な書込処理が発生
  ⇒ CDIR-C側でスパース領域はスキップするように例外処理

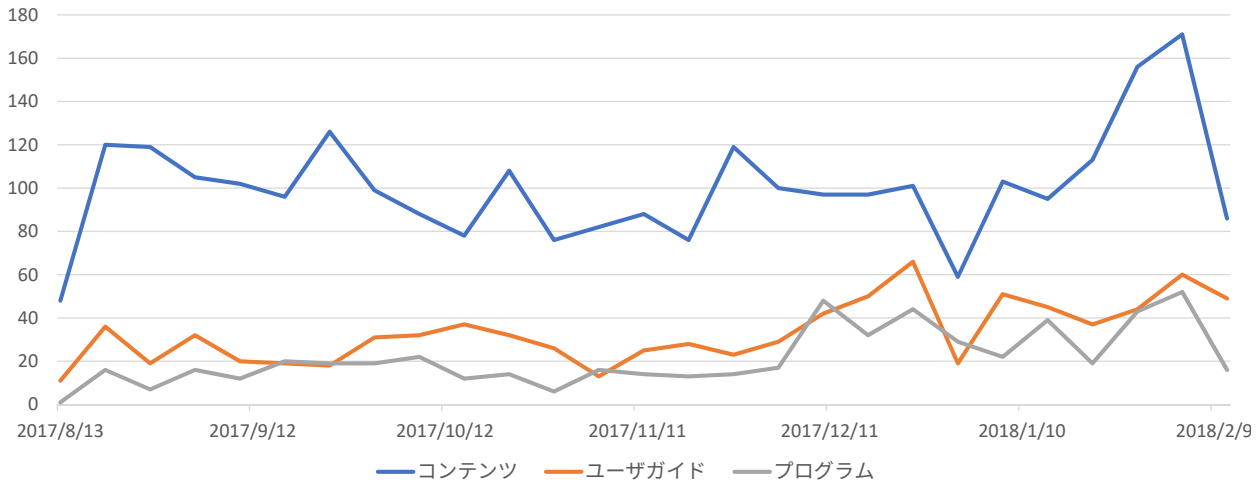
CDIR-C ロギング

CyberDefense

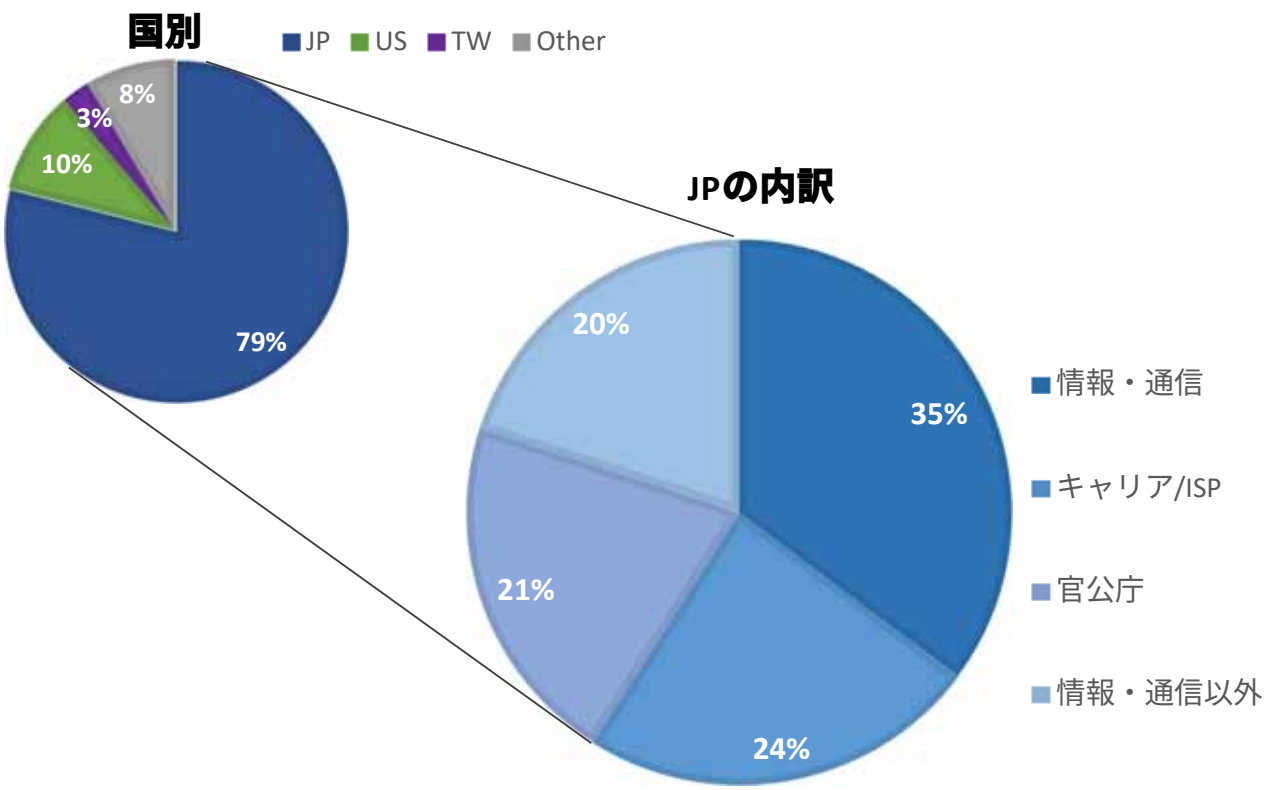
- 取得開始／終了日時
- 取得ファイルのハッシュ値
  - MD5
  - SHA-1
  - SHA-256
- ファイルのタイムスタンプ
  - 作成
  - 最終更新
  - 最終アクセス

CDIR-C アクセス／ダウンロード状況

- 集計期間：直近半年（2017/8/13 – 2018/2/15）
  - コンテンツ　：　2800
  - ユーザガイド：　900
  - プログラム　：　600



CDIR-C アクセス／ダウンロード属性



「証拠保全ガイドライン」における位置づけ

CyberDefense

- CDIR-Cはフォレンジック調査の対象とするか判断（=トリアージ）するための初動対応支援ツール

- 揮発性情報（メモリ）の取得機能があるため、対象をフォレンジック調査することになった場合、「証拠保全ガイドライン」の一部項目を担う

- 「証拠保全ガイドライン」第６版（18～20ページ）
  3.2.2 対象物がコンピュータ（デスクトップ型）で、電源がONの状態の場合
  3.2.3 対象物がコンピュータ（ノート型）で、電源がONの状態の場合

  ④ 揮発性情報の取得
  ・調査の目的、必要性に応じて、揮発性情報を取得する。

CDIR Cloud（プロトタイプ）

CyberDefense

- WebDav経由のデータ送信
- クライアント機能はCDIR-C内に実装済

3. 解析（CDIR-A）

CyberDefense

CDIR-A 概要

CyberDefense

- https://github.com/CyberDefenseInstitute/CDIR-A
- Log Parser Studioライブラリとオリジナルパーサ

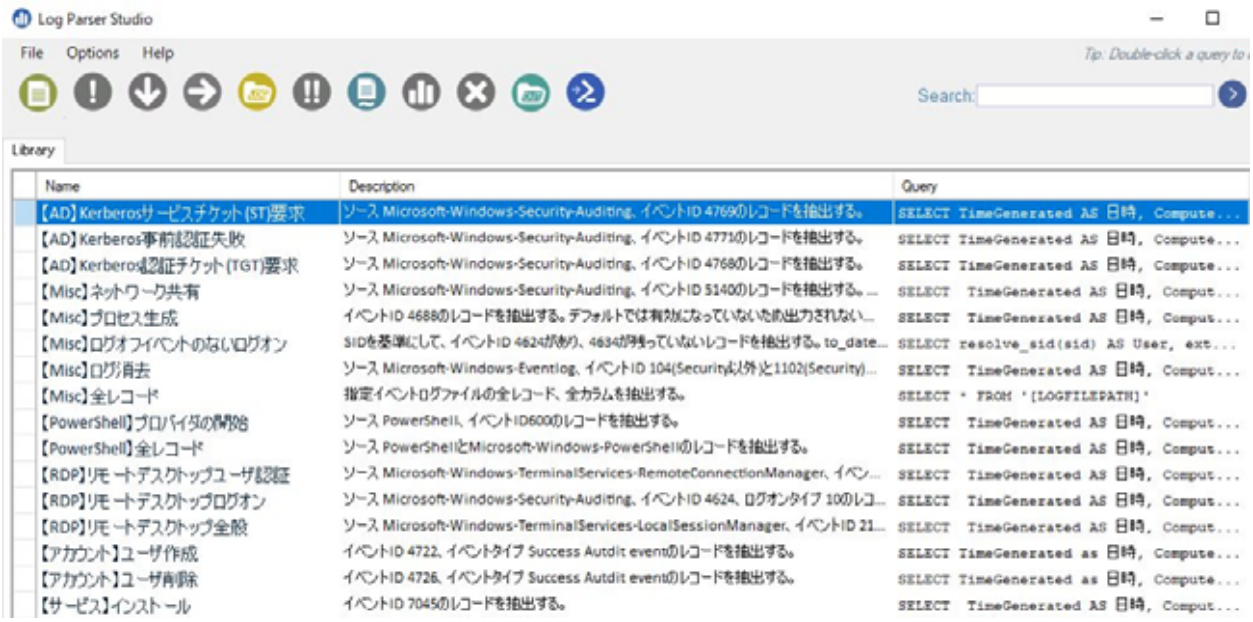
データ種別	ツール
イベントログ	Log Parser Studioライブラリ
プリフェッチ	prefetch.exe
レジストリ	shimcache.exe amcache.exe regruns.exe
ジャーナル	usnjrnl.exe
メタデータ	mft.exe

- メモリ、ブラウザはサードパーティツールを活用

CDIR-A イベントログ解析

CyberDefense

- Log Parser Studio用のライブラリを維持／管理



CDIR-A オリジナルパーサ

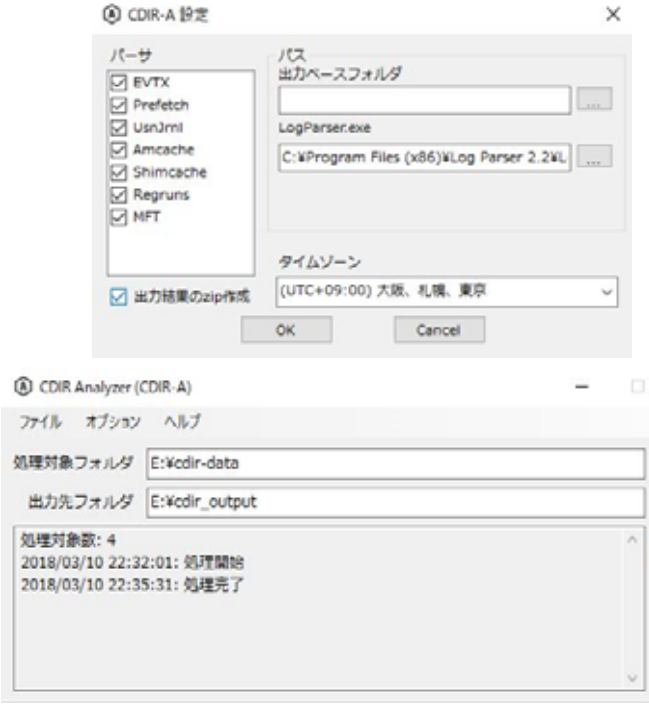
CyberDefense

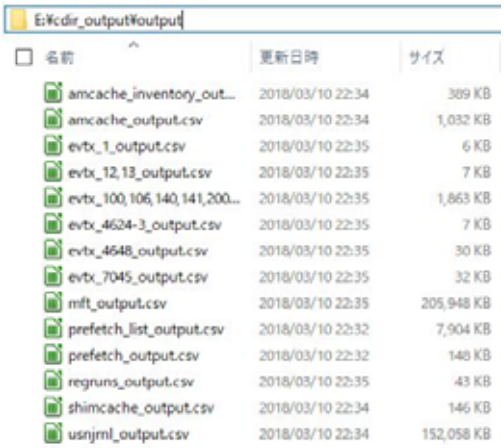
- コマンドライン
- オプション体系の統一
  ⇒ パーサ.exe -o 出力結果フォルダ 入力フォルダ
- 複数台分のデータ処理を考慮

CDIR-A Wrapper（プロトタイプ）

CyberDefense

- 複数のパーサ、複数のデータをGUIで一括処理

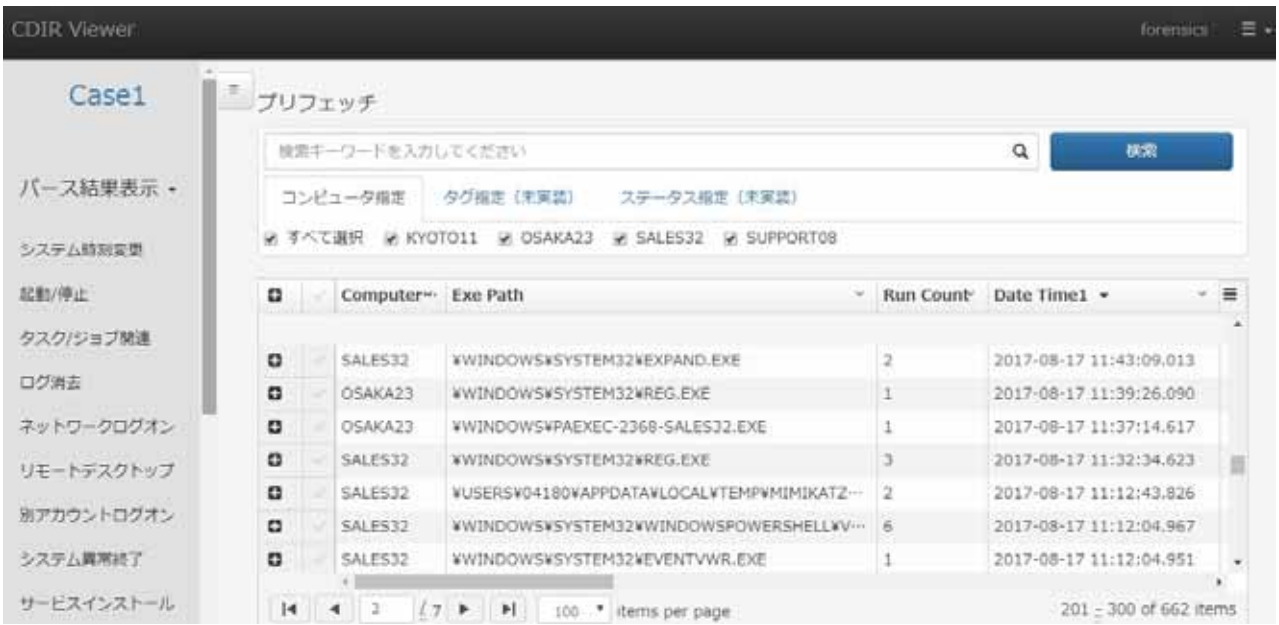




CDIR-V（プロトタイプ）

CyberDefense

- パーサ結果を表示、解析者支援機能を搭載したビューア



サードパーティツールによる解析

- Bulk Extractor
  （http://downloads.digitalcorpora.org/downloads/bulk_extractor/）
- KaniVola
  （https://www.kazamiya.net/KaniVola）
- USN Analytics
  （https://www.kazamiya.net/usn_analytics）
- plaso
  （https://github.com/log2timeline/plaso）
- BrowsingHistoryView
  （https://www.nirsoft.net/utils/browsing_history_view.html）
- RegRipper
  （https://github.com/keydet89/RegRipper2.8）
- ShellBags Explorer
  （https://ericzimmerman.github.io/）

4. ファスト・フォレンジック 適用事例と得られた教訓

Case1

CyberDefense

- ファスト・フォレンジック
  - 外部からの情報提供により対応開始
  - プロキシサーバログから追加で不審な通信を確認
  - 解析結果から追加で横展開の痕跡を確認
- フォレンジック
  - ファスト・フォレンジックにより深刻と判断したPCの詳細調査
- ファスト・フォレンジック導入効果
  - 当初目的の初動対応の早さとして一定の役割を果たす
  - 組織間の調整、連携や手続きに時間がかかっている

Case2

CyberDefense

- フォレンジック
  - クラウドプラットフォーム上のサーバを詳細調査
  - 根本原因の特定
- ファスト・フォレンジック
  - 別サーバで類似事象発覚
  - ネットワーク（RDP）経由のデータ取得／解析
- ファスト・フォレンジック導入効果
  - コストを抑えた対応の実現
  - 有益な情報は得られるが原因・被害状況特定の決定打とはならない

Case3

CyberDefense

- ファスト・フォレンジック&フォレンジック
  - 外部からの情報提供により対応を開始
  - CDIR／ディスク保全に同時に着手
  - 取得完了データ（CDIR-C／ディスクイメージ）を順次解析

- ファスト・フォレンジック導入効果
  - メモリデータ解析により新たなマルウェアを発見
  - ディスク複製もしていたため初動対応の早さという点では効果半減
  - 解析時の被害範囲／深刻度の分類をする上でCDIR-Aが効果を発揮

得られた教訓

CyberDefense

- メモリを保全／解析するかの判断が難しい
  - BSoDのリスク
  - メモリの大容量化
  - 状況によっては役に立たない可能性が高い

- 収集／保全データ拡充の必要性
  - 解析の結果確認したファイルの追加取得
  - アプリケーションログ
  - 不審ファイル

- 現状のCDIRでは数百台~の対応は困難
  - 大規模な対応はEDRを使ったアプローチが望ましい
  - EDRの評価が難しい（導入コスト／解析深度など）

今後の予定

CyberDefense

- 保全／収集機能の強化
  - Linuxサーバ向けの保全／収集ツール
  - CDIR-Cのメンテナンス
  - CDIR-C収集データの追加、カスタマイズ
    - レジストリトランザクションログ
    - $SECURE
    - SRUM
    - パス指定
  - バグ報告／要望の受付
    （https://github.com/CyberDefenseInstitute/CDIR/issues）
- 解析機能の強化
  - パーサのアップデート、拡充