CyberDefense

証拠保全ガイドライン第4版の説明

2015年3月20日

デジタル・フォレンジック研究会
第11期第4回「技術」分科会

名和 利男／サイバーディフェンス研究所

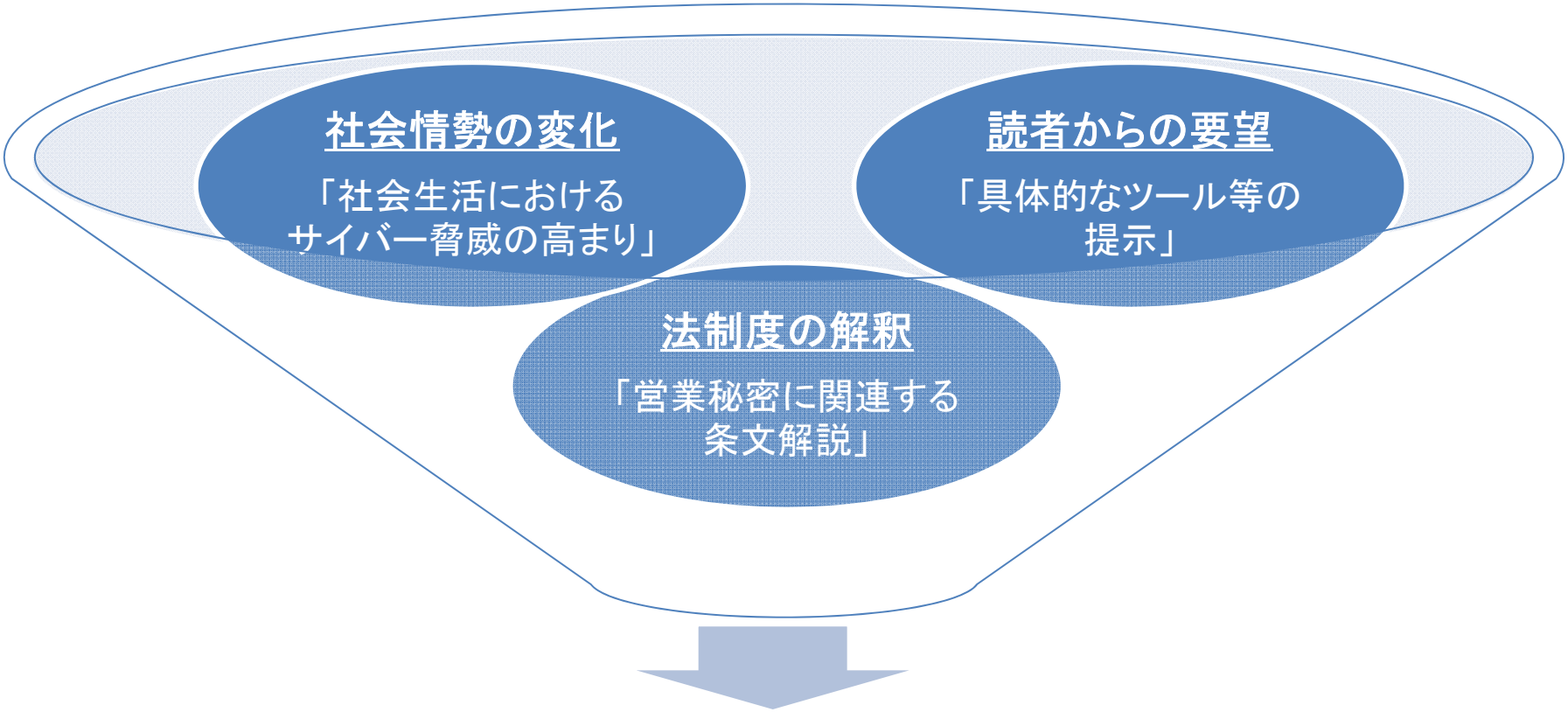
デジタル・フォレンジック研究会とは

特定非営利活動法人
デジタル・フォレンジック研究会　定款

第３条　この法人は、広く一般市民を対象として、情報セキュリティの新しい分野である「デジタル・フォレンジック」の啓発・普及、調査・研究事業、講習会・講演会、出版、技術認定等の事業を通じて、**健全な情報通信技術（IT）社会の実現**に寄与・貢献することを目的とする。

（健全 ＝ 物事が正常に機能して、しっかりした状態にあること）

第4版への改訂の背景



第4版への改訂

改訂ポイント ー 状況認識

「ガイドラインの趣旨」に対する状況認識の追加

“最近のサイバー犯罪やサイバー攻撃で利用される不正プログラムは、痕跡を残さない回避技術が高度化しているため、**コンピュータ・システム内に残存する痕跡やログが極端に少なくなってきている**。一方、メモリ空間で動作する不正プログラムは、メモリの中にその挙動を示す痕跡が残っているが、電源供給を断つと記憶内容が消失してしまう（揮発性が高い）。そのため、**メモリ上の情報の保全の重要性**が高まってきている。”

改訂ポイント ー 状況認識

Windows 内の正規プログラムを動作させる不正スクリプトの事例を紹介

メモリ上で、第三者が作成した「悪意のあるプログラム」は動作せず、
Windows自身が信頼している正規プログラムが動作するため、残存する
痕跡は、PCユーザによる動作と見分けがつかない。

（別資料を投影のみで説明）

改訂ポイント ー 対象物の収集・取得・保全

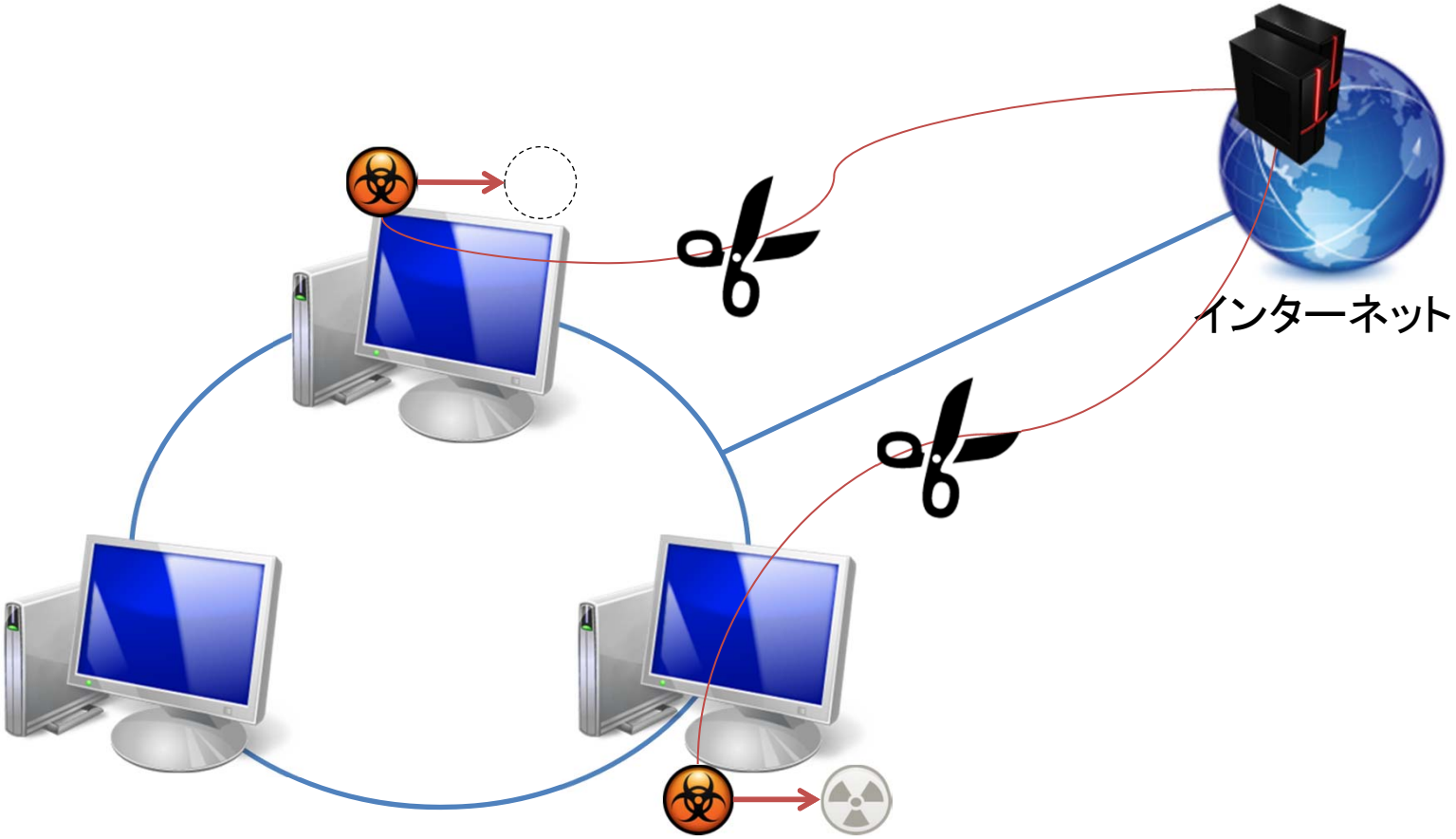
「対象物の収集・取得・保全」に電源に関する措置を追加

○ 電源の供給停止の可否について

- 対象物に電源を供給し続けることで明白な被害（破壊等）の拡大或いはそのおそれが見られる場合、速やかに電源の供給を停止する必要がある。また、**不要な通信のみを避けたい場合、電源の供給を継続したままネットワークから切り離す**。
- 速やかに電源の供給を停止をする必要が見られない場合、**揮発性情報の取得**（後述）を行うまで、電源の供給を停止しないことが望ましい。

改訂ポイント ー 対象物の収集・取得・保全

感染したマルウェアの一部は、C2ホストと通信ができなくなると、
消失や形態を変えて、潜在化するものがある。



改訂ポイント －証拠保全機器の準備

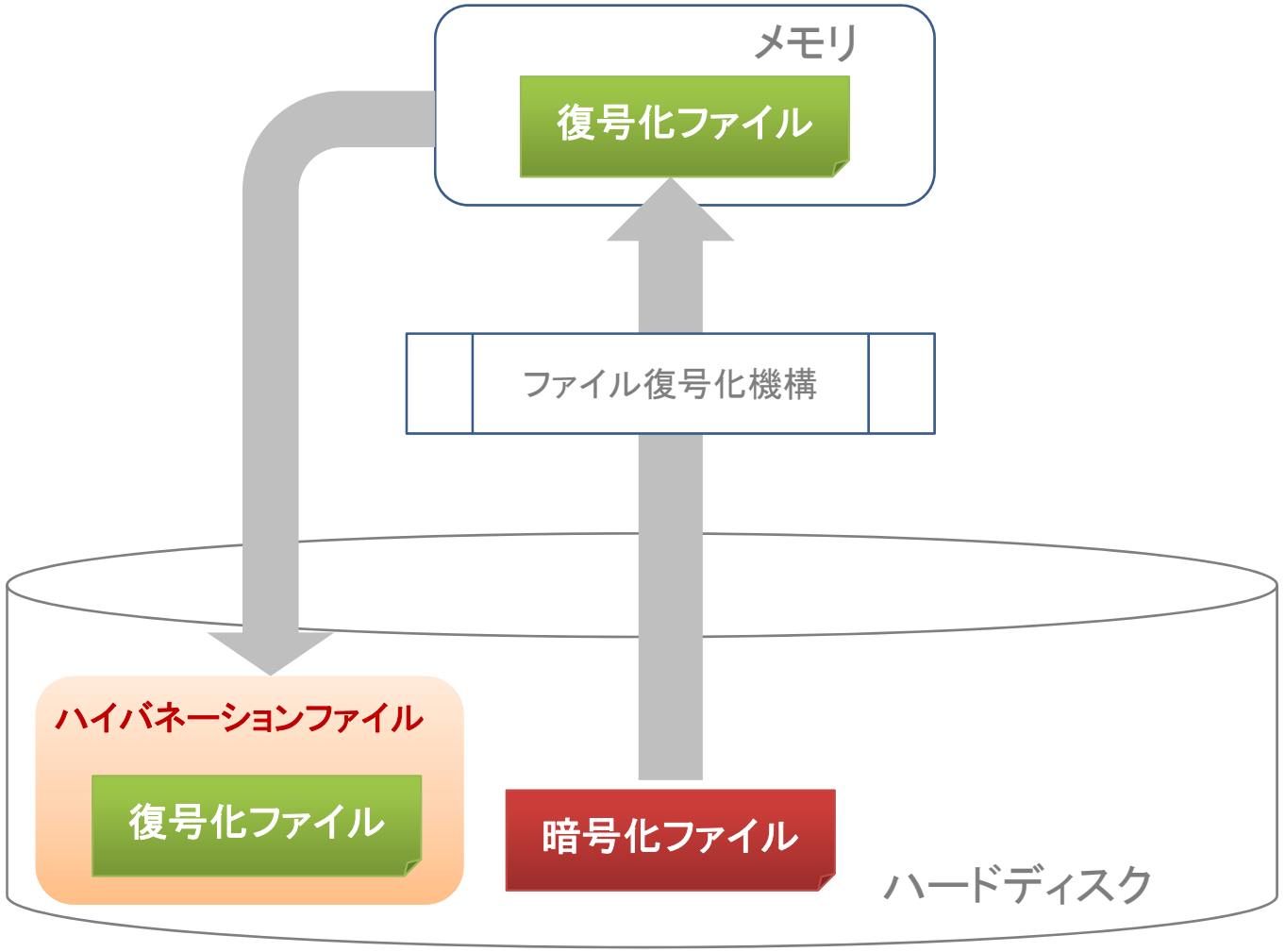
「代表的な収集及び分析ツールの利用時の留意事項」にツールに関する事項を追加

4.3.3　代表的な収集及び分析ツールの利用時の留意事項

- ○　一部のツール利用にあたっては、コンピュータの動作原理の理解が必要
- ○　最近のマルウェアの挙動に関する情報を把握しておくほど、効果が増大
- ○　揮発性情報を収集するツールを利用する暇がない場合 、**OSのハイバネーション機能を使ってHDDに残す**方法もある。ただし、HDD上の一部のデータ（ログや証跡を含む）を上書きするため、HDDの証拠保全の完全性が損なわれる。

改訂ポイント －証拠保全機器の準備

ハイバネーションファイルが保存されたハードディスクは、
盗難されないよう細心の注意を払うことが必要



改訂ポイント ーデジタル・フォレンジックに関連する我が国の主な刑事法

「不正競争防止法」に関する事項を追加

（定義）

第二条第六項

この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

（罰則）

第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律　（平成十一年法律第百二十八号）第二条第四項　に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者

改訂ポイント ーデジタル・フォレンジックに関連する我が国の主な刑事法

「不正競争防止法」に関する事項を追加

営業秘密に関する事項は不正競争防止法に定められている。曖昧な概念で使われる「企業秘密」という言葉とは異なり、「営業秘密」は同法の2条6項によってきちんとした定義がなされている。この条文から「秘密管理性」「有用性」「非公知性」が営業秘密成立の三要件となる。

条文自体の記載は省略しているが、不正競争防止法では、その第2条第1項の各号においてどのような行為が不正競争となるかが定められている。そして同4号～9号までが営業秘密に関しての記載であり、ここに不正と見なされる営業秘密の取得や使用、開示等における様々な場合が列挙されている。

そしてそれらを侵害した場合の罰則規定が第21条に記載されている。こちらもすべての条文の記載を省略しているが、第21条第1項の第1号～第7号の各号において刑罰が科される様々な場合を記載している。2009年（平成21年）の改正によって、競合関係にある場合だけでなく、自己の利益の為に営業秘密を不正に取得したり使用したりした場合でも可罰化されたことが特徴である。

2015年（平成27年）3月時点での刑罰の量刑は、最大で10年以下の懲役もしくは1000万円以下の罰金またはこの併科であるが、**2014年に起きたベネッセでの営業秘密持ち出し事件を経て、これがさらに重罰化される予定なので注意しておく必要がある**。

なお、営業秘密の管理に関する公的な指針としては「営業秘密管理指針」が経済産業省より公表されている。この指針は2015年（平成27年）1月に全面的な改定がなされ、従来の事例を詳細に記載する形式のものから「不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示すもの」に変更された。

改訂ポイント ーデジタル・フォレンジックに関連する我が国の主な刑事法

一般社団法人 日本知的財産協会 JAPAN INTELLECTUAL PROPERTY ASSOCIATION

ENGLISH / HOME / サイト内検索 / 検索 / 検索方法

トップ ＞情報発信 ＞シンポジウム・フォーラム

会員専用ページへ
協会研修会 予約サービス
協会会員サービス
会員専用ページの閲覧には当協会発行のユーザー名・パスワードが必要です。

協会紹介
- 協会概要
- 主な活動
- 入会案内
- 役員一覧
- 会員一覧
- 事務所所在地

協会活動
- 協会日程表
- 協会運営方針
- 政策プロジェクト
- 専門委員会活動
- 国際活動
- 前年度業務報告

情報発信
- 提言・意見
- 外部の会議体への参画
- シンポジウム・フォーラム

機関誌・資料
- 概要
- 「知財管理」誌
- 「知財管理」誌最新号
- 編集方針・投稿規定

研修
- 研修案内
- 日程・会場・講師等の変更
- 空席情報
- お知らせ
- 問い合わせ

Coffee Break

シンポジウム・フォーラム

第1回 技術情報防衛シンポジウム開催

～企業の大切な技術情報を守るために～

【日　時】		2014年9月5日(金)　10:00～17:00
【会　場】		コクヨホール
【主　催】		国際知的財産保護フォーラム(IIPPF)・独立行政法人 情報処理推進機構(IPA)・経済産業省 一般社団法人 日本知的財産協会
【開催趣旨】		あなたの会社は大丈夫ですか？　近年、日本企業における深刻な技術情報流出が次々と発覚しています。グローバル競争が激化する中、オープン＆クローズ戦略など知財戦略の高度化により秘匿技術の価値が高まる一方、人材の流動化、情報管理のIT化によって、流出懸念が増大しています。しかしながら、事の性格上、多くの部分が闇の中にあって防衛策が蓄積・共有されず、知財・情報管理者の戸惑いが解消されずにいます。本シンポジウムでは、技術情報流出の実態、予防策、問題発生時の対応策を紹介し、企業の大切な技術情報を守るための情報を提供していきます。
【プログラム】	10:00	■開会の挨拶 日本知的財産協会 営業秘密プロジェクトリーダー 佐々木剛史
	10:10	■講演 I　「営業秘密保護について」 木尾修文氏（経済産業省 経済産業政策局 知的財産政策室長）代理として 伊万里全生氏（知的財産政策室　総括補佐）
	10:30	■講演 II-1「サイバーセキュリティの観点より、営業秘密情報が置かれている状況について」 名和利男氏（株式会社サイバーディフェンス研究所 理事/上級分析官）
	11:40	■講演 II-2「企業における内部不正の現状と内部不正防止ガイドラインの紹介」 小松文子氏（独立行政法人情報処理推進機構 技術本部 セキュリティセンター 情報セキュリティ分析ラボラトリー長）
	12:30	昼休憩
	13:30	■講演 III「変動する経済環境と営業秘密法制―米国経済スパイ法をめぐって―」 玉井克哉氏　（東京大学　先端科学技術研究センター　教授）
	15:00	休憩

http://www.jipa.or.jp/jyohou_hasin/sympo/jyohobouei_sympo_1.htm

改訂ポイント ーデジタル・フォレンジックに関連する我が国の主な刑事法

IPA

組織における
内部不正防止ガイドライン

独立行政法人情報処理推進機構

http://www.ipa.go.jp/files/000041054.pdf

改訂ポイント ー 代表的な収集分析ツール

「代表的な収集分析ツール」を追加

●システム関連の情報取得ツールの例

- **analyzeMF**
  NTFSファイルシステムからMFTのファイルを解析するツール。
  nalyzeMFT
  https://github.com/dkovar/analyzeMFT
- **Event Log Explorer**
  ローカルコンピュータのイベントログの詳細分析や、ネットワーク上の複数のコンピュータのイベントログを集中管理できるツール。
  Event Log Explorer™ for Windows event log management
  http://eventlogxp.com
- **Log Parser**
  さまざまなログの中から必要な情報を検索し、特定の情報を抜き出すツール。並べ直しやExcel用のデータで出力するなど、多様なログ分析を支援する。
  Log Parser 2.2
  http://www.microsoft.com/download/en/details.aspx?id=24659
- **Log Parser Lizard**
  上述のLog Parse をGUI で使えるようにするツール。
  Lizard Labs
  http://www.lizard-labs.net

改訂ポイント ― 代表的な収集分析ツール

「代表的な収集分析ツール」を追加

●システム関連の情報取得ツールの例（続き）

- **Magnet RAM Capture**
  物理メモリのキャプチャや、データの復旧及び解析ができるフリーツール。
  Acquiring Memory with Magnet RAM Capture
  http://www.magnetforensics.com/acquiring-memory-with-magnet-ram-capture/
- **MoonSols Windows Memory Toolkit**
  メモリの取得や変換を実行するために必要なすべてのユーティリティを含むツール。
  MoonSols Windows Memory Toolkit
  http://www.moonsols.com/windows-memory-toolkit/
- **FTK Imager Lite**
  ハードディスクの情報を参照したり、メモリダンプの出力、VM などのイメージファイルの読み込みなどを行うツール。
  FTK Imager Lite
  http://accessdata.com/product-download/digital-forensics/
- **triage-ir**
  Windowsシステムでマルウェアの攻撃痕跡等の調査に必要となる情報を自動収集するツール。
  triage-ir
  https://code.google.com/p/triage-ir/
- **RTIR**
  Request Tracker for Incident Response の略。インシデントハンドリングに係るワークフローを最適化するためのツール。
  RTIR: RT for Incident Response
  https://www.bestpractical.com/rtir/

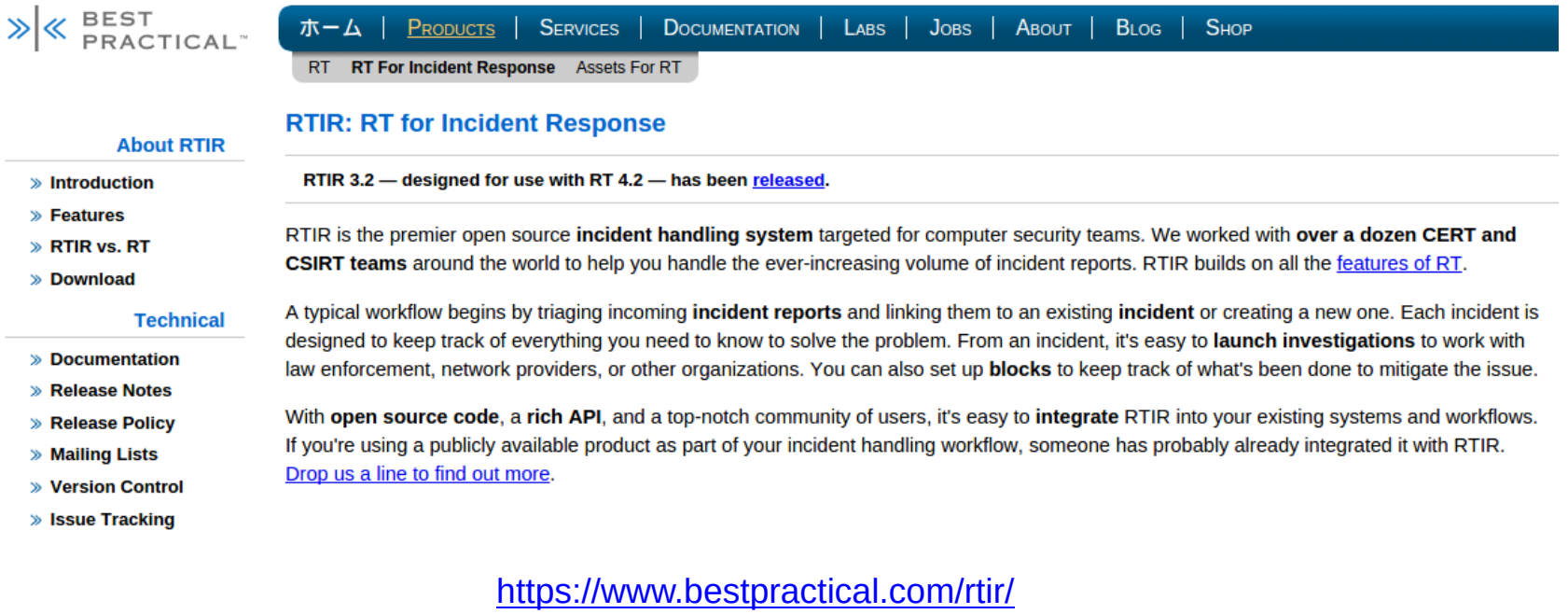
改訂ポイント ー 代表的な収集分析ツール

「代表的な収集分析ツール」を追加

●揮発性メモリの情報取得及び解析ツールの例

- **EnScript**
  Volatility Frameworkをベースにして、64ビット対応やキーワードサーチ機能などEnCaseの特長を生かして改良されたもの。
  enscript
  http://takahiroharuyama.github.io/
- **HGBary Responder**
  HBGary社によって開発・販売されている商用のメモリフォレンジックツール。そのオプション機能として提供されているDigital DNAは、プロセスアドレス空間に含まれるコードを分析して、悪性のコードかどうかをスコアリングする。
  Digital DNA
  http://mcsi.mantech.com/products/digital-dna
- **Redline**
  Mandiant社によって開発・提供されているフリーツール。同社で開発されているMemoryzeという解析ツールのGUIフロントエンドとして使われている。
  Redline ®
  https://www.mandiant.com/resources/download/redline
- **Volatility Framework**
  オープンソースのメモリフォレンジックツール。プロセス情報の列挙など基本的な機能のほか、有志によって様々なプラグインが提供されている。
  volatility An advanced memory forensics framework
  http://code.google.com/p/volatility/

改訂ポイント ー 代表的な収集分析ツール



https://www.bestpractical.com/rtir/

本資料に関する連絡先

名和 利男（Toshio NAWA）
サイバーディフェンス研究所
理事／上級分析官

Email: nawa@cyberdefense.jp
SNS: about.me/nawa
Tel: 03-3242-8700

Office: www.cyberdefense.jp
Response Team: www.cirt.jp