証拠保全ガイドライン第 7 版の説明

2018年8月

名和 利男

アジェンダ

1. 「証拠保全ガイドライン」とは
2. 改定にあたっての状況認識及び要望事項
3. 第 6 版から第 7 版への主な改訂事項
4. 今後について

トピック 1

「証拠保全ガイドライン」とは

「証拠保全ガイドライン」とは

- 想定読者
  - 主に、インシデントの現場で最初に電磁的証拠の保全にあたる「**ファースト・レスポンダ**」
  - これに限らず、**デジタル・フォレンジック関連技術を運用する全ての者**
- 主な特徴
  - （証拠保全ガイドラインに記述されている）手続きにより収集・取得・保全等された電磁的記録が法廷において証拠として必ず採用されることを**保証するものではない**。
  - 犯罪捜査や金融調査等、それぞれの**特性と法制に基づく手続きが存在することを前提**としたものである。
  - 我が国における電磁的証拠保全の一般的な手続きがどうあるべきか、どの程度まで行えばデータが「法的紛争・訴訟に際し利用可能な（Forensically-soundな）」電磁的証拠となりうるか、という運用現場の悩みに対し、**コンセンサスの形成の一助**になることを意図して作成されたもの。

「デジタル・フォレンジックとは」
インシデントレスポンス（*コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。*）や**法的紛争・訴訟**に際し、電磁的記録の**証拠保全**及び**調査・分析**を行うとともに、電磁的記録の改ざん・毀損等についての**分析・情報収集**等を行う一連の科学的調査手法・技術を言います。
https://digitalforensic.jp/home/what-df/

コンセンサスの例：「**自由心証主義**」
訴訟法上の概念で、事実認定・証拠評価について裁判官の自由な判断に委ねることをいう。裁判官の専門的技術・能力を信頼して、その自由な判断に委ねた方が真実発見に資するという考えに基づく。

トピック 2

改定にあたっての状況認識及び要望事項

改定にあたっての状況認識及び要望事項

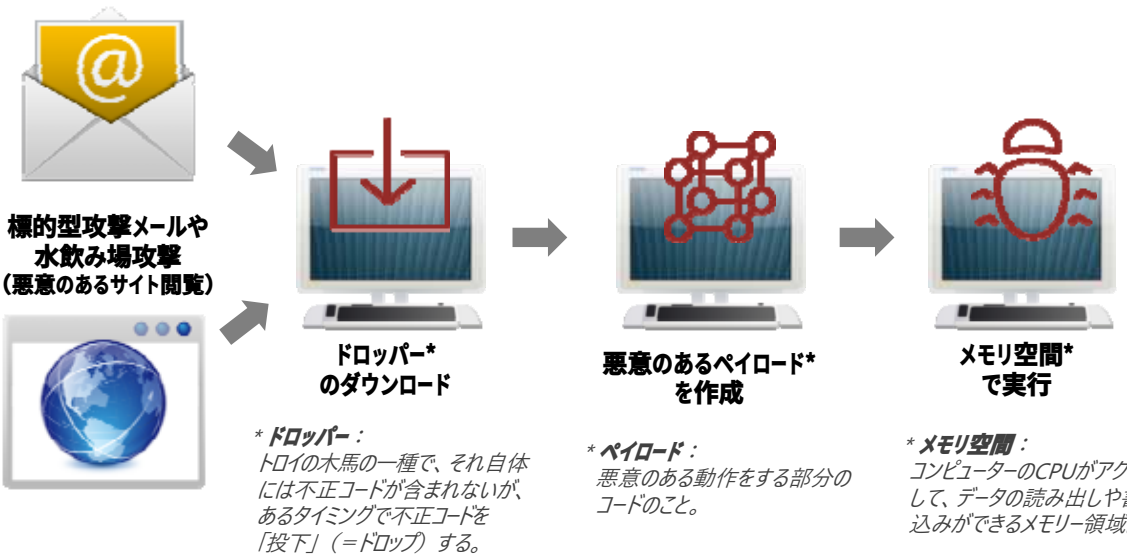
【状況認識】

- ファイルレス攻撃の常態化
- 重要インフラ事業分野等におけるガイドラインの整備
- よく利用されるデバイス（電子機器）の変化

【主な要望事項】

- 「文書体裁が不整合なところがあり、統一化してほしい」
- 「ファスト・フォレンジックを新設してほしい」
- 「アウトソーシングサービス（Webサービスやクラウドサービス等）に関する記述が分散しており、一部重複しているので修正したほうがよい」

【参考】ファイルレス攻撃とは



* ***ドロッパー*** *：*
トロイの木馬の一種で、それ自体には不正コードが含まれないが、あるタイミングで不正コードを「投下」（＝ドロップ）する。

* ***ペイロード*** *：*
悪意のある動作をする部分のコードのこと。

* ***メモリ空間*** *：*
コンピューターのCPUがアクセスして、データの読み出しや書き込みができるメモリー領域。

【参考】重要インフラ事業者等における主なガイドライン

- サイバーセキュリティ経営ガイドライン（経産省）
- 組織における内部不正防止ガイドライン （IPA）
- 営業秘密管理指針及び関連するガイドライン（経産省）
- エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン（資源エネルギー庁）
- 電力制御システムサイバーセキュリティガイドライン（経産省）
- 鉄道分野のサイバーセキュリティ対策の手引（運輸総合研究所）
- 航空分野のサイバーセキュリティ対策の手引（運輸総合研究所）
- 医療情報システムの安全管理に関するガイドライン（厚労省）
- サイバーディフェンス連携協議会 インシデント対応連携に係るポリシー（防衛省）

トピック 3

第 6 版から第 7 版への主な改訂事項

想定読者である「ファースト・レスポンダ」の行動目的の追加

【第 6 版】

- インシデントの現場で最初に電磁的証拠の保全にあたる「ファースト・レスポンダ」 を主な対象としているが、これに限らず、デジタル・フォレンジック関連技術を運用する全ての者が利用可能なものである。

【第 7 版】

- インシデントが検知された或いは発覚した現場において、**即座に実施する被害拡大等のための対処やコンピュータ等を対象とした電磁的証拠の保全作業**にあたる「ファースト・レスポンダ」をはじめとした、デジタル・フォレンジック関連技術を活用する全ての方々が利用可能なものとしている。

「証跡とログ」に対する認識

【第 6 版】

（「証跡とログ」に対する認識に関する記述はなし）

【第 7 版】

- デジタル・フォレンジックへの関わり方やツールの機能等により、取得（抽出）及び分析（解析）の対象となる「証跡とログ」の概念や定義には明示的或いは暗黙的に違いがみられる。

用語の定義及び追加（１）

- インシデント
  - 情報の機密性、完全性又は可用性を毀損する行為やソフトウェアの脆弱性を攻略する行為や手段（Exploit）による侵害等、デジタル・フォレンジックの対象となる事案のこと。具体的には、コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等

- ファースト・レスポンダ
  - デジタル・フォレンジックに関する専門的な技能や豊富な知識を習得しているとは限らないが、専門事業者又は捜査機関に引き継ぐために証拠保全手続きを行う可能性 のある担当者

用語の定義及び追加（２）

- 証跡
  - コンピュータ・システムの仕様上、人や不正プログラムの操作により、ファイル／データ／ネット ワーク/内部等のさまざまな処理により必然的にディスクやメモリ上に残る痕跡のこと。英語圏における "Artifact"（Something observed in a scientific investigation or experiment that is not naturally present but occurs as a result of the preparative or investigative procedure3 ）の概念や定義に近い。
- ログ
  - ソフトウェア等の設計者、開発者、運用者等が特定の目的を持って、一定の出力形態により出力及び記録される情報のこと。英語圏における "Log"（An official record of events during the voyage of a ship or aircraft4 ）の概念や定義に近い。

用語の定義及び追加（３）

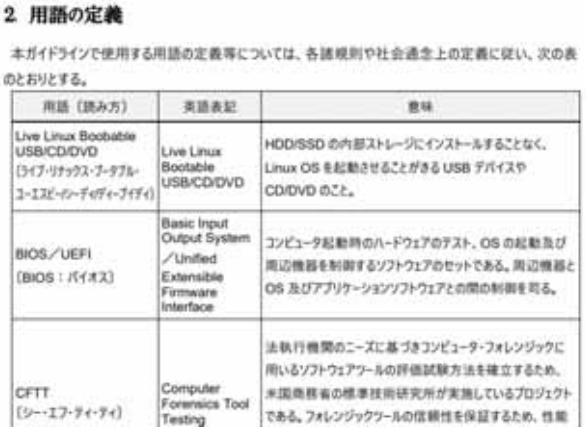
- 「用語の定義」を付録から本編に移動し、いくつかの用語を更新。

【第 6 版】

2　証拠保全ガイドライン用語集（Glossary）

用　語（読み方）	英語表記	意　味	本編頁
		【１】	
1CD－LINUX（ワン・シー・ディ・リナックス）	1CD LINUX	Linux ベースの LiveCD（CD から HDD/SSD にインストールすることなく、OS を起動させること）のこと。	20
		【Ｂ】	
BIOS／UEFI（BIOS：バイオス）	Basic Input Output System／Unified Extensible Firmware Interface	コンピュータ起動時のハードウェアのテスト、OS の起動及び周辺機器を制御するソフトウェアのセットである。周辺機器と OS 及びアプリケーションソフトウェアとの間の制御を司る。	24,27
		【Ｃ】	
CFTT（シー・エフ・ティ・ティ）	Computer Forensics Tool Testing	法執行機関のニーズに基づきコンピュータ・フォレンジックに用いるソフトウェアツールの評価試験方法を確立するため、米国商務省の標準技術研究所が実施しているプロジェクトである。フォレンジック・ツールの信頼性を保証するため、性能	27

【第 7 版】



2　用語の定義

本ガイドラインで使用する用語の定義等については、各諸規則や社会通念上の定義に従い、次の表のとおりとする。

用語（読み方）	英語表記	意味
Live Linux Bootable USB/CD/DVD（ライブ・リナックス・ブータブル・ユーエスビー／シーディ／ディーブイディ）	Live Linux Bootable USB/CD/DVD	HDD/SSD の内部ストレージにインストールすることなく、Linux OS を起動させることができる USB デバイスや CD/DVD のこと。
BIOS／UEFI（BIOS：バイオス）	Basic Input Output System／Unified Extensible Firmware Interface	コンピュータ起動時のハードウェアのテスト、OS の起動及び周辺機器を制御するソフトウェアのセットである。周辺機器と OS 及びアプリケーションソフトウェアとの間の制御を司る。
CFTT（シー・エフ・ティ・ティ）	Computer Forensics Tool Testing	法執行機関のニーズに基づきコンピュータ・フォレンジックに用いるソフトウェアツールの評価試験方法を確立するため、米国商務省の標準技術研究所が実施しているプロジェクトである。フォレンジックツールの信頼性を保証するため、性能

「リテラシー」の分かりやすさ

【第 6 版】

1.4　インシデントレスポンス時に使用する資機材等の熟達

① 証拠保全に利用するツール・ソフトウェア等の機能の熟知

② 証拠保全に利用するツール・ソフトウェア等を利用したシミュレーション等の実施

③ 証拠保全作業に関わる技術力の修得や知見の蓄積に必要なトレーニング等の実施

（考慮すべき事項）

・ 熟達のために専門家や経験者のサポートが必要なことがある場合、付録「８　ＩＤＦ団体会員「製品・サービス区分リスト」（全３８社）」で示しているフォレンジック事業者が提供する教育サービスを利用することが考えられる。

【第 7 版】

3-4. 資器材等の使いこなし

初動対応及び証拠保全のために使用する資器材等を使いこなせる状態にしておく。

- 証拠保全に利用するツール、ソフトウェア等の機能の熟知。
- 証拠保全に利用するツール、ソフトウェア等を利用したシミュレーション等の実施。
- 証拠保全作業に関わる技術力の修得や知見の蓄積に必要なトレーニング等の受講。

（考慮すべき事項）

専門家や経験者による支援が必要な場合は、付録「」．ＩＤＦ団体会員「製品・サービス区分リスト」（全４３社）」で示しているフォレンジック事業者が提供する教育サービスを利用することが考えられる。

TLP: GREEN

「対象物の種類」の更新

【第 6 版】

- 発生したインシデントに関する対象物の種類及び個数
  - コンピュータ（タブレット型／ノート型／デスクトップ型／サーバ型）
  - ネットワーク機器（ルータ、ファイアウォール、侵入検知システム（IDS）、侵入防止システム（IPS））
  - ハードディスクドライブ（以下、HDD／SSD）（バルク／外付け）
  - ストレージメディア（CD／DVD／FD／PD5 ／BD6 ／MO／各種フラッシュメモリ等）
  - より揮発性の高い対象物（メモリ）
  - 携帯電話、スマートフォン、タブレット端末・音楽プレイヤー
  - ゲーム機・IC レコーダ・ネット家電・Ｗｅｂカメラ、防犯カメラ
  - その他、証拠保全を円滑に行うための関連資料（例 ：周辺機器・接続構成図等）

【第 7 版】

- 発生したインシデントに関する対象物の種類及び個数
  - コンピュータ（タブレット型／ノート型／デスクトップ型／サーバ型）
  - ネットワーク機器（ルータ、ファイアウォール、侵入検知システム（IDS）、侵入防止システム（IPS））
  - ハードディスクドライブ（以下、HDD／SSD）（バルク／外付け）
  - ストレージメディア（CD／DVD／ブルーレイディスク（BD）／各種フラッシュメモリ等） - より揮発性の高い対象物（メモリ）
  - 携帯電話、スマートフォン、タブレット端末 - 音楽プレイヤー
  - ゲーム機器（ニンテンドー 3DS6 、プレイステーション 47 、プレイステーション Vita、Nintendo Switch、Xbox One 8 等）
  - IC レコーダ - ストリーミングデバイス（Chromecast9 、Fire TV Stick10 等）
  - スマートスピーカー、家電 IoT 等
  - その他、証拠保全を円滑に行うための関連資料（例：周辺機器・接続構成図等）

TLP: GREEN

「ネットワーク環境」の更新

【第 6 版】

- ネットワーク環境の確認
  - ISP、メールソフト、認証情報、電子メールアドレス、メール転送設定、ブラウザの種類、プロキシ設定等。

【第 7 版】

- ネットワーク環境の確認。
  - WiFi（無線 LAN）及び Bluetooth：設定情報等。
  - メールソフト：認証情報、電子メールアドレス、メール転送設定等。
  - ブラウザ：種類、バージョン、拡張機能（アドオン）、プロキシ設定等。
  - その他のアプリケーション：種類、バージョン、認証情報等。

「ファスト・フォレンジック」の項目追加

ファスト・フォレンジックによる証拠データ抽出

- 対象機器が多岐に渡り揮発性データに残る証拠データが多いと見込まれ、かつ速やかな実態解明や原因究明に偏ったフォレンジック調査が求められる場合、ファスト・フォレンジック（Fast Forensics）を実施することがある。

- ファスト・フォレンジックとは
  - 早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出及びコピーし、解析すること25 である。
  - このニーズの背景には、業務利用されるシステムやサイバー攻撃に利用されるマルウェアのネットワーク化（相互接続）、急増するファイルレス攻撃のメカニズム解明にあたりメモリ上の揮発性情報の取得及び保全の高まり、SSD搭載デバイスとディスクの大容量化等がある。
  - インシデント発生の現場におけるファースト・レスポンダは、一つのデバイスを深く調査する暇がなくなってきており、迅速な原因究明や侵入経路の特定をするために最低限のデータ抽出・解析をすることが求められてきている。
- ファスト・フォレンジックの実施
  - ファスト・フォレンジックにおいて抽出すべき主な証拠データについて、Windows OS の場合は、イベントログ、プリフェッチ、レジストリ、ジャーナル、メタデータ、インターネット（ブラウザによる閲覧履歴、メーラ等の設定及び送受データ）、メモリなどである。
  - これらの証拠データが消失する前に、発生現場におけるファースト・レスポンダが手作業のみで迅速かつ最大限に取得することは困難であるため、専門ツールを利用して実施する。
    ※ 専用ツールは、「H. 代表的な収集及び分析ツール」を参照

「アウトソーシングサービスの証拠保全」の項目追加

アウトソーシングサービスの証拠保全

- コンピュータ・システムに関するアウトソーシングサービスは、大きく分けてデータセンター（ハウジング）プロバイダ、レンタルサーバ（ホスティング）プロバイダ、クラウドプロバイダ、マネージドサービスプロバイダ（MSP）がある。
- 特に、クラウドプロバイダは、契約者に対して提供されるリソースの範囲によって区別があり、仮想化されたコンピュータ・システム基盤をインターネット経由で提供する IaaS（Infrastructure as a Service）、ソフトウェア基盤を提供する PaaS（Platform as a Service）、ソフトウェア部分を提供する SaaS（Software as a Service）等が存在する。機器の稼働状況を監視し、ソフトウェアを最新の状態に保ち、トラブル発生時の対応を請け負うマネージドサービスプロバイダ（MSP）のサービスを、データセンター（ハウジング）プロバイダやレンタルサーバ（ホスティング）プロバイダ等が付加サービスとして提供するケー スが散見されている。
- 最近では、CASB（Cloud Access Security Broker：キャスビー）と言われる、複数のクラウドサービスの 利用ユーザとクラウドプロバイダの間に配置し、単一のコントロールポイントにより、認証、シングルサインオン、アクセス制御、データ暗号化、ログ取得、マルウェア対策等、クラウドサービスへのアクセスに関するセキュリティ ポリシーを適用するサービス又は製品の導入が始まっている。

「民事訴訟におけるデジタル・フォレンジック活用」の主な手続きの追加

- ① 検証（民訴法 232 条）
  - 裁判官が感覚作用を使って事実の認定資料とする方法である。裁判官がコンピュータ自体やデータの状態を視覚等の作用によって心証を得るのがその例である。本案訴訟での正式な証拠調べを待っていたのでは、証拠の変更、改ざん、隠匿等のおそれがある 場合に、本案訴訟を提起する前に、検証等を実施することがあり、これを民訴法上の証拠保全という （民訴法 234 条）。
- ② 書証（民訴法 219 条）
  - 文書に記載された思想・認識を裁判所が事実認定に用いる方法である。専門業者が実施した デジタル・フォレンジック調査の経過や結果等をまとめた調査報告書がその例である。第三者が文書を所持する場合に裁判所にそれを送付させる送付嘱託（民訴法 226 条）もある。
  - 写真・ビデオテープは準文書として書証扱いとされるが（民訴法 231 条）、デジタルの電子媒体は、検証（民訴法 232 条）として扱われることがある。なお、文書は、その成立の真正が否定されると書証にすることができない（民訴法 228 条）。
- ③ 証人（民訴訟 190 条）
  - 証人尋問は、当事者（原告本人・被告本人）以外の者が過去に認識した事実を裁判所で供述し、その供述を事実認定の資料とする方法である。デジタル・フォレンジック調査を行った専門業者が法廷で 証言するのがその例である。
- ④ 鑑定（民訴法 212 条）
  - 特別の学識経験をもつ第三者に専門知識に基づく事実判断を裁判所に報告させる方法である。裁判官が専門業者を指名して、コンピュータやデータ等の解析を行わせそれを報告させる場合がその例で ある。
- ⑤ 調査嘱託（民訴訟 186 条）
  - 官公署、外国の官公署、学校等の団体に対して必要な調査を嘱託する方法がある。

トピック 4

今後について

今後について

- 今回の改定において反映できなかった事項について検討
  - 依頼を受けたレスポンダ（デジタル・フォレンジック技術者等）の力量と再依頼
    - 医療の例：「医師が力量や設備で十分な対応ができない場合、患者を直ちに高度医療機関に転送する法的義務がある。放置した場合、医師に責任が生じる。（最高裁平成15年11月11日）」
  - 保全前から保全後における原本（複製元）の管理及び返却
    - 第 6 版まで一切触れていない。現状、それぞれの専門家それぞれが原本の保全手続きを確立している。

- サイバー脅威（サイバー攻撃／サイバー犯罪）及び内部犯行の動向変化に伴う社会的要請に対する適応努力を継続

本資料に関する連絡先

名和 利男（Toshio NAWA）

SNS: about.nawa.to
PGP: 0xE38B4E01

TLP: GREEN