

「証拠保全ガイドライン 第 8 版」

2019 年 12 月 9 日

特定非営利活動法人デジタル・フォレンジック研究会
「証拠保全ガイドライン」改訂ワーキンググループ

(空白頁)

目 次

1. 本ガイドラインについて	1
1-1. 取り巻く環境の変化(状況認識)	1
1-2. デジタル・フォレンジックの状況	2
1-3. ねらいと方針	3
1-4. 想定読者.....	3
1-5. 留意事項.....	3
1-6. 謝辞.....	4
2. 用語の定義.....	5
3. インシデント発生前の準備	10
3-1. 活動プロセス及び体制の確立.....	10
3-2. 情報収集、情報共有及び分析	10
3-3. 資器材等の選定及び準備.....	11
3-4. 資器材等の使いこなし.....	12
4. インシデント発生直後の対応.....	13
4-1. 初動対応及び証拠保全が未実施の場合	13
4-2. 初動対応及び証拠保全が着手済みである場合	16
4-3. 初動対応及び証拠保全を円滑に進めるための活動	17
5. 対象物の収集・取得・保全.....	18
5-1. 対象物の状態の把握.....	18
5-2. 収集・取得・保全するための対象物の処置	18
5-3. その他、収集・取得・保全する必要性がある対象物	24
6. 証拠保全の機器	28
6-1. 複製先に用いる媒体(記憶装置)	28
6-2. 証拠保全機器に求められる機能.....	28
6-3. 証拠保全ツールに関する要件	30
6-4. その他、証拠保全に必要な機器・機材・施策の準備.....	31

7. 証拠保全の実施	33
7-1. 代替機・代替ツール・代替手段の準備.....	33
7-2. 立会人等.....	33
7-3. 同一性の検証	33
7-4. 証拠保全の正確性を担保する作業内容の記録	33
7-5. 複製先の取扱い	34
7-7. ネットワークログからの証拠データ抽出.....	35
7-8. ファスト・フォレンジックによる証拠データ抽出	37
8. アウトソーシングサービスの証拠保全	38
8-1. 事前に行う準備	38
8-2. インシデント発生直後の対応	38
8-3. 保全方法及び作業手順の検討.....	38
8-4. 証拠作業にあたっての留意点.....	39
8-5. アカウント所有者の同意	39
8-6. 収集・取得・保全	40
付録資料	41
A. チェックシート（PC の場合）.....	41
B. 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	43
C. デジタル・フォレンジック関連の資料紹介	54
D. Chain of Custody (CoC) シート例.....	55
E. 刑事・民事におけるデータ収集と解析フローイメージ図	57
F. 供述証拠と事実認定の実務(概論)	60
G. デジタルデータの証拠化・同一性確認調査手続き報告書例	64
H. 主要なデジタル・フォレンジック調査・解析用ツール(ソフト)	67
I. IDF団体会員「製品・サービス区分リスト」（掲載51社、会社名・URL掲載7社） ..80	
J. 「証拠保全ガイドライン」改訂WGメンバー(所属は 2019 年 12 月現在)	93

1. 本ガイドラインについて

1-1. 取り巻く環境の変化(状況認識)

社会が ICT¹ に深く依存するにつれ、個人や企業・組織間、国境を越えた主体間など、さまざまなレベルの紛争において、電磁的記録の証拠保全及び調査・分析を適切に行い、それぞれの主体における行動の正当性を積極的に検証するデジタル・フォレンジックの必要性・有用性が益々高まっている。また、サイバー攻撃やサイバー犯罪への対応の面でも、デジタル・フォレンジックが重要であることは言うまでもない。

また、民間企業における基幹業務のクラウド化がますます進展する一方、それらを標的としたサイバー攻撃の技術や手法が急激に高度化及び巧妙化しているため、コンピュータ・システムに残存する証跡やログに依存するデジタル・フォレンジックで実態を解明することが困難になるケースが相次いで発生している。そして、インターネットを積極的に利用したサービスやネットワークで繋がることを前提としたアプリケーションサービスや IoT²(特に機器自体に加えてネットワークプロトコル)を悪用したサイバー攻撃が増加傾向にあるため、連鎖的な被害を受ける範囲が拡大している。したがって、調査すべき対象が管理外のコンピュータ・システムや IoT に及ぶことになるため、自組織内で実態解明するには、インターネットとの境界周辺で「ネットワーク上のパケット通信の流れの記録として残されるさまざまなログ(以下、ネットワークログ)等」を集約及び分析することが一般的になってきた。

これに加えて、ここ数年のサイバー攻撃やサイバー犯罪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を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な少なくなってきた。例えば、高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃が急増しており、正規プログラムが残す証跡やログのみで悪意のある挙動を推し量ることが困難になっている。これを本格的に究明するには、電源供給を絶つと消失してしまう特性を持つ(揮発性が高い)メモリ空間に残存するスクリプト等を収集することが必要であるため、メモリ上の情報の保全の重要性がさらに高まってきている。

さらに、さまざまな産業領域における規制緩和や自由化により、付加価値の高いサービス提供、業務効率の向上そしてコストダウン等のために、サプライヤを通じた汎用技術や汎用製品の導入が積極的に行われていることから、クローズドな環境にある産業制御システムの領域においてもサイバー攻撃の発生懸念が高まっている。

特に、2020 年の東京オリンピック・パラリンピック競技大会を契機に、移動通信分野における 5G、放送分野における 4K/8K、製造産業分野における IoT 等が本格的に商用化するとみられているため、社会に深刻な影響を与えるインシデントの発生が予見されている。

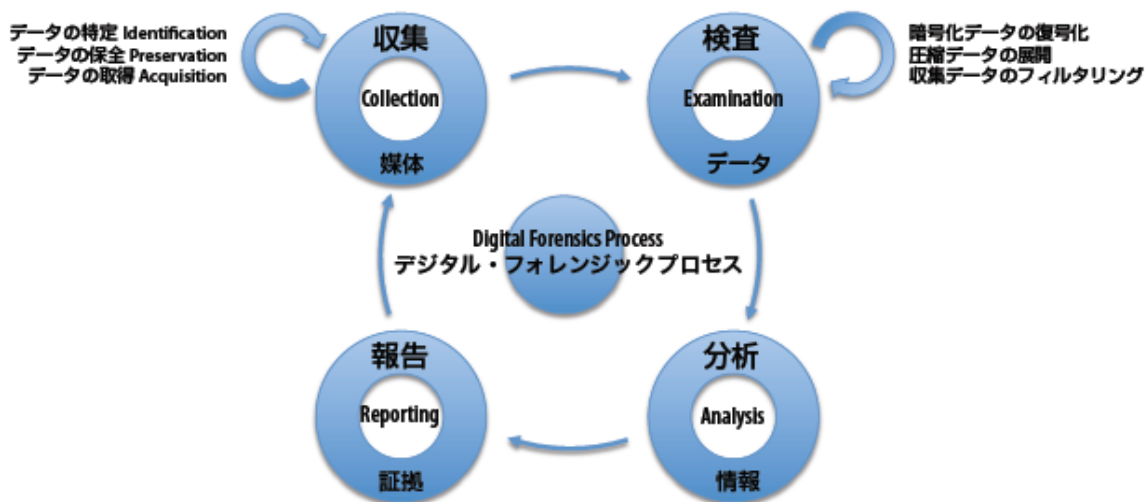
¹ ICT: Information and Communication Technology(情報通信技術)

² IoT: Internet of Things(モノのインターネット。あらゆるものがインターネットを通じて接続されて、モニタリングやコントロールを可能にする概念のこと。)

1-2. デジタル・フォレンジックの状況

デジタル・フォレンジックのプロセス全体像は、下図のように表すことができる。このプロセスの中で基本となるのは電磁的証拠の保全(Digital Evidence Preservation)の手続きである。事故や不正行為、犯罪といったインシデントに関わるデジタル機器に残されたデータの中から、電磁的証拠となり得るものを、確実に、そのまま(As-is)で、収集(Collection)・取得(Acquisition)し、保全(Preservation)しておくことは、デジタル・フォレンジックの運用者にとって最も重要なことである。

この手続きに不備があり、証拠の原本同一性に疑義が生じると、後の電磁的証拠の分析結果の信用性を失うため、これを行う者は非常に神経を使うことになる。



NIST SP800-86 (<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>) 等を参考に当研究会作成

この電磁的証拠の収集・取得・保全に関し、運用上の課題は「取得の対象となるデータはどの範囲であるべきか」、「保全した証拠の原本同一性の保証はどの程度確実にすべきか」の二つである。前者は、主に技術的及び時間的制約から、状況によっては全ての関連データの複製を取得することが現実的でない場合がある。後者も同様の制約から、取得したデータについては変更や改ざんがないという意味での原本同一性を当然確保するとしても、データ複製に関して完全に副作用(複製の過程で発生する僅かな状態変化等)のないデータ複製ができず、取得時に証拠の一部が破損又は紛失する可能性を覚悟しなければならない場合もあり得る。

このような状況に応じた「電磁的証拠の保全をどの範囲で、どこまで原本同一性を保ちつつ行うべきか」という課題に対し、諸外国ではさまざまな標準的手続きのガイドラインが作られており、これらを基準にして、電磁的証拠の保全に関する相場観が醸成されてきた。

これに対し、デジタル・フォレンジックの歴史が比較的浅い我が国においては、未だに広く認識された標準的な取得手続きのガイドラインが存在しないため、それぞれの運用者及び団体が自主的に作成したガイドラインや、海外のガイドラインを参考にしたものを中心に実運用がなされてきた。このような状況は、特に複数の組織が利害関係者となるような事案において、互いの持つ電磁的証拠の相互運用に対して障害となりかねない。

1-3. ねらいと方針

「証拠保全ガイドライン」(以下、「本ガイドライン」という。)は、デジタル・フォレンジック研究会として、我が国における同関連技術の普及を目指す立場から、上述した状況に首尾よく対処できる能力の底上げを図りつつ、我が国における電磁的証拠の保全手続きの参考として、さまざまな事案の特性を踏まえた知見やノウハウをまとめたものである。

特に、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、という運用現場の懸念や悩みに対し、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。

また、本ガイドラインの作成方針及び配慮した事項は、次のとおりである。

- 実際にデジタル・フォレンジック関連技術を実運用している企業からの参加を得て、現時点での我が国における同関連技術の運用状況と大きく乖離しないガイドラインとすること。
- 海外の関連ガイドライン等を参考にしながら、グローバルに活動する企業や組織にも利用できるように配慮しつつ、ノートパソコンや高機能携帯端末の普及率の高い我が国の独自性も反映させたガイドラインとすること。
- デジタル・フォレンジックの観点で基本的なネットワークログの収集と分析の在り方を追求すること。

1-4. 想定読者

インシデントが検知された又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・レスポンド」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。

本ガイドラインにおける「インシデント」及び「ファースト・レスポンド」の定義は、次のとおりである。

- 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)等を指す。
- ファースト・レスポンド:「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」としている。

1-5. 留意事項

本ガイドラインは、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はあるが、記述されている手続き等により収集・取得・保全等された電磁的

記録が裁判等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ことに留意していただく必要がある。

また、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「証拠とログ」の概念や定義には明示的又は暗黙的に違いがみられる。本ガイドラインの本編において使用している「証拠とログ」に対する認識は、次のとおりとする。

- 証拠: 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。

1-6. 謝辞

本ガイドラインの作成に際し精力的にご協力頂いた「デジタル・フォレンジック研究会『技術』分科会ガイドライン作成ワーキンググループ」のメンバー諸氏に、この場を借りて心から御礼申し上げます。

デジタル・フォレンジック研究会理事(「技術」分科会主査) 名和 利男

³ オックスフォード英語辞典における Artifact の定義

⁴ オックスフォード英語辞典における Log の定義

2. 用語の定義

本ガイドイラ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、次の表とのとおりとする。

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・ ユーエスピーシーディ/ディーブイ ディー〕	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、性能等を検証している。 その結果は公開され、ツールの開発や、民間活用に 供されている。
Cookie 〔クッキー〕	Cookie	ユーザ情報をブラウザ内に一時的に記録し参照する 機能のこと。書き込まれる情報には、サイトへの訪問 回数、ユーザ情報、パスワードなどがある。
DCO(装置構成オーバーレイ) 〔ディ・シー・オー〕	Device Configuration Overlay	ハードディスク装置の容量(例えば 80GB)を異なる容 量(例えば 60GB)に OS が認識するように設定するこ とができる機能であり、OS などがアクセス出来ない 領域が生ずる。
FAT32 〔FAT: ファット〕	File Allocation Table 32	Windows 95 OSR 2.0 以降や Windows 98/Me で利 用されるファイルシステム。ディスクを 2 の 32 乗の 小さな単位に分割して管理する。セクター サイズが 512 バイトの場合、最大 2TB までの領域を管理でき る。
HDD/SSD 全体暗号化 〔HDD: ハードディスクドライブ、 SSD: ソリッドストレートドライブ〕	Full Disk Encryption	ディスクドライブ装置等の暗号化機能で、書き込み時 には OS などを含め全て自動的に暗号化され、読出し 時には復号化される。

用語〔読み方〕	英語表記	意味
HDD/SSD パスワードロック 〔HDD:ハードディスクドライブ〕	HDD/SSD Password Lock	ハードディスク装置等のセキュリティ機能でユーザーパスワードを設定すると、電源再投入時に ロック状態となり、記録されているデータにアクセスするコマンドが実行不可となる。
HPA(ホスト保護領域) 〔エイチ・ピー・エイ〕	Host Protect Area/Hidden Protected Area	BIOS 及び OS から、容易にアクセス出来ない ハードディスク上の予約領域であり、ハードディスク装置のユーティリティや診断ツールに関わる情報などが記録される。
IDE 〔アイ・ディ・イー〕	Integrated Drive Electronics	パソコンでマザーボードと内蔵ハードディスクを接続するためのインターフェース。2 台のハードディスクが接続でき、それぞれプライマリー、セカンダリーと呼ばれる。現在 IDE と呼ばれているものは、もとの IDE を拡張した「E-IDE(Enhanced IDE)」という規格で、プライマリー、セカンダリーのそれぞれにマスター、スレーブと呼ばれる 2 台の機器を接続でき、計 4 台の機器が利用できる。
IEEE1667 〔IEEE:アイトリプルイー〕	IEEE 1667	IEEE が発行及び管理をしている「ポータブルストレージデバイスのホスト機器接続時認証に関する標準プロトコル("Standard Protocol for Authentication in Host Attachments of Transient Storage Devices")」という国際標準規格である。
MD5 〔エム・ディ・ファイブ〕	Message Digest Algorithm 5	1991 年に MIT の Ronald L. Rivest 教授により開発された。入力メッセージに対して 128 ビットのハッシュ値を生成するハッシュ関数である。
NTFS 〔エヌ・ティ・エフ・エス〕	NT File System	Windows NT 系(Windows NT/2000～Windows 10)の標準ファイルシステムのこと。複数ユーザがアクセスするサーバでの運用を想定した 設計である。
RAID 〔レイド〕	Redundant Arrays of Independent (Inexpensive) Disks	複数の外部記憶装置(ハードディスク等)をまとめて一台の装置として管理する技術。データを分散して記録することにより、高速化や耐障害性の 向上が図られる。専用のハードウェアを使う方法とソフトウェアで実現する方法がある。分散の方法により RAID 0 から RAID 6 まで 7 つの種類があり、それぞれ高速性や耐障害性が異なる。
RAID ボリューム	RAID Volume	複数のハードディスクを組み合わせ、外部記憶装置の管理単位である一つのボリュームとする。

用語〔読み方〕	英語表記	意味
SATA 〔シリアル・エイ・ティ・エイ／サタ／エス・アタ〕	Serial Advanced Technology Attachment	コンピュータとハードディスクや光学ドライブ等の記憶装置を接続するためのインターフェース規格のこと。従来の ATA 仕様の後継仕様で、2000 年 11 月に業界団体「Serial ATA Working Group」によって仕様の策定が行われた。 Ultra ATA 等の ATA 仕様で採用されていたパラレル転送方式をシリアル転送方式に変更したもの。これにより、SATA ではシンプルなケーブルで 高速な転送速度を実現できた。従来のパラレル方式の ATA 諸規格との互換性も持ち、従来は ドライブ毎に必要なだったジャンパーピン等の設定も SATA では不要になり、ハードディスク等を「接続すればすぐ使える」ようになる」とされている。
SHA-1 〔シャー・ワン／エス・エイチ・エイ・ワン〕	Secure Hash Algorithm 1	1995 年に米国国家安全保障局 (NSA: National Security Agency) がアルゴリズムを開発し、米国政府標準に採用されたハッシュ関数。ハッシュ値のビット長は 160 ビットである。
SHA-2 〔シャー・ツー／エス・エイチ・エイ・ツー〕	Secure Hash Algorithm 2	ハッシュ値がそれぞれ 224 ビット、256 ビット、384 ビット、512 ビットの SHA-224、SHA-256、SHA-384、SHA-512 を総称して SHA-2 と呼ぶ。
イベントログ	Event Logging	OS やアプリケーションが正常に動作しているかどうか、問題があるならば何が原因なのか、などの情報を記録したもの。Windows NT 系列の OS に備わっている。OS の稼働状況を記録する「システムログ」、アプリケーションの稼働状況を 記録する「アプリケーションログ」、ログオンや 警告設定の結果を記録する「セキュリティログ」等に分類されている。各ログは「警告」、「エラー」、「情報」の 3 つに分類されている。
イメージ取得／ イメージによる複製／ イメージコピー	Imaging	記録媒体に記録されている全てのビット列を 正確に複製すること。完全複製／物理複製とも言う。
イメージファイル	Image file	複製元の記録媒体に記録されているビット列を、フォレンジックツールで用いられているフォーマット形式 (例えば EnCase の E01 形式) を用いて、論理的な証拠ファイルとして複製先の記録媒体に複製・保存する。E01 形式では、一定の大きさに分割して複製される。
インシデント	Incident	情報の機密性、完全性又は可用性を侵害する 行為等、デジタル・フォレンジックの対象となる 事案。

用語〔読み方〕	英語表記	意味
書き込み防止	Write protection	完全複製等の際に原本となる記録媒体上の電磁的記録の毀損等を防止するため、当該記録媒体への書き込み信号を吸収し書き込みを防止すること。
監査証跡情報	Audit trail information	爾後の検証に備えて、対象事案、フォレンジック作業の管理者、フォレンジックの対象物及びフォレンジックツールを正確に記録しておくこと。
完全複製／物理複製	Duplicate	記録媒体に記録されている全てのビット列を正確に複写すること。
揮発性情報	Volatile Data	コンピュータのメインメモリ上のデータ等、電源が OFF になると保持されないものをいう。
クリッピング機能	Clipping	複製先ハードディスクの容量が複製元ハードディスクの容量よりも大きい場合、複製元と同容量のサイズまで認識させる機能。
行動履歴	Action history	IT 機器等の証拠物の収集、電磁的記録の取得、解析などのデジタル・フォレンジックの一連の処理に疑念を生じないよう、その作業状況をビデオ、写真及び筆記などにより記録すること。
サイバー攻撃	Cyber attack	コンピュータ・システムやインターネットを利用して、標的のコンピュータやネットワークに不正に侵入し、データの窃取、改ざん、破壊等を行い、システムを機能不全に陥らせる一連の行為。
最大許容停止時間 (MTPD)	Maximum Tolerable Period of Disruption	何らかの事象(例えば大規模震災)が発生した場合、システム(業務)が停止してから再開するまで、許容される最大時間のこと。この時間を越えると、ビジネスへの影響が大きく、BCP の観点から限界と判断される停止時間を指し、ビジネス影響度分析において検討される指標である。
作業ログ	Work log	フォレンジックツールへのコマンド入力及び設定情報並びに出力されたハッシュ値など、フォレンジック作業の正確性を検証できるように作業過程が記録された情報。
システム時計	System Clock	コンピュータに内蔵されている時計で、OS が管理している。

用語〔読み方〕	英語表記	意味
ジャンパーピン	Jumper Pin	マザーボードや拡張カード上に用意されている金属のピンのこと。
収集	Collection	電磁的証拠が蓄積されていると思料される IT 機器等を特定し証拠物として押収すること。又は証拠調べの対象として確保すること。
取得	Acquisition	電磁的証拠を物理複製、論理複製又はイメージ取得すること。
証拠	Evidence	本ガイドラインにおいて「証拠」とは、裁判で証明が必要な事実を立証するための電磁的記録をいう。
証拠保全	Preservation of evidence	収集した IT 機器等の証拠物の電氣的及び物理的な安全性を確保するとともに、取得した電磁的証拠の毀損又は滅失を防ぐため、適性に保存し管理すること。
証拠保全の一貫性	Chain of Custody	証拠物の保管、出納に関しては、記録をとり、管理を適正に行うことが求められる。犯罪捜査規範第 117 条では、「事件の捜査が長期にわたる場合においては、領置物は証拠物件保存簿に記載して、その出納を明確にしておかなければならない」と規定している。

3. インシデント発生前の準備

初動対応及び証拠保全を実施可能な状態にしておかなければ、インシデント発生後に期待される活動ができなくなる可能性が高い。そのため、インシデントが発生する前の段階で、組織のセキュリティポリシーや IT 環境などの状況を考慮した準備をしておく必要がある。

3-1. 活動プロセス及び体制の確立

初動対応及び証拠保全を実施可能な活動プロセス及び体制を確立する。

- 初動対応及び証拠保全において優先されるべきもの(サービス、システム等)の順位の検討及び決定。
- インシデント発生時の初動対応及び証拠保全時に必要と考えられる資機材等の選定と確保。
- システムにおける最大許容停止時間(MTPD)、目標復旧時間(RTO)等の確認。
- インシデントの検出、判断方法の確認。
- インシデント発生時の連絡体制の確認。
- インシデント発生時の調査(原因の究明、被害範囲の特定)方法等の例示。
- インシデントに備えたバックアップ、リストア体制の確立及びテスト。

《考慮すべき事項》

バックアップやリストアに想定以上に時間がかかる、又はバックアップデータの真正性が損なわれてしまう場合があるので留意する必要がある。

- 初動対応及び証拠保全経緯(時系列)の記録方法の確立。
- 初動対応及び証拠保全の手順書の作成。

《考慮すべき事項》

初動対応に関わる部署との協力体制が、人事異動等により機能しなくなる場合があることに留意する必要がある。一定ベルの教育訓練を受けることで実施可能な作業の流れや詳細を記述した指示書である SOP (標準作業手順書)の作成が考えられる。

3-2. 情報収集、情報共有及び分析

初動対応及び証拠保全に関連する情報収集、情報共有及び分析を行うことが可能な体制及び実務能力を獲得する。

- 多様化かつ高度化するインシデントに対して、迅速かつ的確に対応するための関連ニュースや技術情報等の収集及び分析。
- 揮発性情報の取得手順・内容及び範囲(メモリダンプ、アプリケーション関連情報)の明確化及び文書化。

- 初動対応及び証拠保全に関連する外部組織や他部門等との情報共有並びに相互連携の確立。

3-3. 資器材等の選定及び準備

初動対応及び証拠保全において、必要と考えられる資器材等を選定及び準備する。

- 証拠保全時における IT 機器等の保管に使用する梱包材の準備
 - ダンボール、緩衝材、帯電防止袋等。
- 工具等の準備
 - 精密ドライバ、荷札、各種テープ、帯電防止用手袋、テーブルタップ等。
- 初動対応及び証拠保全に必要なコンピュータ、印字装置等の準備
 - ノートパソコン、プリンタ、外部記録装置(主に USB メモリ)、光学ドライブ(主に DVD-R や CD-R)等。
- 初動対応及び証拠保全に必要なツール、ソフトウェアの選定及び準備。
 - 揮発性情報等収集ツール、可視化用ソフトウェア等。

《考慮すべき事項》

情報の取得過程において、オリジナルのデータを極力変更しないこと、極力(原本への)書込みを発生しないこと、不要なネットワーク通信が発生しないこと。

(詳しくは、「6-3. 証拠保全ツールに関する要件」及び「付録資料 D. Chain of Custody (CoC) シート例」を参照)

また、外部 OS 起動用ディスク等を準備しておくことが望ましい。

- フォーマット済みのクリーンな媒体の準備
 - 大容量記憶装置(ハードディスク、SSD 等)、DVD-R や CD-R 等の各種メディア。
- 証拠保全用複製装置の準備
 - 明示的にフォーマット済みのクリーンな媒体へ証拠保全が可能な複製装置。
- カメラ、筆記用具等の準備
 - カメラやビデオカメラ(スマートフォン等で代替えることも可能)、作業確認チェックシート、一貫性追跡記録(CoC)、備忘録用紙、ボールペン等。

《考慮すべき事項》

ボールペンは、記述事項の改ざん防止をすることを期待しているため、消えるボールペン(フリクション⁵ 等)の使用は避けること。

⁵ 「フリクション」は、株式会社パイロットコーポレーションの登録商標です。

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。

《考慮すべき事項》

証拠保全に利用する代表的なツール、ソフトウェアは、次の種類に分けることができる。

- ・ システム関連の情報取得ツール
- ・ 揮発性メモリの情報取得及び解析ツール
- ・ スマートフォンのデータ取得ツール
- ・ クラウド関連の保全ツール

(詳しくは、「付録資料H. 代表的な収集及び分析ツール」を参照)

- 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、「付録資料J. 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。

4. インシデント発生直後の対応

インシデントの検知又は発覚(発生していたことが明らかになった)した直後の初動対応及び証拠保全を適切かつ円滑に実施するため、次のような事項を実施する必要となる。

4-1. 初動対応及び証拠保全が未実施の場合

4-1-1. 発生したインシデントの積極的な把握

(種類)

- 情報流出、データ破壊
- 不正プログラム(マルウェア、悪意のあるスクリプト等)の実行
- 不正アクセス・不許可の持ち出し、コンプライアンス違反
- 設定ミス、操作ミス、物理的故障
- システム悪用、破壊行為、内部犯行

(検知又は発覚のきっかけ)

- ログのレビュー・監視
- 不正検知システム
- 内部通報
- 異常事象の発見・認知
- 外部からの通報

(発生時刻)

- システム時計の正確性の確認(OS のシステムクロック及びハードウェアクロック)

(初動対応の開始までの記録)

発生したインシデントの検知又は発覚から報告又は対応依頼の連絡までの時間及びその間のインシデントに対する対応の有無について記録をとる。

- 発生したインシデントを知る人物及び人数
- インシデントの対象物の確保の有無
 - 確保していた場合：対象物を確保した日時、確保した人物(役職)、確保した場所、確保時の対象物(及びその周辺)に対する行為、確保後の対象物に対する対応(の有無)とその内容を記録する。

《考慮すべき事項》

可能な限り、関係者(当事者)から、対象物を任意に提出することに同意する旨の書面を受領しておく。

- 確保していない場合：対象物を確保する(予定の)日時と場所、確保時の対象物(及びその周辺)の状態を詳細に記録する。

4-1-2. 発生したインシデントに関する対象物の決定(流れ図は図1参照)

(対象物に対する情報収集及び対象物の絞り込み)

- 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／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 OneTM 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)

《考慮すべき事項》

クラウドサービス上のデータが対象である場合は、¹⁸「アウトソーシングサービスの証拠保全」を参照のこと。

- 発生したインシデントに関する対象物の状態(いつ、どこに存在していたか等)
- 発生したインシデントに関する対象物の使い始めと終わり及び使用頻度
- 発生したインシデントに関する対象物の使用者及び管理者

⁶ 「ニンテンドー DS」及び「Nintendo Switch」は、任天堂株式会社の登録商標です。

⁷ 「プレイステーション Vita」は、株式会社ソニー・コンピュータエンタテインメントの登録商標です。

⁸ 「Xbox OneTM」は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

⁹ 「Chromecast」は、Google Inc.の商標または登録商標です。

¹⁰ 「Fire TV Stick」は、Amazon.com、Inc.の商標または登録商標です。

- 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器及びドキュメントの有無

(対象物の選定と優先順位付け)

- 保全を行う前の対象物(デバイス)の選定とその理由
- (対象物が複数ある場合)取り扱う対象物の優先順位及びその理由

4-1-3. 証拠保全を行う上で必要な情報の収集

(対象物の情報)

- 対象物の形状、個数、物理的な状態
 - 対象物のラベル情報(メーカー／型番／モデル名／シリアルナンバー／セクターサイズ／総セクター数／記憶容量)、ケーブルの接続状況、ジャンパーの設定状況、HPA¹¹・DCO¹²の設定の有無等、通常環境下で視認可能な物理的破損・損傷の有無

《考慮すべき事項》

HPA・DCOの設定の有無により、メディアの可読領域が異なる可能性があるため、証拠を取得した際の設定を記録しておく必要がある。

- HDD／SSD・ストレージメディアの記憶容量、インターフェースの状況
 - 特に、HDD／SSDを筐体から取り出せず、外部OS起動用ディスク等で証拠保全を行う場合、光ディスクのドライブ及びUSB/Thunderbolt¹³、ネットワーク接続ポートの存在の有無が重要
- セキュリティ設定の有無
 - HDD／SSDパスワードロック、HDD／SSD全体暗号化又は一部のファイル・フォルダの暗号化、PC周辺のワイヤストッパー、ロッカー、ICカード等

《考慮すべき事項》

HDD/SSDの暗号化が不明の場合、Encrypted Disk Detector¹⁴等のツールでチェックすることができる。また、Bitlockerドライブが復号されて閲覧可能の場合、管理者権限で次を実行すると、回復キーを取得することができる¹⁵。

```
manage-bde -protectors -get c:
```

¹¹ HPA: Host Protected Area 又は Hidden Protected Area。ホスト保護領域。

¹² DCO: Device Configuration Overlay。装置構成オーバーレイ。

¹³ Thunderbolt: パソコンと周辺機器を接続するためのシリアスバス規格の一つ。

¹⁴ Encrypted Disk Detector
<https://www.magnetforensics.com/resources/encrypted-disk-detector/>

¹⁵ Query Your BitLocker ID and Password <https://blogs.msdn.microsoft.com/rob/2013/02/10/query-your-bitlocker-id-and-password/>

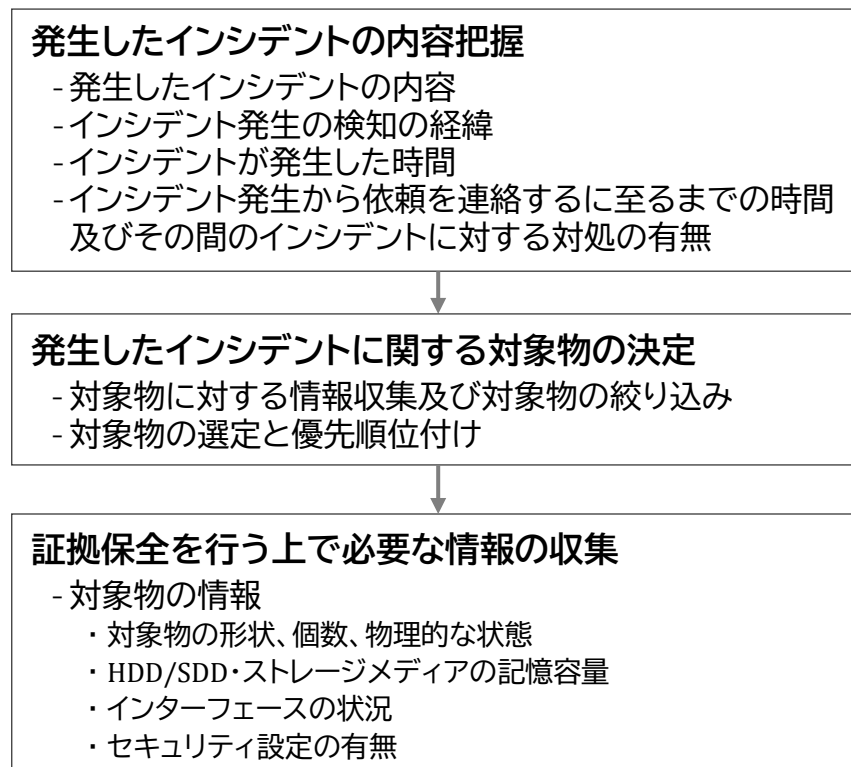


図 1 本節の作業内容を示すフローチャート

4-2. 初動対応及び証拠保全が着手済みである場合

4-2-1. 上記項目 3.1 に関する各種情報の確認

対象物の選定及び情報の収集が完了している場合、それらを次の観点で確認する。

- 「3-1. 活動プロセス及び体制の確立」に関する各種情報の過不足等の有無。
- 「3-1. 活動プロセス及び体制の確立」に関する各種情報の収集の工程及び結果を承認する人物の存在又は承認の有無。

4.2.2 発生直後の初動対応及び証拠保全の実施内容の聴取

- 発生したインシデントに対して実施された初動対応又は証拠保全について、可能な限り 5W1H で聴取。
- 聴取は、初動対応又は証拠保全を実施した者に加えて、それを観察又は監督した者も対しても実施。

4.2.3 対応に過不足が確認された場合の対処

- 収集又は聴取した情報・項目内に、不足している箇所が確認された場合、その情報を補充するための追加的に情報収集又は聴取。

- 収集又は聴取した情報・項目内に、不適切な手続きによって取得された箇所が確認された場合、収集時に実施した作業内容を記録した上で、適切な手続きに基づいて速やかに該当箇所を精査。
- 収集した情報・項目内に、余分な箇所が確認された場合、その情報を収集した基準及び理由について聴取し、不必要と合理的に判断された場合は削除。

4-3. 初動対応及び証拠保全を円滑に進めるための活動

4-3-1. 物理的環境の確保

- 証拠保全の対象物や、証拠保全に用いる機器・ツール・書類が、見やすくかつ管理しやすい程度の広さを有する場所の確保。
- 証拠保全に用いる機器・ツールが十分に稼働するための電力及びプラグ等の確保。
- 初動対応及び証拠保全の作業のみを行えるための場所の確保。
 - 施錠等により初動対応及び証拠保全に関わる人物のみ立ち入り可能な場所の確保(指紋認証・ICカード認証等による入退出管理がより望ましい)。
- 休憩等、初動対応及び証拠保全の作業中に現場を離れる際に必要な施策の実施
 - 作業者の入退室記録、ゲスト用 IC カードの貸与等。

4-3-2 関係組織との連携

- CSIRT／SOC 担当者、法務部門担当者、システム担当者等との連携。
- システム設計者又は管理者との関係構築。
 - 例：構成が複雑なシステム全体ないしその一部の証拠保全を行う際等。
- 内部監査・システム監査担当者との連携。
 - 依頼元組織内のセキュリティやプライバシー施策を十分に考慮・遵守。
- 関係者の確保及び無関係者の排除。
 - 初動対応及び証拠保全の作業工程において、関係ない第三者が関与できない状況を確認。
 - オンサイトで作業を行う場合は、依頼元の担当者が常駐するように心がける。
- 解析担当者との連携。

5. 対象物の収集・取得・保全

5-1. 対象物の状態の把握

5-1-1. 対象物が存在する現場での、収集・取得・保全時の状況把握

- 対象物が置かれている場所、状態。
- 管理者による意図的な隠蔽等の有無の確認。
 - 例: 想定される対象物の置き方、収納方法が不自然な状況であると判断した場合、その状況下となった背景と理由及びその状況下となった経緯と時間・人物についてインタビューする。

5-1-2. 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)の拡大又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する必要があるが見られない場合、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。

5-2. 収集・取得・保全するための対象物の処置

対象物の状態によって、次(図 2)のような客観的かつ合理的な処置を選択する。

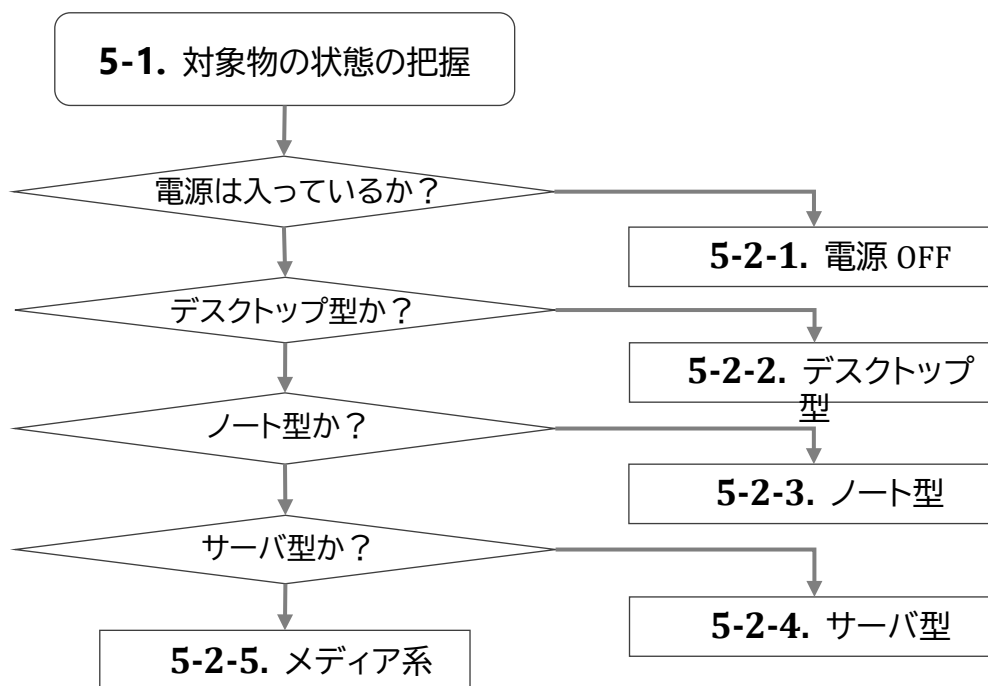


図 2 主な収集・取得・保全するための対象物の処置の選択

5-2-1. 対象物がコンピュータで、電源が **OFF** の状態の場合

- 原則として電源を ON にしてはならない。
 - HDD／SSD 全体暗号化等、やむを得ず電源を ON にしなければ証拠保全ができない場合を除く。ただし、その場合も証拠保全作業の責任者の指揮の下、電源を ON にした時のリスク(ファイルのタイムスタンプや内容の変更などの影響)を受容して、証拠保全作業を実施する。
 - ファームウェアのマルウェア感染や意図的な改ざんが行われる可能性がある場合は、電源を ON にするとインシデントが深刻化する場合がある。
- 無為に HDD／SSD にデータの書き込み等が発生しないように、ケーブル類は全て筐体から取り外す。
 - 電源ケーブル、キーボード・マウス、USB 系のコネクタ類を取り外す。
 - 用途不明の接続ケーブルの場合は、その接続ケーブルについて熟知している人物に用途等を確認し、証拠保全作業の責任者の指揮の下、作業を行う。
 - 各装置・ケーブルの取り外しの際は、解析時におけるシステムの正確な再現、作業後の現状復帰を可能にするため、どのケーブルや機器が、どこに取り付けられていたかを、粘着性の低いタグ、専用の荷札タグ等を貼って明確にする(記録シートに明記／写真撮影等。図 3)。特に証拠保全対象となる機器の固有情報(製造番号、型式等)は確実に記録する。

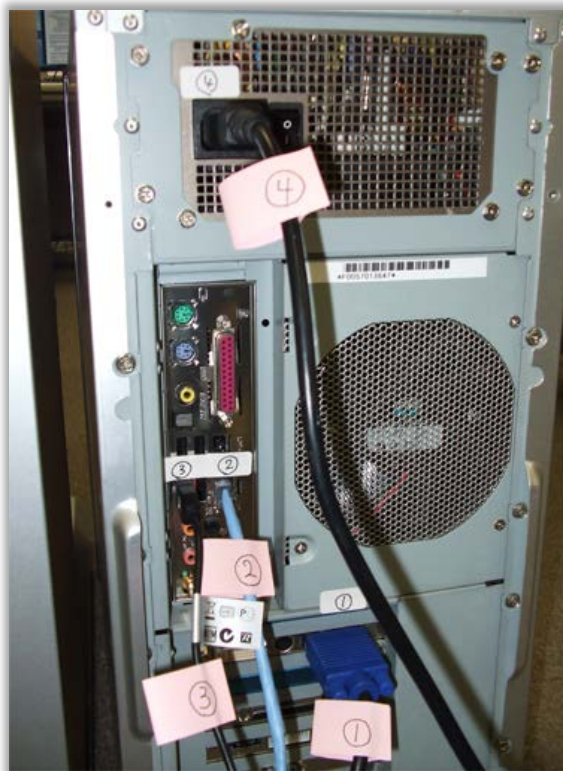


図 3 ケーブル等へのラベル貼付状況の記録

5-2-2. 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

- コンピュータの種類・規格、使用 OS の確認及び確保時点でのシステム時計の正確性(日本標準時等との差異)を目視又はコマンドで確認・記録。
- 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。
- 対象物確保時に、画面やプリンタ等、出力装置に表示又は出力されていた状況を具体的に記録(写真撮影等)。
 - やむを得ない場合を除き、ファイルやアイコン、その他の不審な画面の動き等に極力触れてはならない。
 - 可能であれば、バックグラウンドで稼働していたプロセス等も併せて確認する。
- 揮発性情報の取得。
 - 調査の目的、必要に応じて、揮発性情報を取得する。

《考慮すべき事項》

揮発性情報を取得せず電源ケーブルを抜く場合は、HDD／SSD 上の一部データ消失のリスクより、事実解明が困難になるリスクが高くなる傾向がある。

- やむを得ない場合を除き、ファイルやアイコン、その他の不審な画面の動き等に極力触れてはならない。
- 揮発性情報の取得手順・内容と範囲(メモリダンプ、アプリケーション関連情報)については、事前に準備した、使用 OS に対応する自動収集ツール等を使用し、手順に従って対象範囲を取得する。
- 電源を OFF にする。
 - 例:4.2.6 参照。
- 無為に HDD／SSD にデータの書き込み等が発生しないように、ケーブル類は全て筐体から取り外す。
 - 電源ケーブル、キーボード・マウス、USB 系のコネクタ類を取り外す。
 - WiFi(無線 LAN)及び Bluetooth の機能を停止する。
 - 用途不明の接続ケーブルの場合は、その接続ケーブルについて熟知している人物に用途等を確認し、証拠保全作業の責任者の指揮の下、作業を行う。
- 各装置・ケーブルの取外しの際は、解析時におけるシステムの正確な再現、作業後の現状復帰を可能にするため、どのケーブルや機器が、どこに取り付けられていたかを、粘着性の低

いタグ、専用の荷札タグ等を貼って明確にする(記録シートに明記／写真撮影等)。特に証拠保全対象となる機器の固有情報(製造番号、型式等)は確実に記録する。

5-2-3. 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

- コンピュータの種類・規格、使用 OS の確認及び確保時点でのシステム時計の正確性(日本標準時等との差異)を目視又はコマンドで確認・記録。
- 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。
- 対象物確保時、画面やプリンタ等、出力装置に表示又は出力されていた状況を具体的に記録(写真撮影等)。
 - やむを得ない場合を除き、ファイルやアイコン、その他の不審な画面の動き等に極力触れてはならない。
 - 可能であれば、バックグラウンドで稼働していたプロセス等も併せて確認する。
- 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。
 - やむを得ない場合を除き、アイコン、その他の不審な画面の動き等に極力触れてはならない。
- 電源を OFF にする。
 - 電源ケーブル、キーボード・マウス、USB デバイス系のコネクタ類を取り外す。

《考慮すべき事項》

Fast Boot になっている場合、「Windows の設定」の UEFI 設定で無効にする。また、「4-1-3. 証拠保全を行う上で必要な情報の収集 - セキュリティ設定の有無」を参照。

- 5.2.6 参照。
- デスクトップ型と異なり、ラップトップ型は筐体底面にバッテリーパックがある為、プラグをコンセントから抜いても強制的な電源 OFF にはならない、或いは開いただけで自動的に電源が ON になるものがある。
- そのため、筐体底面のバッテリーパックを取り外した後、プラグをコンセントから抜くことで、電源を強制的に OFF にする。バッテリーパックが外せない場合、電源ボタンの長押しで電源を OFF にする。

5-2-4. 対象物がコンピュータ(サーバ型)で、電源が ON の状態の場合

- サーバ型では、RAID¹⁶ 装置が利用されていることが多々ある。RAID 装置に組み込まれている HDD/SSD のコピーを証拠保全機器で別の HDD に物理コピーしたとしても、元の RAID 装置を使わないと、物理的な仕様の変化等により再構成(原状復旧)が困難な場合がある。
- RAID 装置を別の OS(Live Linux Bootable USB/CD/DVD¹⁷ 等)で起動し、RAID 上で構成されている論理ボリューム単位等で取得することで、RAID ボリュームの再構成が可能。
- RAID 装置を一式持ち帰ることが可能な場合もあるが、会社の業務用サーバ等で利用している場合、RAID 装置の使用有無にかかわらず、サーバの停止が困難である可能性が高い。この場合、業務に大きな影響を与えない範囲で、時間はかかるがイメージ取得を実施する。

5-2-5. 対象物がコンピュータ以外(メディア系)の場合

(外部メディア等の物理的管理と記録)

- 収集・取得・保全する外部メディアの誤廃棄及び紛失等を防止するため、識別目的の札を付ける等、確実な識別及び管理を行う。
- 付けた札には、収集・取得・保全の日時、場所、所有者(又は管理主体)、使用用途、状況、収集・取得・保全に至った経緯及び目的等を記録する。

(外部メディアにアクセスする PC 等の特定)

- IEEE1667¹⁸ 規格や特定ソフトウェアを利用して、デバイスのロック機能を USB メモリに組み込み、接続時に認証(パスワードの入力等)に成功しないと外部メディア内のデータにアクセスできないような設定も考えられるため、外部メディア内のデータにアクセスしていた PC 等を特定する。

(使用されているファイルシステムの特定)

- 外部メディアに使用されているファイルシステムを特定する。

5-2-6. 電源を OFF にする際の注意点

- 感電や帯電を防止するため、貴金属は身につけず、帯電防止用手袋を装着して作業を実施する。
- HDD/SSD 暗号化(例:BitLocker)当のセキュリティ設定や起動を高速化する機能(例:Fast Boot)が、電源 OFF 後の証拠保全を困難にさせることがあることを認識する。

¹⁶ RAID: Redundant Arrays of Inexpensive Disks

¹⁷ 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、直接 Linux OS を起動することができる USB デバイスや CD/DVD。

¹⁸ IEEE1667: ポータブルストレージデバイスの、ホスト機器接続時認証に関する標準プロトコル。

《考慮すべき事項》

「4-1-3. 証拠保全を行う上で必要な情報の収集 - セキュリティ設定の有無」を参照。

- 強制的に電源を OFF にする場合。
 - サーバ系 OS や会計システム等のデータベースが稼働しているデスクトップ型 PC は、原則として、データベースのトランザクション機能を頼りに強制的に電源を OFF にすることも可能である。
 - 想定されるリスクの例：
 - ◇ HDD／SSD に物理的な損傷(不良セクター)が生じやすい。
 - ◇ データ又はファイルが破損し、読み取れなくなる危険性がある。
 - ◇ 稼働中だったプロセスがレジストリやイベントログに書き込まれず、直前の行動が把握できない可能性がある。
 - ◇ 揮発性情報が取得できない。
- 通常のプロセスで電源を OFF にする場合。
 - 想定されるリスクの例：
 - ◇ HDD／SSD に物理的な損傷(不良セクター)が生じやすい。
 - ◇ 揮発性情報が取得できない。

5-2-7. 電源を OFF にしてはならない場合等

- 証拠保全の対象によっては、電源を OFF にしてはならない場合が存在する。
 - メモリに展開中のデータを証拠保全する場合。
 - 通信中のデータの証拠保全。
 - HDD／SSD 全体暗号化等のセキュリティが設定されている場合。(一旦電源を OFF にした後、再度電源を ON にしなければならず、余計なデータの上書き等が発生してしまうため。)
 - 携帯電話、携帯通信機、家電製品、ゲーム機等も、調査の目的、必要に応じて、電源が ON の状態であれば OFF にしてはならない場合がある。携帯電話の機種によっては、電源を OFF にすることで、データの上書きや削除が発生することを考慮する。
- このような機器は、電源を ON にしないと証拠保全ができないため、証拠保全時は電源を ON にする必要がある。

《考慮すべき事項》

一部の携帯電話は、通信が ON になった時点で、遠隔地から削除される仕組みを搭載しているものがある。

5-2-8. 揮発性による処理順序

- ・ 証拠保全においては、揮発性の高い情報から順に処理する。(表1参照)

表 1 証拠収集における揮発性と順序

揮発性:高 ↓ 揮発性:低	レジスタ、キャッシュ
	ルーティングテーブル ¹⁹ 、ARP キャッシュ、プロセステーブル、カーネル統計、メモリ ²⁰
	テンポラリファイルシステム ²¹
	ディスク
	当該システムと関連する遠隔ロギングと監視データ
	物理的設定、ネットワークポロジ
	アーカイブ用メディア

出典:IPA による RFC3227 の日本語訳「証拠収集とアーカイビングのためのガイドライン」
<http://www.ipa.go.jp/security/rfc/RFC3227JA.html>

5-3. その他、収集・取得・保全する必要性がある対象物

5-3-1. サーバ及び通信・監視装置のネットワークログ

国内で多く見られるネットワークシステムをベースに考えると、収集すべきネットワークログは、「セキュリティ対策で利用されるネットワーク機器」、「サーバや PC 上にインストールされているオペレーティング・システム」、そして「Web やメール等のアプリケーション」に大別して考えることができる。

- ・ 「セキュリティ対策で利用される通信・監視装置」で取得すべきネットワークログ
 - プロキシサーバ
外部の Web サイトにアクセスする全ての URL の記録が得られる。
 - IDS 及び IPS
疑わしい挙動や進行しつつある悪質な活動を検知又は防止する措置に関する記録が得られる。但し、予め設定されたルールセットに基づく措置であるため、想定しない未知の挙動等の場合は措置されないことに留意すべきである。
 - ウイルス対策ソフトウェア
マルウェアが侵入又は動作に成功した記録が得られる。但し、全てのマルウェアの存在や活動を検知するものでないことに留意すべきである。

¹⁹ ルーティングテーブル:パケットの配送先に関する経路情報

²⁰ メモリ:コンピュータのメインメモリ(RAM)

²¹ テンポラリファイルシステム:仮想メモリに全ファイルを保持するファイルシステム(TMP FS 等)

- リモートアクセスのソフトウェア
VPN ソフトウェアにより、接続が確立された日時やログインユーザ毎のセッションで送受されたデータ量の記録が得られる。ソフトウェアによっては、リソースの使用状況に関する情報も記録できるものもある。
- 脆弱性管理ソフトウェア
管理対象のサーバのパッチのインストール履歴や脆弱性の有無に関する記録が得られる。
- 認証サーバ(特に、Active Directory のイベントログ)
認証時のアクセス元アドレス、ユーザ名、認証可否、日時の記録が得られる。

《考慮すべき事項》

- ・ Active Directory に対する不正行為は、既存の正規アカウントの悪用が目立ってきているため、日頃から通常時の状況を把握し、異常と推定されるログを見つけやすくしておく必要がある。
- ・ セキュリティ情報が一元管理されているシステム(SIEM 等)の利用や、膨大なイベントログの解析可能な状態にしておくことを推奨する。

- ルータ(特に、Wi-Fi ルータ)
アクセスリスト、および不正に変更された IP ルーティングやスタートアップコンフィグ等の情報が得られる。

《考慮すべき事項》

- ・ ルータのログは、内部バッファが一杯になると古いメッセージから上書きされるため、必要な証拠が得られない状況に陥ることがある。
- ・ 組織規模に関係なく、ルータのログを Syslog サーバ²³ に転送することを推奨する。

- ファイアウォール
設定したポリシーによって発生する実行ログが得られる。
- 検疫システム
検疫(チェック)したコンピュータ・システムの実行記録と検査結果の記録が得られる。
- PC やサーバ上にインストールされている「オペレーティング・システム」で取得すべきネットワークログ
- システムイベント
それぞれのイベントについて記録される情報は異なるが、一般には、イベント毎のタイ

²³ Syslog サーバとは、ログを受信して記録するシステムのこと。プロトコルは RFC5424 として標準化されている。

ムスタンプ、イベントコード、ステータスコード、エラーコード、サービス名、ユーザ名等の記録が得られる。

- 監査記録
認証の成否、ファイルアクセス、セキュリティポリシーの変更、アカウントの変更、権限実行、イベントの種類、操作結果等の記録が得られる。
- メールサーバやそれにアクセスするメール、Web サーバとそれを閲覧するブラウザ、ファイル共有サーバやデータベースサーバとそれらのクライアントソフト、経理システムや ERP(業務統合パッケージ)等の「業務用アプリケーション」から取得すべきネットワークログ
 - クライアントからのアクセスに対するサーバの応答
例えば、メールサーバの場合は送信元／宛先／件名／添付ファイル名等、Web サーバの場合はアクセス元／応答結果等、業務アプリケーションの場合はユーザ名／アクセス先リソース／ログイン・ログアウト時刻等
 - アカウントに関する情報
認証及びその試行回数、アカウント作成／変更／削除、利用した権限、リソースの使用時間等
 - 使用状況に関する情報
トランザクションの件数や一定時間内の頻度、トランザクションのサイズ等

5-3-2. 対象物のマニュアル・ユーザガイド等のドキュメント類

- 証拠保全作業に必要となる下記のような情報を探す。
 - HDD／SSD の取り外し方
 - バッテリーの取り外し方
 - BIOS／UEFI の起動方法と画面の見方(主な BIOS 起動キーは表 2 参照)
 - Web 等で上記の手法を確認
- 依頼元の組織内で策定した、コンピュータ機器に対する取扱いについてのドキュメント

表 2 製造者別の主な BIOS 起動キー

PC 製造者	BIOS 起動キー
Acer	Del 若しくは F2
旧 Compaq	F10 若しくは F1、F2、Del
Dell	F2
eMachines	Tab 若しくは Del、又は F2
Fujitsu	F2
Gateway	F1
Hitachi	F2
HP	F10

IBM/Lenovo	F1 若しくは F12
Lenovo	F1 若しくは F12
NEC	F2
Panasonic	F2
Phoenix Award BIOS 標準	DEL
Sony	F2 若しくは F3 のち F2、F3 のち F1
Toshiba	Esc のち F1

6. 証拠保全の機器

6-1. 複製先に用いる媒体(記憶装置)

6-1-1. 媒体のチェック

- 複製先に用いる媒体は、あらかじめ書込み／読み等のデバイスチェックを行い、正常に動作する状態のものを用意する。なお、フラッシュ系媒体(SSDを含む)は、代替領域等の隠し領域の都合上、無データ状態であることを確認することが難しいため、複製先として証拠保全に用いる場合は注意が必要である。

6-1-2. 無データ状態

- 複製先に用いる媒体は、全て、一切のデータが存在しない状態(ファイルの通常削除レベルではなく、バイナリレベルで一切のデータの存在が確認できない状態)のものを用意する。但し、物理複製に関しても、複製に使用するツールが、複製元の不良セクターをゼロ値等に置き換え、複製先に保存する場合はこの限りではない。

6-1-3. 完全(物理)複製

- 対象物の完全(物理)複製を行う場合、複製先に用いる媒体は、証拠保全機器のクリッピング機能又は他の手段によって、ハードディスクの容量を複製元と同一な状態に設定する。

6-1-4. 可読・可搬媒体

複製先に用いる媒体は、第三者機関等に提出・譲渡する場合を考慮し、可読・可搬な媒体を用意する。

- 複製先に HDD／SSD を用いる場合、汎用性の高い SATA²⁴ 等を利用する。
- イメージによる複製を行う場合、複製先のファイルシステムの制限を考慮する(例:FAT32 ファイルシステムでは扱えるファイルサイズの上限は 4GB)。
- NTFS 等のジャーナリングに対応した、壊れにくいファイルシステムを利用する。

6-2. 証拠保全機器に求められる機能

6-2-1. 書込み防止機能

- 原本に対し、いかなる書込みも行うことができない機能を有する装置を用意するか、原則としていかなる書込みも行うことができない措置を取る(ソフトウェアベース等)。

²⁴ SATA:Serial Advanced Technology Attachment。パソコンとハードディスク等の記憶装置を接続する IDE(ATA)規格の拡張仕様の一つ。

6-2-2. 完全(物理)複製機能

- 現存するデータだけでなく、削除データ・隠しデータ・未使用領域を含めた、対象物全領域（ユーザがインターフェース等を介してアクセスできる領域）を複製する。
- 複製元に不良セクター部分が存在する場合でも、継続して複製を行うことができ、不良セクターの位置等を確認する（これにより、ハッシュ値²⁵が原本と異なった場合に説明が可能となる）。
- 対象物(複製元)を、内容だけでなく記録順・構成も全て物理的に複製する（Single Capture）。
- イメージファイルとして複製する（Linux DD コマンド／EnCase Image 等）。

表 3 証拠保全機器に求められる機能

■書き込み防止機能 - 原本に対しいかなる書き込みも行うことができない
■完全(物理)複製機能 - 対象物全領域を複製することができる - 不良セクターへの対応 - 物理的及びイメージによる複製
■同一性検証機能 - ハッシュ値やバイナリコンペア等による同一性検証 - セクターサイズの表示
■作業ログ・監査証跡情報の表示・出力機能 - 対象物及び複製先の詳細情報 - 作業内容及び各種設定情報 - 作業時間等の作業結果 - 作業者情報 - 機器情報

6-2-3. 同一性検証機能

(同一性の検証(複製時のベリファイ))

- 対象物(複製元)及び複製先のハッシュ値を計算し、これらを照合して同一性を検証する。
- ハッシュ値を用いずに、バイナリコンペア等により同一性を担保しても良い。

²⁵ ハッシュ値は、同一性の補強を行うため、できるだけビット数の高い、衝突耐性の高いアルゴリズムを選定する(MD5 より SHA-2 等)。また、一種類のハッシュ値だけに依存せず、可能であれば二種類のハッシュ値を取得することが望ましい(例:SHA-2 等)。

- 不良セクター等により複製元と複製先のハッシュ値が一致せず、ハッシュ値による同一性検証が困難な場合、検証時の状況(機器の画面等)の写真撮影や複数人の現場立会い等により同一性を担保する。

(セクターサイズの確認機能)

- 1セクターあたりのサイズにより、解析ツールに読み込めなかったり、適切な表示ができなかったり場合に備えて、セクターサイズを確認する。

6-2-4. 作業ログ・監査証跡情報の表示・出力機能

(作業ログ)

- 対象物(複製元)及び複製先についての詳細情報を表示・出力可能
各デバイスのラベル情報(メーカー／型番／モデル名／シリアルナンバー／セクターサイズ／総セクター数／記憶容量)、HPA・DCO の設定の有無等
- 実施した作業内容及び詳細設定情報を表示・出力可能
- 実施した作業の結果を表示・出力可能
作業開始から終了までの時間／複製(検証)、速度／エラー発生時の詳細情報等

(監査証跡情報)

- 実施作業の管理者／所属先／取扱い案件・取扱い証拠に割り振られた番号等を表示・出力可能
- 実施作業に用いられた機器のシリアルナンバー／ソフトウェア・ファームウェアのバージョン等を表示・出力可能

6-3. 証拠保全ツールに関する要件

6-3-1. 完全(物理)複製(Single Capture 又はイメージコピー)が可能

- 対象物と同一の OS 上で起動可能なソフトウェア又はプログラムを利用。
 - GUI(Graphical User Interface)形式又はコマンドラインによる使用。
- 証拠保全ソフトウェア又はプログラムが記録されている USB や DVD／CD デバイス等のブートによる利用。
 - HDD／SSD を筐体から取り出せない、若しくは困難、取り出すことは容易でも原状復帰が困難である場合に利用。
 - USB や DVD／CD 内のデータを読み取るために、対象物の HDD／SSD より CD を優先して起動できるよう、BIOS／UEFI 等で起動順序を確認し、必要に応じて変更。

《考慮すべき事項》

UEFI を採用している場合、従来の BIOS での設定だけでは不十分のため、必ず事前にメーカーの Web サイト等で起動順序の設定方法を確認しておくこと。特に、Fast Boot や Secure Boot に注意すること。

- 対象物の電源が OFF の場合は、起動せずに光ディスクドライブを開けることができる施策を実施(光ディスクドライブに設置されている小さい穴に、クリップを挿入して強制的にドライブを開ける等)。

6-3-2. 信頼できる機関による検証

- CFTT(Computer Forensics Tool Testing²⁶)等の信頼できる機関にて検証されたものが望ましい。

6-3-3. 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/SSD に残す方法もある。ただし、HDD/SSD 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/SSD の証拠保全の完全性が損なわれる。

《考慮すべき事項》

代表的な収集及び分析ツールの使用にあたっては、経済産業省の「情報セキュリティサービス基準審査登録」に登録された製品や本研究会が実施している「日本語処理解析性能評価」を受けた製品等を使用することを推奨する。

6-4. その他、証拠保全に必要な機器・機材・施策の準備

6-4-1. HDD/SSD の物理的制限及び(強制)解除機能の有無の確認

- HPA、DCO 等の確認を実施する。

6-4-2. HDD/SSD パスワード・暗号化に対する準備

- 対象物を起動せず、解析の段階で復号可能な施策があれば、その手法を選択する。
 - ただし、初動対応及び証拠保全に要する時間や優先順位により、その施策が取れない場合もある。
- やむを得ず対象物を起動する場合。

²⁶ CFTT:コンピュータ・フォレンジック用ツールに関し、中立的な立場で、その評価テスト手法を確立することを目的として活動している米国 NIST のプロジェクト。(http://www.cftt.nist.gov/)

- 起動することによるデータの作成・上書き・改変等のリスクを認識すると共に、依頼元に対する十分な説明を行い、同意を得た上で作業する。

6-4-3. IDE²⁷ HDD／SSD に設置されているジャンパーピンの取扱い

- 対象となる HDD／SSD にジャンパーピンがある場合には、その状態を記録しておき、証拠取得時の影響について検討する。

6-4-4. RAID 装置や構造が複雑なサーバ類の証拠保全

- HDD／SSD を取り出すことによって、設定が大幅に変更される、又は原状復帰することが困難な場合、CD ブートによる証拠保全等、証拠保全作業における影響を最小限に抑える手段を取る。

6-4-5. 事前の十分なテスト及び機能の稼働状態のチェック

- 証拠保全作業に用いるツールは、あらかじめ十分なテストを行い、機能の稼働状況をチェックする。

²⁷ IDE: Integrated Drive Electronics。コンピュータにハードディスク等を接続するためのインターフェース規格。

7. 証拠保全の実施

7-1. 代替機・代替ツール・代替手段の準備

予期せぬエラーによる証拠保全作業の中断を想定し、可能な代替手段をあらかじめ用意することを推奨する。

7-2. 立会人等

初動対応及び証拠保全を行う場合、可能な限り、立会人を付けるか、複数人で実施する。

7-3. 同一性の検証

対象物(複製元)及び複製先に対し、完全(物理)複製実施時にハッシュ値の算出を行うなど、同一性を検証する。ライブでのイメージ取得やハードディスクの不良セクター等により、複製元のハッシュ値の算出が困難な場合は、複製先のハッシュ値のみを算出する。証拠の同一性検証に関しては、「4.3 証拠保全ツールに関する要件」にて選定された適切なツールを使用し、かつ、「5.4 証拠保全の正確性を担保する作業内容の記録」を取得し、ツールの信頼性及び証拠保全作業の正確性をもって行う。

7-4. 証拠保全の正確性を担保する作業内容の記録

7-4-1. 活動履歴の記録

(特に、対象物を起動させた状態で)証拠保全を行う際は、許容できないデータの改変等が起きないように、十分に注意を払い、作業に伴う一切の活動履歴を記録する。

7-4-2. 証拠保全に関わる機器の情報の記録

対象物(複製元)及び複製先の媒体だけでなく、証拠保全に関わる一切の機器の情報を記録する。

- 証拠保全に用いた機器のシリアルナンバー／ソフトウェア・ファームウェアのバージョン。
- 対象物(複製元)及び複製先の媒体から算出したハッシュ値。

表 4 対象物のハッシュ値の算出例

- | |
|---|
| <ul style="list-style-type: none">● Windows 標準機能を利用する場合
CertUtil -hashfile <ファイル名> <ハッシュアルゴリズム>
例: > CertUtil -hashfile 対象文書.docx MD5● Windows トラブルシューティングツール(SigCheck²⁸)を利用する場合 |
|---|

²⁸ SigCheck <https://docs.microsoft.com/ja-jp/previous-versions/bb897441%28v%3dmsdn.10%29>

SigCheck -h <ファイル名>

例: >SigCheck -h 対象文書.docx

7-4-3. ビデオ及び写真撮影

- 各工程で行った作業は、状況に応じてビデオや写真に撮影するなどして、後日、可能な限り再現できるようにする。
- 撮影にあたっては、保全機器や対象物の媒体のみを記録するだけでなく、対象物をどこからどのように外し、保全機器につなげ、外し、どこに戻したか等の一連の作業が明確に分かるよう記録する。

7-5. 複製先の取扱い

7-5-1. 厳重な管理

複製先は、他の機器と混在しないように、物理的に分けられたスペースに保管し、解析用途以外では一切触れることができないよう、Chain of Custody(証拠保全の一貫性)を証明できる書類²⁹等を作成して、厳重に管理する。

- 複製先の媒体の保管。
 - 電磁波・静電気・埃等により精密機器にダメージを与えない場所・梱包を用いて保管。
 - 温度・湿度、直射日光等にも留意し、夏場のカビや冬場の結露等にも注意が必要。
- 複製作業だけでなく、梱包・封印作業についても、複製先にダメージを与えないように十分な配慮をすると共に、複数人で作業し、複数人の認証方式で封印することが望ましい。

7-5-2. フォレンジックチーム等への提出・譲渡

- 複製先を、いつ、誰が、誰に、どこで、何を、どのような状態で手渡したかを逐一記録・明記することにより、Chain of Custody(証拠保全の一貫性)を確保する。
- 遠隔地への発送の場合は、壊れ物かつ機密情報扱いとして、然るべき発送業者及びサービスを用いて発送する。
- 搬送する場合も、電磁波・静電気・埃等の影響を受けない場所(磁石、スピーカーの近傍等)は避け、震動防止対策も施す。

7-5-3. 保全対象の確認

- 保全対象の現在の状況を確認する。

²⁹ 「誰が、いつ、何をしたのか」が把握できる書類。

- 保全するデータの範囲、データ種別、データ件数、管理状態(ラベルやタグ情報、フォルダ構造等)を記録する。
- サービスの仕様や設定によっては対象データの過去のバージョンを復元可能な場合があるため、作業手順で想定している保全の範囲に漏れないか確認する。

7-5-4. 保全

- 事前に準備した作業手順に従ってデータの保全を行う。
- 保全されたデータの件数やデータの状態を確認し、事前に想定した保全対象が全て取得されていることを確認し、記録する。

7-5-5. 同一性の検証

- 保全されたデータ、及び一連の保全作業で取得した動画やスクリーンショット等の作業記録に対して、ハッシュ値を算出する。
- 証拠の同一性検証に関しては、「4.3 証拠保全ツールに関する要件」において選定された適切なツールを使用し、かつ、「5.4 証拠保全の正確性を担保する作業内容の記録」を取得して、ツールの信頼性及び証拠保全作業の正確性をもって行う。

7-5-6. 保全のため変更した設定の復元

- 保全作業が完了した場合は、保全のために変更した設定の復元を行うかどうか検討する。
- ただし、インシデントが収束するまでは、排他制御をかけ保全状態を維持した方が良い場合があるため、設定の復元はアカウントの所有者やインシデント担当者、法務担当者を交えて協議した後に実施する。

7-7. ネットワークログからの証拠データ抽出

7-7-1. ネットワークログからのデータ抽出前の留意事項

- 一般的なセキュリティ機器やオペレーティング・システムであれば、共通ログフォーマットであることが多いため、オープンソース情報でログの各項目を調べることができるが、一部の業務用アプリケーションは、独自の設定をしているため、調べにくいことがある。
 - この場合、業務用アプリケーションの開発元に問い合わせる必要がある。
- ネットワークシステム全般の設計、検証及び運用の過程で、ネットワークパフォーマンスや運用監視の都合上、ネットワークログフォーマットが初期状態から変更されている可能性があることに留意しなければならない。
- 取得できていなかった期間を明確にし、取得されていない原因・理由を可能な範囲で確認し、第三者が確認可能な形で記録を残す必要がある。

- ネットワークログに自動的に記録されているタイムスタンプの状態を把握するため、調査で用いる基準時と、データ抽出作業時点での抽出対象システムの時間との誤差を確認する必要がある。
- これらは証拠保全のみならず、その後の調査の前提となるため、ネットワークログのデータ抽出作業を始める前に、必ず行わなければならない。

7-7-2. ネットワークログからのデータ抽出の観点

- ネットワークログの抽出方法の一つとして、特定のネットワークログの抽出ツールとしてサーバに設置するソフトウェアや、取り出したネットワークログを抽出、分析する製品等が存在するが、いずれも部分的な解決にしかならないことが多い。
- 実際のネットワークログの分析作業では、さまざまなツールやプロダクトを併用しながらデータを抽出する。表 4 にネットワークログの分析作業の例を示す。
 - なお、コンピュータ・システムに対するデジタル・フォレンジックや、マルウェア解析等の結果から得られた、IP アドレスやホスト名、コンピュータ名、ポート番号、通信プロトコル等の情報は、情報単体もしくは複数の情報を組み合わせることによって、調査対象を識別するための重要な情報となる。これらの調査のキーとなる情報のことを、以後“キー情報”とする。

表 5 実際のネットワークログの分析作業の例

- | |
|--|
| <p>① コンピュータ・システムに対するデジタル・フォレンジックの結果から得られた「キー情報」に基づく調査</p> <ul style="list-style-type: none"> - 具体的には、サイバー攻撃を受けた範囲の IP アドレスやホスト名(コンピュータ名)、外部アクセス先の IP アドレス等) <p>② 感染したマルウェアの分析結果から得られた「キー情報」に基づく調査</p> <ul style="list-style-type: none"> - 具体的には、マルウェアが使用した IP アドレス及びポート番号、外部ホストとの通信プロトコル等 <p>③ 「キー情報」を基にした、ネットワークログの調査から得られる不審な挙動の検出</p> <ul style="list-style-type: none"> - 同じ ID で一定回数以上の認証試行の繰り返し、同一 IP アドレスから複数 ID への認証試行 (データベースサーバの場合)、アプリケーションサーバや Web サーバ以外からの DB アクセス、システム運用時間外におけるアクセス、極端に長いセッション時間のアクセス、単位時間あたりのセッションの確立回数とそのデータ量等 <p>④ 「キー情報」を基にした、他所で発生している類似したサイバー攻撃又は既存のマルウェアの分析結果から得られた「攻撃シーケンス(コンピュータ及びネットワーク上の攻撃の挙動パターン)」からの「参考情報」の収集</p> <ul style="list-style-type: none"> - この調査を行う者は、最新のサイバー攻撃やマルウェアに関する深い理解が必要 <p>⑤ 関係する可能性がある全てネットワーク機器、オペレーティング・システム、アプリケーション等のネットワークログを、「キー情報」及び「参考情報」を基に相関的な観点で調査</p> |
|--|

7-8. 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。

7-8-1. 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³⁰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・レスポンドは、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侵入・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。

7-8-2. 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・レスポンド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

³⁰ この定義は、「今、現場で求められる Fast Forensics(杉山一郎氏)」の見解を参考とした。
<http://www.digitalforensic.jp/archives/2013/1308.pdf>

8. 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。

8-1. 事前に行う準備

保全対象となるサービスの利用契約や約款において、次の事項を確認する。

- サービスの利用規約、契約書、及び SLA(サービス品質保証)。
- サービスの利用形態及びプロバイダと契約者の間で交わされた契約内容、責任範囲。

8-2. インシデント発生直後の対応

インシデント発生後速やかに、次の事項を記録及び保存する。

- 保全対象になる(可能性の高い)サービスのデータ及びアカウントと発生したインシデントとの関係性。
- 保全が必要であると判断した根拠又は検討内容。

8-3. 保全方法及び作業手順の検討

サービスからの保全方法及び作業手順を確認及び検討する。

- サービスが標準で提供しているデータのバックアップ／エクスポート。

《考慮すべき事項》

データを暗号化している場合は、回復用のキーも取得すること。

- エクスポートが未対応若しくは困難な場合、プロバイダに保全作業を依頼する等の別手段を検討。

- ローカル端末にバックアップやデータのキャッシュが存在する可能性がある場合、ローカル端末の保全を検討。

8-4. 証拠作業にあたっての留意点

アウトソーシングサービスを対象とした証拠保全は、プロバイダにおけるサービスが継続する中で作業することが多いため、次の点について留意する必要がある。

- 可能な限り、立会人を付ける又は複数人で実施する。
- 対象データに対する意図しない改変を防ぐために、作業員は事前にサービスの内容を熟知し作業手順を決めておく。
- 設定状況が明確になっている物理的作業環境及びネットワーク環境を確保する。
- 後日、保全作業を再現できるようにするため、可能であれば通信パケットを取得する。

《考慮すべき事項》

取得した通信パケットを、証拠保全の作業記録と時系列に関連付けておく。

- 提供されるサービスによっては保全後に改めて状況を再現することが困難な場合があるため、作業員がどのようなインターフェースを用い、どのような操作や検索の実行等を詳細に記録する。
- 対象サービスのデータの保存時に、タイムスタンプや表示条件等のさまざまなメタデータを記録する。

《考慮すべき事項》

HTML をブラウザで表示して保存する場合、使用するブラウザによって表示される内容が異なることがあるため、ソースを表示した際のブラウザの種類とバージョンも記録しておく。

8-5. アカウント所有者の同意

アウトソーシングサービスから保全する対象データは、そのデータにアクセスする権限を持つアカウントの所有者の同意が必要になることがある。

- 対象アカウントが個人に属する場合、保全は本人の同意を得て行う。
- 同意の事実を後日確認するため、同意内容を書面に記録する。
- 家族など、保全対象アカウントを複数の人間で管理している事実がある場合、可能な限り全員の同意を得る。
- 同意内容には、保全対象アカウント及びパスワードの開示、排他制御のための作業中のパスワード変更、データのエクスポートの許可等を記載する。
- 本人の同意を得てパスワード等の変更を行う場合は、アカウント設定変更記録を作成して、厳重に管理する。

8-6. 収集・取得・保全

8-6-1. アクセス可能なアカウントのチェック

- アカウントの所有者の同意書や設定変更記録等を確認し、及びデジタル証明書の実在性を検証した上で、対象のアカウントが保全目的でアクセス可能な状態であることを確認する。
- 特にアカウントが排他制御状態にあり、保全作業を実施するのに適した状態であるかの確認を行い、記録する。

8-6-2. 作業記録の作成

- サービスへのログインを含め、保全作業における一連の作業記録を作成する。対象のアカウント名やサービスのアクセス先の情報を客観的に確認可能とするため、必要な情報を書面に記録するとともに、動画やスクリーンショット、写真等、客観的な記録も併せて取得する。
- 必要に応じて、作業を行った際の対象サービスのメタデータや、サービス提供先のサーバとの通信パケットも作業記録とあわせて取得する。
- 排他制御等の目的で必要に応じて設定変更等を行う場合は、変更前の内容と変更後の内容を作業完了後に改めて確認・検証可能な記録を作成する。

8-6-3. サービスの利用状況のチェック

- ブラウザ若しくは専用のクライアントツールを用いてサービスにアクセスし、アカウント及びパスワードを入力して、ログインする。
- 正常に対象サービスへのアクセスが確認された後に、対象ユーザの利用状況を確認するために、サービスの基本設定項目、Cookie 情報及びサービス利用履歴の記録を作成する。
- 一部のサービスでは、他のユーザとファイル等の情報を共有して、外部のユーザに編集権限を与えることが可能なサービスも存在するため、排他制御等の目的で、必要に応じて共有設定の変更や公開の停止等も検討する。
 - 設定を変更する際は、「8.6.2 作業記録の作成」に従って記録を作成する。

付録資料

A. チェックシート（PC の場合）

No.	確認項目		写真	チェック
1	[事前準備] 複製保存用の HDD/SSD を用意する。事前に、ワイプ処理、HDD/SSD 複製装置がサポートする形式でフォーマットしておく。			☐
2	使用する機材の時計を日本標準時刻に合わせる。			☐
3	作業開始の前に、作業場所で、立会人と作業員の写真を撮影(ケース番号、当日の新聞をもって撮影)する。		○	☐
4	PC のシリアル番号などの固体識別番号を記録、写真撮影する。		○	☐
5	電源 ON の場合	OS のシステム時刻を記録する。	○	☐
6		(必要に応じて) 画面やプリンタなど出力装置に表示・出力されている情報を記録する。	○	☐
7		(必要に応じて) メモリなど揮発性情報を記録・保存する。		☐
8		電源を OFF にする。Windows の場合は、電源プラグを抜いて強制的に電源を OFF にする。		☐
9	帯電防止リストバンドの使用、帯電防止手袋の着用、帯電防止マットの準備等、静電気による機材の破損が無いように考慮する。			☐
10	UPS を用意するなど、電源のトラブルにより HDD/SSD 複製作業に影響が無いように配慮する。			☐
11	PC に電源等のケーブルが接続された状態であれば、ケーブルのラベリングをして撮影後、取り外す。		○	☐
12	PC 本体から、原本 HDD/SSD の取り外しを行う前に、HDD/SSD 自体に暗号化機能がある型番でないか確認する。		○	☐
13	PC 本体から、原本 HDD/SSD の取り外しを行う。			☐
14	原本 HDD/SSD にラベル(ケース番号、原本番号)の貼り付けを行う。			☐
15	原本HDD/SSD 表面のメーカーラベル情報の記録。メーカーラベル面、ピン状態を撮影する。		○	☐

No.	確認項目	写真	チェック
16	書き込み防止装置を使用して原本 HDD/SSD が読み込み可能か確認する。暗号化されている場合は、そのまま保全するか、保全方法を変更するか判断する。 (既に暗号化されている事が前提である場合、書き込み防止装置が無い場合は、この項目をスキップする。)		☐
17	複製保存用 HDD/SSD のメーカーラベル情報の記録。複製保存用 HDD/SSD にラベル(ケース番号、原本番号)の貼り付けを行う。		☐
18	HDD/SSD 複製装置に原本 HDD/SSD を接続する。接続状態の写真撮影を行う。	○	☐
19	HDD/SSD 複製装置で表示される原本 HDD/SSD のラベル情報と原本 HDD/SSD の表面のメーカーラベルの情報が同一であるか確認する。HPA 又は DCO 領域が存在するかも確認する。ラベル情報を記録、表示画面の写真撮影を行なう。	○	☐
20	HDD/SSD 複製装置に複製保存用 HDD/SSD を接続する。		☐
21	HDD/SSD 複製装置のメニューを操作して動作モードおよびログ出力など基本設定を確認し、複製を実施する。実行前の写真撮影を行う。	○	☐
22	複製後に HDD/SSD 複製装置に表示される原本 HDD/SSD のハッシュ値を記録、写真撮影を行う。	○	☐
23	HDD/SSD 複製装置のログにより正常に複製が行われたか確認する。	○	☐
24	複製保存用 HDD/SSD のハッシュ値を取得し、原本 HDD/SSD のハッシュ値と複製データのハッシュ値が同一であるか確認する。ハッシュ値の記録、写真撮影を行なう。(HDD/SSD 複製装置のバリファイ機能等で出力イメージの同一性が担保できれば、この項目をスキップする。)	○	☐
25	HDD/SSD 複製装置から原本 HDD/SSD を取り外し、ピンの状態を確認し、写真撮影を行なう。	○	☐
26	原本 HDD/SSD を PC 筐体に戻し、ケーブルも元の接続状態にもどす。	○	☐
27	複製保存用 HDD/SSD は、機器が破損しないように考慮し、移動させる場合は、衝撃吸収性、帯電防止措置のあるケースなどを使用する。		☐

B. 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

<刑法>

(電磁的記録の定義)

第七条の二 この法律において「電磁的記録」とは、電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。

「電磁的記録」という言葉は、昭和 62(1987)年のコンピュータ犯罪関連の刑法一部改正にあたって追加された概念である。

上記の定義により、ハードディスク等の磁気デバイスのみならず、光ディスクや不揮発性メモリ上に記録された情報も電磁的記録として扱われる。逆に、パンチカードは人の知覚によって認識可能なものと見なされ、電磁的記録には該当しない。

(電磁的記録不正作出及び供用)

第百六十一条の二 人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、五年以下の懲役又は五十万円以下の罰金に処する。

2 前項の罪が公務所又は公務員により作られるべき電磁的記録に係るときは、十年以下の懲役又は百万円以下の罰金に処する。

3 不正に作られた権利、義務又は事実証明に関する電磁的記録を、第一項の目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作った者と同じの刑に処する。

4 前項の罪の未遂は、罰する。

昭和 62(1987)年改正時に追加された。例えば、外れ馬券の電磁的記録を当たり馬券のものに改竄し自動払戻機で現金を引き出した行為(甲府地方裁判所 平成元年 3 月 31 日判決)。パソコン通信のホスト コンピュータ内の顧客データベースファイルに虚偽のユーザの記録を置いた行為(京都地方裁判所 平成 9 年 5 月 9 日判決)などがある。また最近では、不正改造された B-CAS カードの使用者や、オンラインゲームのチート行為の摘発に際して本条を適用することも多い。

なお、コンピュータ・プログラムは、電子計算機に対する指令の記録であるから電磁的記録であっても「権利、義務又は事実証明に関する電磁的記録」とはいえない。

不正アクセス行為を手段として私電磁記録不正作出行為が行われた場合、不正アクセス禁止法違反と本条とがともに成立(併合罪)する(最高裁判所 平成 19 年 8 月 8 日決定)。

(支払用カード電磁的記録不正作出等)

第百六十三条の二 人の財産上の事務処理を誤らせる目的で、その事務処理の用に供する電磁的記録であって、クレジットカードその他の代金又は料金の支払用のカードを構成するものを不正に作った者は、十年以下の懲役又は百万円以下の罰金に処する。預貯金の引出用のカードを構成する電磁的記録を不正に作った者も、同様とする。

2 不正に作られた前項の電磁的記録を、同項の目的で、人の財産上の事務処理の用に供した者も、同項と同様とする。

3 不正に作られた第一項の電磁的記録をその構成部分とするカードを、同項の目的で、譲り渡し、貸し渡し、又は輸入した者も、同項と同様とする。

(不正電磁的記録カード所持)

第百六十三条の三 前条第一項の目的で、同条第三項のカードを所持した者は、五年以下の懲役又は五十万円以下の罰金に処する。

(支払用カード電磁的記録不正作出準備)

第百六十三条の四 第百六十三条の二第一項の犯罪行為の用に供する目的で、同項の電磁的記録の情報を取得した者は、三年以下の懲役又は五十万円以下の罰金に処する。情を知って、その情報を提供した者も、同様とする。

2 不正に取得された第百六十三条の二第一項の電磁的記録の情報を、前項の目的で保管した者も、同項と同様とする。

3 第一項の目的で、器械又は原料を準備した者も、同項と同様とする。

(未遂罪)

第百六十三条の五 第百六十三条の二及び前条第一項の罪の未遂は、罰する。

第 163 条の2～第 163 条の3までの一連の条文は、平成 13(2001)年に追加された。このころから、テレフォンカードに代表されるプリペイドカードやクレジットカード等が大量に偽造され社会問題化したことから、電磁的記録の社会的信頼を保護するために刑法に盛り込まれた。

(不正指令電磁的記録作成等)

第百六十八条の二 正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。

一 人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二 前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

2 正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

3 前項の罪の未遂は、罰する。

平成 23(2011)年の刑法一部改正によって追加された条文であり、いわゆる「コンピュータ・ウイルス 作成罪・提供罪／供用罪」である。

第 168 条の 2、第 168 条の 3 は、電子計算機のプログラムに対する社会一般の者の信頼を保護するために設けられた罪であり、文書偽造の罪(刑法第 17 章)等と同様に、社会的法益に対する罪である³¹。

³¹ 法務省公開資料「いわゆるコンピュータ・ウイルスに関する罪について」

(<http://www.moj.go.jp/content/000076666.pdf>)に、本条文に関する分かりやすい解説がある。

第1項が「ウイルス作成罪・提供罪」となり、第2項が「供用罪」となる。

作成・提供・供用とはそれぞれ、

- 「作成」とは、不正指令電磁的記録等を新たに記録媒体上に存在するに至らしめること、
- 「提供」とは、不正指令電磁的記録等を取得しようとする者が事実上これを使用できる状態に置くこと、
- 「供用」とは、不正指令電磁的記録を、電子計算機を使用している者が実行しようとする意思がないのに実行され得る状態に置くこと

を、意味する。

(定義が多少曖昧にはなるが、)平易な言葉で表せば、「提供」はコンピュータ・ウイルスを欲している者にそれを渡るようにすることであり、「供用」は他人のコンピュータに勝手にコンピュータ・ウイルスを仕込むことになる。

第1項第1号の「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」とは、「そのままの状態で電子計算機において動作させることができるもの」ということであり、つまりは、exe 形式やスクリプトのように他の作業を加えずとも実行可能なウイルスのことをいい、第2号の「前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録」はプログラムソースコードの状態のものも含むということになる。また、第1号は電磁的記録に限定している(したがって、本条2項の供用罪の対象にもなる)が、第2号ではその他の記録も含まれるため、必ずしも電子媒体である必要はなく、紙媒体に印刷したものでも良いことになる。

なお、技術者の間で、完成度の低い OS や、深刻なバグを含むプログラム自体がこの「不正指令電磁的記録」にあたるのではないかという誤解があるようであるが、本罪が成立しうるのは、それが不正指令電磁的記録と認識された時点以降の行為であり、仮にそのようなものを開発してしまったからといって、ただちに本罪が適用されるわけではない。また仮にそのような深刻なバグを含むプログラム自体が不正指令電磁的記録とされるには、一般社会通念上の合意が必要となるはずであり、バグが不可避と考えられている現状においてはそのようなことは起こらないと言えよう。つまりは、一部の者だけが、「このようなプログラムは、けしからん」などと言っているにもかかわらず、一般のコンピュータ・ユーザが「このプログラムはウイルスだ」という認識を持つことが必要であろう。

供用罪についても同様で、そのプログラムを第三者が実行できる状態においた時点で不正指令電磁的記録を認識していなければ成立しないと言える。

条文の読み方から、供用罪には第2号の電磁的記録等(つまり、ソースコード状のもの)は含まれない。また、未遂罪が可罰なものも第2項の供用罪のみとなる。

(不正指令電磁的記録取得等)

第百六十八条の三 正当な理由がないのに、前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。

第168条の2と同時に平成23(2011)年の刑法改正によって追加。本条はコンピュータ・ウイルスの「取得」「保管」についての罪を定めたものである。

ここでいう「取得」とは、不正指令電磁的記録等を自己の支配下に移すことを、「保管」とは、不正指令電磁的記録等を自己の支配領域内において置くことをそれぞれ意味するものである。

(わいせつ物頒布等)

第一百七十五条 わいせつな文書、図画、電磁的記録に係る記録媒体その他の物を頒布し、又は公然と 陳列した者は、二年以下の懲役若しくは二百五十万円以下の罰金若しくは科料に処し、又は懲役及び罰金を併科する。電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した者も、同様とする。

2 有償で頒布する目的で、前項の物を所持し、又は同項の電磁的記録を保管した者も、同項と同様とする。

平成 23(2011)年の刑法一部改正で電磁的記録の追加がなされた。すでにわいせつデータを格納した HDD/SSD をわいせつ物と見なすなどの判例(「アルファネット事件」最高裁判所 平成 13 年 7 月 16 日決定「アルファネット事件」)等があり、改正後は、わいせつ画像データを有償頒布する目的であれば、作出 行為以前の段階で、わいせつな電磁的記録の保管として処罰される。

(電子計算機損壊等業務妨害)

第二百三十四条の二 人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。

2 前項の罪の未遂は、罰する。

昭和 62(1987)年刑法一部改正時に追加。

電子計算機損壊等業務妨害罪は、①電子計算機・電磁的記録の損壊、電子計算機への虚偽の情報・不正な指令の入力、その他の方法により、②電子計算機に動作の阻害を生じさせ、③業務妨害をもたらすこと、が必要である。

平成 23(2011)年刑法一部改正時に未遂罪が追加された。例えば、電子計算機を作動不能にさせるウイルスを送り込もうとしたが、防護措置が機能して阻止された場合などがある。

(電子計算機使用詐欺)

第二百四十六条の二 前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する。

詐欺罪(第 246 条)は「人を欺いて」と規定されていて、その対象が人であるため、機械に対して詐欺を行っても適用することができなかった。そこで昭和 62(1987)年刑法一部改正時に本条が追加された。これにより、対象が人でなく電子計算機であっても詐欺が成立することとなった。

コンピュータに偽の情報を送り自身の預金額を増加させる等の犯罪が多発したために設けられた。

盗んだクレジットカードの名義人の氏名と番号を使ってインターネットカード決済代行業者の使用するコンピュータにデータを入力して、電子マネーの利用権を取得した行為が、本条にあたるとした判例がある(最高裁判所 平成 18 年 2 月 14 日決定)。

(公用文書等毀棄)

第二百五十八条 公務所の用に供する文書又は電磁的記録を毀棄した者は、三月以上七年以下の懲役に処する。

(私用文書等毀棄)

第二百五十九条 権利又は義務に関する他人の文書又は電磁的記録を毀棄した者は、五年以下の懲役に処する。

昭和 62(1987)年刑法一部改正時に電磁的記録も文書毀棄の対象となるように文言が追加された。

<不正アクセス禁止法>

前述の「電子計算機損壊等業務妨害罪」(刑法 第234条の2)は、電磁的記録の損壊や 不正な指令を与えるなど、つまりはデータやプログラムの破壊や改竄が適用要件となる。インターネットの普及に伴い、こういった電磁的記録の損壊行為を伴わず、サーバコンピュータ上からただ情報だけを持ち出す行為が急増した。よってコンピュータへの不正アクセスが行われた段階で取り締まることのできる法律の整備が必要となり、平成 12 年(2000 年)に施行されたものが本法である。その後、量刑の強化とフィッシング行為取締に関する規定が追加された改正法が平成 24 年(2012 年)5 月 1 日より施行された。

(「不正アクセス行為」の定義)

第 2 条第4項 この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

- 一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為(当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。)
- 二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報(識別符号であるものを除く。)又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為(当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。)
- 三 電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

平成 24(2012)年の改正で、不正アクセスの定義が、他の定義と同様、第2条にて記載された(従前は 第3条に規定)。不正アクセスは大きく分けて、ID／パスワードを不正に使い侵入する場合と、セキュリティホールをついて侵入する場合の二つに分類されている。条文中の識別符号には、パスワードの他、指紋や虹彩といった身体上の特徴に基づく符号や、署名の形状や筆圧、動態等から特徴を取り出して符号化したものも含まれる。

第3条において、「何人も、不正アクセス行為をしてはならない」と、第 2 条に定義されている行為を行うことを禁止している。

第 11 条により、法改正後は、3年以下の懲役又は100万円以下の罰金(従前は 1 年以下の懲役又は50 万円以下の罰金)と罰則が強化された。

本条文や条文中の文言については、警察庁の Web サイトに詳細な解説が掲載されている。
(http://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf)

不正アクセス罪が成立するかどうかを巡って争われた裁判に、ACCS(コンピュータソフトウェア著作権協会)のサーバのセキュリティホールにシンポジウム中に侵入してみせた事件がある(東京地方裁判所平成 17 年 3 月 25 日判決)。

(他人の識別符号を不正に取得する行為の禁止)

第四条 何人も、不正アクセス行為(第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。)の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。

(不正アクセス行為を助長する行為の禁止)

第五条 何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。

(他人の識別符号を不正に保管する行為の禁止)

第六条 何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。

改正前は「不正アクセス行為を助長する行為の禁止」のみ規定されており、ID／パスワードを他人に提供する行為のみが禁じられていたが、平成 24(2012)年の法改正により、不正アクセス目的での ID／パスワードの取得から提供、保管に至るまで一貫して規制の対象とされることになった。改正後の第 12 条により、これらの行為には「一年以下の懲役又は五十万円以下の罰金」と規定された。改正前は、「不正アクセス行為を助長する行為」に対して「三十万円以下の罰金に処する」という規定のみであったが、改正後では 不正アクセス目的であることを知りながら ID／パスワードを他人に提供した者には懲役刑もありえるという規定になっている。なお、不正アクセス目的であることを知っているか否かを問わず、ID／パスワードを他人に提供する行為に対しても「三十万円以下の罰金」が定められている(第 13 条)。

(識別符号の入力を不正に要求する行為の禁止)

第七条 何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他 当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。

一 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信(公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。)を利用して公衆が閲覧することができる状態に置く行為

二 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール(特定電子メールの送信の適正化等

に関する法律(平成十四年法律第二十六号)第二条第一号に規定する電子メールをいう。)により当該利用権者に送信する行為

平成 24(2012)年改正時に新設された条文で、いわゆる「フィッシング行為」を取り締まる為の規定となる。ID／パスワードの入力を不正に要求すること自体を、Web を用いる場合(第 1 号)、電子メールを用いる場合(第 2 号)のいずれも禁止行為とされている。

違反した場合は、第 12 条の規定により、1年以下の懲役又は50万円以下の罰金が科される。

<刑事訴訟法>

(リモートアクセスによる差押え)

第九十九条第二項

差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

第二百十八条第二項 ※新設

差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

(記録命令付差押え)

第九十九条の二 ※新設

裁判所は、必要があるときは、記録命令付差押え(電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。)をすることができる。

第 99 条 2 項は裁判所が差押えを行う場合、第 218 条第 2 項は捜査機関が行う場合のそれぞれの条文となる。「記録命令付差押え」に関しても、第 218 条第 1 項にも「検察官、検察事務官又は司法警察 職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、差押え、記録命令付 差押え、搜索又は検証をすることができる。(以下略)」と、下線部「記録命令付差押え」という文言が追加 された。

差し押さえるべきパソコンにリモートストレージサービスのアカウントの設定がなされている場合など、差押対象物が電子計算機であるときに、そのコンピュータにネットワークで接続している他の記録媒体(リモートストレージサーバ、メールサーバ、ファイルサーバ等)に記録されているデータを差押え対象となっているコンピュータ等に複写して、これを差し押さえるというものである。

「記録命令付差押え」は、データ等を所持・保管している者や適法なアクセス・利用権限を有している、例えばプロバイダなどの協力的な者に証拠として必要なデータなどをそのまま複写させたり、複数の記録媒体に記録されているデータなどを一つにまとめて新たに電磁的記録を作成し、記録媒体に記録させたりすることをいう。

コンピュータ・システムの管理者などは、裁判所の発する令状によって、上記の作業をすることになる場合があることを念頭においておくべきである。

(電磁的記録に係る記録媒体差押えの執行方法の整備)

第百十条の二 ※ 新設

差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も、同様である。

一 差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。

二 差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。

移転とは「電磁的記録の他の媒体への複写と、差し押さえるべき記録媒体からの当該記録の消去からなる」。

複写、印刷、移転のどれを選ぶかは、処分者(つまり差押えの実行をする人)の裁量となる。爆発物の作り方等のように、その情報を残しておくことが好ましくない場合などには移転が用いられるものと思われる。差押えの方法に不服がある場合には、準抗告(429条1項2号)という不服申し立てができる。

(電磁的記録にかかる記録媒体を対象とする処分への協力要請)

第百十一条の二 ※ 新設

差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状又は搜索状の執行をする者は、処分を受ける者に対し、電子計算機の操作その他の必要な協力を求めることができる。公判廷で差押え又は搜索をする場合も、同様である。

記録媒体の差押え等を行うにあたり、差押えなどを実施する捜査機関等が自ら執行することが困難な場合も多く、また、被処分者の利益の保護等の面からも適当でないことがあることから、搜索・差押えを実施する者が協力を求め、また、これに協力することができる法的根拠を明確にした(第222条第1項)。なお、111条の2は裁判所の差押えの規定があるが、検証にも準用される(142条)。

通信履歴の電磁的記録の保全要請

第百九十七条3項～5項 ※ 新設

3 検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付 差押えをする必要がないと認めるに至ったときは、当該求めを取り消さなければならない。

4 前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。

5 第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。

保全要請は、プロバイダ等の通信事業者等に対して、業務上記録している通信履歴(通信内容は含まれない)のデータ等を一時的に消去しないように求めるものであり、新たな種類の情報を記録することを要請するものではない。

保全要請は、「必要なものを特定し」、「30 日を超えない期間を定めて」「書面」で行う。「特に必要があるときは」延長可能であるが、最大 60 日を超えることはできない。参考までに、サイバー犯罪条約では 90 日間までの証拠の保全を求めている。

(補足)

改正刑事訴訟法に関する解説論文としては、立法に関与した杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について」(法曹時報 64 巻第4～5号)等がある。また、法制審議会の議事録からも解釈を得ることができる。本稿執筆に際しても参考とした。

<不正競争防止法>

(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つて、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二千万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

：

[中略]

：

3 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三千万円以下の罰金に処し、又はこれを併科する。

一 日本国外において使用する目的で、第一項第一号又は第三号の罪を犯した者

二 相手方に日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をする目的があることの情を知って、これらの罪に当たる開示をした者

三 日本国内において事業を行う保有者の営業秘密について、日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をした者

4 第一項(第三号を除く。)並びに前項第一号(第一項第三号に係る部分を除く。)、第二号及び第三号の罪の未遂は、罰する。

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。それ故、技術情報だけでなく顧客名簿などのビジネス情報も営業秘密となり得る。

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～10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、開示等におけるさまざまな場合が列挙されている。2015年(平成27年)には新たに、営業秘密侵害品の譲渡、引渡し、輸出入、電気通信回線を通じた提供等が不正競争行為として追加された。

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。こちらも条文の全てを記載することは紙面都合でしていないが、第21条第1項の第1号～第9号の各号において刑罰が科されるさまざまな場合が規定されている。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。それ故、金銭目的で営業秘密を持ち出して他人に売却した場合も当然に犯罪となる。

ベネッセからの顧客名簿の漏洩、そして東芝・サンディスクや新日鉄住金からの技術情報の海外漏洩などといった深刻な流出事件が続いたため、2015年(平成27年)7月の法改正時に、罰則が大幅に強化された。まず、営業秘密漏洩罪の法定刑が「10年以下の懲役若しくは2千万円以下の罰金、又はこれを 併科」となった(21条1項)。法人の場合は最大5億円の罰金。さらに海外重罰制度(21条3項)が取り入れられ、国外への漏洩や国外で使用する目的での持出に対しては、罰金額の上限が個人で3千万、法人で10億円となる。

さらに、営業秘密の三次取得者・四次取得者といった転得者も営業秘密を不正取得・不正使用した場合は処罰対象となった(21条1項8号)。これによって流出した顧客名簿を販売した者などを取り締まることができる。

注目すべき点として、今期改正より営業秘密侵害の未遂罪が追加されており(21 条 4 項)、経済産業省の解説資料³²によれば、「取得未遂」として『不正アクセス行為は確認されたが、証拠の隠滅等により営業秘密たる情報の持ち出しの事実を確認できなかった場合。社内メールシステムの管理者の地位を利用し、社内幹部宛のメールが自動で自らにも転送されるようなプログラムを埋め込んでいたが、実際に営業秘密情報が転送される前に明るみに出た場合。』が、「開示未遂」として『営業秘密を電話で売り込み、その後メールで営業秘密を不正に開示するべく、送信しようとしたが、メールソフトの不具合により転職先に到達しなかった場合。』が例示されている。よってデジタル・フォレンジックの作業としてはこれらの行為の痕跡を探すことになる。

また、営業秘密を蔵置したサーバが海外にあったとしても、日本国内において事業を行う保有者の情報であれば不正取得となり処罰対象となることも明記された(21 条 6 項)。

さらに、犯罪収益の没収制度の導入(21 条 10 項)、非親告罪化、営業秘密の不正使用に対する差止請求可能期間(除斥期間)の 20 年への延長(15 条)といった強化等が行われている。

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³³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³⁴。

本ガイドラインを公開する直前(平成 30(2018)年5月末)に「不正競争防止法の一部を改正する法律」が成立・公布されており、1年半以内に施行されることになっている。

改正法施行後は、自動走行車両向けの三次元地図データや POS システムで収集したデータ等のいわゆる「ビッグデータ」も保護の対象となる。また、暗号等の技術的制限手段の効果を妨げる「プロテクト破り」を可能とする機器の提供等だけでなく、役務の提供等も不正競争行為に追加される。

³² 平成 27 年不正競争防止法の改正概要

<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/27kaiseigaiyou.pdf>

³³ <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf>

³⁴ 同 指針「はじめに(本指針の性格)」より

C. デジタル・フォレンジック関連の資料紹介

- 「Electronic Crime Scene Investigation: A Guide for First Responders、 Second Edition /Forensic Examination of Digital Evidence: A Guide for Law Enforcement」
<https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>
- 「(CERT) First Responders Guide to Computer Forensics」
<http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7251>
- 「Best Practices In Digital Evidence Collection」
<https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection>
- 「情報セキュリティ関連法令の要求事項集」(平成 23 年 4 月 経済産業省)
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_JohoSecurityKanrenHoreiRequirements.pdf

D. Chain of Custody (CoC)シート例

証拠の概要

インシデントの概要					
件名		インシデントNo.			
事件主担当		引渡先法律事務所・機関			
対象に関する情報					
対象名				対象ID	
対象システム					
メーカー・ベンダー		BIOS Type:			
機種名		BIOS Date:	BIOS Time (24hr):		
シリアル番号		Actual Date:	BIOS Time (24hr):		
設置場所					
備考					
対象記憶媒体					
メーカー・ベンダー		総容量			
機種名		セクタ数(LBA/CHS)			
シリアル番号		I/F Type:	(IDE, SATA, SCSI, USB, Other)		
備考					
複製格納デバイス					
証拠番号		容量			
メーカー・ベンダー		I/F Type:	(IDE, SATA, SCSI, USB, Other)		
機種名		ファイルシステム	(FAT, NTFS, Native, Other)		
シリアル番号		Image file type:	(DD, EnCase E0, EnCase LEF, Native, Other)		
備考					
記憶媒体(バックアップ・作業用コピー)					
証拠番号		容量			
メーカー・ベンダー		I/F Type:	(IDE, SATA, SCSI, USB, Other)		
機種名		ファイルシステム	(FAT, NTFS, Native, Other)		
シリアル番号		Image file type:	(DD, EnCase E0, EnCase LEF, Native, Other)		
作業記録					
複製作業者		証拠取得用機器名			
証拠番号		証拠取得用ソフトウェア名			
作業時刻(Timezone)	Start time: / / , : (TZ)-> Complete time: / / , :				
Image file type:	(DD, EnCase E0, EnCase LEF, Native, Other) File Name:				
Image Hash:()					
Image Hash:()					

一貫性(Chain of Custody) 追跡記録

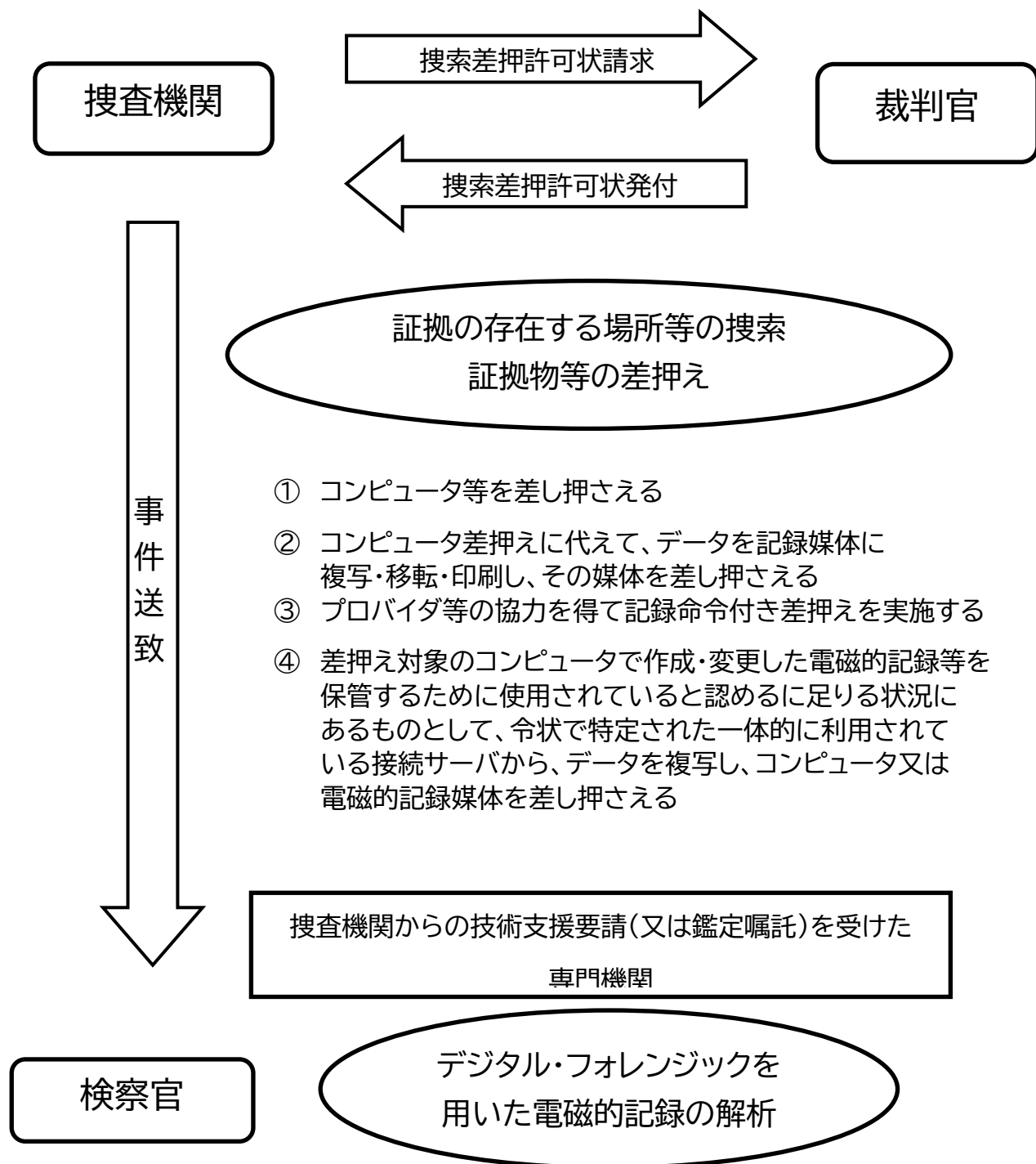
インシデントの概要			
件名		インシデント 番号	
作業者		作業日	
証拠リスト			
証拠番号	容量	証拠の内容	
一貫性			
作業日	作業内容	作業確認者 (Sign & Print Name)	作業受取者 (Sign & Print Name)

* Picture(s) may require to show an identity of the evidence

/

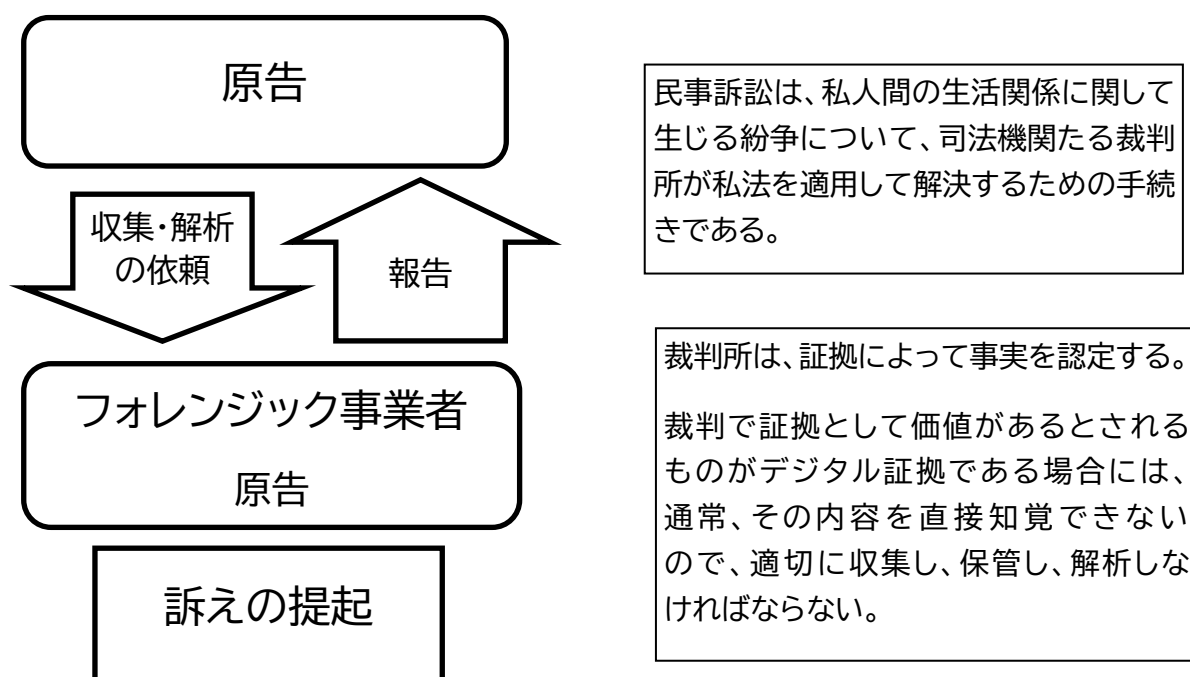
E. 刑事・民事におけるデータ収集と解析フローイメージ図

刑事手続きにおけるデータの収集と解析



解析結果は捜査機関に対して報告書(鑑定書)として提出される。

民事手続きにおけるデータの収集と解析



<参考資料> 日本弁護士連合会

「事件解決への流れ(民事事件・刑事事件)」(PDF 形式・114KB)

http://www.nichibenren.or.jp/library/ja/publication/booklet/data/chottosoudan_pam10.pdf

ただし、民事手続きへのデータの収集・検出の方法は、上記図の原告が行う場合に限られず、被告、裁判所、あるいは第三者が行う場合もある。民事訴訟においてデジタル・フォレンジックが活用される主な手続きは次のとおりである。

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。

裁判における解析データの利用

	刑事訴訟	民事訴訟
証拠能力	書面(データ等の解析結果報告書)は原則として証拠とすることはできないが、鑑定書として、解析した者の証人尋問を前提に証拠となる	特に制約なし
証明力	裁判所の合理的な自由心証	裁判所の合理的な自由心証

F. 供述証拠と事実認定の実務(概論)

※大橋充直会員提供資料:

営利(書式転売等)を伴わない利用や改変使用は、自己責任で自由にお使い下さい。

本稿は、被害民間企業や専門調査会社の調査係員が、被害事実や参考事実を調査して警察に届ける(捜査に協力する)場合に、刑事法の判例通説を踏まえて、事実認定や証拠吟味をする手法のガイドライン(簡略資料)としてまとめた私見(試見)である。

1 基礎概論

(1) 意見法則

これは、要するに「意見や主張は証拠じゃないよ。」というものであり、人が下した「評価・意見・主張」は、事実認定の証拠にならないというもので、「Aは善良な人であるから情報漏えいをするわけがない。無罪を求める。」という上申書や嘆願書を多数法廷に提出しても、裁判所は事実認定の証拠としては使ってくれない(最高裁判決 S24 年 6 月 13 日・最高裁判所刑事判例集 3 巻 7 号 1039 頁)。せいぜい情状証拠として使えるかもしれない程度である。

×例:「社長が、A君が犯人だと決裁されましたから、A君が犯人です。」

×例:「学級会の多数決でB君が犯人と決まったから、B君が犯人だ。」

(2) 伝聞(証拠)法則

これは、要するに「噂」や「伝え聞き」に基づいて事実を認定してはいけない! というルールである。伝聞(ヒア・セイ)は、知覚・認識・記憶・再現・叙述・表現という記憶再現過程に誤りが介在しやすいので、そのまま使うのはよろしくないということである(伝言ゲーム)。理想は、直接目撃した証人から、見たり聞いたりした様子が本当かどうかをさまざまな角度から反対尋問してホントかどうか確かめるということになる。

確かに、「君は 16 日前の昼飯で何を食った?」と質問されても、たいていは答えられないわけで、人の記憶なんか存外いい加減なものである(そのため、捜査機関は 16 日前の昼飯について裏付け証拠を一生懸命収集する。)

(3) 伝聞法則の例外

米国のウイグモアという学者によれば、伝聞証拠でも信用できる場合(特信性の状況的保証)として、「衝動的供述」「臨終の供述」「感情的表現の供述」等を例示した。

ハイテク犯罪では、臨終の供述は問題になる場合がほとんどないので、それ以外を見ると「考えもしないで思わず口から出た言葉は、意外と真実なことが多い」という経験則に基づくものである(ただ、「感情表現の供述」とは、好き嫌いの「感情の認定」にしか使えない。)

×例:C 専務は、事件前に口癖のように「V社なんかサーバクラッシュで潰れてしまえ」と言っていました(犯行前の単なる好悪感情の日常的表現の供述で具体性がない。)

○例:不正アクセスがあったころ、C 先輩は「アナを決めた。V 社に恥をかかせやる!」とサーバールームのアドミン席で叫んでいました(犯行時にセキュリティホールを突い

たという具体的事実を 推測させる衝動的供述で、動機をも推測させる感情的表現につながっている。))。

○例：徹底否認している犯人は、実は逮捕されたときに思わず「えっ！この程度やったことで俺を逮捕 するんですか！」と叫んでしまった(犯行後の検挙時に動揺驚がくした衝動的供述で、犯行を自認する内容を含んでいる。))。

(4) 自白法則

これが有史以来、刑事裁判で一番議論された証拠ルールである。古くは拷問による虚偽自白の強要であり(人権侵害の歴史：刑訴法 319 条参照)、21 世紀では、逆に、「犯人の意図的な虚偽自白によって捜査がかく乱される」点も見逃せない。例えば、「本人が認めているんだから間違いないじゃないか！」という専務の「誤」裁断で、犯人と思われた従業員 A を依願退職で追放したら、実は、真犯人は従業員 B で、たまたま転職を考えていた A が、行きがけの駄賃とばかり、親友 B の罪を引っ被って会社を辞めたという例がある。

もっとも、怖いのは、自白書、上申書、顛末書、自供書、告白書……と称する犯罪を認めた署名押印のある書類が捜査機関に持ち込まれ、当の本人が犯罪を否認しているときである。会社の上司や家族さらには地域社会住人が、義理人情や取引によってたかって、内容虚偽の自白供述書を無理矢理作成させた例も少なくない。

歴史の教訓：自白だけで不利益な処分をしてはならない(自白補強法則)
強制された自白は証拠として採用してはいけない(自白排除法則)

2 供述証拠の信用性(証拠の実質的価値判断)

(1) 自然かつ合理的で「もっともだ」という内容(×不自然・不合理)

○例：自分の失敗談(不利益な事実の供述：刑訴法 322 条参照)

×例：自己に有利な供述(新入社員のセールストークを想起されたい)

(2) 供述が一貫している(×供述がコロコロ変遷する)

○根拠：真の記憶は作為を要しないから何時でも同一の内容を繰り返せる

×根拠：嘘は供述が変遷する(嘘吐きは記憶力がよくなければならない)

(3) 裏付け証拠があり、他の証拠と符合する(×他の証拠と矛盾している)

裏付け証拠が得られた供述証拠なら伝聞供述でも、裁判所は供述の信用性を認める。

例えば、女性従業員 B から「A さんが集金チョコまかして使い込みしています。彼から旅行先で聞きました。」との訴えがあって調べてみたら、A が得意先数社から集金したはずの現金が経理に納金されていないことが帳簿上判明したような場合である。そして、A さんと B さんの不倫旅行の写真とホテルの領収書まで出てきたら完璧である(弘兼憲史著『部長島耕作9巻』(モーニング KC)参照)。

(4) 最良の裏付け証拠は、客観証拠である(刑訴法 323 条参照)。

ア 公文書(外国政府を含む)

- ・出入国記録、議員会館入退館記録、免許取得更新履歴
- イ 業務文書(業務日誌、帳簿や伝票)
 - ・ATM ジャーナル(入出金伝票)、パスモの入出場記録
- ウ 証拠物(証拠写真、チケット、領収書)
 - ・防犯カメラ画像、高速道路通行券、医療保険自己負担領収書
- エ 機械が自動的に作成するもの(コンピュータ・ログ、通信履歴)
 - ・サーバ・アクセスログ、ISP 接続ログ、携帯電話の発着信記録

3 事情聴取と信用性判断の具体例

(1) 供述の信用性判断としての裏付け調査

- ア 裏付け可能な事項は徹底した裏付け調査(ウラトリ)を行う。
 - 供述には裏付けがないと信用されないと思うこと。
 - 「ジャーナリストは自分の母親が『愛している』と言っても裏を取れ」
- イ 裏付けは供述でもいいが証拠物や客観証拠がベターである。
- ウ 裏付け事実のさらなる裏付け(ウラのウラ)はベストである。

(2) 供述の信用性吟味は、具体性と合理的な理由の有無である。

× 娘「パパ大好き、なぜって、だってパパだもん」(理由不備)

△ 娘「だってパパは
おもちゃ買ってくれるし
遊園地連れてってくれるし
オイタしてもママに言いつけないから」

(抽象的事実の供述・現在形の供述)

○ 娘「だってパパは
このおもちゃ買ってくれたし
昨日、遊園地連れてってくれたし
お皿割ってもママに言いつけなかったもん」

(具体的事実の供述・過去形の供述)

(3) 以上の総合例

- ア 供述の裏付け証拠:おもちゃ、遊園地の半券、割れた皿
- イ 裏付けの裏付け:おもちゃ購入のレシート、遊園地のスナップ写真

■参考■刑事訴訟法(昭和二十三年七月十日法律第百三十一号)

第 319 条【自白の排除法則・補強法則】

- 1 強制、拷問又は脅迫による自白、不当に長く抑留又は拘禁された後の自白その他任意にされたものでない疑のある自白は、これを証拠とすることができない。

- 2 被告人は、公判廷における自白であると否とを問わず、その自白が自己に不利益な唯一の証拠である場合には、有罪とされない。
- 3 前二項の自白には、起訴された犯罪について有罪であることを自認する場合を含む。

第 322 条【被告人の自白の証拠能力】

- 1 被告人が作成した供述書又は被告人の供述を録取した書面で被告人の署名若しくは押印のあるものは、その供述が被告人に不利益な事実の承認を内容とするものであるとき、又は特に信用すべき状況の下にされたものであるときに限り、これを証拠とすることができる。但し、被告人に不利益な事実の承認を内容とする書面は、その承認が自白でない場合においても、第三百十九条の規定に準じ、任意にされたものでない疑があると認めるときは、これを証拠とすることができない。
- 2 被告人の公判準備又は公判期日における供述を録取した書面は、その供述が任意にされたものであると認めるときに限り、これを証拠とすることができる。

第 323 条【公文書等の特信書面】

前三条に掲げる書面以外の書面は、次に掲げるものに限り、これを証拠とすることができる。

- 一 戸籍謄本、公正証書謄本その他公務員(外国の公務員を含む)がその職務上証明することができる事実についてその公務員の作成した書面
- 二 商業帳簿、航海日誌その他業務の通常の過程において作成された書面
- 三 前二号に掲げるものの外特に信用すべき状況の下に作成された書面

G. デジタルデータの証拠化・同一性確認調査手続き報告書例

この報告書は、被害民間企業又は専門調査会社係員が、刑事手続きや民事裁判用に提出するための標準的な報告書のひな形モデル例である。具体的な被疑事件や民事訴訟の請求内容によって、記載データや記述内容に過不足が生じるので、提出前のドラフト段階で、警察(検察)や弁護士(民事訴訟代理人)のリーガルチェックを受けて、修正ないし補正してから正式版を起案するのが望ましい。

平成〇〇年〇月〇日(注1)

〇〇警察署長 殿(注2)

〇〇〇〇株式会社 技術調査部

〇〇監査士 〇〇 〇〇 (印) (注3)

デジタルデータの写し作成及び同一性確認調査報告書

第1 デジタルデータの写し作成日時場所等

- 1 作成日時 平成〇〇年〇月〇日……
- 2 作成場所 〇〇県……〇〇丁目〇番〇号 〇〇ビル 6 階
株式会社〇〇〇〇 〇〇支社データセンター
サーバ管理課 サーバルーム(注4)
- 3 作成者 当職及び補助者(弊社技術調査部 〇〇〇〇)
- 4 提供者 上記株式会社〇〇〇〇 〇〇支社データセンター
サーバ管理課長 〇〇 〇〇
- 5 作成物 上記サーバ管理課長〇〇〇〇が管理するサーバのうち、管理番号
LX-2305 のハードディスク内に蔵置されたユーザ番号 09ACBE が
使用する領域内の一切のデジタルデータの写し(注5)
- 6 5の内容 コピーした写しを記録した DVD-R(表面に当職の署名・押印と
「09ACBE の写し」と記載されたもの)のとおり

第2 入手状況

- 1 上記提供者〇〇は、写しを作成する際に、当職に次のとおり申し立てた。
・ユーザ番号 09ACBE が管理・使用している「〇〇〇〇. 〇〇〇」等のデジタルデータ
は、当社が管理するサーバのうち、LX-2305 のハードディスク内のディレクトリ
「09ACBE」内にある。

- ・上記ハードディスクは、他のユーザも現に使用しているので現物の提出が困難である。
- ・上記電子ファイル「〇〇〇〇. 〇〇〇」等のデジタルデータが在中するサーバのハードディスクの提供(提出)に替えて、上記電子ファイル「〇〇〇〇. 〇〇〇」等のデジタルデータの写しを提出(提供)させていただきたい。

これは、当社代表取締役も了承済みである。(注 6)

- 2 当職は上記サーバを構成するハードディスク自体の提供(提出)を受けると、上記会社の業務に重大な支障が出ると判断し、その提供に替えて上記ディレクトリ内のデジタルデータの写しの提供を受けることとした。

そこで、当職は、上記提供者の承諾を得て、上記会社の技術者の協力を得て、……の方法で、上記ディレクトリ内の全てのデジタルデータを DVD-R にコピーし、その DVD-R の筐体表面に油性サインペンを用いて「09ACBE の写し」との表題及び作成年月日時刻を記載した上、当職自身が署名押印した。(注 7)

- 3 その後、上記 DVD-R 内のデジタルデータと上記ディレクトリ内のデジタルデータをハッシュ値を用いて同一性検査を実施したが、両者のハッシュ値が一致したので、両者は同一性を有するデジタルデータであることが確認された。(注 8)

そして、上記提供者は、両ハッシュ値が同一であることを確認してから、当職の求めに応じて、その旨を上記 DVD-R の筐体部分に油性サインペンで付記した上で、「立会人(提供者)」として署名押印した。(注 9)

第3 その他参考事項

本件作成・入手にかかるデジタルデータの写しは、別添上記 DVD-R のとおりである。(注 10)
なお、サーバの所在地(第1中の「2作成場所」)は、サイバーテロ対策で本来的に極秘であるため、本書の開示に際しては、特段の厳重な保秘の措置(例えば、サーバ所在地情報のみ黒塗りマスキング等)をとられることを、本書をもって関係機関に申し入れる。(注 11)

以上

※ コピーメディア(DVD-R 等)筐体部への記載例(注 7)

09ACBE の写し

2012 年 4 月 1 日 17 時 15 分

当職がサーバから写しを作成して同一性を確認した。

(作成者・同一性確認者) 作成監査士 〇〇 〇〇 (印)

本職が提供した原本データと写しの同一性確認に立ち会った。

(提供者・立会人) サーバ管理課長 〇〇 〇〇 (印)

- (注1)作成年月日は、デジタルデータの写しを作成した日ではなくて本件文書を作成した日を記載すること。
- (注2)あて先は省略しても構わないがなるべく記載した方がよい(上司宛でよい)。
- (注3)官民間問わずデジタル・フォレンジック関係の資格は、肩書に付記しておくといよい。尚、作成者の朱肉による押印を忘れないこと(印影印刷は不可)。
- (注4)場所は正確に部屋まで特定すること。
- (注5)オリジナルのデジタルデータの存在場所は、ハードディスクやサーバコンピュータの管理番号等のユニーク名称で特定し、一部の写しを作成する場合には、パーティションやディレクトリ単位(又はファイル名)まで特定すること。
- (注6)刑事裁判で「写し(コピー)」が証拠能力を確実に取得するためには、原本の提出が不可能又は著しく困難であることの疎明が必用である(最高裁決定昭和 35 年 2 月 3 日・最高裁判例集 14 巻 1 号 45 頁、最高裁判決昭和 35 年 3 月 24 日・最高裁刑事判例集 14 巻 4 号 447 頁)。
- (注7)写しを「いつ」「だれが」「どのようなものを」作成したかを必ず筐体表面に記載すること。手続過程の保全と同時に、写しの内容が正確にコピーされているという信用性の問題でもある。また、写しを作成したメディアを特定するため、メディアの筐体部分には、油性サインペンで、本文記載の作成年月日と表題を付して作成者の署名押印し(筐体に直接記載が困難なら付箋紙の上に全て記載し、付箋紙の裏面に両面シールを貼って筐体部分に貼り付けること)、その上から粘着糊付きラッピングシール(ラミネートフィルム等)を貼って固定するとよい。
- (注8)簡単なファイルを幾つかコピーするだけなら、FC(ファイル・コンペア)コマンドでもよい。
- (注9)「第三者たる提供者(デジタルデータ管理人)が立会人として原本との同一性を認証した」という法的意味がある。
- (注 10)法執行機関では、必ず写しメディアを2部作成し、1部はそのまま保管して不測の事態に備え、もう1部を使ってデータ解析をするように教育されている。
- (注 11)サーバ所在地等の機密情報の非開示(又は「インカメラ」:非公開で裁判官と弁護士と検事だけが証拠を見聞できる取調べ)を求める場合は、特段の必要性がある合理的理由を明記すること。

以上

H. 主要なデジタル・フォレンジック調査・解析用ツール(ソフト)

No.	ツール名	国内取扱店／製造・供給元	ツールの特徴や概要
1	Autopsy	ベイス・テクノロジー株式会社 https://www.basistech.jp/solutions/autopsy/Autopsy https://www.autopsy.com/download/	オープンソース GUI で操作しやすいのが特徴。Basis Technology 支援のもと、世界中の何千人ものユーザーと開発者で構成されているオープンソースコミュニティで開発されたソフトウェアで、誰でも無料で利用できる。 ☆「日本語処理解析性能評価」受検製品 2018.3.20:「Autopsy (Ver.4.6.0)」
2	AXIOM / IEF [Internet Evidence Finder] (Magnet Forensics)	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/2206/ https://cyberforensic.focus-s.com/product/96/ MagnetForensics.inc https://www.magnetforensics.com/	ウェブブラウザの履歴や SNS、クラウド、メッセージチャット履歴、ウェブメールカテゴリごとに抽出したデータを表示してくれる。IEF は、強力かつユーザーフレンドリーなフォレンジックツールで、直感的なユーザーインターフェースにより、どんなレベルの方でも簡単に重要な証拠を発見することが出来る。 AXIOM は、IEF 従来の解析機能やデータ共有機能に加え、データ抽出機能を標準搭載し、データ抽出および解析を自動で行うことが出来るようになった IEF の上位版。
3	Arsenal Image Mounter	Arsenal Recon https://arsenalrecon.com/products/	Arsenal Image Mounter は、ディスク イメージの内容を Windows の完全なディスクとしてマウントするツール。Windows に関する限り、アーセナル イメージ マウントによってマウントされるディスク イメージの内容は実際の SCSI ディスクであるため、ユーザーはディスクマネージャとの統合、ボリューム シャドウ コピーへのアクセス、仮想マシンの起動など、ディスク固有の機能を利用できる。
4	analyzeMFT	GitHub - dkovar/analyzeMFT https://github.com/dkovar/analyzeMFT	Python で書かれた Windows のアーティファクト \$MFT を解析するときに使用するオープンソースツール。NTFS(ファイルシステム)の \$MFT ファイルを解析する。

5	Belkasoft Evidence Center (Belkasoft)	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/belkasoft/ Belkasoft https://belkasoft.com/	Windows OS 対応メモリ取得ツール アンチダンピング保護をバイパスするように設計されている。パソコンからスマートフォンまで幅広い解析能力を持ち、著名なフォレンジックツールと連携して使用できる。また、本ソフトには、これからの時代に欠かせないメモリ保全用の無料ツール Live RAM Capturer が付属している。さらに、リモート機能によりターゲット端末のストレージとメモリの保全及び調査ができるため、国外に証拠端末がある場合のリモート捜査にも適している。
6	BlackLight / MacQuisition (BlackBag)	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/2393/ BlackBag Technologies https://www.blackbagtech.com/	WindowsOS のメモリ解析やシステムファイルの観点からの閲覧履歴の解析や、MacOS の APFS、Fusion Drive 等の Mac に特化した解析も可能なフォレンジックツール。MacQuisition は Mac Windows iOS GrayKey Android をサポートする保全ツール。Apple T2 チップを使用して Mac の物理イメージを作成する。BlackLight は取得したデータを解析するツール。この二つは合わせて使用したい。
7	Cain	Linux ディストリビューション https://www.caine-live.net/ https://cain-abel.updatestar.com/ja プロジェクトマネージャー Nanni Bassetti (Bari-イタリア)	CAINE はセキュアブートにも対応している Ubuntu ベースの Linux ライブディストリビューション。GUI でフォレンジック調査が可能、WindowsIR/Live フォレンジックツールも用意されている。カイン&アベルは、パスワード回復ツールで様々な種類のパスワードの回復をすることができ、パスワード解析(暗号化パスワードやハッシュ値をブルートフォースする等)やネットワークスニファ解析を行うツール。尚、アンチウイルスソフトからは「マルウェア」や「悪意あるプログラム」と判定される場合が多い。
8	CDIR Collector (Cyber Defense Institute Incident Response Collector)	株式会社サイバーディフェンス研究所 https://www.cyberdefense.jp/products/cdir.html GitHub - CyberDefenseInstitute/CDIR https://github.com/CyberDefenseInstitute/CDIR	Windows OS 用のファストフォレンジックツールで、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安全にデータを収集する。 多数の端末に感染または侵入の可能性がある、攻撃が現在も進行している可能性がある場合などに効果を発揮する。 CDIR-C で収集したデータは一般的なフォレンジックツールで読み込んで解析することが可能なため、自組織では証拠保全までを実施し、フォレンジック調査を外部のサービスベンダーに依頼することを想定している組織にも有効に活用できる。

9	DEFT (Digital Evidence & Forensics Toolkit) DART (Digital Advanced Response Toolkit)	Stefano Fratepietro https://n0where.net/digital-forensics-toolkit-deft (http://www.deftlinux.net/)	DEFT は、フォレンジック用 Linux ディストリビューションであり、Linux 上で Windows 用のツールを使用するために wine を用いている。DEFT は、Windows で実行可能なフォレンジックシステムであり、フォレンジックおよびインシデントレスポンスに最適なツールを含む DART とペアになっている。DART は、機器のロギングと整合性チェックを備えた GUI を備えている。USB に入れる軽量版の DEFT Zero というバージョンも存在する。
10	Email Auditor 19 (メール監査ツール)	株式会社 FRONTEO http://www.kibit-platform.com/products/email-auditor/	監査官の調査観点を学習した AI が大量の電子メールを解析し、要監査メールを優先度順に自動抽出するメール監査システム。強力な検索システムとの併用も可能で、監査業務の工数を大幅に削減するとともに、内在するリスクの可視化も可能。
11	EnCase (OpenText)	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/63/OpenText https://www.opentext.jp/products-and-solutions/products/security/encase-forensic	証拠保全から調査解析、報告まで可能な統合フォレンジックツールで、APFS やモバイルデータの取得も可能。NIST 等の第三者機関から信頼性を検証されており、法執行機関、民間を問わず幅広く利用されている。裁判での使用例も多岐に渡る。
12	Eric Zimmerman ツール	Eric Zimmerman https://ericzimmerman.github.io/#!index.md	SANS のトレーナーでもある Eric Zimmerman 氏が開発している Windows 用フォレンジックツール群で、どのツールも同じように使用でき使いやすい。新しいバージョンへの対応も早い。
13	Event Log Explorer	FSPRO Labs https://eventlogxp.com/jap	Windows のイベントログを解析するためのツール。複数 PC のログを集中管理する機能もある。個人使用の場合無料で使用できるが商用の場合は有料となる。イベントログを見る際のフィルターリングや検索が便利。
14	Final Forensic / AndrEx (AOS)	リーガルテック株式会社 https://www.fss.jp/aos-ファイナルフォレンジック/	完全日本語ユーザーインターフェースによるパソコンデータの保全・解析・調査ツール。対応 OS は、Windows7、Windows10。 強力なデータ復元機能と高度な検索機能を備え、データ保全、復元、分析、検索を行い分析レポートを作成する。警察、検察などの捜査機関で実績を上げている専門調査ツールで、専門家が行う高度な作業を非常に簡単なインターフェースで操作することが可能。 ☆「日本語処理解析性能評価」受検製品 2018.9.28:「Final Forensics (Ver.4)」

15	F-Response	Agile Risk Management LLC F-Response https://www.f-response.com/software	F-Response は、ソフトウェアユーティリティで、調査者は、選択したツールを使用して IP ネットワーク上でリモートにより物理マシン(ディスク、RAID、ボリューム、メモリ)及びクラウドストレージプロバイダーへの直接の読み取り専用のアクセスを提供するように設計されている。フォレンジック、e ディスカバリ(電子情報開示)、インシデントレスポンス用のデータ検出・収集アプリケーション。
16	FTK [Forensic Tool Kit] (AccessData)	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/87/ AccessData https://accessdata.com/products-services/forensic-toolkit-ftk	GUI のデータ収集、解析ツール。フォレンジックの各過程に応じた機能を搭載したツールを、パッケージソフトウェアとして提供しており、保全やファイル、レジストリ等の解析、暗号化やパスワード解析等目的に応じた対応することが可能。
17	FTK Imager Lite , FTK Imager	Access Data https://accessdata.com/product-download/ftk-imager-lite-version-3-1-1	イメージのマウントやディスクイメージの作成、メモリの保全も可能な無償ツール。FTK Imager は、PC へのインストールを必要とし、FTK Imager Lite は、インストールすることなく使用できる。両者ともメモリダンプの取得も可能となっている。
18	Ghidra (NSA)	米国国家安全保障局(NSA) https://www.nsa.gov/resources/everyone/ghidra/ https://ghidra-sre.org/	NSA(アメリカ国家安全保障局)が開発したリバースエンジニアリングのためのツール群。GHIDRA は、GUI ベースの逆アセンブラで、実行ファイルのバイナリからソフトウェアやマルウェアを解析し、人間にも解読可能なアセンブリ言語に変換してくれる。「GHIDRA」は Java でコーディングされ、Windows・macOS・Linux・Android・iOS で動作する。
19	Griffeye	Griffeye Technologies https://www.griffeye.com/	Griffeye Analyze は、デジタルメディア調査用の汎用ソフトウェアプラットフォームで、Analyze DI Pro には 90 日間の無料トライアル期間がある。グリフィー・インテリジェンス・データベースを使用すると、異なるスタンドアロン・データベースを介して接続することにより、国際的に、全国的に、地区間およびチーム内でインテリジェンスを共有することができる。

20	HX-Recovery for DVR & NVR	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/hx-recovery/	HX-Recovery は、監視カメラや防犯カメラ装置の動画再生や削除された映像を簡単に解析できるフォレンジックツール。監視カメラや防犯カメラ装置の多くは、中国や韓国のメーカーが大半を占めており、この中には世界的に有名なメーカー製品から、OEM 等、各国で無名のメーカー製品となるものまで様々なため、今まで扱いが大変だった証拠動画の再生が簡単にできるようになる。
21	IDA Pro (Hex-Rays)	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/176/Hex-Rays https://www.hex-rays.com/products/ida/	マルウェア解析、プログラムの脆弱性調査などに用いられる機能が豊富なクロスプラットフォームのマルチプロセッサで、逆アセンブラ及びデバッグができ、コンパイラ生成コードとユーザー記述コードを自動峻別し、表示することができる。
22	Intella	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/intella/Vound Colorado https://www.vound-software.com/	Intella は、重要な証拠データを容易に見つけ出す強力なフォレンジックサーチツール。ストレージの進化で削除したデータは技術的に探せなくなり、膨大な既存データから証拠を探さなければならないが、Intella は、対象データの検索結果を視点を変えて確認でき、データと人、データと組織の関係を簡単に可視化できる。 本製品は、デジタル・フォレンジック研究会(IDF)による 2019 年実施の「日本語処理解析性能評価」で高いスコアを獲得している。 ☆「日本語処理解析性能評価」受検製品 2017.12.15:「Intella Professional (Ver.2.0.1)」 ☆「日本語処理解析性能評価」受検製品 2019.3.8:「Intella Professional (Ver.2.2.1)」
23	Kansa	davehull kali.org https://github.com/davehull/Kansa	Windows マシンを対象とした PowerShell ベースのインシデントレスポンス用フレームワーク。WinRM を利用することで、数千台規模のリモート端末のデータ収集が可能となる。
24	KIBIT Automator(AI ツール)	株式会社 FRONTEO https://legal.fronteo.com/products/kibit-automator/	ドキュメントレビューに用いられる業界スタンダードツールである Lit i View、Relativity に実装可能なプラグインツール。AI を用いた、Assisted Learning、Heat Map、ハイライト機能等により、ドキュメントレビューの劇的な高速化、高品質化、コスト削減を同時に実現可能。

25	Kali Linux	kali.orgOffensive Security https://www.kali.org/downloads/	ペネトレーションテストを目的とした Linux ディストリビューションで、フォレンジックツールや解析ツールも多く含まれている。脆弱性診断のため疑似攻撃をするために使われている。
26	LACE	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/209/ BlueBear LES https://bb-les.ca/solutions/	画像・動画解析用ツール。他のファイルに埋め込まれた画像、動画ファイルの抽出を行うとともに、重複ファイルの削除や顔認証を通じて効率的に画像のレビュー、分類が可能。
27	Lit i View E- DISCOVERY(データ 解析ツール)	株式会社 FRONTEO https://legal.fronteo.com/products/e-discovery/	e ディスカバリの世界標準である EDRM に準拠し、全作業をワンストップでサポートする。英語はもちろんアジア各国に特有のアプリケーションや文字コードにも広く対応し、e ディスカバリ支援に必要な全機能及び AI を搭載したスタンダードツール。 ☆「日本語処理解析性能評価」受検製品 2017.1.19：「Lit i View E-DISCOVERY (Ver.7.12.203548)」
28	Lit i View XAMINER(データ解 析ツール)	株式会社 FRONTEO https://legal.fronteo.com/products/xaminer/	豊富なフォレンジック調査経験で蓄積された知見やノウハウをベースに独自開発された、AI 搭載データ解析ツール。AI による自動仕分け機能や相関関係作成機能、アジア言語への対応力からなる高精度な検索能力、高度なメール解析機能は、調査の高速化に寄与する。メールの会話内容から人物の行動を分析する Central Linkage などの機能がある。 ※官公庁限定販売製品
29	Log Parser(Lizard)	Lizard Labs Software http://www.lizard-labs.com/log_parser_lizard.aspx	Microsoft LogParser に GUI を提供するツールで、SQLクエリを利用してレジストリ、ファイルシステム及び Active Directory サービスのログを解析する。ログファイル、XML ファイル、CSV ファイル等のテキストベースのデータへのユニバーサルクエリアクセスと、イベントログ、IIS ログ等の Windows OS上の主要なデータソースへのユニバーサルクエリアクセスを提供する非常に強力な自由で汎用性が高い。

30	MacQuisition	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/2415/	MacQuisition CFC Edition は、Targeted Data Collection/Live Data Acquisition/Forensic Imaging と用途に応じた柔軟な保全に対応した 3-in-1 ソリューション。10 年以上の経験豊富な調査官がテストし使用している本製品は、MacOSX 上で動作する。FusionDrive[SSD+HDD]含む 185 種類以上の MacPC から安全に起動し、データを取得することができ、Mac の複雑な分解を行わず USB ブートにより保全を行うことができる。
31	Magnet RAM Capture	MagnetForensics.inc https://www.magnetforensics.com/resources/magnet-ram-capture/	MAGNET RAM キャプチャは、容疑者のコンピュータの物理メモリをキャプチャするように設計された無料のメモリキャプチャツールで、メモリ内でのみ見つかる貴重なアーティファクトを復元および解析できる。キャプチャーしたメモリデータは、raw 形式でエクスポートされる。 最新バージョン:v1.20(2019 年 7 月 24 日リリース) -仮想セキュアモードが有効になっている Windows 10 システムからの RAM 取得をサポートできるようになった。
32	Magnet ACQUIRE	MagnetForensics.inc https://www.magnetforensics.com/products/magnet-acquire/	iOS、Android、ハードディスク、リムーバブルメディアからイメージを取得するためのツール。ACQUIRE は、信頼性の高い高速抽出と直感的なユーザーインターフェイスを兼ね備えており、データを迅速かつ簡単に提供でき、取得するデータの品質が最大化され、アクティビティログとドキュメントを使用して、使用されたメソッドを理解できる。
33	MSAB Office(モバイルフォレンジックツール)	株式会社 FRONTEO https://legal.fronteo.com/products/msab/MSAB https://www.msab.com/ja/	モバイルフォレンジック用オールインワンプラットフォームで、WindowsPC 上で起動するように設計されている。20,000 以上の機種に対応し、最大 3 台同時に端末内のデータ抽出が可能。データ抽出ツールである「XRY」に加え、データ解析用ソフトウェアである「XAMN Spotlight」もバンドルされた、オールインワンのモバイル端末フォレンジックツール。
34	NetHunter	kali-nethunter-project Kali Linux NetHunter https://www.kali.org/kali-linux-nethunter/	Nexus や OnePlus デバイスのための Android 用モバイルペネトレーション用プラットフォームで、HID Keyboard Attacks、BadUSB attacks、Evil AP MANA attacksなどをサポートしている Android ROM オーバーレイ。NetHunter は、Offensive Security とコミュニティが開発するオープンソースプロジェクト。

35	Nuix Workstation	Nuix Japan https://www.nuix.com/jp/products/nuixworkstation	膨大なデータを短時間で処理でき、大量の非構造化データ、半構造化データ、そして構造化データを処理し、情報を抽出できる。スピード、規模、そして正確さでデータを処理、検索、インデックス化し、法執行調査、規制対応調査、企業不正調査、情報ガバナンスなどの調査を支援する。
36	Nuix Investigate	Nuix Japan https://www.nuix.com/jp/products/nuixinvestigate	ケースデータをいつでもどの Web ブラウザーからでも、共有、検索、分析できる共同作業で解決する環境を提供する。強力な可視化によって、主要人物が誰なのか、また何をしているかが一目で分かるため、情報に基づくより優れた決定をより迅速に下すことができる。 ※「日本語処理解析性能評価」受検製品 2018.6.29:「Nuix investigation&Response (Ver.7.4.5)」→再評価実施予定
37	Nuix Discover	Nuix Japan https://www.nuix.com/jp/products/nuixringtail	エンド・トゥ・エンドの e ディスカバリ(証拠開示)を提供するツールで、プロセッシング、レビュー、分析、プレディクティブ・コーディング技術が統合され、より良い証拠を迅速に解明できる。訴訟や規制案件への戦略に速やかに取り組める。
38	Oxygen Forensic Detective	株式会社サイバーディフェンス研究所 https://www.cyberdefense.jp/products/oxygen.html Oxygen Forensics, Inc. https://www.oxygen-forensic.com/en/	直感的な操作が可能なスマートフォンやタブレットの調査に特化したモバイルフォレンジックツール。12,000 種類以上のデバイスをサポート。 iOS デバイスや Android デバイスを始めとしたスマートフォンを対象にデータ抽出、アプリケーションデータ解析、位置情報解析、コミュニケーションの可視化、実用的なレポート(PDF/Excel 等)の出力までスマートフォンの調査に必要な機能を網羅している。また、クラウドサービスにも対応しており、主要なクラウドサービスからのデータ取得、解析が可能。デバイス単体の解析だけでなく、複数のデバイスから収集したデータを統合して解析できる「Communication Statistics」機能は、犯罪捜査の効率を飛躍的に向上させる。 ※官公庁、法執行機関のお客様のみへの販売となる。

39	PassWare Kit	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/192/Passware Inc https://www.passware.com/	コンピュータ上のあらゆるパスワードや暗号化で保護されたファイルを検知し、それらを復号する、コンピュータ・フォレンジックにおける優れたパスワードリカバリソフトウェア。メモリ内からのパスワード抽出にも対応。
40	PC-3000	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/pc3000/ ACE Lab https://www.acelaboratory.com/	障害を抱えた HDD や SSD、NAND メモリ製品からデータを抽出できるフォレンジックツールで、異音を発する HDD でも各メーカー用に搭載された豊富な特殊コマンドで異常動作を制御することができる。また、SSD のファームウェア障害、破壊されたメモリ製品など使用不可の記憶媒体の調査や近年普及しているデータが自動で消失する SED 仕様のストレージの証拠保全も対応できる。
41	Phone Breaker (Elcomsoft)	ElcomSoft Co. Ltd https://www.elcomsoft.jp/eppb.html	iOS、Windows Phone、Windows10 Mobile、および BlackBerry10 を実行しているデバイスから情報を抽出し、ハードウェアアクセラレーションを使用してバックアップを復号化し、パスワードを取得するツール。
42	Paladin Linux / RECON (SUMURI)	SUMURI https://sumuri.com/software/paladin/ https://sumuri.com/software/recon-triage/	Ubuntu ベースの Linux ライブディストリビューション。RECON LAB は、Mac 上で動作し、他のフォレンジックツールで見逃されたデータのリカバリを可能にする。Windows、Mac、Linux、iOS、アンドロイド、グーグルテイクアウト自動分析もできる。
43	Plaso	GitHub - log2timeline/plaso https://github.com/log2timeline/plaso	plaso は、Python で実装されたスーパータイムラインを生成するツールのためのバックエンドエンジン。
44	RECON IMAGER	株式会社 FRONTEO (Web サイト問い合わせフォーム) https://legal.fronteo.com/contact/ SUMURI https://sumuri.com/software/recon-imager/	外部ブートプログラムによる、Apple 社製 PC 用証拠保全ツール。T2 チップ搭載機・APFS ファイルシステムストレージからの論理イメージ形式 (Spareimage) でのデータ取得も可能で、ローカルタイムマシースナップショットも論理イメージに内包する形で取得可能。

45	RECON LAB	株式会社 FRONTEO(Web サイト問い合わせフォーム) https://legal.fronteo.com/contact/ SUMURI https://sumuri.com/software/recon-lab/	Mac OS/iOS/Windows OS 等の解析が可能な、フォレンジック用解析ソフトウェア。Apple Metadata の自動抽出機能、解析対象データのスーパータイムライン作成機能、アーティファクトの自動分類機能等、調査の効率化と高速が可能となる様々な機能を実装している。RECON LAB には、あらゆるタイプのデータに対して統合されたビューアが含まれている。さらに、SQLite ビューアなどの高度なビューアを使用すると、RECON LAB 内で SQLite クエリを実行して高度な分析とレポートを作成できる。
46	Redline	FireEye, Inc. https://www.fireeye.jp/services/freeware/redline.html https://fireeye.market/apps/211364	ホスト調査を実施するための無償ツール。メモリやファイルを解析し、セキュリティ脅威の診断プロファイルを作成して、不正な活動の痕跡を特定する。
47	Rekall	GitHub - google/rekall https://github.com/google/rekall	分析しているのと同じプラットフォーム上で実行するように特別に設計された唯一のメモリ分析プラットフォームで、Python で実装されたメモリフォレンジック用無償ツール。Windows は、XPから10まで、Linux は、カーネル 2.6.24 から最新まで、Mac OS X は、10.7-10.12.xまで幅広くサポート。
48	ResponderPro	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/168/	物理メモリの解析を行い、稼働中のプロセスの機能に応じて、独自の DDNA を用いたスコアリングを行い、従来のアンチウィルスソフトでは検知できなかったマルウェアを探し出すメモリ解析ツール。
49	SIFT Workstation (SANS)	SANS.orgSANS Digital Forensics and Incident Response https://digital-forensics.sans.org/community/downloads	SANS の提供する ubuntu ベースの Linux ディストリビューションである SIFT ワークステーションは、様々な設定で詳細なフォレンジック検査を実行するように設計された無料のオープンソースインシデント対応とフォレンジックツールのグループ。インシデント対応で各種のフォレンジックツール群に連携させることができる。SIFT は、高度なインシデント対応機能と侵入に対する詳細なデジタルフォレンジック技術を、自由に利用でき、頻繁に更新される最先端のオープンソースツールを使用して実現できることを示している。

50	Simple SEIZURE TOOL for Forensic(S STF) Simple SEIZURE TOOL for Android(S STA)	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/sst/ https://www.kumanan-pcnet.co.jp/forensic/ssta/	SSTF は、国内特許(特許第 6559984 号)を取得した次世代のフォレンジックツールで、急速に増加しているマザーボードにメモristoreージが直接実装されているため分解困難なパソコンやタブレット端末等に対して、パソコンに接続し電源を入れるだけでパソコンや分解困難な電子端末、稼働中のサーバーデータまで幅広く簡単な操作で証拠保全ができるようになる。 SSTA は、スマートフォンを簡単に保全できるフォレンジックツールで、端末のスクリーンショット機能を用いて自動で確実に保全でき、SNS の証拠画像などからテキストを抽出することが可能になる。これにより課題となっているスマートフォンの殆どが内部データを保全できなくなり、証拠となる画面をカメラで手動撮影せざるを得ず時間と労力だけを浪費する現状を改善できる。
51	Splunk	マクニカネットワークス株式会社 https://www.macnica.net/splunk/index.html/ Splunk Inc https://www.splunk.com/ja_jp/software/splunk-enterprise.html	様々な IT システムから生成されるデータの収集、検索、分析、可視化を行うデータ分析プラットフォームで、ログファイルやファイル時系列などのビッグデータを解析するためのツール。無償版もある。
52	Tsurugi (剣) Linux	つるぎ Linux チーム https://tsurugi-linux.org/	完全に無料のオープンソースプロジェクトによるツールで、DFIR 調査、マルウェア分析とオープンソースの INTelligence 活動をサポートするように設計された大幅にカスタマイズされた Linux ディストリビューション。このディストリビューションには、詳細なフォレンジックまたはインシデント対応調査を行うために必要なツールの最新バージョンと、カーネルレベルでのデバイス書き込みブロッキング、専用の Computer Vision 分析セクション、OSINT プロファイルスイッチャーなどの機能が含まれている。
53	TZWorks (の各種 パーサー)	TZWorks Limited Liability Company https://tzworks.net/about.html	有償ツール。レジストリ ハイブ、ジャーナリング ファイル、その他の重要なファイルなど、オペレーティング システムによってロックダウンされた分析を必要とするファイルは、クラスター レベルで生データを読み取ることによって調べることができる。このライブデータ収集は並列処理と組み合わせられ、生データを読み取り可能/使用可能な結果にほぼリアルタイムで応答側に変換し、データトリアージを実行できるようにする。

54	UFED 4PC (Cellebrite)	サン電子株式会社 https://www.sun-denshi.co.jp/ Cellebrite https://www.cellebrite.com/en/platforms/	スマートフォンからデータ抽出、デコード、分析するためのツールで、UFED 4PC は高コストパフォーマンスの一気に通貫システム。携帯端末や PDA 等数多くのモバイル機器に対応、アプリケーションソフトとしてコンピュータ(ノート PC・タブレット PC 含む)1 台でデータの抽出から解析までを可能にした。Logical 抽出が可能な標準モデルの「UFED 4PC LOGICAL」と Physical Dump、File System Dump まで兼ね備えたハイエンドモデルの「UFED 4PC ULTIMATE」がある。
55	UFED Mobilogy Touch	サン電子株式会社 https://www.sun-denshi.co.jp/df/mobilogy/ Cellebrite https://www.cellebrite.com/en/platforms/	持ち運び可能な UFED4PC のポータブル版スマートフォン用ツールで、世界中の携帯電話約 4,000 機種をサポート。携帯電話に保存された電話帳、写真、SMS メッセージ、ビデオ、オーディオファイル、着信音などのデータをほかの端末(多くの場合新たに購入した端末)に移行できる機能を持っている。また、データを USB メモリーや SD カードなどのローカルメモリーにバックアップしたり、保存したデータを他の端末に書き込むこともできる。
56	VFC5(Virtual Forensic Computing)	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/vfc/	VFC は、E01 や DD などの証拠イメージファイルを仮想起動できるフォレンジックツール。証拠イメージから実際のパソコンと同じ状態で起動させることができるため、使用していた環境をそのまま調査できるようになる。Windows パソコンにおいてはログインパスワードをバイパスできるため、押収したパソコンを起動することなく利用者像を確認できる。また WEB や SNS のログイン状態確認やリストアポイントを用いたマルウェア調査などにも最適。
57	Volatility Framework	volatilityfoundation.org The Volatility Foundation https://www.volatilityfoundation.org	無償のメモリフォレンジックツールで、動いていたプロセス、ネットワーク情報などメモリ上にしか残らない情報が得られる。AXIOM や EnCase など、Volatility のプラグインを持ち、同機能を使用するツールも存在する。

58	VizX (Ziuz)	株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/product/213/ZIUZ https://www.ziuz.com/ja/	児童に対する性的虐待の調査等に役立ち、画像や映像から Exif 情報などの抽出ができる画像・動画解析用ツール。しきい値以上の変化があった動画のみ集中的に表示することで、監視カメラ等の重要なシーンを見逃さず、短時間でレビュー可能。服の模様やタトゥーから同じ模様を持つ被写体を見つけ出す。PhotoDNA 技術を VizX2 に導入して画像を照合する機能が追加された。
59	X-Ways Forensics	株式会社ディアイティ https://www.dit.co.jp/products/xways/forensics/index.html X-Ways AG https://www.x-ways.net/	ドイツ製のフォレンジック解析ツールで、ウイルス感染、不正アクセス等のセキュリティインシデントが発生した際に、その証拠となるデジタルデータの取得を容易にするために開発された。コンピュータフォレンジックに必要とされるすべての機能を搭載し、ドリルダウン方式を採用することにより、専門家でなくても容易に利用できるように設計されている。RVS の機能が使い易い。 ☆「日本語処理解析性能評価」受検製品 2017.1.19:「X-Ways Forensics(Ver.19.0 SR-12)」

I. IDF団体会員「製品・サービス区分リスト」

(掲載51社、会社名・URL掲載7社)

このリストは、IDF団体会員企業でリスト掲載(公開)を希望された企業からの提供情報をIDFへの入会順で掲載しています。このため全ての団体会員企業を掲載しては ありません。

区分:①製品(ハード、ソフト)販売(フォレンジックに関連する製品)

②フォレンジック調査

a PC・サーバ等、 b ネットワーク機器等、 c 携帯電話・スマートフォン

d 記録デバイス等、 e その他

③ファスト・フォレンジック ④訴訟支援・コンサルティング ⑤eディスカバリ

⑥トレーニング・人材育成 ⑦ネットワーク監視・記録 ⑧データリカバリ、

⑨情報漏洩調査・脆弱性調査 ⑩サイバー・インシデント演習(フォレンジックを含む)支援

⑪ポリシー・組織構築支援(CSIRTその他) ⑫予兆把握・自動調査処理ツール等

⑬その他

注:製品・サービス区分リストの内容は、各社の責任においてご提供頂いた内容となります。

IDF団体企業名	サービス区分	主要製品等
株式会社フォーカスシステムズ https://cyberforensic.focus-s.com	①、②-a,c,d、 ③、④、⑤、⑥、 ⑧、⑪	・各種フォレンジックツール EnCase/FTK/IEF・AXIOM 等 ・Mac/iPhone(HFS+/APFS)解析・保全ツール BlackLight/MacQuisition ・HDD/SSD 保全・書込防止装置 Falcon-NEO/ Tableau/WriteProtectPortable ・携帯端末保全・解析ツール UFED シリーズ ・マルウェア解析 Responder Pro/IDA Pro/Shadow3 ・各種トリアージツール EnCase Portable/AD Triage ・公式トレーニング DF120/210/320/FTK/AXIOM ・フォレンジック調査・緊急対応サービス 他

IDF団体企業名	サービス区分	主要製品等
株式会社 FRONTEO http://www.fronteo-legal.com	①、②、③、④、 ⑤、⑥、⑦、⑧、 ⑨、⑪、⑫	・各種フォレンジックツール -Lit i View XAMINER 人工知能搭載レビューツール -MSAB Office(XRY/XAMN) モバイル端末データ抽出・解析ツール -UltraBlock 書き込み防止装置) 他 -RECON IMAGER MacOS 端末データ抽出・解析ツール ・フォレンジック調査トレーニング(9 コース) ・KIBIT Email Auditor 人工知能搭載 Email 監査ツール ・KIBIT Knowledge Probe 人工知能搭載データ分析支援システム) 他 ・フォレンジック調査サービス ・eDiscovery サービス
株式会社 NTT データ https://www.nttdata.com/jp/ja	④	・サイバーセキュリティ強化コンサルティング ・ログ取得状況アセスメント
株式会社ラック https://www.lac.co.jp	②、③、⑥、⑦、 ⑨、⑩、⑪	・緊急対応サービス「サイバー119」 ・マネージド・ディテクション・アンド・レスポンス (MDR) ・ラックセキュリティアカデミー フォレンジック・ ハンズオン トレーニング ・JSOC マネージド・セキュリティ・サービス(MSS) ・情報漏えいチェックサービス ・APT 攻撃耐性診断サービス「APT 先制攻撃」 ・セキュリティ診断 ・セキュリティコンサルティングサービス
デロイト トーマツ リスク サービス株式会社 https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/dtrs/dtrs-company-profile.html	②-a,b,c,d、③、 ⑥、⑦、⑧、⑨、 ⑩、⑪、⑫	デロイト トーマツ リスクサービスは、サイバーセキュリティ、IT ガバナンス、事業継続管理(BCM)等に関する多くの知見やノウハウ・実績に基づき、デロイト トーマツ グループと有機的に連携を図りながら、総合的に企業の IT 領域のリスク管理活動を支援します。また、サイバー領域においては、デロイトメンバーファームとの連携により、世界 20 か所以上に拠点を構えるサイバーインテリジェンスセンター(CIC)と連携し、各国で収集・分析した高度なサイバーインテリジェンスの提供によりクライアントのインシデントレスポンスに係る工数を低減します。

IDF団体企業名	サービス区分	主要製品等
株式会社ディアイティ https://www.dit.co.jp	①、②-a,b,d、 ⑥、⑦、⑧、⑨、 ⑩、⑪	・フォレンジックツール X-Ways Forensics ・ネットワーク解析ソフトウェア Savvius Omnipeek ・暗号化データ通信ソフトウェア Tectia SSH Client/Server ・サイバー情報パトロールサービス・脆弱性診断 ・トレーニング フォレンジック基礎、X- Ways ハンズオン ・インシデント対応 フォレンジック調査・ログ解析
株式会社オーク情報システム https://www.oakis.co.jp	①、⑦	・ネットワークフォレンジックサーバ 『NetEvidence Ax』の販売・開発
ネットエージェント株式会社 https://www.netagent.co.jp	②-a,b,c,d,e(IoT 機器)、③、⑧、 ⑨、⑩、⑪、⑫、 ⑬(IoT 機器、セ キュリティ診断 (自動車セキュリ ティ検査等)、 ゲームセキュリ ティ診断(チート 対策等))	・フォレンジック調査 ・ゲームセキュリティ(チート対策など) ・IoT 機器セキュリティ診断(自動車セキュリティ検査 など) ・P2P 調査サービス ・脆弱性診断サービス ・WAF ・ホワイトハッカーコンサルティング
株式会社ピーシーキッド https://www.pckids.co.jp	①、②-a,d、⑦、 ⑧、⑨	・コンピュータ・フォレンジック調査 ・ネットワーク・フォレンジック製品販売 ・データリカバリサービス ・ペネトレーションテスト ・その他デジタルデータに関するサービス
リーガルテック株式会社 https://www.aos.com	①、②-a,b,c,d,e (カーナビ、ド ライブレコー ダー、防犯カメ ラ、EDR、ドロー ン等)、③、④、 ⑤、⑥、⑦、⑧、 ⑨	・サービス フォレンジック調査サービス データ復旧サービス e ディスカバリーサービス ・フォレンジックツール販売/トレーニング/サポート Final Forensics(PC フォレンジック) AndrEx3(Android スマホデータ抽出) AOS Fast Forensics(PC ファストフォレンジック) AOS Professional(動画復元) AOS Enhancement(画像鮮明化) Nuix Investigation and Response(不正調査 支援 解析)

IDF団体企業名	サービス区分	主要製品等
ハミングハッズ株式会社 https://www.hummingheads.co.jp	①	エンドポイントセキュリティ「セキュリティプラットフォーム(SeP)」、アンチウイルスソフト「ディフェンスプラットフォーム(DeP)」、ソフトウェアロボット「AI Humming Heads (AIHH)」の販売など
株式会社サイバーディフェンス研究所 https://www.cyberdefense.jp	①、②、③、⑥、⑨、⑩	・Oxygen Forensic Detective(スマートフォン解析ツール) ・フォレンジック調査 ・マルウェア解析 ・ペネトレーションテスト ・サイバー演習の実施及びシナリオ作成 ・サイバーインテリジェンス ・各種ハンズオントレーニング ・コンサルティング、開発、調査研究 等
エンカレッジ・テクノロジー株式会社 https://www.et-x.jp	①	製品名:システム証跡監査ツール ESS REC 特徴:コンピューターのシステム操作を動画とテキストで記録し証拠として保全する監査ツール。不正防止・インシデント発生時の原因究明及び証拠保全として利用可能。導入実績 460 社以上
アイフォレンセ日本データ復旧研究所株式会社 https://www.daillo.com	①、②-a,c,d,e(ドライブレコーダーや防犯カメラの他、意図的に破壊されたり、故障した機器も調査可)、③、④、⑥、⑧、⑨	1. 破壊や故障した情報記憶媒体のデータ復旧 2. 消失したデジタルデータの解析調査及び復元 3. 事件捜査や内部不正調査でのフォレンジック調査 4. カメラやビデオの写真画像や映像動画の復元 5. 削除済みファイルの復旧及び削除経緯の調査 6. 他社対応不可案件のリトライ 7. データ保全複製ソフト及び機器の動作検証サービス 8. データ消去ソフト及び機器の消去性能検証サービス 9. HDD・SSD の構造及び動作仕様に関する技術 講義・トレーニング・講演 10. 現存するソフトウェアでの上書き消去が不可能なデータエリアとその部分の消去方法の研究 調査 他
サン電子株式会社 https://www.sun-denshi.co.jp	①、②-c,d、⑥	・Cellebrite UFED シリーズ(UFED Touch2、UFED4PC、UFED KIOSK、UFED Analytics) ・Cellebrite 公式トレーニング ・SASA Software 社 ファイル無害化システム『Gate Scanner』

IDF団体企業名	サービス区分	主要製品等
株式会社くまなんピーシー ネット https://www.kumanan-pcnet.co.jp	①、②-a,c,d、 ③、④、⑤、⑥、 ⑧	・WDR Forensic Solution フォレンジックサービス、ツール開発 Simple SEIZURE TOOL for Forensic (パソコン、タブレット証拠保全ツール) - Simple SEIZURE TOOL for Android (スマートフォン証拠保全ツール) - Intella (フォレンジック、レビュー、e ディスカバリ、日本語解析ツール) - Belkasoft (パソコン、スマートフォン対応フォレンジックツール) - HX-Recovery (監視カメラ／防犯カメラ解析、再生ツール) - VFC5 (証拠イメージ／証拠ディスク仮想起動ツール) - SecureAge (PKI 暗号、監視、APT 対策、情報漏えい対策ソフトウェア) ・PC-3000 JAPAN (HDD、SSD、NAND メモリデータ復旧ツール、トレーニング) ・WinDiskRescue (WD 公認データ復旧サービス、証拠品鑑定)
三井物産セキュアディレクション 株式会社 https://www.mbsd.jp	②、⑨、⑪	・フォレンジック調査 ・マルウェア解析 ・感染調査 ・情報漏洩調査サービス ・CSIRT 構築支援
NTT データ先端技術株式会社 http://www.intellilink.co.jp	①、②、③、④、 ⑦、⑨、⑩、⑪	・セキュリティ・インシデント救急サービス ・CSIRT/SOC 構築支援/運用支援サービス ・脆弱性情報配信サービス ・サイバー攻撃対応演習(机上演習・技術演習)サービス ・セキュリティコンサルティングサービス、セキュリティ監査サービス ・不正アクセス監視サービス、標的型攻撃検知・解析サービス、セキュリティログ評価サービス ・セキュリティ診断サービス、脆弱性診断・管理サービス ・インテリジェントログ管理製品、セキュリティイベント管理 (SIEM)製品、EDR 製品 ・情報漏えい対策ソフト、改ざん検知ソフト、統合型 ・PC 暗号化ソフト 他

IDF団体企業名	サービス区分	主要製品等
株式会社 KPMG FAS https://home.kpmg.com/jp/ja/home/about/fas.html	②-a,b,c,d、③、④、⑤、⑥、⑦、⑧、⑨、⑩、⑪、⑫	フォレンジック調査 情報セキュリティ脆弱性調査 e-Discovery(Relativity、Nuix) 他
P.C.F. FRONTEO 株式会社 https://www.pcf.co.jp	②、③、④、⑨、⑪	・PCI Forensic Investigators (PFIs)認定調査 ・クレジットカード他ペイメントカード情報漏えい調査サービス ・PCIDSS 準拠業務支援サービス ・WEB アプリケーション診断サービス ・プラットフォーム診断サービス ・情報セキュリティ診断サービス
DATA HOPE 東北データ復旧(有限会社コミュニティアイ) https://www.datahope.jp	②-a、⑧、⑨	・データ復旧 ・デジタル・フォレンジックサービス
株式会社ワイ・イー・シー https://www.kk-yec.co.jp	①、②-a,c,d、③、⑤、⑥、⑦、⑧、⑨	・捜査支援/証拠保全ツール -DemiYG シリーズ(HDD コピー機) -PCAIDIV(HDD 書込防止装置) -USB3.0WriteProtector(USB 書込防止装置) -Mobiledemi(スマートフォン初動捜査支援ツール) -Evidencetracer(フォレンジック初動捜査ソフトウェア) -Evidencetracer EX(マルウェア等調査支援用ソフトウェア) -データ復旧サービス(物理/論理/オンサイト) -フォレンジック調査サービス -電波遮断シールド BOX/バッグ -データ消去サービス(センドバック/オンサイト)
PwC サイバーサービス(同) https://www.pwc.com/jp/cybersecurity	②、⑥、⑨、⑩、⑪、⑫	デジタル・フォレンジック 脆弱性診断 ペネトレーションテスト レッドチーム演習 インシデントレスポンスアドバイザリー インシデントディテクション&リカバリー CSIRT/SOC 構築支援

IDF団体企業名	サービス区分	主要製品等
SecureWorks Japan 株式会社 https://www.secureworks.jp	②-a・b・d、⑦、 ⑨、⑩、⑪、⑫	マネージド・セキュリティサービス(セキュリティ監視による検知機能の強化、インシデント対応との連携等) セキュリティコンサルティング(CSIRT 構築支援、CSIRT の有効性を実証するレッド・チームテスト等) インシデント管理&レスポンスサービス(インシデントレスポンス、マルウェア解析、システム・ネットワーク脆弱性診断、標的型攻撃対応訓練、標的型攻撃ハンティング) インシデント対応を迅速に行う為の事前契約を頂くことで事故発生時の初期対応をより迅速に行うことが可能です。
デロイト トーマツ ファイナンシャルアドバイザリー合同会社 https://www2.deloitte.com/jp/ja/pages/risk/solutions/frs/forensic.html	②、③、④、⑤、 ⑥、⑨	デジタル・フォレンジックを用いた電子データの証拠保全およびドキュメントレビューをはじめとする調査・分析、信頼性の高い国内のデータセンターを活用した、安全なクラウド型データマネジメントにより、クライシスの予防から対処までを支援することで、企業をリスクから守ります。 ・コンピュータ・フォレンジック: 不正・不祥事調査/情報漏洩調査/情報セキュリティ監査支援/PC 等の業務外利用調査/退職者 PC 調査 ・データマネジメント: -企業データ管理アドバイザリーサービス -国内で安全に電子データを管理するクラウドサービス「LD3」 -不正の早期発見に役立つメールモニタリング -上文書の適切な管理を可能にするペーパースキャン
マクニカネットワークス株式会社 https://www.macnica.net	①、③、⑦、⑫	・スレットハンティング&IR ツール (TeamT5 ThreatSonar) ・ネットワーク・フォレンジック装置 (Symantec Security Analytics) ・リアルタイムレスポンスプラットフォーム(Tanium) ・EDR + NGAV + Hunting(CrowdStrike Falcon) ・標的型攻撃対策(FireEye) ・ログ相関分析基盤(Splunk) ・セキュリティイベント管理(McAfee SIEM) ・スレットハンティングサービス ・インシデント対応サービス

IDF団体企業名	サービス区分	主要製品等
EY 新日本有限責任監査法人 https://www.eyjapan.jp/services/assurance/forensics	②-a,b,c,d、④、⑤、⑧、⑨、⑩	・フォレンジックトレーニング -Windows 8 / 8.1 / 10 -Macintosh -モバイルデバイス -ファイルシステム ・フォレンジック調査/インシデント対応支援 ・CSIRT 態勢評価・整備・運営支援サービス ・サイバー犯罪診断 ・eDiscovery 支援サービス ・Forensic Data Analytics
株式会社アクアシステムズ https://www.aqua-systems.co.jp	①、②-e (データベース)、⑨	・データベース監査ツール(AUDIT MASTER) ・データベースセキュリティコンサルティング ・データベース監査コンサルティング ・データベース監査ログフォレンジック調査
株式会社 DD-RESCUE http://www.dd-rescue.jp	②-a、⑧	・データ復旧サービス全般 ・簡易フォレンジックサービス ・フォレンジックツール(X-Ways Forensics)
データテック株式会社 https://www.data-tech.co.jp	⑧	・データリカバリー(重度物理障害・高難度データ復旧) -パソコン内蔵 HDD/外付け HDD データ復旧 -Mac 内蔵 HDD/SSD/外付け HDD データ復旧 -NAS(各種 RAID) データ復旧 -サーバー(各種 RAID) 修理&データ復旧 -USB メモリー 修理&データ復旧 -SD/microSD カード等、各種メモリーカード データ復旧 -デジタルビデオカメラ データ復旧 -SSD データ復旧
松久産業株式会社 http://www.matsuhisa-kk.com	①、②-a・b・e(画像(動画、静止画)解析調査)、④、⑥、⑦、⑨、⑪、⑫、⑬(画像解析調査、ビデオ画像認識解析・保管システム開発販売)	・パケット・ログを漏れなく収集し安心・安全に保管する装置「NetGuardian Packet」 ・パケット・ログを分析する装置「PacketAnalyst」 ・パケット・ログやアクセス・ログを安心・安全に長期保存する大容量一括保管管理システム「StorageGuardian」 ・安心・安全に大切なデータを護る「SecureNAS」 ・安心・安全を実現する統合多層防御ゲートウェイ/UTM「NetGuardian Gate」 ・安心安全な IoT 環境を実現する「SecureIoTAP」 ・熟練した人の技とコンピュータによるセキュリティ・フォレンジック関連サービス「SmartSecurityResearch」

IDF団体企業名	サービス区分	主要製品等
株式会社テリロジーワークス http://www.terilogyworx.com	①、②-a、⑦、 ⑨、⑫	・ネットワーク・フォレンジック(momentum Forensics) ・コンピュータ・フォレンジック(CyberTriage) ・パケットキャプチャ/長期保存(momentum Probe/Storage) ・ネットワーク監視・記録(SevOne) ・ネットワークセキュリティ監査(RedSeal) ・Threat Intelligence Service(KELA) ・Spirent 脆弱性調査サービス(Spirent)
株式会社ベルウクリエイティブ https://belue-c.jp	①、⑦、⑨	顧客要望に合わせて、診断から運用まで一貫通の支援ができることを強みとし、自社セキュリティソフトウェア『ParnaWall(パルナウォール)』は導入や運用が手軽な上、WEB アプリケーションへの攻撃による情報漏えいで最も多い SQL インジェクション攻撃を防御、検知する最新の技術を実装しております。 ・セキュリティサービス『SPM(セキュア・パッケージ・マネジメントサービス)』は、各企業で運用されているサーバにインストールされているパッケージソフト、コンポーネントのセキュリティ情報(脆弱性情報、影響度、リスク)を手軽に把握する事が可能となる脆弱性管理サービスです。 今後の IoT ビジネスに欠かせない、質の高いソリューションやサービスを生み出す事を使命と考えております。
ストーンビートセキュリティ株式会社 https://www.stonebeat.co.jp	②-a,b,d、③、 ⑤、⑥、⑦、⑧、 ⑨、⑩、⑪	【教育トレーニング】 セキュリティ基礎、サイバー演習、Hacking Expert、Incident Response、デジタル・フォレンジック、メモリフォレンジック、マルウェア解析、標的型メール訓練、CSIRT 対応演習、など 【対策支援】 脆弱性診断、セキュリティ健康診断、セキュリティコンサルティング、インシデント対応、セキュリティ監査、フォレンジック、マルウェア解析、など 【案件支援】 セキュリティシステムの構築支援・運用支援、CSIRT の構築支援・運用支援、など
株式会社シマンテック https://www.symantec.com/ja/jp	①、②、⑥、⑦、 ⑨、⑩、⑪	・セキュリティ脆弱性診断(Web、NW、Mobile、IoT) ・セキュリティアドバイザリサービス ・Advanced Threat Protection(標的型攻撃対策) ・Symantec Endpoint Protection(セキュリティ強化) ・マネージドセキュリティサービス(ログ監視) ・Cyber Skills Development(トレーニング) ・Symantec Incident Response(インシデント対応) ・Security Analytics(ネットワーク・フォレンジック) ・DeepSight Managed Adversary and Threat Intelligence(脅威・攻撃者情報提供) ・EDR Cloud

IDF団体企業名	サービス区分	主要製品等
株式会社富士通エフサス https://www.fujitsu.com/jp/group/fsas	⑦、⑨、⑪	・セキュリティサービス全般(セキュリティポリシー策定、セキュリティ監査、CSIRT 構築支援) ・ウイルス振る舞い検知サービス ・次世代ファイアウォール運用サービス ・インターネットゾーンのセキュリティサービス ・イントラネットゾーンのセキュリティサービス ・標的型メール訓練サービス ・機密情報保護 & 共有ソリューション ・次世代エンドポイント運用サービス
株式会社 PFU http://www.pfu.fujitsu.com	②-a,b、⑥、⑦、⑨、⑪	・デジタル・フォレンジックサービス ・マルウェア検体解析サービス ・インフラ脆弱性診断・Web アプリ脆弱性診断サービス ・ベンチマーク診断サービス ・インシデントレスポンス支援サービス ・通信ログ分析サービス ・CSIRT 構築・運用支援サービス ・CSIRT 訓練サービス ・標的型サイバー攻撃対策支援サービス ・標的型攻撃・ネットワーク診断サービス
デジタルデータソリューション 株式会社 https://www.digitaldata-solution.co.jp	①、②-a,b,c,d、③、⑧	・フォレンジック調査 ・データ復旧 ・不正通信監視・通知・遮断機器(DDH BOX)
NEC ソリューションイノベータ 株式会社 https://www.nec-solutioninnovators.co.jp	①、②-a,b、⑥、⑦、⑨、⑩、⑪	・フォレンジック調査(ハードウェア、ネットワーク) ・セキュリティコンサルティング(CSIRT 構築支援、情報セキュリティポリシー策定 等) ・セキュリティ監視分析サービス(ハードウェア、ネットワーク、インシデント分析 等) ・セキュリティ脆弱性診断サービス(プラットフォーム脆弱性診断、Web アプリケーション脆弱性診断 等) ・セキュリティ監査(ログ監査、情報セキュリティ 等) ・解析サービス(ログ解析、マルウェア解析 等) ・サイバー攻撃対応ソフトウェア(CylancePROTECT 等) ・セキュリティ専門技術教育(フォレンジック研修 等) ・サイバー演習(インシデント対応演習 等) ・その他(サイバー犯罪捜査協力/演習支援、脆弱性情報提供サービス 等)

IDF団体企業名	サービス区分	主要製品等
リーガレックス合同会社 https://legalex.co.jp/	②-a,b,c,d、④、⑥、⑧、⑨、⑬ (DF 専門家と公認会計士・公認不正検査士による一体的な会計不正調査・支援)	<サービスの特徴> ・デジタル・フォレンジックス担当官(某法執行機関で犯則調査に従事し、現在も法執行機関に DF 技術を指導)、公認会計士、公認不正検査士が連携して不正調査を実施又は支援すること。 ・大手監査法人(いわゆる Big4)で 5 年以上の実務経験を有する公認会計士を数十名擁し、数万件以上の大量のドキュメントレビューを効果的・効率的に処理することが可能であること。 ・主に法律事務所様(第三者委員会から社内調査、個人事件まで)の支援業務を行っていること。 ・粉飾決算や横領事件等の会計系不正調査の強みを活かし、品質偽装事件等の実績も有すること。 ・東京、大阪、福岡に拠点があり、全国いずれの地域であつても(また複数地域同時であつても)サービスを ご提供できること。
Nuix Japan https://www.nuix.com/jp	①、②、③、④、⑤、⑥、⑨、⑩、⑪、⑫、⑬ (Twitter、Facebook 等 SNS フィードのリアルタイムモニタリング)	各種 e ディスカバリー/デジタル・フォレンジック製品 ・Nuix Workstation(統合データ分析プラットフォーム) ・Nuix Web Review, Analytics & Intelligence (分析、レビュー、インテリジェンス構築) ・Nuix Ringtail (AI 機能搭載ドキュメントレビュープラットフォーム) ・Nuix Collection Suite, Data Finder, Imager (データ収集、移動、削除) ・Nuix Adaptive Security (MITRE Attack Framework に準拠した EDR 製品) ソリューション: e ディスカバリー、デジタル・フォレンジック、企業不正調査、メール調査、インシデントレスポンス、エンドポイントセキュリティ、内部脅威対策、ビヘイビアモニタリング、データプライバシー、GDPR 対策、データライフ サイクル管理サービス: 侵入テスト、脆弱性診断、インシデントレスポンス、セキュリティコンサルティング、製品トレーニングおよび導入支援
大日本印刷株式会社 https://www.dnp.co.jp	①、⑥、⑨、⑩、⑪	・サイバー・インシデント対応演習(CIRM コース 基礎演習/実践演習/産業制御系・基礎) ・トレーニング(サイバーオフェンスプロフェッショナルコース) ・情報セキュリティ対策ソフト(CWAT) ・CSIRT 構築支援コンサルティング ・Web 脆弱性診断

IDF団体企業名	サービス区分	主要製品等
株式会社モノリスワークス http://www.monolithworks.co.jp	②-a,c,d、⑦、⑨、⑫	・フォレンジック調査 ・脆弱性診断・侵入テスト (Web/HTML5 SPA/NW/iOS/Android/Windows/Mac etc.) ・ホワイトボックス診断 ・改修コンサルティング ※DEFCON CTF 上位入賞実績のある診断員による深いレベルでの診断が特徴 ・Android アプリケーション自動診断ツール (trueseeing) ※DEFCON 25 Demo Lab/CODE BLUEなどで発表しOSSとして公開
株式会社ブロードバンドセキュリティ https://www.bbsec.co.jp	②-a,b,d、③、④、⑥、⑦、⑧、⑨、⑩、⑪、⑫	・各種フォレンジックツール (EnCase、FTK、F-Response 等) ・HDD/SDD 保全・書き込み防止装置 ・各種 Filesystem 解析ツール ・マルウェア解析ツール ・フォレンジック調査・緊急対応サービス
ナビプラス株式会社 https://security.naviplus.co.jp	②-a,b,c,d、⑧、⑨、⑪	・各種フォレンジックツール(FTK/Xways 等) ・マルウェア解析(IDA Pro 等) ・フォレンジック調査 ・緊急対応サービス ・各種コンサルティング 等
ベイシス・テクノロジー株式会社 https://www.basistech.jp	①	・フォレンジックツール(Autopsy 等) Autopsy®は、Basis Technology 支援のもと、オープンソースコミュニティで開発されたソフトウェアで、どなたでも無料で利用可能です。Autopsyには、捜査におけるさまざまなユースケースに対応できる一連の標準モジュールが付属していますが、アドオンによる拡張が可能な設計になっています。オープンソースコミュニティによるアドオン・モジュールも日々産まれています。
株式会社アップラス https://dokuta-s.com	②-a,b,c,d,e(IoT、家電、住宅設備、ゲーム機、その他の情報端末全般)、③、④、⑦、⑧、⑨、⑫	・Dr.セキュリティ®(マルウェア、サイバー攻撃、不正アクセス、その他の情報セキュリティ・インシデントの調査及び法的措置の補助等のサービス) ・個人及び中小企業向けの情報セキュリティ・サービス(コンサルティング、セキュリティ関連システム及びプログラムの開発、セキュリティ機器や設備の導入など)

IDF団体企業名	サービス区分	主要製品等
株式会社スプラウト https://sproutgroup.co.jp	①、②-a,c、③、④、⑥、⑨、⑩、⑪	・ファストフォレンジックソリューション(CyCraft AIR) ・ファストフォレンジック、ディスクフォレンジック調査 ・インシデントレスポンス支援 ・マルウェア解析 ・セキュリティ診断(脆弱性診断) ・ペネトレーションテスト ・セキュリティコンサルティング ・脅威リサーチ(ダークウェブ調査) ・セキュリティ教育コンテンツ ・バグ報奨金プラットフォーム(BugBounty.jp)
株式会社パソコンドック 24 https://www.pcdock24.com	⑥、⑧	・各種ハードウェア修理 (Windows 系 PC・Mac 系 PC・ファクトリー系 PC など) ・データリカバリー全般 ・高難易度なハードウェア修理の技術講習 (LCD 交換・回路修復)
株式会社神戸デジタル・ラボ http://www.proactivedefense.jp	②-a,b、③、⑥、⑨、⑪	・インシデント対応&フォレンジック調査 ・インシデント対応トレーニング ・セキュリティポリシー策定支援 ・Web アプリ脆弱性診断 ・スマホアプリ脆弱性診断 ・サーバ・ネットワーク脆弱性診断
オープンテキスト株式会社 https://www.opentext.jp	①、⑤、⑥	フォレンジック/トリアージ: OpenText EnCase Endpoint Investigator

その他の IDF 団体会員

株式会社インターネットイニシアティブ	https://www.ij.ad.jp/
LINE 株式会社	https://linecorp.com/
公益財団法人金融情報システムセンター	https://www.fisc.or.jp/
株式会社リクルートテクノロジーズ	https://recruit-tech.co.jp/
株式会社サンエイ	http://sanei.company/
ネットワンシステムズ株式会社	https://www.netone.co.jp/
JBCC 株式会社	https://www.jbcc.co.jp/

J.「証拠保全ガイドライン」改訂WGメンバー(所属は 2019 年 12 月現在)

※五十音順

座 長 名和 利男	株式会社サイバーディフェンス研究所 専務理事／上級分析官、 兼 PwC サイバーサービス合同会社 最高技術顧問、IDF 理事
副座長 松本 隆	株式会社ディー・エヌ・エー システム本部 セキュリティ部、IDF 理事
委 員 伊原 秀明	株式会社ラック サイバー救急センター
委 員 上原 哲太郎	立命館大学 情報理工学部 教授、IDF 副会長
委 員 金子 寛昭	株式会社フォーカスシステムズ サイバーフォレンジックセンター
委 員 小山 幸輝	PwC サイバーサービス合同会社 マネージャー
委 員 アグニ サング	大日本印刷株式会社 AB センター
委 員 篠原 明彦	ネットエージェント株式会社 技術部サービスグループ 課長
委 員 須川 賢洋	新潟大学大学院 現代社会文化研究科・法学部 助教、IDF 理事
委 員 杉山 一郎	EY 新日本有限責任監査法人 Forensics 事業部 プリンシパル
委 員 大徳 達也	株式会社サイバーディフェンス研究所 情報分析部 部長／上級分析官
委 員 谷口 浩	東京電力ホールディングス株式会社 セキュリティ統括室 室長
委 員 野崎 周作	株式会社 FRONTEO 執行役員 技師長
委 員 舟橋 信	株式会社 FRONTEO 取締役、 株式会社セキュリティ工学研究所 取締役、IDF 理事
委 員 守本 正宏	株式会社 FRONTEO 代表取締役社長、IDF 理事
委 員 山内 崇	株式会社ピーシーキッド 常務取締役 データ復活サービス部 フォレンジックサービス部
オブザーバー 安富 潔	京都産業大学 法学部 客員教授、慶應義塾大学 名誉教授、 渥美坂井法律事務所・外国法共同事業 弁護士、IDF 会長
佐々木 良一	東京電機大学 研究推進社会連携センター 総合研究所 特命教授 兼 サイバーセキュリティ研究所 所長、IDF 理事 兼 顧問
櫻庭 信之	シティユーワ法律事務所 パートナー弁護士、IDF 理事
西川 徹矢	笠原総合法律事務所 弁護士、IDF 理事
坂 明	公益財団法人東京オリンピック・パラリンピック競技大会組織委員会

○個人の立場でオブザーバーとして「証拠保全ガイドライン」改訂検討・作業に参加していただいた方々

東 隆夫、石切山 開、乾 奈津子、猪股 晃匡、内田 謙一、枝村 和茂、遠藤 淳人、
尾野村 研吾、金山 栄一、川崎 隆哉、木田 宗志、小林 隆一、砂原 圭太、添田 誠二、
常見 敦史、鳥飼 貞一、西村 朋子、野本 靖之、萩原 栄幸、原島 一郎、福谷 優、
北條 孝佳、松ヶ谷 新吾、松原 一彦、水戸部 一貴、宮崎 謙二郎、両角 智之、柳 裕二
(氏名のみ記載、敬称略、五十音順)

IDF 事務局

委員・事務局長	丸谷 俊博	株式会社フォーカスシステムズ 新規事業推進室 室長
事務局	押切 悠希	株式会社フォーカスシステムズ 新規事業推進室
事務局	佐藤 瑠奈	株式会社フォーカスシステムズ 新規事業推進室
事務局	鈴木 涼介	株式会社フォーカスシステムズ 新規事業推進室
事務局	小林 佳柚	株式会社フォーカスシステムズ 新規事業推進室
事務局	中移 絵美	株式会社フォーカスシステムズ 新規事業推進室
事務局	一居 政宏	株式会社 FRONTEO リスクコンサルティング部
事務局	櫻井 拓弥	株式会社 FRONTEO リスクコンサルティング部

以上

(空白頁)