「証拠保全ガイドライン 第10版」

2025 年 3 月 15 日

特定非営利活動法人デジタル・フォレンジック研究会
「技術」分科会・「人材育成」分科会 合同
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. 取り巻く環境の変化（状況認識）

社会が ICT[1] に深く依存する中、個人・企業・組織間、さらには国境を越えた紛争において、電磁的記録を証拠として適切に保全・調査・分析する「デジタル・フォレンジック」の重要性が、従来にも増して高まっている。これらの対応は、サイバー攻撃やサイバー犯罪への対策のみならず、法的紛争や内部不正への対処において不可欠となっている。

一方で、業務システムは急速にクラウド化が進み、企業の基幹系やコミュニケーション手段がクラウド上で運用されるケースが当たり前になってきた。クラウドサービス（IaaS、PaaS、SaaS）特有の環境下での証拠保全には、従来型のオンプレミスシステムとは異なる考慮が必要である。クラウド上の証跡やログ、外部提供者であるクラウドサービスプロバイダとの調整、国際的なデータ移転やログ保持期限等の課題が顕在化している。

さらに、インターネットを前提とするサービスや IoT[2]デバイス、ビヨンド 5G、DX（デジタルトランスフォーメーション）の推進、膨大なデータ流通が進展する中で、クラウドサービス上に蓄積される情報は格段に増加した。これにより、従来の手法では対応が難しい揮発性情報（メモリ上の情報やクラウド固有の一時ファイル）や、ログ管理・証拠取得の範囲が大幅に拡大している。

こうした背景を踏まえ、本ガイドラインでは新たに「9. クラウドサービス」を設け、クラウド特有の証拠保全手順・留意事項を整理し、読者が多様な環境下でのインシデント対応に活用できるよう配慮している。

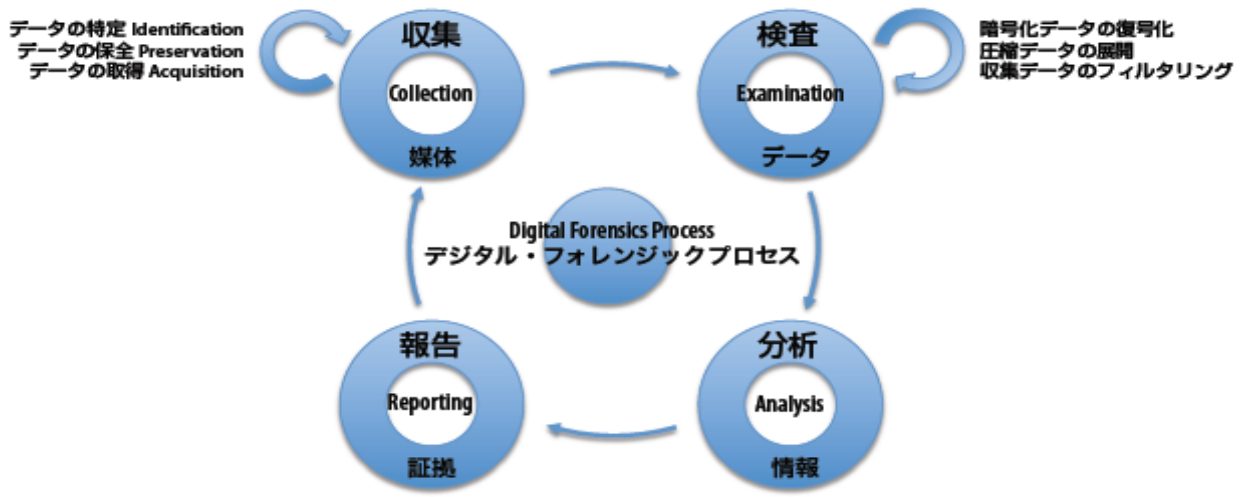
1-2. デジタル・フォレンジックの状況

デジタル・フォレンジックは、インシデントに関わるデジタル機器上の電磁的記録を確実かつ正確に（As-is）で、収集（Collection）・取得（Acquisition）し、保全（Preservation）しておくことすることを基盤として、分析・解析（Analysis）を行い、法的紛争やトラブルにおける適正な立証に資するものである。その重要性は、インターネットを介した不正アクセスやマルウェア攻撃など、さまざまなサイバーインシデントを受けて、高まり続けている。

---

[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。）



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

しかしながら、昨今のクラウドサービス活用によって、従来のオンプレミス型環境とは異なる課題が表面化している。クラウド環境では、ログや証跡の取得範囲が事前設定や契約内容、サービスプロバイダの提供する機能に大きく左右され、電源 ON/OFF の概念も曖昧となり得る。揮発性情報やトランザクションログ、アクセス制御ログなど、クラウド特有の証拠保全対象への対応力が求められる。このため、本ガイドラインはクラウドサービスにおける証拠保全・調査手続きを示す章（「9. クラウドサービス」）を新設し、グローバル化・リモート化する IT 環境に即した指針を提示する。

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」となり得るか、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および配慮した事項は、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または発覚した現場において、即座に実施する被害拡大等のための対処やコンピュータ等を対象とした電磁的証拠の保全作業にあたる「ファースト・レスポンダ」をはじめとした、デジタル・フォレンジック関連技術を活用するすべ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」および「ファースト・レスポンダ」の定義は、次のとおりである。

- インシデント：情報の機密性、完全性また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および環境の不正使用、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・レスポンダ：「デジタル・フォレンジックに関する専門的な技能や豊富な知識を習得しているとは限らないが、専門事業者また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）および分析（解析）の対象となる「証跡とログ」の概念や定義には明示的また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「証跡とログ」に対する認識は、次のとおりとする。

- 証跡：コンピュータ・システムの仕様上、人や不正プログラムの操作により、ファイル/データ/ネットワーク/内部等のさまざまな処理により必然的にディスクやメモリ上に残る痕跡のこと。英語圏における ”Artifact”（*Something observed in a scientific investigation or experiment that is not naturally present but occurs as a result of the preparative or investigative procedure*[3] ）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およ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 aircraft*[4] *)*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る。

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、次の表のとおりとする。

用語〔読み方〕	英語表記	意味
Live Linux Boobable USB/CD/DVD 〔ライブ・リナックス・ブータブル・ユーエスビー/シーディ/ディーブイディー〕	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きる USB デバイスや CD/DVD のこと。
BIOS／UEFI 〔BIOS：バイオス/UEFI:ユーイーエフアイ〕	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 の起動およ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 およ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(たとえば 80GB)を異なる容量(たとえば 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 などがアクセスできない領域が生ずる。
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 などを含めすべて自動的に暗号化され、読出し時には復号化される。
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・ピィ・エイ〕	Host Protect Area／Hidden Protected Area	BIOS および OS から、容易にアクセスでき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。

用語〔読み方〕	英語表記	意味
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、元の 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 が発行および管理をしている「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 11）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 1 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て、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。
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 ドライブごとに必要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。

用語〔読み方〕	英語表記	意味
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」等に分かれている。各ログは「警告」、「エラー」、「情報」の三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すべてのビット列を正確に複写すること。完全複製／物理複製ともいう。
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（たとえば 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写・保存する。E01 形式では、一定の大きさに分割して複写される。
インシデント	Incident	情報の機密性、完全性また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。
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およ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すべ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、写真および筆記などにより記録すること。

用語〔読み方〕	英語表記	意味
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（たとえば大規模震災）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およ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。
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。また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、論理複製また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気的およ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または滅失を防ぐため、適正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

初動対応およ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. 活動プロセスおよび体制の確立

初動対応および証拠保全を実施可能な活動プロセスおよび体制を確立する。

- 初動対応およ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）の順位の検討および決定。
- インシデント発生時の初動対応およ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およびテスト。

> ***《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、また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。*

- 初動対応および証拠保全経緯（時系列）の記録方法の確立。
- 初動対応およ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、情報共有および分析

初動対応および証拠保全に関連する情報収集、情報共有および分析を行うことが可能な体制およ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および分析。
- 揮発性情報の取得手順・内容および範囲（メモリダンプ、アプリケーション関連情報）の明確化および文書化。
- 初動対応およ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. 資器材等の選定および準備

初動対応および証拠保全において、必要と考えられる資器材等を選定および準備する。

- 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。
- 初動対応およ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。
- 初動対応および証拠保全に必要なツール、ソフトウェアの選定および準備。
  - 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)書き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」および「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することも可能)、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。*

3-4. 資器材等の使いこなし

初動対応およ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および解析ツール*
> - *スマートフォンのデータ取得ツール*

[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。

・ クラウド関連の保全ツール

（詳しくは、「付録資料H. 代表的な収集および分析ツール」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または発覚(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および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がある。

4-1. 初動対応およ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

(検知または発覚のきっかけ)

- 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およびハードウェアクロック)

(初動対処の開始までの記録)

発生したインシデントの検知または発覚から、報告または対処依頼の連絡までの時間およびその間のインシデントに対する対処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および人数
- 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(およびその周辺)に対する行為、確保後の対象物に対する対処(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(およびその周辺)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およ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および個数

- 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 3DS[6]、プレイステーション Vita[7]、プレイステーション 4、Nintendo Switch、Xbox One™ [8] 等)
- IC レコーダ
- ストリーミングデバイス(Chromecast[9]、Fire TV[10] Stick 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、「8. アウトソーシングサービスおよびコミュニケーションツール」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および使用頻度
- 発生したインシデントに関する対象物の使用者および管理者
- 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およ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およびその理由

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、HPA[11] ・DCO[12] の

---

[6] 「ニンテンドー DS」および「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・インタラクティブエンタテインメントの登録商標です。
[8] 「Xbox One™」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 LLC の商標または登録商標です。
[10] 「Fire TV Stick」は、Amazon Technologies, Inc.の商標または登録商標です。
[11] HPA:Host Protected Area または 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。

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および USB/Thunderbolt[13] 、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 全体暗号化または一部のファイル・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/SDD の暗号化が不明の場合、Encrypted Disk Detector[14] 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:*

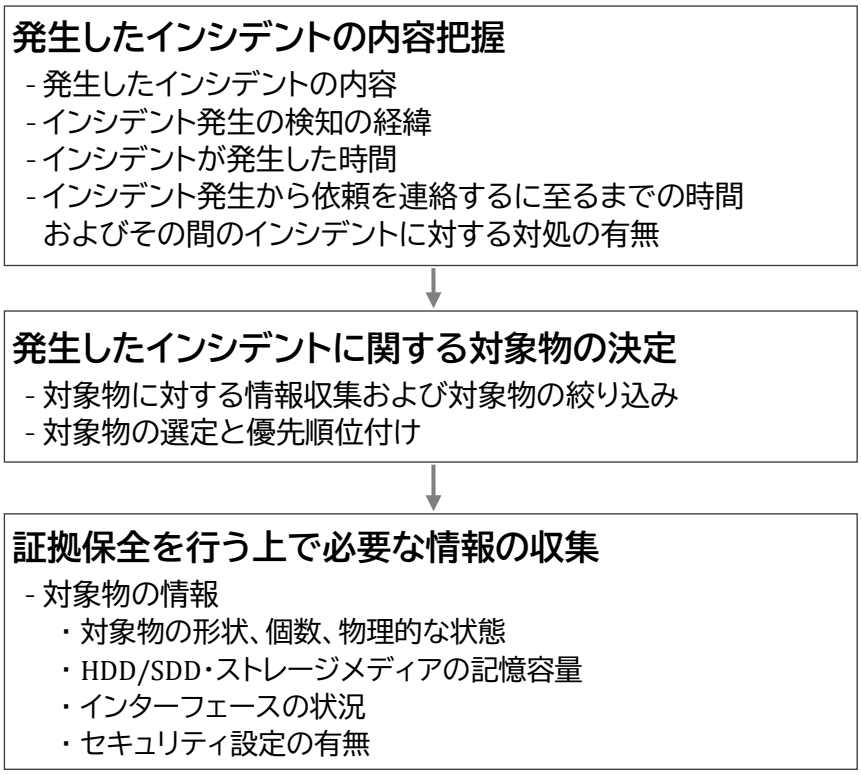


図 1 本節の作業内容を示すフローチャート

---

[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/

4-2. 初動対応およ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

対象物の選定およ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. 活動プロセスおよび体制の確立」に関する各種情報の過不足等の有無。
- 「3-1. 活動プロセスおよび体制の確立」に関する各種情報の収集の工程および結果を承認する人物の存在または承認の有無。

4.2.2 発生直後の初動対応およ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または証拠保全について、可能な限り 5W1H で聴取。
- 聴取は、初動対応または証拠保全を実施した者に加えて、それを観察または監督した者に対しても実施。

4.2.3 対応に過不足が確認された場合の対処

- 収集または聴取した情報・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または聴取。
- 収集または聴取した情報・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およ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. 初動対応およ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、見やすい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およびプラグ等の確保。
- 初動対応およ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およ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、初動対応およ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。
- システム設計者また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。

- 関係者の確保および無関係者の排除。
  - 初動対応およ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保。
  - 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およ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)の拡大また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。

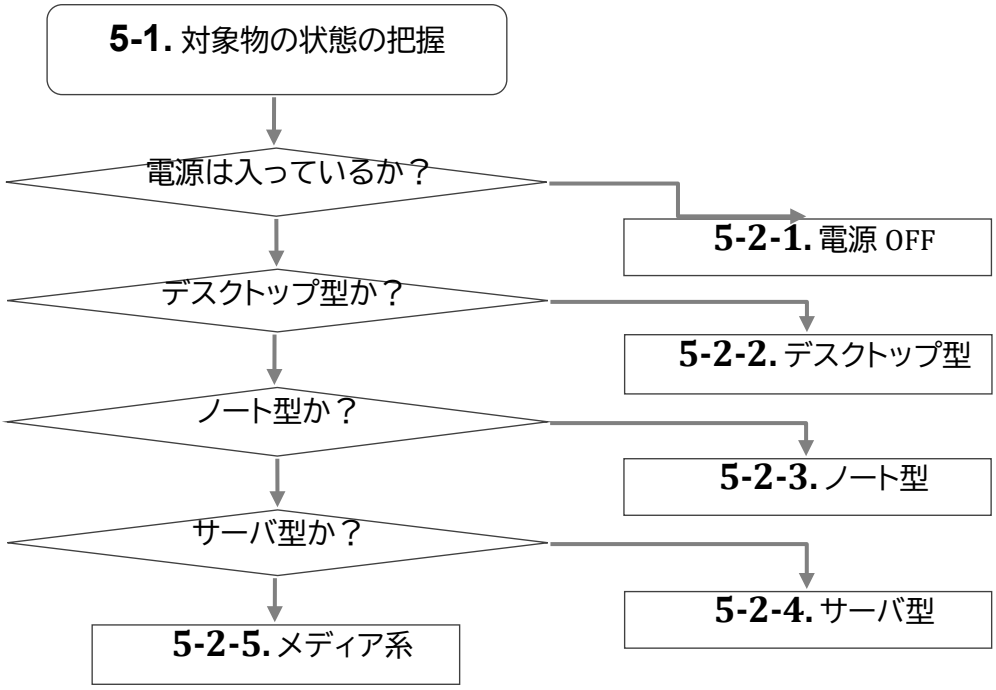


図 2 主な収集・取得・保全するための対象物の処置の選択

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、ケーブル類はすべ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。

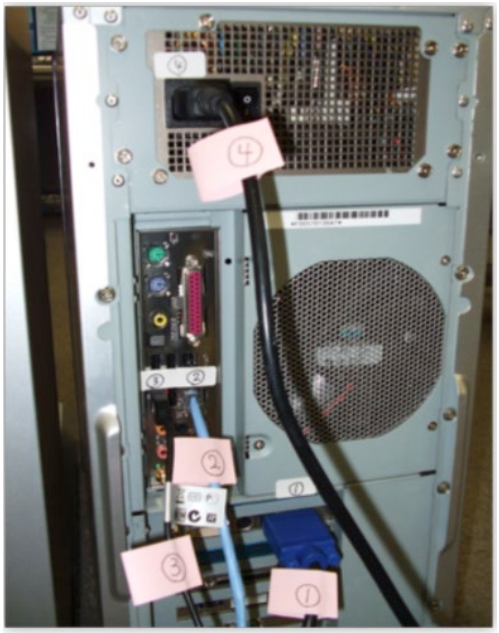


図 3: ケーブル等へのラベル貼付状況の記録

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 の確認およ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）を目視またはコマンドで確認・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、出力装置に表示また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／SDD 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:5.2.6 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、ケーブル類はすべ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)および 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 の確認およ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)を目視またはコマンドで確認・記録。
- ネットワーク環境の確認。
  - WiFi(無線 LAN)および 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、出力装置に表示また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ため、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、また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、RAID[16] 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/DVD[17] 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および紛失等を防止するため、識別目的の札を付ける等、確実な識別および管理を行う。
- 付けた札には、収集・取得・保全の日時、場所、所有者（または管理主体）、使用用途、状況、収集・取得・保全に至った経緯およ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）

- IEEE1667[18] 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。

---

[16] AID：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。

（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。

> ***《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動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。
    - ✧ データまた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	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
揮発性:低	物理的設定、ネットワークトポロジ
	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. サーバおよび通信・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すべての URL の記録が得られる。
  - IDS および IPS
    疑わしい挙動や進行しつつある悪質な活動を検知または防止する措置に関する記録が得られる。ただし、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
    マルウェアが侵入または動作に成功した記録が得られる。ただし、すべ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。
  - 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ごと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)

[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)

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[22] 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、イベントごとのタイムスタンプ、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ラ、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
    たとえば、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
    認証およびその試行回数、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

---

[22] 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。

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 または F2
旧 Compaq	F10、F2、F1、または Del
Dell	F2
eMachines	Tab、Esc、Del、または F2
Fujitsu	F2
Gateway	F1
Hitachi	F2
HP	F10
IBM/Lenovo	F1 または F12
Lenovo	F1 または F12
NEC	F2
Panasonic	F2
Phoenix Award BIOS 標準	DEL
Sony	F2 または F3 のち F2、F3 のち F1
Toshiba	Esc のち F1
Dynabook	F2
Microsoft (Surface)	音量 up ボタン+電源ボタン

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、あらかじめ書き込み／読み込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、すべて、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。ただし、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また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 SATA[23] 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機能を有する装置を用意するか、原則としていかなる書き込みも行うことができない措置を取ること（ソフトウェアベース等）。

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

[23] 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。

の位置等を確認する（これにより、ハッシュ値[24]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・構成もすべ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
- 物理的およ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
- 対象物および複製先の詳細情報
- 作業内容および各種設定情報
- 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）およ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よい。
- 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）

[24] 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）。

- 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）およ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
- 実施した作業内容およ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 またはイメージコピー）が可能

- 対象物と同一の OS 上で起動可能なソフトウェアまたはプログラムを利用。
  - GUI（Graphical User Interface）形式またはコマンドラインによる使用。
- 証拠保全ソフトウェアまた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、または困難、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、デバイスごとの変更仕様や 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 Testing[25] ）等の信頼できる機関にて検証されたものが望ましい。

---

[25] 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/）

6-3-3. 代表的な収集およ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》***
>
> *代表的な収集および分析ツールの使用に当たっては、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 の物理的制限および（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、初動対応およ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。
  - 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ともに、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. IDE[26] 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、また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およ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。

[26] IDE：Integrated Drive Electronics。コンピュータにハードディスク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

初動対応およ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)および複製先に対し、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、「6-3. 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、「7-4. 証拠保全の正確性を担保する作業内容の記録」を取得し、ツールの信頼性およ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、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)およ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)およ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

● 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(SigCheck[27])を利用する場合 SigCheck -h <ファイル名> 例: `>SigCheck -h 対象文書.docx`

7-4-3. ビデオおよび写真撮影

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

- 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、物理的に区分けさ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[28]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ともに、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

- 複製先への手渡しについて、手渡し日時、担当者、受領者、場所、対象物、及びその状態を詳細に記録・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、然るべき発送業者およ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。
- 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がないか確認する。

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すべ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、およ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

[28] 実施者、実施日時、およびその行為内容が明確に記録された書類。

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、「6-3. 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、「7-4. 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、ツールの信頼性およ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よい場合があるため、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。

7-6. ネットワークログからの証拠データ抽出

7-6-1. 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、検証および運用の過程で、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。

7-6-2. 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

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

- 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)

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

- 具体的には、マルウェアが使用した IP アドレスおよびポート番号、外部ホストとの通信プロトコル等

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

- 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

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また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(コンピュータおよ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

- 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

⑤ 関係する可能性があるすべ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」および「参考情報」を基に相関的な観点で調査

- たとえば、IP アドレス、ホスト名、時間帯、ID／アカウント名、不審な挙動パターン等

7-7. 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。

7-7-1. 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およびコピーし、解析すること[29] 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および保全の高まり、SSD 搭載デバイスとディスクの大容量化等がある。

インシデント発生の現場におけるファースト・レスポンダは、一つのデバイスを深く調査する暇がなくなってきており、迅速な原因究明や侵入経路の侵入・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。

7-7-2. 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

[29] 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

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、メーラ等の設定および送受データ）、メモリなどである。

これらの証拠データが消失する前に、発生現場におけるファースト・レスポンダが手作業のみで迅速かつ最大限に取得することは困難であるため、専門ツールを利用して実施する。

※ 専用ツールは、「H. 代表的な収集および分析ツール」を参照

8. アウトソーシングサービスおよびコミュニケーションツール

組織が利用する業務システムやコミュニケーション手段（メール、チャット、Web 会議ツール、SNS 式情報共有ツール等）が、外部のサービスプロバイダによるアウトソーシングサービス（ホスティングサービス、マネージドサービス、ASP サービス等）を通じて提供されるケースが増えている。これらのサービス上でやり取りされるデータには重要な証拠資料が含まれ得るため、インシデント発生時には、当該アウトソーシングサービスおよびコミュニケーションツールからの証拠保全も必要となる。

本章では、アウトソーシングサービスおよびコミュニケーションツールに共通する証拠保全手順・留意点をまとめる。なお、純然たるクラウドサービス（IaaS/PaaS/SaaS など）特有の考慮点やログ取得・保持に関わる詳細事項は、別章「9. クラウドサービス」に譲る。

8-1. 事前に行う準備

アウトソーシングサービスおよびコミュニケーションツールを対象とする証拠保全では、サービス利用契約や約款の事前確認が重要である。

- 利用契約・約款、SLA（サービス品質保証）の確認
- サービス利用範囲、責任分担の明確化
- 証拠保全手続きの対応可否や条件（バックアップ取得手段、エクスポート機能の有無）の事前把握

また、コミュニケーションツールの場合、その管理者またはユーザマニュアルを参照し、以下を確認する。

- バックアップ／エクスポート機能の有無と適用範囲
- 電子情報開示（eDiscovery）の機能と適用範囲
- API や連携アプリケーションによるデータ取得手段の有無

8-2. インシデント発生直後の対応

インシデントが発生、または発覚した直後は、対象となり得るサービス上のデータやアカウント、記録類とインシデントとの関係性を即座に確認し、保全が必要なデータやその根拠を明確化する。

- 保全対象となる（可能性の高い）データ、記録、およびアカウントとインシデントとの関連付け
- 保全必要性の根拠、検討内容を記録

8-3. 保全方法および作業手順の検討

サービスが標準提供するバックアップ／エクスポート機能や、関連ツールを活用し、可能な範囲でデータを取得する。

- サービス提供側が備える標準的なバックアップ、エクスポート機能の利用
- 機密性保持のため、暗号化データの場合は回復用キーも確保
- エクスポートが未対応の場合、サービスプロバイダへの証拠保全依頼や別の代替手段を検討
- ローカル端末（キャッシュなど）に対象データがある場合は、そのローカル端末保全も検討

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やコミュニケーションツールは、サービス継続中に保全手続きを進めることが多い。そのため、以下の点に留意する。

- 作業は可能な限り立会人を付けるか、複数人で実施し、客観性を確保
- 意図しない改変を防ぐため、事前に手順を明確化し、担当者はサービスの基本的な操作、設定内容を十分に理解した上で実施
- 作業環境は、通信パケット取得やネットワーク構成図の記録など、後日再現可能な状態で確保
- 保全手順・操作過程は詳細に記録し、可能であれば動画、スクリーンショット、写真で記録
- タイムスタンプ、表示条件、メタデータ等を適宜記録し、後日の検証に備える

8-5. アカウント所有者の同意

対象となるアカウントが個人に帰属する場合、保全には本人同意が必要になることがある。

- 保全対象アカウントやパスワード開示、作業中のパスワード変更、データエクスポート許可など同意内容を明確化
- 同意は書面で記録する
- 家族等、複数管理者がいる場合は可能な限り全員の同意を取得
- パスワード変更等を行う場合は、変更記録を厳重管理

8-6. 収集・取得・保全

事前に策定した作業手順に従って、データの収集・取得・保全を実施する。

- 保全対象データの件数や状態を確認
- 事前想定した保全対象がすべて取得されているか確認し、記録
- 必要に応じてメタデータや作業時点の通信パケットを取得し、保全状態を裏付ける

8-7. 保全のための設定変更と復元

保全のために行った設定変更等は、インシデント収束後に元に戻すかどうか検討する。

- アカウント所有者やインシデント担当者、法務担当者と協議の上、必要に応じて復元措置を実行

9. クラウドサービス

クラウドサービスの利活用が進むつれ、電磁的証拠の保全手続きについてクラウドサービスの特性を考慮した電磁的証拠の保全の方法や固有の手続きの必要性が生じてきた。以下にクラウドサービス特有の証跡や保全手法についてのガイドラインを提供する。

9-1. クラウドサービスにおける役割分担

クラウドサービスの管理にあたっては、クラウドサービスの提供者である CSP((Cloud Service Provider))とクラウドサービスの利用者である CSC(Cloud Service Customer)に役割が分類される。提供されるサービスの形態(IaaS, PaaS, SaaS 等)[30]により、それぞれが管理する領域が異なることを意識する必要がある。一般的にデータセンター、ネットワークやハードウェアは CSP が管理を行うが、OS より上、ミドルウェアやアプリケーションはサービスの形態によりどちらが管理をするかが分かれる。

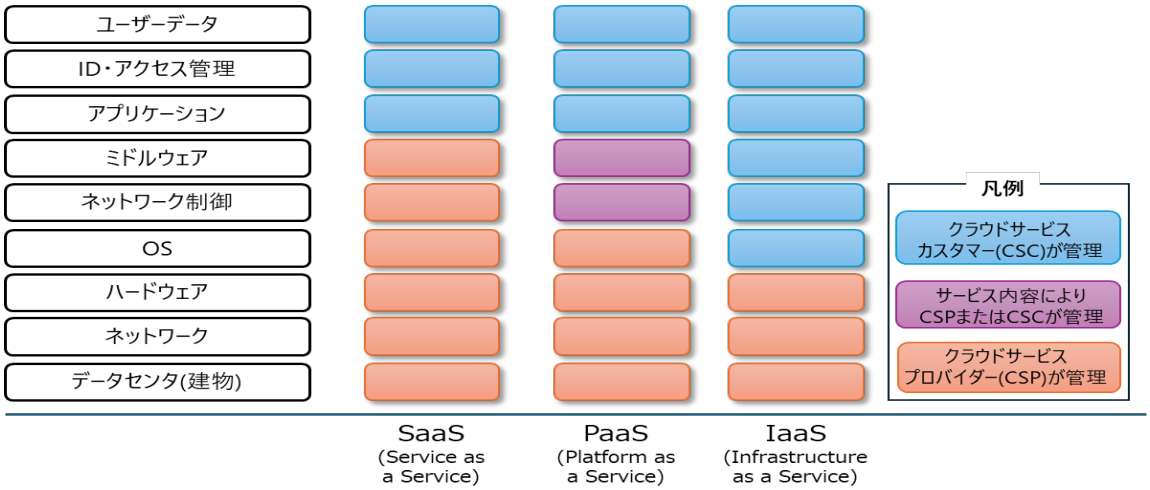


図 4: クラウドサービスの提供形態と役割分担

CSC と CSP との管理の役割の違いは証拠保全やインシデント対応にも当てはまる。CSC の管理領域については CSC がセキュリティ対策や証跡の取得、保全の実施をする必要がある。一方で、CSP の管理領域については、CSP がセキュリティ対策や証跡の取得、保全を実施する。一般に CSC からは CSP が管理する領域についての直接証跡を取得することは困難ではあるが、クラウド環境の保守作業の実施履歴や実施内容についてはサービスヘルスポータルや管理者へのメール通知などを通じて情報通知の仕組みが提供されるものがある。

---

[30] IaaS(Infrastructure as a Service):仮想化されたコンピュータ・システム基盤(OS、Hardware、Network 等)を提供する形態
PaaS(Platform as a Service):Web API やフレームワーク等を通じてソフトウェア基盤(Middleware 等)を提供する形態
SaaS(Software as a Service):Web ポータルなどを通じてアプリケーションを提供する形態

9-2. クラウドサービスにおける証拠

9-2-1. クラウドサービスにおける証跡

クラウドサービスではほとんどの操作はユーザ ID やクレデンシャルによる認証と API による指示により行われる。これらのログを証跡として取得することでクラウド上でだれが、いつ、どのような操作が行なったかを分析することができる。クラウドへの操作の内容は、クラウドのリソースの作成や設定の変更、削除といった処理を扱うコントロールプレーン操作とユーザのデータの作成、更新、削除といった処理を行うデータプレーン操作とに分かれる。一般に認証とコントロールプレーン操作はログ保管期限が設定されているものの標準でログが取得可能であるが、データプレーン操作については明示的にログを取得する設定を行う必要がある。

また、オンプレミス環境における調査と同様に、認証ログの解析結果はインシデントの影響範囲を確認する上で重要な手がかりとなる。クラウドサービスにおいては認証ログはユーザによる対話的な認証のほか、サービスによる認証、自組織以外のユーザアカウントによる認証なども含まれる。ユーザによる対話的な認証以外の認証や他組織からの認証についても認証ログを適切に取得・保持する設定となっているか、確認が必要である。

一方、仮想マシンなどで利用される仮想デバイスのストレージ上のデータはオンプレミス環境でのデータ保全と同様の方法で実施可能である。ただし、クラウド環境では直接発災ホストからハードディスク等のストレージを取り出すことはできない為、クラウド環境上の仮想デバイスからストレージデータをエクスポートする手順について確認をしておく必要がある。また、たとえば、Azure の仮想マシンの場合、仮想ディスクのイメージを dd コマンドやディスクイメージ抽出ツールを使用してエクスポートする方法のほか、仮想ディスクのスナップショットを取得しダウンロードする方法や別の仮想ディスクを作業用の仮想マシンに接続してディスクイメージのコピーを取得する方法なども考えられる。

9-2-2. クラウドサービスにおける証跡の保持期間

クラウドサービスのログ取得に関しては、CSP からサービスの一環としてログ取得および保管機能が提供されている場合がある。規定の状態ではログの保持期間が 30 日などの期間で固定されている場合があるので注意する。ログの種別とそれぞれの保持期間を確認することが重要である。

クラウドサービスではログの保持期間を経過したログデータは自動的に破棄されるが、破棄されたログデータを回復させることは極めて困難であるため、インシデント対応の初期の段階でログデータの外部保管を行う必要がある。

9-3. クラウドサービスにおける証拠管理の考慮点

9-3-1. クラウドサービスの操作ログや更新記録

クラウドサービスではサービスや仮想マシンの認証情報を用いてクラウドについてのさまざまな操作が可能なように構成できる。このような操作の証跡を取得するためには、インシデントが確認されている仮想マシンやサービスのログ以外にも、認証システムのログおよびクラウドサービス自体のログ（アクティビティログ）の保全も行う。

9-3-2. クラウドサービスの停止や再起動に関する注意

クラウドサービスには、データの保管をせずにサービス終了もしくはリソース削除をすると揮発性のあるデータや更新データが破棄されるサービスがあるため不用意にサービス停止や再起動を行わないよう注意する。また、ストレージ暗号化を使用している場合は、暗号鍵が入手できない場合はストレージ上のデータにアクセスできないため、暗号鍵の保全を含め保全するる。

9-3-3. 各地域・越境のデータ保全等

個人情報や機微情報のデータ越境、各国規制などの法的問題が発生する可能性がある。また、リージョン間のデータ転送は一般に有償であり、大量データの転送を行う場合には転送コストが発生することに注意が必要である。

9-3-4. ログのフォーマットやログの保管形態

クラウドサービスではサービスごとにログの保管場所、保管方法、保管形式（フォーマット等）が異なる。自組織が使用しているサービスごとに、どこにどのような形式でログが保管されているかを確認する必要がある。

9-3-5. ログ取得の設定がなされていなかった場合の対応

ログ取得の設定の多くは事前に設定しておく必要がある。設定がなされていなかった場合は標準で提供されるログ（アクティビティログやアクセスログの一部）の保全を最優先で実施する。これらのログは保管期限が設定されており時間の経過とともに消失するため、過去の分から優先して別のストレージにエクスポートする等により保全する必要がある。

9-4. データ保全へのクラウドサービスの活用

クラウドで提供されるストレージサービスには、データ保全に役立つハッシュの取得、履歴の確保（バージョニング機能）、長期保管、リーガルホールド（書き込み、消去を禁止した状態での長期保管）などの機能が提供されるものがあるので利用を検討するとよい。

ストレージサービス以外にもクラウド環境で提供される以下のようなサービスを活用することで、インシデント対応および証拠保全を効率化することができる。

- クラウドベースのセキュリティ検出、分析サービス
- データウェアハウス（ETL(データ変換)、大規模データ検索や統計処理）
- AI サービスによる文字、画像、音声認識
- 仮想ネットワークやファイアウォール機能（仮想マシンやサービスの隔離等）
- 暗号鍵管理サービス（データの暗号化や署名に使用する証明書の管理等）

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ないように考慮する。			□
10	UPS を用意するなど、電源のトラブルにより HDD/SSD 複製作業に影響がないように配慮する。			□
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 の取外しを行う前に、HDD/SSD 自体に暗号化機能がある型番ではないか確認する。		○	□
13	PC 本体から、原本 HDD/SSD の取外しを行う。			□
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。		○	□
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ことが前提である場合、書き込み防止装置がない場合は、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。		○	□

No.	確認項目	写真	ﾁｪｯｸ
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 または 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 複製装置のベ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 をとりはずし、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戻す。	○	□
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. クラウド環境におけるサービスとログ

表 6: クラウドサービスの提供形態と代表的なクラウドサービス

提供形態	クラウドサービスの例
IaaS	• Microsoft Azure Virtual Machines (Azure VM) • Amazon Elastic Compute Cloud (EC2) • Google Compute Engine (GCE)
PaaS	• Google App Engine • Microsoft Azure App Service • AWS Lambda • AWS Elastic Beanstalk
SaaS	• Google Workspace • Microsoft 365 • Slack • Dropbox • Zoom

表 7: クラウド環境におけるログの特徴

ログ種別	認証ログ	クラウド操作に関するログ	
		データプレーン	コントロールプレーン
目的	クラウドサービスに対する認証のログ	クラウドリソース上におけるデータ処理のログ	クラウドリソースの管理や制御のログ
保持している証跡の例	・クラウドリソースにおける認証ログ(対話的ログオン、サービスログオン) ・クラウドテナントに対するログインログ(クロステナントアクセスを含む)	・データの保存ログや転送ログ ・NW トラフィックログ ・アプリケーション利用ログ	・リソースの作成、更新、削除ログ ・リソースの使用状況ログや料金ログ ・セキュリティやアクセス制御の設定内容
フォレンジック調査で想定されるユースケース	・なりすましによる不正ログイン有無の調査	・インスタンス内に保存されたデータ漏洩有無の調査	・インスタンスの不正な作成や起動有無の調査
主な被記録ユーザ	クラウドサービス利用者(CSC)のエンドユーザ、各種 Web サービス、自組織以外のテナントのエンドユーザ	CSC のエンドユーザ、各種 Web サービス、自組織以外のテナントのエンドユーザ	CSC の管理者(CSC のエンドユーザ、各種 Web サービス、自組織以外のテナントのエンドユーザが含まれることもある)
取得方法	クラウドサービスが標準で提供、一部については CSC 取得設定が必要	CSC による取得の設定	クラウドサービスが標準で提供する

備考	監査ログには一般的にユーザやグループに対するID/パスワードの変更操作や権限の変更操作が含まれる。	CSC が扱う作業領域であるため、原則として CSP が参照することはできない。証拠保全やデータ保管、データの保全は CSC 自身による準備が必要となる。	コントロールプレーンのログは CSP から CSC への料金請求を裏付ける証跡となり、原則として CSP によって提供・管理されているが、標準で提供される機能以上の長期保管やデータ保全は CSC が実施する必要がある。

表 8: 主なクラウドサービスのログとデフォルト保存期間

クラウドサービス	ログ取得サービス	保存対象ログ種別			保持期間 (デフォルト値)	備考
		認証	データプレーン	コントロールプレーン		
AWS	AWS CloudTrail	○※1	-	○※1	90 日	※1 CloudTrail は AWS に関連する各種ログデータを収集できるデータストア。
	Amazon CloudWatch Logs	-	○	○※2	無期限	※2 ログの保持期間は 1 日から無期限まで設定可 設定内容に応じた料金が発生する点に注意。
Azure	Microsoft Entra ID	○	-	-	30 日	・Microsoft Entra ID P1, P2 における保持期間。ライセンス形態によってログの保持期間は異なり、Microsoft Entra ID Free の場合は 7 日間となる。
	Azure Monitor	-	○	○	30~90 日程度	・ログ種別によって保持期間が異なる。詳細については以下のリンクを参照。 https://learn.microsoft.com/ja-jp/azure/azure-monitor/logs/data-retention-configure?tabs=portal-3%2Cportal-1%2Cportal-2
Microsoft 365	Microsoft 365 監査ログ	○	-	-	180 日	・詳細については以下のリンクを参照 https://learn.microsoft.com/ja-jp/purview/audit-solutions-overview
Google Cloud（旧 GCP）	Cloud Audit Logs	○	-	-	400 日	・監査ログは Cloud Logging の_Required バケットにて保持される。
	Cloud Logging	-	○	○	_Required：400 日 _Default：30 日 ユーザ定義：30 日	・_Required ログバケットには監査ログが主として含まれ、保持期間の変更はできない。 ・_Default ログバケットには_Required バケット以外のログエントリが含まれ、1~3650 日の範囲で保持期間の変更ができる。 ・ユーザ定義のログバケットにはユーザが指定した Google Cloud プロジェクトや関連するログが含まれ、1~3650 日の範囲で保持期間の変更ができる。

C. 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、磁気的方式その他人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。（なお、民事訴訟法第 3 条の 7 第 3 項にも同様の定義規定が置かれている。）

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および供用）

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、義務または事実証明に関する電磁的記録を不正に作った者は、五年以下の懲役または五十万円以下の罰金に処する。

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

3　不正に作られた権利、義務また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一の刑に処する。

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。言ってみれば、本来とは異なるデータ（電磁的記録）を作り出す罪であり、たとえば、外れ馬券の電磁的記録を当たり馬券のものに改ざん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。一般に第 1 項を「私電磁的記録」、第 2 項を「公電磁的記録」と呼ぶ。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。たとえば、モンスターハンターフロンティ G 内においてゲームのプログラムを改変しチート行為を代行したとして、有罪になった事例などがある（奈良地方裁判所　平成 29 年 1 月 17 日判決）。

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、義務また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また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、十年以下の懲役また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、または輸入した者も、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、五年以下の懲役また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、三年以下の懲役また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、器械また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　第百六十三条の二およ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、または提供した者は、三年以下の懲役また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、また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]。

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、それぞれ意味する。

（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、また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よいことになる。

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、本罪が成立し得るのは、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」などと言っていても通用せず、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 。

---

[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。

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、または保管した者は、二年以下の懲役また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、また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、または懲役および罰金を併科する。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、また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。既に褻データを格納した 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、また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、また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、五年以下の懲役また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。たとえば、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、また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、また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つか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また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　権利または義務に関する他人の文書また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某妨害罪」（刑法 第二百三十四条の二）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かいざんが適用要件となる。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および当該アクセス管理者また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。）また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およ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また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、三年以下の懲役または百万円以下の罰金（従前は一年以下の懲役または五十万円以下の罰金）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を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。第六条およ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およ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「一年以下の懲役また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、放送また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、一年以下の懲役または五十万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）

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また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または他の記録媒体に複写した上、当該電子計算機また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また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または他の記録媒体に複写した上、当該電子計算機また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）

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（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、または印刷させた上、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 条第 2 項は裁判所が差押を行う場合、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」に関しても、第 218 条第 1 項にも「検察官、検察事務官または司法警察職員は、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、記録命令付差押、捜索また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」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」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、たとえばプロバイダなどの協力的な者をして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、または移転した上、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、または移転させた上、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。差押の方法に不服がある場合には、準抗告（第 429 条第 1 項第 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、差押状または捜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。公判廷で差押または捜索をする場合も、同様である。

記録媒体の差押等を行うにあたり、差押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、捜索・差押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、第 111 条の 2 は裁判所の差押の規定あるが、検証にも準用される（第 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、検察事務官または司法警察員は、差押または記録命令付差押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また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または記録命令付差押をする必要がないと認めるに至つたときは、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　第二項また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または営業上の情報であって、公然と知られていないものをいう。

第二条第七項

この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、および管理されている技術上又は営業上の情報（営業秘密を除く。）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、またはこれを併科する。

一　不正の利益を得る目的で、また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、または人を脅迫する行為をいう。以下この条において同じ。）または管理侵害行為（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、またはこれを併科する。

一　日本国外において使用する目的で、第一項第一号また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また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また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。）、第二号およ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」は同法の第 2 条第 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。そして同第 4 号～第 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。こちらも条文のすべ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、自己の利益のため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、またはこれを併科」となった(第 21 条第 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(第 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ち出しに対しては、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(第 21 条第 1 項第 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(第 21 条第 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ため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(第 21 条第 6 項)。

さらに、犯罪収益の没収制度の導入(第 21 条第 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(第 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。他にも「秘密情報の保護ハンドブック」を始め各種文章が経産省より公開 [34] されている 。

---

[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] https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

不競法は、産業に密接した法のため 2,3 年の短い周期で改正が行われており、平成 30（2018）年改正時には、「限定提供データ」という概念が追加され、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』の不正取得なども不正競争行為の対象とされ、使用差止や民事的損害賠償などの対象となった。限定提供データの定義は令和 5（2023）年改正時に微修正（多少の範囲の拡大）が行われてる。ただし、まだ罰則規定はない。

またこちらも条文自体が長く複雑なため記載を省略しているが、同法第 2 条第 1 項第 17 号・第 18 号には「技術的制限手段」の回避を禁じる規定（刑事罰アリ）がある。この技術的制限手段とは、有料放送のスクランブル解除コードのような『アクセスコントール』のことを言い、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・ソフトウェアの提供等もこれに該当する。平成 30（2018）年改正時には、従来の機器・ソフトの提供などに加えて役務の提供等、すなわちアクセスコントールの回避を代行するような行為も不正競争行為に追加されており、その後は実際にこの役務の提供を理由とする検挙も行われている。

＜個人情報保護法＞

第百七十九条

個人情報取扱事業者（その者が法人（法人でない団体で代表者又は管理人の定めのあるものを含む。第百八十四条第一項において同じ。）である場合にあっては、その役員、代表者又は管理人）若しくはその従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、一年以下の懲役又は五十万円以下の罰金に処する。

第百八十四条

法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、次の各号に掲げる違反行為をしたときは、行為者を罰するほか、その法人に対して当該各号に定める罰金刑を、その人に対して各本条の罰金刑を科する。

一　第百七十八条および第百七十九条　一億円以下の罰金刑

二 [以下 略]

個人情報保護法は組織に対して個人情報の管理の在り方を示すための法律であるため、情報を不正に持ち出した場合の科（とが）が記載されている箇所はほとんどないのだが、個人情報データベース等の不正提供や盗用については「個人情報データベース等不正提供等罪」として罰則規定がある。平成27（2015）年改正で新設され令和 2（2020）年改正時に法定刑が引き上げられた。

D. 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

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		セク多数(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	

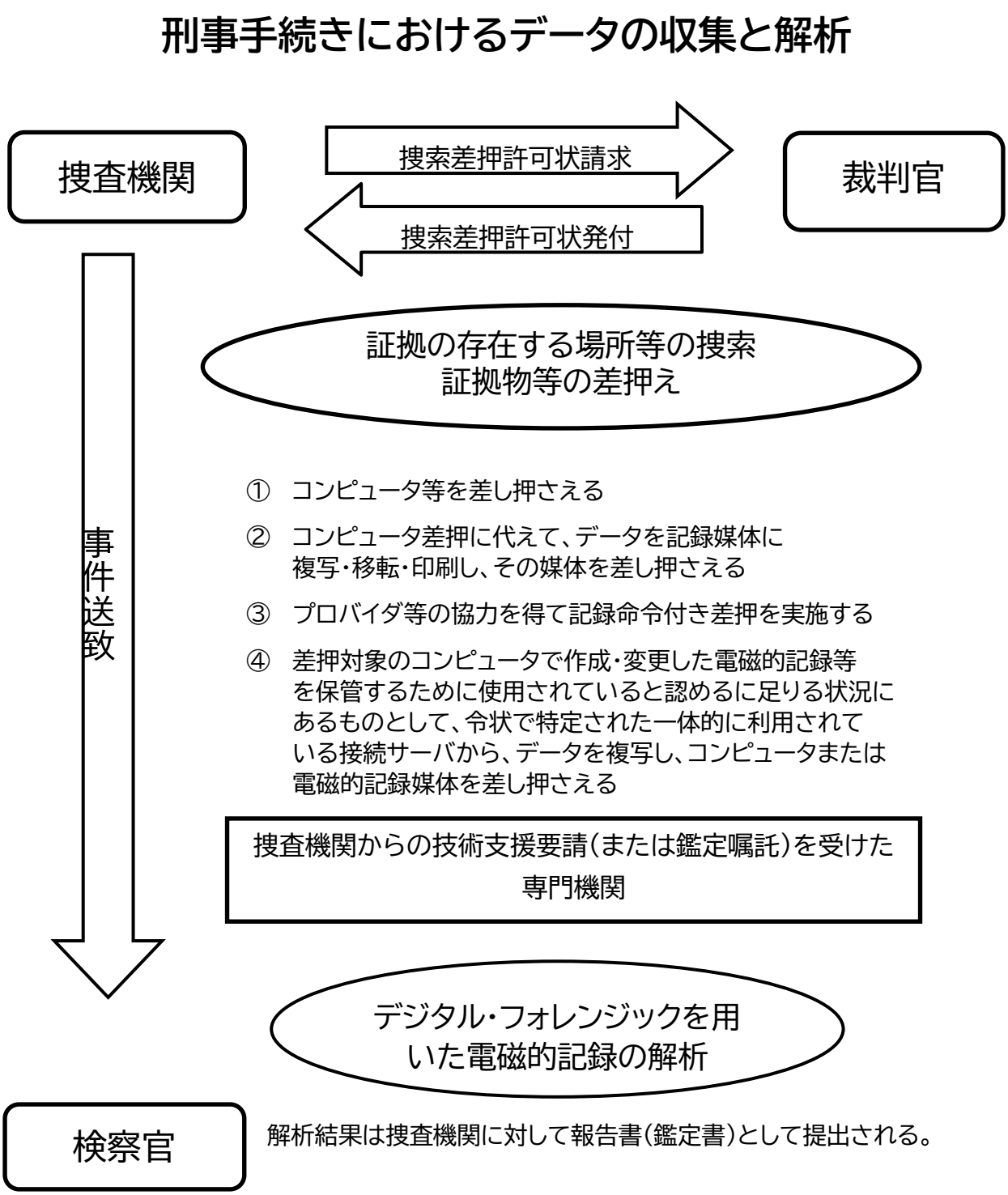
証拠リスト		
証拠番号	容量	証拠の内容

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)

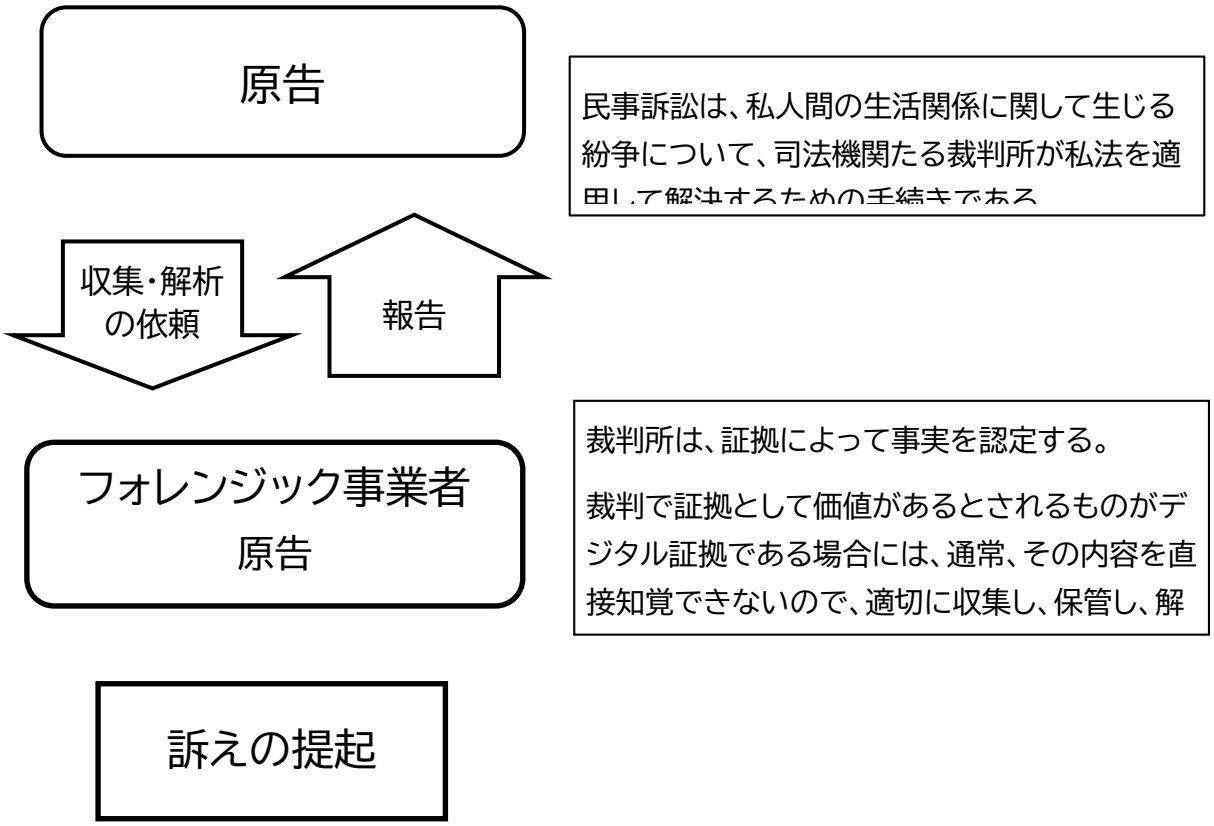
* Picuture(s) may require to show an identity of the evidence

/

F. 刑事・民事におけるデータ収集と解析フローイメージ図



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・顕出の方法は、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（民訴法第 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。

令和 4（2022）年民訴法改正により、裁判所は、当事者に異議がなく、かつ、相当と認めるときは、オンライン方式を活用する検証が可能になった（同法第 232 条の 2）。

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（民訴法第 234 条）。

② 書証（民訴法第 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（民訴法第 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（民訴法第 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（民訴法第 228 条）。

令和 4（2022）年民訴法改正により、電磁的記録に記録された情報の内容に係る証拠調べの申出は、当該電磁的記録を提出し、または当該電磁的記録を利用する権限を有する者にその提出を命ずることを申し立てて行うことになった。この場合、電磁的記録の提出は、記録媒体または電子情報処理組織を使用する方法により行う(同法第 231 条の 2)。

③ 証人（民訴訟第 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。

令和 4（2022）年民訴法改正により、裁判所は、相当と認めるときで当事者に異議がない場合、証人が遠隔地に居住するか否かにかかわらず、オンライン方式での証人尋問の実施が可能になった（同法第 204 条第 3 号）。参考人等の審尋（同法 187 条第 3 項第 4 項）や当事者本人尋問（同法 210 条）も同様である。

④ 鑑定（民訴法第 212 条・第 215 条第 1 項）

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。

令和 4（2022）年民訴法改正により、鑑定人は、電子情報処理組織を使用してファイルに記録する方法や電磁的記録媒体を提出する方法によることが可能になった（同法第215条第 2 項・第 4 項)。

⑤ 調査嘱託（民訴訟第 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。

⑥ 裁判所外での証拠調べ

令和 4（2022）年民訴法改正により、裁判所外で証拠調べを行う際、裁判所は、相当と認めるときは、当事者の意見を聴いて、オンライン方式によることが可能になった（同法第 185 条第 3 項）。

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

G. 供述証拠と事実認定の実務（概論）

※大橋充直会員提供資料：

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！とい得るルである。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 日前の昼飯で何を喰った？」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:刑訴法第 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。たとえば、「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、顛末末書、自供書、告白書……と称する犯罪を認めた署名押印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、義理人情や取引でよってたかって、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:刑訴法第 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。

たとえば、女性従業員 B から「A さんが集金チョロ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(刑訴法第 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)を行なう。

→ 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、拷問または脅迫による自白、不当に長く抑留また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また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、または特に信用

すべき情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 被告人の公判準備また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情況の下に作成された書面

H. 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、被害民間企業また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○○年○月○日（注 1）

○○警察署長　殿（注 2）

○○○○株式会社　技術調査部

○○監査士　○○　○○　(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○○年○月○日……

2　作成場所　　○○県……○○丁目○番○号　○○ビル 6 階

株式会社○○○○　○○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　○○○○）

4　提 供 者　　上記株式会社○○○○　○○支社データセンター

サーバ管理課長　○○　○○

5　作 成 物　　上記サーバ管理課長○○○○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○○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「○○○○. ○○○」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「○○○○. ○○○」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「○○○○. ○○○」等のデジタルデータの写しを提出(提供)させて頂きたい。

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すべ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(たとえば、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) ○○監査士 ○○ ○○ (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 ○○ ○○ (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（またはファイル名）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または著しく困難であることの疎明が必用である（最高裁判所昭和 35 年 2 月 3 日決定・最高裁判例集 14 巻 1 号 45 頁、最高裁判所昭和 35 年 3 月 24 日決定・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。手続き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すべて記載し、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（または「インキャメラ」；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

I. 代表的な収集および分析ツール

●システム関連の情報取得ツールの例

- ArtifactCollector
  マルチプラットフォーム対応のアーティファクト収集ツール。定義済みのアーティファクトテンプレートを用いて、ログ、設定ファイル、メモリイメージなどを自動的に取得可能。
  https://github.com/forensicanalysis/artifactcollector
- Autopsy
  オープンソースのデジタル・フォレンジックツールで、ファイルの回復、システムアーティファクトの収集、タイムラインの作成を行う。
  https://www.autopsy.com/
- CDIR Collector
  Windows システムの主要データを収集し、証拠保全を支援するオープンソースツールセット。システム情報、ネットワーク構成、プロセス情報などを収集。
  https://github.com/CyberDefenseInstitute/CDIR
- CYLR
  Windows システム上のイベントログやレジストリ情報、ファイルメタデータなどの重要アーティファクトを効率的に収集し、標準化された形式で出力するためのツール。
  https://github.com/orlikoski/CyLR
- Eric Zimmerman ツール群
  Prefetch ファイル、レジストリ、MFT、ブラウザ履歴、イベントログなど、幅広いアーティファクトを効率的かつ詳細に解析可能なコマンドラインツール。
  https://ericzimmerman.github.io/#!index.md
- Event Log Explorer
  ローカルコンピュータのイベントログの詳細分析や、ネットワーク上の複数のコンピュータのイベントログを集中管理できる。
  http://eventlogxp.com
- F-Response
  ネットワーク越しに対象システムのディスクやメモリ、クラウドストレージなどへ読み取り専用アクセスを提供し、リモートフォレンジックイメージ取得を可能にする
  https://www.f-response.com/
- Log Parser
  多様なフォーマットのログから必要な情報を抽出・整形し、Excel 形式での出力も可能。
  Windows イベントログ、IIS ログ、ファイルシステムのスキャン結果などを扱える。
  http://www.microsoft.com/download/en/details.aspx?id=24659
- Log Parser Lizard
  上述の Log Parse を GUI で使えるようにする
  http://www.lizard-labs.net
- FTK Imager Lite
  ハードディスク、メモリ、仮想マシンのイメージを取得・閲覧するためのツールで、証拠データを損なうことなく証拠保全用にイメージングする機能を持つ。
  http://accessdata.com/product-download/digital-forensics/

- RTIR（RT for Incident Response）
  Request Tracker for Incident Response の略。インシデントハンドリングに係るワークフローを最適化する。
  https://www.bestpractical.com/rtir/
- SPECTR
  フォレンジックトリアージツール。初動段階でログや設定情報、メタデータなどを迅速に収集し、システム全体の状況把握や簡易解析を支援。
  https://github.com/alpine-sec/SPECTR3
- UAC (Universal Artifact Collector)
  Windows 環境上でさまざまなフォレンジックアーティファクト（イベントログ、レジストリ、ファイル、ネットワーク情報など）をコマンドラインから一括収集する。
  https://github.com/tclahr/uac

●システム関連の解析ツールの例

- analyzeMFT
  NTFS ファイルシステムの Master File Table (MFT)を解析するためのツールで、ファイルの作成、変更、アクセスなどのメタデータを抽出し、フォレンジック分析に有用。
  https://github.com/dkovar/analyzeMFT
- Bulk Extractor
  デジタル証拠の大規模なデータ分析に向いており、パスワード、URL、クレジットカード番号などを大量のデータから抽出する
  https://www.kali.org/tools/bulk-extractor/
- LogonTracer
  Windows のイベントログからログオン情報を可視化し、潜在的な不正アクセスを特定するためのツールであり、アカウントの不正使用の分析に役立つ
  https://github.com/JPCERTCC/LogonTracer
- Velociraptor
  インシデント対応のためのアーティファクト収集や、エンドポイントのフォレンジック分析を迅速に行えるオープンソース
  https://docs.velociraptor.app/

●揮発性メモリの情報取得ツールの例

- AVML (Acquire Volatile Memory for Linux)
  Microsoft が提供するオープンソースのメモリキャプチャツールで、Linux システムでのメモリダンプ取得を支援し、Azure 環境での利用も可能。
  https://github.com/microsoft/avml
- Belkasoft Live RAM Capturer
  32/64 ビット環境に対応した無償のメモリダンプツールで、揮発性データの取得に優れ、デジタル・フォレンジックの証拠保全に活用される。
  https://belkasoft.com/ram-capturer
- DumpIt
  無償で提供されている Windows および Mac 向けのメモリキャプチャツールで、簡単な操作で

メモリダンプを取得可能。
https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/

- Dumpit の Linux 版
  Linux 上でメモリイメージをダンプするためのツール。システムに対する影響を最小化しながらメモリ内容を取得でき、フォレンジック調査に必要な初動保全作業を支援する。
  https://github.com/MagnetForensics/dumpit-linux

- LiME (Linux Memory Extractor)
  Linux 環境向けのメモリキャプチャツールで、ライブメモリのダンプを取得し、デジタル・フォレンジックでの解析を可能にする。
  https://github.com/504ensicsLabs/LiME
- Redline
  Mandiant 社が提供する無償の揮発性メモリキャプチャおよび解析ツールで、Memoryze の GUI フロントエンドとして動作し、メモリダンプの解析に利用される。
  https://www.mandiant.com/resources/download/redline
- Winpmem
  Windows 環境で動作するメモリイメージ取得ツール。システムメモリを整合性を保ったままキャプチャし、Volatility など他の解析ツールへの入力として用いることが可能。
  https://github.com/Velocidex/WinPmem

●揮発性メモリの解析ツールの例

- HBGary Responder Professional
  HBGary 社によって開発・販売されている商用のメモリフォレンジックツール。そのオプション機能として提供されている Digital DNA は、プロセスアドレス空間に含まれるコードを分析して、悪性のコードかどうかをスコアリングする
  http://www.countertack.com/countertack-technology-digital-dna
- Magnet RAM Capture
  物理メモリのキャプチャを行い、データの復旧と解析を支援する無償ツールで、Windows システムで揮発性データの保全に利用される。
  http://www.magnetforensics.com/acquiring-memory-with-magnet-ram-capture/
- Rekall
  Google が支援するオープンソースのメモリフォレンジックフレームワークで、揮発性データの深層解析に適した多様なプラグインが備わっている。
  http://www.rekall-forensic.com/
- Volatility Framework
  オープンソースのメモリフォレンジックツール。プロセス情報の列挙など基本的な機能のほか、有志によってさまざまなプラグインが提供されている。
  http://code.google.com/p/volatility/
- Volatility の GUI (Volatility Workbench)
  コマンドラインツールである Volatility を GUI 上で利用可能にするツール。メモリ解析のワーク

フローを簡易化し、ダンプファイル中のプロセスやモジュール、ネットワーク接続などの可視化・解析を容易にする。
https://www.osforensics.com/tools/volatility-workbench.html
https://github.com/sk4la/volatility3-docker
https://github.com/ufrisk/MemProcFS

●スマートフォンのデータ取得ツールの例

- Magnet Acquire
  Magnet Forensics 社が開発および提供しているスマートフォンの論理データの取得をするツール。無料でありながら、Rooting に対応している。
  https://www.magnetforensics.com/magnet-acquire/

●クラウドフォレンジックを支援するツールの例

- AWS CloudTrail
  AWS 環境でのアクティビティログの取得や監査のためのツール。すべてのアカウントアクションが記録され、フォレンジック調査や監査に役立つ。
  https://aws.amazon.com/cloudtrail/
- AWS Snapshot
  AWS 環境でのボリュームスナップショットを用いたデータ保全ツール。EBS ボリュームのスナップショットを取得し、証拠保全やバックアップに活用できる。
  https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html
- AWS Security Hub
  AWS 内のセキュリティ情報を統合して監視するツール。複数の AWS サービスからのセキュリティデータを集約し、脅威の特定やリスク評価に有用である。
  https://aws.amazon.com/security-hub/
- Azure Security Center
  Azure 環境でのセキュリティ管理と脅威監視のためのツール。セキュリティ設定の強化、脅威の検出、そしてリスク管理を支援する機能を提供する。
  https://azure.microsoft.com/en-us/services/defender-for-cloud/
- Google Cloud Logging (旧 Stackdriver)
  Google Cloud（旧 GCP）環境におけるログの取得と管理のためのツール。クラウドリソースやアプリケーションの活動を収集・管理し、異常検出や調査に利用される。
  https://cloud.google.com/logging
- Microsoft-Extractor-Suite
  PowerShell ベースのモジュールで、Microsoft 365 および Azure 環境からのデータ収集に特化したツール。インシデント対応やセキュリティ調査において、ログ、監査情報、構成情報などの取得を自動化することで効率的な初動対応と可視化を実現する。
  https://github.com/invictus-ir/Microsoft-Extractor-Suite

J. 海外のデジタル・フォレンジック関連情報

- Guideline for Evidence Collection and Archive – IEFT
  IETF が提供する RFC3227 は、デジタル・フォレンジックにおける証拠収集および保存の標準的なガイドラインであり、事件発生時における証拠保全のベストプラクティスを示している。日本語訳も提供されている。
  https://www.ietf.org/rfc/rfc3227.txt
  https://www.ipa.go.jp/security/rfc/RFC3227JA.html
- Digital Intelligence and Investigation – CERT/CC
  CERT/CC（Computer Emergency Response Team Coordination Center）が提供するデジタルインテリジェンスおよび捜査に関するリソースは、サイバーインシデントにおける証拠収集、解析、対応のための情報やツールを網羅しており、デジタル・フォレンジックの実践者に有用である。
  http://www.cert.org/digital-intelligence/
- Network Forensics Handbook – ENISA
  ENISA（European Union Agency for Cybersecurity）が提供する『Network Forensics Handbook』は、ネットワーク上の証拠収集と解析の手法に関する実践的ガイドラインで、ネットワークフォレンジックに関わる専門家のスキル向上を支援する。
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/network-forensics-handbook/view
- Method validation in digital forensics – GOV.UK
  英国政府が提供するデジタル・フォレンジックにおける手法の検証ガイドは、フォレンジック分析の品質と信頼性を確保するための基準を示しており、証拠収集や分析手法が裁判所で認められるための信頼性評価基準として活用される。
  https://www.gov.uk/government/publications/method-validation-in-digital-forensics
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
  米国国立標準技術研究所（NIST）が提供するガイドで、フォレンジック技術をインシデント対応に統合するためのベストプラクティスと手法を示している。
  https://csrc.nist.gov/pubs/sp/800/86/final
- SWGDE (Scientific Working Group on Digital Evidence) Best Practices
  デジタル証拠に関するベストプラクティスを策定する米国の専門組織で、デジタル証拠の収集、保全、解析、報告に関する最新のガイドラインを提供している。
  https://www.swgde.org/
- INTERPOL Digital Forensics Guidelines
  国際刑事警察機構（INTERPOL）によるデジタル・フォレンジックガイドラインで、国際的な事件捜査におけるデジタル証拠収集と保全の標準を提供する。
  https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
- Artifact Reference Guide – Microsoft Incident Reponse Team
  Microsoft 365 環境におけるインシデントレスポンスを強化するため、Unified Audit Logging（UAL）や Microsoft Entra（旧 Azure AD）のログ収集・分析手法をまとめたガイド
  https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MSFT-IR-UAL-Entra-Guide-JAN24.pdf

K. IDF団体会員「製品・サービス区分リスト」

（製品・サービス内容掲載 50 社、会社名・URL掲載 5 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が、掲載を希望されない団体会員の団体名・社名等は記載しておりません。

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データリカバリー、
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

※ 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 FRONTEO https://legal.fronteo.com/	①、②-a,b,c,d、③、④、⑤、⑥、⑧、⑨、⑪、⑫、⑬（経済安全保障ソリューション）	・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 Offife(XRY/XAMN) モバイル端末データ抽出・解析ツール -UltraBlock 書込み防止装置　他 -RECON ITR 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 Communication Meter 人工知能搭載 メール＆チャット 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

IDF団体企業名	サービス区分	主要製品等
株式会社ラック https://www.lac.co.jp/	②-a、③、⑥、⑦、⑨、⑩、⑪	・緊急対応サービス「サイバー119」 ・マネージド EDR サービス ・ラックセキュリティアカデミー　デジタル・フォレンジックコース ・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 攻撃耐性検証（標的型攻撃疑似テスト） ・セキュリティ診断 ・セキュリティコンサルティング
フューチャーセキュアウェイブ株式会社 https://www.dit.co.jp/	①、②-a,b,d、③、⑥、⑦、⑧、⑨、⑩、⑪	・フォレンジックツール（X-WaysForensics）日本語版開発及び代理店 ・コンピュータフォレンジックサービス ・脆弱性診断サービス ・セキュリティコンサルティングサービス ・危機管理対応支援サービス ・EDR 製品（CrowdStrike、FortiEDR） ・特権管理製品（CyberArk、SSH） ・クラウドセキュリティ（Forcepoint） ・セキュリティ対策製品（Fortinet） ・セキュリティ意識向上トレーニング＆フィッシングシミュレーション（KnowBe4）
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
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
AI データ株式会社 https://www.fss.jp/forensic-tool/	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、カーナビ等)、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 Fast Forensics(PC ファスト・フォレンジック) Final Forensics(PC フォレンジック) AndrEx3(Android スマホデータ抽出) 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) UFED（携帯電話データ抽出・分析）
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

IDF団体企業名	サービス区分	主要製品等
エンカレッジ・テクノロジ株式会社 https://www.et-x.jp/	①	製品名：システム証跡監査ツール ESS REC 特長：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 500 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/	②-a,c,d,e(ドライブレコーダー、防犯カメラの他、故障した機器も対応可)、③、④、⑥、⑧、⑨	デジタル・フォレンジック調査サービス ・社員や退職者の機密データ持ち出し・情報漏洩 ・未払い残業代請求時のパソコン操作履歴解析 ・職務と無関係なネット閲覧履歴 ・怪文書、告発文、過労死、自殺、行方不明 ・証拠隠滅（データ消去）経緯の解明 ・契約書や請求書の偽造や不正請求 ・ランサムウェア被害調査 ・訴訟用資料作成、弁護士や裁判官への解説 ・極秘対応可 データ復旧サービス ・ファイルサーバやデータベース等のデータ復旧 ・撮影データ（結婚式、番組制作、取材映像など） ・消失原因と経緯調査及び報告書作成 ・ランサムウェア被害対処 ・クリーンルーム（HDD の分解）データ復旧 ・Apple MacBook、Microsoft Surface のデータ復旧 その他 ・データ消去ソフト及び機器の消去性能検証 ・アメリカ拠点あり（日本人 DF 解析者常駐） ・講義、講演、講習会など
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』
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

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.kumananpcnet.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) Sound Cleaner II (各種音声データ解析、鮮明化ツール) VFC7 (証拠イメージ／証拠ディスク仮想起動ツール) ・PC-3000 JAPAN (HDD、SSD、NAND メモリデータ復旧ツール、トレーニング) ・WinDiskRescue (データ復旧サービス、証拠品鑑定)
株式会社 NTT データ先端技術 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 ・Threat Hunting 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・TLPT 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 合同会社 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
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/cm/3r.html	②、④、⑤、⑨、 ⑬(データマネジ メント)	・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/PC 等の業務外 利用調査/退職者 PC 調査/訴訟支援(E-Discovery) ・経験豊富なレビュワーによるマネージドレビュー ・ボイスフォレンジック ・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 -紙文書の適切な管理を可能にするペーパースキャン ・個人情報検索サービス
EY 新日本有限責任監査法人 https://www.ey.com/ja_jp/forensic- integrity-services	②-a,b,c,d,e(各 種クラウドサー ビス、EDR ログ 等)、③、④、 ⑤、⑥、⑨、⑩、 ⑪、⑬	・初動対応(トリアージ)支援 ・サイバーフォレンジック(インシデントレスポンス) ・サイバーセキュリティ・フォレンジックトレーニング -Windows Forensics -Mac Forensics -File System -マルウェア解析基礎 -プライベートトレーニング(例:CSIRT 向けカスタマイズトレーニング) ・CSIRT 構築・運用支援 ・不正調査、第三者委員会等調査支援 ・eDiscovery 支援サービス ・Forensic Data Analytics

IDF団体企業名	サービス区分	主要製品等
NRI セキュアテクノロジーズ株式会社 https://www.nri-secure.co.jp/	②、③、⑥、⑦、⑨、⑩、⑪、⑫	セキュリティ事故対応支援 PFI クレジットカード情報漏えい調査サービス マネージド EDR サービス　ファスト・フォレンジック セキュリティ資格取得支援（SANS、CISSP） セキュリティ人材育成 セキュリティ運用 セキュリティログ監視サービス(NeoSOC)(400 種以上のデバイスの監視に対応) セキュリティ診断（IoT/OT 含む） サイバーアタックシミュレーション(TLPT) サイバー攻撃対応机上演習サービス 工場向けセキュリティ耕育インシデント対応訓練プログラム セキュリティポリシー・ガイドライン策定支援 組織内 CSIRT 総合支援(構築・運用・評価) 組織内 PSIRT 向け支援サービス CIO/CISO 支援サービス 各種法規制・ガイドライン準拠支援サービス マネージド脅威情報分析サービス
株式会社コンステラ セキュリティジャパン https://www.constella-sec.jp/	、②-a、③、④、⑦、⑨、⑩、⑫	・ネットワークフォレンジック（THX-Capture,THX-Storage,THX-RAA） ・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（THX シリーズ） ・ファストフォレンジック（ThreatSonar） ・エンドポイントセキュリティ（ThreatSonar） ・Bitsight（セキュリティリスクスコアリング/EASM） ・脆弱性調査・ペネトレーションテスト（Spirent Security Lab） ・ネットワーク監視（THX シリーズ）
株式会社ベルウクリエイティブ https://belue-c.jp/	②-a,b、③、④、⑦、⑨、⑩、⑪、⑫	顧客要望に合わせて、診断から運用まで一気通貫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・マネージメントサービス) 』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。

IDF団体企業名	サービス区分	主要製品等
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、⑥、⑦、⑧、⑨、⑩、⑪	【対策支援】 ・デジタル・フォレンジック、マルウェア解析、インシデント対応 ・ペネトレーションテスト、脆弱性診断 ・セキュリティ監査、リスクアセスメント、セキュリティコンサルティングなど 【教育トレーニング】 ・演習やワークショップを取り入れた教育を提供中（主なコース）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、ペンテスター養成コース、インシデントレスポンス、CSIRT 対応訓練など 【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 PFU http://www.pfu.fujitsu.com/	②-a,b、⑥、⑦、⑨、⑩	・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://digitaldata-forensics.com/	②-a,b,c,d、③、⑦、⑧、⑨	365 日年中無休、法人様駆けつけ対応可能。最短 30 分で初動対応の打合せ設定を行います。 ＜フォレンジック調査＆インシデント対応支援＞ランサムウェア感染、情報漏えい、 Web システムのサーバー攻撃被害、不正アクセスなどの被害原因・感染経路特定、 封じ込め、再発防止策のご提案を行います。社内不正、退職時のデータの持ち出し、 職務慢怠調査など、PC・スマホの操作履歴調査も対応可能。 累計 3.9 万件以上の相談対応実績あり。 ＜脆弱性診断・ペネトレーションテスト＞有資格者の技術者がサイバー攻撃から企業の 情報セキュリティを守るための実践的な診断をご提供します。 ＜その他＞データ復旧、セキュリティ対策製品の提供にも幅広く対応。

IDF団体企業名	サービス区分	主要製品等
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、④、⑥、⑦、⑨、⑪、⑫、⑬	・SIEM/フォレンジック製品（RSA NetWitness） ・エンドポイント侵害診断サービス（BlackBerry Protect） ・セキュリティコンサルティング（BCP・リスク対策、リスクアセスメント、情報セキュリティ監査等） ・情報セキュリティ研修サービス ・脆弱性診断サービス（プラットフォーム、Web アプリケーション） ・情報セキュリティポリシー策定支援サービス、CSIRT 構築運用支援サービス ・サイバー攻撃疑似偵察サービス ・その他（脆弱性情報提供サービス等）
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
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

IDF団体企業名	サービス区分	主要製品等
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ー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）
株式会社シンプレクス・リスク・マネジメント https://simplex-rm.com/	①、②-a、③、⑥、⑪	・ファストフォレンジックソリューション(CyCraft AIR) ・デジタル・フォレンジック ・マルウェア解析 ・インシデントレスポンス支援 ・セキュリティコンサルティング ・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 https://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 ・スマホアプリ脆弱性診断 ・Web 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	・OpenText EnCase Endpoint Investigator リモートフォレンジック/トリアージソリューション
株式会社ファイブドライブ https://www.fivedrive.jp/	②-a,b、③、④、⑨、⑩、⑪	・インシデント対応支援 ・マルウェア解析 ・ログ解析 ・脆弱性診断（Web アプリケーション、プラットフォーム、無線 LAN、データベース、ソースコード等） ・ペネトレーションテスト

IDF団体企業名	サービス区分	主要製品等
セコムトラストシステムズ株式会社 https://www.secomtrust.net/	②、③、⑥、⑦、⑨、⑪	・情報セキュリティサービス：セコムプロフェッショナルサポート（インシデント対処、フォレンジック）、セコムサイバー道場（教育）、セキュアエンドポイント（NGAV＋EDR） ・運用/監視サービス：マネージド WAF サービス、セコム不正侵入検知/予防サービス、マネージド/セキュリティサービス、マネージドファイアウォールサービス、DoS 攻撃対策サービス ・セキュリティ診断サービス：セコムセキュリティ診断サービス（ペネトレーションテスト）、Web アプリケーション診断サービス、セコムトータルセキュリティ診断（プラットフォーム診断） ・監査サービス：情報セキュリティ監査サービス ・認証サービス：セコムパスポート for Web シリーズ（SSL サーバー証明書）、セコムあんしんログインサービス
IJB.INC https://www.ijbinfo.com/jp/	①、②-a,c,d、③、⑦、⑫、⑬（ネットワークを介した複数のコンピュータフォレンジックと行為の収集を利用した企業の監査）	各種フォレンジックツール - Qator Live：SSD の形態の非設置型フォレンジックツールとして PC 及びノートパソコンなどのライブ システムに USB ポートに接続してデータ復旧及び キーワード検索及び使用の痕跡などの迅速な調査・分析。 - Qator Forensic：専門フォレンジックツールとして現場で収集されたデータを元通りに、検索、インターネット痕跡など具体的に調査を実施する。 - Qator Enterprise：企業のセキュリティ監査用の マルチターゲットフォレンジックツールの同時多数のコンピュータでフォレンジック業務実行。 - MobileWay：出入セキュリティステッカー破損時のモバイルフォレンジック技術を利用して、モバイル機器を通じた資料の流出時関連資料回復と検索を通じた獲得。 - Privacy Finder：PC に保存されている個人情報（住民登録番号、クレジットカード番号、電話番号、電子メールなど）について保有している現状をリモートで把握して流出の可能性を事前に遮断。
GMO サイバーセキュリティ by イエラエ株式会社 https://gmo-cybersecurity.com/	②-a,b,c,d,e、③、④、⑧、⑨、⑩、⑬（インシデントレスポンス・攻撃復旧支援・脆弱性診断・ペネトレーションテスト・マルウェア解析）	・インシデントレスポンス ・フォレンジック調査 ・脆弱性診断（webアプリ/スマートフォンアプリ） ・ソーシャルゲームチート対策診断 ・ネットワーク診断 ・仮想通貨/ブロックチェーン診断 ・耐タンパー性診断 ・ペネトレーションテスト ・セキュリティトレーニング ・マルウェア解析　他

IDF団体企業名	サービス区分	主要製品等
株式会社 CyCraft Japan https://www.cycraft.com/ja-jp/	③、⑬(フォレンジック調査情報/Threat Intelligenceサービス)	・ファスト・フォレンジックによるインシデントレスポンス用パッケージ/サービス -「迅速性」と「網羅性」に着眼したソリューション -フォレンジックベースの分析システム -分析にAIを利用することにより、省力化と分析高速化を実現 -AIで分析し、レポートを出力まで自動で行うことが可能 -リモートでの対処 -アナリストが分析することが可能なプラットフォームを用意 -アナリストによる分析により、より詳細かつ可視化された報告が可能 ・CyberTotal:1クリックでグローバル脅威インテリジェンスを照会 -業種、国別の脅威ソースのAIによるラベリング -ハイレベルなAPI統合インターフェイス -データエンリッチ化を実現
株式会社 foxcale https://www.foxcale.com/	②-a,c,d、③、④	フォレンジック調査サービス ・デジタル・フォレンジックを活用した各種電子情報の保全・解析およびドキュメントレビュー(自社開発ツールfoxcopeを利用)をはじめとする調査・分析サービスをワンストップで提供しております。 ・大手会計事務所出身者、捜査機関出身者、弁護士等より、第三者委員会調査を始めとする各種の不正・不祥事調査を行っております。 ・また、様々な社内調査等においても、デジタル・フォレンジックの活用も含めた初動対応のご支援・コンサルティングなど幅広いサービスを提供しております。
クオリティネット株式会社 https://www.quality-net.co.jp/	①、 ②-a,b,c,d、③、④、⑤、⑥、⑧、⑨	フォレンジックツールの販売(正規代理店) ・総合型フォレンジックツール EnCase Forensic、FTK、AXIOM、Nuix ・リモート型フォレンジックツール EnCase Endpoint Investigator、AXIOM Cyber ・SNS・クラウドデータ保全・調査ツール AXIOM Cloud ・iOS・Androidデバイスのパスワード解除及びデータ取得ツール Graykey ・Mac/iPhone保全・解析ツール Digital Collector(旧MacQuisition)、Inspector(旧BlackLight) ・HDD/SSD保全・書込防止装置 Falcon-NEO、Tableau、WriteProtectPortable ・物理メモリ・マルウェア解析ツール Responder Pro、IDA Pro、Shadow3 メーカー公認トレーニングの実施 ・EnCase(DF120/210/320)、FTK、AXIOMフォレンジック調査・緊急対応サービスの実施 ・対象:PC(Windows／Mac／Linux)、スマホ等

IDF団体企業名	サービス区分	主要製品等
株式会社東陽テクニカ https://toyo-slc.com/	①、②-b、③、⑦、⑨、⑬ （脅威インテリジェンス提供、クラウドセキュリティ）	・TOYO ThunderBOT（ポータブル型ネットーワークフォレンジックシステム） 脅威インテリジェンスを用いて、通信情報からセキュリティインシデントの可視化 ・ネットワークフォレンジック調査 ・脅威インテリジェンス提供サービス ・パブリッククラウドワークロードセキュリティ対策製品
アスエイト・アドバイザリー株式会社 https://asueito.com/	①、②、③、④、⑤、⑥、⑦、⑨、⑩、⑪	・フォレンジック調査 ・WEB/ネットワークの脆弱性診断、ペネトレーション テスト ・ISMS/P マーク認証取得コンサルティング ・マネージド・セキュリティ・サービス（MSS） ・標的型攻撃対策訓練支援 ・情報セキュリティ対策研修 ・e-ディスカバリ支援、コンサルティング ・CSIRT 構築支援 ・ALMIGHT（メールレビューツール）
太陽グラントソントン・アドバイザーズ株式会社 https://www.grantthornton.jp/aboutus/advisors/	②	会計不正調査と同時に提供するデジタル・フォレンジック調査（世界各国の Grant Thornton メンバーファームと連携した海外調査対応含む）
MSAB Japan 株式会社 https://www.msab.com/ja/	①、②－c, d, e（自動車、ドローン）、③、⑥	・モバイルフォレンジック・ツール －「MSAB Office ロジカル＆フィジカル」（「XRY」＋「XAMN」） モバイル、ドローンのデータ抽出解析カービング・ツール －「MSABキオスク」、「MSABタブレット」 XRYフルパワーを搭載、フルカスタマイズ管理機能搭載端末 －「XRYエクスプレス」 タブレットの機能をお持ちのPCで使えるソフトウェア －「XEC」（エグゼック） MSAB製品クライアント管理ツール －「iVe」（アイビー） 自動車データのフォレンジック抽出・解析ツール ・アンドロイド・アプリ型モバイルフォレンジック・ツール －「RAVEN」（レイヴン） スマホ to スマホで抽出、デコード、検索 スマホ単体でフォレンジック捜査完結、XAMNでの解析も可能 ・ファスト・フォレンジック －「Detego」（ディティーゴ） 高速、高機能なPCファストフォレンジック・ツール ・フォレンジック・サービス、各種トレーニング、アクセサリ －「Access Service」 抽出・解析サービス －「Advanced Acquisition Lab」（AAL） MSABの高度な抽出ノウハウをご提供するサービス ・オンサイト、オンライン、オンデマンド各種トレーニング ・ケーブル・バッグ、5G ファラデイバッグ、ケーブル等アクセサリ

IDF団体企業名	サービス区分	主要製品等
NEC セキュリティ株式会社 https://www.nec-security.co.jp/	②、③、⑥、⑦、⑨、⑩、⑪	・インシデントレスポンス（フォレンジック調査）サービス -マルウェア解析 ・「セキュリティ教育サービス」 -サイバーセキュリティトレーニング、ハンズオントレーニング ・InfoCIC 監視サービス（MDR（マネージドディテクションレスポンス）、WEB 感染型マルウェア検出、マルウェア検知、ネットワークセキュリティログ監視など） ・マネジメントコンサルティングサービス（CSIRT 構築・運用支援、サイバー攻撃リスク分析、情報セキュリティ監査サービスなど） ・セキュリティ診断サービス ・セキュア設計支援サービス ・セキュリティツール・ソリューション提供
株式会社オリエント https://www.orient-t.net/	③、④、⑥、⑨、⑩、⑪、⑫	・「C-Audit」（シー・オーディット）） / セキュリテイ版人間ドック - スウィープ・ディスカバリ、内部脆弱性、すり抜け脅威診断、サイバーハイジーン、内部不正調査 ・セキュリティ診断 -Web アプリケーション診断、SOC, EDR 第三者評価等 ・サイバーセキュリティ・コンサルティング - 組織構築支援、ソリューション評価、技術・プリセールス教育 - 各種リスクコンプライアンス支援 - 事業開発支援 ・サイバーセキュリティ教育
エムオーテックス株式会社 https://www.lanscope.jp/cpms/incident-response-service/	②、③、⑦、⑨	・インシデント対応サービス - ファスト・フォレンジック調査（全量調査） - デジタル・フォレンジック調査 - マルウェア解析 ・セキュリティ監視サービス - NDR（Darktrace）のネットワークセキュリティ監視 ・セキュリティ診断（脆弱性診断） - Web アプリケーション診断 - ネットワーク脆弱性診断 - ペネトレーションテスト - ゲームセキュリティ診断 - クラウドセキュリティ診断 - サイバーリスク健康診断（Panorays）

IDF団体企業名	サービス区分	主要製品等
株式会社デジタル鑑識研究所 https://dflabo.co.jp/	②、③、④、⑨	・デジタル鑑識 - フォレンジック調査サービス ・ファスト・フォレンジック ・訴訟支援 - 司法に対応した証拠保全と書類作成 - 警察対応等指導 ・情報漏洩調査 - UGINT 脅威インテリジェンス
インターネット セキュア サービス 株式会社 https://www.isskk.co.jp/	②-a,b,c,d、③、⑥、⑦、⑨、⑩、⑪、⑫、⑬（セキュリティコンサルティング、スレット・インテリジェンス、インシデント・レスポンス・サービス）	・サイバー・スレット・インテリジェンスサービス - リテーナーサービス - ワンタイムサービス ・脆弱性診断サービス ・アタック・サーフェス・マネージメント（ASM）サービス ・脆弱性管理サービス ・インシデント・レスポンスサービス - ファストフォレンジック - フォレンジック - 各種ログ分析・調査 - インシデント対応 PMO 支援 ・CSIRT 運用支援 ・各種セキュリティトレーニング ・セキュリティ・エスカレーション・センター®サービス

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.iij.ad.jp/
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	https://www.recruit.co.jp/company/profile/
JBCC 株式会社	https://www.jbcc.co.jp/
デロイト トーマツ サイバー合同会社	https://www.deloitte.com/jp/cyber

L.「証拠保全ガイドライン」改訂WGメンバー（所属は2025年2月現在）

※五十音順

「技術」分科会

座　長	名和 利男	日本サイバーディフェンス株式会社　シニアエグゼクティブアドバイザー、IDF理事
副座長	松本 隆	株式会社ディー・エヌ・エー　IT 本部　セキュリティ部、IDF理事
委　員	上原 哲太郎	立命館大学　情報理工学部　教授、IDF会長
委　員	湯淺 墾道	明治大学　公共政策大学院　ガバナンス研究科　教授、IDF副会長
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	櫻庭 信之	第一東京弁護士会　弁護士、IDF理事
委　員	北條 孝佳	西村あさひ法律事務所　パートナー　弁護士、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	東京海上ホールディングス株式会社　IT企画部　リスク管理グループ
委　員	野﨑 周作	有限責任あずさ監査法人　不正リスク対応支援グループ　マネージング・ディレクター
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	ｱｸﾞﾅﾆ ｻﾝｼﾞｪ	大日本印刷（株）　ABセンター
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
委　員	坂　明	公益財団法人　公共政策調査会　専務理事
委　員	砂原 圭太	クオリティネット株式会社　フォレンジック調査員
委　員	小林 隆一	東京地方検察庁刑事部サイバー係 先端犯罪検察ユニット（JPEC）　検事
委　員	川崎 隆哉	株式会社リクルート　経営管理 リスクマネージメント室 CSIRT ユニット インシデントレスポンスグループ

「人材育成」分科会

座　長	小山　覚	NTT コミュニケーションズ株式会社 情報セキュリティ部長
委　員	渡邉 浩一郎	日本マイクロソフト株式会社 クラウドソリューションアーキテクト CISSP, CISA, CEH
委　員	柴山　芳則	株式会社アルファ・ウェーブ　サイバーセキュリティ事業部事業部長
委　員	松井　政裕	NTT コミュニケーションズ株式会社　情報セキュリティ部　主査
委　員	新井　亮太	NTT コミュニケーションズ株式会社　情報セキュリティ部
委　員	廣澤　龍典	株式会社 NTT データグループ、IDF「若手活動」WG 主査
委　員	植草　祐則	特定非営利活動法人 デジタル・フォレンジック研究会 事務局長

オブザーバー

安冨 潔	慶應義塾大学　名誉教授、弁護士（渥美坂井法律事務所・外国法共同事業）
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、IDF理事　兼　顧問

IDF事務局

委員・事務局長 植草 祐則　特定非営利活動法人デジタル・フォレンジック研究会　理事

以上

（空白頁）