「証拠保全ガイドライン 第7版」

2018年7月20日

特定非営利活動法人デジタル・フォレンジック研究会

「証拠保全ガイドライン」改訂ワーキンググループ

© 2018 NPO Institute of Digital Forensics.

（空白頁）

© 2018 NPO Institute of Digital Forensics.

目 次

1. 本ガイドラインについて 1
   1-1. 取り巻く環境の変化（状況認識） 1
   1-2. デジタル・フォレンジックの状況 2
   1-3. ねらいと方針 3
   1-4. 想定読者 3
   1-5. 留意事項 4
   1-6. 謝辞 4
2. 用語の定義 5
3. インシデント発生前の準備 11
   3-1. 活動プロセス及び体制の確立 11
   3-2. 情報収集、情報共有及び分析 11
   3-3. 資器材等の選定及び準備 12
   3-4. 資器材等の使いこなし 13
4. インシデント発生直後の対応 14
   4-1. 初動対応及び証拠保全が未実施の場合 14
   4-2. 初動対応及び証拠保全が着手済みである場合 17
   4-3. 初動対応及び証拠保全を円滑に進めるための活動 18
5. 対象物の収集・取得・保全 19
   5-1. 対象物の状態の把握 19
   5-2. 収集・取得・保全するための対象物の処置 19
   5-3. その他、収集・取得・保全する必要性がある対象物 26
6. 証拠保全の機器 29
   6-1. 複製先に用いる媒体（記憶装置） 29
   6-2. 証拠保全機器に求められる機能 30
   6-3. 証拠保全ツールに関する要件 31
   6-4. その他、証拠保全に必要な機器・機材・施策の準備 32
7. 証拠保全の実施 34
   7-1. 代替機・代替ツール・代替手段の準備 34
   7-2. 立会人等 34
   7-3. 同一性の検証 34
   7-4. 証拠保全の正確性を担保する作業内容の記録 34
   7-5. 複製先の取扱い 35

© 2018 NPO Institute of Digital Forensics.

7-6. ネットワークログからの証拠データ抽出 36
7-7. ファスト・フォレンジックによる証拠データ抽出 38
8. アウトソーシングサービスの証拠保全 39
8-1. 事前に行う準備 39
8-2. インシデント発生直後の対応 39
8-3. 保全方法及び作業手順の検討 39
8-4. 証拠作業にあたっての留意 40
8-5. アカウント所有者の同意 40
8-6. 収集・取得・保全 41
付録資料 42
A. チェックシート （PC の場合） 42
B. デジタル・フォレンジックに関連する我が国の主な刑事法 44
C. デジタル・フォレンジック関連の資料紹介 56
D. Chain of Custody（CoC）シート例 57
E. 刑事・民事におけるデータ収集と解析フローイメージ図 59
F. 供述証拠と事実認定の実務（概論） 62
G. デジタルデータの証拠化・同一性確認調査手続き報告書例 66
H. 代表的な収集及び分析ツール 69
I. 海外のデジタル・フォレンジック関連情報 71
J. ＩＤＦ団体会員「製品・サービス区分リスト」（全４３社） 72
K. 「証拠保全ガイドライン」改訂ＷＧメンバー（所属は 2018 年 7 月現在） 82

© 2018 NPO Institute of Digital Forensics.

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

また、民間企業における基幹業務のクラウド化がますます進展する一方、それらを標的としたサイバー攻撃の技術や手法が急激に高度化及び巧妙化しているため、コンピュータ・システムに残存する証跡やログに依存するデジタル・フォレンジックで実態を解明することが困難になるケースが相次いで発生している。特に、インターネットを積極的に利用したサービスやネットワークで繋がることを前提としたアプリケーションサービスやIoT[2] を悪用したサイバー攻撃が増加傾向にあるため、連鎖的な被害を受ける範囲が拡大している。したがって、調査すべき対象が管理外のコンピュータ・システムやIoTに及ぶことになるため、自組織内で実態解明するには、インターネットとの境界周辺で「ネットワーク上のパケット通信の流れの記録として残されるさまざまなログ（以下、ネットワークログ）等」を集約及び分析することが一般的になってきた。

これに加えて、ここ数年のサイバー犯罪やサイバー攻撃で利用される不正プログラムは、痕跡を残さない回避技術を高度化しているため、コンピュータ・システム内に残存する痕跡やログが極端に少なくなってきている。例えば、高機能化したコマンド方式のシェル及びスクリプト実行環境を悪用した正規プログラムを用いた攻撃が急増しており、正規プログラムが残す証跡やログのみで悪意のある挙動を推し量ることが困難になっている。これを本格的に究明するには、電源供給を絶つと消失してしまう特性を持つ（揮発性が高い）メモリ空間に残存するスクリプト等を収集することが必要であるため、メモリ上の情報の保全の重要性がさらに高まってきている。

---

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

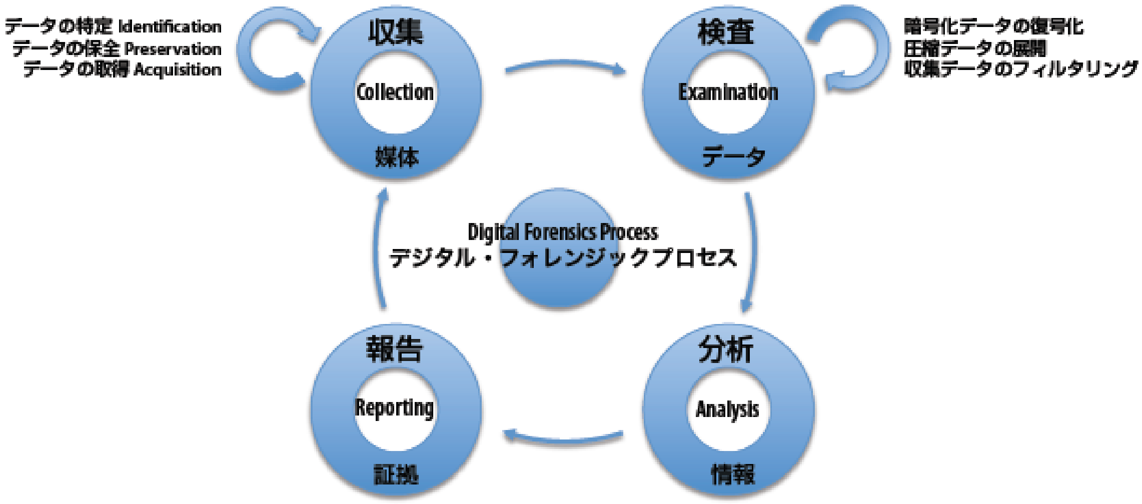
[2] IoT：Internet of Things（モノのインターネット。あらゆるものがインターネットを通じて接続されて、モニタリングやコントロールを可能にする概念のこと。）

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

1-2. デジタル・フォレンジックの状況

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

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



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

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

© 2018 NPO Institute of Digital Forensics.

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

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

1-3. ねらいと方針

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

特に、我が国における電磁的証拠保全の一般的な手続きがどうあるべきか、どの程度まで行えばデータが「法的紛争・訴訟に際し利用可能な（Forensically sound な）電磁的証拠」となり得るか、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及び配慮した事項は、次のとおりである。

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

1-4. 想定読者

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

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

- インシデント：情報の機密性、完全性又は可用性を毀損する行為やソフトウェアの脆弱性を攻略する行為や手段（Exploit）による侵害等、デジタル・フォレンジックの対象となる事案のこと。具体的には、コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等を指す。
- ファースト・レスポンダ：「デジタル・フォレンジックに関する専門的な技能や豊富な知識を習得しているとは限らないが、専門事業者又は捜査機関に引き継ぐために証拠保全手続きを行う可能性のある担当者」としている。

1-5. 留意事項

本ガイドラインは、犯罪捜査や金融調査等、それぞれの特性と法制に基づく手続きが存在することを前提としたものではあるが、記述されている手続き等により収集・取得・保全等された電磁的記録が裁判等において証拠として必ず採用されることを保証するものではないことに留意していただく必要がある。

また、デジタル・フォレンジックへの関わり方やツールの機能等により、取得（抽出）及び分析（解析）の対象となる「証跡とログ」の概念や定義には明示的又は暗黙的に違いがみられる。本ガイドラインの本編において使用している「証跡とログ」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及び記録される情報のこと。英語圏における “Log”（*An official record of events during the voyage of a ship or 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いただいた「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

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

用語〔読み方〕	英語表記	意味
Live Linux 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〕	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〕	Basic Input Output System ／Unified Extensible Firmware Interface	コンピュータ起動時のハードウェアのテスト、OS の起動及び周辺機器を制御するソフトウェアのセットである。周辺機器と OS 及びアプリケーションソフトウェアとの間の制御を司る。
CFTT 〔シー・エフ・ティ・ティ〕	Computer Forensics Tool Testing	法執行機関のニーズに基づきコンピュータ・フォレンジックに用いるソフトウェアツールの評価試験方法を確立するため、米国商務省の標準技術研究所が実施しているプロジェクトである。フォレンジックツールの信頼性を保証するため、性能等を検証している。その結果は公開され、ツールの開発や、民間活用に供されている。
Cookie 〔クッキー〕	Cookie	ユーザ情報をブラウザ内に一時的に記録し参照する機能のこと。書き込まれる情報には、サイトへの訪問回数、ユーザ情報、パスワードなどがある。
DCO（装置構成オーバーレイ） 〔ディ・シー・オー〕	Device Configuration Overlay	ハードディスク装置の容量(例えば 80GB)を異なる容量(例えば 60GB)に OS が認識するように設定することができる機能であり、OS などがアクセス出来ない領域が生ずる。
FAT32 〔FAT：ファット〕	File Allocation Table 32	Windows 95 OSR 2.0 以降や Windows 98/Me で利用されるファイルシステム。ディスクを 2 の 32 乗の小さな単位に分割して管理する。セクターサイズが 512 バイトの場合、最大 2TB までの領域を管理できる。

用語〔読み方〕	英語表記	意味
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、書込み時には OS などを含め全て自動的に暗号化され、読出し時には復号化される。
HDD/SSD パスワードロック 〔HDD：ハードディスクドライブ〕	HDD/SSD Password Lock	ハードディスク装置等のセキュリティ機能でユーザーパスワードを設定すると、電源再投入時にロック状態となり、記録されているデータにアクセスするコマンドが実行不可となる。
HPA（ホスト保護領域) 〔エイチ・ピィ・エイ〕	Host Protect Area／Hidden Protected Area	BIOS 及び OS から、容易にアクセス出来ないハードディスク上の予約領域であり、ハードディスク装置のユーティリティや診断ツールに関わる情報などが記録される。
IDE 〔アイ・ディ・イー〕	Integrated Drive Electronics	パソコンでマザーボードと内蔵ハードディスクを接続するためのインターフェース。2 台のハードディスクが接続でき、それぞれプライマリー、セカンダリーと呼ばれる。現在 IDE と呼ばれているものは、もとの IDE を拡張した「E-IDE（Enhanced IDE）」という規格で、プライマリー、セカンダリーのそれぞれにマスター、スレーブと呼ばれる 2 台の機器を接続でき、計 4 台の機器が利用できる。
IEEE1667 〔IEEE：アイトリプルイー〕	IEEE 1667	IEEE が発行及び管理をしている「ポータブルストレージデバイスのホスト機器接続時認証に関する標準プロトコル（"Standard Protocol for Authentication in Host Attachments of Transient Storage Devices"）」という国際標準規格である。
MD5 〔エム・ディ・ファイブ〕	Message Digest Algorithm 5	1991 年に MIT の Ronald L. Rivest 教授により開発された。入力メッセージに対して 128 ビットのハッシュ値を生成するハッシュ関数である。
NTFS 〔エヌ・ティ・エフ・エス〕	NT File System	Windows NT 系（Windows NT/2000～Windows 10）の標準ファイルシステムのこと。複数ユーザがアクセスするサーバでの運用を想定した設計である。

用語〔読み方〕	英語表記	意味
RAID 〔レイド〕	Redundant Arrays of Independent (Inexpensive) Disks	複数の外部記憶装置(ハードディスク等)をまとめて一台の装置として管理する技術。データを分散して記録することにより、高速化や耐障害性の向上が図られる。専用のハードウェアを使う方法とソフトウェアで実現する方法がある。分散の方法により RAID 0 から RAID 6 まで 7 つの種類があり、それぞれ高速性や耐障害性が異なる。
RAID ボリューム	RAID Volume	複数のハードディスクを組み合わせて、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 ドライブ毎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。
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。

用語〔読み方〕	英語表記	意味
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 3 つに分類されている。
イメージ取得／イメージによる複製／イメージコピー	Imaging	記録媒体に記録されている全てのビット列を正確に複写すること。完全複製／物理複製とも言う。
イメージファイル	Image file	複製元の記録媒体に記録されているビット列を、フォレンジックツールで用いられているフォーマット形式（例えば EnCase の E01 形式）を用いて、論理的な証拠ファイルとして複製先の記録媒体に複写・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、完全性又は可用性を侵害する行為等、デジタル・フォレンジックの対象となる事案。
書き込み防止	Write protection	完全複製等の際に原本となる記録媒体上の電磁的記録の毀損等を防止するため、当該記録媒体への書き込み信号を吸収し書き込みを防止すること。
監査証跡情報	Audit trail information	爾後の検証に備えて、対象事案、フォレンジック作業の管理者、フォレンジックの対象物及びフォレンジックツールを正確に記録しておくこと。
完全複製／物理複製	Duplicate	記録媒体に記録されている全てのビット列を正確に複写すること。
揮発性情報	Volatile Data	コンピュータのメインメモリ上のデータ等、電源が OFF になると保持されないものをいう。

© 2018 NPO Institute of Digital Forensics.

用語〔読み方〕	英語表記	意味
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させないよう、その作業状況をビデオ、写真及び筆記などにより記録すること。
サイバー攻撃	Cyber attack	コンピュータ・システムやインターネットを利用して、標的のコンピュータやネットワークに不正に侵入し、データの窃取、改ざん、破壊等を行い、システムを機能不全に陥らせる一連の行為。
最大許容停止時間 (MTPD)	Maximum Tolerable Period of Disruption	何らかの事象（例えば大規模震災）が発生した場合、システム（業務）が停止してから再開するまで、許容される最大時間のこと。この時間を越えると、ビジネスへの影響が大きく、BCP の観点から限界と判断される停止時間を指し、ビジネス影響度分析において検討される指標である。
作業ログ	Work log	フォレンジックツールへのコマンド入力及び設定情報並びに出力されたハッシュ値など、フォレンジック作業の正確性を検証できるように作業過程が記録された情報。
システム時計	System Clock	コンピュータに内蔵されている時計で、OS が管理している。
ジャンパーピン	Jumper Pin	マザーボードや拡張カード上に用意されている金属のピンのこと。
収集	Collection	電磁的証拠が蓄積されていると思料される IT 機器等を特定し証拠物として押収すること。又は証拠調べの対象として確保すること。
取得	Acquisition	電磁的証拠を物理複製、論理複製又はイメージ取得すること。

用語〔読み方〕	英語表記	意味
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及び物理的な安全性を確保するとともに、取得した電磁的証拠の毀損又は滅失を防ぐため、適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、記録を取り、管理を適正に行うことが求められる。犯罪捜査規範第117条では、「事件の捜査が長期にわたる場合においては、領置物は証拠物件保存簿に記載して、その出納を明確にしておかなければならない」と規定している。

3. インシデント発生前の準備

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

3-1. 活動プロセス及び体制の確立

初動対応及び証拠保全を実施可能な活動プロセス及び体制を確立する。

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

《考慮すべき事項》

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

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

《考慮すべき事項》

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

3-2. 情報収集、情報共有及び分析

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

- 多様化かつ高度化するインシデントに対して、迅速かつ的確に対応するための関連ニュースや技術情報等の収集及び分析。

- 揮発性情報の取得手順・内容及び範囲（メモリダンプ、アプリケーション関連情報）の明確化及び文書化。
- 初動対応及び証拠保全に関連する外部組織や他部門等との情報共有並びに相互連携の確立。

3-3. 資器材等の選定及び準備

初動対応及び証拠保全において、必要と考えられる資器材等を選定及び準備する。

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

《考慮すべき事項》

- *情報の取得過程において、オリジナルのデータを極力変更しないこと。*
- *情報の取得過程において、極力（原本への）書込みを発生しないこと。*
- *情報の取得過程において、不要なネットワーク通信が発生しないこと。*
  （詳しくは、「4. 3　証拠保全ツールに関する要件」参照）
- *外部 OS 起動用ディスク等。*

- 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

初動対応及び証拠保全のために使用する資器材等を使いこなせる状態にしておく。

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

《考慮すべき事項》

専門家や経験者による支援が必要な場合は、付録「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。

---

[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。

4. インシデント発生直後の対応

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

4-1. 初動対応及び証拠保全が未実施の場合

4-1-1. 発生したインシデントの積極的な把握

（種類）

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

（検知又は発覚のきっかけ）

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

（発生時刻）

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

（初動対処の開始までの記録）

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

- 発生したインシデントを知る人物及び人数
- インシデントの対象物の確保の有無

- 確保していた場合： 対象物を確保した日時、確保した人物（役職）、確保した場所、確保時の対象物（及びその周辺）に対する行為、確保後の対象物に対する対処（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（及びその周辺）の状態を詳細に記録する。

4-1-2. 発生したインシデントに関する対象物の決定（流れ図は図１参照）

（対象物に対する情報収集及び対象物の絞り込み）

- 発生したインシデントに関する対象物の種類及び個数
  - コンピュータ（タブレット型／ノート型／デスクトップ型／サーバ型）
  - ネットワーク機器（ルータ、ファイアウォール、侵入検知システム（IDS）、侵入防止システム（IPS））
  - ハードディスクドライブ（以下、HDD／SSD）（バルク／外付け）
  - ストレージメディア（CD／DVD／ブルーレイディスク（BD）／各種フラッシュメモリ等）
  - より揮発性の高い対象物（メモリ）
  - 携帯電話、スマートフォン、タブレット端末
  - 音楽プレイヤー
  - ゲーム機器（ニンテンドー 3DS[6]、プレイステーション 4[7]、プレイステーション Vita、Nintendo Switch、Xbox One™ [8] 等）
  - IC レコーダ
  - ストリーミングデバイス（Chromecast[9]、Fire TV Stick[10] 等）

---

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

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

[8] 「Xbox 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 Inc.の商標または登録商標です。

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

  - 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）
- 発生したインシデントに関する対象物の状態（いつ、どこに存在していたか等）
- 発生したインシデントに関する対象物の使い始めと終わり及び使用頻度
- 発生したインシデントに関する対象物の使用者及び管理者
- 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器及びドキュメントの有無

（対象物の選定と優先順位付け）

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

4-1-3. 証拠保全を行う上で必要な情報の収集

（対象物の情報）

- 対象物の形状、個数、物理的な状態
  - 対象物のラベル情報（メーカー／型番／モデル名／シリアルナンバー／セクターサイズ／総セクター数／記憶容量）、ケーブルの接続状況、ジャンパーの設定状況、HPA[11]・DCO[12] の設定の有無等、通常環境下で視認可能な物理的破損・損傷の有無

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

- HDD／SSD・ストレージメディアの記憶容量、インターフェースの状況
  - 特に、HDD／SSD を筐体から取り出せず、外部 OS 起動用ディスク等で証拠保全を行う場合、光ディスクのドライブ及び USB/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

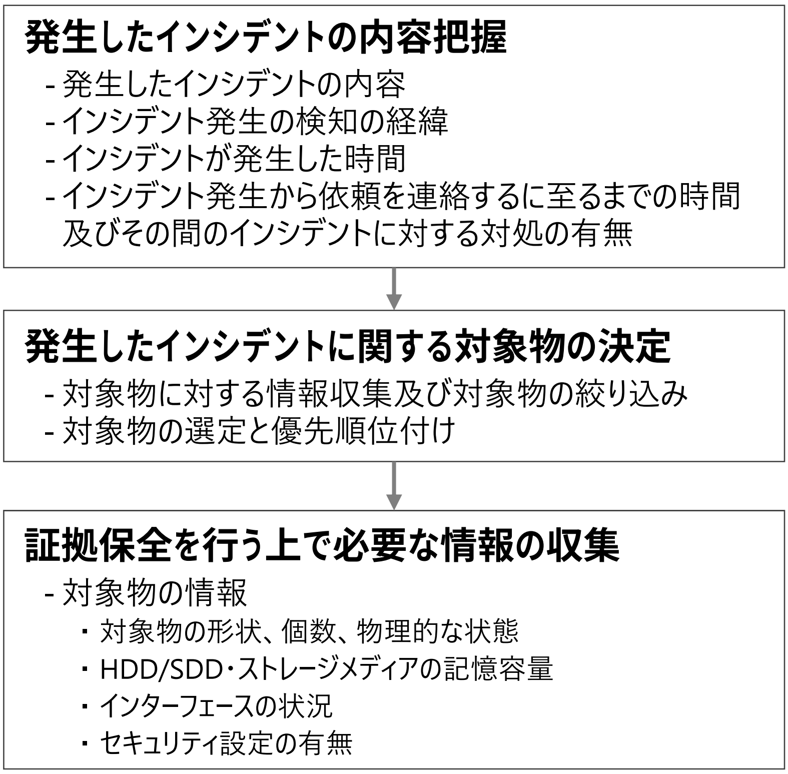
---

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

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

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

- HDD／SSD パスワードロック、HDD／SSD 全体暗号化又は一部のファイル・フォルダの暗号化、PC 周辺のワイヤストッパー、ロッカー、IC カード等



発生したインシデントの内容把握

- 発生したインシデントの内容
- インシデント発生の検知の経緯
- インシデントが発生した時間
- インシデント発生から依頼を連絡するに至るまでの時間及びその間のインシデントに対する対処の有無

発生したインシデントに関する対象物の決定

- 対象物に対する情報収集及び対象物の絞り込み
- 対象物の選定と優先順位付け

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
  - ・ HDD/SDD・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
  - ・ セキュリティ設定の有無

図 1 本節の作業内容を示すフローチャート

4-2. 初動対応及び証拠保全が着手済みである場合

4-2-1. 上記項目 3.1 に関する各種情報の確認

対象物の選定及び情報の収集が完了している場合、それらを次の観点で確認する。

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

4-2-2. 発生直後の初動対応及び証拠保全の実施内容の聴取

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

4-2-3. 対応に過不足が確認された場合の対処

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

4-3. 初動対応及び証拠保全を円滑に進めるための活動

4-3-1. 物理的環境の確保

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

4-3-2. 関係組織との連携

- CSIRT／SOC 担当者、法務部門担当者、システム担当者等との連携。
- システム設計者又は管理者との関係構築。
  - 例：構成が複雑なシステム全体ないしその一部の証拠保全を行う際等。
- 内部監査・システム監査担当者との連携。
  - 依頼元組織内のセキュリティやプライバシー施策を十分に考慮・遵守。
- 関係者の確保及び無関係者の排除。
  - 初動対応及び証拠保全の作業工程において、関係ない第三者が関与できない状況を確保。
  - 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及びその状況下となった経緯と時間・人物についてインタビューする。

5-1-2. 電源の供給停止の可否について

- 対象物に電源を供給し続けることで明白な被害（破壊等）の拡大又はそのおそれが見られる場合、速やかに電源の供給を停止する必要がある。また、不要な通信のみを避けたい場合、電源の供給を継続したままネットワークから切り離す。
- 速やかに電源の供給を停止する必要が見られない場合、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。

© 2018 NPO Institute of Digital Forensics.

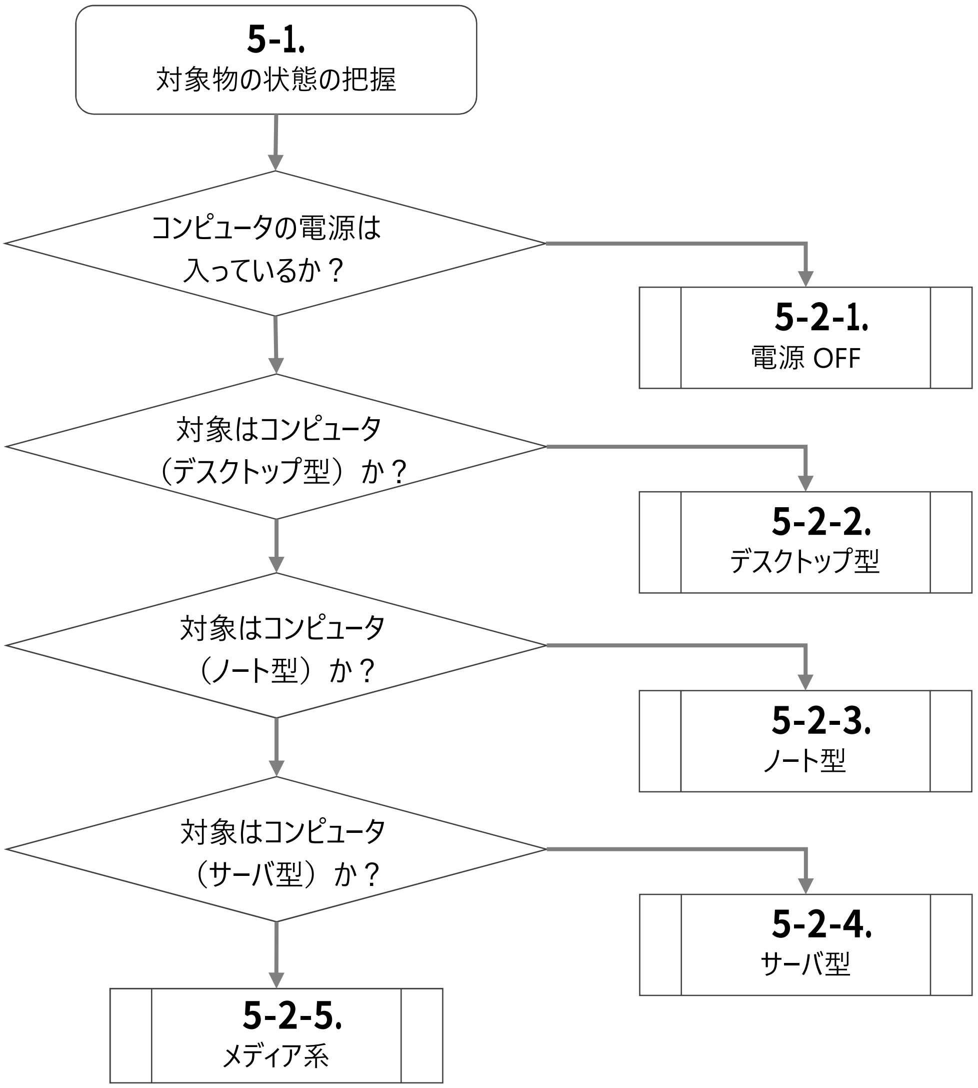


図 2 主な収集・取得・保全するための対象物の処置の選択

5-2-1. 対象物がコンピュータで、電源が OFF の状態の場合

- 原則として電源を ON にしてはならない。
  - HDD／SSD 全体暗号化等、やむを得ず電源を ON にしなければ証拠保全ができない場合を除く。ただし、その場合も証拠保全作業の責任者の指揮の下、電源を ON にした時のリスク（ファイルのタイムスタンプや内容の変更などの影響）を受容して、証拠保全作業を実施する。
  - ファームウェアのマルウェア感染や意図的な改ざんが行われる可能性がある場合は、電源を ON にするとインシデントが深刻化する場合がある。
- 無為に HDD／SSD にデータの書き込み等が発生しないように、ケーブル類は全て筐体から取り外す。
  - 電源ケーブル、キーボード・マウス、USB 系のコネクタ類を取り外す。

- 用途不明の接続ケーブルの場合は、その接続ケーブルについて熟知している人物に用途等を確認し、証拠保全作業の責任者の指揮の下、作業を行う。

- 各装置・ケーブルの取り外しの際は、解析時におけるシステムの正確な再現、作業後の現状復帰を可能にするため、どのケーブルや機器が、どこに取り付けられていたかを、粘着性の低いタグ、専用の荷札タグ等を貼って明確にする（記録シート に明記／写真撮影等。図 3）。特に証拠保全対象となる機器の固有情報（製造番号、型式等）は確実に記録する。

図 3 ケーブル等へのラベル貼付状況の記録

5-2-2. 対象物がコンピュータ（デスクトップ型）で、電源が ON の状態の場合

- コンピュータの種類・規格、使用 OS の確認及び確保時点でのシステム時計の正確性（日本標準時等との差異）を目視又はコマンドで確認・記録。
- ネットワーク環境の確認。

© 2018 NPO Institute of Digital Forensics.

  - ISP、メールソフト、認証情報、電子メールアドレス、メール転送設定、ブラウザの種類、プロキシ設定等。

- 対象物確保時に、画面やプリンタ等、出力装置に表示又は出力されていた状況を具体的に記録（写真撮影等）。
  - やむを得ない場合を除き、ファイルやアイコン、その他の不審な画面の動き等に極力触れてはならない。
  - 可能であれば、バックグラウンドで稼働していたプロセス等も併せて確認する。
- 揮発性情報の取得。
  - 調査の目的、必要に応じて、揮発性情報を取得する。
  - 削除ファイルの復元への影響を最小限にしたい場合は、揮発性情報を取得せず、電源ケーブルを抜く。
  - 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、ケーブル類は全て筐体から取り外す。
  - 電源ケーブル、キーボード・マウス、USB 系のコネクタ類を取り外す。
  - WiFi（無線 LAN）及び Bluetooth の機能を停止する。
  - 用途不明の接続ケーブルの場合は、その接続ケーブルについて熟知している人物に用途等を確認し、証拠保全作業の責任者の指揮の下、作業を行う。
- 各装置・ケーブルの取り外しの際は、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）。特に証拠保全対象となる機器の固有情報（製造番号、型式等）は確実に記録する。

5-2-3. 対象物がコンピュータ（ノート型）で、電源が ON の状態の場合

- コンピュータの種類・規格、使用 OS の確認及び確保時点でのシステム時計の正確性（日本標準時等との差異）を目視又はコマンドで確認・記録。
- ネットワーク環境の確認。
  - WiFi（無線 LAN）及び Bluetooth：設定情報等。
  - メールソフト：認証情報、電子メールアドレス、メール転送設定等。
  - ブラウザ：種類、バージョン、拡張機能（アドオン）、プロキシ設定等。
  - その他のアプリケーション：種類、バージョン、認証情報等。
- 対象物確保時、画面やプリンタ等、出力装置に表示又は出力されていた状況を具体的に記録（写真撮影等）。
  - やむを得ない場合を除き、ファイルやアイコン、その他の不審な画面の動き等に極力触れてはならない。
  - 可能であれば、バックグラウンドで稼働していたプロセス等も併せて確認する。
- 揮発性情報の取得。
  - 調査の目的、必要性に応じて、揮発性情報を取得する。
  - やむを得ない場合を除き、アイコン、その他の不審な画面の動き等に極力触れてはならない。
- 電源を OFF にする。
  - 電源ケーブル、キーボード・マウス、USB デバイス系のコネクタ類を取り外す。
  - 5.2.6 参照。
  - デスクトップ型と異なり、ラップトップ型は筐体底面にバッテリーパックがある為、プラグをコンセントから抜いても強制的な電源 OFF にはならない。
  - 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[14] 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[15] 等）で起動し、RAID 上で構成されている論理ボリューム単位等で取得することで、RAID ボリュームの再構成が可能。
- RAID 装置を一式持ち帰ることが可能な場合もあるが、会社の業務用サーバ等で利用している場合、RAID 装置の使用有無にかかわらず、サーバの停止が困難である可能性が高い。この場合、業務に大きな影響を与えない範囲で、時間はかかるがイメージ取得を実施する。

5-2-5. 対象物がコンピュータ以外（メディア系）の場合

（外部メディア等の物理的管理と記録）

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

（外部メディアにアクセスする PC 等の特定）

- IEEE1667[16] 規格や特定ソフトウェアを利用して、デバイスのロック機能を USB メモリに組み込み、接続時に認証（パスワードの入力等）に成功しないと外部メディア内のデータにアクセスできないような設定も考えられるため、外部メディア内のデータにアクセスしていた PC 等を特定する。

（使用されているファイルシステムの特定）

- 外部メディアに使用されているファイルシステムを特定する。

5-2-6. 電源を OFF にする際の注意点

- 感電や帯電を防止するため、貴金属は身につけず、帯電防止用手袋を装着して作業を実施する。
- 強制的に電源を OFF にする場合。

---

[14] RAID：Redundant Arrays of Inexpensive Disks

[15] 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。

[16] 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。

  - 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。
    - ✧ データ又はファイルが破損し、読み取れなくなる危険性がある。
    - ✧ 稼働中だったプロセスがレジストリやイベントログに書き込まれず、直前の行動が把握できない可能性がある。
    - ✧ 揮発性情報が取得できない。
- 通常のプロセスで電源をOFFにする場合。
  - 想定されるリスクの例：
    - ✧ HDD／SSDに物理的な損傷（不良セクター）が生じやすい。
    - ✧ 揮発性情報が取得できない。

5-2-7. 電源をOFFにしてはならない場合等

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

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

5-2-8. 揮発性による処理順序

- 証拠保全においては、揮発性の高い情報から順に処理する。（表1参照）

表 1 証拠収集における揮発性と順序

揮発性：高	レジスタ、キャッシュ
	ルーティングテーブル[17]、ARP キャッシュ、プロセステーブル、カーネル統計、メモリ[18]
	テンポラリファイルシステム[19]
	ディスク
	当該システムと関連する遠隔ロギングと監視データ
↓	物理的設定、ネットワークトポロジ
揮発性：低	アーカイブ用メディア

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

5-3. その他、収集・取得・保全する必要性がある対象物

5-3-1. サーバ及び通信・監視装置のネットワークログ

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

- 「セキュリティ対策で利用される通信・監視装置」で取得すべきネットワークログ
  - プロキシサーバ

    外部の Web サイトにアクセスする全ての URL の記録が得られる。
  - IDS 及び IPS

    疑わしい挙動や進行しつつある悪質な活動を検知又は防止する措置に関する記録が得られる。但し、予め設定されたルールセットに基づく措置であるため、想定しない未知の挙動等の場合は措置されないことに留意すべきである。
  - ウイルス対策ソフトウェア

    マルウェアが侵入又は動作に成功した記録が得られる。但し、全てのマルウェアの存在や活動を検知するものでないことに留意すべきである。

---

[17] 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

[18] メモリ：コンピュータのメインメモリ（RAM）

[19] 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）

© 2018 NPO Institute of Digital Forensics.

- リモートアクセスのソフトウェア

  VPN ソフトウェアにより、接続が確立された日時やログインユーザ毎のセッションで送受されたデータ量の記録が得られる。ソフトウェアによっては、リソースの使用状況に関する情報も記録できるものもある。

- 脆弱性管理ソフトウェア

  管理対象のサーバのパッチのインストール履歴や脆弱性の有無に関する記録が得られる。

- 認証サーバ

  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。

- ルータ

  トラフィックを遮断した記録が得られる。

- ファイアウォール

  設定したポリシーによって発生する実行ログが得られる。

- 検疫システム

  検疫（チェック）したコンピュータ・システムの実行記録と検査結果の記録が得られる。

- PC やサーバ上にインストールされている「オペレーティング・システム」で取得すべきネットワークログ

  - システムイベント

    それぞれのイベントについて記録される情報は異なるが、一般には、イベント毎のタイムスタンプ、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

    例えば、メールサーバの場合は送信元／宛先／件名／添付ファイル名等、Web サーバの場合はアクセス元／応答結果等、業務アプリケーションの場合はユーザ名／アクセス先リソース／ログイン・ログアウト時刻等

  - アカウントに関する情報

    認証及びその試行回数、アカウント作成／変更／削除、利用した権限、リソースの使用時間等

- 使用状況に関する情報

  トランザクションの件数や一定時間内の頻度、トランザクションのサイズ等

5-3-2. 対象物のマニュアル・ユーザガイド等のドキュメント類

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

表 2　製造者別の主な BIOS 起動キー

PC 製造者	BIOS 起動キー
Acer	Del 若しくは F2
旧 Compaq	F10 若しくは F1、 F2、 Del
Dell	F2
eMachines	Tab 若しくは Del、又は F2
Fujitsu	F2
Gateway	F1
Hitachi	F2
HP	F10
IBM/Lenovo	F1 若しくは F12
Lenovo	F1 若しくは F12
NEC	F2
Panasonic	F2
Phoenix Award BIOS 標準	DEL
Sony	F2 若しくは F3 のち F2、 F3 のち F1
Toshiba	Esc のち F1

© 2018 NPO Institute of Digital Forensics.

6. 証拠保全の機器

6-1. 複製先に用いる媒体（記憶装置）

6-1-1. 媒体のチェック

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

6-1-3. 完全（物理）複製

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

6-1-4. 可読・可搬媒体

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

- 複製先に HDD／SSD を用いる場合、汎用性の高い SATA[20] 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。

---

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

6-2. 証拠保全機器に求められる機能

6-2-1. 書込み防止機能

- 原本に対し、いかなる書込みも行うことができない機能を有する装置を用意するか、原則としていかなる書込みも行うことができない措置を取ること（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、不良セクターの位置等を確認する（これにより、ハッシュ値[21] が原本と異なった場合に説明が可能となる）。
- 対象物（複製元）を、内容だけでなく記録順・構成も全て物理的に複製する（Single Capture）。
- イメージファイルとして複製する（Linux DD コマンド／EnCase Image 等）。

表 3　証拠保全機器に求められる機能

■書き込み防止機能
- 原本に対しいかなる書込みも行うことができない

■完全（物理）複製機能
- 対象物全領域を複製することができる
- 不良セクターへの対応
- 物理的及びイメージによる複製

■同一性検証機能
- ハッシュ値やバイナリコンペア等による同一性検証
- セクターサイズの表示

■作業ログ・監査証跡情報の表示・出力機能
- 対象物及び複製先の詳細情報
- 作業内容及び各種設定情報
- 作業時間等の作業結果
- 作業者情報
- 機器情報

---

[21] 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）。

6-2-3. 同一性検証機能

（同一性の検証（複製時のベリファイ））

- 対象物（複製元）及び複製先のハッシュ値を計算し、これらを照合して同一性を検証する。
- ハッシュ値を用いずに、バイナリコンペア等により同一性を担保しても良い。
- 不良セクター等により複製元と複製先のハッシュ値が一致せず、ハッシュ値による同一性検証が困難な場合、検証時の状況（機器の画面等）の写真撮影や複数人の現場立会い等により同一性を担保する。

（セクターサイズの確認機能）

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

6-2-4. 作業ログ・監査証跡情報の表示・出力機能

（作業ログ）

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

（監査証跡情報）

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

6-3. 証拠保全ツールに関する要件

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

- 対象物と同一の OS 上で起動可能なソフトウェア又はプログラムを利用。
  - GUI（Graphical User Interface）形式又はコマンドラインによる使用。
- 証拠保全ソフトウェア又はプログラムが記録されている DVD や USB デバイス等のブートによる利用。

- HDD／SSDを筐体から取り出せない、若しくは困難、取り出すことは容易でも原状復帰が困難である場合に利用。
- 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、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[22]）等の信頼できる機関にて検証されたものが望ましい。

6-3-3. 代表的な収集及び分析ツールの利用時の留意事項

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

> *《考慮すべき事項》*
>
> *代表的な収集及び分析ツールの使用に当たっては、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の物理的制限及び（強制）解除機能の有無の確認

- HPA、DCO等の確認を実施する。

---

[22] 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/）

6-4-2. HDD／SSD パスワード・暗号化に対する準備

- 対象物を起動せず、解析の段階で復号可能な施策があれば、その手法を選択する。
  - ただし、初動対応及び証拠保全に要する時間や優先順位により、その施策が取れない場合もある。
- やむを得ず対象物を起動する場合。
  - 起動することによるデータの作成・上書き・改変等のリスクを認識すると共に、依頼元に対する十分な説明を行い、同意を得た上で作業する。

6-4-3. IDE[23]　HDD／SSD に設置されているジャンパーピンの取扱い

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

6-4-4. RAID 装置や構造が複雑なサーバ類の証拠保全

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

6-4-5. 事前の十分なテスト及び機能の稼働状態のチェック

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

---

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

7. 証拠保全の実施

7-1. 代替機・代替ツール・代替手段の準備

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

7-2. 立会人等

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

7-3. 同一性の検証

対象物（複製元）及び複製先に対し、完全（物理）複製実施時にハッシュ値の算出を行うなど、同一性を検証する。ライブでのイメージ取得やハードディスクの不良セクター等により、複製元のハッシュ値の算出が困難な場合は、複製先のハッシュ値のみを算出する。証拠の同一性検証に関しては、「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、ツールの信頼性及び証拠保全作業の正確性をもって行う。

7-4. 証拠保全の正確性を担保する作業内容の記録

7-4-1. 活動履歴の記録

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

7-4-2. 証拠保全に関わる機器の情報の記録

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

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

7-4-3. ビデオ及び写真撮影

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

7-5. 複製先の取扱い

7-5-1. 厳重な管理

　複製先は、他の機器と混在しないように、物理的に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[24] 等を作成して、厳重に管理する。

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

7-5-2. フォレンジックチーム等への提出・譲渡

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

7-5-3. 保全対象の確認

- 保全対象の現在の状況を確認する。
- 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。

---

[24] 「誰が、いつ、何をしたのか」が把握できる書類。

- 保全されたデータの件数やデータの状態を確認し、事前に想定した保全対象が全て取得されていることを確認し、記録する。

7-5-5. 同一性の検証

- 保全されたデータ、及び一連の保全作業で取得した動画やスクリーンショット等の作業記録に対して、ハッシュ値を算出する。
- 証拠の同一性検証に関しては、「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、ツールの信頼性及び証拠保全作業の正確性をもって行う。

7-5-6. 保全のため変更した設定の復元

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

7-6. 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、検証及び運用の過程で、ネットワークパフォーマンスや運用監視の都合上、ネットワークログフォーマットが初期状態から変更されている可能性があることに留意しなければならない。
- 取得できていなかった期間を明確にし、取得されていない原因・理由を可能な範囲で確認し、第三者が確認可能な形で記録を残す必要がある。
- ネットワークログに自動的に記録されているタイムスタンプの状態を把握するため、調査で用いる基準時と、データ抽出作業時点での抽出対象システムの時間との誤差を確認する必要がある。
- これらは証拠保全のみならず、その後の調査の前提となるため、ネットワークログのデータ抽出作業を始める前に、必ず行わなければならない。

7-6-2. 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、情報単体若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 4　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 アドレス及びポート番号、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又は既存のマルウェアの分析結果から得られた「攻撃シーケンス（コンピュータ及びネットワーク上の攻撃の挙動パターン）」からの「参考情報」の収集
- 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全てネットワーク機器、オペレーティング・システム、アプリケーション等のネットワークログを、「キー情報」及び「参考情報」を基に相関的な観点で調査
- 例えば、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及びコピーし、解析すること[25] である。

このニーズの背景には、業務利用されるシステムやサイバー攻撃に利用されるマルウェアのネットワーク化（相互接続）、急増するファイルレス攻撃のメカニズム解明にあたりメモリ上の揮発性情報の取得及び保全の高まり、SSD 搭載デバイスとディスクの大容量化等がある。

インシデント発生の現場におけるファースト・レスポンダは、一つのデバイスを深く調査する暇がなくなってきており、迅速な原因究明や侵入経路の特定をするために最低限のデータ抽出・解析をすることが求められてきている。

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、イベントログ、プリフェッチ、レジストリ、ジャーナル、メタデータ、インターネット（ブラウザによる閲覧履歴、メーラ等の設定及び送受データ）、メモリなどである。

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

※ 専用ツールは、「H. 代表的な収集及び分析ツール」を参照

---

[25] 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

© 2018 NPO Institute of Digital Forensics.

8. アウトソーシングサービスの証拠保全

コンピュータ・システムに関するアウトソーシングサービスは、大きく分けてデータセンター（ハウジング）プロバイダ、レンタルサーバ（ホスティング）プロバイダ、クラウドプロバイダ、マネージドサービスプロバイダ（MSP）がある。

特に、クラウドプロバイダは、契約者に対して提供されるリソースの範囲によって区別があり、仮想化されたコンピュータ・システム基盤をインターネット経由で提供する IaaS（Infrastructure as a Service）、ソフトウェア基盤を提供する PaaS（Platform as a Service）、ソフトウェア部分を提供する SaaS（Software as a Service）等が存在する。機器の稼働状況を監視し、ソフトウェアを最新の状態に保ち、トラブル発生時の対応を請け負うマネージドサービスプロバイダ（MSP）のサービスを、データセンター（ハウジング）プロバイダやレンタルサーバ（ホスティング）プロバイダ等が付加サービスとして提供するケースが散見されている。

最近では、CASB（Cloud Access Security Broker：キャスビー）と言われる、複数のクラウドサービスの利用ユーザとクラウドプロバイダの間に配置し、単一のコントロールポイントにより、認証、シングルサインオン、アクセス制御、データ暗号化、ログ取得、マルウェア対策等、クラウドサービスへのアクセスに関するセキュリティポリシーを適用するサービス又は製品の導入が始まっている。

8-1. 事前に行う準備

保全対象となるサービスの利用契約や約款において、次の事項を確認する。

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

8-2. インシデント発生直後の対応

インシデント発生後速やかに、次の事項を記録及び保存する。

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

8-3. 保全方法及び作業手順の検討

サービスからの保全方法及び作業手順を確認及び検討する。

- サービスが標準で提供しているデータのバックアップ／エクスポート。

《考慮すべき事項》
データを暗号化している場合は、回復用のキーも取得すること。

- エクスポートが未対応若しくは困難な場合、プロバイダに保全作業を依頼する等の別手段を検討。
- ローカル端末にバックアップやデータのキャッシュが存在する可能性がある場合、ローカル端末の保全を検討。

8-4. 証拠作業にあたっての留意点

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

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

《考慮すべき事項》
取得した通信パケットを、証拠保全の作業記録と時系列に関連付けておく。

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

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

8-5. アカウント所有者の同意

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

- 対象アカウントが個人に属する場合、保全は本人の同意を得て行う。
- 同意の事実を後日確認するため、同意内容を書面に記録する。
- 家族など、保全対象アカウントを複数の人間で管理している事実がある場合、可能な限り全員の同意を得る。

- 同意内容には、保全対象アカウント及びパスワードの開示、排他制御のための作業中のパスワード変更、データのエクスポートの許可等を記載する。
- 本人の同意を得てパスワード等の変更を行う場合は、アカウント設定変更記録を作成して、厳重に管理する。

8-6. 収集・取得・保全

8-6-1. アクセス可能なアカウントのチェック

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

8-6-2. 作業記録の作成

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

8-6-3. サービスの利用状況のチェック

- ブラウザ若しくは専用のクライアントツールを用いてサービスにアクセスし、アカウント及びパスワードを入力して、ログインする。
- 正常に対象サービスへのアクセスが確認された後に、対象ユーザの利用状況を確認するために、サービスの基本設定項目、Cookie 情報及びサービス利用履歴の記録を作成する。
- 一部のサービスでは、他のユーザとファイル等の情報を共有して、外部のユーザに編集権限を与えることが可能なサービスも存在するため、排他制御等の目的で、必要に応じて共有設定の変更や公開の停止等も検討する。
    - 設定を変更する際は、「8-6-2. 作業記録の作成」に従って記録を作成する。

付録資料

A. チェックシート　（PC の場合）

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

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 又は DCO 領域が存在するかも確認する。ラベル情報を記録、表示画面の写真撮影を行なう。	○	□
20	HDD/SSD 複製装置に複製保存用 HDD/SSD を接続する。		□
21	HDD/SSD 複製装置のメニューを操作して動作モードおよびログ出力など基本設定を確認し、複製を実施する。実行前の写真撮影を行う。	○	□
22	複製後に HDD/SSD 複製装置に表示される原本 HDD/SSD のハッシュ値を記録、写真撮影を行う。	○	□
23	HDD/SSD 複製装置のログにより正常に複製が行われたか確認する。	○	□
24	複製保存用 HDD/SSD のハッシュ値を取得し、原本 HDD/SSD のハッシュ値と複製データのハッシュ値が同一であるか確認する。ハッシュ値の記録、写真撮影を行なう。（HDD/SSD 複製装置の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 を取り外し、ピンの状態を確認し、写真撮影を行なう。	○	□
26	原本 HDD/SSD を PC 筐体に戻し、ケーブルも元の接続状態にもどす。	○	□
27	複製保存用 HDD/SSD は、機器が破損しないように考慮し、移動させる場合は、衝撃吸収性、帯電防止措置のあるケースなどを使用する。		□

B. デジタル・フォレンジックに関連する我が国の主な刑事法

＜刑法＞

（電磁的記録の定義）
第七条の二　この法律において「電磁的記録」とは、電子的方式、磁気的方式その他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。

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

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

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

3　不正に作られた権利、義務又は事実証明に関する電磁的記録を、第一項の目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作った者と同一の刑に処する。

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

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

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

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

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

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

（不正電磁的記録カード所持）

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

（支払用カード電磁的記録不正作出準備）

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

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

3　第一項の目的で、器械又は原料を準備した者も、同項と同様とする。

（未遂罪）

第百六十三条の五　第百六十三条の二及び前条第一項の罪の未遂は、罰する。

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

（不正指令電磁的記録作成等）

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

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

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

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

3　前項の罪の未遂は、罰する。

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

第 168 条の 2、第 168 条の 3 は、電子計算機のプログラムに対する社会一般の者の信頼を保護するために設けられた罪であり、文書偽造の罪（刑法第 17 章）等と同様に、社会的法益に対する罪である[26]。

---

[26] 法務省公開資料「いわゆるコンピュータ・ウイルスに関する罪について」（http://www.moj.go.jp/content/000076666.pdf）に、本条文に関する分かりやすい解説がある。

第1項が「ウイルス作成罪・提供罪」となり、第2項が「供用罪」となる。

作成・提供・供用とはそれぞれ、

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

を、意味する。

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

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

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

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、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。

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

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

（わいせつ物頒布等）
第百七十五条　わいせつな文書、図画、電磁的記録に係る記録媒体その他の物を頒布し、又は公然と陳列した者は、二年以下の懲役若しくは二百五十万円以下の罰金若しくは科料に処し、又は懲役及び罰金を併科する。電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した者も、同様とする。
2　有償で頒布する目的で、前項の物を所持し、又は同項の電磁的記録を保管した者も、同項と同様とする。

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

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

昭和62（1987）年刑法一部改正時に追加。

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

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

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

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

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

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

（公用文書等毀棄）
第二百五十八条　公務所の用に供する文書又は電磁的記録を毀棄した者は、三月以上七年以下の懲役に処する。
（私用文書等毀棄）
第二百五十九条　権利又は義務に関する他人の文書又は電磁的記録を毀棄した者は、五年以下の懲役に処する。

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

＜不正アクセス禁止法＞

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

（「不正アクセス行為」の定義）
第 2 条第 4 項　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。
一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）
二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを　除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

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

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

第 11 条により、法改正後は、三年以下の懲役又は百万円以下の罰金（従前は一年以下の懲役又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にシンポジウム中に侵入してみせた事件がある（東京地方裁判所　平成 17 年 3 月 25 日判決）。

（他人の識別符号を不正に取得する行為の禁止）
第四条　何人も、不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。
（不正アクセス行為を助長する行為の禁止）
第五条　何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。
（他人の識別符号を不正に保管する行為の禁止）
第六条　何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。

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

© 2018 NPO Institute of Digital Forensics.

(識別符号の入力を不正に要求する行為の禁止）

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

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

二　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為

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

違反した場合は、第 12 条の規定により、一年以下の懲役又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え）

第九十九条第二項

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

第二百十八条第二項　※新設

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

（記録命令付差押え）
第九十九条の二　※新設
　裁判所は、必要があるときは、記録命令付差押え（電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。）をすることができる。

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

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

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

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

（電磁的記録に係る記録媒体差押えの執行方法の整備）
第百十条の二　※ 新設
　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も、同様である。
一　差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。
二　差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。

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

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

（電磁的記録にかかる記録媒体を対象とする処分への協力要請）
第百十一条の二　※ 新設
　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状又は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。公判廷で差押え又は捜索をする場合も、同様である。

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

通信履歴の電磁的記録の保全要請
第百九十七条３項～５項　※ 新設
３　検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、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　第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。

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

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

（補足）

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

© 2018 NPO Institute of Digital Forensics.

＜不正競争防止法＞

（定義）
第二条第六項
　この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

（罰則）
第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは二千万円以下の罰金に処し、又はこれを併科する。
一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律　（平成十一年法律第百二十八号）第二条第四項 に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者
：
[中略]
：
３　次の各号のいずれかに該当する者は、十年以下の懲役若しくは三千万円以下の罰金に処し、又はこれを併科する。
一　日本国外において使用する目的で、第一項第一号又は第三号の罪を犯した者
二　相手方に日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をする目的があることの情を知って、これらの罪に当たる開示をした者
三　日本国内において事業を行う保有者の営業秘密について、日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をした者
４　第一項（第三号を除く。）並びに前項第一号（第一項第三号に係る部分を除く。）、第二号及び第三号の罪の未遂は、罰する。

　営業秘密に関する事項は不正競争防止法に定められている。曖昧な概念で使われる「企業秘密」という言葉とは異なり、「営業秘密」は同法の 2 条 6 項によってきちんとした定義がなされている。この条文から「秘密管理性」「有用性」「非公知性」が営業秘密成立の三要件となる。それ故、技術情報だけでなく顧客名簿などのビジネス情報も営業秘密となり得る。

　条文自体の記載は省略しているが、不正競争防止法では、その第 2 条第 1 項の各号においてどのような行為が不正競争となるかが定められている。そして同 4 号～10 号までが営業秘密に関しての記載であり、ここに不正と見なされる営業秘密の取得や使用、開示等におけるさまざまな場合が列挙されている。2015 年（平成 27 年）には新たに、営業秘密侵害品の譲渡、引渡し、輸出入、電気通信回線を通じた提供等が不正競争行為として追加された。

そして、それらを侵害した場合の罰則規定が第 21 条に記載されている。こちらも条文の全てを記載することは紙面都合でしていないが、第 21 条第 1 項の第 1 号～第 9 号の各号において刑罰が科されるさまざまな場合が規定されている。2009 年(平成 21 年）の改正によって、競合関係にある場合だけでなく、自己の利益の為に営業秘密を不正に取得したり使用したりした場合でも可罰化された。それ故、金銭目的で営業秘密を持ち出して他人に売却した場合も当然に犯罪となる。

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

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

注目すべき点として、今期改正より営業秘密侵害の未遂罪が追加されており（21 条 4 項）、経済産業省の解説資料[27] によれば、「取得未遂」として『不正アクセス行為は確認されたが、証拠の隠滅等により営業秘密たる情報の持ち出しの事実を確認できなかった場合。社内メールシステムの管理者の地位を利用し、社内幹部宛のメールが自動で自らにも転送されるようなプログラムを埋め込んでいたが、実際に営業秘密情報が転送される前に明るみに出た場合。』が、「開示未遂」として『営業秘密を電話で売り込み、その後メールで営業秘密を不正に開示するべく、送信しようとしたが、メールソフトの不具合により転職先に到達しなかった場合。』が例示されている。よってデジタル・フォレンジックの作業としてはこれらの行為の痕跡を探すことになる。

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

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

なお、営業秘密の管理に関する公的な指針としては「営業秘密管理指針」が経済産業省より公表[28] されている。この指針は 2015 年（平成 27 年）1 月に全面的な改定がなされ、従来の事例を詳細に記載する形式のものから「不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示すもの」に変更された[29] 。

---

[27] 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

[28] http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf

[29] 同 指針「はじめに（本指針の性格）」より

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

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

C. デジタル・フォレンジック関連の資料紹介

- 「Electronic Crime Scene Investigation: A Guide for First Responders、 Second Edition /Forensic Examination of Digital Evidence: A Guide for Law Enforcement」
  https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

- 「(CERT) First Responders Guide to Computer Forensics」
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7251

- 「Best Practices In Digital Evidence Collection」
  https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection

- 「情報セキュリティ関連法令の要求事項集」（平成２３年４月　経済産業省）
  http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_JohoSecurityKanrenHoreiRequirements.pdf

D. Chain of Custody（CoC）シート例

証拠の概要

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

一貫性（Chain of Custody）追跡記録

インシデントの概要			
件名		インシデント番号	
作業者		作業日	

証拠リスト		
証拠番号	容量	証拠の内容

一貫性			
作業日	作業内容	作業確認者 (Sign & Print Name)	作業受取者 (Sign & Print Name)

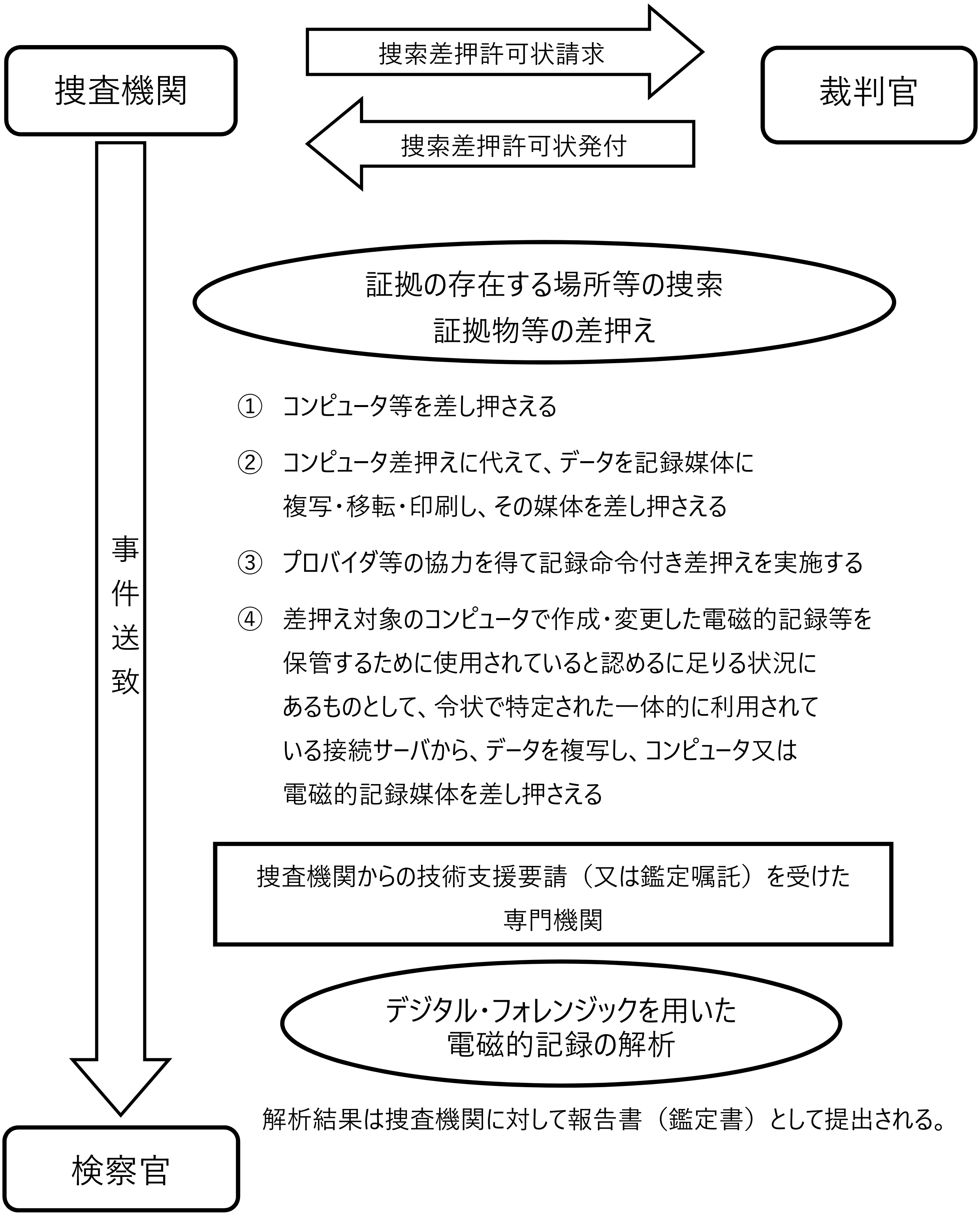
* Picuture(s) may require to show an identity of the evidence

/

© 2018 NPO Institute of Digital Forensics.

E. 刑事・民事におけるデータ収集と解析フローイメージ図

刑事手続きにおけるデータの収集と解析



① コンピュータ等を差し押さえる

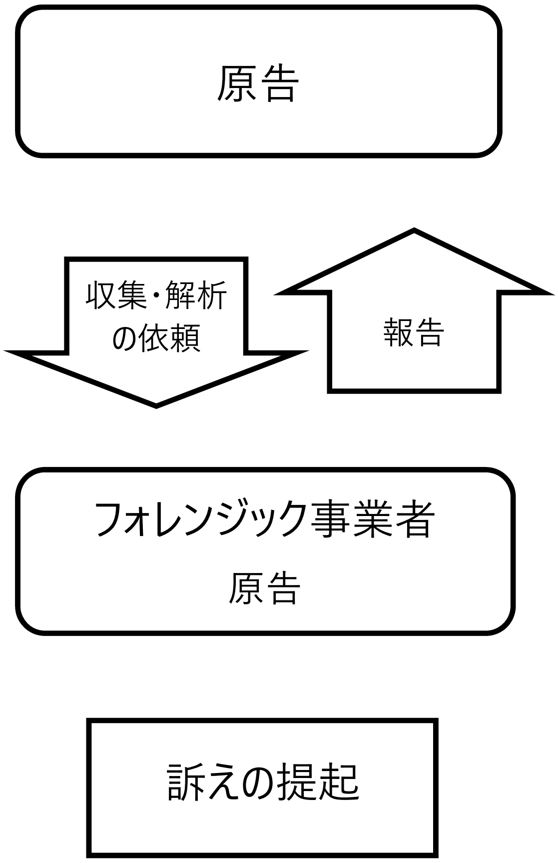
② コンピュータ差押えに代えて、データを記録媒体に複写・移転・印刷し、その媒体を差し押さえる

③ プロバイダ等の協力を得て記録命令付き差押えを実施する

④ 差押え対象のコンピュータで作成・変更した電磁的記録等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として、令状で特定された一体的に利用されている接続サーバから、データを複写し、コンピュータ又は電磁的記録媒体を差し押さえる

解析結果は捜査機関に対して報告書（鑑定書）として提出される。

民事手続きにおけるデータの収集と解析



民事訴訟は、私人間の生活関係に関して生じる紛争について、司法機関たる裁判所が私法を適用して解決するための手続きである。

裁判所は、証拠によって事実を認定する。

裁判で証拠として価値があるとされるものがデジタル証拠である場合には、通常、その内容を直接知覚できないので、適切に収集し、保管し、解析しなければならない。

＜参考資料＞日本弁護士連合会

「事件解決への流れ（民事事件・刑事事件）」（PDF 形式・114KB）

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

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

① 検証（民訴法 232 条）

裁判官が感覚作用を使って事実の認定資料とする方法である。裁判官がコンピュータ自体やデータの状態を視覚等の作用によって心証を得るのがその例である。

本案訴訟での正式な証拠調べを待っていたのでは、証拠の変更、改ざん、隠匿等のおそれがある場合に、本案訴訟を提起する前に、検証等を実施することがあり、これを民訴法上の証拠保全という（民訴法 234 条）。

②　書証（民訴法 219 条）

文書に記載された思想・認識を裁判所が事実認定に用いる方法である。専門業者が実施したデジタル・フォレンジック調査の経過や結果等をまとめた調査報告書がその例である。第三者が文書を所持する場合に裁判所にそれを送付させる送付嘱託（民訴法 226 条）もある。

写真・ビデオテープは準文書として書証扱いとされるが（民訴法 231 条）、デジタルの電子媒体は、検証（民訴法 232 条）として扱われることがある。なお、文書は、その成立の真正が否定されると書証にすることができない（民訴法 228 条）。

③　証人（民訴訟 190 条）

証人尋問は、当事者（原告本人・被告本人）以外の者が過去に認識した事実を裁判所で供述し、その供述を事実認定の資料とする方法である。デジタル・フォレンジック調査を行った専門業者が法廷で証言するのがその例である。

④　鑑定（民訴法 212 条）

特別の学識経験をもつ第三者に専門知識に基づく事実判断を裁判所に報告させる方法である。裁判官が専門業者を指名して、コンピュータやデータ等の解析を行わせそれを報告させる場合がその例である。

⑤　調査嘱託（民訴訟 186 条）

官公署、外国の官公署、学校等の団体に対して必要な調査を嘱託する方法がある。

裁判における解析データの利用

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

F. 供述証拠と事実認定の実務（概論）

※大橋充直会員提供資料：

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

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

1　基礎概論

(1) 意見法則

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

×例：「社長が、Ａ君が犯人だと決裁されましたから、Ａ君が犯人です。」

×例：「学級会の多数決でＢ君が犯人と決まったから、Ｂ君が犯人だ。」

(2) 伝聞（証拠）法則

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

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

(3) 伝聞法則の例外

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

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

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

○例：不正アクセスがあったころ、Ｃ先輩は「アナを決めた。Ｖ社に恥をかかせやる！」とサーバルームのアドミン席で叫んでいました（犯行時にセキュリティホールを突いたという具体的事実を推測させる衝動的供述で、動機をも推測させる感情的表現につながっている。）。

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

(4) 自白法則

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

もっとも、怖いのは、自白書、上申書、顛末末書、自供書、告白書……と称する犯罪を認めた署名押印のある書類が捜査機関に持ち込まれ、当の本人が犯罪を否認しているときである。会社の上司や家族さらには地域社会住人が、義理人情や取引でよってたかって、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 322 条参照）

×例：自己に有利な供述（新入社員のセールストークを想起されたい）

(2) 供述が一貫している（×供述がコロコロ変遷する）

○根拠：真の記憶は作為を要しないから何時でも同一の内容を繰り返せる

×根拠：嘘は供述が変遷する（嘘吐きは記憶力がよくなければならない）

(3) 裏付け証拠があり、他の証拠と符合する（×他の証拠と矛盾している）

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

例えば、女性従業員 B から「A さんが集金チョ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 323 条参照）。

ア　公文書（外国政府を含む）

・出入国記録、議員会館入退館記録、免許取得更新履歴

イ　業務文書（業務日誌、帳簿や伝票）

・ATM ジャーナル（入出金伝票）、パスモの入出場記録

ウ　証拠物（証拠写真、チケット、領収書）

・防犯カメラ画像、高速道路通行券、医療保険自己負担領収書

エ　機械が自動的に作成するもの（コンピュータ・ログ、通信履歴）

・サーバ・アクセスログ、ISP 接続ログ、携帯電話の発着信記録

3　事情聴取と信用性判断の具体例

(1) 供述の信用性判断としての裏付け調査

ア　裏付け可能な事項は徹底した裏付け調査（ウラトリ）を行う。

→　供述には裏付けがないと信用されないと思うこと。

→　「ジャーナリストは自分の母親が『愛している』と言っても裏を取れ」

イ　裏付けは供述でもいいが証拠物や客観証拠がベターである。

ウ　裏付け事実のさらなる裏付け（ウラのウラ）はベストである。

(2) 供述の信用性吟味は、具体性と合理的な理由の有無である。

×　娘「パパ大好き、なぜって、だってパパだもん」（理由不備）

△　娘「だってパパは
おもちゃ買ってくれるし
遊園地連れてってくれるし
オイタしてもママに言いつけないから」
（抽象的事実の供述・現在形の供述）

○　娘「だってパパは
このおもちゃ買ってくれたし
昨日、遊園地連れてってくれたし
お皿割ってもママに言いつけなかったもん」
（具体的事実の供述・過去形の供述）

(3) 以上の総合例

ア　供述の裏付け証拠：おもちゃ、遊園地の半券、割れた皿

イ　裏付けの裏付け：おもちゃ購入のレシート、遊園地のスナップ写真

■参考■刑事訴訟法（昭和二十三年七月十日法律第百三十一号）

第 319 条【自白の排除法則・補強法則】

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

2　被告人は、公判廷における自白であると否とを問わず、その自白が自己に不利益な唯一の証拠である場合には、有罪とされない。

3　前二項の自白には、起訴された犯罪について有罪であることを自認する場合を含む。

第 322 条【被告人の自白の証拠能力】

1　被告人が作成した供述書又は被告人の供述を録取した書面で被告人の署名若しくは押印のあるものは、その供述が被告人に不利益な事実の承認を内容とするものであるとき、又は特に信用すべき情況の下にされた

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　被告人の公判準備又は公判期日における供述を録取した書面は、その供述が任意にされたものであると認めるときに限り、これを証拠とすることができる。

第 323 条【公文書等の特信書面】

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

一　戸籍謄本、公正証書謄本その他公務員（外国の公務員を含む）がその職務上証明することができる事実についてその公務員の作成した書面

二　商業帳簿、航海日誌その他業務の通常の過程において作成された書面

三　前二号に掲げるものの外特に信用すべき情況の下に作成された書面

G. デジタルデータの証拠化・同一性確認調査手続き報告書例

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

平成○○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）させていただきたい。

これは、当社代表取締役も了承済みである。（注 6）

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

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

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

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

第 3　その他参考事項

本件作成・入手にかかるデジタルデータの写しは、別添上記 DVD-R のとおりである。（注 10）

なお、サーバの所在地（第 1 中の「2 作成場所」）は、サイバーテロ対策で本来的に極秘であるため、本書の開示に際しては、特段の厳重な保秘の措置（例えば、サーバ所在地情報のみ黒塗りマスキング等）をとられることを、本書をもって関係機関に申し入れる。（注 11）

以上

※　コピーメディア（DVD-R 等）筐体部への記載例（注 7）

09ACBE の写し

2012 年 4 月 1 日　17 時 15 分

当職がサーバから写しを作成して同一性を確認した。

（作成者・同一性確認者）　○○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）。

© 2018 NPO Institute of Digital Forensics.

（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（又はファイル名）まで特定すること。

（注６）刑事裁判で「写し（コピー）」が証拠能力を確実に取得するためには、原本の提出が不可能又は著しく困難であることの疎明が必用である（最高裁決定昭和35年2月3日・最高裁判例集14巻1号45頁、最高裁判決昭和35年3月24日・最高裁刑事判例集14巻4号447頁）。

（注７）写しを「いつ」「だれが」「どのようなものを」作成したかを必ず筐体表面に記載すること。手続過程の保全と同時に、写しの内容が正確にコピーされているという信用性の問題でもある。また、写しを作成したメディアを特定するため、メディアの筐体部分には、油性サインペンで、本文記載の作成年月日と表題を付して作成者の署名押印し（筐体に直接記載が困難なら付箋紙の上に全て記載し、付箋紙の裏面に両面シールを貼って筐体部分に貼り付けること）、その上から粘着糊付きラッピングシール（ラミネートフィルム等）を貼って固定するとよい。

（注８）簡単なファイルを幾つかコピーするだけなら、FC（ファイル・コンペア）コマンドでもよい。

（注９）「第三者たる提供者（デジタルデータ管理人）が立会人として原本との同一性を認証した」という法的意味がある。

（注10）法執行機関では、必ず写しメディアを2部作成し、1部はそのまま保管して不測の事態に備え、もう1部を使ってデータ解析をするように教育されている。

（注11）サーバ所在地等の機密情報の非開示（又は「インキャメラ」：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

H. 代表的な収集及び分析ツール

●システム関連の情報取得ツールの例

- analyzeMFT
  NTFS ファイルシステムから MFT のファイルを解析するツール。
  https://github.com/dkovar/analyzeMFT

- CDIR Collector
  Windows から主要データを保全するためのオープンソース等を活用したツールセット。
  https://github.com/CyberDefenseInstitute/CDIR

- Event Log Explorer
  ローカルコンピュータのイベントログの詳細分析や、ネットワーク上の複数のコンピュータのイベントログを集中管理できるツール。
  http://eventlogxp.com

- Log Parser
  さまざまなログの中から必要な情報を検索し、特定の情報を抜き出すツール。並べ直しや Excel 用のデータで出力するなど、多様なログ分析を支援する。
  http://www.microsoft.com/download/en/details.aspx?id=24659

- Log Parser Lizard
  上述の Log Parser を GUI で使えるようにするツール。
  http://www.lizard-labs.net

- FTK Imager Lite
  ハードディスクの情報の参照や、メモリダンプの出力、VM などのイメージファイルの読み込みなどを行うツール。
  http://accessdata.com/product-download/digital-forensics/

- triage-ir
  Windows システムでマルウェアの攻撃痕跡等の調査に必要となる情報を自動収集するツール。
  https://code.google.com/p/triage-ir/

- 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ためのツール。
  https://www.bestpractical.com/rtir/

© 2018 NPO Institute of Digital Forensics.

●揮発性メモリの情報取得及び解析ツールの例

- Belkasoft Live RAM Capturer
  32/64 bit にそれぞれ対応した無償のメモリダンプツール。
  https://belkasoft.com/ram-capturer

- 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や、データの復旧及び解析ができるフリーツール。
  http://www.magnetforensics.com/acquiring-memory-with-magnet-ram-capture/

- MoonSols Windows Memory Toolkit
  メモリの取得や変換を実行するために必要なすべてのユーティリティを含むツール。
  http://www.moonsols.com/windows-memory-toolkit/

- Redline
  Mandiant 社によって開発・提供されているフリーツール。同社で開発されている Memoryze という解析ツールの GUI フロントエンドとして使われている。
  https://www.mandiant.com/resources/download/redline

- Rekall
  Google が提供しているオープンソースのメモリ解析フレームワーク。
  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/

●スマートフォンのデータ取得ツールの例

- Magnet Acquire
  Magnet Forensics 社が開発及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/

I. 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
  https://www.ietf.org/rfc/rfc3227.txt
  （邦訳）証拠収集とアーカイビングのためのガイドライン – RFC3227
  https://www.ipa.go.jp/security/rfc/RFC3227JA.html

- Digital Intelligence and Investigation - CERT/CC
  http://www.cert.org/digital-intelligence/

- Network Forensics Handbook – ENISA
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/network-forensics-handbook/view

- Defense Computer Forensics Laboratory (DCFL) – DC3
  http://www.dc3.mil/digital-forensics/

- Method validation in digital forensics - GOV.UK
  https://www.gov.uk/government/publications/method-validation-in-digital-forensics

J. ＩＤＦ団体会員「製品・サービス区分リスト」（全４３社）

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 訴訟支援・コンサルティング、④　e -Discovery、⑤ トレーニング・人材育成、

⑥ ネットワーク監視・記録、⑦ データリカバリ、⑧ 情報漏洩調査・脆弱性審査、

⑨ サイバー・インシデント演習（フォレンジックを含む）支援、

⑩ ポリシー・組織構築支援（CSIRT その他）、⑪ 予兆把握、自動調査処理ツール等、

⑫ 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いただいた内容となります。

ＩＤＦ団体企業名	サービス区分	主要製品等
株式会社フォーカスシステムズ https://cyberforensic.focus-s.com/	①、②-a・c・d、③、④、⑤、⑥、⑧、⑨、⑩、⑪	・各種フォレンジックツール(EnCase/FTK/IEF・AXIOM 等) ・Mac/iPhone(HFS+/APFS)解析・保全ツール (BlackLight/MacQuisition) ・HDD/SSD 保全・書込防止装置 (Falcon-NEO/Tableau/WriteProtectPortable) ・マルウェア解析(Responder Pro/IDA Pro/Shadow3) ・各種トリアージツール(EnCase Portable/AD Triage) ・公式トレーニング(DF120/210/320/FTK/AXIOM) ・フォレンジック調査・緊急対応サービス 他
株式会社 FRONTEO http://www.fronteo-legal.com/	①、②、③、④、⑤、⑥、⑦、⑧、⑨、⑪	・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) - MSABOffice (XRY、モバイル端末データ解析ツール) - Solo-4(HDD 複製装置) - UltraBlock(書込み防止装置)他 ・Lit i View SNS MONITORING (SNS 監視ツール) ・フォレンジック調査 ・フォレンジック調査トレーニング eDiscovery サービス ・KIBIT Email Auditor(人工知能搭載 Email 監査ツール) ・KIBIT Knowledge Probe(人工知能搭載データ分析支援システム)他
株式会社 NTT データ https://www.nttdata.com/	③	・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、⑤、⑥、⑧、⑨、⑩	・緊急対応サービス「サイバー119」 ・情報漏えい調査 ・セキュリティ診断 ・APT 攻撃耐性診断サービス「APT 先制攻撃」 ・JSOC マネージド・セキュリティ・サービス ・ラックセキュリティアカデミー（フォレンジック・ハンズオントレーニング）
デロイト トーマツ リスクサービス株式会社 https://www2.deloitte.com/jp/dtrs	②-a・b・c・d、⑤、⑥、⑦、⑧、⑨、⑩	デロイト トーマツ リスクサービスは、サイバーセキュリティ、IT ガバナンス、事業継続管理(BCM)等に関する多くの知見やノウハウ・実績に基づき、デロイト トーマツ グループと有機的に連携を図りながら、総合的に企業の IT 領域のリスク管理活動を支援します。また、サイバー領域においては、デロイトメンバーファームとの連携により、世界 20 か所以上に拠点を構えるサイバーインテリジェンスセンター(CIC)と連携し、各国で収集・分析した高度なサイバーインテリジェンスの提供により、クライアントのインシデントレスポンスに係る工数を低減します。
株式会社ディアイティ http://www.dit.co.jp/	①、②、⑤、⑥、⑧、⑨、⑩	・フォレンジックツール　：X-WaysForensics ・リモートフォレンジックツール　：F-Response ・フォレンジックサービス　：コンピュータフォレンジックサービス、通信ログ解析サービス、ウィルス感染切り分けサービス ・教育　：捜査機関向けフォレンジック教養、X-WaysForensics 教育、CSIRT 机上演習サービス
株式会社オーク情報システム http://www.oakis.co.jp/	①、⑥	・ネットワーク・フォレンジックサーバ『NetEvidence』の開発・販売
ネットエージェント株式会社 https://www.netagent.co.jp/	①、②- a ・b・c、③、⑤、⑥、⑧	・フォレンジック調査サービス ・P2P 調査サービス ・脆弱性診断サービス ・WAF ・ホワイトハッカーコンサルティング ・ネットワーク・フォレンジック製品開発販売(PacketBlackHole) ・ファイアウォール製品開発販売(One Point Wall) ・HTTPS 可視化製品開発販売(Counter SSL Proxy)
株式会社ピーシーキッド https://www.pckids.co.jp/	①、②-a・c、⑦、⑧	・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 ・その他デジタルデータに関するサービス

ＩＤＦ団体企業名	サービス区分	主要製品等
AOS リーガルテック株式会社 https://www.aos.com/	①、②-a・b・c・d・e(防犯カメラ、ドライブ・レコーダー)、③、④、⑤、⑦、⑧	・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、フォレンジック調査トレーニング、e-Discovery サービス ・フォレンジックツール販売 - Final Forensics(PC フォレンジック)、AndrEx 2 (Android データ抽出)、AOS Professional(動画復元)、AOS Enhancement(画像鮮明化)、Nuix Investigation and Response(不正調査支援解析ソフトウェア)
ハミングヘッズ株式会社 https://www.hummingheads.co.jp/	①	・エンドポイント情報漏洩対策ソフト「Security Platform (SeP)」 ・アンチウイルスソフト「Defense Platform (DeP)」 ・自動化ツール・RPA ツール「AI Humming Heads (AIHH)」 ・高速履歴分析ツール「スーパーサーチエンジン」 等
FTI コンサルティング https://www.fticonsulting.com/about/locations/regions/japan	②-a・c・d、③、④	・Ringtail、Radiance、Acuity、FTI Investigate 等のレビューツールを活用した e-Discovery 対応 ・訴訟サポート ・ビジネス・業務・IPO デューデリジェンス ・政治リスク・競合他社評価 ・反社会的勢力調査 ・投資・出資後のビジネスモニタリング ・コンプライアンスレビュー ・不正調査・贈収賄・汚職関連調査 ・保険請求関連調査　等
株式会社サイバーディフェンス研究所 https://www.cyberdefense.jp/	①、②、⑤、⑧、⑨	・Oxygen Forensic Analyst(スマートフォン解析ツール) ・フォレンジック調査 ・CDIR(Cyber Defense Institute Incident Response Collector) ・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　他
エンカレッジ・テクノロジ株式会社 http://www.et-x.jp/	①	・ESS REC： - システム操作の内容を動画とテキストで克明に記録 - 不正操作をリアルタイムに検知・管理者にアラームを送信するなどのアクションを実行 - 金融機関などリスク管理等で採用多数

ＩＤＦ団体企業名	サービス区分	主要製品等
ベライゾンジャパン合同会社 http://www.verizonenterprise.com/jp/	②-a・b・c・d・e(Net Flow)、③、④、⑤、⑥、⑦、⑧、⑨、⑩、⑪、⑫	・海外拠点を含むインシデント対応及びフォレンジック調査 - グロバールフォレンジック調査対応 - セキュリティコンサルティング - PCIDSS 対応(QSA、PFI 機関） - 脆弱性検査 - Network Threat Hunting - マルウエアコード分析(24 時間 SLA) - DarkNet/Clearnet 調査 - 内部不正調査支援 - インシデントレスポンス支援(トレーニング、模擬訓練) - eDiscovery(訴訟支援）
アイフォレンセ日本データ復旧研究所株式会社 http://www.daillo.com/	①、②-a・b・c・d・e(意図的に破壊されたり、故障して動作しない HDD も調査対象)、③、⑤、⑦、⑧	1. 破壊や故障した 情報記憶媒体のデータ復旧 2. 消失したデジタルデータの解析調査及び復元 3. 事件捜査や内部不正調査でのフォレンジック調査 4. カメラやビデオの写真画像や映像動画の復元 5. 削除済みファイルの復旧及び削除経緯の調査 6. データ保全複製及び消去ツールの動作検証サービス 7. HDD・SSD の構造及び動作仕様に関する技術講義・トレーニング・講演 8. 現存するソフトウェアでの上書き消去が不可能なデータエリアとその部分の消去方法の研究調査 他
サン電子株式会社 http://www.sun-denshi.co.jp/	①、②-c・d・e(ドローンの飛行ルートや写真/動画等のデータ解析)、⑤	・Cellebrite 社(イスラエル)が開発するデジタルインテリジェンス/モバイルフォレンジック機器及びサービス - UFED Touch2 - UFED 4PC - UFED inField KIOSK - UFED Analytics - UFED Cloud Analyzer - Cellebrite Advanced Investigative Servise - Cellebrite 認証取得公式トレーニング ・AR スマートグラスによる犯罪捜査支援システム
株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/	①、②-a・c・d、④、⑤、⑦	・WDR Forensic(フォレンジックサービス、フォレンジックツール) - 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) - DVR Examiner(監視カメラ、防犯カメラフォレンジックツール) - SecureView(スマートフォン、携帯端末証拠保全キット) - SecureAge(PKI 暗号、監視、APT 対策、情報漏えい対策ソフトウェア) ・PC-3000 JAPAN(HDD、 SSD、 NAND メモリデータ復旧ツール、トレーニング) ・WinDiskRescue(WD 公認データ復旧サービス、証拠品鑑定)

ＩＤＦ団体企業名	サービス区分	主要製品等
三井物産セキュアディレクション株式会社 https://www.mbsd.jp/	②、⑧、⑩	・フォレンジック調査 ・マルウェア解析 ・感染調査 ・情報漏えい調査サービス ・CSIRT 構築支援
NTT データ先端技術株式会社 http://www.intellilink.co.jp/	①、②、③、⑥、⑧、⑨、⑩	・セキュリティ・インシデント救急サービス ・CSIRT/SOC 構築支援/運用支援サービス ・脆弱性情報配信サービス ・サイバー演習システム「SyprisCyberRange」 ・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
SCSK 株式会社 https://www.scsk.jp/sp/sys/	①、②-b、⑧、⑩	・脆弱性診断ツール(BeyondTrust Retina、WebInspect、IBM Security AppScan、Fortify SCA) ・SIEM ソリューション(ArcSight、IBM Security QRadar) ・不正侵入防御システム(TippingPoint) ・Web アプリケーションセキュリティ(BIG-IP ASM) ・標的型攻撃対策(Lastline、標的型メール訓練サービス) ・クラウドセキュリティ(CASB)(Netskope) ・セキュリティ運用(SOC)(監視対象：PaloAlto、Fortigate、TrendMicro DeepSecurity、CheckPoint vSEC、TippingPoint、BIG-IP ASM、Lastline) ・フォレンジック調査(ネットワークフォレンジック) ・脆弱性診断サービス(脆弱性診断、脆弱性診断、体制構築支援) ・セキュリティコンサルティング(サイバーセキュリティ経営アセスメント、セキュリティポリシー策定支援、SOC/CSIRT 構築支援) 他
株式会社 KPMG FAS https://home.kpmg.com/jp/ja/home/about/fas.htm	②-a・b・c・d、③、④、⑤、⑥、⑦、⑧、⑨、⑩、⑪	・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
Payment Card Forensics 株式会社 http://www.pcf.co.jp/	②、③、⑧、⑩	・PCI Forensic Investigator (PFIs)認定調査 ・クレジットカード他ペイメントカード情報漏えい調査サービス ・PCIDSS 準拠支援サービス ・WEB アプリケーション診断サービス ・ネットワークペネトレーション診断サービス ・情報セキュリティ診断サービス
DATA HOPE 東北データ復旧 (有限会社コミュニティアイ) https://www.datahope.jp/	②-a、⑦、⑧	・データ復旧 ・デジタル・フォレンジックサービス
株式会社データサルベージ https://www.data-salvage.jp/	①、②-a・c、⑦	■サービス区分 ・製品(ハード、ソフト)販売(フォレンジックに関連する製品) ・フォレンジック調査(PC・サーバ等、携帯電話・スマートフォン) ・データリカバリ ■主要製品等 ・HDD 等のストレージ保全ツール(MASAMUNE Clone) ・Android iOS 向けのデータ消去ツール(MASAMUNE Erasure)
株式会社ワイ・イー・シー https://www.kk-yec.co.jp/	①、②-a、⑤、⑦、⑧、⑨	・各種フォレンジックツール・サービス・トレーニング・データリカバリ ・HDD 保全装置(DemiYG1040/ForensicDemi 等) ・書込み防止装置(PCAIDⅢ/USB3.0WriteProtector) ・解析ソフトウェア(DfasPortable/DfasPro/DfasEnterprise/EvidenceTracer/Mobiledemi) ・電波遮断装置（シールドボックス、シールディングバッグ） ・トレーニング（フォレンジック導入支援、データリカバリ、各種初級） ・データリカバリ（論理障害/物理障害） ・フォレンジック調査サービス
PwC サイバーサービス合同会社 https://www.pwc.com/jp/cybersecurity	②、⑤、⑧、⑨ ⑩、⑪	・デジタル・フォレンジック ・脆弱性診断 ・ペネトレーションテスト ・レッドチーム演習 ・インシデントレスポンスアドバイザリー ・インシデントディテクション＆リカバリー ・CSIRT/SOC 構築支援

ＩＤＦ団体企業名	サービス区分	主要製品等
Dell SecureWorks Japan 株式会社 https://www.secureworks.jp/	②-a・b・d、⑥、⑧、⑨、⑩、⑪	・マネージド・セキュリティサービス(セキュリティ監視による検知機能の強化、インシデント対応との連携等) ・セキュリティコンサルティング(CSIRT 構築支援、CSIRT の有効性を実証するレッド・チームテスト等) ・インシデント管理&レスポンスサービス(インシデントレスポンス、マルウェア解析、システム・ネットワーク脆弱性診断、標的型攻撃対応訓練、標的型攻撃ハンティング) ・インシデント対応を迅速に行う為の事前契約を頂くことで事故発生時の初期対応をより迅速に行うことが可能です。
マクニカネットワークス株式会社 https://www.macnica.net/	①、⑥、⑪	・ネットワーク・フォレンジック装置(Symantec Security Analytics) ・リアルタイムレスポンスプラットフォーム(Tanium) ・EDR + NGAV + Hunting(CrowdStrike) ・標的型攻撃対策＆レスポンスツール(FireEye) ・ログ相関分析基盤(Splunk) ・セキュリティイベント管理(McAfee SIEM)
EY 新日本有限責任監査法人 https://www.eyjapan.jp/services/assurance/fids/	②-a・b・c・d、④、⑤、⑧、⑨⑩	・フォレンジックトレーニング - Windows 8 / 8.1 / 10 - Macintosh - モバイルデバイス - ファイルシステム ・フォレンジック調査/インシデント対応支援 ・CSIRT 態勢評価・整備・運営支援サービス ・サイバー犯罪診断 ・eDiscovery 支援サービス ・Forensic Data Analytics
株式会社アクアシステムズ https://www.aqua-systems.co.jp/	①、②-e(データベース)、⑧	・データベース監査ツール(AUDIT MASTER) ・データベースセキュリティコンサルティング ・データベース監査コンサルティング ・データベース監査ログフォレンジック調査
株式会社 DD‐RESCUE http://www.dd-rescue.jp/	①、②-a、⑦	・データ復旧サービス全般 ・簡易フォレンジック調査 ・フォレンジックツール(X-Ways forensics) ・MRT Recovery Tools (disk repair、data recovery)
データテック株式会社 https://www.data-tech.co.jp/	⑦	・データリカバリ/データ復旧サービス全般 ・故障して全く動作しない HDD 等、高難度・重度物理障害を含む全てのデータ救出・復旧(全国宅配受付・持込受付・訪問出張　緊急対応) ・PC 内蔵・外付 HDD/各種 Server/NAS – 全 RAID 可 ・USB メモリ/SD/microSD/CF 等、重度物理障害 ・デジタルカメラやビデオの写真画像や動画の救出・復旧

ＩＤＦ団体企業名	サービス区分	主要製品等
松久産業株式会社 http://www.matsuhisa-kk.com/	①、②-a・b・e(画像(動画、静止画)解析調査)、③、⑤、⑥、⑧、⑩、⑪、⑫(画像解析調査、ビデオ画像認識解析・保管システム開発販売)	・パケット・ログを漏れなく収集し安心・安全に保管する装置「NetGuardian Packet」 ・パケット・ログを分析する装置「PacketAnalyst」 ・パケット・ログやアクセス・ログを安心・安全に長期保存する大容量一括保管管理システム「StorageGuardian」 ・安心・安全に大切なデータを護る「SecureNAS」 ・安心・安全を実現する統合多層防御ゲートウェイ/UTM「NetGuardian Gate」 ・安心安全な IoT 環境を実現する「SecureIoTAP」 ・熟練した人の技とコンピュータによるセキュリティ・フォレンジック関連サービス「SmartSecurityResearch」
株式会社テリロジーワークス http://www.terilogyworx.com/	①、②-a、⑥、⑧、⑪	・ネットワーク・フォレンジック(momentum Forensics) ・コンピュータ・フォレンジック(CyberTriage) ・パケットキャプチャ/長期保存(momentum Probe/Storage) ・ネットワーク監視・記録(SevOne) ・ネットワークセキュリティ監査(RedSeal) ・Threat Intelligence Service(KELA) ・Spirent 脆弱性調査サービス(Spirent)
株式会社ベルウクリエイティブ https://belue-c.jp/	①、⑥、⑧	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。 の開発および提供を行っております。 今後の IoT ビジネスに欠かせない、質の高いソリューションやサービスを生み出す事を使命と考えております。
ストーンビートセキュリティ株式会社 https://www.stonebeat.co.jp/	②-a・b・d、③、⑤、⑥、⑦、⑧、⑨、⑩	【教育トレーニング】 ・セキュリティ基礎・サイバー演習・Hacking Expert・Incident Reponse ・標的型メール訓練・デジタル・フォレンジック・CSIRT 対応演習 【対策支援】 ・脆弱性診断・セキュリティ健康診断・セキュリティコンサルティング ・インシデント対応・セキュリティ監査・フォレンジック・マルウェア解析 【案件支援】 ・セキュリティシステムの構築・運用システム ・CSIRT 構築支援・運用支援

© 2018 NPO Institute of Digital Forensics.

株式会社シマンテック https://www.symantec.com/ja/jp/	①、②、⑤、⑥、⑧、⑨、⑩	・セキュリティ脆弱性診断(Web、NW、Mobile、IoT) ・セキュリティアドバイザ理サービス ・Advanced Threat Protection(標的型攻撃対策) ・Symantec Endpoint Protection(セキュリティ強化) ・マネージドセキュリティサービス(ログ監視) ・Cyber Skills Development(トレーニング) ・Symantec Incident Response(インシデント対応) ・Security Analytics(ネットワーク・フォレンジック) ・DeepSight Managed Adversary and Threat Intelligence(脅威・攻撃者情報提供) ・EDR Cloud
株式会社富士通エフサス http://www.fujitsu.com/jp/group/fsas/	⑥、⑧、⑩	・セキュリティサービス全般(セキュリティポリシー策定、セキュリティ監査、CSIRT 構築支援) ・ウイルス振る舞い検知サービス ・次世代ファイアウォール運用サービス ・インターネットゾーンスキャンサービス ・イントラネットゾーンスキャンサービス ・標的型メール訓練サービス ・機密情報保護＆共有ソリューション
株式会社 PFU https://www.pfu.fujitsu.com/	②-a・b、⑤、⑥、⑧、⑩	・標的型サイバー攻撃対策支援サービス ・デジタル・フォレンジック ・インフラ脆弱性診断、Web ｱﾌﾟﾘ脆弱性診断、セキュリティベンチマーク診断、セキュリティログ分析 ・CSIRT 構築・運用支援 ・標的型攻撃メール訓練サービス ・標的型・ネットワーク診断サービス ・インシデントレスポンスサービス ・マルウェア検体解析
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、⑥、⑦、⑧	・フォレンジック調査 ・データ復旧サービス
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、⑤、⑥、⑧、⑨、⑩	・フォレンジック調査(ハードウェア、ネットワーク) ・セキュリティコンサルティング(CSIRT 構築支援/ポリシー策定支援 等) ・セキュリティ監視分析サービス ・脆弱性診断サービス、脆弱性情報提供サービス ・解析サービス(ログ、マルウェア等) ・各種セキュリティ対策ソフトウェア ・セキュリティ専門技術教育、サイバー演習

ＩＤＦ団体企業名	サービス区分	主要製品等
MYK アドバイザリー株式会社 https://www.myka.co.jp/	②-a・b・c・d、③、⑤、⑦、⑧、⑩、⑫(DF 専門家と公認不正検査士でもある会計士が連携することによる会計不正調査との一体調査)	＜サービスの特徴＞ 大阪及び福岡を拠点とした西日本を中心に下記のサービスをご提供いたします 1. 元法執行機関での犯則調査 DF 担当官によるデジタル・フォレンジック調査 2. 同 DF 指導事務官による各種フォレンジックツールを用いた DF 調査支援(UFED 等各種フォレンジックツールに関するベンダートレーニング講師) 3. テクノロジー支援型レビュー(TAR)機能を搭載したオンラインレビューツール 4. 社内に複数擁する公認会計士/公認不正検査士と連携した一体調査 5. 調査後の再発防止策の立案・整備から平時化後の内部監査支援まで一気通貫でご提供 ＜主要ツール＞ ・解析ソフトウェア(Intella、X-ways)等、スマホデータ保全・解析ツール（Oxygen Forensic 等）、書込防止装置（PCAIDⅢ等）

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/
LINE 株式会社	https://linecorp.com/
公益財団法人金融情報システムセンター	https://www.fisc.or.jp/
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/about-deloitte/articles/dtfa/deloitte-tohmatsu-financial-advisory.html
NRI セキュアテクノロジーズ株式会社	https://www.nri-secure.co.jp/
株式会社サンエイ	https://sanei.company/
ネットワンシステムズ株式会社	https://www.netone.co.jp/

K. 「証拠保全ガイドライン」改訂ＷＧメンバー（所属は 2018 年 7 月現在）

※五十音順

座　長	名和　利男	株式会社サイバーディフェンス研究所 専務理事／上級分析官、 兼 PwC サイバーサービス合同会社 最高技術顧問、IDF 理事
副座長	松本　隆	株式会社ディー・エヌ・エー システム本部 セキュリティ部、IDF 理事
委　員	伊原　秀明	株式会社ラック サイバー救急センター
委　員	上原　哲太郎	立命館大学 情報理工学部 教授、IDF 副会長
委　員	金子　寛昭	株式会社フォーカスシステムズ サイバーフォレンジックセンター
委　員	小山　幸輝	PwC サイバーサービス合同会社 マネージャー
委　員	篠原　明彦	ネットエージェント株式会社 技術部サービスグループ 課長
委　員	須川　賢洋	新潟大学大学院 現代社会文化研究科・法学部 助教、IDF 理事
委　員	杉山　一郎	EY 新日本有限責任監査法人 FIDS 事業部 プリンシパル
委　員	大徳　達也	株式会社サイバーディフェンス研究所 情報分析部 部長／上級分析官
委　員	谷口　浩	東京電力ホールディングス株式会社 セキュリティ統括室 室長
委　員	野崎　周作	株式会社 FRONTEO 執行役員 技師長
委　員	舟橋　信	株式会社 FRONTEO 取締役、株式会社セキュリティ工学研究所 取締役、IDF 理事
委　員	守本　正宏	株式会社 FRONTEO 代表取締役社長、IDF 理事
委　員	山内　崇	株式会社ピーシーキッド 常務取締役 データ復活サービス部 フォレンジックサービス部
委　員	山崎　輝	株式会社サイバーディフェンス研究所 情報分析部 上級分析官

オブザーバー

安冨　潔	京都産業大学 法務研究科 客員教授・法教育総合センター長、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）、IDF 会長
佐々木　良一	東京電機大学 研究推進社会連携センター 総合研究所 特命教授 兼 サイバーセキュリティ研究所 所長、IDF 理事 兼 顧問
櫻庭　信之	シティユーワ法律事務所 パートナー弁護士、IDF 理事
西川　徹矢	笠原総合法律事務所 弁護士、IDF 理事
坂　明	一般財団法人日本サイバー犯罪対策センター 理事

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

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

IDF 事務局

委員・事務局長	丸谷　俊博	株式会社フォーカスシステムズ 新規事業推進室 室長
事務局	山田　菜穂	株式会社フォーカスシステムズ 新規事業推進室
事務局	鈴木　洋佑	株式会社フォーカスシステムズ 新規事業推進室
事務局	長沢　紗希	株式会社フォーカスシステムズ 新規事業推進室
事務局	金　怜恵	株式会社 FRONTEO クライアントテクノロジー部
事務局	一居　政宏	株式会社 FRONTEO リスクコンサルティング部
事務局	田坂　麻紘	株式会社 FRONTEO クライアントテクノロジー部
事務局	清川　ひかる	株式会社 FRONTEO クライアントテクノロジー部

以上