「証拠保全ガイドライン　第 1 版」

2010 年 4 月 5 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」分科会ワーキンググループ

ガイドラインの趣旨

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、様々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と言える。そのデジタル・フォレンジックに関連した技術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、電磁的証拠となりうるものを、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頼性を失うため、これを行う者は、非常に神経を使うことになる。

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 2 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なきデータ複製ができず、取得時に証拠の一部が破損また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うる。

このような状況に応じた「電磁的証拠の保全をどの範囲で、どこまで原本同一性を保ちつつ行うべきか」という課題に対し、特に欧米では様々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。

本ガイドラインは、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このような状況に対処するため、我が国での電磁的証拠の保全手続きの参考として、様々な事案についてその特性を踏まえつつ広く利用して頂けるガイドラインを目指して作成されたものである。

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

本ガイドラインの立ち位置は、以下のようにまとめられる。

- 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を心がけた。
- 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を心がけた。

本ガイドラインは、インシデントの現場で最初に電磁的証拠の保全にあたる「ファースト・レスポンダー」を主な対象としているが、これに限らず、デジタル・フォレンジック関連技術を運用する全ての者が利用可能なものである。本ガイドラインは、この手続きにより収集・取得・保全等された電磁的記録が法廷において証拠として必ず採用されることを保証するものではなく、また、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、我が国における電磁的証拠保全の一般的な手続きがどうあるべきか、どの程度まで行えばデータが「法的紛争・訴訟に際し利用可能な（Forensically-sound な）」電磁的証拠となりうるか、という運用現場の悩みに対し、コンセンサスの形成の一助になることを意図して作成された。各現場においてご活用頂ければ幸いである。

最後に、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）　上原哲太郎

目　次

4　証拠保全機器の準備

4.1　複製先（コピー先、以下同じ）に用いる媒体（記憶装置）

4.1.1　媒体のチェック

4.1.2　無データ状態

4.1.3　完全（物理）複製

4.1.4　可読・可搬媒体

4.2　証拠保全機器に求められる機能

4.2.1　書込み防止機能

4.2.2　完全（物理）複製機能

4.2.3　同一性検証機能

4.2.4　作業ログ・監査証跡情報の表示・出力機能

4.3　証拠保全ツールに関する要件

4.3.1　完全（物理）複製が可能な機能

4.3.2　信頼できる機関による検証

4.3.3　その他

4.4　その他、証拠保全に必要な機器・機材・施策の準備

4.4.1　HDD の物理的制限の認識及び（強制）解除機能の有無の確認

4.4.2　HDD パスワード・暗号化に対する準備

4.4.3　IDE HDD に設置されているジャンパーピンの取扱い

4.4.4　RAID 装置や構造が複雑なサーバー類に対する準備

4.4.5　事前の十分なテスト及び機能の稼働状態のチェック

5　証拠保全作業中・証拠保全作業後

5.1　代替機・代替ツール・代替手段の準備

5.2　立会人等

5.3　同一性の検証

5.4　証拠保全の正確性を担保する作業内容の記録

5.4.1　行動履歴の記録

5.4.2　証拠保全に関わる機器の情報の記録

5.4.3　ビデオ及び写真撮影

5.5　複製先の取扱い

5.5.1　厳重な管理

5.5.2　フォレンジックチーム等への提出・譲渡

付録

○ 関連資料

○ 「技術」分科会ＷＧメンバー

○ IDF 団体会員「製品・サービス区分リスト」

1　事前に行う準備

インシデントレスポンス（初動対応、証拠保全）では、以下のような事前準備が必要と考えられる。

1.1　インシデントレスポンスを想定した初動対応、証拠保全プロセスの検討及び体制の確立

○ インシデントレスポンス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、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[2]）、目標復旧時間（RTO[3]）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

○ インシデントレスポンスの経緯（時系列）の記録方法の確立

○ インシデントレスポンスを想定した初動対応、証拠保全の手順書の作成

1.2　インシデントレスポンスに関連する情報収集、情報共有及び分析

○ 多様化するインシデントに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）の確認

○ インシデントレスポンス関連組織等との情報共有、コネクションの確立

1.3　インシデントレスポンス（初動対応、証拠保全）時に必要と考えられる資機材等の選定及び準備

○ 証拠保全時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

– 精密ドライバー、荷札、各種テープ、白手袋、テーブルタップ等

○ 初動対応、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（CD-R ドライブ）等

○ 初動対応、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

（基準例）

・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。

---

[2] 最大許容停止時間（Maximum Tolerable Period of Disruption）

[3] 目標復旧時間（Recovery Time Objective）

（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

- ハードディスク、CD-R 等の各種メディア

○ 証拠保全用複製装置の準備

- 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

- ビデオカメラ、作業確認チェックシート、備忘録用紙、ボールペン等

1.4 インシデントレスポンス時に使用する資機材等の熟達

○ 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実施

2　インシデント発生（または発覚、以下同じ）直後の対応

2.1　インシデントレスポンスが未実施の場合の活動

2.1.1　発生したインシデントの内容の把握

2.1.1.1　発生したインシデントの内容

○ 情報流出

○ ウイルス感染・発症

○ 不正侵入・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・破壊

2.1.1.2　インシデント発生の検知の経緯

○ ログのレビュー

○ 不正検知システム

○ 内部告発

○ 自己申告

○ 外部からの通報

2.1.1.3　インシデントが発生した時間

○ システム時計の正確性の確認

2.1.1.4　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[4]。

– 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。

2.1.2　発生したインシデントに関する対象物の決定

2.1.2.1　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（デスクトップ型／ノート型／サーバー型）

– 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）（バルク／外付け）

– ストレージメディア（CD／DVD／FD／PD[5]／BD[6]／MO／各種フラッシュメモリ等）

---

[4] 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。

[5] PD：Phase-change Dual 又は Phase-change Disc。相変化記憶媒体。

– 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
– 音楽プレイヤー
– ゲーム機器（Wii、NINTENDO DS[7]、PS3[8]等）
– IC レコーダ
– 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

2.1.2.2　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

2.1.3　証拠保全を行う上で必要な情報の収集

2.1.3.1　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[9]・DCO[10]の設定の有無[11]等、通常環境下で視認可能な物理的破損・損傷の有無。
○ HDD・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 を筐体から取り出せず、専用 CD ブートで証拠保全を行う場合、光ディスクのドライブ及び USB/FireWire[12]、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 パスワードロック、HDD 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。

2.2　インシデントレスポンスが着手済みである場合の活動

---

[6] BD：Blu-ray Disc。

[7] 「Wii」及び「NINTENDO DS」は任天堂株式会社の登録商標です。

[8] 「PS3」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。

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

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

[11] これら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。

[12] FireWire：パソコンと周辺機器を結ぶ転送方式の一つである「IEEE 1394」規格の愛称。

2.2.1　上記項目 2.1 に関する各種情報の確認[13]

○ 上記項目 2.1 に関する各種情報の過不足等の有無

○ 上記項目 2.1 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または承認の有無

2.2.2　インタビュー以前のインシデントレスポンス内容の確認（電源を抜いたかどうか等）

2.2.3　対応に過不足が確認された場合の対処

○ 収集した情報・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インタビューまたは情報収集。

○ 収集した情報・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な該当箇所の情報収集。

○ 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を聴取し、不必要と判断された場合は削除。

2.3　インシデントレスポンスを円滑に進めるための活動

2.3.1　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、見やすく且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

○ インシデントレスポンスの作業のみを行えるための場所の確保
施錠等によりインシデントレスポンス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、インシデントレスポンス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、GUEST 用 IC カードの貸与等

2.3.2　関係組織との連携

○ 法務部門担当者、システム担当者との連携

○ 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

○ 関係者の確保及び無関係者の排除
インシデントレスポンス作業工程において、関係ない第三者が関与できない状況を確保。
また、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

[13] 対象物の選定及び情報の収集は、先方によって終了しているものとする。

3　対象物の収集・取得・保全

3.1　対象物の状態の把握

○ 対象物が存在する現場の、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

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、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。

3.2　収集・取得・保全するための対象物の処置

3.2.1　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 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。但し、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。

○ 無為に HDD 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）。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。

3.2.2　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。

– 削除ファイルへ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、直後に決めた対象範囲を取得する。

○ 電源を OFF にする

- 3.2.6 参照

○ 無為に HDD 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）。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。

3.2.3　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、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

- 3.2.6 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。

3.2.4　対象物がコンピュータ（サーバー型）で、電源が ON の状態の場合

○ サーバー型では、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 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（1CD-LINUX[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ー等で利用している場合、RAID 装置の使用有無に拘わらず、サーバー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。

3.2.5　対象物がコンピュータ以外（メディア系）の場合

3.2.5.1　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（または管理主体）、使用用途、状況、収集・取得・保全に至った経緯及び目的等を記録する。

3.2.5.2　外部メディアにアクセスする PC 等の特定

○ IEEE 1667[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。

3.2.5.3　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。

3.2.6　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

– サーバー系 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、原則としては、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。

– 強制的に電源を OFF にした場合、想定されるリスクの例は以下の通り：

---

[14] RAID：Redundant Arrays of Inexpensive Disks

[15] 1CD-LINUX：PFM によって Vine Linux を CD にインストールしたシステム。CD ドライブと RAMDISK のみでハードディスクを使用しないで起動でき、 インターネットオールインワンサーバとして使用できる。

[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。

・HDD に物理的な損傷（不良セクター）を生じやすい。
・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

– 通常のプロセスで電源を OFF にした場合、想定されるリスクの例は以下の通り：
・OS の終了処理や更新、その他のアプリケーション等により、データの上書きや削除等が発生することを考慮する。
・揮発性情報が取得できない。

3.2.7　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 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。
上記のような機器は、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。
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可能性がある。

3.2.8　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。

3.3　その他、収集・取得・保全する必要性がある対象物

3.3.1　対象物のマニュアル・ユーザー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 の取り外し方
– バッテリーの取り外し方
– BIOS の起動方法と画面の見方
– 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

4　証拠保全機器の準備

4.1　複製先（コピー先、以下同じ）に用いる媒体（記憶装置）

4.1.1　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。尚、フラッシュ系媒体は、代替領域等の隠し領域の都合上、証拠保全には向かない。

4.1.2　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。

4.1.3　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。

4.1.4　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 を用いる場合、汎用性の高い SATA[17]等を利用する。

○ イメージによる複製を行う場合、2TB 以上のデータが、FAT32 ファイルシステムでは扱えないため、コピー先のファイルシステムを選択する。

○ 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。

4.2　証拠保全機器に求められる機能

4.2.1　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）。

4.2.2　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[18]が原本と異なった場合において、説明が

---

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

[18] 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-1 や 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

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／EnCase Image 等)。

4.2.3　同一性検証機能

4.2.3.1　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。

4.2.3.2　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い場合に備えて、セクターサイズを確認する。

4.2.4　作業ログ・監査証跡情報の表示・出力機能

4.2.4.1　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（コピー）（検証）速度／エラー発生時の詳細情報等

4.2.4.2　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

4.3　証拠保全ツールに関する要件

4.3.1　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 CD／FD ブートによる利用

– HDD 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

値を取得することが望ましい。(SHA-1 と SHA-2 等)

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 より CD を優先して起動できるよう、BIOS 等で起動順序を確認し、必要に応じて変更
- 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）

4.3.2　信頼できる機関による検証

○ CFTT（Computer Forensics Tool Testing[19]）等の信頼できる機関にて検証されたものを利用

4.4　その他、証拠保全に必要な機器・機材・施策の準備

4.4.1　HDD 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。

4.4.2　HDD 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。

- 但し、インシデントレスポンスにかか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。

4.4.3　IDE[20] HDD 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 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。

4.4.4　RAID 装置や構造が複雑なサーバー類の証拠保全

○ HDD 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。

4.4.5　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と、機能の稼働状況をチェックする。

[19] 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/）

[20] 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。

5　証拠保全作業中・証拠保全作業後

5.1　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。

5.2　立会人等

証拠保全、インシデントレスポンス等を行う場合、可能な限り、立会人を付けるか、複数人で実施する。

5.3　同一性の検証

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

5.4　証拠保全の正確性を担保する作業内容の記録

5.4.1　行動履歴の記録

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

5.4.2　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

5.4.3　ビデオ及び写真撮影

各工程で行った作業は、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。また、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。

5.5　複製先の取扱い

5.5.1　厳重な管理

複製先は、他の機器と混在しないよう、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[21]等を作成して、厳重に管理する。

---

[21] 「誰が、いつ、何をしたのか」が把握できる書類。

○ 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。

5.5.2　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、壊れ物且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。

付録

○ 関連資料

- ■「Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition /Forensic Examination of Digital Evidence: A Guide for Law Enforcement」
- ■「(CERT) First Responders Guide to Computer Forensics」
- ■「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 21 年 6 月　経済産業省）

○ 「技術」分科会ＷＧメンバー（所属は 2010 年 3 月現在）

座　長	上原哲太郎	京都大学 学術情報メディアセンター 准教授
副座長	山田　　晃	独立行政法人情報処理推進機構 セキュリティセンター 調査役
委　員	伊原　秀明	株式会社 Ji2　フォレンジックエバンジェリスト
委　員	小山　幸輝	株式会社カカクコム 情報セキュリティ室 アシストマネージャー
委　員	坂　　明	慶應義塾大学　政策・メディア研究科 教授
委　員	篠原　明彦	ネットエージェント株式会社 フォレンジック調査部 部長代行
委　員	芝　　啓真	株式会社フォーカスシステムズ フォレンジックセキュリティ室 主任
委　員	杉山　一郎	株式会社 UBIC 事業部 フォレンジックディビジョン 課長
委　員	名和　利男	株式会社サイバーディフェンス研究所 上級分析官
委　員	西山　俊彦	株式会社 UBIC 取締役
委　員	本庄　　豊	株式会社ワイ・イー・データ 情報セキュリティ事業部技術グループ 担当課長
委　員	松本　　隆	ネットエージェント株式会社 フォレンジックエバンジェリスト
委　員	守本　正宏	株式会社 UBIC 代表取締役社長
委　員	山内　　崇	株式会社ピーシーキッド 取締役
オブザーバー	萩原　栄幸	株式会社ピーシーキッド 上席研究員

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	田澤　奈々	株式会社フォーカスシステムズ 新規事業推進室
事務局	椎原　麻衣	株式会社フォーカスシステムズ 新規事業推進室
事務局	安田　央奈	株式会社フォーカスシステムズ 新規事業推進室

○ **ＩＤＦ団体会員「製品・サービス区分リスト」（全 33 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・訴訟支援・コンサルティング
③ トレーニング、 ④ ネットワーク監視・記録、 ⑤ データリカバリー
⑥ その他

ＩＤＦ団体企業名	ｻｰﾋﾞｽ区分	主要製品等
株式会社フォーカスシステムズ http://www.focus-s.com	①、②、③、④、⑥	各種ﾌｫﾚﾝｼﾞｯｸﾂｰﾙ全般（書込防止装置、解析ｿﾌﾄｳｪｱ、HDD 複製ﾂｰﾙ、解析ﾜｰｸｽﾃｰｼｮﾝ等）、ﾌｫﾚﾝｼﾞｯｸﾄﾚｰﾆﾝｸﾞ、DB 監視ｿﾌﾄｳｪｱ（Chakra）、eDiscovery ｿﾌﾄｳｪｱ（Nuix）、ﾌｫﾚﾝｼﾞｯｸ調査・訴訟支援ｻｰﾋﾞｽ 他
株式会社 UBIC http://www.ubic.co.jp	①、②、③、④、⑥	ICS、Access Data、Digital Intelligence 各社製品、ﾌｫﾚﾝｼﾞｯｸ調査士養成ｺｰｽ
株式会社ラック http://www.lac.co.jp	②、③、④	ｻｲﾊﾞｰ救急ｾﾝﾀｰ、ｻｲﾊﾞｰ 119、ｾｷｭﾘﾃｨｱｶﾃﾞﾐｰ「ﾃﾞｼﾞﾀﾙﾌｫﾚﾝｼﾞｯｸ BOX ｼﾘｰｽﾞ」、JSOC 監視ｻｰﾋﾞｽ、情報漏洩ﾁｪｯｸｻｰﾋﾞｽ
株式会社ディアイティ http://www.dit.co.jp	①、②、③	X-Ways Forensics 社製品、ﾌｫﾚﾝｼﾞｯｸｻｰﾋﾞｽ、捜査機関向け Forensics 専攻教養ｺｰｽ、捜査機関向けｲﾝﾃﾘｼﾞｪﾝｽ専攻教養ｺｰｽ、民間向けｺﾝﾋﾟｭｰﾀﾌｫﾚﾝｼﾞｯｸ技術者養成ｺｰｽ
株式会社オーク情報システム http://www.oakis.co.jp	①、④	ﾈｯﾄﾜｰｸﾌｫﾚﾝｼﾞｯｸｻｰﾊﾞ『NetEvidence』の開発・販売
ネットエージェント株式会社 http://www.netagent.co.jp	①、②、④、⑥	PacketBlackHole、OnePointWall、USB 関所守、Winny 特別調査員、P2P 調査ｻｰﾋﾞｽ、ﾌｫﾚﾝｼﾞｯｸ調査ｻｰﾋﾞｽ
株式会社ワイ・イー・データ http://www.yedata.co.jp	① ② ⑤ ⑥	データ調査、データ復旧、データ複製、データ消去 データ復旧ソフト EasyRecovery メール復旧ソフト PowerControls
株式会社ピーシーキッド http://www.pckids.co.jp	①、②、③、⑤、⑥	ﾈｯﾄﾜｰｸﾌｫﾚﾝｼﾞｯｸ製品『NetEvidence』の正規代理店、ﾌｫﾚﾝｼﾞｯｸ調査・訴訟支援・ｺﾝｻﾙﾃｨﾝｸﾞｻｰﾋﾞｽ提供、ﾄﾚｰﾆﾝｸﾞ、ｾﾐﾅｰ実施、『ﾃﾞｰﾀ復活ｻｰﾋﾞｽ』提供、ﾃﾞｰﾀｺﾋﾟｰ、ﾃﾞｰﾀ消去等のﾃﾞｰﾀ処理ｻｰﾋﾞｽ提供
AOS テクノロジーズ株式会社 http://fss.jp	①、②、③、⑤	AOS Forensics Toolkit 他
ハミングヘッズ株式会社 http://www.hummingheads.co.jp	①	情報漏洩対策ｿﾌﾄ「ｾｷｭﾘﾃｨﾌﾟﾗｯﾄﾌｫｰﾑ」、ｿﾌﾄｳｪｱﾛﾎﾞｯﾄ（自動化ﾂｰﾙ）「ｲﾝﾃﾘｼﾞｪﾝｽﾌﾟﾗｯﾄﾌｫｰﾑ」

KS オリンパス株式会社 http://www.ksolympus.co.jp/index2.html	①	Medical Forensic System
インターナショナルリスクリミテッド http://www.intl-risk.com/japan/index.htm	①、②、⑤、⑥	AttenexPatterns、Ringtail Legal Ringtail QuickCull、TrialMax
株式会社 Ji2 http://www.ji2.co.jp	①、②、③、⑤、⑥	Guidance Software、Clearwell、Susteen、Atola Technology, Logicube 各社製品、各種 EnCase(r) 公式ﾄﾚｰﾆﾝｸﾞｺｰｽ、Windows ﾌｫﾚﾝｼﾞｯｸのための要素技術ｾﾐﾅｰ、ﾃﾞｰﾀﾘｶﾊﾞﾘｰ ﾄﾚｰﾆﾝｸﾞ
株式会社サイバーディフェンス研究所 http://www.cyberdefense.jp/	②、③	情報漏えい初動支援ｻｰﾋﾞｽ、ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ&ﾌｫﾚﾝｼﾞｯｸｾﾐﾅｰ
アマノタイムビジネス株式会社 http://www.e-timing.ne.jp/	①	ﾀｲﾑｽﾀﾝﾌﾟｻｰﾋﾞｽ
エンカレッジ・テクノロジ株式会社 http://www.et-x.jp	①	ESS REC、SEER INNER、ESS AutoAuditor 等
エムオーテックス株式会社 http://www.motex.co.jp	④	LanScopeCat6 LanScopeGuard3 LanScopeEco
ベライゾンビジネス http://www.verizonbusiness.com/jp	②、③、④、⑤、⑥	情報資産ﾃﾞｨｽｶﾊﾞﾘ&情報漏えいｱｾｽﾒﾝﾄ＆対策、ﾌｫﾚﾝｼﾞｯｸ＆ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ（IR）QIRA 調査ﾚﾎﾟｰﾄ
株式会社英揮情報システム http://www.eiki-infosys.co.jp/	①、②、③、④	IDEA,CASE WARE 各種製品

その他の IDF 団体会員

シーア・インサイト･セキュリティ株式会　http://www.seer.jp/
株式会社 NTT データ　http://www.nttdata.co.jp/
株式会社東証システムサービス　http://www.tssx.co.jp/
日本オラクル株式会社　http://www.oracle.com/lang/jp/index.html
TDC ソフトウェアエンジニアリング株式会社　http://www.tdc.co.jp/
有限責任監査法人トーマツ　http://www.tohmatsu.com/view/ja_JP/jp/companies/audit/
株式会社インフォセック　http://www.infosec.co.jp/
ソニー株式会社　http://www.sony.co.jp/
株式会社エス・シー・ラボ　http://www.optic.or.jp/com/sc-lab/sc-lab.html
株式会社アイアイジェイテクノロジー　http://www.iij-tech.co.jp/
財団法人　保安電子通信技術協会　http://www.hotsukyo.or.jp/
ソレラ　ネットワークス　ジャパン株式会　http://soleranetworks.co.jp/
クオリティ株式会社　http://www.quality.co.jp/
株式会社カカクコム　http://corporate.kakaku.com/

以上