主要なデジタル・フォレンジック調査・解析用ツール（ソフト）

No.	ツール名	区分	国内取扱店　（製造・供給元）	ツールの特徴や概要
1	Autopsy	調査・解析	ベイシス・テクノロジー株式会社 https://www.basistech.jp/solutions/autopsy/ Autopsy https://www.autopsy.com/download/	オープンソースGUIで操作しやすいのが特徴。Basis Technology 支援のもと、世界中の何千人ものユーザーと開発者で構成されているオープンソースコミュニティーで開発されたソフトウェアで、誰でも無料で利用できる。☆「日本語処理解析性能評価」受検製品2018.3.20：「Autopsy (Ver.4.6.0)」
2	analyzeMFT	調査・解析	GitHub - dkovar/analyzeMFT https://github.com/dkovar/analyzeMFT	pythonで書かれたWindowsのアーティファクト＄MFTを解析するときに使用するオープンソースツール。NTFS（ファイルシステム）の＄MFTファイルを解析する。
3	Arsenal Image Mounter	証跡保全	Arsenal Recon https://arsenalrecon.com/products/	Arsenal Image Mounterは、ディスク イメージの内容を Windows の完全なディスクとしてマウントするツール 。Windows に関する限り、アーセナル イメージ マウントによってマウントされるディスク イメージの内容は実際の SCSI ディスクであるため、ユーザーはディスク マネージャとの統合、ボリューム シャドウ コピーへのアクセス、仮想マシンの起動など、ディスク固有の機能を利用できる。
4	AXIOM / IEF [Internet Evidence Finder] (Magnet Forensics)	調査・解析	https://www.magnetforensics.com/	ウェブブラウザの履歴やSNS、クラウド、メッセンジャーチャット履歴、ウェブメールカテゴリーごとに抽出したデータを表示してくれる。。IEFは、強力かつユーザーフレンドリーなフォレンジックツールで、直感的なユーザーインターフェースにより、どんなレベルの方でも簡単に 重要な証拠を発見することが出来る。 AXIOMは、IEF従来の解析機能やデータ共有機能に加え、データ抽出機能を標準搭載し、データ抽出および解析を自動で行うことが出来るようになったIEFの上位版。
5	Belkasoft Evidence Center（Belkasoft）	証跡保全	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/belkasoft/ Belkasoft https://belkasoft.com/	Windows OS対応メモリ取得ツール アンチダンピング保護をバイパスするように設計されている。パソコンからスマートフォンまで幅広い解析能力を持ち、著名なフォレンジックツールと連携して使用できる。また、本ソフトには、これからの時代に欠かせないメモリ保全用の無料ツール Live RAM Capturerが付属している。さらに、リモート機能によりターゲット端末のストレージとメモリの保全及び調査ができるため、国外に証拠端末がある場合のリモート捜査にも適している。
6	BlackLight / MacQuisition（BlackBag）	調査・解析	BlackBag Technologies https://www.blackbagtech.com/	WindowsOSのメモリ解析やシステムファイルの観点からの閲覧履歴の解析や、MacOSのAPFS、FusuionDrive等のMacに特化した解析も可能なフォレンジックツール。 MacQuisition はMac Windows iOS GrayKey Android をサポートする保全ツール。Apple T2チップを使用してMacの物理イメージを作成する。BlackLightは取得したデータを解析するツール。この二つは合わせて使用したい。
7	Caine	統合ツール	Linux ディストリビューション https://www.caine-live.net/ https://cain-abel.updatestar.com/ja プロジェクトマネージャー Nanni Bassetti(Bari-イタリア)	CAINEはセキュアブートにも対応しているUbuntuベースのLinuxライブディストリビューション。GUIでフォレンジック調査が可能、WindowsIR/Liveフォレンジックツールも用意されている。 カイン&アベルは、パスワード回復ツールで様々な種類のパスワードの回復をすることができ、パスワード解析（暗号化パスワードやハッシュ値をブルートフォースする等）やネットワークスニファ解析を行うツール。 尚、アンチウイルスソフトからは「マルウェア」や「悪意あるプログラム」と判定される場合が多い。
8	CDIR Collector（Cyber Defense Institute Incident Response Collector）	証跡保全	株式会社サイバーディフェンス研究所 https://www.cyberdefense.jp/products/cdir.html GitHub - CyberDefenseInstitute/CDIR https://github.com/CyberDefenseInstitute/CDIR	Windows OS用のファストフォレンジックツールで、調査対象端末の汚染や業務への影響を最小限に抑えながら安全にデータを収集する。多数の端末に感染または侵入の可能性があり、攻撃が現在も進行している可能性がある場合などに効果を発揮する。 CDIR-Cで収集したデータは一般的なフォレンジックツールで読み込んで解析することが可能なため、自組織では証拠保全までを実施し、フォレンジック調査を外部のサービスベンダーに依頼することを想定している組織にも有効に活用できる。
9	DEFT(Digital Evidence＆Forensics Toolkit) DART(Digital Advanced Response Toolkit)	統合ツール	Stefano Fratepietro https://n0where.net/digital-forensics-toolkit-deft (http://www.deftlinux.net/)	DEFTは、フォレンジック用Linuxディストリビューションであり、Linux上でWindows用のツールを使用するためにwineを用いている。DEFTは、Windowsで実行可能なフォレンジックシステムであり、フォレンジックおよびインシデントレスポンスに最適なツールを含むDARTとペアになっている。DARTは、機器のロギングと整合性チェックを備えたGUIを備えている。USBに入れる軽量版のDEFT Zeroというバージョンも存在する。
10	Email Auditor 19（メール監査ツール）	調査・解析	株式会社FRONTEO http://www.kibit-platform.com/products/email-auditor/	監査官の調査観点を学習したAIが大量の電子メールを解析し、要監査メールを優先度順に自動抽出するメール監査システム。強力な検索システムとの併用も可能で、監査業務の工数を大幅に削減するとともに、内在するリスクの可視化も可能。
11	EnCase（OpenText）	調査・解析	OpenText https://www.opentext.jp/products-and-solutions/products/security/encase-forensic	証拠保全から調査解析、報告まで可能な統合フォレンジックツールで、APFSやモバイルデータの取得も可能。NIST等の第三者機関から信頼性を検証されており、法執行機関、民間を問わず幅広く利用されている。裁判での使用例も多岐に渡る。タブレット、スマートフォン、GPS など 25 種類のモバイルデバイスを含む、最も広範囲な種類のデバイスからデータを取得でき、証拠の整合性を保ちながら、詳細な調査結果レポートを生成できる。
12	Eric Zimmerman ツール	調査・解析	Eric Zimmerman https://ericzimmerman.github.io/#!index.md	SANSのトレーナーでもあるEric Zimmerman氏が開発しているWindows用フォレンジックツール群で、どのツールも同じように使用でき使いやすい。新しいバージョンへの対応も早い。
13	Event Log Explorer	調査・解析	FSPro Labs https://eventlogxp.com/jap	Windowsのイベントログを解析するためのツール。複数PCのログを集中管理する機能もある。個人使用の場合無料で使用できるが商用の場合は有料となる。イベントログを見る際のフィルターリングや検索が便利。
14	Final Forensic / AndrEx（AOS）	統合ツール	リーガルテック株式会社 https://www.fss.jp/aos-ファイナルフォレンジック/	完全日本語ユーザーインターフェースによるパソコンデータの保全・解析・調査ツールです。対応OSは、Windows7、Windows10。 強力なデータ復元機能と高度な検索機能を備え、データ保全、復元、分析、検索を行い分析レポートを作成する。警察、検察などの捜査機関で実績を上げている専門調査ツールで、専門家が行う高度な作業を非常に簡単なインターフェースで操作することが可能。 ☆「日本語処理解析性能評価」受検製品2018.9.28：「 Final Forensics(Ver.4)」
15	F-Response	証跡保全	Agile Risk Management LLC F-Response https://www.f-response.com/software	F-Responseは、ソフトウェアユーティリティで、調査者は、選択したツールを使用してIPネットワーク上でリモートにより物理マシン（ディスク、RAID、ボリューム、メモリ）及びクラウドストレージプロバイダーへの直接の読み取り専用のアクセスを提供するように設計されている。フォレンジック、e-ディスカバリ（電子情報開示）、インシデントレスポンス用のデータ検出・収集アプリケーション。
16	FTK [Forensic Tool Kit]（AccessData）	統合ツール	AccessData https://accessdata.com/products-services/forensic-toolkit-ftk	GUIのデータ収集、解析ツール。フォレンジックの各過程に応じた機能を搭載したツールを、パッケージソフトウェアとして提供しており、保全やファイル、レジストリ等の解析、暗号化やパスワード解析等目的に応じた対応することが可能。
17	FTK Imager Lite , FTK Imager	証跡保全	Access Data https://accessdata.com/product-download/ftk-imager-lite-version-3-1-1	イメージのマウントやディスクイメージの作成、メモリの保全も可能な無償ツール。FTK Imager は、PCへのインストールを必要とし、FTK Imager Lite は、インストールすることなく使用できる。両者ともメモリダンプの取得も可能となっている。

Ｎｏ.	ツール名	区分	国内取扱店　（製造・供給元）	ツールの特徴や概要
18	Ghidra (NSA)	調査・解析	米国国家安全保障局(NSA) https://www.nsa.gov/resources/everyone/ghidra/ https://ghidra-sre.org/	NSA(アメリカ国家安全保障局)が開発したリバースエンジニアリングのためのツール群。 GHIDRAは、GUIベースの逆アセンブラで、実行ファイルのバイナリからソフトウェアやマルウェアを解析し、人間にも解読可能なアセンブリ言語に変換してくれる。「GHIDRA」はJavaでコーディングされ、Windows・macOS・Linux・Android・iOSで動作する。
19	Griffeye	調査・解析	Griffeye Technologies https://www.griffeye.com/	Griffeye Analyzeは、デジタルメディア調査用の汎用ソフトウェアプラットフォームで、Analyze DI Proには90日間の無料トライアル期間がある。グリフィー・インテリジェンス・データベースを使用すると、異なるスタンドアロン・データベースを介して接続することにより、国際的に、全国的に、地区間およびチーム内でインテリジェンスを共有することができる。
20	HX-Recovery for DVR & NVR	調査・解析	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/hx-recovery/	HX-Recoveryは、監視カメラや防犯カメラ装置の動画再生や削除された映像を簡単に解析できるフォレンジックツール。監視カメラや防犯カメラ装置の多くは、中国や韓国のメーカーが大半を占めており、この中には世界的に有名なメーカー製品から、OEM等、各国で無名のメーカー製品となるものまで様々なため、今まで扱いが大変だった証拠動画の再生が簡単にできるようになる。
21	IDA Pro (Hex-Rays)	調査・解析	Hex-Rays https://www.hex-rays.com/products/ida/	マルウェア解析、プログラムの脆弱性調査などに用いられる機能が豊富なクロスプラットフォームのマルチプロセッサで、逆アセンブラ及びデバッガができ、コンパイラ生成コードとユーザー記述コードを自動峻別し、表示することができる。
22	Intella	調査・解析	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/intella/ Vound Colorado https://www.vound-software.com/	Intellaは、重要な証拠データを容易に見つけ出す強力なフォレンジックサーチツール。ストレージの進化で削除したデータは技術的に探せなくなり、膨大な既存データから証拠を探さねばならにが、Intellaは、対象データの検索結果を視点を変えて確認でき、データと人、データと組織の関係を簡単に可視化できる。 本製品は、デジタル・フォレンジック研究会(IDF)による2019年実施の「日本語処理解析性能評価」で高いスコアを獲得している。 ☆「日本語処理解析性能評価」受検製品2017.12.15：「Intella Professional (Ver.2.0.1)」 ☆「日本語処理解析性能評価」受検製品2019.3.8：「Intella Professional (Ver.2.2.1)」
23	Kali Linux	統合ツール	kali.org Offensive Security https://www.kali.org/downloads/	ペネトレーションテストを目的としたLinuxディストリビューションで、フォレンジックツールや解析ツールも多く含まれている。脆弱性診断のため疑似攻撃をするために使われている。
24	Kansa	証跡保全	davehull kali.org https://github.com/davehull/Kansa	Windowsマシンを対象としたPowerShellベースのインシデントレスポンス用フレームワークです。WinRMを利用することで、数千台規模のリモート端末のデータ収集が可能となる。
25	KAPE (Kroll Artifact Parser and Extractor)	証跡保全	クロール・インターナショナル・インク https://www.kroll.com/ja-JP	トリアージのために必要な証跡を対象の Windows機器から収集するためのプログラム。ファイルの収集とコマンドやプログラムを指定することで実行結果の収集もできるライブフォレンジックツール。一般的に収集すべき証跡は標準で組み込まれており利用者が選択することが可能。
26	KIBIT Automator(AIツール)	調査・解析	株式会社FRONTEO https://legal.fronteo.com/products/kibit-automator/	ドキュメントレビューに用いられる業界スタンダードツールであるLit i View、Relativityに実装可能なプラグインツール。AIを用いた、Assisted Learning、Heat Map、ハイライト機能等により、ドキュメントレビューの劇的な高速化、高品質化、コスト削減を同時に実現可能。
27	LACE	調査・解析	BlueBear LES https://bb-les.ca/solutions/	画像・動画解析用ツール。他のファイルに埋め込まれた画像、動画ファイルの抽出を行うとともに、重複ファイルの削除や顔認証を通じて効率的に画像のレビュー、分類が可能。
28	Lit i View E-DISCOVERY(データ解析ツール)	調査・解析	株式会社FRONTEO https://legal.fronteo.com/products/e-discovery/	eディスカバリの世界標準であるEDRMに準拠し、全作業をワンストップでサポートする。英語はもちろんアジア各国に特有のアプリケーションや文字コードにも広く対応し、eディスカバリ支援に必要な全機能及びAI を搭載したスタンダードツール。 ☆「日本語処理解析性能評価」受検製品2017.1.19：「Lit i View E-DISCOVERY(Ver.7.12.203548)」
29	Lit i View XAMINER(データ解析ツール)	調査・解析	株式会社FRONTEO https://legal.fronteo.com/products/xaminer/	豊富なフォレンジック調査経験で蓄積された知見やノウハウをベースに独自開発された、AI搭載データ解析ツール。AIによる自動仕分け機能や相関関係作成機能、アジア言語への対応力からなる高精度な検索能力、高度なメール解析機能は、調査の高速化に寄与する。メールの会話内容から人物の行動を分析するCentral Linkageなどの機能がある。 ※官公庁限定販売製品
30	Log Parser(Lizard)	解析支援	Lizard Labs Software http://www.lizard-labs.com/log_parser_lizard.aspx	Microsoft LogParserにGuiを提供するツールで、SQLクエリを利用してレジストリ、ファイルシステム及びActive Directory サービスのログを解析する。ログファイル、XMLファイル、CSVファイル等のテキストベースのデータへのユニバーサルクエリアクセスと、イベントログ、IISログ等のWindows OS上の主要なデータソースへのユニバーサルクエリアクセスを提供する非常に強力で自由で汎用性が高い。
31	MacQuisition	証跡保全	BlackBag Technologies https://www.blackbagtech.com/	MacQuisition CFC Editionは、Targeted Data Collection/Live Data Acquisition/Forensic Imagingと用途に応じた柔軟な保全に対応した3-in-1ソリューションです。10年以上の経験豊富な調査官がテストし使用している本製品は、MacOSX上で動作する。FusionDrive[SSD+HDD]含む185種類以上のMacPCから安全に起動し、データを取得することができ、Macの複雑な分解を行わずUSBブートにより保全を行うことができる。
32	Magnet Acquire	証跡保全	MagnetForensics.inc https://www.magnetforensics.com/products/magnet-acquire/	iOS、Android、ハードディスク、リムーバブルメディアからイメージを取得するためのツール。ACQUIREは、信頼性の高い高速抽出と直感的なユーザーインターフェイスを兼ね備えており、データを迅速かつ簡単に提供でき、取得するデータの品質が最大化され、アクティビティログとドキュメントを使用して、使用されたメソッドを理解できる。
33	Magnet RAM Capture	証跡保全	MagnetForensics.inc https://www.magnetforensics.com/resources/magnet-ram-capture/	MAGNET RAMキャプチャは、容疑者のコンピュータの物理メモリをキャプチャするように設計された無料のメモリキャプチャツールで、メモリ内でのみ見つかる貴重なアーティファクトを復元および解析できる。キャプチャーしたメモリデータは、raw形式でエクスポートされる。最新バージョン:v1.20（2019年7月24日リリース）–仮想セキュアモードが有効になっているWindows 10システムからのRAM取得をサポートできるようになった。
34	MSAB Office	統合ツール	株式会社FRONTEO https://legal.fronteo.com/products/msab/ MSAB https://www.msab.com/ja/	モバイルフォレンジック用オールインワンプラットフォームで、WindowsPC上で起動するように設計されている。20、000以上の機種に対応し、最大3台同時に端末内のデータ抽出が可能。データ抽出ツールである「XRY」に加え、データ解析用ソフトウエアである「XAMN Spotlight」もバンドルされた、オールインワンのモバイル端末フォレンジックツール。
35	Net Hunter	解析支援	kali-nethunter-project Kali Linux NetHunter https://www.kali.org/kali-linux-nethunter/	NexusやOnePlusデバイスのためのAndroid用モバイルペネトレーション用プラットフォームで、HID Keyboard Attacks、BadUSB attacks、Evil AP MANA attacksなどをサポートしているAndroid ROMオーバーレイ。NetHuntelは、Offensive Securityとコミュニティが開発するオープンソースプロジェクト。
36	Nuix Discover	証拠開示	Nuix Japan https://www.nuix.com/jp/products/nuixringtail	エンド・トゥ・エンドのeディスカバリー(証拠開示)を提供するツールで、プロセッシング、レビュー、分析、プレディクティブ・コーディング技術が統合され、より良い証拠を迅速に解明できる。訴訟や規制案件への戦略に速やかに取り組める。

Ｎｏ.	ツール名	区分	国内取扱店　（製造・供給元）	ツールの特徴や概要
37	Nuix Investigate	解析支援	Nuix Japan https://www.nuix.com/jp/products/nuixinvestigate	ケースデータをいつでもどのWebブラウザーからでも、共有、検索、分析できる共同作業で解決する環境を提供する。強力な可視化によって、主要人物が誰なのか、また何をしているかが一目で分かるため、情報に基づくより優れた決定をより迅速に下すことができる。 ※「日本語処理解析性能評価」受検製品2018.6.29：「Nuix investigation&Response(Ver.7.4.5)」→再評価実施予定
38	Nuix Workstation	調査・解析	Nuix Japan https://www.nuix.com/jp/products/nuixworkstation	膨大なデータを短時間で処理でき、大量の非構造化データ、半構造化データ、そして構造化データを処理し、情報を抽出できる。スピード、規模、そして正確さでデータを処理、検索、インデックス化し、法執行調査、規制対応調査、企業不正調査、情報ガバナンスなどの調査を支援する。
39	Oxygen Forensic Detective	統合ツール	株式会社サイバーディフェンス研究所 https://www.cyberdefense.jp/products/oxygen.html Oxygen Forensics, Inc. https://www.oxygen-forensic.com/en/	直感的な操作が可能なスマートフォンやタブレットの調査に特化したモバイルフォレンジックツール。39000以上のデバイスをサポート。iOSデバイスやAndroidデバイスを始めとしたスマートフォンを対象にデータ抽出、アプリケーションデータ解析、位置情報解析、コミュニケーションの可視化、実用的なレポート(PDF/Excel 等)の出力までスマートフォンの調査に必要な機能を網羅している。また、クラウドサービスにも対応しており、主要なクラウドサービスからのデータ取得、解析が可能。デバイス単体の解析だけでなく、複数のデバイスから収集したデータを統合して解析し、共通の知り合いを洗い出す事も可能。また顔認識機能にも対応(Faces) 写真に写り込んだ人物の顔を識別して表示する。これらの機能は、犯罪捜査の効率を飛躍的に向上させる。 ※官公庁、法執行機関のお客様のみへの販売となる。
40	Paladin Linux / RECON (SUMURI)	統合ツール	SUMURAI https://sumuri.com/software/paladin/ https://sumuri.com/software/recon-triage/	UbuntsベースのLinuxライブディストリビューション。RECON LABは、Mac上で動作し、他のフォレンジックツールで見逃されたデータのリカバリを可能にする。Windows、Mac、Linux、iOS、アンドロイド、グーグルテイクアウト自動分析もできる。
41	PassWare Kit	解析支援	Passware Inc https://www.passware.com/	コンピュータ上のあらゆるパスワードや暗号化で保護されたファイルを検知し、それらを復号する、コンピュータ・フォレンジックにおける優れたパスワードリカバリソフトウェア。メモリ内からのパスワード抽出にも対応。
42	PC-3000	証跡保全	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/pc3000/ ACE Laboratory https://www.acelaboratory.com/	障害を抱えたHDDやSSD、NANDメモリ製品からデータを抽出できるフォレンジックツールで、異音を発するHDDでも各メーカー用に搭載された豊富な特殊コマンドで異常動作を制御することができる。また、SSDのファームウェア障害、破壊されたメモリ製品など使用不可の記憶媒体の調査や近年普及しているデータが自動で消失するSED仕様のストレージの証拠保全も対応できる。
43	Phone Breaker (Elcomsoft)	解析支援	ElcomSoft Co. Ltd https://www.elcomsoft.jp/eppb.html	iOS、Windows Phone、Windows10 Mobile、およびBlackBerry10を実行しているデバイスから情報を抽出し、ハードウェアアクセラレーションを使用してバックアップを復号化し、パスワードを取得するツール。
44	Plaso	調査・解析	GitHub - log2timeline/plaso https://github.com/log2timeline/plaso	plasoは、Pythonで実装されたスーパータイムラインを生成するツールのためのバックエンドエンジン。
45	RECON IMAGER	証跡保全	株式会社FRONTEO https://legal.fronteo.com/contact/ SUMURI https://sumuri.com/software/recon-imager/	外部ブートプログラムによる、Apple社製PC用証拠保全ツール。T2チップ搭載機・APFSファイルシステムストレージからの論理イメージ形式(Spareimage)でのデータ取得も可能で、ローカルタイムマシーンスナップショットも論理イメージに内包する形で取得可能。
46	RECON LAB	調査・解析	株式会社FRONTEO株式会社FRONTEO https://legal.fronteo.com/contact/ https://legal.fronteo.com/contact/ SUMURI https://sumuri.com/software/recon-lab/	Mac OS／iOS／Windows OS等の解析が可能な、フォレンジック用解析ソフトウェア。Apple Metadataの自動抽出機能、解析対象データのスーパータイムライン作成機能、アーティファクトの自動分類機能等、調査の効率化と高速が可能となる様々な機能を実装している。RECON LABには、あらゆるタイプのデータに対して統合されたビューアが含まれている。さらに、SQLiteビューアなどの高度なビューアを使用すると、RECON LAB内でSQLiteクエリを実行して高度な分析とレポートを作成できる。
47	Redline	統合ツール	FireEye, Inc. https://www.fireeye.jp/services/freeware/redline.html https://fireeye.market/apps/211364	ホスト調査を実施するための無償ツール。メモリやファイルを解析し、セキュリティ脅威の診断プロファイルを作成して、不正な活動の痕跡を特定する。
48	Rekall	調査・解析	GitHub - google/rekall https://github.com/google/rekall	分析しているのと同じプラットフォーム上で実行するように特別に設計された唯一のメモリ分析プラットフォームで、pythonで実装されたメモリフォレンジック用無償ツール。Windowsは、XPから10まで、Linuxは、カーネル2.6.24から最新まで、Mac OS Xは、10.7-10.12.xまで幅広くサポート。
49	Responder Pro	調査・解析	GoSecure,Inc. https://www.gosecure.net/	物理メモリの解析を行い、稼働中のプロセスの機能に応じて、独自のDDNAを用いたスコアリングを行い、従来のアンチウィルスソフトでは検知できなかったマルウェアを探し出すメモリ解析ツール。
50	SIFT Workstation (SANS)	統合ツール	SANS.org SANS Digital Forensics and Incident Response https://digital-forensics.sans.org/community/downloads	SANSの提供するubuntsベースのLinuxディストリビューションであるSIFTワークステーションは、様々な設定で詳細なフォレンジック検査を実行するように設計された無料のオープンソースインシデント対応とフォレンジックツールのグループ。インシデント対応で各種のフォレンジックツール群に連携させることができる。SIFTは、高度なインシデント対応機能と侵入に対する詳細なデジタルフォレンジック技術を、自由に利用でき、頻繁に更新される最先端のオープンソースツールを使用して実現できることを示している。
51	Simple SEIZURE TOOL for Forensic(SSTF) Simple SEIZURE TOOL for Android(SSTA)	証跡保全	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/sst/ https://www.kumanan-pcnet.co.jp/forensic/ssta/	SSTFは、国内特許(特許第6559984号)を取得した次世代のフォレンジックツールで、急速に増加しているマザーボードにメモリストレージが直接実装されているため分解困難なパソコンやタブレット端末等に対して、パソコンに接続し電源を入れるだけでパソコンや分解困難な電子端末、稼働中のサーバーデータまで幅広く簡単な操作で証拠保全ができるようになる。 SSTAは、スマートフォンを簡単に保全できるフォレンジックツールで、端末のスクリーンショット機能を用いて自動で確実に保全でき、SNSの証拠画像などからテキストを抽出することが可能になる。これにより課題となっているスマートフォンの殆どが内部データを保全できなくなり、証拠となる画面をカメラで手動撮影せざるを得ず時間と労力だけを浪費する現状を改善できる。
52	Splunk	解析支援	マクニカネットワークス株式会社 https://www.macnica.net/splunk/index.html/ Splunk Inc https://www.splunk.com/ja_jp/software/splunk-enterprise.html	様々なITシステムから生成されるデータの収集、検索、分析、可視化を行うデータ分析プラットフォームで、ログファイルやファイル時系列などのビッグデータを解析するためのツール。無償版もある。

Ｎｏ.	ツール名	区分	国内取扱店　（製造・供給元）	ツールの特徴や概要
53	Tsurugi (剣) Linux	統合ツール	つるぎLinuxチーム https://tsurugi-linux.org/	完全に無料のオープンソースプロジェクトによるツールで、DFIR調査、マルウェア分析とオープンソースのINTelligence活動をサポートするように設計された大幅にカスタマイズされたLinuxディストリビューション。このディストリビューションには、詳細なフォレンジックまたはインシデント対応調査を行うために必要なツールの最新バージョンと、カーネルレベルでのデバイス書き込みブロッキング、専用のComputer Vision分析セクション、OSINTプロファイルスイッチャーなどの機能が含まれている。
54	TZWorks (の各種パーサー)	調査･解析	TZWorks Limited Liability Company https://tzworks.net/about.html	有償ツール。レジストリ ハイブ、ジャーナリング ファイル、その他の重要なファイルなど、オペレーティング システムによってロックダウンされた分析を必要とするファイルは、クラスター レベルで生データを読み取ることによって調べることができる。このライブデータ収集は並列処理と組み合わされ、生データを読み取り可能/使用可能な結果にほぼリアルタイムで応答側に変換し、データトリアージを実行できるようにする。
55	UFED 4PC (Cellebrite)	統合ツール	サン電子株式会社 https://www.sun-denshi.co.jp/ Cellebrite https://www.cellebrite.com/en/platforms/	スマートフォンからデータ抽出、デコード、分析するためのツールで、UFED 4PCは高コストパフォーマンスの一気通貫システム。携帯端末やPDA等数多くのモバイル機器に対応、アプリケーションソフトとしてコンピュータ(ノートPC･タブレットPC含む)1台でデータの抽出から解析までを可能にした。Logical抽出が可能な標準モデルの「UFED 4PC LOGICAL」とPhysical Dump、File System Dumpまで兼ね備えたハイエンドモデルの「UFED 4PC ULTIMATE」がある。
56	UFED Mobilogy Touch	証跡保全	サン電子株式会社 https://www.sun-denshi.co.jp/df/mobilogy/ Cellebrite https://www.cellebrite.com/en/platforms/	持ち運び可能なUFED4PCのポータブル版スマートフォン用ツールで、世界中の携帯電話約4、000機種をサポート。携帯電話に保存された電話帳、写真、SMSメッセージ、ビデオ、オーディオファイル、着信音などのデータをほかの端末(多くの場合新たに購入した端末)に移行できる機能を持っている。また、データをUSBメモリーやSDカードなどのローカルメモリーにバックアップしたり、保存したデータを他の端末に書き込むこともでききる。
57	VFC5(Virtual Forensic Computing)	解析支援	株式会社くまなんピーシーネット https://www.kumanan-pcnet.co.jp/forensic/vfc/	VFCは、E01やDDなどの証拠イメージファイルを仮想起動できるフォレンジックツール。証拠イメージから実際のパソコンと同じ状態で起動させることができるため、使用していた環境をそのまま調査できるようになる。Windowsパソコンにおいてはログインパスワードをバイパスできるため、押収したパソコンを起動することなく利用者像を確認できる。またWEBやSNSのログイン状態確認やリストアポイントを用いたマルウェア調査などにも最適。
58	VizX (Ziuz)	調査･解析	ZIUZ https://www.ziuz.com/ja/	児童に対する性的虐待の調査等に役立ち、画像や映像からExif情報などの抽出ができる画像･動画解析用ツール。しきい値以上の変化があった動画のみ集中的に表示することで、監視カメラ等の重要なシーンを見逃さず、短時間でレビュー可能。服の模様やタトゥーから同じ模様を持つ被写体を見つけ出す。PhotoDNA技術をVizX2に導入して画像を照合する機能が追加された。
59	Volatility Framework	調査･解析	volatilityfoundation.org The Volatility Foundation https://www.volatilityfoundation.org	無償のメモリフォレンジックツールで、動いていたプロセス、ネットワーク情報などメモリ上にしか残らない情報が得られる。 AXIOMやEnCaseなど、Volatility のプラグインを持ち、同機能を使用するツールも存在する。
60	X-Ways Forensics	統合ツール	株式会社ディアィティ https://www.dit.co.jp/products/xways/forensics/index.html X-Ways AG https://www.x-ways.net/	ドイツ製のフォレンジック解析ツールで、ウイルス感染、不正アクセス等のセキュリティインシデントが発生した際に、その証拠となるデジタルデータの取得を容易にするために開発された。コンピュータフォレンジックに必要とされるすべての機能を搭載し、ドリルダウン方式を採用することにより、専門家でなくても容易に利用できるように設計されている。RVSの機能が使い易い。 ☆「日本語処理解析性能評価」受検製品2017.1.19:「X-Ways Forensics(Ver.19.0 SR-12)」