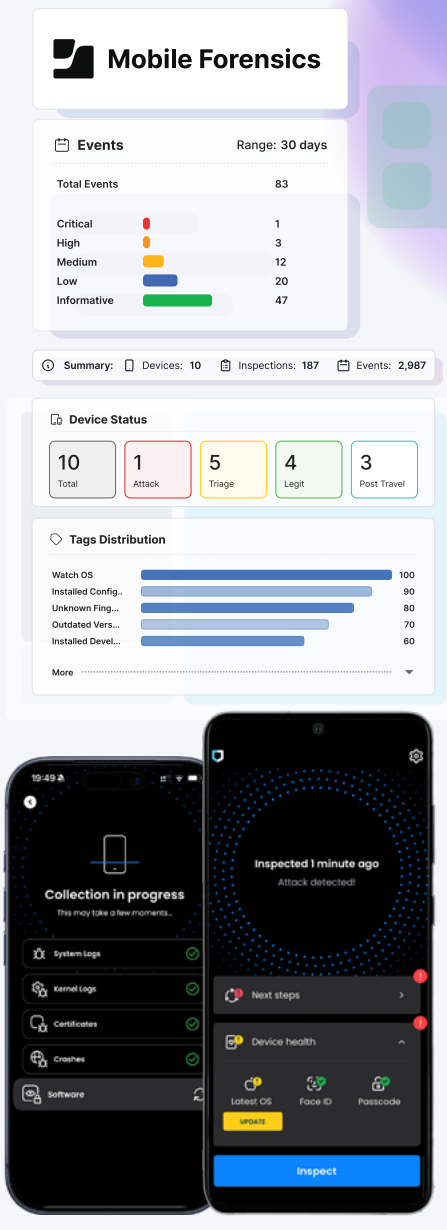


Jamf Mobile Forensics

高度なサイバー攻撃からモバイルデバイスを保護。

政府関係者、企業の経営層、政治家など、**狙われやすい重要人物が直面する脅威に対抗するには、実践的な防御戦略が欠かせません。**高度標的型攻撃（APT）、商用スパイウェア、国家主導のサイバー攻撃、そしてゼロクリック・エクスプロイト。こうした脅威に対抗するため、情報システム部門やセキュリティ担当者には、デバイスの整合性を継続的に分析し、侵害の痕跡（IOC）を特定することが求められています。しかも、ユーザの業務を妨げることなく、侵襲的なエージェントの導入や個人特定情報（PII）の露出も回避した上での実行が不可欠です。

Jamf Mobile Forensicsは、モバイル脅威対策に高度なレイヤーを追加し、従来のツールでは見逃すおそれのある脅威の検出と調査を支援します。



主なメリット

- 標的型攻撃やゼロデイ攻撃をネットワークへの侵入前に検出
- デバイスのルート化やジェイルブレイクをせずに、システム、クラッシュ、カーネル、アプリのログを詳細に分析
- フォレンジック分析を簡素化し、手作業の調査を削減
- 狙われやすいユーザのプライバシーを保護し、デバイスの信頼性を確保

モバイルエクスプロイトチェーン

モバイルエクスプロイトチェーンとは、以下のようにデバイスへの侵入から連鎖的に侵害を進行させる仕組みです。

悪意のある添付ファイル/WebKitエクスプロイト → 初期侵入 → コード実行（WebContentプロセスの侵害） → 権限昇格 → ステルス/防衛回避 → 侵入後活動（データ収集、マイク/カメラへのアクセスなど） → C2通信 → クリーンアップ/フォレンジック回避

脅威とエクスプロイトチェーンを分析できれば、セキュリティ部門が事態を把握し対応策を特定するうえで役立ちます。そのための可視性を提供するのが、Jamf Mobile Forensicsです。

モバイルフォレンジック分析に要する時間を数週間から数分に短縮できます。

リモートでのデジタルフォレンジックとインシデント対応

ダウンタイムを削減し、重要人物の生産性を維持

- 独自の挙動分析により、デバイスの異常な挙動、ゼロデイ攻撃、PegasusやPredatorなどのスパイウェアのIOCを検出
- デバイスレベルのテレメトリを調査して、リスクの拡大を阻止
- 即時の分析により、情報システム部門やセキュリティ担当者は必要な手順を把握し、高度な攻撃に速やかに対応可能

プロアクティブな脅威ハンティング

複雑なセキュリティデータを実用的なインテリジェンスに変換

- イベントのタイムライン、種類、重大度をインシデント別にまとめることで、調査業務を簡素化
- イベントのタイムラインを自動化し、デバイスがいつ、どのように侵害されたかを 直接調査
- ファイル、アプリ、プロセス、クラッシュログなどを分析して、未知のIOCを検出

人間主体のAI活用分析

AI分析がフォレンジック調査をアシスト

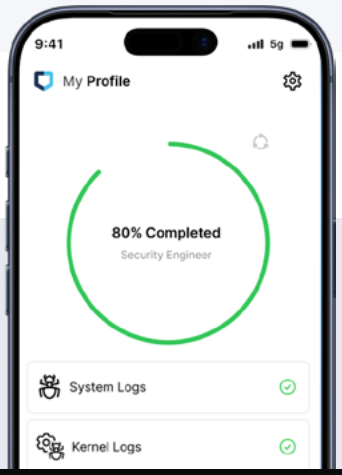
- デバイスのクラッシュや異常の分析に要する手作業の調査を削減
- インシデントの概要をまとめ、修復のための推奨対応策を提示
- AI分析はデフォルトで無効になっているため、組織はAIの使用を制御できる

*AI分析はクラウド専用の機能です。

設計段階からプライバシーを考慮したフォレンジック

プライバシーとデバイスの完全性に関するあらゆる懸念からユーザを保護

- 個人特定情報（PII）の取得はなし。分析で、パスワード、写真、動画、メッセージ、連絡先、通話履歴、ブラウザ履歴、2要素認証トークン、アプリデータへのアクセスは不要
- リモートDFIRアプリは、組織が設定した間隔でサイレントスキャンを実行し、デバイスのセキュリティ情報をユーザに提供



Jamf Mobile Forensicsは、**Jamf Threat Labs**がサポートしています。Jamf Threat Labsは、モバイルマルウェアやスパイウェアに関する調査を発表し、Jamf Mobile Forensicsエンジンの継続的な改善に取り組むセキュリティ研究者、アナリスト、エンジニアで構成されたチームです。

jamf

www.jamf.com/ja/

© 2026 Jamf, LLC. All rights reserved.

詳細については、Jamfの担当者までお問い合わせいただくか、
トライアルへお申し込みください。