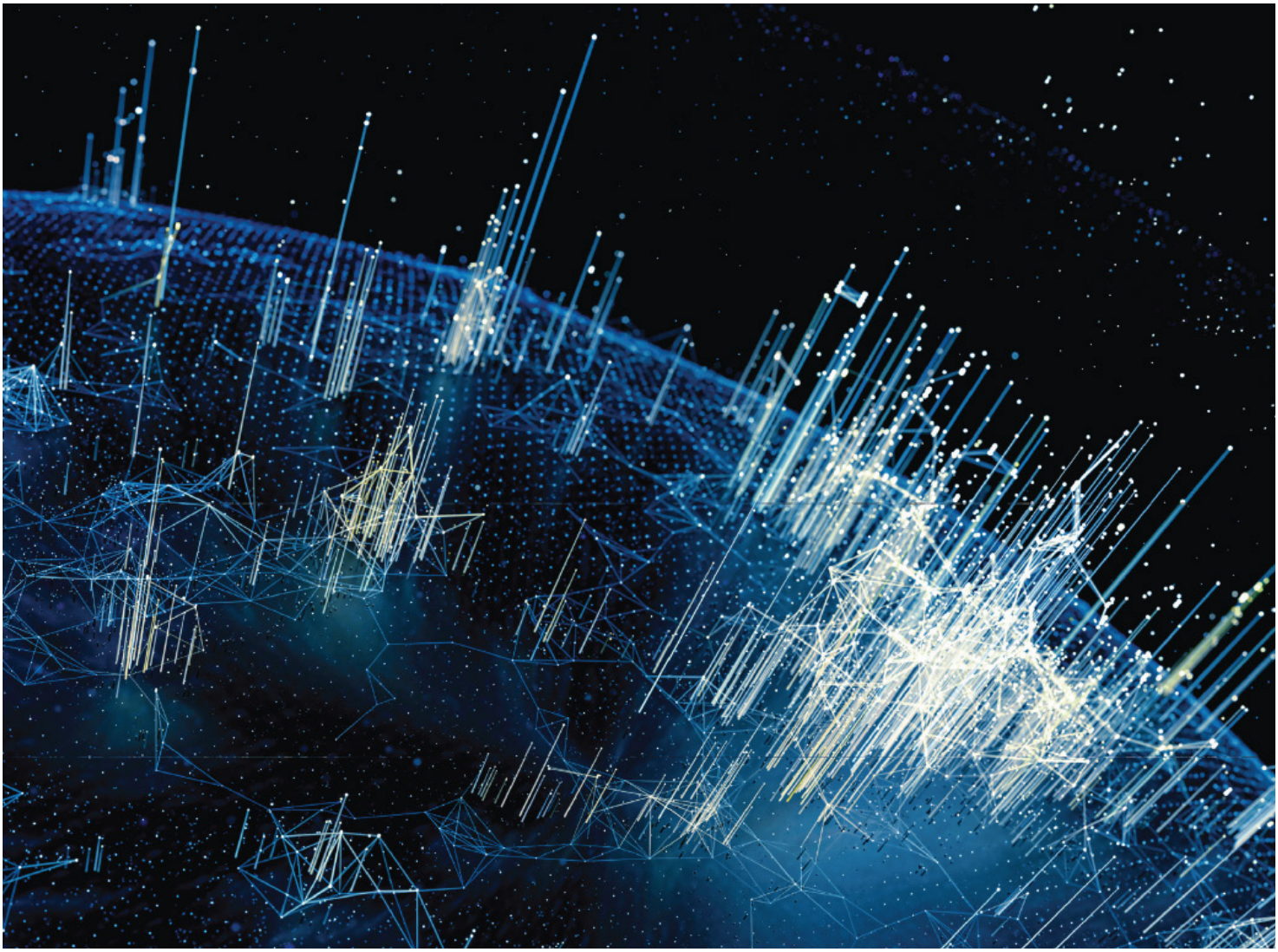
FTI TECHNOLOGY レポート

クラウドファーストにおけるデジタルフォレンジックの活用
～アジア太平洋地域の紛争とディスカバリー～



EXPERTS WITH IMPACT™

FTI CONSULTING

クラウドデータソースと職場で使用されるメッセージングアプリケーションの普及は、デジタルフォレンジック、調査、情報ガバナンスにおける新たなサイクルに拍車をかけている。クラウドベースのプラットフォームの全体的なユーザー数と、ビジネス目的で利用される様々なアプリケーションは、特にハイテク大手が人工知能で革新し、新しいコラボレーション・インターフェースをリリースするにつれて、増加の一途をたどるだろう。その結果、弁護士は、膨大かつ複雑で、急速に変化するデータの中で、フォレンジックの防御性、電子証拠の収集、データ保全、情報ガバナンスに認められた原則をどのように守るかに取り組むことになる。

本稿では、エマージング・データ・ソースとは何かという基本的な事項から、それらをめぐる具体的な法的・技術的課題、フォレンジック的に防御可能な方法でそれらを扱うためのソリューション、そして法務チームがこの新しいパラダイムに適応する際の指針となる最近の判例までを取り上げる。

新たなデータソースの定義

エマージング・データ・ソースとは、クラウドベースのプラットフォーム、コラボレーション・ツール、メッセージング・アプリケーションなど、ビジネスやコミュニケーションに利用されるものを指す。アジア太平洋地域では、Microsoft 365、Google Workspace、Box、Dropbox-、Slack、Zoom、WhatsApp、WeChat、DingTalk、Larkなどがよく知られている。ほとんどの人がこれらのツールに慣れ親しんでおり、日々の仕事や個人的なコミュニケーションで簡単に使っているが、バックエンドの複雑さや技術的なニュアンスの違いにより、紛争、証拠開示、規制遵守、情報ガバナンスの文脈では、いくつかの根強い課題が発生している。さらに、データや文書の量は常に増加しており、新たなデータソースの種類は、新たなプラットフォームを通じて常に拡大しており、また、各プラットフォームに存在する数多くのフォーマットや、それらに含まれるメタデータの種類にも違いがある。その結果、以下のような具体的な課題が浮上している：

アクセスと保全

新たなデータソースは、会社のシステム、従業員のコンピュータ、業務で使用される個人用デバイスに広がっている。従来の会社の文書や電子メールにアクセスし、保存することは日常的なプロセスだが、従業員の個人的な携帯電話上の暗号化されたWhatsAppデータに対してアクセスすることは容易ではない。特定のアプリケーションやデバイスにアクセスすることに関する多くの法的および実際的な課題はさておき、従来のフォレンジックツールやワークフローは、多くのクラウドソースに対して、フォレンジック的に問題のない完全なデータ収集を実行するプラグアンドプレイ機能を備えていない。

重複、ほぼ重複、変更可能なファイル

「動的な文書」（リンクされたコンテンツ、または最新の添付ファイルと呼ばれることもある）では、1つの文書の多数のバージョンが作成され、保存されるシステムが膨大に存在する。法務チームは、メッセージにリンクされた文書を収集し、レビューすることを任務としているため、その文書のどのバージョンが関連性があるのか、すべてのバージョンをレビューおよび/またはプロダクションする必要があるのか、バージョン間の変更が関連性があるのか、より広範なデータセットと照らし合わせて分析する必要があるのかを判断し、記録する必要がある。

メタデータ抽出

電子メールや文書などの従来のデータソースでは、メタデータ（電子メールの差出人、宛先、cc、送信日、件名、文書の作成日、最終アクセス日、最終更新日）は、フォレンジック・ツールやeディスカバリ・ツールを使って簡単に自動抽出できる。新しいデータソースの場合、メタデータの抽出は難しく、データ構造の深い理解とメタデータ情報を解析するスクリプトの技術が必要となる。

認証

クラウドベースのソースが関与している場合、情報を認証するための従来のプロセスが問題となる。例えば、データが多数の別々のリポジトリから1つのチャット・メッセージに接続された場合、元のソースはどのように決定され、検証されるのか。チームは、どのように文書化し、保存された記録から出入りするデータの流れを明確に説明できるのか。

クラウドエンドポイントへの認証はもう一つの課題だ。各クラウド・エンドポイントは様々な認証プロトコルを実装しており、認証と認可のための標準が登場した一方で、クラウド・プロバイダーは程度の差こそあれ、これらの様々なオプションを実装している。

対象者の識別

個人／対象者とその活動を適切に、あるいは効率的に特定するプロセスは、今や、特定の文書やチャット・チャンネルへのアクセス、許可、参加というレンズを通して評価されなければならない。一つの文書が、共有ワークスペースにおける複数の貢献者のコンテンツを含んでいる場合、その文書がカストディアンであると言えるのか。コミュニケーション・チャンネルに積極的には参加していないがメンバーというだけで、対象者のデータとしていいのか。一般的に、クラウドソースを扱う場合、対象者という概念にすら問題がある。通常、クラウドソースにはユーザーや共有ドライブのようなエンティティがある。対象者を特定しようとすると、ソースが不明瞭になり、最新のクラウドプラットフォームでは機能しないことが多く、伝統的なフォレンジック収集の哲学に反する。

データの保持と廃棄

フォレンジック調査のワークフローが新たなデータソース間で困難であるのと同じ理由で、情報ガバナンスもまた困難である。データの収集と保全が容易でない場合、自動化された持続可能な防御可能な保存・廃棄プロセスを実現することも難しい。しかし、このようなプロセスがなければ、データ量とデータリスクは増大し続け、データの肥大化と複雑化のサイクルが繰り返されることになる。

フォレンジックの防御性の実現

根本的に、伝統的な概念やアプローチは、もはや新しいデジタルの状況には適用できない。しかし、デジタルフォレンジックの原則である、証拠能力、真正性、再現性、証拠の継続性に忠実でありながら、新しいデータの技術的なニュアンスにより合致した新しいアプローチやツールに傾注することは可能である。例えば、適切なアプローチがあれば、法務チームはリンクされた文書内のメタデータに基づき、ある時点の情報を認証することができる。API（アプリケーション・プログラミング・インターフェース）は、フォレンジック調査やeディスカバリーにおける防御のアプローチを近代化するための重要な要素である。世界中の何百万人もの開発者と何十億人ものユーザーが、データを抽出・交換し、ソリューションを開発するための安全で一貫性のある信頼できる方法を提供するために、信頼できるテクノロジー企業が提供するAPIに依存している。これらは現代のデータ・エコシステムにおける基盤となるインフラだ。それらがどのように機能するかを理解し、それらを使用する際のプロトコルとAPIに関する詳細を文書化することで、防御のための強力な基盤を提供することができる。

特に、多くの新しいデータソースはエクスポート機能を持たないか、データエクスポートのフォーマットやスループットに大きな制限があるため、APIは調査においてデータを収集し、インジェストやレビューが可能なフォーマットに変換するために不可欠である。フォレンジックデータ収集において、APIは、例えば、ネイティブ・ファイルやその他のコンテンツを取得するため、特定のメタデータを取得するため、および／またはバージョン情報を取得するために使用される。

調査におけるデータやアーティファクトの完全性の維持

調査におけるフォレンジックの防御性の核心は、データや成果物の完全性を維持することにある。どのような調査においても、潜在的な証拠価値を維持するためには、収集された元のデータは変更されないままでなければならない。

クラウドベースのプラットフォームを扱う場合、従来のストレージメディアには存在しないような独自の成果物や補足的な成果物が含まれていることが多いため、この完全性は特に重要である。

クラウドプラットフォーム特有のアーティファクトは、ユーザーアクセスログ、ネットワークトラフィックデータ、アプリケーションメタデータから、共有アクセス環境の残骸、ドキュメントのバージョン、チャットメッセージングデータまで多岐にわたる。これらのアーティファクトは、ユーザーの行動、データの変更履歴、その他の重要な要素に関する洞察を提供することができるため、調査において極めて重要な要素である。多くのクラウドプラットフォームでは、アクティビティログやバージョン履歴が過去に遡って存在することが一般的である。これらのログを完全に保存するための迅速な対応がなければ、調査にとって重要なデータが永久に破壊されてしまう可能性がある。

結論

クラウドデータソース、コラボレーションツール、メッセージングアプリケーションの飛躍的な成長に象徴される今日のデジタル環境の絶え間なく変化する性質は、デジタルフォレンジックの分野やその他の隣接するワークストリームを根本的に再構築している。

デジタルフォレンジックを強化し、クラウドデータソースを横断することは、必須かつ複雑な課題である。新たなデータによってもたらされる課題に対処するには、データの性質を理解することと、フォレンジックの防御性の原則を尊重する新しいテクノロジーとアプローチの統合との間の共生関係が必要である。

SANDEEP JADAV
Senior Managing Director
+852 3768 4730
sandeep.jadav@fticonsulting.com

CHELSEA YE
Senior Director
+86 21 3892 6129
chelsea.ye@fticonsulting.com