2023 年 6 月 1 日

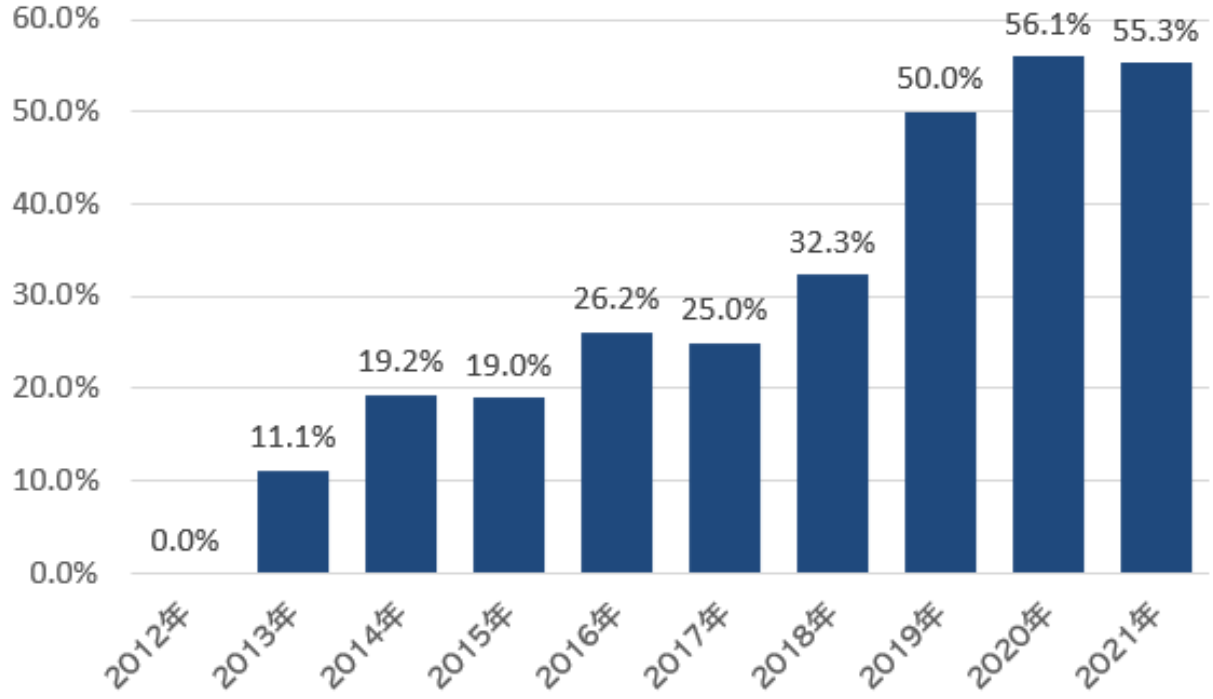
不正調査とデジタルフォレンジックの活用
～近年のトレンドと社内リソースで行う初動対応～

Epiq Systems 合同会社
早川浩佑
中島大輔

1．はじめに

弊社 Epiq（エピック）は E ディスカバリ対応の老舗企業としてサービスを展開しており、近年では数多くの不正調査をデジタルフォレンジックと E メール調査専用ツールを提供することによりサポートしております。そこで、過去 10 年間（2012 年 1 月～2021 年 12 月）に公表された第三者委員会や外部調査委員会による調査報告書を分析した結果、対象事案の内容は、「不正会計・横領・不実開示」が全体の 52%で最も多く、次いで「偽装・品質偽装・不当表示」が全体の 14%を占めることがわかりました。また、デジタルフォレンジックの採用率に注目して分析した結果、10 年間の報告書のうち 30.7%においてデジタルフォレンジック調査が言及されていました。特に 2019 年から 2021 年にかけては、半数以上の報告書でフォレンジック調査が言及されている傾向が見られました。

【2012～2021 年公開の第三者委員会調査報告書等からのデジタルフォレンジック記載の割合】



このような背景を踏まえ、本稿ではデジタルフォレンジックの活用や不正調査時のワークフロー、初動対応などについて解説します。

２．電子データを対象とした不正調査の初動（初期調査とデータ保全）

不正調査の始まりは、その端緒の発覚です。端緒を掴んだ後の初期調査とその後の調査方針決定を経て、本格的な詳細調査が始まります。初期調査では、隠滅されるおそれのある証拠を速やかに保全する必要があります。不正・不祥事についての調査が始まったことを知れば、関係者は自らに不利な証拠の隠滅や有利な証拠の作出等の行為、具体的には文書、PC やスマートフォンに保存したデータ等の破棄や、関係者の口裏合わせ等を行う恐れがあります。したがって、文書、PC やスマートフォンの確保、口裏合わせに先んじた証言の録取等により、証拠保全を実施します。初期調査の段階で、デジタルフォレンジックの専門会社に証拠保全や一部の分析を依頼することもあります。

しかし、多くの場合、初期調査段階では外部の専門会社を起用するための予算を確保することが難しい場合もあるかと思いますので、社内リソースにてデータ保全を行えるワークフローを持つことが有事での理想的な初動対応のひとつと言えます。

３．社内にある IT インフラを活用したデータ保全

近年では、クラウドサービスにオプションとして証拠保全や初期調査に必要な分析機能が提供されていますが、不正調査に関わる法務部門やコンプライアンス部門の担当者と IT 担当者間での知識とコミュニケーションのギャップがあると思われ、社内インフラ機能が十分に活用出来ていない状況がまだ多いと思われます。例えば、クラウド型のファイル共有サービスである「Box」を利用している場合は、「Box Governance」というオプション、クラウド型のオフィス向け総合サービス「Microsoft 365（旧 Office 365）」では「電子情報開示（eDiscovery）」というデータを消去から守る機能があります。特に Microsoft365 では企業向けパッケージプランを選択している場合が多く、前出の「電子情報開示（eDiscovery）」という機能は E3 または E5 と呼ばれるライセンスに標準で組み込まれており、Microsoft365 内に保存されているデータであれば比較的簡単にデータの保全を行うことが可能です。Microsoft365 ユーザー企業であれば、この機能が実装されている可能性が高いので、IT 担当者と確認することで、社内リソースで行えるデータ保全ワークフローを確立出来ると思います。特に、不正調査では E メールやチャットなどのコミュニケーションデータを中心に調査することが多いために、これらのデータ保全機能は不正調査において有効となると考えます。
実際に不正調査のサポートを弊社が行う際でも、E メールデータやチャットデータに関しては

Microsoft365 ユーザー企業であれば、IT 担当者の方に依頼してデータの保全からエクスポートを行うことが多くなっています。

４．不正調査における削除データ復元

特に意図した不正に関する情報は、通常、意図的に隠蔽されています。紙であれば破棄、データであれば削除されていると考えるのが自然です。そのため、削除された電子文書や業務ファイル、電子メール、写真ファイル、動画データ、スマートフォンの内部データなどを復元し、隠蔽された情報を調査することは、デジタルフォレンジックを導入する大きなメリットであるといえます。

デジタルフォレンジック専門家は、その状況に応じて適切な復元技術や復元ツールを駆使し、削除されたデータの復元を試みます。また、復元後の電子メールに代表される膨大なデジタルデータを限られた期間で効率的に分析するためには、要件に応じたデータ加工が必要となる場合があります。複数人の復元電子メールに対して高度な検索・分析を行う必要がある場合、柔軟かつ高速に、しかも一元的な検索・分析ができるように、電子メールデータを加工し、分析用 DB に格納するのもデジタルフォレンジック専門家の仕事です。

５．電子メール分析・レビュー技術と事例

不正調査において、保全された大量データの中から証拠となり得る情報を見つけ出すためには、保全データの中にあるさまざまな情報を有効かつ効率的に検索・分析する必要があります。公開されている第三者委員会・外部調査委員会の報告書によると、レビュー（データ閲覧）対象となるファイル数が数万から数十万件となる調査もあり、限られた時間内でレビューを終わらせるためには、多くの人数を投入するか、IT（情報技術）を駆使するか、または両方を併用することが求められます。

IT を駆使する場合、例えば、大量のデータを特定キーワードや特定期間で絞り込んだり、ファイルの最終更新日時や電子メールの送受信日時等で時系列に分析し、電子メールの送受信アドレス・頻度から交友関係を洗い出したり、処理目的に応じた柔軟かつ迅速な検索・分析を行う必要があります。

特に、電子メールやチャットなどのデジタルデータとして保存されたコミュニケーションの内容を精査する場合、さまざまな技術とノウハウを駆使して、有効かつ効率的に検索・分析を実施します。

■検索・分析前のデータ加工技術
保全されたデジタルデータは、調査のためにさまざまな加工を施す必要があります。この加工において技術的に要求されるのは、高速な処理スピードと、調査委員会の要求に応じてテラバイトクラスの大規模データまで処理できる拡張性です。

また、検索においては、さまざまな条件を付けてデジタルデータをフィルターにかけるための加工も必要です。加工により、多種多様なファイル形式のデータを横断的に検索でき、データファイルの種類・サイズ・範囲・対象とする人や時期などを複数条件づけることも可能で、目的のドキュメントを素早く探すことができます。

調査には、事案によっては複数多言語対応が必要で、これもデータ加工技術を使うことで、英語、フランス語、中国語、日本語等々のドキュメントに対して、メタデータに基づく分類、検索、フィルタリングなど全ての機能が適応します。外国語文書を自動で検出することで、レビュー前に文書の仕分けをしておくことも効率的でしょう。

■柔軟かつ迅速な検索技術
不正調査における検索は、柔軟で迅速である必要があります。検索するキーワードと完全に一致していなくても、表記の異なりや同義語も含め、柔軟に解釈して検索する「ファジー検索」や、語形が変化する単語を検索できる「ステミング検索」など、一般には聞きなれない検索技術が有益な場合があります。

検索する文字列を「正規表現」で扱うことができる技術が迅速な検索に有効な場合もあります。検索する「キーワード」の単語・文節を自由に設定する技術により、検索時間を大幅に短縮できる可能性が高まります。

また、迅速性だけでなく、漏れのない日本語検索のための技術もあります。N-Gram 方式（Unigram）を採用することで、日本語を含むアジア言語は「１文字単位」で検索可能となり、漏れを防ぐのに有効です。

■高度な電子メール分析技術
膨大な電子メールのデータの中から、目的に合致したデータを効率的に探すために、数多くの高度な分析技術があります。代表的なものを２つご紹介します。

ひとつ目は、複数人の間で複雑に絡み合い、証拠価値が高いと言われる電子メールやチャットなどのスレッド群を分析する技術です。スレッドを同じファミリーとして扱うことで、更新日時の新しいものの内容を精査し、タグ付けすることができます。これにより、管理が難しいと言われる電子メールやそのスレッドを矛盾なく分類することができます。

ふたつ目は、関係分析という高度な電子メール分析技術です。この技術では、メールの送受信者のあらゆるやりとりのタイムラインを、視覚的に認識できるコミュニケーションマップとして表示することができます。この技術を使うと、人物や組織の関係性を可視化できるのみならず、選択した人物や組織間の電子メール文書群へジャンプしてレビューすることも可能となります。

■架空取引による不正会計事案での事例

東証一部上場企業の営業の現場で、営業成績が足りない場合に売り上げを先行計上したり、急きょ発生した工事費用を協力業者に支払わせる一方、その業者に工事を架空発注してお金を戻したりしていたという事案があります。この不適切取引の調査報告書から、電子メール分析・レビューを行った際の規模的な事例を読み取ることができます。

この不適切な取引行為の調査では、調査対象とした 27 名の電子メールの総数が約 210 万件あり、キーワードの使用と期間指定を行うことで約 5 万件程度まで絞りこみを行い、実際に人の目で内容を確認するドキュメントレビューを行ったとされています。これらの電子メールを確認した結果、約 900 件が本調査に関連するメールであると特定され、そのうち約 100 件の電子メールが不正行為に関連する可能性があるデータとして発見されたと報告されています。

なお、この報告書では、約 210 万件の電子メールから 5 万件まで絞り込んだ 84 種類の「検索キーワード」も調査報告書では一部公開されています。

■人工知能技術の利用
多人数や長期間にわたるコミュニケーションの内容を精査する必要がある場合、ドキュメントレビュー対象となるファイル数が数万から数十万件となる場合があります。通常、不正調査に与えられる時間はそれほど多くなく、限られた時間内で大量のドキュメントレビューを終わらせるためには、多くの人数を投入しての作業となることもあります。

第三者委員会／外部調査報告書の中には、こうした大量のドキュメントレビューを効率的に終わらせるための技術を利用したことが記載されたものがあります。具体的には、AI（人工知能）エンジン、機械学習やプレディクティブコーディング（コーディング予測機能）と呼ばれる先端技術・機能を利用したと記載された複数の報告書があります。

６．チャットの分析・レビュー技術

新型コロナウイルス感染症の拡大リスクに対応するため、多くの企業・組織が在宅勤務によるテレワークを余儀なくされました。株式会社パーソル総合研究所が 2022 年 8 月に公開した『新型コロナウイルス感染症の第 7 波感染拡大下におけるテレワークの実態』調査では、在宅勤務を併用する新しい働き方に対応するための新しい施策の導入実態が明らかになりました。

これによると、最も多くの企業・組織で採用された施策は、Zoom などの「遠隔会議システムの導入・利用促進」でした。次いで多いのが「ビジネスチャットツールの導入・利用促進」となっています。コロナ以前には「Zoom」や「Teams」の存在すら知らない人が多数派でしたが、今や日常的に利用するツールとなりました。

■不正調査とチャット
社内コミュニケーションにビジネスチャットを導入し、使用する企業や組織が増えれば、不正調査でのコミュニケーションの精査を行う上で、電子メールデータと共にチャットで行われているコミュニケーションも対象となるのは必然です。このことは、既に公開されている第三者委員会の外部調査報告書からも知ることができます。
多くの人が利用しているスマートフォンのチャットアプリである LINE の様に、メッセージのやり取りはチャットで行われることが主流となってきています。　現実の不正調査で対象となるのは、主に会社資産を使用したビジネスチャットです。第三者委員会などの調査報告書を調べると、調査対象となるチャットデータとして名前があがる頻度が多いのは「Microsoft Teams」です。

■チャットの分析・レビューの留意点
不正調査を行うという観点で、チャットで行われたコミュニケーションを精査する留意点とし

ては、①データの取得方法と、②内容を確認するレビューの 2 点があげられます。電子メールでは、メール 1 通が独立したファイルとして保存されますが、チャットの場合はそうではありません。
不正調査で対象となる頻度の多い「Microsoft Teams」チャットを例に取ると、調査のためにチャットデータのエクスポート（外部への書出し）を行った場合、それぞれの会話の吹き出しが 1 通のファイルとなって書き出されてしまいます。分析・レビューを実施するためには、閲覧しやすい形式に整理する必要があります。また、電子メールに添付ファイルがある場合、このファイルを容易に取得ができますが、チャットの場合には、メッセージ本文とは別の場所に添付ファイル保存されている場合があり、データ取得時には、このあたりの考慮が必須と考えて良いでしょう。

■電子メール分析・レビューとの相違点
電子メールの場合、そのメールの送信日、送信者、受信者、件名、メール本文と各項目が独立したフィールドとして記録されます。メール本文以外の、このメールを表す属性や関連する情報のことを「メタ情報」と呼びます。不正調査のための分析をする際、「メタ情報」を用いると、送信日時や受信者を指定したフィルタリングや絞り込みが比較的容易に実施できます。
一方、チャットは日常のコミュニケーションを、「ひとつの掲示板」に会話として書き込んでいくイメージです。通常の会話を電子的に再現する手段としては非常に便利なツールですが、そのままの状態では、調査のためのフィルタリングや絞り込みには適していません。電子メールとは異なり、チャットで交わされた会話の「メタ情報」が独立したフィールドとなっていない場合があるため、絞り込みや、閲覧しやすい環境を実現するための考慮が必要になります。

デジタルフォレンジックの技術を用いてチャットの内容の精査を行う場合、チャットで行われたコミュニケーションをエクセルなどのフォーマットに変換を行うことでレビューを行う方法や、チャットをオリジナルに近い形に成形を行うことで効率的な作業を行える環境を整えるという方法などがあります。

７．終わりに

不正調査に関する事実確認や、対象者へのインタビュー内容を充実させるため電子データの精査を行うことは引き続きトレンドとなると思われます。弊社を含め、専門業者は法律事務所の弁護士などの作業効率を高めるサポートをテクノロジを駆使し行っておりますが、企業側の努力としては、隠匿される可能性あるデータを最小限に抑えることとなると考えます。不正調査には、刑事事件や規制当局対応につながる事案もあるために、事案によっては出来る限り早い

段階でデータを消去されることから守るデータ保全を社内リソースで行える体制とワークフロー構築を検討されることをお勧めします。対応する機会は少ないかと思いますが、M365 などのクラウドベースのシステムを導入している企業に関しては、不正調査に有用なデータ保全などの機能が新たに投資を行うことなく実施できる可能性がありますので、少しでも有益な情報となればと思い情報をお伝えさせて頂きました。

以上

＜筆者略歴＞

早川浩佑（はやかわ　こうすけ）
Epiq Systems 合同会社　シニアディレクター　公認不正検査士
日本企業やグローバル企業の訴訟案件・調査案件に関するソリューション提案やマネジメント全般、及び当事者である企業及び法律事務所と連携を取りながら、ワークフローの最適化を図る。ニーズにマッチしたサポートに定評があり、クライアントの訴訟・調査戦略の実現に尽力する。
Email：khayakawa@epiqglobal.com

中島大輔（なかじま　だいすけ）
Epiq Systems 合同会社　ディレクター　公認不正検査士
15 年以上日本企業を中心に国際訴訟や規制当局対応の E ディスカバリの効率化設計を最新のテクノロジを使用したベストプラクティスにて、正当性を保ったワークフローを提案。また、不正調査では公認不正検査士としてクライアントのニーズに合わせた調査手法のアドバイスを提供。
Email：daisuke.nakajima@epiqglobal.com

掲載日：2023 年 6 月 15 日