JPR&C Research&Consulting
JPR&C アナリスト・レポート
JPR&C Analyst Report
Vol. 20

2025 年 7 月 18 日

デジタル・フォレンジック
――インシデント発生を前提とした企業のリスク管理

JPR&C 調査部　尾崎　和彦

はじめに

企業活動がサイバー空間へ拡大し、あらゆる情報がデジタルデータとして生成・蓄積される現代において、企業は複雑かつ巧妙化するリスクに直面しています。サイバー攻撃による機密情報の窃取、役職員による情報の持ち出し、流用といった内部不正など、デジタルデータを巡るインシデントは増加傾向にあります。これらの事案は、直接的な財務損失に加え、社会的信用の低下を通じて、事業継続に影響を及ぼす経営上の重要リスクといえます。

このような状況は、インシデントの発生を完全に防止することが困難であり、その発生を前提とした対策が求められることを示唆しています。企業が持続的に成長するためには、インシデント発生時に迅速かつ的確に対応し、被害を最小化するとともに、原因を究明して再発防止策を講じる一連のプロセス、すなわちインシデントレスポンス体制の構築が不可欠です。このインシデントレスポンスにおいて中核的な役割を担う科学的調査手法が「デジタル・フォレンジック」です。

デジタル・フォレンジック（コンピューター・フォレンジックとも呼ばれます）は、PC やサーバー等のデジタル機器に残された電子的記録を収集・保全し、解析・分析を通じてインシデントの全容を解明する技術・手法の総称です。そのプロセスには、法廷証拠としての活用にも堪えうる厳格性と客観性が要求されます。

本稿では、デジタル・フォレンジックに焦点を当て、その具体的なプロセスと企業活動における重要性を解説します。併せて、導入における課題や、今後の企業に求められるデジタルリスク管理体制のあり方について考察します。

デジタル・フォレンジックの戦略的重要性とプロセス

デジタル・フォレンジック調査は、主に「保全」「解析」「報告」という 3 つのプロセスで実行されます。このプロセスを遵守することは、得られた情報の証拠能力を担保する上で重

要です。

1. 証拠保全

インシデント発生時、最初に着手すべきは、対象機器の現状を維持することです。デジタルデータは容易に改変・消去され、証拠価値が損なわれる可能性があるため、専門家は専用のツールを用いて記録媒体の完全な複製（イメージング）を作成します。その際、原本のデータが変更されていないことを証明するために「ハッシュ値」を算出し、証拠の「同一性」と「完全性」を確保します。この初期対応の成否は、その後の調査結果に大きく影響します。

2. 解析・分析（Analysis）

保全したデータを基に、専門のアナリストがインシデントの痕跡を詳細に調査します。主な分析手法は以下の通りです。

- タイムライン分析: ファイルの作成・更新日時等の情報を時系列で整理し、不正行為の全体像を可視化します。
- 削除済みデータの復元: 意図的に削除されたデータを復元し、隠蔽工作の有無やその内容を調査します。
- マルウェアの特定・解析: 不正プログラムを特定・解析し、攻撃者の目的や情報漏洩の範囲を特定します。
- ログ解析: 各種ログを横断的に分析し、不正アクセスの侵入経路や内部での挙動を追跡します。

これらのプロセスは、主に以下の場面で企業のリスク管理に寄与します。

- 内部不正の解明: 役職員による不正行為の事実関係を、客観的証拠に基づき解明します。
- サイバー攻撃の被害調査: 攻撃経路、被害範囲、情報漏洩の有無を特定し、迅速な復旧と再発防止策の策定に繋げます。
- 法的紛争への備え: 訴訟において、自社の正当性を主張するための電子的証拠を確保・提出します。

企業インテリジェンスとデジタル・フォレンジックの相関性

しかしながら、デジタル・フォレンジックの役割は、比喩的にいえば、インシデントの「化石」を発掘する考古学に留まりません。デジタル・フォレンジックで得られる知見は、次の攻撃を予見し、先手を打つための価値ある「戦略情報」であり、守りのコストを攻めの投資に変える起点といえます。インシデントの教訓を未来の企業防衛のための体制構築へと昇華させることによって、総合的な企業価値向上に資するプロセスへと進化させることにこ

そ、企業の本質的課題があるといえます。

その意味で、デジタル・フォレンジックは、企業において、その事業を取り巻く情報を体系的に収集・分析し、リスクや機会の兆候を先読みして、戦略的な意思決定に資する活動、すなわち企業インテリジェンスの一環と捉えることが重要となります。

デジタル・フォレンジックにおけるインテリジェンス・サイクルについて、たとえば以下のような事例で考えてみましょう。

1. 調査（デジタル・フォレンジック）： ある不正調査の結果、「営業部の A 氏が、個人契約のクラウドストレージを経由して競合他社へ顧客リストを漏洩させた」という手口が判明したとします。
2. 学習（インテリジェンスへ反映）： この「手口」という生きた情報を、インテリジェンス・システムにフィードバックします。その結果、「個人用クラウドへの業務ファイルのアップロード」という行動パターンのリスクレベルを引き上げ、監視を強化するルールが追加されました。
3. 検知と抑止（インテリジェンスの制度化）： 後日、別の従業員 B 氏が同様の行動（個人用クラウドへの大量のファイルアップロード）を行った際、システムが即座に異常を検知し、セキュリティ担当者にアラートが送信されました。
4. 介入（類似インシデントへの事前対応）： アラートを受けた担当者は、不正が実行に移される前に B 氏へのヒアリング等の初動対応をとることが可能となりました。

このように、フォレンジックで得たインシデントという「点」の情報を、インテリジェンスの制度化を通じて「線」や「面」の防御策へと進化させるプロセスが、企業のレジリエンス向上につながります。

社内インテリジェンス機能としてのフォレンジック体制

デジタル・フォレンジック能力を有効に活用するには、社内インテリジェンス機能として位置づけることが重要です。特に、法務・コンプライアンス部門や情報システム部門が担う役割は大きいと言えます。

これらの部門は、インシデント発生時に、被害拡大防止、証拠保全、外部専門家との連携、経営層への報告、関係各所への説明など多岐にわたる業務を担います。平時からフォレンジックに関する基礎知識を習得し、インシデントを想定した訓練を定期的に実施することで、有事の際に的確な判断を下せる体制を構築する必要があります。外部専門家への依頼基準や報告手順などを明確化したプレイブックの整備は、初動対応の誤りを防ぐ上で有効です。

すべての調査を内製化することは困難であっても、インシデントの初期評価（トリアージ）

を行い、外部専門家と的確に連携できる専門知識を有する担当者を社内に配置することは、コストの最適化と対応の迅速化に寄与します。この担当者こそが、企業のインテリジェンス機能の中核となり得ます。

むすびにかえて

デジタルデータが企業活動の根幹をなす現代において、デジタル・フォレンジックは、すべての企業にとって不可欠なリスク管理基盤として位置づけられます。インシデント発生を前提とし、その健全性を維持し、有事の際には原因を究明して適切な対策を講じる能力が求められています。一方で、フォレンジック調査は自社の役職員のプライバシーに関わる可能性があるため、その実施には厳格な規律と高い倫理観が要求されます。

企業を取り巻くリスク環境が複雑化する中、自社のリソースのみで最先端の脅威に対応し続けることは困難です。そのため、最新の脅威情報や高度な分析能力を持つ専門のインテリジェンスファームを平時からパートナーとして活用することは、極めて有効な選択肢となります。

こうした外部の専門家らと連携しつつ、社内のインシデントの兆候を早期に察知し、調査で得た知見を未来の防御へと繋げる「企業インテリジェンス」としてのデジタル・フォレンジック体制を確立すること。この二つの取り組みを内外で推進することが、不確実性の高い事業環境において企業価値を維持・向上させるための重要な指針となります。

《著者略歴》
尾崎 和彦（おざき かずひこ） 大学卒業後、民間信用調査会社および専門金融機関にて専門調査員として勤務し、延べ 1000 社以上の企業の信用調査に従事。2022 年 10 月当社にシニア・アナリストとして参画。各種の業界慣習・商流に通暁し、また財務・人事組織・開発に係る企業の非財務リスク・アセスメントを得意とする。