「法」と「IT技術」

～環境変化に伴う次世代の危機管理～

デジタルフォレンジックの現場を知り尽くす佐々木氏と、危機管理対応の
スペシャリストである尾崎弁護士が、IT技術の進化によりもたらされた新たな企業不正、
企業犯罪の現状を語ります。企業に求められる対応策は何か。
デジタル環境における法的・技術的な課題を探ります。

写真／弘田充　構成・制作／レクシスネクシス・ジャパン企画制作部

【対談】

AOSテクノロジーズ株式会社 代表取締役社長

佐々木隆仁

Takamasa Sasaki

1964年、東京都生まれ。89年、早稲田大学理工学部卒業。大手コンピューターメーカーに入社し、OSの開発に従事した後、1995年に独立。AOSテクノロジーズ社を立ち上げ、リーガルテクノロジーを中心とした事業を推進。2000年よりデータ復元ソフト「ファイナルデータ」を発売し、01年日経サービス優秀賞受賞。01年データ復旧サービス「Data119.jp」を開始する。02年米国支社を設立し、法務IT推進会を発足。03年よりデジタルフォレンジック事業に注力。10年、11年、12年にBCN AWARDシステムメンテナンス部門最優秀賞受賞。著書に『2000年対応あなたのパソコンが誤動作しないための本』（かんき出版）、『デジタルデータは消えない』（幻冬舎）などがある。

西村あさひ法律事務所パートナー弁護士

尾崎恒康

Tsuneyasu Ozaki

1996年、検事任官。東京地検特捜部検事、法務省大臣官房行政訟務課付検事、総務省行政管理局課長補佐等を経て、2005年、弁護士登録。2008年より西村あさひ法律事務所パートナー。危機管理、コンプライアンス、訴訟紛争等を主に担当。粉飾決算等の不適正会計、インサイダー取引、独占禁止法違反、製品・食品・施設事故、情報漏洩、環境規制違反などの危機管理案件を多く手掛ける。

役員や従業員による不正行為の増加

尾崎　ここ数年、役員や従業員のインサイダー取引に関わる案件についての相談が目立ちます。これは証券取引等監視委員会による積極的な摘発が背景にあるわけですが、その大きな一因として、証券取引等監視委員会や証券取引所、あるいは証券会社等の間で、IT技術に基づく情報共有体制の整備が進んできたということが挙げられるのではないかと思います。

佐々木　これまで見逃されていたような不正行為が、きちんとすくいあげられているということですね。

尾崎　もちろん、2005年の証券取引法（当時）改正で導入された課徴金制度のおかげで、刑事罰しか用意されていなかった当時と比べ、当局が摘発しやすくなったという事情がありますが、それに、IT技術の進化による摘発環境の整備も加わり、摘発件数が増えているという面もあると思います。

佐々木　尾崎さんのおっしゃった動きは我々も肌で感じています。昨年12月に証券取引等監視委員会がデータ収集専用ツール「ヌイックス」を導入したのですが、これは我々が金融庁に提供させていただいたものです。

尾崎　どういうソフトなんですか？

佐々木　サーバーというものは容量が巨大で、すべてのデータを精査するには時間と労力が必要となります。ヌイックスは、前もって調査に必要なデータの種類や作成・変更日時を指定しておくことで、重要なデータのみを収集することができるというもので、アメリカの証券取引委員会では多くの実績を残しています。

情報共有の体制整備とデジタルデータの解析

尾崎　佐々木さんのお仕事でも、インサイダー取引に関わる案件は増えていますか。

佐々木　はい。我々のところに持ち込まれる案件も増えてきています。インサイダー取引の場合、取引に関与しているのが誰なのかを特定することが何よりも重要ですが、そのための決め手として、携帯電話やスマートフォンの解析が活用されています。いわゆるデジタルフォレンジックと呼ばれるアプローチです。

以前であれば、関与を決定づける証拠がなく、白黒はっきりしなかったものが、いまはデジタル機器を調査することで、正確に特定することができるようになりました。通話履歴やメールで送受信されたデータ、あるいは撮影された画像データを復元・解析することで、その「証拠」が導き出されるのですから。

尾崎　しかし、いまおっしゃったようなデータは、ユーザーが簡単に削除できるのではないかと思っている人が多いと思いますよ。

佐々木　そう思われがちなのですが、実は削除することは難しいのです。デバイス上では削除されたと見えるデータでも、内部にはその痕跡がきちんと保存されています。我々が関わった案件でも過去3年分の通話履歴を復元し、いつ誰と会話したのかを、時系列に沿って精査した事例もあります。スマートフォンになると、GPS機能が搭載されていますから、通話履歴に加え、位置情報の特定も可能です。

尾崎　当局の調査・捜査も、情報共有体制の整備とデータ解析技術の進歩という両者の相乗効果で、摘発件数を増やしている、つまり、情報共有体制の整備によって当局が事件性の高い事例の端緒を迅速に把握することが可能となったことに加え、確度の高いデータ解析技術が立件時の証拠収集に大きな効力を発揮しているといえるかもしれません。

佐々木　最近、社員が会社のトイレにこもって、スマートフォンで株の売買をしていたという事例もありました。トイレの中でトレードをするということで「トイレーダー」と呼ばれているようですが（笑）、これも場合によっては、インサイダー取引につながる危険性があるでしょう。それ以前に就業規則に抵触する可能性も高い。

尾崎　IT環境の進化が、むしろ不正行為を助長している例という見方もできますね。他方、仮にその事例で、インサイダー取引や就業規則違反の疑いありとして社内調査を行い、スマートフォンの任意提出やデータ解析にまでこぎ着けることができたとすれば、以前であれば、株の売買をしていたことを推認させる「状況」しか指摘できなかった事例において、履歴の調査等を行うことで、確たる「事実」として裏付けを取ることができるという点でIT環境の進化が役立つということもいえます。

佐々木　我々が担当した案件では、自分のアカウントではなく、他人のアカウントを使って取引をしていたものもありました。デジタルデバイスで便利になった反面、簡単に違法行為に手を染めてしまう人間も出てきました。モラルハザードが生じているという意味では、IT環境の進化は諸刃の剣ともいえそうです。

事後対策ではなく、事前対策を重視すべき

尾崎　情報漏洩に関する事例も増えました。過失もありますし、意図的なケースもあります。情報の内容についても、個人情報もあれば、企業の機密事項もある。千差万別です。

佐々木　意図的な情報漏洩にはどんな事例がありますか。

尾崎　例えば、X社に勤務していた開発担当者Aが、海外のY社に転職するにあたり、X社での研究内容をY社への「手土産」として持ち出すという事例などが典型例でしょう。Y社が競合他社の企業秘密を入手するために、Aに対し、高額の報酬を条件に機密事項を持ち出させようと働きかけることなどが契機となります。

佐々木　海外の企業だと、誰がキーパーソンかを徹底的に調べ上げて、意図的に接近するパターンが多いですよね。転職云々は、いわば口実にすぎなくて、最初から機密事項を得ることが目的で……。

尾崎　そういうことを仕掛けられてしまうと、企業としてはなかなか防ぐのが難しい。機密情報を持ち出すAも当該企業の情報管理体制の穴をあえて突いてくるわけで、事前対策のアドバイスをするのが難し

い事例ですね。そもそも、我々のもとに相談にいらっしゃるのは、「事前」ではなく「事後」のことが多いわけですが。

佐々木　残念なことに、我々のところにいらっしゃる方々も、ほぼ同じ状況です。「事前対策」の重要性を、もっと告知しないと、こうした事例は増え続ける一方です。

尾崎　情報漏洩に関しては、各企業が相応のコストをかけてこれを防ぐシステムの構築に努めているわけですが、問題の根は深く、企業だけで対応できる問題ではないとも思っています。日本企業の最先端の技術情報が他国に流出してしまうのは、国際競争力の低下を招くことになりかねません。しかし、国内では、そうした事例に適時適切に対応できるだけの法的な環境が必ずしも整っていない。国の政策レベルでの対応も必要だと思います。

佐々木　いまの指摘は、非常に重要だと思います。国内には、現在、ｅディスカバリーに関する法律がないに等しい。それゆえ、民間企業の間でも、デジタルフォレンジックに対する意識が、まだまだ低い。告知不足という意味では、我々の責任でもありますが。

尾崎　おっしゃるように、日本におけるｅディスカバリー法の整備は、企業秘密や知的財産権などをめぐる紛争において、日本企業が訴訟を通じて解決を図る際の強力な武器になることなどが期待されるわけで、そのような法整備を日本でも早急に進めることにつき検討を進めていく必要はあるでしょうね。

佐々木　我々の仕事は、警察からの依頼も多いのです。それは犯罪に関わる事例が多いということでもあるのですが、逆にいうと、顕在化しないようなものを、私企業が調査しようとしても、何からどうやって手をつけていいのか分からない。もっといってしまうと、情報が漏洩していることにすら気づいていないケースもある。そうなると、尾崎さんが指摘したように、国力の低下を招く危険性すら出てきます。

　現在進行形で進んでいる事態に対処するには、ことが起こってからでは手遅れです。そのためには「事前対策」に目を向けていただくほかないのです。

適切な初動と事実調査

佐々木　危機管理ということでいいますと、不祥事が発覚したとき、「事後対策」の面でも、さまざまなアドバイスをなさっていますよね。

尾崎　ええ、そうですね。

佐々木　マスコミ報道などを見ていますと、情報開示のタイミングの悪さが、本来の事件とは別の火種になってしまうというケースも多々見受けられます。

尾崎　不祥事の情報開示については、それが必要な事案では、そのタイミングの見極めと、正確かつ合理的な説明ができるかどうかがポイントの一つだと思っています。単に開示が早ければよいというものでもない。不祥事らしきものの端緒を把握したとして、迅速な事実調査を通じて正確な事実関係を解明しないまま、先走った形で不正確な情報を開示してしまった場合、それが上場企業であれば、それによって市場を動揺させ、株価に無用な悪影響を与えるおそれもあるわけです。

佐々木　後から訂正しても、もはや時すでに遅しで、情報がひとり歩きする危険性もありますからね。

尾崎　ですから、正確な情報を可能な限り速やかに開示することが重要ですが、そのタイミングは事案によります。また、不祥事に関する開示と同時あるいはさほど間を置かずに、原因の究明とこれを踏まえた効果的な再発防止策を打ち出せるのが理想的です。企業が対外的に自浄能力を十分に示すことが、当該企業へのダメージを最小限に食い止めることにつながると思います。

IT環境における危機管理

佐々木　役員や従業員の不祥事は、いつの時代にも存在していたと思うんです。ただ、以前に比べると、内部告発の手段が確実に増えています。ここ数年、信じられないような事件や不祥事が、次々に明るみに出ています。それはＩＴ環境の整備と無関係ではないでしょう。

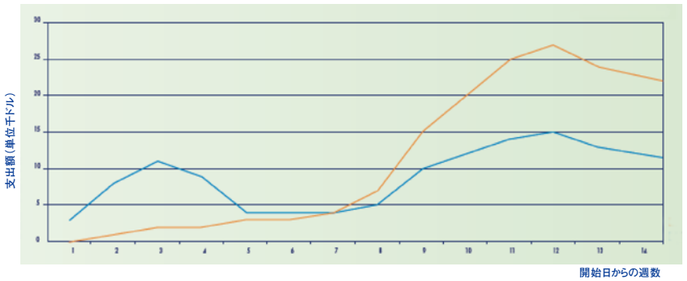
尾崎　いわゆる公益通報者保護法制定の影響もあり、内部告発に対する意識が変わったこともあるでしょうが、ＩＴ環境の進化に伴い、不祥事に関する情報を、社内のみならず当局やマスコミに対して直接通報したり、ブログやネット上の掲示板に掲載したりするなど、手段も多様化しています。

佐々木　理想をいえば、不祥事がないに越したことはないのですけれども、現実問題として、そうもいっていられない、ということですよね。

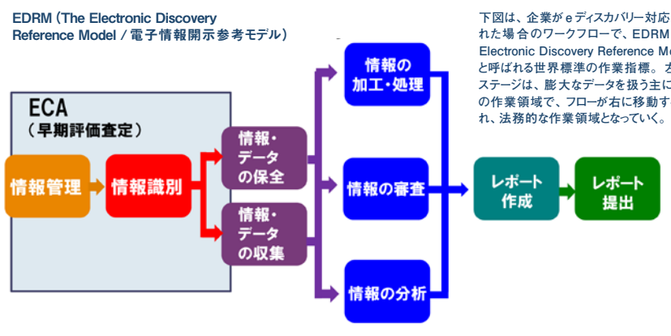
尾崎　不祥事対応は、社内でいち早く端緒を把握したうえで、迅速適切な事実調査と、リスク分析を踏まえた対応策の構築を速やかに行うことが重要です。とはいえ現状は、企業が不祥事を把握していない中で、いきなり当局の調査・捜査やマスコミの報道が先行するというケースが少なくありません。その場合、企業の対応は後手後手に回ってしまうことが多い。

佐々木　結局、危機管理という側面においては、大事にならないうちに不祥事の芽を摘み取っておけるような仕組みやシステムを構築しておくべきということですよね。

尾崎　おっしゃるとおりです。企業にとっては、完全には防ぎきれない不祥事の芽を早期に把握する体制と、これを把握した後に迅速適切な対応策を講じ得る体制とを、平時より整備しておくことが、危機管理の重要な課題の一つといえます。



訴訟に発展し得る問題が発生した場合、徹底的に争うか、和解に持ち込むか等の判断を下す必要が生じる。そのためには、訴訟事実を正確に評価し、収集すべき情報の対象を絞り込み、訴訟全体のリスクを計算して、対応を戦略的に判断し計画することが重要となる。このような訴訟の初期段階においてリスク・バリューを評価することを「ECA（Early Case Assessment）：訴訟案件の早期評価査定」と呼び、従来のアプローチに比べて訴訟費用が低く抑えられることが知られている。



下図は、企業がｅディスカバリー対応を迫られた場合のワークフローで、EDRM（The Electronic Discovery Reference Model）と呼ばれる世界標準の作業指標。左側のステージは、膨大なデータを扱う主にIT系の作業領域で、フローが右に移動するにつれ、法務的な作業領域となっていく。