Topics

eDiscovery対応の概要と平時の取り組みについて 後編

Forensics事業部　公認不正検査士　松原 努　　米国弁護士　Daryl Osuch

▸ Tsutomu Matsubara

10年超にわたり、医薬、電気機器、自動車、自動車部品、精密機器、食品、化学、ゴム、商社、機械、海運等の幅広いセクターの日系企業に民事訴訟、当局調査などにおけるeDiscovery対応支援を提供。Forensic & Integrity Services eDiscovery対応チームのリーダー、シニアマネージャー。

▸ Daryl Osuch

外資系法律事務所の弁護士として、日系企業を含む多くのクライアントのeDiscovery対応戦略の立案から、データ収集、データ処理と分析、ドキュメントレビュー、プロダクション、関連する供述の計画、実行および支援などの業務に従事。自動車、自動車部品、化学、金融、物流等の業界に精通。Forensic & Integrity Services eDiscovery対応チームのシニアマネージャー。

Ⅰ　はじめに

前編（本誌 2020年7月号）ではeDiscoveryの歴史と対応の基本ルールについて簡単に説明しましたが、後編となる本稿では、eDiscovery対応の流れ、制裁事例、平時における取り組みのポイントについて説明します。

Ⅱ　eDiscovery対応の流れ

1. Information Governance（情報の管理）

規制、法令等に関連して将来的に発生し得るさまざまなリスクを軽減するために組織内のデータを管理し、ルールや手続きを策定します。原則として、eDiscovery対応に関する事前準備はこのタイミングで完了している必要があります。

2. Identification（情報の特定）

訴訟が合理的に予見される段階になると、訴訟に関係する可能性がある情報を保全するためにヒアリングやデータマッピングなどの手法を用いて、情報を誰が保有または管理しているか、そしてどこに保存されているかを特定します。ここで特定された情報の保有者または管理者をカストディアンと呼びます。

3. Preservation and Collection（情報の保全と収集）

特定された情報の削除や毀損（きそん）を防止するために、カストディアンやIT管理者などの関係者に訴訟に関連する可能性がある情報に対する保全義務が発生したことを通知※1し、リーガルホールドを実行します。システム上のデータは、自動削除機能の停止やバックアップを実施します。保全された情報は証拠性を損なわない方法でハードディスク等に複製され、Chain of Custody（CoC）※2とともに保管されます。

4. Processing, Review and Analysis（情報の処理、レビューと分析）

複製された情報は専用システムに取り込まれ、日付範囲やキーワード検索などによる絞り込みが実施されます。次に、内容を精査するためのレビューや分析が実施され、訴訟に関係のない情報、訴訟に関係のある開示対象の情報と秘匿特権などにより開示対象外となる情報に分類されます。従来のレビューは人間の目視によって行われていたため、莫大（ばくだい）なコストが掛かっていましたが、相手方と合意の上で、TAR※3などの技術

※1　この通知をリーガルホールドノーティス（Legal Hold Notice）と呼ぶ。
※2　米国の民事訴訟などの法的手続きに際して、物理的または電子的な証拠の取得、保管、移転、廃棄までの一連の手続きを時系列で記録した文書をChain of Custodyと呼ぶ。

を利用し、コストを削減する動きが徐々に浸透し始めています。

5. Production（データの提供）

レビュー等によって開示対象と判断されたデータは、相手方と合意した形式で出力され、相手方へ提供されます。

6. Presentation（証拠の提示）

前記データの一部が証言録取や本審理の中で、参考人の証言、争点となっている事実の主張や反証、陪審への説明の際に証拠として使用されます。

Ⅲ　制裁事例

1. 事例①：137 S. Ct. 1178 (2017).

被告は製造業A社で、A社製品の不具合によって事故が発生したとして原告Bによって提起された訴訟です。A社はBからの試験データに関する開示請求を、データが残っていないとの理由で拒否しましたが、後にデータが残っていたことが判明したものです。A社の偽証に対する制裁として、裁判所はBの訴訟費用のうち被告の偽証以降に発生した訴訟費用の実費270万ドルの支払いを命じました。

2. 事例②：2008 WL 638108（S.D. Cal. Mar. 5, 2008）.

被告C社とその競合である原告D社との間では、2007年に提起された訴訟を含めて4件の訴訟が発生し、最終的に18年まで続きましたが、本件はそのうちの3番目の訴訟です。eDiscovery対応の中で、C社による情報の特定、特定漏れに対する改善対応、検索条件の指定、弁護士を含む関係者間のコミュニケーション等が不十分であったため、裁判所はC社に850万～870万ドルの支払い※4を命じました。

Ⅳ　平時における取り組みのポイント

平時に実行可能なeDiscovery対応への取り組みのポイントを下記に記載します。情報の保全義務が発生している状況下では実施できないものもありますので、必ず専門家にご相談ください。

1. 社内トレーニングによる啓蒙活動の実施

訴訟に関係する可能性がある部門やIT部門を対象とした社内トレーニングを実施し、関係者にeDiscovery対応のリスクについて正しく認識してもらうことが社内での準備を進めるための第一歩です。社内で適当な講師がアサインできない場合は、お気軽にForensics事業部の専門家にご相談ください。

2. 文書管理規定の策定または見直し

日系企業の多くがメールや電子ファイルなどのビジネス上の記録を長期間保管していますが、eDiscovery対応では訴訟に関連する全ての情報を相手方に開示しなければならないため、情報のハンドリングに莫大なコストが掛かります。文書管理規定の策定または見直しを行うことで、情報の保管期間が短くなり、将来のeDiscovery対応コストの削減が可能となります。

3. IT環境の棚卸しとドキュメンテーション

eDiscovery対応のスピードは、証拠開示が必要となった訴訟や調査の種類によっても異なるため、本稿では記載していませんが、情報の特定や保全の不備により制裁を受ける企業が散見されていることを踏まえて、それぞれの対応を極めて短い期間でミスなく完了させなければなりません。事前にIT環境の棚卸しとドキュメンテーションを行うことによって対応時間を短縮し、不注意から生じる情報の特定漏れを防止する効果が期待できます。

Ⅴ　おわりに

本稿では、eDiscovery対応の概要と平時の取り組みについて、過去の制裁事例を交えながら解説しました。どのようにeDiscoveryリスクに備えるかは、企業のビジネス戦略によっても大きく異なりますが、企業が保有する情報の増加に伴ってeDiscovery対応のコストも急速に増加しており、平時における取り組みの重要性が増していることに疑いの余地はありません。本稿がeDiscoveryリスクに対する平時の取り組みを検討するきっかけとなれば幸いです。

お問い合わせ先
Forensics事業部
E-mail：forensics.ediscovery@jp.ey.com

※3　熟練したレビュアーのレビュー結果に基づき、コンピューターソフトウエアが文書を処理して、訴訟の争点に対する関連性の有無や秘匿特権の該非などを分類する一連のプロセスをTAR（Technology Assisted Review）と呼ぶ。
※4　当該判決は15年のFRCP改正前であり、直近のルール下では制裁額が減額される可能性がある。