論　説

eディスカバリの実践的対応

大　平　恵　美*

抄　録　2006年の連邦民事訴訟規則（FRCP）の改正によりｅディスカバリが正式に導入され，すでに８年ほどが経過した。この８年ほどの間にｅディスカバリのやり方等についてある程度固まってきたとはいえ，まだまだ進歩している分野であり，またそれぞれのフェーズにおいて争いがあるのも事実である。ｅディスカバリは大変だ，費用がかかると言われているが，実際に経験をしている日本企業はそんなに多いわけではない。特に知財の分野で考えると，米国に進出している日本企業ならば，特許権侵害を問われる可能性はいつでも存在する。しかしながら訴訟に至り，そしてｅディスカバリを行うフェーズに突入する日本企業は数少ないのが実情である。そのため，実際にｅディスカバリに直面したときに何をどうしたらよいのかよくわからず，作業が後手後手に回ることがよくある。そこで，日本企業がｅディスカバリに直面した場合にどう対応をすべきかについて考察する。

目　次

1．はじめに

米国の民事訴訟法におけるｅディスカバリは年々コストのかかる大掛かりな手続きとなってきており，米国の法曹界でも問題となっている。特に，かかる手続きに慣れていない日本企業が特許権侵害訴訟に巻き込まれた場合，電子データが証拠として使われる割合は0.0074%と非常に低いに[1)]もかかわらず，膨大な費用と情報の流出という多大なリスクを負うことになる。ｅディスカバリの手続きを法律的な側面及び実践的な側面の両面から理解をすることが，そのリスクを避ける第一歩となることであろう。そして，法的側面についてはすでに色々な場で説明されている。そこで，本稿ではｅディスカバリの手続きを実践的な側面から考察することとする。

2．ｅディスカバリの概要

ｅディスカバリは，「ｅ」が付くだけあって，紙のディスカバリの時代とは異なり，作業自体が複雑になっている。紙のディスカバリの時代には，関連する書類を会議室に集め，１ページずつ書類を見て，関連する書類のコピーを取って，相手方に開示していた。しかしながら，電子の時代となった現代においては，書類開示は電子データによって行われるのが一般的である。一見すると簡単に見えるが，実際に体験すると色々な問題点や不明な点があることがわかる。

* DSA Legal Solutions, Professional Corporation
カリフォルニア州弁護士・日本国弁理士
Emi OHIRA

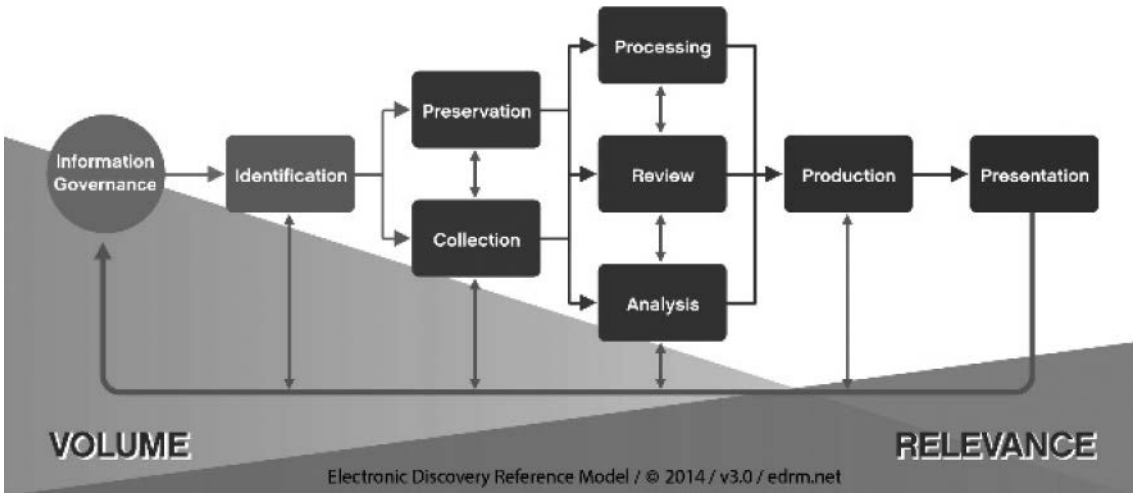

図1　Electronic Discovery Reference Model

eディスカバリは，図1に示すEDRM（Electronic Discovery Reference Model）[2]と言われるモデルに従って行われるのが一般的である。従って，まずはこのEDRMを理解することが必要である。

(1) Information Governance

この時点では，訴訟が起こることが予期されていない。したがって，適切な情報管理規定を運用している段階である。

(2) Identification

Legal Hold（証拠保全義務，Litigation holdとも呼ばれる）が発生し，事件に関連する書類を保持している者及びその者のデータの保存先を特定しなければならない。

(3) Preservation

証拠保全を行う。なお，この時点では，関連するデータの改変や破棄が行われないよう管理する。

(4) Collection

eディスカバリの手続きのために保全したデータを収集する。

(5) Processing

収集したデータの容量を減らす作業をする。

(6) Review

関連性及び秘匿特権等についての評価をする。

(7) Analysis

内容の評価をする。

(8) Production

関連するデータを適切な方法で開示する。

(9) Presentation

Deposition（証言録取）等において活用される。

この流れを見ると，簡単なような気がしてしまうが，実はそうではない。そこで，一つ一つのフェーズについて説明をしたいと思う。そして，そのフェーズごとに，問題点も併せて説明する。

3．各フェーズの説明

3. 1　Information Governance

簡単に言ってしまえば，訴訟の可能性もない平和な段階である。この段階で重要なことは，

適切な情報管理規定を適切に運用することである。よくあるのは，「規定はあります。でも，運用はよくわかりません。」のパターンである。例えば，サーバーに10年以上前の資料が保存されている。そして，情報管理規定によれば，その資料の保存期間は３年で，本来は存在してはならない資料であるような場合が該当する。この場合，情報管理規定では３年保管となっているから３年分のデータについて保全すればよいのではなく，保管している10年以上のデータを保全する必要がある。このことは何を意味しているのか？存在するべきではなかったデータの収集等にかかる費用が余分にかかることと，場合によっては関連する書類で提出しなくても良かった書類の提出が余儀なくされることを意味する。そうなったときに，きちんと管理をしておけばよかったのに，と悔しがっても後の祭りとなるため情報管理規定の適切な運用が重要となる。

さて，実際の訴訟では情報管理規定の提出を要求されることがあり，その場合，情報管理規定を提出せざるを得ない。この時，要求する相手方は何を見るかといえば，要求された側が情報管理規定にきちんと従った情報管理をしているのかということである。これによって何がわかるかというと，きちんと管理していればその年月分の書類しか開示してもらえないことがわかる。一方，きちんと管理していなければ長期間にわたる書類の開示を要求することができる。さらには，Safe HarborといわれるFRCP（The Federal Rules of Civil Procedure：連邦民事訴訟規則）37条の証拠の破棄に関する規定[3]の適用の可否がわかる。実際に，あるケース[4]では，原告は18年分の書類の開示を裁判所に命じられた。このケースは，特許権侵害訴訟であり，被告が原告に対して18年分の電子データの開示を求めた。なお，この要求の前にも，原告に少なくとも５年間分の電子データの開示が要求されていた。そこで原告は追加のデータ収集にはレビュー費用を除いても約100万ドルから150万ドル（約１億円から1.5億円）の費用がかかることを証明し，被告の18年分のデータの開示の要求に対して「合理的にアクセス可能ではない」として反論していた。これに対し，裁判所は追加のデータは「合理的にアクセス可能ではない」と判断したものの，被告が原告に開示を強制するだけの正当な理由があると認定している。そして，最終的にはデータの関連性と電子データの開示にかかる原告の費用のほか，他の情報源からの同じ情報の取得の困難性を考慮したところ，争点の重要性との関係からその法外な費用は正当化されると裁判所は認定した。そして，この被告の申し立ては認められたため，原告は18年分のデータを開示せざるを得なくなった。その一方，費用の80％を被告が負担することとなった（費用転嫁）。つまり，データを長期間持っていればその分だけ訴訟の際に開示せざるを得なくなる可能性が高いということがわかる。このケースは，非常に長期間保管しているデータの開示を求められたということで，米国の法曹界でもかなり話題になった。実際，書類開示の要求では期間が指定されることがあるが，その期間について通常当事者間で取り決めがなされる。その際に，保管していれば合意された期間分の開示に応じるしかないが，情報管理規定に従って適切に運用をしており，かつその期間のデータが残っていない場合，書類の開示は避けられるのである。

また，情報管理規定は証拠隠滅を証明するための基礎となりうる。つまり，保管期間が３年の書類が作成後３年以内にも関わらず存在しなければ，削除した可能性が高いと考えられ，証拠隠滅が疑われることもある。

ここで何が言いたいかというと，最低でも日ごろから情報管理規定をしっかり運用することが重要ということなのである。

3. 2 IdentificationとPreservation

IdentificationとPreservationは同時に行われることが通例であるため，両方を一緒に説明することにする。このIdentificationとPreservationとは，訴訟になるかもしれないという状態（reasonably foreseeable）になり，Legal Holdをしなければならない段階をいう。Legal Holdは「証拠保全義務」のことを言い，実際には関連する書類を誰が，どこに保管しているのかを特定し，その書類を保持している可能性の高い者に対して関連する書類を改変・削除しないように通知をし，保全をすることになる。

このLegal Holdについては，色々な注意点がある。注意点としては，（1）Legal Holdをする時期，（2）Legal Holdをする範囲（対象者・保存機器），（3）そのやり方，が挙げられる。

（1）Legal Holdをする時期

Zublake v. UBS Warburg LLC[5]事件において，Legal Holdは「訴訟が合理的に予測されうる（reasonably foreseeable）」ときに発生すると判示された。では，この訴訟が合理的に予測されうるときとはいつであろうか？例えば，裁判所命令が出されたとき[6]，訴訟が提起されたとき[7]，ディスカバリ要求又は召喚状の受領日[8]，証拠保全のための手紙を受領したとき[9]，訴訟提起の意思を固めて，その準備のために行動を起こした時[10]が挙げられる。日本企業の場合，特許権侵害訴訟については原告になるより被告になることが多いが，その場合のLegal Holdの時期はどうだろうか。考え方は同じであるが，気を付けなければならないのは，警告状やライセンス交渉の存在である。警告状が強固な訴訟も辞さないような内容のものであれば，警告状を受け取った時点がLegal Holdをする時期である。逆に，ライセンス契約をしたいという程度のソフトな内容である場合は，注意が必要である。最初は友好な交渉状況であっても，途中で訴訟をも辞さないような状況になればその時点がLegal Holdをする時期となる。いずれにしても，ケースバイケースであるため，第三者からアクションを起こされた場合，そのアクションがどの程度のものかしっかり見定める必要がある。ちなみに，Legal Holdをするか否かについては，数人の合議体で決定をし，議事録になぜLegal Holdをするのか（しないのか）を明示しておくべきである。証拠保全の時期について争いが生じた際に，この議事録が活きてくることになる。つまり，このときの議事録がreasonably foreseeableかどうかの判断に一役買うのである。もちろん，その判断理由などがどうみても合理的でない独りよがりな場合，逆に足を引っ張ることになるので，合理的に考えて訴訟の有無が予測可能か否かについて行ったしっかりした判断を議事録に残さなければならない。万が一迷ったら，普段から付き合いのある信頼のおける米国弁護士に相談するのも一つの手段であろう。この時，日本の弁護士・弁理士に相談するということも考えられるが，餅は餅屋ということもあり，また米国における弁護士秘匿特権との絡みがあるため，やはり米国弁護士に相談するのがベストであると言わざるを得ない。

また，日本企業の場合，この手続きに慣れていないこともあり，Legal Holdに時間をかける傾向がある。確かに関連する書類を保有する人とその書類が保存されている機器を特定し，保全をするのは意外と大変である。また，その予算を取るのも大変だと推察される。その大変さについては後述するとして，大変だということで時間が徒過してしまうことは，証拠隠滅を主張される恐れのある行為である。実際，Apple Inc. v. Samsung Electronics Co., Ltd. et al.[11]のケースでは，裁判に慣れていると思われる両社が証拠隠滅をしたとしてお互いに申し立てを

行い，証拠保全の時期について争った。その結果，両者とも証拠保全の時期に証拠保全をきちんとしておらず，証拠を隠滅したと裁判所から認定された。このケースでは，８か月ほどの違い（訴訟提起時か警告時）を争い，証拠保全の時期は警告時と判断され，証拠隠滅をしたとして両者ともに制裁が課されたが，両者とも同程度の制裁だったので相殺となった。つまり，このケースから明らかな通り，Legal Holdの時期から数か月たってもLegal Holdを行っていない場合，他の要件を満たすことを条件に証拠隠滅の制裁を課せられることになる。そうならないためにも，速やかにLegal Holdを行わなければならない。それでは，実際にLegal Holdからどれぐらいの期間猶予が許されるのか？残念ながら，これについての回答はない。つまり，速やかに行うことが要求されており，猶予期間を議論する余地がないということである。このことを肝に銘じてLegal Holdは速やかに行うよう心掛けてほしい。

(2) Legal Holdをする範囲

Custodian（関連する書類を保有している可能性の高い人）の特定であるが，特許権に関わるからといって特許に関わる研究者や知的財産部の従業員だけが対象となるわけではない。例えば，損害額の算定に関していえば，原価や販売価格などが問題になるため海外営業に関わる従業員の保有するデータが関連する。そうすると，この海外営業に関わる従業員がCustodianとして挙げられるであろう。このように，特許権侵害に関する要件を検討し，それにかかわる書類を保有している人をピックアップしていくことになる。このとき忘れてはいけないのが，退職した元従業員の保有しているデータの存在や，請負等により第三者を雇い入れている場合，その者の保有するデータが対象になることもある。その場合，そういった者たちを漏れなく検証していかなければならない。業務請負等で雇用している者については不明確であったが，最近これについて判決[12]が出たため基準がある程度明確になったと言える。

当該判決においてFRCP 34(a)の“Possession, Custody, or Control”の定義をどう解釈するか判事されている。その解釈とは，書類を物理的に所有していることは要求されておらず，管理していればよいというものである。このケースでは，被告が現在又は過去に雇用されている委託業者にLegal Holdをかけていなかったため，これらの者が管理する関連する書類を原告に提出できていなかった。そこで，裁判所は期限を決めて，これらの者の管理する関連する書類を提出するよう求めた。つまり，訴訟当事者が所有していることは必要ではなく，業務委託をしているような第三者が管理する書類であっても，提出をしなければならないことがあるということである。また，業務請負のような当事者の従業員でない者に対しても，Legal Holdを出さなければいけないこともこのケースから明らかである。従って，協力会社からの従業員が案件に関する書類を管理しているような場合，この者にもLegal Holdを行っていく必要がある点に注意する必要がある。

次に，これらの者たちが使用した機器を洗い出していく作業を行う。これは，デスクトップPC，ラップトップPC，携帯電話，スマートフォン，サーバー，場合によっては，自宅のPCなど全ての機器を洗い出していく。なお，使用しているソフトウェアの確認も必要となる。

これらの作業については，チェックリストを作成し，チェックリストに従って，従業員のインタビューを行い，検討していくこととなる。この時，あまり狭い範囲で行うと訴訟になった時にLegal Holdをかけていなかったと言われる恐れがあるため，少し広めの範囲でLegal Holdをすることをお勧めする。

Custodianに目を奪われてしまい忘れがちであるが，通常のデータベースも同様に特定していく必要がある。例えば，会議資料を特定のデータベースにより保管している場合で，かつ関連するデータがありうる場合，かかるデータベースもLegal Holdの対象となることを忘れないで欲しい。

(3) そのやり方（Preservation）

Legal Holdでは，データの保全をすればよいのはわかるが，どのようにやるのか？という疑問がわいてくるのではないかと思われる。実際，企業によって導入しているシステムが異なるため，Legal Holdのやり方は同じではない。

このやり方であるが，デスクトップなど個別の機器の場合，単純に全てのデータをコピーして，ハードディスクドライブなどのメディアに保管しておけばよい。そうすれば，Legal Hold後のデータへのアクセスも可能となり，従業員にとっては楽である。問題はサーバーであろう。サーバーの場合，データへのアクセスを禁止し，削除・改変を禁止することは可能である。しかしながら，場合によっては企業の業務に支障が生じる。この場合，Legal Holdをかけるデータの量は半端ではないため（今であれば，1.5から２テラバイトになるであろう），業務に対する影響は半端ではない。では，どうしたらよいのか？Collectionを行ってくれるｅディスカバリ業者にデータの収集を頼むことも一つの選択肢としてありうる。しかし，Legal Holdの時点では書類の開示要求の範囲が不明であることもあり，Collectionに無駄が多いことも否めない。また，実際に当事者の弁護士同士でCustodian等を決めたわけではないため，範囲も広くかなり無駄になる可能性は高い。やはり，ここは自社の情報システム部の知恵を借りて，Legal Holdを行う必要がある。例えば，使っていないサーバーがあれば，そこにLegal Holdをかけるデータをコピーすることが考えられる。そうすれば，業務に支障をきたすこともなく，データを保全することができる。

次に，電子メールの存在を考えなければならない。まず，自動削除機能などの機能を停止する必要がある。次に，Custodianとなりうる者のメールを全てコピーし，サーバー等に保管する必要がある。Office 365やGoogle（ビジネス用）等のクラウドサービスを利用した電子メールの場合，ｅディスカバリ用のオプションがあるので，それを利用すると良い。しかしながら，クラウドサービスを利用した電子メールサービスのうち，ｅディスカバリに対応していない場合が厄介である。その場合，クラウドシステムに残っている電子メールを全てダウンロードして，pstファイル等でエクスポートをしてハードディスクドライブ等に保管するしかない。いずれにしても，その道のプロである，情報システム部の知恵を借りるのが一番である。

次に，Legal Hold Notice（Preservation Letter：証拠保全要請通知）を関連する書類を保有している可能性が高い者に送付する必要がある。これは，事件の概要等を記載し，関連する書類を削除しないよう要請をするものである。このとき，これらの者がきちんと理解をして実施するかどうか監督する必要があり，電子メールで通知する場合，その内容を理解し実行する旨の返信をもらっておくと良い。また，Legal Hold Noticeを誰にいつ出したかなどを管理しなければならないので，リストを作るべきである。この作業をサービスとして提供しているベンダーも米国にはたくさんあるので利用することもできるが，日本の企業の場合，そこまで訴訟があるわけではないため，表計算ソフト等での管理でも間に合うのではないかと思われる。

意外と忘れてしまうのが，ソフトウェアのアップデートをしてはいけないという点である。データのコピーを取って別のサーバー等に保全

する場合は良いが，現在使っているサーバー上で保全する場合，ソフトウェアのアップデートがなされてしまうことがある。このアップデートによりデータの内容が変わってしまうことがあり許されるものではないため，注意をしていただきたい。こういった点については，実際にこの場面になり，情報システム部が呼ばれても瞬時の理解は難しいため，事前にある程度の手順を決めておくことが重要であろう。

3. 3 Collection

Collectionとは，要するにデータの収集である。前述したPreservationにおいて保全したデータのうち，Custodianとして確定された者の関連するデータを全て収集する。収集とは，簡単に言うとデータのコピーである。通常，eディスカバリベンダーがデータ収集用のソフトウェア（FTK, enCaseなど）を使って，サーバーやPC等からデータをコピーする作業をいう。ちなみに，裁判所がこれらソフトウェアを使うようにと指示することはないが，従来のやり方の場合，あとから疑義が生じないよう，世界的に定評のあるフォレンジックツール（電子情報の科学捜査のためのソフトウェア）であるこれらのソフトウェアを使って作業が行われてきた。しかしながら，技術の進歩は速く，最近ではCollection作業の必要のないeディスカバリプラットフォームも登場している。データをコピーする速度やコピーするデータの容量によるが，数日の時間をかけて行われる。なお，業務に支障をきたさないように，週末や夜中に行われることが多い。また，サーバーは通常セキュリティがかかっているため，Collection業者が実際の作業を行う際にセキュリティがかかっていると作業ができなくなってしまう。そのため，セキュリティをCollection作業の前に解除しておくことが必要となる。従って，この作業には情報システム部が関わらなければならないため，Collection業者と打ち合わせをする際には情報システム部の担当者の同席が必須である。

この時の注意点としては，とにかく漏れのないCollectionを行うことである。Collection作業の失敗については，Cashe La Poudre Feeds LC v. Land O'Lakes, Inc.[13] のケースにおいて，被告は現従業員の保有する電子データの検索をし，元従業員が作成した電子データの印刷バージョンを作成したが，元従業員の電子データを探そうとしなかった。これは，通常退職する際に電子データは削除されるため，元従業員のデスクトップに電子データはないだろうという弁護士の意見に基づくものであった。結果として，Legal Hold発生後に元従業員のデスクトップのデータが削除され，関連する書類が削除された可能性があると判断されたため，証拠隠滅として制裁を課されている。このようなケースもあるため，米国弁護士任せではなく，企業がCollectionについてきちんと把握していることが重要である。

なお，Collectionを行うタイミングであるが，微妙に難しい。というのも，和解をする可能性があるのにCollectionを早々に行うと費用が無駄になる恐れがあるからである。この点，和解交渉とMeet and Confer（事前協議）の状況を見ながらの作業となるであろう。担当弁護士との情報交換を密にすることが無駄なCollectionを避けるカギとなる。

3. 4 Processing

このProcessingの作業は，色々な形式のデータファイルを一つのソフトウェアで見ることができるようにするための作業である。例えば，ワードのファイルをエクセルのソフトで開けることはできない。それぞれのソフトウェアで開けていたら，大量のデータのReview作業（この次の作業）をこなすことができない。また，CADファイルなどの場合，訴訟のためにCAD

のソフトウェアをインストールするなどということは非常に無駄な作業である。従って，テキストデータを抽出し，イメージデータに変換することにより，一つのソフトウェア（いわゆる，ｅディスカバリプラットフォーム）で全てのデータを見ることができるようにするのである。もともとコンピュータサイエンスは，アルファベットの国が発祥地であるため，日本語などの２バイト文字の言語に上手く対応していないｅディスカバリベンダーも存在する。そして，うまく対応していない場合，文字化けが生じてReviewをするときに読めなかったり，Processingの段階でひと手間かかったりすることがあるので，あとで困らないように，そのベンダーが本当にきちんとできるのか，そのテクニカルサポートに係る費用がどれぐらいかかるのかなどについて，事前にきちんと聞いておくとよい。ちなみに，日系のベンダーにこだわる必要は全くなく，こういったことにきちんと対応している米系のベンダーは多いので，価格などを比較して決定してほしい。特に，価格については全てのフェーズの価格を検討していただきたい。

次に，Culling（情報選別。フィルタリングともいう）といわれる作業を行うのであるが，この作業は，重複書類を削除する作業（Deduplication）であり，データ量を削減するものである。この作業は，Reviewをするデータ量を減らす重要な作業である。通常は，この作業をｅディスカバリベンダーが行う。ただし，この作業を経たからといって，全ての重複データが削除されているとは限らない。データのハッシュ値によって，システムが判断していくものであり，人の目によって判断していくものではないため，ハッシュ値が少しでも異なれば重複データと判断されないからである。また，電子メールの場合，単なる転送であっても，ハッシュ値が異なるため，重複データとは判断されず，実質的に同一内容であったとしても削除されずに残る点には注意する必要がある。

3. 5　ReviewとAnalysis

まず，Reviewについて説明する。Reviewとは，データを収集し，Processingが終わり，ｅディスカバリプラットフォームで見られるようになった電子データを，Responsive（開示要求に対する応答の対象），Privileged（秘匿特権の対象）などのタグをつけて，相手方に開示をする書類を選別する作業をいう。基本的なやり方としては，関連するか否かなどについてタグをつけていくInitial Reviewを行い，Quality Controlとして同様の作業を繰り返す２回目のレビューを行う。そして，Privilege Reviewは同時に行ったり，別で行ったりする。最近では，Predictive Codingという技術を使うこともあるが，基本的には人間が行う作業であるため，一番コストがかかる部分であり，機密情報を扱う作業であるため，誰が行うかについて注意を払う必要がある。実際この点にあまり注意を払っていない日本企業が非常に多いが，この考え方は改めるべきと考える。例えば，訴訟を多く抱えているGoogle，AppleやIntelなど米国企業では，機密情報を扱うからという理由で，この作業を社内で行うことが多い。これらの企業がこの作業のために，直接臨時で弁護士を雇うことも少なくない。特に，これらの企業は，機密レベルの高い情報については，並々ならぬ注意を払っている。ただし，外国語については社内で扱いきれないため，その言語に精通した米国弁護士を臨時で雇ってその作業を行っているのが現実である。特に，特許権侵害訴訟の場合，技術が絡んでくるため，技術を知らない者が行うと非常に効率が悪いだけでなく，事件に関連性のないデータが開示される恐れもある。また，コストの問題もあるため，日本企業もこの手続きのあり方について検討を始めても良い時期が来ているのではないかと考える。

次に，タグ付けについて少し説明する。まず，相手方から開示要求のあった内容に関連する書類については，Responsiveというタグをつけていく。この「関連する書類」とは，相手方からの書類開示要求に該当する書類をいい，実際の証拠として関連のある（relevant）書類よりも広い範囲の書類が該当する。なお，相手方からの要求は，特許技術に関するものだけではなく，マーケティング資料・顧客情報・価格や実施料に関する資料など多岐にわたり，非常に広い範囲の書類となる。特に，被告になる場合，例えば故意侵害（Willful Infringement）に関する書類，原告になる場合，例えばMisuse（濫用）やInequitable Conduct（不公正行為）に該当するような行為に関する書類には要注意である。なお，開示要求を見ることで相手の狙いが見えてくる場合があることから，よく検討するべきである。

次に，関連するか否かの判断の他に，Confidentialに関してもタグ付けを行う。Confidentialは，その字のごとく，秘密に関するタグ付けである。そして，そのタグにはConfidential, Highly Confidential（Attorneys’ Eyes Only），Not Confidentialの３種類がある。この違いであるが，Confidentialは，社外秘のものが該当する。基本的に，通常の社内での電子メールや社内で回覧される書類などは，全てこのカテゴリーに含まれる。特許権侵害訴訟において，Not Confidentialにお目にかかることはあまりない。例えば，特許公報そのものは，Not Confidentialであるが，電子メールに添付されているその特許公報の写しはConfidentialとなる。また，価格表や技術的な書類，他社特許の比較表など，非常にセンシティブな書類については，“Attorneys’ Eyes Only”（Highly Confidential）として，タグ付けをすることになる。このタグ付けにより，相手方当事者の弁護士はその書類を見ることになるが，当事者は見ることができない。従って，弁護士がこのカテゴリーに入る書類を使って，裁判所に意見を出したりすると，当事者が知らない情報がでてくるため，びっくりすることがある。このカテゴリーに入る書類は，相手方当事者が見ることがないため，安心してしまう。しかしながら，Apple Inc. v. Samsung Electronic Co. Ltd. et al.[14] において，被告と代理人事務所は，原告らの実施料率の記載されていたライセンス契約書がHighly Confidentialであったにもかかわらず，90人の被告の社員と19の法律事務所の130人の弁護士に，その書類（電子メール）を開示した。そして，その制裁として２億円を原告らに支払うよう命じられた。このケースは，極端なケースであるため，参考にならないかもしれない。しかしながら，このケースからわかるように，Highly Confidentialとあっても，こういうこともありうるのだと頭の片隅に置いておいてほしい。

最後に，一番問題となるPrivileged Documentについて説明する。Privileged Documentには，弁護士秘匿特権とAttorney Work Productの２種類があり，このカテゴリーに入る書類は相手方に開示をしなくても良い。そのため，この点について争われることが非常に多い。Attorney Work Productは，訴訟の準備のため，又は，訴訟を予期して作成された書類が該当する。例えば，Legal Holdの通知や訴訟のためのクレーム解釈検討のための書類がこれに該当する。また，訴訟準備のための原告の特許についての侵害の可否の検討などもこのカテゴリーに入る。問題は，弁護士秘匿特権の判断である。弁護士秘匿特権は，弁護士とクライアントのコミュニケーションであり，法的助言を含んだものでなければならない。米国弁護士と直接やり取りをしている場合は，基本的に問題ない。しかしながら，日本企業の場合，米国企業と異なり，企業内弁護士や企業内弁理士がジェネラル

カウンシル（法務顧問）等としての役割を果たしていなかったり，そもそも存在しないことがある。また，コミュニケーションに，米国での特許に関する法的助言が含まれていても，それが米国弁護士の意見を踏まえて書いたものなのか，知的財産部内での意見なのかがはっきりしないものが多い。実際このような状況の下でPrivilegeを確定するのは，非常に頭の痛い問題である。いずれにしても，電子メールを含む書類を作成する場合，だれが何について法的助言をしているのか明確にすることが重要である。

なお，日本企業にとっての悩みの種の一つは，他社の特許権について検討した書類を故意侵害に関する書類として開示せざるを得ないことであろう。特に，研究者等は「抵触」等の単語を駆使し，電子メール等を作成してきたような場合，弁護士秘匿特権に保護される範囲ではないため開示せざるを得ない。こうならないように事前に対策を講じるべきである。その対策とは，弁護士秘匿特権の活用，不要データの整理や社員研修に他ならない。

開示せざるを得ないから仕方がない，ではなく，開示しないような対策を練っておき開示を避けることが一番重要である。

因みに，どのベンダー（ｅディスカバリプラットフォーム）を利用するかについてであるが，今は法律事務所から進められるまま使っている日本企業が多いと思う。そのプラットフォームでよいのであろうか？また，実際の契約内容を検討しているのであろうか？例えば，訴訟終了後のデータの廃棄についてまで検討しているか？実際に，この点について争っているケースが，州裁判所レベルであるが存在する[15]。このケースにおいて，原告の50テラバイトを超すデータをホスティングしていた被告は原告のデータ返却依頼に対して８万ドルを支払わない限り，20テラバイトを超す非常に機密性の高いデータを，破棄すると脅迫していた。そのため，原告は被告に対してデータの破棄禁止を求める差し止め請求をしている。この例は，非常にまれなケースかもしれないが，訴訟終了後のデータ返却等についても検討をするべきである。

3. 6 Production

Productionは，書類開示といわれ，関連する書類であり秘匿特権等により開示義務のない書類を相手方に開示する手続きをいう。まず，Productionの検討に入る前に，eDiscovery Protocolについて説明したい。

これは，開示する際にどうやって開示をするのかについてのガイドラインである。裁判所がスタンダード版を当事者弁護士に与えるが，これで進める必要はなく，修正をして当事者間で決めることができる。従って，このeDiscovery Protocolをきちんと読み，自社のデータの保管状況（メタデータなど）や電子メールの性質などを検討した上で，自分たちの弁護士に相手方弁護士と話し合いをしてもらうことが必要である。例えば，電子メールの開示については，添付ファイルをどうするのかというのは非常に重要である。電子メール本文は関連していても，添付ファイルは関連していないにもかかわらず秘密レベルが高いことがある。そして，取り決めで決めていない場合，電子メールと添付ファイルを一緒に出さざるを得ないことがある。電子メールと添付ファイルの関係について争われたある事件[16]では，最終的には，この争点についての明確な回答はなかったが，Special masterから，FRCP26（f）の当事者間の事前協議において，電子メールと添付ファイルの開示についてきちんと取り決めをするべきだとの提言があった。このケースでは，開示するデータについての期間が決められており，電子メールはその期間内だったので原告は被告に対して開示したが，添付書類はその期間外に作成されたものだという理由（Not Responsive）で開示をしな

かったために問題となった。なお，期間外のメールであっても開示書類に含まれたものもあったが，それについては意図せず開示したものと原告は主張した（このメールの添付書類は開示されていない)。ちなみに，被告は関連する期間内のメールを特定し，添付書類も期間内に作成されたものであると信じていた。

電子メールと添付書類については，別々で検討されるべきであるという考え方がある。一方，ビジネス上一体として取り扱われているから一体として開示するべきとの考え方も存在する。このように見解がいくつかあるため争われることがあり，その開示方法についてきちんと当事者間で取り決めをしておくことが重要である。また，メタデータの取り扱い，紙のデータの取り扱いなどについても，きっちり決めておくことを忘れないでほしい。

次に，書類開示の方法は，通常はメディアに保存をして開示をする方法や，サーバーへのアクセス権を与えてアクセスをさせる方法がある。また，元々のデータ形式で開示するか，Tiff Fileで開示するかという問題もある。そして，Privilege Logを提出することも忘れてはいけない。これらは，FRCP2 6(f) のMeet and Conferにおいて，当事者の代理人が決める事項である。また，開示する時期・Custodianなどについても同様であり，当事者の代理人が決めることになる。一括で開示する場合もあれば，五月雨式に出すような場合もある。いずれにしても，当事者の弁護士間できっちり取り決めをする必要がある。

ここで，誤解のないように説明するが，開示された書類のすべてが証拠として採用されるわけではない。証拠として採用されるためには，証拠法に基づき認められなければならないからである。特に，電子メールは伝聞証拠に該当することが多く，証拠として認められない場合が多い。しかしながら，開示された書類は，相手方の弁護士により分析され，Deposition等に利用される。なお，Depositionで答えた内容は証拠として採用される。従って，開示された書類の内容の分析をきちんと行うことは非常に重要である。ここで忘れてはいけないのは，翻訳の存在である。特許権侵害訴訟において相手方に翻訳を提出するか否かについては，当事者同士で決めることになるためその合意に従うが（相手方のために翻訳文を提出することはほとんどない)，少なくとも自分達の担当弁護士が読めるよう翻訳をするのが原則である。従って，その場合は，どの範囲の翻訳を行うかについては担当弁護士と相談して決めると良いであろう。

次に，間違って開示してしまった書類はどうなるのか？という点について触れたい。例えば，秘匿特権により保護されている書類を，間違って開示してしまった場合，相手方から回収することができる。このとき相手方があっさり返却又は破棄してくれればよいが，してくれない場合には，裁判所に申し立てをし認められた場合に限りその書類は返却されることになる。このとき，間違って開示してしまった書類に記載されている内容について全て秘匿特権を失うのかという疑問があると思う。意図的に開示した場合は，そのテーマに関連する内容について全て秘匿特権を失うことになる（Federal Rules of Evidence：連邦証拠規則502条）が，意図せず開示してしまって返却される場合，関連する事項についても秘匿特権を失うことはない。いずれにしても，秘匿特権により保護される書類を開示しない努力をすることが重要である。

3. 7 Presentation

Presentationとは，開示された書類がDeposition等において利用されることをいう。なお，Depositionでは，相手方に開示した自社の書類を見せられて色々なことを質問される。この時の証言の内容は証拠となるため，証言の内容に

は注意をする必要がある。

4．おわりに

eディスカバリは，LegalとITの融合であるため，eディスカバリベンダーのサービスと担当法律事務所に依拠する手続きであり，法務部・知的財産部の部員にはよくわからないものだと思われている節がある。しかしながら，この進め方を理解していれば，企業が自分達でeディスカバリを効率よく進めることも可能となり，機密情報の開示の阻止やコスト削減も可能となる。

本稿では，eディスカバリのより実践的な対応について言及した。とはいえ，全てを書ききることはできなかったが，重要なところは押さえたと思う。日本企業がeディスカバリの必要性に迫られたとき，本稿がeディスカバリの実務における道標となることを心より祈念する。

注　記

1) Randall R. Rader, The State of Patent Litigation at 8, 2011
2) EDRM LLCが提唱するeディスカバリの手順を示すモデル。図1は下記サイトより引用。http://www.edrm.net/（参照日：2014年10月14日）
3) FRCP37(e)は，Safe Harbor Ruleと言われており，ESIを情報管理規定に従って削除してしまった場合，一定の条件の下制裁を免れられるという例外が規定されていたが，この例外規定がなくなるという方向にある。
4) Takeda Pharmaceutical Co., Ltd. v. Teva Pharm. USA, Inc.（2010 WL 2640492（D.Del. June 21, 2010））
5) Zublake v. UBS Warburg LLC（220 F.R.D. 212）
6) Victor Stanley, Inc. v. Creative Pipe, Inc.（Victor Stanely II）, 269 F.R.D. 497, 521（D. Md. 2010）
7) Danis v. USN Commc'ns, Inc., No.98 C 7482, 2000 WL 1694325（N.D. Ill. Oct. 23, 2000）
8) Mosaid Techs. V. Samsung Elecs. Co., 348 F. Supp. 2d 332（D.N.J. 2004）
9) Optowave Co. v. Nikitin, No.6：05-cv-1083-Orl-22DAB, 2006 WL 3231422（M.D. Fla. Nov. 7, 2006）
10) Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 640-41（S.D. Tex. 2010）
11) Apple Inc. v. Samsung Electronics Co., Ltd. et al.,（11-cv-1846）
12) Miriam Haskins, et al v. First American Title Insurance Company, Civil No.10-5044（D.N.J. 2012）
13) Cashe La Poudre Feeds LC v. Land O'Lakes, Inc., 2007 U.S. Dist. LEXIS 15277（D. Colo. Mar. 2, 2007）
14) Apple Inc. v. Samsung Electronics Co. Ltd. et al.,（5：11-cv-01846）※現在控訴中
15) GlaxsoSmithKline LLC v. Discovery Works Legal Inc.（Case No.650210/2013 in the Supreme Court of the State of New York, County of New York）
16) Apple Inc. v. Samsung Electronic Co. Ltd. et al.,（5：11-cv-01846）

参考文献

・https://thesedonaconference.org/（参照日：2014年10月14日）
・Jay E Grenig, Electronic Discovery and Records and Information Management Guide, 2013, Thomson Reuters
・Jay E. Grenig, Federal Civil Discovery and Disclosure, 2104, Thomson Reuters
・J. Edwin Dietel. Designng an Effective Corporate Information, knowledge Management, and Records Retention Compliance Program, 2014, Thomson Reuters
・Shira A. Scheindlin, Electronic Discovery and Digital evidence：Cases and Materials, 2012, Westlaw

（原稿受領日　2014年11月８日）