

平成 28 年 1 月 28 日

欧州で「海外内部通報制度」を導入する際の留意点
～個人情報保護法制の要求事項～

TMI 総合法律事務所
大江修子
波田野晴朗

1. 海外内部通報制度

近年、法令遵守（コンプライアンス）意識の高まりにより、多くの企業において、内部通報窓口を通じて従業員から会社の不正行為の通報を受領する、内部通報制度が設けられている。内部通報窓口は、総務、法務、内部監査等を担当する社内部署に設置される場合もあるが、外部の専門業者や法律事務所を通報窓口を設定している会社も多い。さらに、近年では、海外でビジネスを行う企業にとって、国内のみならず海外におけるコンプライアンスも重要な課題となっている。特に、贈賄禁止規則、輸出管理令、競争法、環境法等の罰則が重く厳格な法令違反や会計不正については、企業に致命的な打撃を与え得るものであり、未然の防止と違反行為発覚時の迅速な対応が極めて重要となる。そこで、近年では、グローバルにコンプライアンスを確保するため、海外ビジネスの拠点（現地子会社等）において、日本と同様の内部通報制度を、自ら又は専門業者や弁護士事務所などの第三者に外部委託する方法によって導入することを検討する日本企業が増加している。

一方で、内部通報には通報者の情報のみならず特定の違反者に関する情報が含まれていることが多いため、従業員から通報窓口への内部通報の過程で、個人情報の提供行為が行われる場面が一般的に想定される。このため、海外において内部通報制度を導入・運用するに際しては、当該国の個人情報保護法制に留意する必要がある。

この点、欧州は、依然として、企業がグローバル展開を行う際の重要な市場であり、子会社を設けている企業も多い。他方で、欧州は厳格な個人情報保護制度を布いているので、内部通報制度の導入及び運用に際して、特に個人情報保護法制への留意が必要となる。

そこで、本稿では欧州における個人情報保護法制の内容及び内部通報制度の導入に際して留意すべき点を概説する。

2. 欧州諸国の個人情報保護法制

(1) 法制度の基本的枠組み

英国、フランス、ドイツ等の EU 加盟国ではそれぞれ個別に個人情報保護法が定められているが、これらの EU 加盟国の個人情報保護法は全て、通称「データ保護指令（Data

Protection Directive)¹ と呼ばれる EU 指令 (Directive)² を基礎とするものである。

EU 指令 (Directive) は、それ自身が EU 加盟国内において直接に法的効力を有するものではないが、EU 加盟国は EU 指令の内容に沿った国内法を制定する義務を負う。データ保護指令も EU 加盟国に同指令の内容に従った個人情報保護法を設けることを求めており、各 EU 加盟国ではデータ保護指令に沿った個人情報保護法を定めている。したがって、データ保護指令の概要を理解することで、EU 加盟国の個人情報保護法制の基本的枠組を理解することができる。

ただし、EU 指令に定められた事項には、詳細の決定を各 EU 加盟国の裁量に委ねている事項も多く、EU 指令を国内で具体化する方式や手段、解釈も一次的には各加盟国の裁量に委ねられている。このため、EU 指令に基づく国内法の内容は各加盟国で一定の違いが生じ得る。個人情報保護法についても同様であり、等しくデータ保護指令に基づくとはいえ、各加盟国の規制内容は全く同じではない。そこで、個別事案において個人情報保護法を遵守しようとするためには、適用される各国法を詳細に検討する必要がある。

(2) 適用範囲

データ保護指令は、EU 加盟国内に所在 (establishment) するデータ管理者による個人情報の取扱いについての規制を求めており、また、データ管理者が EU 加盟国内に所在しない場合であっても、国際公法の観点から法の適用が認められる場合や、EU 内の設備 (equipment) を使用した個人情報の取扱い (媒介目的の場合を除く) についても、同指令に従った規制を求めている。

具体的な適用範囲は、データ保護指令の文言からは必ずしも明確ではなく、詳細な定めは国内法に委ねられているが、EU 加盟国の個人情報保護法が、日本の会社にも適用される場合があることに留意が必要となる。

(3) 規制対象

データ保護指令下の個人情報保護制度では、個人情報の取扱者として、自らの判断で個人情報を取り扱う「データ管理者 (data controller)」と、データ管理者のために個人情報を取り扱う「データ取扱者 (data processor)」が想定されている。データ保護指令が規制の対象としているのはデータ管理者であり、データ管理者はデータ取扱者がデータ保護指令に従って個人情報を取り扱うことについて責任を負う。そして、データ管理者は監督庁への事前届出 (notification) をしなければならない。

¹ <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046>

² Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995]

(4) 個人情報の定義

データ保護指令では、「個人データ (personal data)」が保護の対象となるが、これは、コンピュータ等で自動処理される情報やアクセスが容易となるように構築されている情報のうち、特定された自然人、または、識別番号または身体的、生理的、精神的、経済的、文化的もしくは社会的な個性に係る一つまたは複数の要素によって、直接または間接的に特定可能な自然人に関する情報と定義されている³。もっとも、EU 加盟国が各々制定する国内法における個人データの定義は、データ保護指令と完全には一致していない場合がある。

また、データ保護指令は、EU 加盟国に対し、人種、民族、政治的見解、信仰、思想信条、労働組合への加入、健康または性生活等の基本的人権に深く関連する特定の情報（いわゆるセンシティブデータ）について、取扱いに本人の明確な同意を必要とするなど、特別な保護を義務付けている（同指令 8 条）⁴。なお、現行の日本の個人情報保護法ではセンシティブデータについて特別の取扱いを求めているが、平成 27 年改正の個人情報保護法では「要配慮個人情報」としてセンシティブデータについての取扱いが定められることとなった。

(5) 取扱原則

データ保護指令では、個人データの取扱いに関して以下のような取扱原則を定めている。

- ① 個人データは適法かつ公正に取り扱われなければならない。
- ② 個人データは特定された適法な目的のために取得されなければならない、利用目的に反する方法で利用されてはならない。
- ③ 個人データは、利用目的に十分かつ関連したものでなければならない、必要な範囲内のものでなければならない。
- ④ 個人データは、必要な範囲内で正確かつ、必要に応じて最新の状態に保たれていなければならない。利用目的との関連で不正確または不完全な個人データについては修正または削除するための合理的な措置がとられなければならない。
- ⑤ 個人データは、利用目的に必要な期間を超えて、本人を特定可能な状態で保持されてはならない。

³ "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

⁴ 日本の現行法では個人情報の取扱いについて情報の性質による区別はしていないが、改正法によって「要配慮個人情報」という類似の概念が導入されている。

これに加え、個人データの欧州経済領域（EEA）⁵外への移転については、次に述べるように、別途規制が強化されている。

(6) 域外移転

データ保護指令によれば、個人データを、EEA 域外であって同指令の個人データ保護と同程度の保護が保障されない国または地域へ移転（transfer）⁶すること（以下「域外移転」という。）は認められない。この点、親子会社間での個人データの移転であっても、域外移転規制の対象となる。個人データの適切な保護が認められた国であるか否かは欧州委員会が判断することとなるが、現状において、日本は適切な保護が保証された国であるとは認められていない⁷。

ただし、データ保護指令では、域外移転が認められる例外事由も定めている。

まず、データ保護指令は、本人の同意がある場合を、域外移転規制の例外として定めている。もっとも、本人の同意は、本人に移転の具体的な内容を伝えた上で、特定の移転行為に対して、同意の意思が任意かつ明確に表示されたものでなければならず、黙示の同意では不十分とされている。特に、被用者が雇用者に対して行う場合の本人（被用者）の同意は、何ら不利益を被ることなく同意を留保し又は任意に撤回することができなければならないが、雇用者と被用者の関係を鑑みて、そもそも、本人（被用者）の同意のみに依存した域外移転は推奨されていない⁸。

次に、欧州委員会が承認した標準条項を含む契約が締結された場合に係る例外であり、実務上はこの例外事由が最も重要である。これは、個人データの譲渡人と譲受人との間で、欧州委員会が承認した標準条項を含む契約を締結し、当該契約条項に従った個人データの移転がされる場合には、EEA 域外への個人データの移転であってもデータ保護指令上適法な移転として認められるというものである。なお、標準条項は、欧州委員会が承認し

⁵ European Economic Area の略であり、オーストリア、ベルギー、ブルガリア、キプロス、クロアチア、チェコ共和国、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、アイerland、アイスランド、イタリア、ラトビア、リヒテンシュタイン、リトアニア、ルクセンブルグ、マルタ、オランダ、ノルウェー、ポルトガル、ポーランド、ルーマニア、スロバキア、スロベニア、スペイン、スウェーデン、英国から構成される。

⁶ 実質的な情報の伝達を意味しており、経由（transmit）はこれに含まれない

⁷ 2015年6月現在では、アンドラ、アルゼンチン、カナダ、スイス、フェロー諸島、ガーンジー、イスラエル、マン島、ジャージー、ニュージーランド、ウルグアイのみが認められている。米国もセーフハーバー原則の適用を前提に適切な保護があるものと認められていたが、2015年10月6日に、欧州司法裁判所（CJEU）は、欧州委員会が米国と締結しているセーフハーバー協定は無効であるとする判決を下した。

⁸ Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995

た条項をそのまま使用しなければならず修正は認められない。そこで、実務上は、標準条項を契約書の一部に組み込むか、添付することが多い。

さらに、欧州委員会は、「個人データの国際移転に関するルール（Binding Corporate Rules: BCRs）に従う場合」にも個人データの域外移転を認めている。BCRsは、主要なEU加盟国の監督官庁の承認を経た、EEA域外の支店に対して個人データを移転する場合の会社間ルールであり、グループ会社間において個人データを域外移転する場合の活用が想定されている。もっとも、実務的には、この承認手続には時間とコストがかかるため、現状において利用例はきわめて少ないと言われている⁹。

このほかの例外事由として、法的主張（legal claim）¹⁰または重要な公共の利益に必要な場合、本人の重大な利益の保護に必要な場合、公開登録情報の場合などが定められている。

(7) 監督官庁等

個人情報保護法の執行のため、データ保護指令は、各EU加盟国に対して、個人データの取扱い状況を監督する独立した行政機関の設置を義務付け、当該行政機関に強力な捜査権限や執行権限を付与すべきことを定め（同指令28条）、さらには、個人情報保護法違反には制裁を科すことを求めている（同指令24条）。制裁の方法などの具体的な制度設計は各EU加盟国に委ねられているが、たとえば英国などでは、強制権限を有する情報コミッショナー（Information Commissioner's Office: ICO）は、強制捜査権限に加えて、違反行為に対して最大50万ポンドを上限とする制裁金を科す権限を有するなど、厳格な罰則が定められている。これに対し、日本の現行法下では独立した監督機関はなく、制裁金も定められていない。平成27年改正によって独立した監督機関である個人情報保護委員会が設立されたものの、制裁金は改正法でも定められていない。

(8) EU規制の改正

近年の個人情報保護に関する関心の一層の高まりを受けて、データ保護指令は数年以内に大幅な改正が行われることが予定されている。その基本的性格もEU指令（Directive）から、EU加盟国内において直接適用が認められるEU規則（Regulation）に変更され、一般データ保護規則（General Data Protection Regulation）となる予定である。新たな規則によれば、EU規則とすることによるEU圏内における規制の統一化、個人データの管理義務の強化、適用範囲の拡大、本人の権利の拡充等の個人情報保護の強化に加え、違反時の罰則についても大幅な引き上げが予定されている。特に違反時の罰則の上限は、前

⁹ EU規則への改正項目には、このBCRsの活用の推進が含まれている。

¹⁰ ただし、法的主張（legal claim）の例外は、本人に関連する訴訟の防御活動に必要な場合など場面が限定されており、将来の裁判に備えるためなどには認められるべきではないとされている（前記注8、14頁参照）。

年度全世界売上の4%又は2000万ユーロのいずれか大きい金額という極めて高額な制裁金の上限が定められる見込みである。このような新たな一般データ保護規則は2018年までに施行されることが予定されている。

3. 内部通報制度と欧州個人情報保護法制

(1) 内部通報制度と個人情報保護法

内部通報制度を導入し、通報窓口から会社の不正行為等の通報を受け付けた場合、会社が受領する情報には、通報者自身の個人情報に加えて、不正行為関与者などの第三者の個人情報が含まれる場合が想定される。通報者自身の個人情報は、本人からの直接取得であり、情報の取扱いについて個別同意が得られる場面も多く、個人情報保護法上の問題が生じるおそれは実務的には比較的小さい。一方で、通報内容に含まれた第三者の個人情報については、特にそれが不正行為に関与した者（以下「通報対象者」という。）の個人情報であった場合などには、その情報の取扱いについて通報対象者本人の同意を得ることは、そもそも期待しにくいし、調査や証拠収集の観点からも適切ではない。したがって、内部通報制度の導入及び運用に際してはこのような通報対象者等第三者の個人情報の取扱いが個人情報保護法に抵触することがないような制度設計が必要となる。

この点、内部通報制度の運用として、理論上は、通報内容が完全に匿名化され、個人情報が全く含まれない状態にすることにより、個人情報保護法の適用外とするという方向性も考え得る。しかし、それでは不正行為の調査自体が困難となって制度が機能しなくなる可能性が高く、また実際の運用に際して通報者である一般従業員が匿名化を徹底することが期待できるのかも疑問である。そうであるとすれば、実務上通報内容には個人情報が含まれることを前提とした制度設計をすべきであろう。

(2) EU加盟国内における内部通報制度

EU加盟国内の子会社において内部通報制度を設ける場合には、データ保護指令に基づいて当該加盟国が制定する個別の個人情報保護法の規制に沿ったものでなければならない。なお、欧州子会社の内部通報窓口を欧州子会社内ではなく、日本の本社に設けた場合であっても、なおデータ保護指令に基づく個人情報保護法が適用され、欧州子会社又は日本の本社がデータ管理者としての義務を負うことになり得る。そこで、EU加盟国内の子会社の従業員向けの内部通報制度を設ける場合には、データ保護指令に基づいた当該EU加盟国の個人情報保護法の規制に沿った制度設計が求められる。また、欧州子会社（その従業員）から日本の親会社（内部通報受付窓口）への個人情報の移転については、域外移転に該当することになる点に留意が必要である。

(3) 欧州委員会の意見書

ア 欧州委員会の意見書

欧州委員会は、EU 加盟国内の会社で内部通報制度を設けることに関する意見書 (Opinion)¹¹を作成して公表している¹²。同意見書は、会計、内部会計統制、監査、贈賄防止、金融犯罪防止を目的とする内部通報制度を専ら対象とするものであるとのことだが、上記以外の不正行為の通報をその目的に含む内部通報制度においても参考になる。以下に、意見書の内容を紹介する。

イ 内部通報制度に対する個人情報保護法制の適用

意見書では、まず、内部通報制度は個人データの取扱いを含む場合があるのだから、内部通報制度の導入及び運用に際しては、個人情報保護制度の遵守が必要となるということを前提として確認する。特に、一般的に各国において内部通報者を保護するための法制度 (例えば日本の公益通報者保護法) が多く存在するのに対して、通報対象者に対する保護を定めたものはないことに着目し、かかる通報対象者の個人情報保護の重要性を強調している¹³。

そして、内部通報制度そのものについては、法的義務の遵守又はデータ管理者に該当する企業の正当な利益の保護のために必要な措置として正当性が認められ得るとしつつも¹⁴、個人情報保護の観点からは、制度運用は抑制的でなければならないとし、匿名通報を許容する制度についても否定的な見解をとると共に、個人データの取扱いや保持期間についてもデータ保護指令の原則を厳格に適用すべきとしている¹⁵。

ウ 通報対象者の権利

上記のとおり、意見書では、特に通報対象者の権利を重視している。そして、データ保護指令において、本人を通じずに第三者が個人データを取得した場合には、その事実を本人は知らされなければならないとされていることを踏まえ、通報の事実は内部通報制度の責任者によって通報対象者に知らされなければならないとしている。一方で、かかる通報対象者への連絡が、通報事実の調査や証拠の収集等を阻害するおそれを踏まえ、そのようなおそれが存在する限りにおいては、その連絡が遅延することが許容されるとする。ただし、具体的な遅延及びその期間の妥当性についてはケースバイケースの判断が必要とされている。また、データ保護指令が、利用目的との関連で不正確または不完全な個人データについては修正または削除するための合理的な措置がとられな

¹¹ Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime

¹² http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf

¹³ III (意見書 6 頁)

¹⁴ IV, 1 (意見書 7 頁・8 頁)

¹⁵ IV, 2 (意見書 10 頁・11 頁)

ければならないとしていることを踏まえ¹⁶、通報事実に係る個人データについても、通報対象者が情報にアクセスし、内容の確認、訂正をする機会が与えられる必要があり、不正確又は不完全な情報を削除することができなければならないとしている。もっとも、かかる本人の権利に基づいて、通報対象者が、通報者の情報そのものにアクセスする権限までは認められないとの意見も示されている¹⁷。

エ 内部通報体制

内部通報制度の実施にあたっては、秘密保持が維持される十分な情報管理体制が確保されていなければならないとする。他方、外部の第三者への内部通報制度のアウトソースの可能性は否定しておらず、そのような場合には、契約等によって、当該第三者による適切な情報保護体制が保証されるような措置を講じる必要があるとしている¹⁸。そして、専門業者や、法律事務所、コールセンターなどに内部通報制度を外部委託する場合であっても、会社はデータ管理者としての責任を負う。したがって、外部委託業者に対し、会社との関係で、秘密管理や保持期間等に関して、データ保護指令が定める個人データの取扱原則を遵守させなければならないとする¹⁹。

オ グループ会社との情報共有

さらに、EU加盟国内の子会社が、国外のグループ会社と内部通報された情報を共有することについて、原則として各EU加盟国内に情報を留めるべきであるとしつつも、調査の必要性や組織体制によっては情報共有の必要性が認められ、秘密管理体制が維持される場合は、一定の範囲で情報の共有が許容されるとしている。もっとも、EEA域外のグループ会社と情報を共有する場合には、域外移転規制に従い、標準条項の使用等、データ保護指令が認めた方法による移転が必要であるとしている。

(4) 国内法規たる個人情報保護法

内部通報制度と個人情報保護法の関係についての欧州委員会の見解は、内部通報制度とデータ保護指令の内容に関する分析及び留意事項として参考になるものではある。しかし、上述のとおり、データ保護指令は各EU加盟国に対して同指令に沿った個人情報保護法の制定を義務付けるに過ぎず、同指令の要求事項を実現する国内法の立法は、各EU加盟国の立法機関に委ねられている。このため、各EU加盟国の個人情報保護法は基本的枠組において同様であるものの、その具体的な規制内容は、完全に一致するものではない。特に、各EU加盟国は、自らの立法判断により、データ保護指令を超えた範囲で個人情報

¹⁶ 一定の期間内の削除を求める国もある。

¹⁷ IV, 4 (意見書 13 頁)

¹⁸ IV, 5 (意見書 14 頁)

¹⁹ IV, 6 (意見書 16 頁)

を保護する法制度を導入することは可能であるため、個人情報保護に対する考え方²⁰によって、個人情報の保護レベルには EU 加盟国ごとに違いが生じている。この観点から、内部通報制度に関する規制も、EU 加盟国ごとに異なり得るところで、データ保護指令の要求事項を超えたより厳格な制度を導入している国もある。具体的には、たとえば、内部通報制度について当局からの事前承認の取得又は届出を要求する制度を有する国や、通知を受けた時点で通報対象者に対して通報内容を通知しなくてはならないと明文で定めていたり、一定期間内に通報対象者に関する情報を削除することを求めたりしている国もある（詳細や具体的運用については紙面の都合上本稿では割愛する）。そこで、内部通報制度の具体的な導入に際しては、各国の個人情報保護法の詳細及び具体的な運用を確認することが不可欠である。さらに、内部通報制度は個人情報保護法のみならず各国の労働法上の問題も生じ得るところであり²¹、これら関連する国内法規の影響も検証する必要がある。

4. 留意事項のまとめ

以上のとおり、欧州において内部通報制度を導入するに際しては、個人情報保護法制との関係で、留意すべき点がある。本項において指摘した留意点をまとめると、以下のとおりである。

- EU 加盟国において内部通報制度を導入する際には、その運用に際して、個人情報の取扱いが含まれることを前提とし、各国の個人情報保護法制に沿った制度設計が必要となる。
- EU 加盟国が定める個人情報保護法制は、データ保護指令に従ったものであり、日本よりも遥かに厳格な制度であり、違反によるリスクも大きい。
- 2018 年までに導入される一般データ保護規則では適用範囲が広がり、制裁金の上限を全世界売上の 4% 又は 2000 万ユーロとするなどの厳罰化が予定されている。
- 欧州の子会社の従業員からの、個人情報を含む内部通報を、日本の親会社が直接受け付けたり、あるいは欧州の子会社と共有したりする場合には、個人情報の域外移転が生じるため、データ保護指令が定める厳格な域外移転規制を遵守する必要がある。
- 内部通報情報に個人情報が含まれる場合には、不正行為への関与者の情報だとしても、当該対象者への通知が必要となる。
- 具体的な規制は、各 EU 加盟国が定める国内法によるため、内部通報制度を導入する各国ごとに、その法規制の内容や運用を検証する必要がある。
- 制度の導入に際しては、個人情報保護法制のみならず各国の労働法等の関連法令の

²⁰ たとえば、一般的には、フランスやドイツは、英国などと比較して、特に個人情報保護への意識が強いと言われている。

²¹ I（意見書 4 頁）参照。具体的には、内部通報制度の導入に際して、従業員への個別通知や、従業員代表等との協議を要求する国もある。

検証も必要となる。

5. おわりに

内部通報制度の導入は、グローバルなコンプライアンスを確保するために有効であるが、制度の導入及び運用によって、重大な法律違反を引き起こすのは本末転倒である。

欧州の個人情報保護制度は日本の制度とは基本的な枠組が大きく異なることに加え、その罰則は日本法よりもはるかに重い。また、欧州（特にフランスやドイツでは）、日本と比較しても個人情報保護に対する国民の意識が極めて高く、個人情報の不適切な取扱いや重大な法令違反と共に大きな社会的評価の失墜をもたらすおそれがある。

本稿は、欧州で内部通報制度を導入することを検討する際の初歩的で一般的な留意事項を概説したものにすぎない。実際に、内部通報制度をEU各加盟国において導入するには、対象国の個人情報保護法の具体的な内容及び運用を確認する必要があり、現地の専門家や欧州における内部通報制度の導入に知見を有する国内の専門業者らと十分に相談した上で、慎重な制度設計を行うことが必須となろう。

以上

<お問い合わせ先>

TMI 総合法律事務所

〒106-6123 東京都港区六本木6丁目10番1号 六本木ヒルズ森タワー23階

電話(代表)03-6438-5511 Fax(代表)03-6438-5522

<http://www.tmi.gr.jp/>

大江 修子 E-mail: noe@tmi.gr.jp TEL:03-6438-5467

波田野晴朗 E-mail: shatano@tmi.gr.jp TEL:03-6438-5604

【筆者略歴】

大江 修子（おおえ・ながこ）

http://www.tmi.gr.jp/staff/n_oe.html

1996年 早稲田大学法学部卒業

1998年 司法修習終了（50期）・弁護士登録（東京弁護士会）
虎ノ門総合法律事務所入所

2004年 ハーバードロースクール卒業(LL.M)・

Kramer Levin Naftalis & Frankel LLP(NY)にて研修（～2005年）

2005年 あさひ・狛法律事務所（現在は西村あさひ法律事務所）入所

2007年 TMI 総合法律事務所入所、翌年パートナー就任

(主な取扱い分野)

クロスボーダー取引、海外進出サポート、国内外の訴訟・紛争解決、知的財産戦略支援、知的財産権関係契約・紛争法務、労働審判・労働関係訴訟等への対応、国際相続、出入国関連、その他一般企業法務。

(主な著書)

「著作権の法律相談(第Ⅰ巻)(第Ⅱ巻)」(2016/01)、「アメリカの最高裁判例を読む-21世紀の知財・ビジネス判例評釈集-[IIP研究論集13]」(2015/02)、「M&Aを成功に導く知的財産デューデリジェンスの実務(第2版)」(2013/04)、「ソフトウェア取引の法律相談」(2013/02) 等

波田野 晴朗 (はたの・せいろう)

http://www.tmi.gr.jp/staff/s_hatano.html

2001年 東京大学法学部第二類卒業

2004年 司法修習終了(57期)・弁護士登録(第一東京弁護士会)
TMI 総合法律事務所入所

2005年 経済産業省知的財産政策室勤務

2007年 TMI 総合法律事務所復帰

2011年 ロンドン大学クイーン・メアリー卒業(LL.M.)

ロンドンのシモンズ・アンド・シモンズ法律事務所勤務

2012年 TMI 総合法律事務所復帰

(主な取扱い分野)

IT・情報・通信関連法、国際企業取引、一般企業法務、紛争(訴訟)、M&A、知的財産法等。

(主な著書・論文)

「IT・インターネットの法律相談」(2016/01/07)、「英国でのインターネット接続事業者に対する著作権侵害に基づくアクセス防止措置請求」竹田稔先生傘寿記念「知財立国の発展へ」発明促進協会(2013)「ソフトウェア取引の法律相談」(2013/02)、「個人情報管理ハンドブック(第2版)」(2008/4)、「2項推定に関する実務的論点—ごみ貯蔵機器事件を踏まえて—」知財研フォーラム100号(2015)、「親子会社間の情報管理で気をつけるべきこと」(ビジネス法務 2014) 等

掲載日：2016年2月15日