＜AIPPI セミナー開催報告＞

ＡＩＰＰＩ・ＪＡＰＡＮ欧州知財セミナー

EU 一般データ保護規則（GDPR）と新技術への影響について

1）開催日時：平成 30 年 2 月 8 日（木）13：30～17：00

2）会　　場：金沢工業大学大学院　虎の門キャンパス　11 階　1111 講義室

3）講 演 者：英国 Bristows LLP

Mark Watts 博士（英国弁護士）

Edward Nodder 氏（英国弁護士）

4）内容

1. 欧州一般データ保護規則についての基礎知識

一般データ保護規則（GDPR）は、2018 年 5 月 25 日に適用開始。全ての EU 加盟国の既存のデータ保護法に置き換わり、EU 内での制度調和が図られる。罰金が、最大、2000 万ユーロ又は世界の売上の 4%であり、非常に高い。

GDPR の日本企業への適用範囲は、①データ管理者又は処理者が EU 内に存在する（例：日本企業の子会社)。②日本企業が EU 内の個人に対して商品やサービスを提供している。③EU 内の個人の行動監視を行っている場合、が挙げられる。

各加盟国に存在するデータ保護局（DPA）のうち、一つの DPA を主当局とする制度（ワンストップショップ）となっている。

一般的な基本原則（通知義務、処理の「根拠」(例：同意)、目的限定、セキュリティ確保、欧州経済領域（EEA）外に個人情報を移転することの制限、データ主体者の権利）は、従来通りである。

域外移転の制限については、既存の制度と同様であり、①適切性決定。②適切な保護措置（拘束力のある会社のルールや欧州データ保護シール等)。③外国法の執行要件、のいずれかを満たす場合、域外への移転が認められる。

通知義務については、①正当な利益を含む処理の根拠。②保持する期間。③第三者への開示。④データ主体者の権利等、従来よりも詳細な情報を個人に通知する必要がある。

同意については、①同意をひとまとめにするのは難しくなる、②不必要な処理を条件とすることはできない等、真の「同意」の基準が高くなる。

データ主体者の権利としては、①主体者のアクセス権、②抹消される権利（管理者がやむを得ない正当な理由を示すことができない限り、抹消される権利)、③異議を申し立てる権利、④データポータビリティの権利（自分が提供したデータを、別のデータ管理者に送るために、一般に使用されている機械で読み込める形式で受領する権利)、⑤自動化された決定、があり、②と④は新規のものである。

GDPR では、新たに、データ処理者は直接的な義務の対象となった。例えば、管理者と書面による契約を締結する義務の連帯責任、セキュリティ確保、データ違反を管理者に報告、再委託前の同意、データ移転等。

GDPR では、新たに、設計上のプライバシー保護、事実上のプライバシー保護及びデータ保護インパクト評価も必要となった。設計上のプライバシー保護としては、①最初からプライバシー保護措置を前提とした設計、②匿名化等、が挙げられる。事実上のプライバシー保護としては、デフォルトでできる限りプライバシーを保護する設定が挙げられる。データ保護インパクト評価では、ハイリスクな処理について、リスクを特定し、保護措置を講じる必要がある。

GDPR では、新たなセキュリティ基準として、①「適切な」セキュリティ措置、②処理者に直接的な義務が課される、③暗号化、が必要となった。また、違反の通知については、①DPA に 72 時間以内に違反を報告、②リスクの高い違反については個人に通知、が必要である。

GDPR では、新たな説明責任として、管理者は、遵守を「説明」できなければならない。例えば、①文書化されたデータ保護のポリシーと管理状況、②リスクに応じたアプローチをとることができるかどうか、③データ保護責任者等の研修を受けた職員、等について説明できなければならない。また、管理者と処理者は、すべての処理を文書化しなければならない。

2. 一般データ保護規則と新テクノロジー

(1)新テクノロジーに関する GDPR のメリットとデメリット

新しい技術に対する GDPR のメリットとして、①適用法に関してより明確になる、②ワンストップショップ。③匿名化されたデータ、④処理目的の変更、⑤説明責任、⑥設計上のプライバシー確保、⑦プライバシーインパクト評価、デメリットとして、①個人情報の定義の広さ、②同意に関する子供の年令がハーモナイズされていない、③透明性要件が細かい、④データポータビリティの権利、⑤抹消の権利、⑥事実上のプライバシー保護、⑦事前協議、⑧データ移転の制限、⑨莫大な罰金、が挙げられる。

(2)新テクノロジーに関する GDPR 上の課題

クラウドコンピューティングに関する GDPR 上の主な課題としては、①処理者に直接課される義務、②適用法、③説明責任、④セキュリティ確保、⑤データ保護責任者、⑥データ処理の記録、⑦DPA や現地監査への協力、がある。クラウド契約に関する実務上の影響として、①契約が長く複雑になる、②処理者が契約手続を主導する範囲が広がる可能性、③コンプライアンスが販売上の主要な問題になる、④お互いがリスクに晒されるため、相互の上限設定や保障条項を設ける可能性、⑤コンプライアンスへの協力に関する規定が詳細になる可能性、⑥処理者は、義務が確実に下請けにも課されるようにすることが難しい、⑦複数層からなるクラウドの取り決めを文書化することが難しい、⑧多くのクラウドサービスにとってコンプライアンスが難しい問題として残る、ことが挙げられる。

マシーンラーニングに関連する GDPR 上の課題としては、自動化された決定がある。GDPR の下では、自動化された処理のみに基づくものであって、法的効果が生じたり、個人に重要な影響を与えるものについては、決定の対象とならない権利がある。自動化された意思決定は、①契約上の必要性がある、②十分な保護措置を含む法律に基づいて認められている、③明示的な同意がある、場合に認められる。また、個人には、①人による介入の要求、②見解の表明、③決定への異議、④使われたロジックについて「意味のある情報」の提供を受ける、権利がある。また、マシーンラーニングには、公正さと透明性に関する課題もある。例えば、アルゴリズムとトレーニングに関する公正さの課題として、①品質（埋め込まれたバイアスのリスク）、②量（データのミニマム化が規模のメリットを損ねる可能性）、③ラベリング（信用性）、が挙げられる。不透明さの課題として、①「ブラックボックス」（専門家でも説明がつかない）、②データ主体者には理解できない、③営業秘密、④第三者の要素（例：ワトソンインサイド等）、が挙げられる、GDPR において、個人は、不当なマシンから保護されなければならないとの前提に立っている。

顔認識に関する GDPR 上の課題として、①家庭内の例外、②生体識別データ（機密性の高い個人情報であり、EU 加盟国は、生体識別データについて追加要件を導入できる）、③相当性（個人情報に相当するかどうか）、④処理の根拠、登録及び同意、⑤データ保護のインパクト評価、⑥第三者の同意が必要

な可能性、⑦プロファインリング、⑧法執行アクセス、⑨データ保持、⑩忘れられる権利、が挙げられる。

IoT に関する GDPR 上の課題として、①いつ「物」に関する情報が（機密性の高い）個人情報になるか（個人情報の範囲）、②セキュリティ確保、③データ保護の基本原則と処理の合法性（目的限定とデータミニマムの問題、「同意」に基づく処理と契約上の必要性の問題、「正当な利益」の根拠の問題）、④透明性の確保、⑤「データポータビリティ」がどのように適用されるのか等、がある。

拡張現実に関する GDPR 上の課題として、①位置情報追跡、②プロファイリング、③ユーザーでないものの情報の扱い、④マーケティング、⑤プライバシーインパクト評価、⑥子供のデータ、が挙げられる。

本セミナーは、企業知財部や特許事務所にご勤務の方で欧州特許実務に携わっておられる実務者にとって、非常に有意義な内容となった。参加費：AIPPI・JAPAN 会員 5,000 円（会員以外 10,000 円）。本セミナーでは 30 名以上の参加者にお集まりいただき、成功裡に終了した。　　以上