Vol.2016-EIP-71 No.1
2016/2/19

IoT（Internet of Things：モノのインターネット）と情報保護の在り方ーEU における取り組みを参考にー

寺田麻佑[†1] 板倉陽一郎[‡2]

本論考においては，IoT(Internet of Things,モノのインターネット）に伴う諸問題を考察する．IoT に関してわが国がどのような取り組みを行っているのか，また今後どのような問題に対処する必要があるのかにつき，EU における IoT に関する政策の在り方を参考にしながら検討を行う．

IoT (Internet of Things) and the Way of Protection of Information -In Reference to the Measures in EU-

MAYU TERADA[†1] YOICHIRO ITAKURA [‡2]

In this article, various problems regarding IoT (Internet of Things) are considered. The topics include the recent update on Japan's way of treating the issues in IoT and the possible problems that we may encounter in the future. To think about the issues of IoT especially those related to the way of protection of information, this paper considers the policy and actual measures on IoT that are taken in EU.

1. IoT とは何か

IoT とは，Internet of Things の略称であり，モノのインターネットと訳される場合が多い．ネットワークの発達により，ありとあらゆる「モノ」がインターネットにつながる時代となっている．そして,「モノ」がそれぞれ繋がり,「モノ」同士が通信をおこなうことを,「モノのインターネット」（IoT：Internet of Things）という．IoT は二つの種類の通信を包含している．すなわち，モノとモノ（thing-to-thing）をを繋ぐ場合と，機械と機械（Machine-to-Machine, M2M）を繋ぐ場合である．このようなモノとモノを繋ぐ通信は，制限された範囲においても成立するし（Intranet of things），一般にアクセス可能な状況（Internet of things）においても成立する[1].

IoT はモノとモノが繋がってそれぞれの「モノ」が通信行うことであるが，そのなかで，直接的なデータ漏えいの可能性や，IoT が創り出すビッグデータそのものがプライバシー情報として企業に把握されてしまうかもしれないといった問題点を包含し，現在，様々な観点から IoT が関連する法的諸問題について，検討が進められている．

以下では，改正個人情報保護法と IoT に関する論点をみたうえで，２．において欧州の IoT 政策を検討し，最後に IoT に関する諸問題につき，欧州の政策を参考にしながら，今後どのような規則制定等が望ましいのかについて述べることとしたい．

1.1 IoT と改正個人情報保護法

IoT の進展に伴って，製品ごとに様々なセンサー等がつけられ，それらのセンサーやチップ等によって，これまでは収集できなかったような高精度の情報が大量に集められることが可能となった．

これらの情報は，ビッグデータとして，分析や調査の対象となることが期待されている．

しかし，そのようなデータが，企業にとって良いように集められてしまうのでは，消費者にとってモノを使う上で脅威となりうる．そこで，利活用等が行われるとしても，それらは法の規定にも即した適切な活用が求められることとなる．

さらに，ビッグデータ化されることが予定されていない情報等において,漏洩のリスクに関する検討も必要である．

個人情報保護に関しては，個人情報の定義を定めている条項が重要な判断要素となるところ，改正後の個人情報保護法における定義規定は以下の通りである．

（定義）
第２条 この法律において「個人情報」とは，生存する個人に関する情報であって，
次の各号のいずれかに該当するものをいう．
一 当該情報に含まれる氏名，生年月日その他の記述等（文

†1 国際基督教大学教養学部准教授
Associate Professor of Law, College of Liberal Arts, International Christian University
‡2 弁護士・ひかり総合法律事務所
Attorney at Law, Hikari Sogoh Law Offices

書，図画若しくは電磁的記録（電磁的方式（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式をいう．次項第２号において同じ.）で作られる記録をいう．第 18 条第２項において同じ.）に記載され，若しくは記録され，又は音声，動作その他の方法を用いて表された一切の事項（個人識別符号を除く.）をいう．以下同じ.）により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む.）
二 個人識別符号が含まれるもの
２ この法律において「個人識別符号」とは，次の各号のいずれかに該当する文字，番号，記号その他の符号のうち，政令で定めるものをいう．
一 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字，番号，記号その他の符号であって，当該特定の個人を識別することができるもの
二 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ，又は個人に発行されるカードその他の書類に記載され，若しくは電磁的方式により記録された文字，番号，記号その他の符号であって，その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ，又は記載され，若しくは記録されることにより，特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの
３ この法律において「要配慮個人情報」とは，本人の人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう．
４ この法律において「個人情報データベース等」とは，個人情報を含む情報の集合物であって，次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く.）をいう．
一 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
二 前号に掲げるもののほか，特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの
５ この法律において「個人情報取扱事業者」とは，個人情報データベース等を事業の用に供している者をいう．ただし，次に掲げる者を除く．
一 国の機関
二 地方公共団体
三 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）第２条１項に規定する独立行政法人等をいう．以下同じ.
四 地方独立行政法人（地方独立行政法人法（平成 15 年法律第 118 号）第２条第１項に規定する地方独立行政法人をいう．以下同じ.）
６ この法律において「個人データ」とは，個人情報データベース等を構成する個人情報をいう．
７ この法律において「保有個人データ」とは，個人情報取扱事業者が，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって，その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は１年以内の政令で定める期間以内に消去することとなるもの以外のものをいう．
８ この法律において個人情報について「本人」とは，個人情報によって識別される特定の個人をいう．
９ この法律において「匿名加工情報」とは，次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって，当該個人情報を復元することができないようにしたものをいう．
一 第１項第１号に該当する個人情報 当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む.）．
二 第１項第２号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む.）．
10 この法律において「匿名加工情報取扱事業者」とは，匿名加工情報を含む情報の集合物であって，特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの（第 36 条第１項において「匿名加工情報データベース等」という.）を事業の用に供している者をいう．ただし，第５項各号に掲げる者を除く

改正個人情報保護法においては，従来の定義規定文言に加えて，「個人識別符号」（法 2 条 1 項 2 号，2 項）という概念が定められた．個人識別符号該当性については，様々な議論が交わされており，個人情報保護委員会における政令と併せて判断する必要がある[2].

さらに，今般の改正によって新たに定められた匿名加工情報（2 条 9 号）の在り方も問題となる．

今後，どのように個人情報を取り扱っていくのか，IoT に関連するリスクに関してどのように考えていくべきなのかについては，改正個人情報保護法の下で制定される，個人情報保護委員会の規則による基準（36 条 1 項）と併せて

検討していく必要がある.

2. IoT に関する欧州の政策

IoT に関する欧州の政策を検討するにあたり，以下，先ず，欧州委員会が 2009 年に出した「モノのインターネットー欧州のためのアクション・プラン」とする報告書の内容をみたうえで，その後の IoT に関する欧州委員会のコンサルテーションと政策の動向を踏まえ，データ保護機関の 2010 年の会議における IoT に関する意見をまとめ，次に，欧州連合（EU）のデータ保護指令第 29 条作業部会（Article 29 Working Party）による IoT に関する意見をまとめ，さらにデータ保護プライバシー・コミッショナー会議において出された「モノのインターネットに関するモーリシャス宣言（2014 年 10 月 14 日第 36 回会議）」の概要をまとめたうえで，欧州データ保護規則案に盛り込まれる予定の IoT 関連の保護規定をまとめることとする.

2.1 2009 年の「モノのインターネットー欧州のためのアクション・プラン」

欧州委員会は，2009 年に「モノのインターネットー欧州のためのアクション・プラン」とする報告書を発表した[3]. この報告書においては，欧州委員会が今後取り組むべき課題が 14 アクション示された. それらの例は以下の通りである.

１． ガバナンス
　欧州委員会は，IoT のガバナンスにとって必要な原則を策定するために，すべての関係するディスカッションや決定や会議等のイニシアチブを取り，また，促進する．さらに，分散型管理に関するアーキテクチャを設定することに取り組む.

２． プライバシーとデータの保護
　欧州委員会は，プライバシーと個人情報の保護に関する法的な問題を含めた問題に関して，継続してモニターを行なう.

３． 「チップの沈黙」
　個人がそれぞれのネットワーク環境から，いつでも離脱可能であるべきとする「チップの沈黙」を保障するための技術や法的な根拠の検討を行う.

４． 今後現れるリスクの識別
　欧州委員会は，IoT の信頼性や社会への受容，セキュリティの確保に必要とされる課題を明らかにし，必要な措置を講じる.

５． 経済と社会にとって不可欠な資源としての IoT
　欧州委員会は，IoT を欧州域内の経済そして社会にとって不可欠な資源として位置づける.

６． IoT に一定の標準・基準を備えることを要求することの検討（ITU や ISO などの標準化団体等が関係するもの）
　欧州委員会は，IoT に関する標準（基準）の作成を，標準化機構・機関に要請する.

７． IoT に関する研究プロジェクトへの資金援助とその研究の発展
　欧州委員会は，研究開発枠組みプログラムにおける IoT 分野の研究開発プロジェクトへの資金援助を行い，IoT に関する研究を発展させる.

８． ＰＰＰ（パブリック・プライベート・パートナーシップ）の推進
　欧州委員会は，IoT が重要な役割を果たすことが出来る 4 つの公私協働プログラムを推進する.【既に欧州経済再生プランで欧州委員会より提案されていた，グリーンカー，エネルギー効率の高い建物，未来の工場（委員会提案）に加え，未来のインターネットプロジェクトを追加する.】

９． イノベーションとパイロットプロジェクト（技術革新）
　欧州委員会は，競争と革新に関する枠組みプログラム（ＣＩＰ）を通じて，気候変動やデジタル・デバイドに対応する IoT アプリケーションのパイロットプロジェクトを開始する.

１０． 各関連機関の認識の向上
　欧州委員会は，他の欧州の機関（欧州議会，欧州理事会，欧州経済社会委員会，データ保護指令第 29 条作業部会）や関係する機関に，IoT の発展について定期的に報告を行う.

１１． 国際的対話
　欧州委員会は，IoT に関する情報の共有や共同事業を推進するために，国際的なパートナー機関と積極的に対話を行う.

１２． 環境対応
　欧州委員会は，廃棄物産業の恒常的監督のためのＲＦＩＤタグの活用等について，タグの利点等を検討する研究を行う.

１３． 統計
　欧州統計局（Ｅｕｒｏｓａｔ）は，ＲＦＩＤ技術の使用に関する統計報告の出版を開始する．また，IoT 関連の技術の導入の監視に関して，そのインパクトを計算する

１４． 発展状況の評価
　欧州委員会は，欧州レベルにおいてその代表的なステークホルダーとの会合を開催し，マルチステークホルダープロセスを開始し，IoT の進展状況を把握する.

上記のアクション・プランは RFID タグの利用状況を含めて，IoT に関して起こりうるリスクに関して様々な項目を取りあげている.

IoT に関する上記アクション・プランが出された時点（2009 年）においては，当該プランの中においても，「IoT はまだそれほど現実化していない」と評価されていた．

しかし，その後インターネットにつながる製品の割合は市場において増大し，IoT に関する諸問題がより強く意識されるようになってきた．2009 年から 6 年以上が経過した現在においては，IoT は技術の発展に伴う問題のなかでも，情報（データ）漏洩のリスクとも関連して，電子機器（IoT に関連した機器）の消費者の保護の観点から，最も対応すべき問題の一つとなっている．

2.2 欧州委員会におけるその後の IoT に関するコンサルテーションと政策

2009 年のアクション・プランを踏まえて，欧州委員会においては，プライバシーと情報（データ）保護の関係や，IoT インフラストラクチャーのセキュリティの問題などについて，マルチステークホルダー（企業，団体，政府機関，個人等）から意見が聴取された．

もっとも，欧州委員会が行ったコンサルテーションにおいては，IoT に関する政策に関する意見が分かれていた．

すなわち，多様なステークホルダーのうち，産業界からは，IoT に関する産業の成長の妨げとなるような規制への反対意見が出され，反対に，消費者団体や個人等からは，データの保護やセキュリティの確保に関してしっかりとし対策を取るべきであるといった意見が出されている[4].

このように政策論が対立している状況ではあるが，利害の調整を図るために対話は続けられている．

2.3 2010 年の欧州データ保護機関による，プライバシー・コミッショナー国際会議における IoT に関する意見[5]

2010 年 4 月 29 日にプラハで開かれたプライバシー・コミッショナー国際会議における，欧州データ保護機関による意見の概要は，以下の通りであった．

・情報の流通に関する同意がしっかりと取られるべきであり，特に RFID（Radio Frequency Identification）が頻繁に利用されるようになってきている現状に鑑みて，オプトアウトによって同意を取る方法は欧州データ保護指令の枠組みによって求められる「同意」とは認められないものである．

・欧州データ保護指令第 29 条作業部会は IoT に関する法律や原則の適用に関して積極的な役割を果たしていくべきである．

・企業の説明責任と，製品に関するプライバシー・バイ・デザインが IoT が製品等の初期設定の段階から，プライバシー問題に対応することのできることとなる基盤を作る．

・ＲＦＩＤタグは，一番初めの販売の段階においては，すべての機能を解除されているべきである．

ＲＦＩＤとは，ＲＦＩＤタグと呼ばれる媒体に，モノや人の個別の情報を記録し，それらを無線通信によって書き込む自動認識システムのことをいい，わが国においては電車等の電子券に利用されていることが多いものである．

かかるＲＦＩＤに関する議論を含めて，まだ IoT に関するリスクの議論がそれほど認識されていなかった 2010 年 4 月の段階において，欧州データ保護機関が国際会議で示した認識は注目に値するものである．

2.4 欧州連合（EU）のデータ保護指令第 29 条作業部会（Article 29 Working Party）による IoT に関する意見

欧州連合(EU)のデータ保護指令第 29 条作業部会(Article 29 Working Party）は，2014 年 9 月に意見を公表した[6]. この作業部会は，データ保護指令（Directive 95/46/EC）に基づいて設立された，データ保護とプライバシーに関する独立した諮問機関である[7].

この意見によれば，IoT のシステムに内在するデータ保護に関係するリスクの認識から，消費者は製品のライフサイクル全般にわたって，その製品がどのような情報を有するかについて，その内容を知る権利があり，ＥＵに関わる企業はすべからく，情報の提供等については消費者の希望する通りに，その提供を行うべきであるとされた．

また，無料かつ安全に情報を常に提供されるという個人の権利の拡張は，モノへの信頼と，革新的な技術発展の鍵となるものであり，関連する企業や製品の提供者が，このような情報の提供に関する消費者の期待に応えることが，今後の競争環境の中でも利点となっていくものである，という．

さらに，IoT に関して問題となりうる製品からの情報漏れ等に関し，リスクに消費者が悩まされないよう，可能な限りの最大の保証が，利害関係者から消費者に対してなされるべきであり，特に情報の流通に関しては，必ず消費者が情報を提供されるように制度を設計すべきであるとしている．

そして，IoT に関して起こりうる様々な問題に対して，ＷＰ29（29 条作業部会）は今後も発展の推移を見守り，国内・国際を問わない各種規制機関や，法制定関係者と協力をしていくと発表している．

ＥＵの 29 条作業部会は以上のように強い意見を発表しており，今後，ガイドライン等などによる枠組み作りだけではなく，国際的に流通するインターネットにつながった様々な製品の規格のうち，少なくともＥＵ域内に提供され

るものやＥＵ域内で製造されるものに関しては，消費者を守るための厳しい基準が法律的に設けられていくことになることが予測できる．

2.3 モノのインターネットに関するモーリシャス宣言（2014 年 10 月 14 日第 36 回データ保護プライバシー・コミッショナー国際会議）

世界各国におけるプライバシーとデータ保護に関する監督官庁関係者や有識者等が集まる国際会議であるデータ保護･プライバシーコミッショナー国際会議において, 2014 年（第 36 回），IoT に関して検討が行われ，モノのインターネットに関する宣言[8]が採択された．

この宣言においては，以下の観察と結論が示された．

・IoT に接続する機器から獲得されるビッグデータの取扱いは, 様々な問題を引き起こす. そのようなデータ全体は, 量的にも質的にも増加してきているところ，かかるビッグデータの識別性と保護は既に大きな挑戦となってきている．このようなデータは，パーソナルデータとして取り扱われるべきである．
・IoT の価値は，機器が創り出しているものではなく，IoT に関係する新たなサービスとデータに存在しているものである．
・透明性の重要性：IoT 関連機器を提供する者は，それら機器が収集するデータがどのような目的で，どのような期間保管され，利用されるのかについて明らかにするべきである．製品の提供者は，消費者を驚かせるような（データ収集等の）仕様は除去すべきである．IoT 関連機器やアプリケーションを購入する際に, 消費者には, 適切で十分な, そして理解しやすい情報が提供されるべきである．

現実に利用されているプライバシー・ポリシーは，明確かつ理解しやすい方法で情報を提供しているものとは言えない．そのような理解しにくいポリシーの上に成り立つ「同意」をもって，インフォームドコンセントが成立したと言うべきではない．それぞれの会社は，プライバシー・ポリシーがもはや,「会社」を訴訟から守るための手段ではなく，消費者を守るものであることへの意識の変化を経験する必要がある．
・プライバシー・バイ・デザインが，変わったものであるともはや認識されてはならない．革新的な技術を販売する際の，重要な販売の要素とならなければならない．
・IoT は多くのセキュリティー問題を提示する．単純なファイアーウォールはもはや有効ではない．リスクを最小にするために，データはその接続端末そのものの上で処理されるべきである（ローカル端末処理）．もしも，ローカルな処理が難しい場合には，それぞれの会社は，データの保護のために，機器や端末の暗号化を保証すべきである．
・データ保護及びプライバシーに関する監督官庁は，IoT の発展を引き続き監視し，もしも関連する法律が侵された状況が発見された場合には，適切な法執行を，監督官庁が統一して，もしくは国際協力の手段によって，なすべきである．
・IoT に関係するすべての者は，IoT の適用と IoT から得られるビッグデータに関する建設的な議論に関わり，取りうる選択肢について認識を高める必要がある．

かかるモーリシャス宣言からは，IoT に関して生じうるリスクについて，製品等を提供する企業側に最大限の配慮を求め，かつ，企業等が取得しうる情報について，これまでのプライバシー・ポリシーのような条項による同意の取り方ではなく，情報提供の在り方も含めて詳細な，しっかりとした同意を取ることが求められていることが分かる．

より分かりやすい，消費者が製品に関連するデータに関してコントロールを及ぼすことを可能とするようなデータの移転が IoT に関して求められている．

2.4 欧州データ保護規則案と IoT 関連条項

1995 年に採択され, 1998 年に発効した欧州データ保護指令は，個人の基本的人権と自由の保護を目的とするものであり，特にその 25 条において，ＥＵ域内の企業等から，ＥＵからみて十分なレベルのパーソナルデータ保護措置を設けていない国の企業等へのパーソナルデータの移転を禁止している[9].

かかる欧州データ保護規則について，新たな技術の発展等に即した規則とするために, 現在議論が進められており, 2017 年に新たな規則案が施行される予定となっている．

なお，欧州データ保護規則案は 2012 年 1 月に公表され, 2014 年 3 月に欧州議会において修正案が採択され，さらに 2015 年 6 月に欧州連合理事会修正案が合意された状況にある．

かかるデータ保護規則案のなかで，IoT に関係するものとして新たに導入が予定されている権利としては，１）忘れられる権利，２）データ・ポータビリティの権利，３）プライバシー・バイ・デザイン，などがある[10].

それらは具体的には以下の通りの権利や考え方である．

１）　忘れられる権利（Right to be forgotten）とは，同意して収集されたデータの保存期限が切れた場合や，本人がデータの消去を要求した場合に，当該本人のデータの消去を行うことを権利として認めるものである（規則案 17 条）．
２）　データ・ポータビリティの権利とは，サービスや製品等の利用者が，他の事業者等にサービス等を

切り替える場合に，切り替える前の元の事業者から個人データを入手し，移転することができることを保障する権利である（規則案 18 条）．

3） プライバシー・バイ・デザインとは，サービス等の導入や製品の製造の際に，その設計の段階から，あらかじめプライバシーの対策を講じることであり，規則案においては，プライバシー・バイ・デザインが原則となるべきであることを提案している（規則案 30 条 3 項）

欧州データ保護規則の中に上記の権利等が組み込まれることによって，欧州の製品等に関する IoT 関連の規制がより整備されることとなろう．

3. IoT に関する今後の対応—おわりに

欧州の IoT に関する政策は，消費者が情報をはじめから最後までコントロール可能とすることを目標として，リスク低減措置を様々な観点から検討しているものと評価できる．

IoT はバズワードでもあるが，インターネット接続の常態化，製品市場の中での発展によって，これからますますモノのインターネット（IoT）が組み込まれた製品が作られていくことが容易に想定される．あらゆる情報が名寄せされ得る他，当然に，情報流出によって生じるリスクをも避ける制度設計が求められることになる．

我が国においては，個人情報保護法が番号法の制定とともに改正され，IoT に対応する法的規制又は運用上の方策もこれから整備されていくこととなる状況である．個人情報保護委員会が設置されたわけだが，同委員会が旗振り役となるのか，従来の主務官庁である経済産業省や総務省が振興策を絡めた方策を編み出すのか，試行錯誤の最中である．

モノとモノがインターネットで繋がっているということは，モノが国境を越えて繋がっていくことも意味する．越境が身近な欧州において整備されようとしている様々な IoT 関連の法的基盤は，輸出等においてはもちろん遵守しなければならない条項となるうえに，国際標準となる可能性もあるため，今後も参考にされよう．国際的な情勢をみつつ，我が国においても，情報の利活用の中で，IoT に関してリスクを負う消費者保護の仕組みの構築が望まれる．

参考文献

[1] Commission of the European Communities, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Internet of Things-An action plan for Europe*, COM(2009) 278 final., p.2.
[2] 日置巴美・板倉陽一郎『平成 27 年改正個人情報保護法のしくみ』（商事法務，2015 年）37 頁．
[3] Commission of the European Communities, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Internet of Things-An action plan for Europe*, COM(2009) 278 final.
[4] http://ec.europa.eu/.../newsroom/cf/dae/document.cfm?doc_id=1746 (2016 年 1 月 25 日最終閲覧)
[5] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Internet_Things_EN.pdf (2016 年 1 月 25 日最終閲覧)
[6] Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, Adopted on 16 September 2014, WP 223.
[7] http://ec.europa.eu/justice/data-protection/index_en.htm (2016 年 1 月 25 日最終閲覧)
[8]36th International Conference of Data Protection and Privacy Commissioners, *Mauritius Declaration on the Internet of Things*, Balaclava, 14 October 2014. http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf (2016 年 1 月 25 日最終閲覧)
[9] See, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[10] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM(2012) 11 final.