EUデータ保護規則案の動向と個人データ越境移転

株式会社国際社会経済研究所　情報社会研究部 主任研究員　小泉（こいずみ）　雄介（ゆうすけ）

1. はじめに：グローバルな個人データ保護動向

急速なICTの進歩やグローバル化の進展によって、クラウドコンピューティング等において大量のデータが国境を越えて流通するようになり、またSNSなどオンラインサービスにおいて個人が自分のデータを公開したり、スマートフォンや監視カメラ、ウェアラブル端末等、企業が個人からデータを収集する手段が多様化している。このような個人データを取り巻く環境変化を受けて、EUや米国、OECD、APEC、欧州評議会などにおいて、全世界的に既存のデータ保護制度の見直し作業が進められている（表1参照）。また、2013年6月に元NSA職員スノーデン氏の証言によるPRISM*1の発覚の影響を受けて、ロシア、中国、ブラジル等の国々ではデータローカライゼーション*2と呼ばれる動きも生じている。

■表1. 全世界的なデータ保護制度見直しの動き

EU	・1995年　EUデータ保護指令 採択 ・2012年1月　EUデータ保護規則案 公表 ・2014年3月　EU規則案欧州議会修正案の採択 ・2015年6月　EU規則案欧州連合理事会修正案の合意
米国	・1974年　プライバシー法（連邦行政機関を対象）制定 ・民間分野は自主規制中心（医療、金融、教育等を除く） ・2012年2月　消費者プライバシー権利章典 公表 ・2012年3月　FTCのプライバシー・フレームワーク公表 ・2015年2月　消費者プライバシー権利章典法案 公表
OECD	・1980年　プライバシーガイドライン 採択 ・2013年7月　プライバシーガイドライン改定
APEC	・2004年　APECプライバシー・フレームワーク 採択 ・2011年　越境プライバシールール（CBPR）採択 ・2014年4月　日本のCBPRへの参加が認められる
欧州評議会（CoE）	・1980年　個人データ保護条約第108号　採択 ・2012年11月　同条約見直し案を諮問委員会が採択 ・2014年12月　データ保護アドホック委員会が見直し案を承認
日本	・2003年　個人情報保護法 制定 ・2014年6月　パーソナルデータの利活用に関する制度改正大綱 ・2015年9月　個人情報保護法改正法 成立

我が国でもデータ利活用に向けたルール明確化及び海外制度との国際的調和という産業界からの要請を受け、2013年9月からIT総合戦略本部パーソナルデータ検討会において個人情報保護法の見直しが行われ、2015年3月に改正法案が国会提出された。当初は6月初旬に参議院で可決され、改正法案成立となる予定であったが、6月1日に日本年金機構が公表した年金情報漏洩事件の影響によって、与野党合意により審議見送りとなっていた。その後、8月28日に修正法案が参議院で可決され、9月3日に衆議院で可決、成立した。今後は2016年1月に第三者機関である個人情報保護委員会が設置され、1月以降に政令や委員会規則が制定される。改正法が全面施行されるのは2017年の見込みである。

本稿では、EUにおけるデータ保護法制改定の動向と、EUからの個人データ越境移転を中心とした日本企業にとっての課題について記載したい。

2. EUデータ保護指令の改定（EUデータ保護規則案）

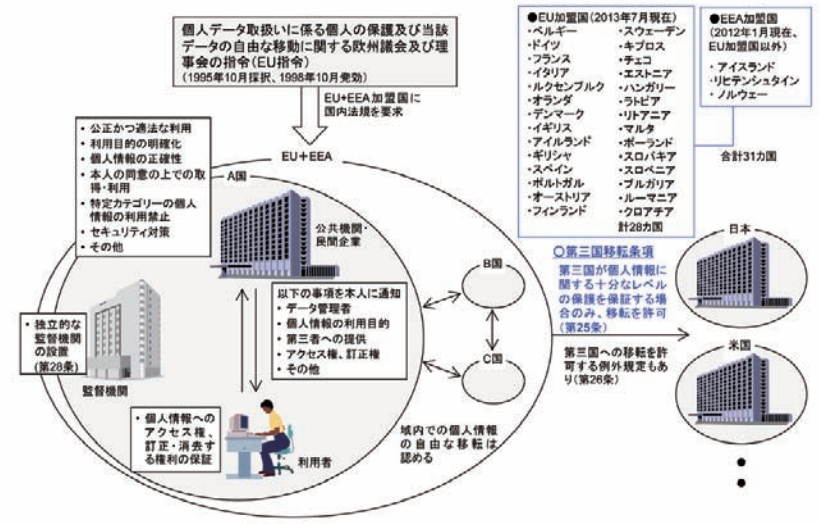
2.1　EUデータ保護指令

EUデータ保護指令（EU指令）*3は1995年に採択され、1998年に発効している。個人の基本的人権と自由を保護し、かつ加盟国間でのデータの自由な流通を妨げないことを目的としている。EU加盟国及びEEA（欧州経済領域）加盟国合計31か国に対して同指令に基づく国内法規を要求するものである。その第25条において、EU域内の企業等から十分なレベルの個人データ保護を講じていない第三国の企業等への個人データの移転を禁じているため（第三国移転条項）、データ保護の分野では極めて影響力の強いフレームワークとなっている。

2.2　EUデータ保護指令改定の背景

2012年1月25日に欧州委員会からEU指令の改定案が提出

＊1　米国政府による米国インターネット企業からの個人データ収集プログラム。
＊2　自国民の個人データを自国内のデータベースに保存することを企業に義務付ける動き。
＊3　正式名称は「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95／46／EC指令」。



■図1．EUデータ保護指令の概要

されたが、これは近年の以下のような課題に対処するためのものである。

①急速なICT技術の進歩とグローバル化の進展と、それによるリスクの拡大

②現行のデータ保護スキームに対する企業の不満の増大

－　多国籍企業にとって負担が大きい非効率・非整合的な規制の緩和要求の増大*4

欧州のあるデータ保護監督機関によれば、①については、EU市民や監督機関にとっての懸念はとりわけ下記二つの国であるという。

●米国：

一つは、全世界の消費者から個人データを収集する米国の多国籍企業である。欧州委員会がEUデータ保護規則案に「忘れられる権利」や域外適用条項、高額な課徴金などEU指令よりも厳しい規定を盛り込んだ一つの理由がこのような米国企業であり、ここには、純粋なデータ保護の観点のほかに、非関税障壁の観点も含まれているという。

もう一つの懸念材料は、9.11後に制定された米国愛国者法（PATRIOT法）によって裁判所の関与無しに米国企業の現地法人（欧州現地法人など）からデータ収集できる米国政府である。

●データ保護法の整備されていない新興国（中国など）：

欧州企業が低賃金・低価格を理由に、新興国の企業にデータ処理の委託（オフショアリング）を行った場合、データ保護法が整備されていないため、EU市民の人権が十分に保障されない恐れがある。

2.3　EUデータ保護規則案と日本企業への影響

上述の背景を受け、2012年1月に提出されたEUデータ保護指令の改定案は、EUデータ保護規則案（EU規則案）と指令案の二つから成る*5が、主要な条項を含むのはEU規則案*6である。EU規則案では、従来の「指令（Directive）」から「規則（Regulation）」に格上げがなされている。規則への格上げにより、EU法を加盟国へ直接適用し、EU域内でのデータ保護ルールの一元化が図られることとなった。現行のEU指令では国内法規を各国で制定する必要があるため、アイルランド・英国は規制が緩く、ドイツ・フランスは厳しいというEU内の温度差があり、データ保護上の不均衡のみならず、企業立地条件面での不均衡ともなっていた。

EU規則案の日本企業への影響は、大きくは以下の三つがある。

＊4　EU指令の下では、加盟国ごとに異なる国内法や、各国の監督機関の決定を遵守する必要があった。管理者は原則として全てのデータ処理内容を監督機関に通知する義務があった。また、BCR（拘束的企業準則）の承認には三つの監督機関のレビューが必要だった。

＊5　一般的なデータ保護のフレームワークを規定した規則案と、犯罪の防止・捜査・発見・訴追、刑事罰の執行の目的で処理される個人データの保護に関する指令案。

＊6　正式名称は「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則の提案」。

①EU域内から第三国へのデータ移転（第三国移転条項）

現行のEU指令と同様、EU規則案においてはEU域内から十分なレベルの個人データ保護を講じていない第三国への個人データ移転が禁じられている。日本はデータ保護レベルの十分性を未だ認められていない、すなわち十分性認定を受けていないため、EU域内からデータ移転を受ける日本企業は個別に「標準契約条項*7」を利用したり、企業グループ内で効力を持つ「拘束的企業準則（Binding Corporate Rule：BCR）*8」を採用したり、もしくは本人からデータ移転に関する同意を取得するといった措置を講じる必要がある。

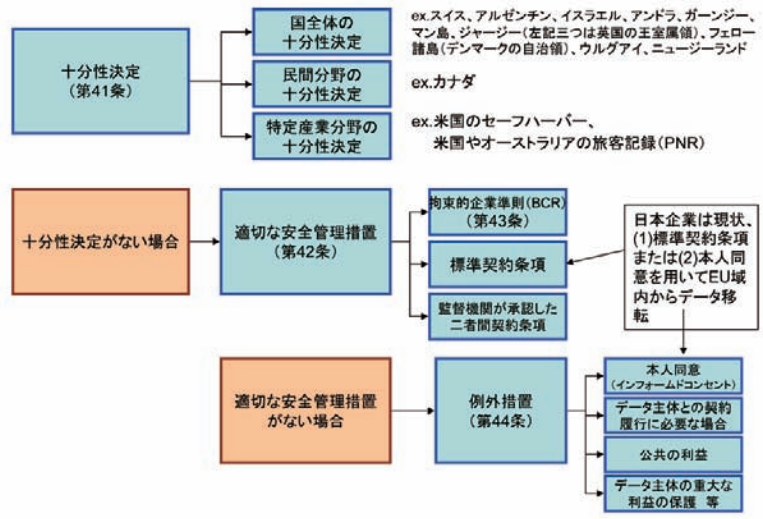
EUからデータ移転にあたってデータ保護の十分性を認められている国は、スイス、カナダ、アルゼンチン、イスラエル、ウルグアイ、ニュージーランド等があり、また米国は特例としてセーフハーバー協定*9をEUと結んでいる。日本は個別企業の自助努力（標準契約条項の利用等）によって粛々とEUからのデータ移転を受けているのが現状だが、中長期的に見れば産業界全体として大変な労力・コスト負担であり*10、このままでは十分性認定*11を受けた上記の国々の企業に比べて著しい不利益を被ることとなる。

②域外適用条項の新設

EU域外企業がEU居住者に直接的に商品・サービスを提供する場合、EU域内でデータ処理を行っていなくても、EU規則が当該企業に域外適用されるという条項（第3条2項）が新設された。域外のオンラインサービス企業、パーソナルクラウド企業、オンライン広告企業、スマホアプリ企業等がこの条項の対象になると考えられる。

③EU域内企業に対する義務の強化

その他、EU域内企業（日本企業の現地法人含む）に対しては、データを収集する個人からの明示的な同意の取得、本人がデータ消去を求めた際の「忘れられる権利（right to be forgotten）」の保障、データ違反時（漏洩等）の監



■図2.　EU規則案における第三国へのデータ移転方法

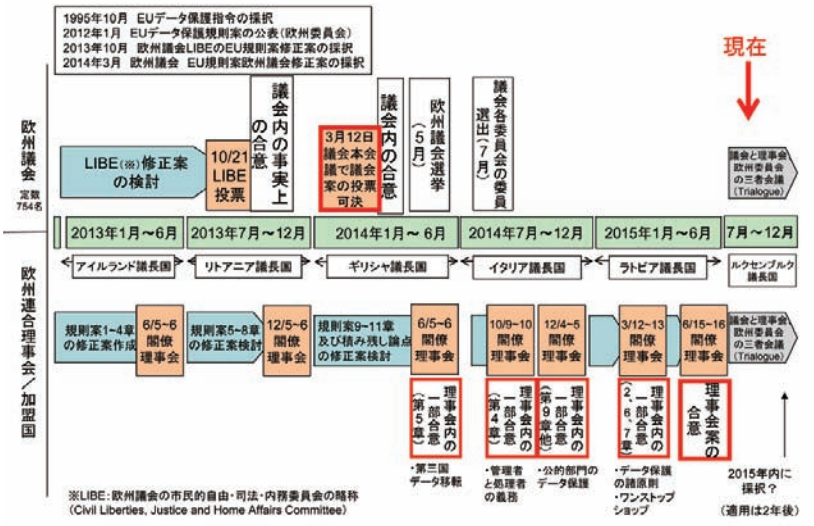
＊7　EU域内企業と域外企業の間での個人データ移転を対象とする。両者間でこの標準契約条項を含めた契約を締結する。

＊8　多国籍企業の企業グループ内での個人データ移転を対象とする。2015年7月20日時点で、全世界で70の企業グループがBCRの承認を取得しているが、日系の企業グループは未だない。

＊9　セーフハーバー7原則を遵守すると自己宣言する米国企業に対して「十分なレベルの保護」を行っていることを認める協定。

＊10　標準契約条項の問題点は、相手企業ごと・案件ごとに締結が必要、弁護士費用等のコスト、監督機関の承認に時間がかかる、欧州企業に日本企業側のデータ取扱いに関する責任が発生することなどが挙げられる。また本人同意の問題点は、消費者全員の同意取得は困難、従業員データでも国により労働組合の同意が必要であることなどが挙げられる。また本人同意に基づく従業員データ移転の妥当性については欧州内でも議論がある。

＊11　個人情報保護法改正法の改正条項のうち、個人情報保護委員会の設置、要配慮個人情報の導入、小規模事業者の除外規定削除、第三国移転の制限等については、EUからの十分性認定取得を主な理由とする改正と考えられる。



■図3.　EUデータ保護規則案の審議スケジュール

督機関や本人への報告義務、データ保護オフィサーの設置等の義務の強化に加えて、罰則（課徴金）が強化された。

2.4　EUデータ保護規則案の審議状況

欧州委員会によるEU規則案の提出後、EUの立法機関である欧州議会と欧州連合理事会でそれぞれ審議されている。下院にあたる欧州議会では2014年3月に議会修正案が採択され、上院にあたる欧州連合理事会でも審議が続けられてきた。理事会での審議は遅れていたが、ようやく2015年6月15日の司法・内務閣僚理事会（JHA）において理事会修正案が合意された。これで議会案と理事会案の両方が出揃ったことにより、同年6月24日から欧州議会・理事会・欧州委員会による非公式の三者会議（トライローグ）が開始され、2015年内の三者合意が目標とされている。

2.5　欧州委員会提案、欧州議会案、理事会案の比較

EUデータ保護規則案のうち、日本企業にとっての影響が大きい「EU域内から第三国へのデータ移転」と「域外適用」に関連する条項について、欧州委員会案（2012年1月）*12、欧州議会修正案（2014年3月）*13、欧州連合理事会修正案（2015年6月）*14の三者を比較分析した。

(1)　第42条　適切な安全管理措置による第三国へのデータ移転

■表2.　第42条についての比較

	欧州委員会案（2012年1月）	欧州議会案（2014年3月）	欧州連合理事会案（2015年6月）
第42条 適切な安全管理措置による第三国へのデータ移転	・欧州委員会による十分性認定がない第三国への個人データ移転は、以下の安全管理措置がある場合に可能。 (a) BCR (b) 欧州委員会に採択された標準契約条項 (c) EU加盟国の監督機関に採択された標準契約条項 (d) EU加盟国の監督機関にオーソライズされた契約条項	・欧州委員会による十分性認定がない第三国への個人データ移転は、以下の安全管理措置がある場合に可能。 (a) BCR (aa) 有効な「欧州データ保護シール」（EU域内の管理者および第三国の受領者におけるもの） (b) 欧州委員会に採択された標準契約条項 (c) EU加盟国の監督機関に採択された標準契約条項 (d) EU加盟国の監督機関にオーソライズされた契約条項	・欧州委員会による十分性認定がない第三国への個人データ移転は、以下の安全管理措置がある場合に可能。 (o) 公的機関間での法的拘束力のある文書 (a) BCR (b) 欧州委員会に採択された標準契約条項 (c) EU加盟国の監督機関に採択された標準契約条項 (d) 承認された行動規範（第三国の受領者におけるもの） (e) 承認された認証制度（第三国の受領者におけるもの）

＊12　http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
＊13　http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN
＊14　http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/

当初の委員会案は、適切な安全管理措置によるデータ移転の手段として、現行指令と同様のBCRや標準契約条項等のみが挙げられていた。これに対し、議会案と理事会案の双方には、日本のJEITA（一般社団法人電子情報技術産業協会）の意見*15等を反映する形で、「データ保護シール（認証制度）」が追加されている。

議会案が欧州で単一の「欧州データ保護シール」を規定し、当該シールの取得をEU域内企業と第三国の企業の両者に求めるのに対し、理事会案は複数の認証制度／シール制度の共存を許容するものであり、かつ当該認証制度の取得を第三国の企業のみに求めるものとなっている。これらの点で、理事会案の方が日本企業にとって望ましい案となっている。

(2) 第39条　認証

委員会案では認証制度について具体的な内容は記載されておらず、詳細は欧州委員会の委任法令等で定めるとされている。それに対し、議会案と理事会案では認証制度について具体的な内容が記載されている。

議会案では欧州で単一の「欧州データ保護シール」の認証手続きについて具体的な規定がなされている。EU各国の監督機関が企業を認証するというものであり、認証の有効期間は最大5年間である。他方、理事会案は複数の認証制度を許容するものであり、EU各国の監督機関から認定を受けた認証機関が企業を認証するという構造が規定されている。また、認証の有効期間は最大3年間である。両者を比較すると、より多様な認証制度を許容するという点で、理事会案の方が日本企業にとって好ましい案となっている。

(3) 第3条2項　域外適用

委員会案では、例えば日本ドメインの日本語のショッピングサイトで、EU居住者がたまたま商品を注文し、個人情報を入力してしまったような場合も、第3条2項の対象となるのかが曖昧であり、日本のオンラインサービス事業者等にとって法的不確実性が高い規定となっていた。

これに対し、議会案では前文（20）において、域外適用にあたっては、EU域外企業がEU居住者に商品・サービスを提供するという意図が明白かどうかを確認するべきという文章が追加された。

更に、理事会案では欧州司法裁判所のアルペンホフ判例に基づき、前文（20）において域外適用の基準をより明確化した。すなわち、EU域外企業のサイトで使われている言語（ドイツ語を使っている場合等）や支払通貨（ユーロ、ポンドを使っている場合等）、サイトにEU向けのサービスと言及していること等が、域外適用の対象となることの条件であることが明確になり、日本企業にとっての法的不確実性は低減されることとなった。

■表3.　第39条についての比較

	欧州委員会案（2012年1月）	欧州議会案（2014年3月）	欧州連合理事会案（2015年6月）
第39条 認証	・EU加盟国と欧州委員会は、データ保護認証制度の設立を促進する。 ・認証制度の詳細は欧州委員会が委任法令や実施法令で定める。	・「欧州データ保護シール」の認証手続きについて規定。 ・EU各国の監督機関が管理者や処理者を認証する。 ・監督機関は第三者監査機関（third party auditors）を認定することができる。 ・認証の有効期間は最大5年間。	・EU加盟国と欧州データ保護評議会と欧州委員会は、データ保護認証制度の設立を促進する。 ・認証機関（または監督機関）が管理者や処理者を認証する。 ・認証基準はEU各国の監督機関または欧州データ保護評議会が承認（approve）する。 ・認証の有効期間は最大3年間。 ・第42条2項（e）にいう、第三国へのデータ移転の枠内での第三国受領者における適切な安全管理措置の存在を証明する目的で、認証制度を制定することができる。
第39a条 認証機関と手続き	（なし）	（なし）	・EU各国の監督機関（またはEC765/2008に基づくEU各国の認定機関）が認証機関を認定する。 ・認証制度の詳細は欧州委員会が委任法令や実施法令で定める。

＊15　「EUデータ保護規則案に対するJEITA意見書」（2012年9月）
http://home.jeita.or.jp/press_file/20121214172407_QmZqTgt0AW.pdf。

■表4.　第3条2項についての比較

	欧州委員会案（2012年1月）	欧州議会案（2014年3月）	欧州連合理事会案（2015年6月）
第3条2項 域外適用	・EU域外企業であっても、以下の場合、EU居住者のデータを取扱う管理者に対してはEU規則が適用される。 (a) EU居住者に商品やサービスを提供している場合 (b) EU居住者の個人の行動をモニターしている場合	・EU域外企業であっても、以下の場合、EU居住者のデータを取扱う管理者や処理者に対してはEU規則が適用される。 (a) EU居住者に商品やサービスを提供している場合 (b) EU居住者の個人の行動をモニターしている場合	・EU域外企業であっても、以下の場合、EU居住者のデータを取扱う管理者に対してはEU規則が適用される。 (a) EU居住者に商品やサービスを提供している場合 (b) EU域内での行動に限り、EU居住者の個人の行動をモニターしている場合
前文（20）	「個人が本規則の下で認められている保護を奪われないことを保証するために、EU域内に事業所を持たない管理者による、EU域内に居住するデータ主体の個人データの処理は、当該処理活動が当該データ主体への商品若しくはサービスの提供に関係している場合、又は当該データ主体の行動をモニタリングする場合には、本規則の適用対象となる。」	・欧州委員会案に下記を追記 「管理者がEU域内のデータ主体に商品又はサービスを提供しているか否かを決めるためには、当該管理者がEU域内の一つ以上の加盟国に居住するデータ主体へのサービス提供を意図していることが明白かどうかが確認されるべきである。」	・欧州議会案に更に下記を追記。 「単に当該管理者または仲介者のWebサイトにアクセスできることでは、そのような意図の証拠としては不十分である。また、当該管理者のメールアドレスや連絡先にアクセスできることや、当該管理者が所在する第三国で一般に使われている言語を使用していることだけでも、そのような意図の証拠として不十分である。一つ以上のEU加盟国で一般に使われている言語または通貨で商品やサービスを注文できるか、EU域内に居住する消費者向けのサービスだと言及しているかといった要素が、そのような意図を明白なものとしうるだろう。」 ※欧州司法裁判所のアルペンホフ判例（C-144/09）に基づき、EU居住者に商品・サービスを提供しているか否かの基準をより明確化している。

3. EUからのデータ移転：今後の見通し

高度にグローバル化した社会環境では、データの国境を越えた流通や利活用をいたずらに妨げないことが重要である。現行EU指令及び新たなEU規則案におけるデータ移転制限に対しては、日本企業の多くは標準契約条項や本人同意で対処しているところであるが、2015年度より日本政府は欧州委員会と十分性認定に向けた対話を開始する予定となっている。EUとの取引のある日本企業としては、EUデータ保護法制に適合するための手段として、この十分性認定の下でデータ移転を行うことが最も個々の企業の負担が少なく、望ましい姿である。したがって、グループ企業間でのデータ移転や、欧州企業からのデータ処理・保管の受託を含め、EU域内企業と何らかの個人データ授受を行っている産業界は、日本政府による十分性認定に向けた取組みを一丸となって支援すべきである。

なおEU規則案については、JEITA等からの要望を受けて、欧州議会案、欧州連合理事会案で共に、「適切な安全管理措置による第三国へのデータ移転」の一つの措置として、「認証制度」が追加されている。これは、日本で普及している第三者認証制度を用いた越境データ移転に道を開くものである。日本国全体（もしくは民間分野全体としての）十分性認定に長期間を要することとなった場合には、次善策として、日本で一定の要件に基づく認証を取得した企業は無条件でEUからデータ移転を受けられるような措置の実現を目指すべきである。

ただし現状のEU規則案（委員会案、議会案、理事会案）の規定では、データ移転にあたって日本の認証制度を直接適用できる訳ではなく、EU側の何らかのお墨付きが必要とされる。仮に日本企業にEU側の認証制度の取得が必要となった場合、現行の標準契約条項やBCRと負担はあまり変わらなくなる。したがって、日本の認証制度を活かせる形でのデータ移転を実現することが重要である。一つの方策として、日本の認証制度やAPECの越境プライバシールール（CBPR）等とEUのシール制度との相互承認（mutual recognition）の仕組みを新たなEU規則案の枠組みに組み込んでもらえるよう、日本産業界からEUに対して引き続き要望を行っていく必要があるだろう。