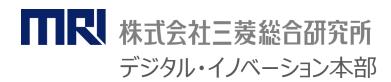
EU・eプライバシー規則(案)に関する議論の状況

2020年11月5日





目次

1.	ePrivacy規則(案)の概要	-2
2.	ePrivacy規則(案)の検討経緯	-3
3.	ePrivacy規則(案)の構成	-6
4.	ePrivacy規則(案)の検討状況	-8
4.	【参考】クッキー使用における欧州司法裁判所の見解────	17
5.	【参考】 ePrivacy指令に関する欧州司法裁判所の決定—————	18

1. ePrivacy規則(案)(ePrivacy Regulation)の概要

- ePrivacy規則は、現行のePrivacy指令(ePrivacy Directive)を置き換えるものとして、欧州委員会が2017年1 月に提案したもので、GDPRの特別法という位置づけになる。
- ePrivacy指令で適用対象外となっていた、インターネットベースのOTTサービス (VoIP、メッセージサービス、ウェブメール等) についても、技術中立的に規制の対象とする。
- 保護対象は個人のデータに限定されず、法人による通信の保護も目的とする。
- ウェブサイトや動画、音楽等のコンテンツだけでなく、コンテンツの送受信のために処理されるデータ(メタデータ) も対象とする。
- GDPRと同様、EU域内に拠点がない日本企業であっても、EU域内のユーザに電子通信サービスを提供する場合や、EU域内のエンドユーザの端末に情報を保存する場合などには域外適用される可能性がある。
- GDPRが発効する2018年5月までの成立が見込まれていたが、加盟国間で意見が割れていたためその後も協議が続けられた。しかし、2019年12月に、EU常駐代表委員会(COREPER)*にて修正案が否決され、審議はいったん停止した。
- その後、改めて修正案をとりまとめる作業がEU理事会にて行われてきているが、まだ議論が収束しておらず、 2020年11月現在で未成立な状況にある。(2020年5月に進捗レポートを発表した以降は、COVID-19の影響 で実質的に検討が進んでいない。)
- 現在、電子通信メタデータやクッキー等の技術により収集した情報の取扱い(例:取扱いが可能な法的根拠、 犯罪防止等を目的とした使用などの例外規定、等)が大きな論点となっている。
 - * 加盟国の代表又は副代表から構成される常任委員会で、EU理事会の議題を決定する権限を持つため、ここで否決されることは廃案となることを 意味する。この場合、欧州委員会は、提案を取り下げるか、6ヶ月以内に修正案を提出することができる。



2. ePrivacy規則(案)の検討経緯

- 2019年5月に欧州議会選挙があったことも影響し、2019年4月以降は修正案の検討・改訂作業に大きな進展はみられなかった。
- 2019年12月にいったん否決され、EU理事会にて再提案に向けた検討(規則案の修正)が進められてきているが、まだ合意には至っておらず、2020年5月以降はCOVID-19のために審議が事実上停止している。

時期	法案等の状況	EU関係機関の動向	業界団体等の動向
2017年1月	欧州委員会がePrivacy規則案を発表		
2017年4月		第29条作業部会が意見を発表 EDPS(欧州データ保護観察官)が意見を提出	
2017年7月			IAB EuropeがePirvacy規則に対するポジションペーパーを公表
2017年9月			ICDPが、欧州議会の議員に向けた、ePrivacy 規則が業界に与える影響について説明した書 簡に署名
2017年10月	欧州議会LIBE(市民的自由・司法・内務委員 会)で修正採択	EDPSが再度意見を提出	
2017年11月			ICDPが、欧州議会LIBEに対し、ePrivacy規則 に関する書簡を提出
2017年12月	EU理事会、修正版ePrivacy規則案を発表		
2018年3月	EU理事会が新たな規則案を発表		EDiMAが2017年10月のePrivacy規則案 1 ~ 5条に関し意見を表明
2018年5月		EDPBが第1回総会にTePrivacy規則に関する声明を採択	57者のステークホルダーが、TTE Councilに対し てePrivacy規則案を慎重に検討するよう要請 する書簡に共同署名
2018年7月	EU理事会が新たな規則案を発表		
2018年9月	EU理事会が新たな規則案を発表		



2. ePrivacy規則(案)の検討経緯(Cont.)

(つづき)

時期	法案等の状況	EU関係機関の動向	業界団体等の動向
2018年10月	EU理事会が新たな規則案を発表		
2018年11月			IAB EuropeがePrivacy規則案に対するポジションペーパーを再度公表 66者のステークホルダーが、TTE Councilに対してePrivacy規則案を慎重に検討するよう要請する書簡に共同署名
2019年2月	EU理事会が新たな規則案を発表 (4日、15日、 22日にそれぞれ発表)		11者のステークホルダーが欧州委員会に対して ePrivacy規則案に対する新たな影響評価を実 施するように要請する書簡を提出
2019年3月		EDPBが審議促進を求める声明を発表	
2019年5月	EU理事会が進捗レポートを発表		
2019年7月	改訂されたePrivacy規則に関連する統合文 書をEU理事会が発表		
2019年9月	EU理事会がePrivacy規則の改訂版を公開		
2019年10月	EU理事会がePrivacy規則の改訂版を公開		
2019年11月	EU理事会がePrivacy規則の改訂版を公開、 進捗レポートを発表		
2019年12月	COREPERにて修正案が否決される		
2020年2月	EU理事会がePrivacy規則の改訂版(改訂 部分のみ)を公開		
2020年3月	EU理事会がePrivacy規則の改訂版を公開		
2020年5月	EU理事会が進捗レポートを発表		

4

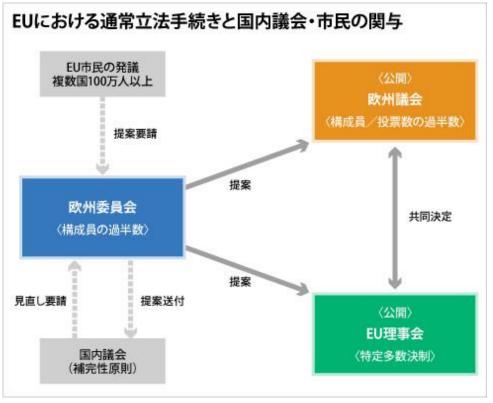
【参考】 EUにおける立法プロセス

- EUの立法プロセスには、「通常立法手続」と「特別立法手続(諮問手続と同意手続)」との2種類があり、ほとんどの場合は 通常立法手続が用いられている。
- 通常立法手続の場合は、欧州委員会が提出した法案を、EU理事会(閣僚理事会)と欧州議会が共同で採択する。(閣 僚理事会と欧州議会が立法府といえる。)
- ePrivacy規則も「通常立法手続」で審議されている。

欧州委員会

(The European Commission)

- EUの行政執行機関として、 法令の立案、政策の施行、 法の執行、国際条約の交渉 などを行う。「EUの政府、内 閣 ともいわれる。
- 法案提出権は、特別の場合 を除いて、欧州委員会が独 占している。



出典:

駐日欧州連合代表部「EUの法律はどのように決められていますか?」

http://eumag.jp/questions/f0813/

国立国会図書館 リサーチナビ「EU法の立法過程」

https://rnavi.ndl.go.jp/research_guide/entry/eu-rippou.php

欧州議会

(The European Parliament)

- 5年ごとの直接選挙で選ばれる議員で構成。欧州市民の利益を代表する機関で、EUの活動を監督するほか、法令を制定する権限をEU理事会と共有する。
- ただし、欧州議会は賛否の表明はできるが、理事会の立場に修正を求めることはできない。

EU理事会(閣僚理事会)

(The Council of the European Union)

- 加盟国政府の閣僚で構成され、主たる 役割はEUの法律を成立させること。通 常はこの立法権限を欧州議会と共有す る。
- ・ EU理事会での決定は、全会一致を必要とする少数の案件を除いて、多くが各加盟国に割り振られた加重票を用いた特定多数決で行われる。



3. ePrivacy規則(案)の構成

● 最新のePrivacy規則(案)(2020年3月公表)の構成は以下のとおり。同意、ユーザ端末の義務、秘密保持対象やその例外、域内での規制機関等について修正が重ねられてきている。(※2017年1月の委員会当初案との差異を赤字(太字/取消線)で表示)

Article	項目	Article	項目
1	対象事項	13	緊急通信に関連する発信者及び接続先の識別情報の表示及び 非表示に関する例外
2	実態的範囲	14	着信のブロッキング不要な電話、悪意のある電話、迷惑電話
3	領域的範囲と代表	15	公的に利用可能なディレクトリ
4	定義	16	求められていない通信 及び ダイレクトマーケティング通信
4a	同意	17	【削除】 検出されたセキュリティŧリスクに関する情報
5	電子通信データの秘密	18	独立 監督機関
6	電子通信データの許容される処理	19	欧州データ保護会議
6a	電子通信コンテンツの許容される処理	20	越境協力及び一貫性の手続
6b	電子通信メタデータの許容される処理	21	救済
6c	電子通信メクデータの互換処理	22	補償の権利と責任
6d	児童性的虐待の防止を目的とした電子通信データの処理	23	行政制裁金を課す際の一般条件
7	電子通信データの保存及び消去	24	罰則
8	エンドユーザーの端末機器 <mark>の保存</mark> 情報 <mark>及び関連情報</mark> の保護	25	委任法令の運用
9	【削除】同意	26	コミッティー (注: COCOM (Communications Committee) が、欧州委員会の執行権限遂行を支援する)
10	【削除】プライバシー設定のために提供される情報と選択肢	27	廃止
11	制限	28	モニタリング及び評価条項
12	発着端末識別情報の保存及び制限	29	施行及び適用

【参考】主な論点と意見(2018年12月時点)

- ◆ 大きな論点として、個人情報やプライバシー情報の保護の強化と、産業振興・イノベーション促進のバランスをどう考えるのかという点が挙げられる。
- 業界団体や各国政府はePrivacy規則(案)によって新産業・新サービス創出やイノベーションが抑制されることを懸念している。特に、順調に成長しているインターネット広告分野や、IoTやAIなど今後の発展が期待される分野において、各国企業の成長の可能性を小さくすることは避けたいと考えている模様である。

論点	論点に関する	条文への反映状況	
神流	EUの関係機関	業界団体等	
①プライバシー設定 によるブラウザのゲー トキーパー化 (10条)	ブラウザ等のソフトウェアは、デフォルトで追跡 拒否と設定する(欧州議会LIBE)	多くのウェブサイトでユーザに同意を要求するようになり、利便性が低下する。 10条は大幅に改定するか、削除するべき (IAB Europe)	EU理事会案(2019年2月22 日版)では第10条が削除さ れている。
②ユーザ端末の情報 利用時の同意以外 の処理手段の是非 (8条1項)	「正当な利益に基づく」例外は認められない。 電子通信データの処理またはユーザ端末の 処理能力の使用の前に、必ず合理的な同 意を取得すること(EDPB)	「正当な利益に基づく」データ処理を、データ所有者の権利を侵さない範囲で許容するべき。 具体的な例外を列挙している現状の第8 条は不適当。(IAB Europe)	「正当な利益に基づく」データ 処理を許容する記載は反映さ れていない。
③M2M通信を対象 に含むことの是非 (5条)	ePrivacy規則(案)が既存のePrivacy指令の規制レベルを下回ってはならない。 現行のePrivacy指令ではM2Mの提供に使用される伝送サービスも適用範囲に含まれている。(EDPB)	広範な「デジタル経済」: メディア、コネクテッドカー、医療テクノロジー、スマートマニュファクチャリング 等への影響がある。(ステークホルダー共同書簡)	EU理事会案(2019年2月22 日版)では本文での明記は 削除されたものの、前文に M2M通信も含むことが記載さ れている。
④トラッキングウォー ルの許容可能性 (8条)	ターゲティング広告を提供するためのデータ処 理はサービスの提供に必要とみなすことができ ない。(EDPS)	広告提供はサービス提供にとって必須ではないが、サービス提供者の利益モデルにとって必須である。(IAB Europe)	欧州議会LIBEの修正採択案 では追記されたものの、EU理 事会案には反映されていない。

4. ePrivacy規則(案)の検討状況

2019年3月以降の検討状況の概略は以下のとおり。

年月	主な改訂ポイント・議論
2019年5月 進捗レポート	 ● ePrivacy規則が新しいテクノロジーに与える影響、児童虐待(児童ポルノ)画像の防止・発見・報告に関する 問題、データ保持に関する問題、監督当局の権限などについての検討が継続されている。
2019年7月 ドラフト	● 5月の進捗レポートの観点を踏まえつつ、第12条~第16条(※)と関連するリサイタルの修正内容のみに焦点を当てている。
	※ 発着端末識別情報の保存及び制限、緊急通信に関連する発信者及び接続先の識別情報の表示及び非表示に関する例外、不要な電話、悪意のある電話、迷惑電話、公的に利用可能なディレクトリ、求められていない通信及びマーケティング通信
2019年9月	● 児童ポルノを構成する素材の検出、削除及び報告を目的とする電子通信データの処理について検討された。
ドラフト	 ■ 電子通信メタデータの処理に関する規定の修正などについても検討されているが、ダイレクトマーケティングや クッキーに関する規定の修正内容は軽微なものに留まった。
2019年11月	■ 通信の秘密に関する条項(リサイタル(17)~(19b)、第6条~第6d条)の修正が提案された。
ドラフト	● 加盟国の多くは、児童ポルノだけでなく、テロ等の重大犯罪防止にも適用されるべきとの意見だとされた。
2020年2月 ドラフト	電子通信メタデータの処理や、クッキー及びその類似技術の配置を可能とする根拠として、「正当な利益 (legitimate interest)」の導入が提案された。
(2020年5月 進捗レポート)	● 異論も多く、さらなる議論が必要な状況。(※COVID-19の影響により、6月以降は審議が停止されている。)

4. ePrivacy規則(案)の検討状況(1)2019年5月進捗レポート

- 2019年3月のドラフト発表以降については、欧州議会選挙があったこともあり、検討状況に大きな進展はない。
- 欧州理事会から2019年5月に発表された進捗レポートでは、主に以下の4点について検討していることが示されている。

進捗レポート(2019年5月)のポイント

● ePrivacy規則が新しいテクノロジーに与える影響、児童虐待画像の防止・発見・報告に関する問題、データ保持に関する問題、監督当局の権限などについての検討が継続されている。

主な検討観点	概要
新しいテクノロジーに与える影響	 M2M、IoT、人工知能などの新しい技術とePrivacy規則がどのように相互作用するかについて、 継続的に議論を進めている段階。 複数のエンドユーザの状況および同意の問題に対処する13条、20a条および21条に関連した Recitalに、多くの説明などを記載することを検討している。
児童虐待画像の防止・ 発見・報告に関する問題	 EUレベルではこの問題への対応が支持されていたが、ePrivacy規則案では、どのように対応するかについて、各国代表団の見解が分かれている 電子通信データの処理に関する第6条にこの目的の規定を含めることを提案したが、他の加盟国は、制限に関する第11条に照らして別個の法律行為で対処することができると主張。適切なセーフガードを確保する必要性についても議論された。
データ保持に関する問題	● ePrivacy規則の規定が、既存および将来のデータ保持制度が欧州連合基本憲章の要件を 準拠する可能性を維持することを保証する方法について議論。(現状のePrivacy規則案の各条 項と構造を単に再現するだけでは、十分ではない)
監督当局に関する規定	憲章第8条(3)に由来する独立性の要件を尊重しつつ、加盟国に一層の柔軟性を与える。第19条: 欧州データ保護会議、第20条: 協力および手続の一貫性について、大幅な簡素化と明確化を図る。

4. ePrivacy規則(案)の検討状況(2)2019年7月ドラフト版①

- 2019年7月に、改訂された統合文書がEU理事会から公開された。
- 2019年7月の会合では、5月の進捗レポートの観点を踏まえつつ、第12~16条と関連するリサイタルの修正 内容のみに焦点を当てている。
- 発行された改訂版規則案では、議長国の承認に基づき以下の変更点を新たに導入した。

該当箇所	変更理由	概要
第4条定義 3.(f) リサイタル32	第16条「求められていないダイレクトマーケティング」の規定の範囲内にあるサービスを明確化	第4条3.(f) • 「ダイレクト・マーケティング・コミュニケーション」とは、書面によるものであれ口頭によるものであれ、1人または複数の特定のエンドユーザに向けて、公開されている電子コミュニケーション・サービスを介して直接送信されるあらゆる形態の広告を意味する。これには、音声通話の発信、人との対話を伴うまたは伴わない自動通話および通信システムの使用、電子メッセージなどが含まれる。
		リサイタル32 ・ 本規則において、ダイレクト・マーケティング・コミュニケーションとは、自然人又は法人が、 <mark>公的に利用可能な</mark> 電子通信サービスを利用して1人又は複数の特定のエンドユーザに 直接送付するあらゆる形態の広告をいう。
第13条	第13条の簡略化	第13条タイトル (変更前) *1 発着端末識別情報の保存および制限、着信拒否、緊急サービスの提供に関する例外 (変更後) 緊急通信に関連する発信者及び接続先の識別情報の表示及び非表示に関する例外

*1 直前のドラフト版におけるタイトルであるため、当初案(p.6)とは若干異なる。



4. ePrivacy規則(案)の検討状況(2)2019年7月ドラフト版②

● 変更点(つづき)。

該当箇所	変更理由	概要
第13条 (つづき)	第13条の簡略化	第13条2項の削除 (削除文) 加盟国は、透明性のある手続きの確立と、公的に利用可能な数ベースの対人 通信サービスの提供者が、エンドユーザが望まない、悪意のある、または迷惑な 通話の追跡を要求する場合に、一時的に電話回線識別の提示の排除を無効 にするか、または対処しなければならない状況に関して、より具体的な規定を制 定しなければならない。
第13条2項を第 14条1a項に移動	一貫性を目的として、 悪意のある迷惑電話に 関する全ての条項を1つ に集約	※上記の削除文を第14条1a項に追記

4. ePrivacy規則(案)の検討状況(3)2019年9月ドラフト版①

- 2019年9月18日に、EU理事会がePrivacy規則の改訂版を公開した。
- このドラフトにおいては、児童ポルノを構成する素材の検出、削除及び報告を目的とする電子通信データの処理について検討された。
- 電子通信メタデータの処理に関する規定の修正などについても検討されているが、ダイレクトマーケティングやクッキーに関する規定の修正内容は軽微なものに留まった。

改訂・検討のポイント

1. 「児童ポルノを構成する素材の検出、削除及び報告」に関連する修正について、以下の2つの選択肢が示され、議論を通じて当該箇所への見解を表明することが求められた。(この議論が行われている間、議長国は、関連する条項にいかなる修正も導入していない:選択肢の提示し、議論を求めたのみ)

選択肢	概要	
選択肢①	第29条施行および適用の規則を維持するが、第3項(a) (発効日前に、プロバイダが処	この妥協案は、多くの代表団の懸念(主に一時的な性質と サービス提供者間の平等)に対処することが可能。
	理を開始…)を削除し、 <u>規則の一時的な性</u> 質を変更する(そのような処理に関する特定 の法律が施行されるまで)。	加えて、「加盟国が、法執行機関又は他の権限のある当局への通知に関する規則を国内法令で規定することが可能であること」を明確にすることができる。
選択肢②	児童ポルノを構成する素材の検知・削除・ 報告を目的とした電子通信データの処理に 関する <u>新条項6dを導入する</u> 。(※新条項	この選択肢は、処理内容の比例性を確保するために提供される保障措置の妥当性について、慎重な考慮を必要とするだろう。
	6dの案は、次頁参照)	この場合、加盟国は、第11条(制限)に従って、法執行機関 又は他の権限のある当局に通知する際の規則を国内法令 で規定することができる。

https://data.consilium.europa.eu/doc/document/ST-12293-2019-INIT/en/pdf

4. ePrivacy規則(案)の検討状況(3)2019年9月ドラフト版②

く新たに提案された第6d条>*1

第6d条 児童ポルノを構成する素材の検出、削除及び報告を目的とする電子通信データの処理

- 1. 第6条1 (電子通信データの許容される処理) に影響を与えることなく、番号と紐づかない対人通信サービス*2の提供者は、使用される技術が次の特性の全てを満たす場合は、指令2011/93/EU*3の第2条(c) に定義される児童ポルノを構成する要素を検出、削除及び報告することのみを目的として、電子通信データを処理することを許可される。
 - i. 電子通信に添付された素材の再変換不可能なデジタル署名(ハッシュ)を作成し、そのハッシュを児童ポルノを構成するものとして、以前に確実に特定された素材のハッシュを含むデータベースと比較することを唯一の目的とする。
 - ii. データベースとの比較の直後に、電子通信に添付された一致しないデータのハッシュを消去する。
 - iii. 児童ポルノの構成要素の誤検出率を最大1/500億に制限する。
 - iv. ハッシュによって児童ポルノを構成する素材が検出された場合を除き、電子通信データは保存されない。

- *1 ここに示すのは2019年9月ドラフト版における条文案である。(その後も修正が行われており、最新版は上記とは異なる。)
- *2 電話番号等と紐づかないが個人間でのコミュニケーションを提供するサービス。(例えばSNSのメッセージングサービス等。)
- *3 児童の性的虐待並びに性的搾取及び児童ポルノグラフィーの撲滅に関するEU指令

4. ePrivacy規則(案)の検討状況(3)2019年9月ドラフト版③

- その他に、議長国の修正案をふまえ、以下の変更が導入された。これらは、9月24日の電気通信情報社会作業部会をはじめとして、今後も引き続き議論されることとされた。
 - 議長国からの修正案(第1~4a条、及び第18条~29条)

該当箇所	理由など	変更概要
リサイタル7a	第2条2(a)の文言との 整合性を図る	本規則は、国家安全保障及び防衛に関する活動のような <mark>連邦法の範囲外の活動に関連する基本的権利及び自由の保護</mark> には適用されない。
リサイタル8 第3条2	削除された第10条「プライバシー設定のために 提供される情報と選択 肢」の関連箇所の修正	リサイタル8 本規則は,電子通信サービスの提供者,公的に利用可能なディレクトリの提供者 及びイン ターネット上の情報の検索及び提示を含む電子通信を可能にするソフトウェアの提供者 に 適用されるべきである。
		第3条2 地理的適用範囲と代理人電子通信サービスの提供者、公に利用可能なディレクトリの提供者、電子通信を可能にするソフトウェアの提供者、電子通信サービスを使用してダイレクトマーケティング通信を送信又は提示する者、処理及び保存の能力を使用する者、又はエンドユーザの端末機器によって処理され若しくは排出され、若しくは格納された情報を収集する者が連合に存在しない場合は、連合に代表者を書面で指定しなければならない。
リサイタル26	「立法」という言葉を導 入	この規則は、必要に応じて公共の安全を確保するために、電子通信の合法的傍受の実施や、限られた期間のデータの保持を規定する"立法"措置など、・・・
第2条2 (e)		エンドユーザが受信後に処理する電子通信コンテンツ又は、エンドユーザが電子通信コンテンツの記録、保存その他の処理を委託された第三者が処理する電子通信コンテンツ;

4. ePrivacy規則(案)の検討状況(4)2019年11月ドラフト

● 2019年11月の改訂版では、主な変更点として、通信の秘密に関する条項(序文(17)~(19b)、第6条~第6d条)が挙げられる。また、加盟国の多くは、テロ等の重大犯罪防止にも適用されるべきとの意見とされた。

条	概要
第6条 電子通信データの許可され た処理	 電子通信ネットワーク及びサービスの提供者が電子通信データの処理を許可される場合(電信通信サービスの提供の必要/電子通信ネットワーク・サービスのセキュリティの維持・回復、技術的欠陥・誤り・セキュリティリスク・攻撃の検出の必要/エンドユーザの端末機器への攻撃検出の必要/EU法・国内法の遵守) 電子通信データを処理することが許される条件(特定の目的のために必要な期間、匿名化が不可能な場合) 電子通信ネットワーク・サービスの代理を務める第三者による電子通信データの処理
第6a条 [旧 第6条(3)] 電子通信コンテンツの処理 許可	 電子通信ネットワーク及びサービスの提供者が電子通信コンテンツの処理を許可される場合(利用者が個人的な使用のために要求するサービスを目的として、本人が同意し、他者の権利・利益に悪影響を及ぼさない場合/1つ以上の特定の目的のために電子通信コンテンツを処理することに、関係する全エンドユーザが同意した場合) ネットワークおよびサービス提供者による事前の評価及び監督機関との協議の義務
第6b条 [旧 第6条(2)] 電子通信メタデータの許可 された処理	 電子通信ネットワーク及びサービスの提供者が電子通信メタデータの処理を許可される場合(ネットワーク管理・最適化に必要/料金計算・請求に必要/1つ以上の特定の目的のために通信メタデータを処理することに、関係する全エンドユーザが同意した場合/緊急時に、法に従い自然人の死活的利益を保護することが必要/統計的目的や科学的研究のために必要で、適切な条件の下で処理される場合)
第6c条 [旧 第6条(2a)] 電子通信メタデータの互換 処理	 電子通信メタデータが、収集された以外の目的で取り扱われる(追加処理される)場合に、当初の目的との整合性を判断するための考慮事項(収集目的と追加の目的との関係/収集された状況、特にエンドユーザとプロバイダの関係/メタデータの性質及び追加処理の態様/エンドユーザに起こり得る結果/仮名化・暗号化等の適切な保護手段の存在) 整合性があるとみなされる場合に、追加処理が許可される条件(不要になった場合に直ちに消去/処理対象の限定/エンドユーザの分析や識別等の禁止) 電子通信ネットワーク及びサービスの提供者の責務(データの第三者との共有禁止/DPIA及び監督機関との事前協議/エンドユーザによる異議申立の権利)
第6d条 [新] 児童性的虐待の防止を目的 とした電子通信データの処理	 番号独立の対人通信サービスの提供者は、使用される処理技術が条件を満たす場合に、児童の性的虐待及び搾取を防止することのみを目的として、電子通信データを処理することを許される(ハッシュの作成目的/ハッシュの消去/誤検出率) DPIA及び監督機関との事前協議の実施

4. ePrivacy規則(案)の検討状況(5)2020年3月ドラフト

● 2020年3月の改訂版では、電子通信メタデータの処理や、クッキー及びその類似技術を配置できる根拠として「正当な利益(legitimate interest)」の導入を提案したが、異論も多く、さらなる議論が必要な状況。

法的根拠としての 「正当な利益」の 導入

- (1) 電子通信メタデータの処理
- (2) クッキー及び類似技術の配置

を行うことができる根拠として「正当な利益(legitimate interest)」の導入を提案 (「正当な利益」以外の根拠を排除するため、第6b条の修正、第6c条の削除、第8条の修正、関連するリサイタルの修正を実施)

条件及び 保護措置

「正当な利益」を根拠とする場合の条件及び保護措置は以下のとおり:

- データ保護影響評価(DPIA)を実施し、必要に応じて関連する監督当局に相談すること。
- 適切なセキュリティ対策を実施すること。
- 実施しているデータ処理活動に関する情報をエンドユーザーに提供すること。
- データ処理に対する異議申立の権利をエンドユーザーに提供すること。
- メタデータやクッキーまたは類似の技術を使用して収集した情報について、事前に匿名化されている場合を除き、第三者と共有しないこと。

「正当な利益」を 根拠とできる事例

「正当な利益」を根拠としてクッキー等を用いることができる状況の例を例示(→リサイタルの修正案):

- エンドユーザーがサービス提供者と既存の顧客関係にあり、情報社会サービスのセキュリティ確保、不正行為の防止、技術的欠陥の検出、セキュリティ脆弱性やその他のセキュリティバグの修正を目的して、(一定の条件の下で)使用する場合
- 直接的な金銭の支払いがなくてもアクセス可能な、主として広告を財源として提供されるウェブサイトのコンテンツやサービス(オンライン新聞やその他の出版物、視聴覚メディアサービスなど)を提供する場合

加盟国の主な意見

- メタデータやクッキー等を通じて収集された情報が、エンドユーザーの性質や特徴を把握したり、個々のプロファイルを作成するために使用されたり、GDPRにおけるセンシティブな個人情報を含む場合や、エンドユーザーが子供である場合には、事業者の利益よりもエンドユーザの利益が優先されてしまう(※必要以上に、という主張と考えられる)
- 「正当な利益」以外の根拠を復活させるべき
- 「情報社会サービス」の範囲のさらなる明確化が必要等

【参考】 クッキー使用における欧州司法裁判所の見解

● 2019年10月1日、欧州司法裁判所(CJEU)は、オンラインのウェブ閲覧行動を追跡するクッキーを保存する企業に対し、インターネットユーザからの能動的な同意を取得しなければならないとの裁定を下した。

背景·経緯

- オンラインの宝くじ会社Planet49は、プロモーション抽選の中で、①ユーザがサードパーティの広告を受信すること、②Planet49がクッキーを設定してユーザをオンラインで追跡できるようにすること、の2つのチェックボックスを提示していたが、②のチェックボックスには事前にチェックが入っていた。
- これに対して、ドイツの消費者団体が、「パートナーが提供する製品のターゲット広告に役立つような情報(クッキーによるオンラインでの追跡情報)を収集していたことに関する明示的な同意プロセスが存在しなかった」として法的措置を講じた2013年の事案が契機となっている。

裁定結果 ·理由

● 裁定結果:「クッキーを保存するために事前にチェックした同意ボックスは法的に有効ではない。
 必須でないクッキー(ターゲット広告用のクッキーの追跡など)を保存またはアクセスする前に、明示的な同意を得る必要がある。」

<裁定理由等>

- ■ユーザの機器に保存またはアクセスされる情報が個人データであるかどうかは関係ない。
- 私生活への干渉からユーザを保護することを目的としており、隠された識別子や他の同様のデバイス がユーザの端末機器に知らずに侵入するリスクから保護するために、明示的な同意が必要。
 - ▶ 一方で、「ウェブサイトのユーザが個人データの処理に実際に同意したか否か」を客観的に判断することは、事実上不可能であると認識
- ●以下の情報は、ユーザに提供されるべき明確かつ包括的な情報の一部であるため、サービスプロバイ ダはこれらをユーザに提供しなければならない。
 - ▶ クッキーの作動期間
 - サードパーティーの当該クッキーへのアクセス可否

【参考】 ePrivacy指令に関する欧州司法裁判所の決定①

欧州司法裁判所(CJEU)は、2020年10月6日、英国の安全保障・情報機関による大量の通信データ(トラフィックデータ、位置データ)の取得と利用が違法であるか否かについて、これらの活動はePrivacy指令の規制対象となり(例外には該当せず)、これを認める国内法は排除される、との決定を下した。

背黒

- 英国の様々な安全保障・情報機関(GCHQ、MI5、MI6)が大量の通信データを取得・利用していることが、英国国会の情報安全委員会による報告書を含む形で2015年初頭に公表された。
- 2015年6月5日、NGOであるプライバシー・インターナショナルは、外務・英連邦大臣、内務大臣、およびこれらの安全保障・情報機関を相手取り、英国の捜査権限裁判所にて、これらの行為の違法性を申し立てた。
- 同裁判所は、審理の結果、以下の点について欧州司法裁判所(CJEU)に付託することを決定した。

付託内容 (要点)

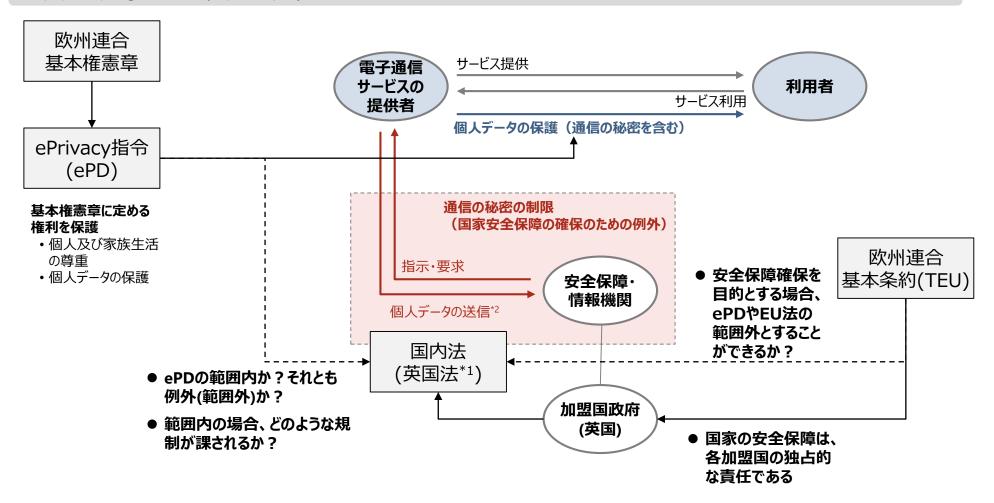
- (1) 加盟国の国務大臣が、電子通信ネットワークの提供者に対して、加盟国の安全保障・情報機関に大量の通信データを提供しなければならないと指示・要求することは、**EU法及びePrivacy指令による規制の範囲に含まれるか**?
- (2) 上記への回答が「含まれる」の場合、
 - 国務大臣の指示・要求に対し、欧州基本権憲章や判例に基づき、どのような要件が付されるか?
 - もしそうであれば、**国家安全保障のために大量データの取扱いが必要であることを考慮した上で、これらの要件がどのよう** に、またどの程度適用されるのか?
- 欧州司法裁判所(CJEU)は以下の決定を行った。

CJEUの 決定

- (1) ePrivacy指令の第1条(3)、第3条及び第15条(1)は、欧州連合基本条約の第4条(2)に照らして読まれるが、国家安全保障を保護する目的で、国家機関が、トラフィックデータ及び位置データを安全情報機関に転送することを通信サービスの提供者に要求することを可能にする国内法令が、同指令の範囲内にあることを意味する。
- (2) ePrivacy指令の第15条(1)は、欧州連合基本条約の第4条 (2)、欧州連合基本権憲章の第7条、第8条、第11条及び第52条(1)に照らして解釈されるが、**国家安全保障を保護する目的で、国家機関が、電子通信サービスの提供者に対し、トラフィックデータ及び位置データを安全情報機関に一般的かつ無差別に送信することを要求することを可能にする国内法令を排除する**ものと解釈されなければならない。

【参考】 ePrivacy指令に関する欧州司法裁判所の決定②

決定の対象とされた問題は以下のように整理された



^{*1 1984}年電気通信法(第94条)、2000年捜査権限規則法(RIPA)(第21条(4)及び(6))が参照されている。

^{*2} トラフィックデータ及び位置デーダ並びにRIPA第21条(4)及び(6)に従い使用されるサービスに関する情報が含まれる。当該規定は、特に、(i)通信の発信元及び宛先の特定、(ii)通信の日付、時刻、長さ及び種類の決定、(iii)使用されるハードウェアの特定、及び(iv)端末機器及び通信の位置の特定に必要なデータを含む。そのデータは、特に、ユーザの名前及びアドレス、発呼者の電話番号及びその者によって呼び出された番号、通信の発信元及び宛先のIPアドレス、並びに訪問されたウェブサイトのアドレスを含む。

【参考】ePrivacy指令に関する欧州司法裁判所の決定③

CJEUは付託事項を2つの問いに整理した上で、下記のように判示した。

質問1 (EU法・ePDの範囲内か?)

eプライバシー指令(ePD) 第1条(3)

- 特定分野における「国の活動」(刑法、公安、防衛及び国家安全保障の分野 における活動が含まれる)を範囲外としている
- ただし、「国の活動」とは国家または国家当局の活動である

第3条

• ePDは<u>電子通信サービスの提供に関連する個人データの取扱いに適用</u>される

15条(1)

- ePDに規定される条件が満たされる場合にのみ、加盟国は(ePDが規定する 権利・義務を制限する)国内立法措置を採択できる ⇒それらの立法措置は ePDの規定に従うものであり、当然ながらePDの範囲内に入ることが前提となる
- 判例によれば、15条(1)と3条の適用範囲は、トラフィックデータ、位置データの保持を電子通信サービスの提供者に要求する立法措置だけでなく、権限を有する国家当局による当該データへのアクセスを認めることを要求する立法措置にも及ぶ:後者の立法措置は、必然的に提供者によるデータの取扱いを含み、国家に特徴的な活動とはみなせない
- 判例により、送信による個人データの開示は、ePD第3条の取扱いを構成し、ePDの範囲に含まれる

欧州連合基本条約(TEU) 第4条(2)

• 判例によれば、加盟国は、<u>国家安全を保護する目的で国家的措置がとられたという事実だけでは、EU法を適用不可能にし、加盟国がその法律を遵守する</u> 義務を免除することはできない

刑事司法指令(EU 2016/680)

• 電子通信サービスの提供者に取扱義務を課すことなく直接データを収集する場合には、刑事司法指令を条件として、国内法のみの対象となる。その場合、国内憲法、基本権憲章の要件に適合しなければならない

質問2(範囲内の場合、どのような要件が課されるか?)

eプライバシー指令(ePD) 前文(6), (7)

• ePDの目的は、電子通信サービスの利用者を、新技術、特にデータの自動化された 保存及び処理のための容量の増大に起因する個人データ及びプライバシーに対する リスクから保護すること

第5条(1)

- この目的のため、「加盟国は、<u>国内法規を通じ</u>、(略)、<u>通信および関連するトラフィッ</u> クデータの機密性を確保するものとする」と規定
- 「特に、加盟国は、第15条(1)に従って合法的に許可されている場合を除き、利用 者以外の者による通信及び関連する交通データの傍受、盗聴、保存又はその他の 種類の傍受又は監視を関係利用者の同意なしに禁止するものとする。」と強調

15条(1)

- 国家の安全保障、防衛及び公共の安全、並びに犯罪行為又は電子通信システム の不正使用の防止、捜査、探知及び訴追のために民主主義社会内で必要かつ適 切かつ相応な措置を構成している場合、データの限られた期間の保持を規定する立 法措置を採択することができる
- EU基本権憲章第7条(個人及び家庭生活の尊重)・第8条(個人データの保護)の権利は<u>絶対的な権利ではない</u>: 憲章第52条(1)から、条件に適合する場合(法律で規定、権利の本質を尊重、比例原則に従う、真に必要)には制限を課すことができ、またTEU第4条(2)をふまえると、国家安全保障の確保は重要な目的
- 他方、第3文にて、**比例性の原則**を含むEU法の一般原則および憲章で保証された 基本的権利に従わない限り、ePDで規定された権利および義務の範囲を制限する 立法措置を採択することは許されないことが明らか
- (本件で問題となっている)電子通信サービスの提供者に、一般的かつ無差別の送信によってトラフィックデータおよび位置データを安全保障・情報機関に開示することを求める国内法は、「厳密に必要であり、正当化される」と考えられる限度を超える
- 従って、当該国内法は排除されるべき

【参考】 ePrivacy指令に関する欧州司法裁判所の決定④

● 英国・捜査権限裁判所が欧州司法裁判所(CJEU)に付託した内容・決定は具体的には以下のとおり。

状況設定

以下の場合:

- (a) [安全保障・情報機関が]提供された[大量通信 データ]を使用する能力は、テロ対策、スパイ活動及 び核拡散防止の分野を含む連合王国の国家安全 保障の保護のために不可欠である。
- (b) [安全保障・情報機関]による[大量通信データ]の使用の基本的な特徴は、[それらのデータ]を一箇所に集めて行う、標的を定めない大量処理技術によって、国家安全保障に対する未知の脅威を発見することである。その主な有用性は、ターゲットの迅速な特定とそれに対する配置、ならびに差し迫った脅威に直面した際の行動の基礎を提供することにある。
- (c) 提供後は、電子通信ネットワークの提供者は、[大 量通信データ]を(通常のビジネスに必要な期間を超 えて)保持する必要はなく、([安全保障・情報機 関])のみが保持する。
- (d) 国内裁判所は、(一定の留保事項を条件として)[安全保障・情報機関]による[大量通信データ]の使用における保護措置は、基本権憲章*1の要件と整合的であると認定した。
- (e) 国内裁判所は、[2016年12月21日判決TEL 2 (C 203/15およびC 698/15、 EU:C:2016:970)の119項から125項]に規定された要件を課すことは、該当する場合、[安全保障・情報機関]による国家安全保障を確保するためにとられる措置を阻害し、それによって英国の国家安全を危険にさらすことになると認定した。

付託内容(質問として整理)

- (1) TEU*2第4条および[指令2002/58*3] 第1条(3)を考慮し、電子通信ネットワークの提供者に対して、加盟国の[安全保障・情報機関]に大量通信データを提供しなければならないという国務大臣の指示・要求は、EU法および[指令2002/58]の範囲に含まれるか。
- (2) 質問(1)に対する回答が「はい」の場合、 基本権憲章によって課された要件に加え て、[2016年12月21日判決119項から 125項、TEL 2 (C 203/15およびC 698/15、EU:C:2016:970)に規定さ れた保有通信データに適用される要件] 又はその他の要件のいずれかが、国務大 臣によるそのような指示に適用されるか。

そして、もしそうであれば、国家安全保障を保護するために一括取得及び自動化された処理技術を使用するという[安全保障・情報機関]の本質的な必要性を考慮した上で、これらの要件がどのように、またどの程度適用されるのか。また、基本権憲章に他の点で準拠している場合には、これらの能力がこれらの要件が課されることによって決定的に妨害される可能性がどの程度あるのか。

決定

- (1) ePrivacy指令の第1条(3)、第3条及び 第15条(1)は、欧州連合基本条約の第 4条(2)に照らして読まれるが、国家安全 保障を保護する目的で、国家機関が、ト ラフィックデータ及び位置データを安全情 報機関に転送することを通信サービスの 提供者に要求することを可能にする国内 法令が、同指令の範囲内にあることを意 味するものと解釈しなければならない。
- (2) ePrivacy指令の第15条(1)は、欧州連合基本条約の第4条(2)、欧州連合基本権憲章の第7条、第8条、第11条及び第52条(1)に照らして解釈されるが、国家安全保障を保護する目的で、国家機関が、電子通信サービスの提供者に対し、トラフィックデータ及び位置データを安全情報機関に一般的かつ無差別に送信することを要求することを可能にする国内法令を排除するものと解釈されなければならない。
- *1 欧州連合基本権憲章(Charter of Fundamental Rights of the European Union)
- *2 欧州連合基本条約(Treaties of the European Union)
- *3 ePrivacy指令

【参考】 ePrivacy指令に関する欧州司法裁判所の決定 【関連法令】

ePrivacy指令

前文

- (2) 本指令は基本的権利を尊重し、特に欧州連合の基本的権利憲章で認められている原則を遵守することを目的としている。特に、<u>本指令は、当該憲章の第7条及</u>び第8条に定められた権利の完全な尊重を確保しようとするものである。
- (6) インターネットは、広範な電子通信サービスを提供するための共通のグローバルなインフラを提供することで、従来の市場構造を覆そうとしている。<u>インターネット上で公開されている電子通信サービスは、利用者に新たな可能性をもたらすと同時に、個人情報やプライバシーに新たなリスクをもたらしている</u>。
- (7) 公衆通信ネットワークに関しては、<u>自然人の基本的権利と自由、および法人の正当な利益を保護するために、特に加入者および利用者に関連するデータの自動保存および処理能力の増大に関連して</u>、特定の法的、規制的、技術的な規定を設けるべきである。

第1条 範囲と目的

- (1) この指令は、<u>電子通信分野における個人データの処理に関して、基本的な権利と自由、特にプライバシーに関する権利の同等レベルの保護を確保するために必要な</u> 加盟国の規定を調和させ、共同体における当該データ及び電子通信機器とサービスの自由な移動を確保するものである。
- (3) 本指令は、欧州連合条約のタイトルV及びVIが対象とするような欧州共同体を設立する条約の範囲外の活動には適用されず、いかなる場合においても、<u>公安、防衛、国家の安全保障(活動が国家の安全保障に関連する場合には国家の経済的福利を含む)及び刑法の分野における国家の活動に関する活動には適用され</u>ないものとする。

第3条 関連サービス

本指令は、データ収集及び識別装置を支援する公衆通信ネットワークを含む共同体の公衆通信ネットワークにおける公衆利用可能な<u>電子通信サービスの提供に関連した個人データの処理に適用される</u>ものとする。

第5条 通信の秘密

(1) 加盟国は、国内法により、公衆通信網及び一般に利用可能な電子通信サービスを利用した通信及び関連するトラヒックデータの機密性を確保しなければならない。 特に、加盟国は、第15条(1)に基づき法的に許可された場合を除き、関係する利用者の同意を得ることなく、利用者以外の者による通信及び関連するトラヒック データの盗聴、盗聴、保存、その他の種類の傍受又は監視を禁止しなければならない。本項は、秘密保持の原則を損なうことなく、通信の伝達に必要な技術的保管を妨げるものではない。

第15条

(1) 加盟国は、当該制限が国家安全保障(すなわち国家安全保障)、防衛、公安、及び指令 95/46/EC の第13条(1)項で言及されているように犯罪又は電子 通信システムの不正使用の予防、調査、検出及び起訴を保護するための民主主義社会における必要かつ適切かつ比例した措置である場合には、本指令の第5条、第6条、第8条(1)、(2)、(3)及び(4)、並びに第9条に規定されている権利及び義務の範囲を制限するための立法措置を採用することができる。この目的のために、加盟国は特に、本項に定める根拠に基づいて正当化された限られた期間のデータ保持を規定する立法措置を採用することができる。本項で言及されるすべての措置は、欧州連合条約第6条(1)項及び(2)項で言及されるものを含む共同体法の一般原則に従うものとする。

※下線は資料作成者による

【参考】 ePrivacy指令に関する欧州司法裁判所の決定 【関連法令】

欧州連合基本条約

第4条

(2) 連合は、加盟国の条約上の平等を尊重するとともに、加盟国の基本的な構造、政治的及び憲法に内在する国民的アイデンティティを尊重しなければならない。また、 国家の領土的完全性の確保、法と秩序の維持、国家の安全保障の確保を含む、加盟国の本質的な国家機能を尊重しなければならない。特に、<u>国家の安全保障</u> は、各加盟国の独占的な責任であることに変わりはない。

欧州連合基本権憲章

第7条 私生活・家庭生活の尊重

何人も、自分のプライベートや家族の生活、家庭やコミュニケーションを尊重する権利を有する。

第8条 個人データの保護

- (1) すべての人は、自分に関する個人情報を保護する権利を有する。
- (2) このようなデータは、特定の目的のために、関係者の同意または法律で定められたその他の正当な根拠に基づいて、公正に処理されなければならない。すべての人は、 自分に関する収集されたデータにアクセスする権利と、それを修正してもらう権利を有する。

第52条 権利と原則の範囲と解釈

(1) この憲章で認められている権利及び自由の行使に対する制限は、<u>法律で定められ、かつ、それらの権利及び自由の本質を尊重しなければならない。比例の原則に従い、制限を行うことができるのは、必要であり、かつ、組合が認識する一般的利益の目的又は他の者の権利及び自由を保護する必要性を真に満たす場合に限られる</u>。