資料２

ePrivacy規則（案）とパーソナルデータの提供に関する消費者の意識

株式会社三菱総合研究所
社会ICTイノベーション本部

目次

１． ePrivacy規則（案）について

ePrivacy規則（案）に関する議論のプロセス

- 2017年1月欧州委員会がePrivacy規則（案）を発表してから、2018年12月現在まで議論が続いており、閣僚理事会では複数回にわたり修正案が公表されている。
- 現在は、議会の修正採択を受けて、閣僚理事会が関係機関（EUの他の機関）や各国政府と協議しつつ新たな規則案を策定している段階である。

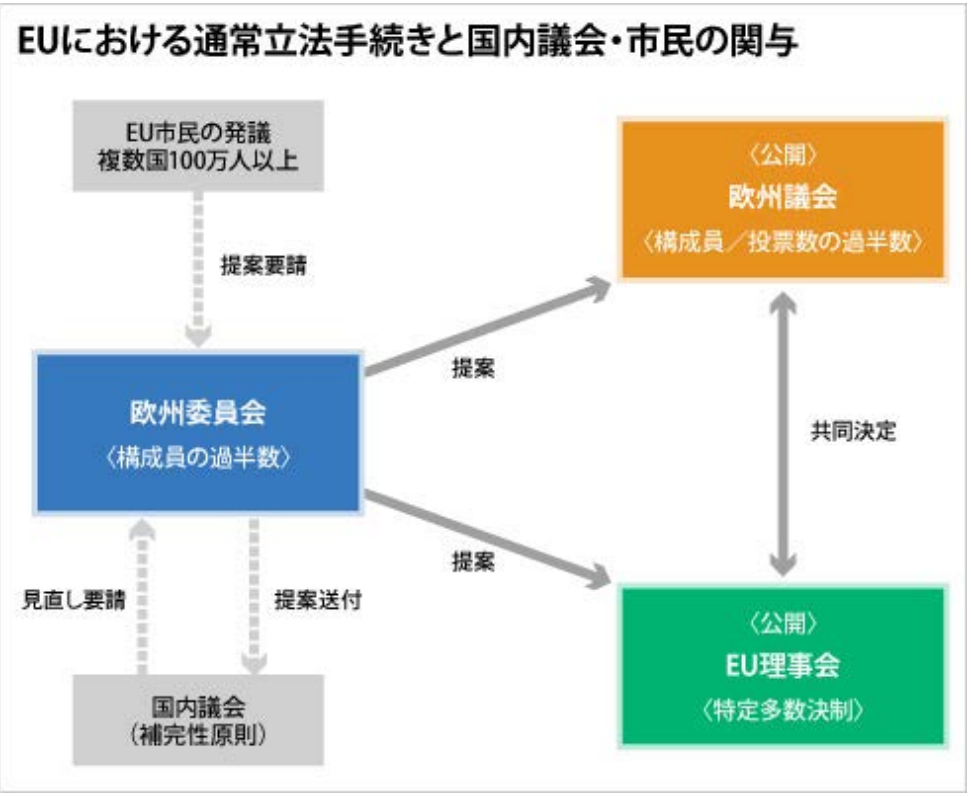
時期	法案等の状況	EU関係機関の動向	業界団体等の動向
2016年5月	GDPRの採択		
2017年1月	欧州委員会がePrivacy規則案を発表		
2017年4月		第29条作業部会が意見を発表	
2017年4月		EDPS（欧州データ保護観察官）が意見を提出	
2017年7月			IAB EuropeがePirvacy規則に対するポジションペーパーを公表
2017年9月			ICDPが、欧州議会の議員に向けた、ePrivacy規則が業界に与える影響について説明した書簡に署名
2017年10月	欧州議会LIBE（市民的自由・司法・内務委員会）で修正採択	EDPSが再度意見を提出	
2017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	閣僚理事会、修正版ePrivacy規則案を発表		
2018年3月	閣僚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回総会にてePrivacy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	閣僚理事会が新たな規則案を発表		
2018年9月	閣僚理事会が新たな規則案を発表		
2018年10月	閣僚理事会が新たな規則案を発表		
2018年11月			IAB europeがePrirvacy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

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。



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。

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

ePrivacy規則（案）の構成

- 2018年10月に閣僚理事会が公表したePrivacy規則（案）の構成は以下のとおり。

Article	項目	Article	項目
1	目的	15	公的に利用可能なディレクトリ
2	実態的範囲	16	依頼していないダイレクトマーケティング
3	領域的範囲と代表	~~17~~	~~【削除】検出されたセキュリティリスクに関する情報~~
4	定義	18	独立監督機関
4a	同意	19	欧州データ保護会議
5	電子通信データの秘密	20	協力及び手続の一貫性
6	電子通信データの許容される処理	21	救済
7	電子通信データの保存及び消去	22	補償の権利と責任
8	エンドユーザーの端末機器情報の保護	23	行政制裁金を課す際の一般条件
~~9~~	~~【削除】同意~~	24	罰則
~~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~~	25	委任法令の運用
11	制限	26	コミッティー*
12	発着端末識別情報の保存及び制限	27	廃止
13	発着端末識別情報の保存及び制限、着信拒否、緊急サービスの提供に関する例外	28	モニタリング及び評価条項
14	着信のブロッキング	29	施行及び適用

青地で削除されているものは、委員会当初案（2017年1月版）から削除されたものを示している。

*COCOM（Communications Committee）が、欧州委員会の執行権限を遂行することを支援することを記載している。

EU関係機関の意見の要点

- 現代社会において、電子通信は思想や宗教、表現、集会の自由等、基本的な権利の行使にあたって重要な役割を果たしており、通信の秘密が守られることの必要性は増している。
- GDPRに規定されたデータ保護レベル以上の保護や、既存のePrivacy指令以上の保護をePrivacy規則で確保するべき。
  - 技術中立的な形で、**OTTサービスも含めたあらゆる形式の電子通信（M2M通信・クラウド上の電子通信データ等**も含む）を規制対象とすること。
  - 通信の秘密の原則がコンテンツ・メタデータ双方を包含することを明記し、**コンテンツとメタデータを同等の保護**にすること。
  - ユーザの同意に基づかない処理、例えば「正当な利益」に基づく電子通信データの処理が行われる可能性を排除すること。
  - トラッキングの許可が得られないことを理由にウェブサイトやサービスへのアクセスをブロックする**「トラッキング・ウォール*」を明確に禁止**すること。
  - エンドユーザ端末から発信される情報に対して、GDPRと同等の保護すること。
  - ブラウザ等のプライバシー設定はデフォルトでエンドユーザ端末の情報取得を拒否とすること。

*トラッキングウォールとは、ユーザが、自身の情報をそのサイトの管理者が広告目的等で使用、保存することを許可しない限り、サイトのコンテンツを読んだり見たりできなくなるようにする機能

業界団体等の意見の要点

■ ePrivacy規則（案）については、ヨーロッパのデジタル・トランスフォーメーションに対する経済的・社会的悪影響を考慮し、慎重に議論を進めるべき。

- インターネット広告業
  - ユーザが提供したデータを利活用する広告モデルにより、ユーザは無料でオンライン上のコンテンツを楽しむことができている。
  - ブラウザ等でデフォルトでユーザ端末の情報を取得しない設定とすることや、多数のウェブサイトでユーザに同意を要求することは、ユーザの利便性低下につながる。
  - 電気通信事業者に対するものと同じ規定をグローバルなプラットフォーマーに対して課した場合、**EU市場からの撤退や、機能の制限などが起こる**ことが危惧される。

- その他ステークホルダー（製造業／金融業／モビリティ産業等）
  - 通信の秘密を保護するという目的から逸脱し、個人情報とそうではない情報のどちらの処理についても大幅に制限している。
  - 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　等の分野において、**データを利活用したイノベーティブな製品やサービスを提供し続けることができなくなるほどの負担**になる可能性がある。

これまでの論点と主な意見

- 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	論点に関する主な意見		条文への反映状況
	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）	閣僚理事会案（2018年10月版）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）	「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）	欧州議会LIBEの修正採択案では追記されたものの、閣僚理事会案（2018年10月版）では削除されている。
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、閣僚理事会案には反映されていない。

論点ごとのドラフトへの反映状況
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）

- 欧州議会LIBEでの修正採択の際に、ブラウザ等のソフトウェアはデフォルトでエンドユーザの端末情報の取得を禁止する設定とすることが追記された。
- しかし、各国政府との議論において、競争上の問題等複数の疑念が提示され、閣僚理事会案（2018年7月版）では10条全体が削除された。2018年10月版でも削除されたままである。

委員会当初案(2017年１月)	欧州議会LIBE（市民的自由･司法･内務委員会）修正採択案(2017年10月)	閣僚理事会案（2018年10月版）
1.Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. 2.Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.	1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall: *(a) **by default,** have privacy protective settings activated to prevent other parties from transmitting to or storing information on the terminal equipment of a user and from processing information already stored on or collected from that equipment, except for the purposes laid down by Article 8(1), points (a) and (c);*	**（削除）**

*ブラウザのゲートキーパー化：ブラウザにエンドユーザ端末の情報の取得を禁止する機能を持たせる場合、ウェブサイトごとのユーザ端末の情報の取得可否をブラウザが判断することになる。これをブラウザのゲートキーパー化と呼ぶ。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN

論点ごとのドラフトへの反映状況
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）

- 委員会当初案8条では、ユーザ端末に保存された、及び関連した情報の保護について規定されている。ユーザ端末に保存された情報やユーザ端末から発信された情報の取得や、ユーザ端末の処理能力等の利用は原則禁止とし、例外となる場合を列挙している。
- 欧州議会LIBEの修正採択案やこれまでの閣僚理事会案でも、例外となる場合を列挙する記載としており、GDPRが許容する「正当な利益（legitimate interest）」のような包括的な記載は行われていない。（例外となる場合は追加されている）

委員会当初案(2017年１月)	閣僚理事会案（2018年10月版）
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the enduser; or (d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the enduser	1.The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or (d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user **or by a third party on behalf of the provider of the information society service provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.; or** **(da) it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose; or** **（以降、(e)ソフトウェアのアップデートや(f)緊急通報に関する例外が追記）**

*※欧州議会LIBEの修正採択案と閣僚理事会案（2018年10月版)で大きな変更がないため、欧州議会LIBEでの修正は割愛している。
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN

論点ごとのドラフトへの反映状況
③M2M通信を対象に含むことの是非（5条）

- 欧州議会LIBEでの修正採択の際に、電子通信データの秘密の範囲にM2M通信が明示され、閣僚理事会案に一時反映された。
- しかし、人と人の相互作用が限られているデバイス／ソフトウェアのアプリケーション間の通信は、EECCにおける電子通信サービス（ European Electronic Communications Code：欧州電子通信コード）の定義から外れるという意見から、閣僚理事会案（2018年月3版）では該当する文章が削除された。2018年10月版でも削除されたままである。

委員会当初案(2017年１月)	欧州議会LIBE（市民的自由･司法･内務委員会）修正採択案(2017年10月)	閣僚理事会案（2018年10月版）
Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	1. Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or any processing of electronic communications data regardless of whether this data is in transit or stored, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation. （中略） 1b. **Confidentiality of electronic communications data shall also include** terminal equipment and **machine-to-machine communications** when related to a user.	Electronic communications data shall be confidential. Any interference with processing of electronic communications data, such as by including listening, tapping, storing, monitoring, scanning or other kinds of interception, or surveillance or and processing of electronic communications data, by anyone other than the end-users concerned, shall be prohibited, except when permitted by this Regulation. **（1b.の記述は削除）**

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN

論点ごとのドラフトへの反映状況
④トラッキングウォールの許容可能性(8条）

- 欧州議会LIBEでの修正採択の際には、トラッキングウォール*を禁止することに加え、サービスのビジネスモデルがターゲティング広告によるものであってもデータ処理への同意は得られない、と記載された。
- 一方で、閣僚理事会案には反映されず、2018年10月版でも反映されていないままである。

委員会当初案(2017年１月）	欧州議会LIBE（市民的自由･司法･内務委員会）修正採択案(2017年10月）	閣僚理事会案（2018年10月版）
（なし）	**1a. No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of processing or storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.**	**記載されていない**
Recital 24 (略)	**Recital24** **（略、以下が追記された）** **Where a business model is based on targeted advertising, consent should not be considered as freely given if access to the service is made conditional on data processing. In such cases, the end-user should be provided with other fair and reasonable options that do not process his or her communications data, such as i.e. subscription, paid access, or limited access to parts of the service.**	**記載されていない**

*トラッキングウォールとは、ユーザが、自身の情報をそのサイトの管理者が広告目的等で使用、保存することを許可しない限り、サイトのコンテンツを読んだり見たりできなくなるようにする機能

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN

その他の論点
①エンドユーザーの端末情報の収集（8条2項）

- 委員会当初案では、ユーザ端末から発信される情報の収集は原則禁止だが、「(a)接続の確立に必要な場合」と、「(b)取得方法・目的・責任者、エンドユーザーが収集を停止・最小化するために必要な方法等の情報が明確かつ目立つ形で通知される場合」は可能とされていた。
- 最新の閣僚理事会案ではより厳しい記載となっており、エンドユーザーの同意がある場合か又は統計目的利用の場合でしか(b)の例外は認められない、とされている。

委員会当初案(2017年１月)	閣僚理事会案（2018年10月版）
2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or (b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	2. The collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment shall be prohibited, except if on the following grounds: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing or maintaining a connection; or **(b) the end-user has given his or her consent; or** **(c) it is necessary for the purpose of statistical counting that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose.** 2a. For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice is shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. 2b. For the purpose of paragraph 2 points (b) and (c), Tthe collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN

その他の論点
②電子通信メタデータの処理（委員会当初案2017年1月版）

- ePrivacy規則における「電子通信データ」は、電子通信サービスを通じて交換されるコンテンツである「電子通信コンテンツ」と、電子通信コンテンツの送信・配布・交換のために処理される「電子通信メタデータ」に分類される。（第4条）なお、電子通信データの定義については、委員会当初案から、最新の閣僚理事会案まで、大きな変更はない。
- 第5条において、電子通信データは秘密であり、その処理も原則禁止とされている。ただし、第6条に電子通信データの処理を可能とする場合が記載されている。

電子通信データ

定義：電子通信コンテンツと電子通信メタデータ
処理が可能となる場合：
(a)通信の伝送に必要な場合
(b)セキュリティを維持・復元する場合、技術的障害やエラーの発見に必要な場合

電子通信メタデータ

定義：電子通信コンテンツを送信、配布、交換するために電子通信サービスにより処理されるデータ
- 通信元や通信先の追跡・特定に使用されるデータ
- 電子通信サービスの提供時に生成されるデバイスの位置データ
- 通信の日付・時間・期間・種類等

処理が可能となる場合：
(a)法が義務付けるサービス品質への適合に必要な場合
(b)課金、相互接続料金の算定、不正利用の検知と抑止・加入、加入等に必要な場合
(c)一つまたは複数の特定された目的のためにエンドユーザーが同意した場合

電子通信コンテンツ

定義：電子通信サービスを通じて交換されるテキスト、音声、動画、画像、サウンド等のコンテンツ
処理が可能となる場合：
(a)通常のサービス提供に関して、エンドユーザーが同意した場合
(b)匿名データでは実施できない一つ以上のサービス提供に本人が同意した場合で、かつ監督機関と事前協議を行なった場合

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010
http://www.soumu.go.jp/main_content/000579806.pdf

※本ページの条文はすべて委員会当初案（2017年1月版）の内容

その他の論点
②電子通信メタデータの処理（閣僚理事会案2018年10月版）

- 欧州委員会のワーキングパーティーにおいて、電子通信メタデータの処理についてはAI/IoTの進展等の急速なデジタル化の進展を踏まえ、将来を見据えたものにする必要があるとの議論があった。（閣僚理事会案2018年7月版）
- 結果、閣僚理事会案（2018年7月版）において、GDPR第6条(4)の記載を参照し、電子通信メタデータの追加的取扱いに関する事項(2a)とセーフガード(2aa)が追記された。最新の2018年10月版でもそのままとなっている。

電子通信メタデータの追加的取扱いに関する記載（第6条）（閣僚理事会案2018年10月版）

（前略）
(2a)パラグラフ１、2に示された目的で取得した電子通信メタデータが収集された目的以外の目的のための取扱いが、データ主体の同意に基づくものではなく、又は、第 11項に定める対象を保護するために民主主義の社会において必要かつ比例的な手段を構成するEU法若しくは加盟国の国内法に基づくものではない場合、サービス提供者は、別の目的のための取扱いが、その電子通信メタデータが当初に収集された目的と適合するか否かを確認するため、特に、以下を考慮に入れる。

(a)電子通信メタデータが収集された目的と予定されている追加的取扱いの目的との間の関連性。
(b)特にエンドユーザとサービス提供者との間の関係と関連して、その電子通信メタデータが収集された経緯
(c)電子通信メタデータの性質、特に、GDPR第9条及び第10条で規定する情報を明らかにしないか否か。
(d)予定されている追加的取扱いの結果としてエンドユーザに発生する可能性のある事態。
(d)適切な保護措置の存在。

追加的取扱いは以下のすべての場合を満たす場合にのみ、互換性があると認められる。

- 情報が匿名化された状態では実施できず、また、目的を達した場合、その情報通信メタデータが削除または匿名化されること。
- 利用するデータが仮名化された情報通信メタデータに限定されること。
- プロファイリングのためではないこと。

(2aa)
(2a)項の目的のために、事業者は、

- データが匿名化されていない場合、第三者に提供してはならない。
- 事前にデータ保護影響評価（GDPR35条に基づく）を行い、規制当局（GDPR36条に基づく）に結果を通知しなければならない。
- (2a)項に基づく処理に関してユーザに通知し、いつでも、簡単かつ効果的に反対する権利を与えなければならない。ユーザの反対があれば電子通信メタデータをその目的で処理することは禁止される。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN

２．パーソナルデータの提供に関する消費者の意識

パーソナルデータ提供等に係る消費者向け国際アンケート調査　概要

- 平成29年総務省調査研究「安心・安全なデータ流通・利活用に関する調査研究」の中で実施された、国際消費者アンケート調査の結果を利用し、パーソナルデータの提供に関する消費者の不安等を分析した。

付注２　安心・安全なデータ流通・利活用に関する調査研究（パーソナルデータ提供等に係る消費者向け国際アンケート調査）

1）調査概要

本アンケート調査では、我が国を含む６か国における消費者を対象に、パーソナルデータの提供に関する認識や考え方、企業の取り組みに対する期待等について調査した。国際比較を通じて、我が国消費者に係るパーソナルデータ提供等に係る現状及び課題について分析を行った。

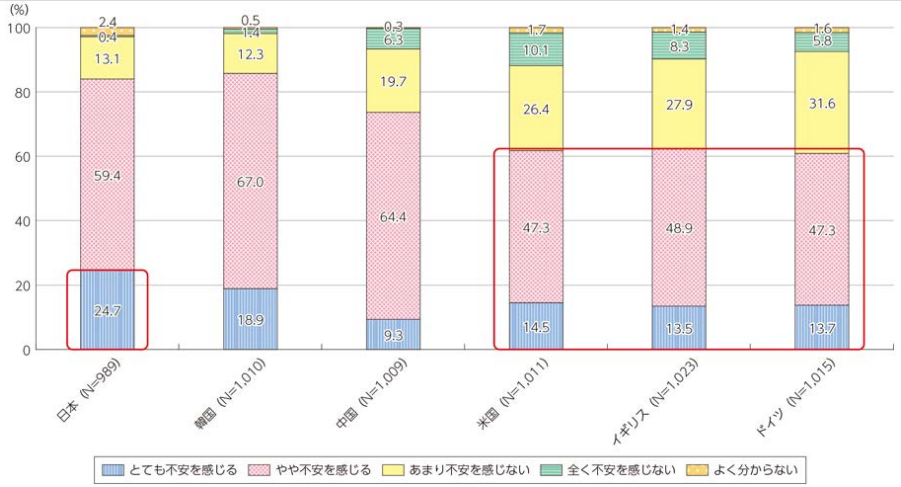
表．調査概要

項目		概要						
調査対象		日本・韓国・中国・米国・英国・ドイツの一般消費者（20 歳～ 69 歳男女）						
調査方法		インターネットアンケート調査						
抽出方法		各国のアンケート調査会社が保有するアンケート回答モニターより、性年代区分毎に均等に回収できるように抽出						
調査期間		2017 年３月						
本調査有効回答数	性年代	日本	韓国	中国	米国	英国	ドイツ	合計
	男性 20-29 歳	103	103	103	103	103	103	618
	男性 30-39 歳	103	103	103	103	103	103	618
	男性 40-49 歳	103	103	103	103	103	103	618
	男性 50-59 歳	103	103	103	103	103	103	618
	男性 60-69 歳	103	103	103	103	103	103	618
	女性 20-29 歳	103	103	103	103	103	103	618
	女性 30-39 歳	103	103	103	103	103	103	618
	女性 40-49 歳	103	103	103	103	103	103	618
	女性 50-59 歳	103	103	103	103	103	103	618
	女性 60-69 歳	103	103	103	103	103	103	618
	全体	1030	1030	1030	1030	1030	1030	6180
主な調査項目	－ICT の利用状況 －パーソナルデータの提供状況 －パーソナルデータの提供に対する認識・考え方 －パーソナルデータを提供時における条件・重視する点 －企業の取り組みに対する期待 －パーソナルデータを利用したサービスの利用意向 －PDS・情報銀行等の新たな流通モデルに対する評価							

http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/29fuchuu.pdf

パーソナルデータの提供に関する利用者の意識（国際比較）　①不安感

パーソナルデータ提供時の不安感



- パーソナルデータの提供について「不安を感じる」という回答の割合は、日・中・韓のアジア3ヶ国で 7割超であるのに対し、米・英・独の3ヶ国は6割程度で、明確な差がある。
- **我が国利用者は、「とても不安を感じる」割合が他国と比べて高い。**

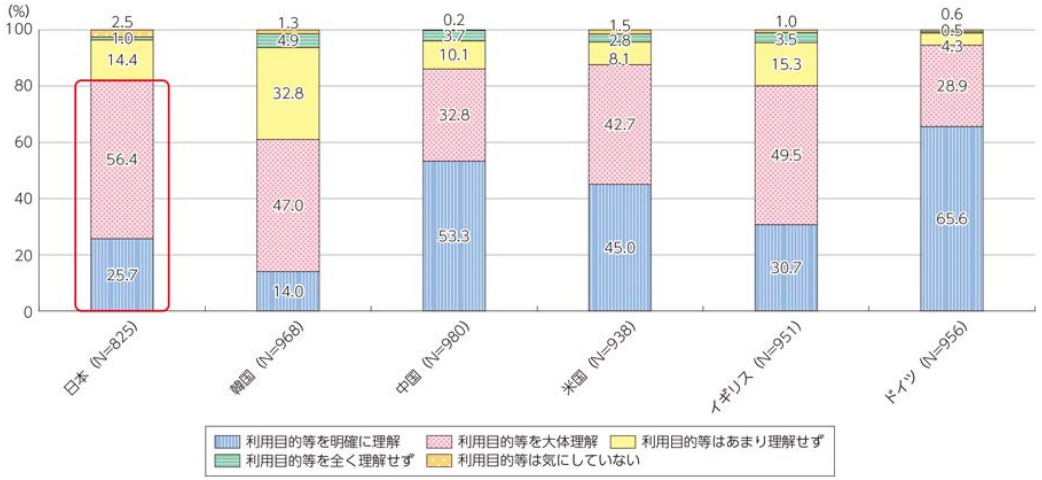
各パーソナルデータの提供に対する不安感

- 6ヶ国共通で提供に強い不安感があるデータは、「口座情報」や「公的な個人識別番号」、「生体情報」、「位置情報、行動履歴」である。
- 日・中・韓の3ヶ国は、基本情報である「氏名、住所」、「連絡先」、「生年月日」について米・英・独よりも提供に警戒心が強い。
- 日本は「Webサイトへのアクセス履歴」の提供に対する不安感が、6ヶ国で一番高い。

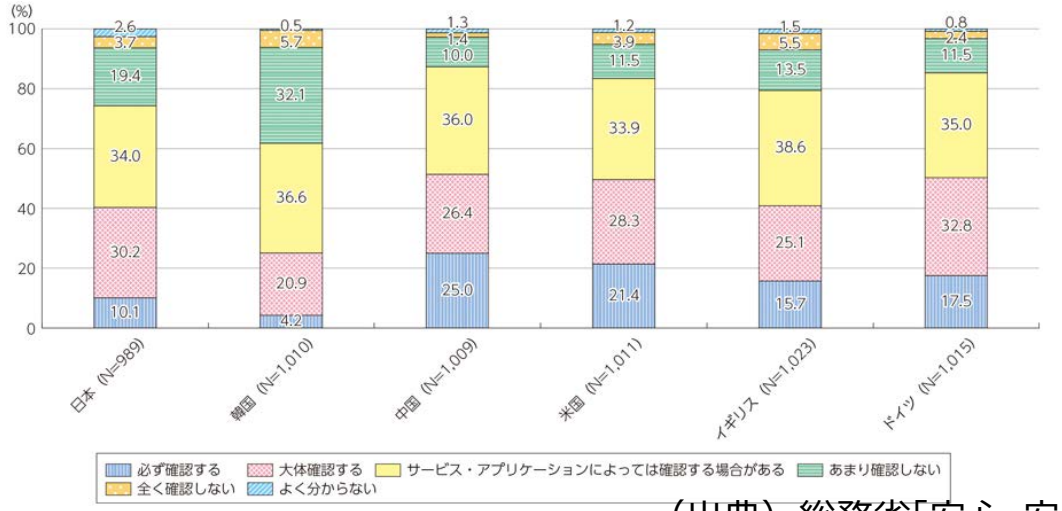
（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

パーソナルデータの提供に関する利用者の意識（国際比較）　②理解度

パーソナルデータ提供時の利用目的等の理解度



パーソナルデータ提供時の利用目的等の確認状況



- パーソナルデータ提供時の利用目的等の理解度について見ると、我が国の利用者の理解度は、「明確に理解」と「大体理解」とを合わせて8割を超えている。

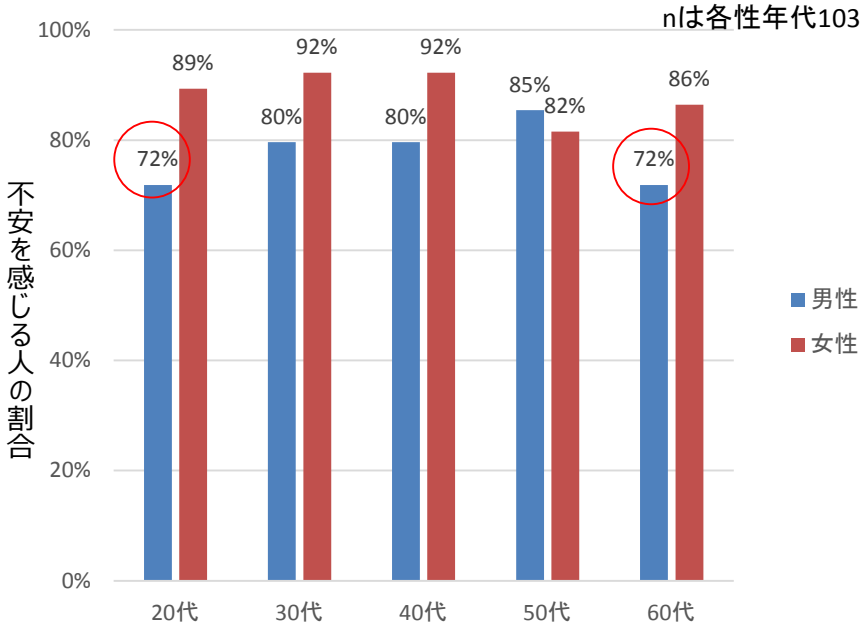
- パーソナルデータ の理解度と確認状況の関係について見ると、米・英・独・中の5ヶ国では一定の相関が見られる。

（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

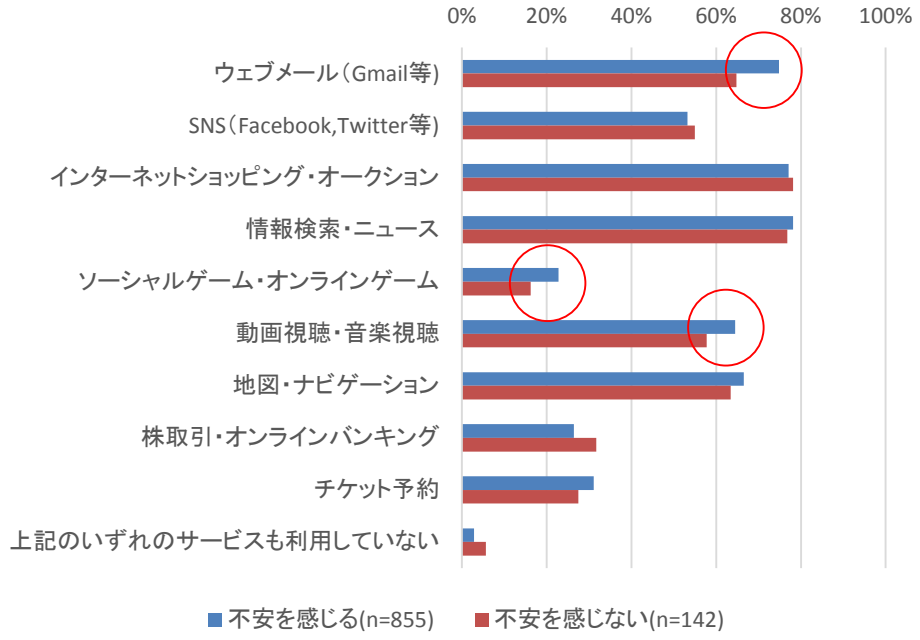
パーソナルデータの提供に関する利用者の意識　③不安感×基本属性

- 性・年代別にみると、40代を除き、女性の方が不安を感じる割合が高い。男性でも、20代と60代が特に不安を感じる人の割合が低い。
- ウェブメールやゲーム、動画・音楽視聴サービスの利用者では、パーソナルデータの提供時に不安を感じる人が多い。

パーソナルデータ提供時の不安度と性・年代の関係



パーソナルデータ提供時の不安度とサービス利用状況の関係



■分類の定義

「あなたは、企業等が提供するサービスやアプリケーションを利用するにあたり、あなたのパーソナルデータを提供することについてどのように思いますか。あてはまるものをお選びください。」という設問の回答に基づき、

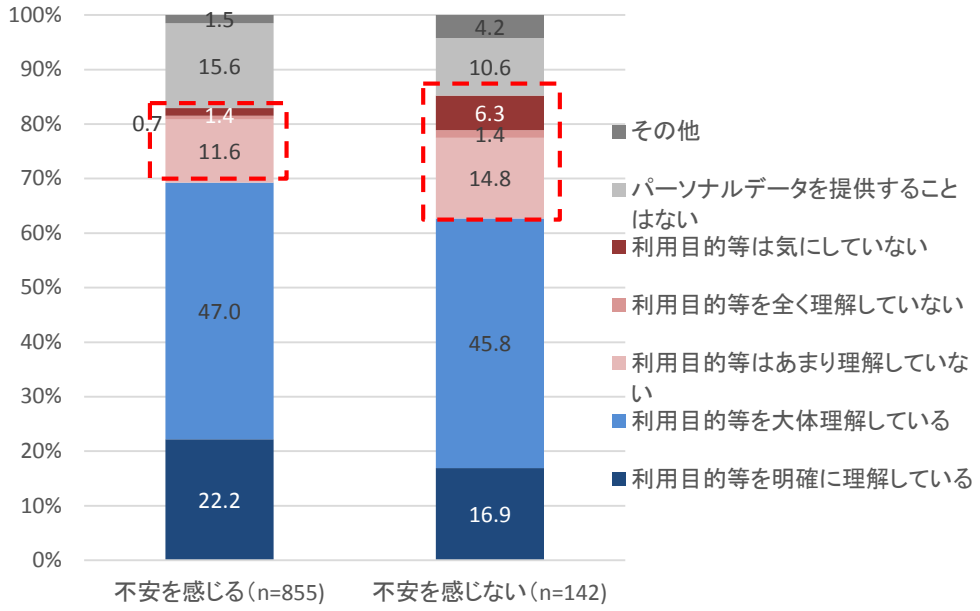
- 「とても不安を感じる」「やや不安を感じる」と回答した人を「不安を感じる」に分類。
- 「あまり不安を感じない」「全く不安を感じない」と回答した人を「不安を感じない」に分類。

（出典）総務省「パーソナルデータ提供等に係る消費者向け国際アンケート調査」（平成29年）をもとに作成

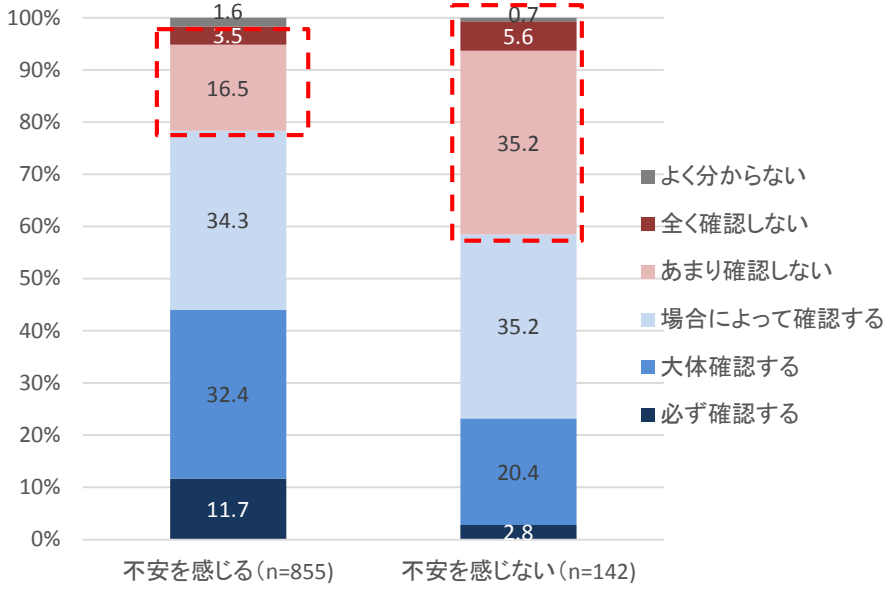
パーソナルデータの提供に関する利用者の意識　④不安感×理解度

- 我が国においては、パーソナルデータ提供時に不安を感じる人の方が、パーソナルデータ提供時の利用目的の理解度が高い。
- 同様に、パーソナルデータ提供時に不安を感じる人の方が、利用目的をよく確認している。
- 以上のことから、**パーソナルデータの提供に不安を感じない人は、不安を感じている人と比べて、利用目的を確認・理解せずに利用している人が多い傾向にある。**

パーソナルデータ提供時の不安度と利用目的の理解度の関係



パーソナルデータ提供時の不安度と
利用目的の確認状況の関係



（出典）総務省「パーソナルデータ提供等に係る消費者向け国際アンケート調査」（平成29年）をもとに作成

３．その他（構成員限り）

参考資料

【参考1-1】 第29条作業部会の意見（2017年4月）（注）

- 端末の物理的追跡をGDPRと同等の保護にすること。
  - 端末から発信（emit）された情報の利用（Wi-Fi追跡等）を、明確かつ目立つ表示による通知とオプトアウトで許容することの修正（8条2項）。
- コンテンツとメタデータを同等の保護にすること。
  - ただしスパム検知とボットネット対策を明確に許容する等
- ブラウザ等のプライバシー設定を、単なるオプション提供ではなく、デフォルトで追跡拒否とすること（10条1・2項）。
- ユーザのウェブサイトやサービスの利用について、トラッキング（追跡）の許可を条件とする「トラッキング・ウォール*」を明確に禁止すること。
- 全体として、ePrivacy規則がGDPRによる保護を下回らないようにすること。
  - EDPS（欧州データ保護監察官）もほぼ同様の事項を指摘（→【参考2】）

（注）上記は以下からの引用である。
生貝直人「EU電子通信プライバシー規則案と関連する法政策の状況」（第1回プラットフォームサービスに関する研究会　資料3、p.10）

*トラッキングウォールとは、ユーザが、自身の情報をそのサイトの管理者が広告目的等で使用、保存することを許可しない限り、サイトのコンテンツを読んだり見たりできなくなるようにする機能

http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

【参考1-2】 EDPSの意見（2017年4月） （1/2）

- ePrivacy規則に対するEDPSの立場を明らかにした。
  - GDPR第7条に規定される権利を保護するための法的手段（legal tool）としてのePrivacy規則の必要性を指摘。
    - OTTサービスも対象としている／メタデータとコンテンツ双方の保護を意図している等
  - DPA（データ保護機関）に対しては、執行力の授与と、EDPB（欧州データ保護委員会）との協力構造の構築の双方が必要。
- 問題点についても指摘している。
  - 法令としての複雑さが、各保護対象データに対する保護レベルのギャップの原因となりうる点
    - 基本的権利に関する法令である本規則に対し、自由市場に関する法令であるEECC内の種々の定義を流用している
    - そのことが複雑性の原因であると指摘し、独自の定義を採用することを提言
  - ePrivacy規則（案）の地理的範囲がGDPR第3条で規定している地理的範囲と一致するか曖昧な記載になっており、OTT事業者が第3国でデータを管理する懸念を排除できていない点
  - GDPRに規定されたデータ保護レベル以上の保護を本規則でも確保するべきである点
    - ユーザーの同意の確実な確保・トラッキングウォールの禁止・デフォルトでの個人情報保護等
  - 権利の範囲設定に関しては問題があるため要検討

https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

【参考1-2】 EDPSの意見（2017年4月） （2/2）

- 「通信の秘密」の原則がコンテンツ・メタデータ双方を包含することを明記すること
- M2M通信・クラウド上の電子通信データ等に関しても対象とすること
- 「正当な利益に基づく（under the legitimate interest ground）」メタデータの処理が行われる可能性を排除すること
- メタデータの定義において、電子通信またはサービスの提供に必要ないデータを除外しないこと（当時の提案では意図せずにそれらを除外していた）
- プライバシー保護設定をデフォルトとすること・ユーザーの自由な同意の撤回・変更機会の確保を義務とすること
- 通信の秘密の制限に関してはCJEU（欧州連合司法裁判所）の判例（EU:C:2016:970）を十分に参照し、最小限のものにとどめること ※「通信の秘密は、国家機関による犯罪対策のためのログ保存に関する立法を予め対象外と考えるべき」とする判断
  - 同時に、開示請求の透明性を確保するための規定を設けること
- DPAに対して、エンフォースメントを行う権限を認めること
- ユーザの意図しない通信（迷惑メール等）について効果的に対策すること
  - 半自動応答システム等の使用についてはユーザの同意を必要とすること
  - 意図しない通信について、識別用のcode/prefixを用意すること

https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

【参考1-3】 閣僚理事会修正（2018年3月）

- GDPRとの関係性を明確化（［修正］recital 2aa/2a）
  - ePrivacy規則が詳細を述べている部分と、あくまでGDPRを補完している部分の区別
- 第三者がデータを処理する際にGDPRに基づきデータの削除・匿名化を行う義務の明確化（［追加］recital 15a）
- 事業者がサービスの副次的機能として個人間コミュニケーションサービスを行う場合をePrivacy規則の対象に含めること（［修正］recital 11a）
  - 個人間コミュニケーションサービス：メッセージングサービス・VoIP・Webメール等
- EECCにおける定義を参照していることから不要と思われるトランスミッション層／アプリケーション層の区別に関する言及を削除（［削除］article 5）
  M2M通信におけるものも含めた「一度限りの（one-off）同意」についての言及（［追加］recital 19b）
- 緊急通報受理機関が緊急時に発信するものに限り、ユーザの同意なしに非通知電話をかけることを可能とした（［修正］article 13）
- ユーザが自分自身で電子通信データを処理することはePrivacy規則の対象外であることを明確化（［修正］recital 8）

http://data.consilium.europa.eu/doc/document/ST-6726-2018-INIT/EN/pdf

【参考1-4】 EDPBの声明（2018年5月）

- ePrivacy規則が既存のePrivacy指令の規制レベルを下げないこと
- 技術中立的な形で（in technology neutral way）、OTTサービスも含めたあらゆる形式の電子通信を規制対象とすること
- 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（「正当な利益に基づく」例外は認められない）
- 技術中立的な形で、ユーザ同意の取得方法を規定すること
  - デフォルトでプライバシーを保護する設定を適用すること
  - 透明性の確保された情報も含め、ユーザを設定に関してきちんとガイドすること
- 今後新たな例外を設ける場合は十分な検査を行うこと
  - 特に、公的機関がデータ処理を行う場合に広範な例外を設ける場合は十分に吟味すること
  - ユーザの位置情報やメタデータの無差別なモニタリングを許容するような例外は認めるべきではないこと
- 「クッキー・ウォール」（＝トラッキングウォール）は許容できないこと
- 完全に匿名化された電子通信データの活用は奨励されるべきこと

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf

【参考1-5】 閣僚理事会修正（2018年7月）

- AI・IoTをはじめとした情報通信分野における今後の技術革新の中で、EU市民の利便性とEU企業の競争力強化に資するイノベーションを阻害しないため、GDPR第6条（4）を参照しつつ、本規則に準拠して電子通信メタデータの処理をすることを可能に（［追加］article 6(2a)）
- 電子通信メタデータの保護手段について、GDPR第6条（2）で言及されているものに若干の変更を加えたものを追加した（［修正］article 6(2a)）
- 通信料金の計算等でメタデータを処理している事業者については、当該処理作業が許容されること（［修正］article 6(2)(f)）
- ユーザの端末内の情報の取得についての詳細に言及したが、当該変更がGDPR第7条（4）及び29条作業部会のガイドラインと適合的に作用するかについて議論を求めること（［修正］recital 20）
- プライバシー設定に関する項目について「同意疲れ」現象のように、ユーザの利便性とアプリ・ブラウザの利便性の双方の観点から懸念点があることから、削除も含めて議論を求めること（［削除検討］article 10）

http://data.consilium.europa.eu/doc/document/ST-10975-2018-INIT/EN/pdf

【参考1-6】 閣僚理事会修正（2018年9月、2018年10月）

■2018年9月修正

- 現在の議論において基本的な疑問点が多く生じたため、当面、前回修正案で提示された方向性に基づいて議論を行っていくが、修正に関する議論を受け付けている旨を各国に対して説明
  - GDPRと比較したときの本規則のスコープの設定の問題
  - 通信の秘密と個人データ保護の両立に関する問題
  - 位置情報の取り扱いに関する公平な競争の問題
  - 本規則等の厳しい規制と、EUの設定するAI・IoT・自動運転等の技術に関する目標の両立に関する問題
- その他、議論の収束に向けて動いている部分もある
  - 規則の厳密性等に関しては次回会合で方向性について議論
  - 情報セキュリティ施策に関連して、本規則の適用範囲を明確化（［追加］article 2(2)(f)）

http://data.consilium.europa.eu/doc/document/ST-12336-2018-INIT/EN/pdf

■2018年10月修正

- ユーザの端末の保護のための電子通信データ処理については許容すること（［追加］article 6(1)(a)）
- 児童ポルノ等の違法活動の防止に関する電子通信データの処理について国内法・EU法との関係を明記すること（［修正］recital 26）
- 各国監督官庁による本規則の運用についての記述を簡略化（［修正］article 18）

http://data.consilium.europa.eu/doc/document/ST-13256-2018-INIT/EN/pdf

【参考1-7】 ICDPから欧州議会議員/LIBEへの書簡（2017年9月/10月）

■ ICDP から欧州議会議員（2017年9月）

- 本規則により影響を受ける様々な業界団体が連名で署名した欧州議会議員への公開書簡
- 欧州議会における議論に関する多くの付属文書では以下の主要な論点について詳細に言及されているのにも関わらず、議会での意志決定に反映されていない現状を指摘している。
  - （2017年9月時点では施行されていない）GDPR・EECCとの実質的・合理的な整合性
  - ユーザの権利と自由を確保しつつ、欧州の発展に資するデジタル領域におけるイノベーションを阻害しないような柔軟性

■ ICDPから欧州議会LIBEへの書簡（2017年11月）

- ePrivacy規則（案）に関するさまざまな問題点を指摘
  - 広範な産業に対する悪影響を生じるリスク
  - データの処理方法だけではなく、加盟国の法執行機関と企業の間の関係性をも規定しているが、そうした規定には、企業やそのユーザまで含めた十分が議論が必要であること
  - GDPR・EECC等との整合性の問題
- GDPRに関連した企業の投資を無駄にしないためにも、データ保護に関する法的安定性を確保するための規則は重要であるが、上記のような状況があるなか、本規則を制定・施行することは拙速であり、更なる議論が必要である。

※ICDP：EuroISPAやIAB Europe、Japan Business Council in Europe等のEUの業界団体からなる連盟

https://www.iabeurope.eu/policy/industry-coalition-for-data-protection-writes-letter-to-meps-on-eprivacy/
http://edima-eu.org/wp-content/uploads/2017/11/ICDP-Joint-Letter-on-ePrivacy-Regulation.pdf

【参考1-8】 EDiMAの声明（2018年5月）

- 1)デジタル・コミュニケーションサービスでは、サービスの提供にあたって、電子通信データを「処理」することはほぼ不可欠である。処理できなければ、スパムフィルタ・マルウェア対策・受信フォルダの自動処理など不可能である
  →本規則第5条の適用範囲が「処理」ではなく、通信の「傍受」に限定されていることを明確にするべきである
- 2)ユーザーのデータ処理同意についての定期的確認（periodic reminder）に関して、ユーザが拒否できるように規定したことが進歩ではあるが、依然として「同意疲れ」を誘発し、結果としてユーザから選択の能力を奪いうる規定が残っている
  →本規則第9条（3）の定期的確認に関する規定を削除するべきである
- 3)附属的なコミュニケーションサービスにまで対象を広げた場合、オンライン上での活動のほとんどがこの規則の対象となることになる。国内の電気通信事業者に対するものと同じ規定をグローバルなプラットフォーマーに対して課した場合、EU市場からの撤退や、機能の制限などが起こることが危惧される
  →小規模な附属的サービスに関する規定を削除するべきである

EDiMA：Google, Apple, Facebook, Amazon Eu等が加盟する、欧州におけるオンラインプラットフォーマーの業界団体。

http://edima-eu.org/wp-content/uploads/2017/12/EDiMA-reaction-to-October-Presidency-text-arts.-1-5.pdf

【参考1-9】 ステークホルダーからTTE Councilへの書簡

■57者のステークホルダーによる書簡（2018年4月）

- TTE Council内で本規則に関する議論があまり進んでいない中、決定まではより長い時間が必要である。
  - 通信の秘密は重要であるが、EUにおけるデータ保護の法的枠組みの透明化のためにも、さらなる意見収集が必要である
- 適用範囲・GDPRとの重複
  - 既存のEU内のデータ保護フレームワークとの齟齬がありながら、それを置き換えようとしている点を問題視
  - 個人データ（GDPRの対象）と電子通信データ・端末情報（本規則の対象）で異なる規則が適用されていて、しかも前者ほどセンシティブではない後者のデータに強い規制がかけられることになる。
- 産業への影響
  - 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

■66者のステークホルダーによる書簡（2018年11月）

- GDPRとの対象範囲が重なることへの懸念を再度表明。
  - 企業にとっての透明性
  - ヨーロッパのデジタル・トランスフォーメーションに関する経済的・社会的悪影響

http://edima-eu.org/wp-content/uploads/2018/12/Joint-Letter-on-the-draft-Regulation-on-terrorist-content-online.pdf
https://www.egba.eu/uploads/2018/11/ePR-Nov.-2018-joint-letter-FINAL.pdf

【参考1-10】 IAB Europeのポジションペーパー（2018年11月）

- 合意のもとであれば、広告等のためのデータ処理を許容するべきである
  - 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。
  - 有料サービス提供必須化などの施策も不適当である。
- GDPRで採用されている原則を引き続き採用するべきである。
  - 具体的には、「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こと。
  - 具体的な例外を列挙している現状の第8条は不適当である。
- ブラウザが技術レベルでデータ処理を拒否せねばならない規定は削除するべきである。
  - その場合、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
- GDPRで得た教訓をもとに、民間企業にとって十分な移行期間を準備するべきである。
  - 具体的には、18～36か月程度

***IAB Europe**：欧州におけるオンライン広告産業の業界団体。欧州各国のIAB及びGoogle等が加盟。

https://www.iabeurope.eu/wp-content/uploads/2018/11/31.10.2018-IABEU-ePR_Position_Paper1.pdf