Vol.2018-SPT-31 No.4
Vol.2018-EIP-82 No.4
2018/11/2

Draft adequacy decision - Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan に関する一考察
通信の秘密と我が国のデータ保護に関する分析

加藤尚徳[†1]　村上陽亮[†1]

概要：我が国と EU の間では、General Data Protection Regulation（GDPR）における十分性の認定に向けた交渉が進められている。2018 年 9 月 5 日、十分性に認定に係る Draft adequacy decision - Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan が公開された。ここでは、十分性認定に向けた我が国のデータ保護に関する現状が分析されている。分析は、個人情報保護法のみならず、データ保護に係る諸法令に及んでおり、通信の秘密に係る憲法及び電気通信事業法も含まれている。本稿では、ドラフト全体を概観し、通信の秘密とデータ保護について考察を加える。

キーワード：個人情報，データ保護，プライバシー, GDPR，　十分性認定

Consideration for Draft adequacy decision - Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan

NAONORI KATO[†1]　YOSUKE MURAKAMI[†1]

Abstract: Between Japan and the EU, negotiations towards accreditation of adequacy in the General Data Protection Regulation (GDPR) are in progress. On September 5, 2018, Draft adequacy decision on Commitment Implementing Decision of XXX pursuant to regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan is published. Here, the current situation concerning Japan's data protection towards adequacy certification is analyzed. Analysis extends not only to the Personal Information Protection Law but also various laws and regulations concerning data protection, including the Constitution and the Telecommunications Business Act on Secrecy of Communications. In this paper, we overview the entire draft and discuss communication secrets and data protection.

Keywords: Personal Information, Data Protection, Privacy, GDPR, Adequacy decision

1. はじめに

2018年5月25日、GDPR（General Data Protection Regulation、一般データ保護規則、以下 GDPR）の全面適用がはじまった。GDPR では、第三国または国際機関に対する個人データの移転を行う場合に、一定の要件を課している。その要件の一つに十分性の認定がある。当該第三国または国際機関が EU から見てデータ保護の水準が満たされるものであれば、十分性の認定を行うというものである。現在のところ、我が国はこの十分性の認定を受けておらず、欧州からの越境データ移転を行う際には、その他の要件を満たしてこれを行う必要がある。

一方で、個人情報保護委員会の設立や個人情報保護法の改正など、我が国のデータ保護水準の高まりを受けて、我が国と欧州との間で、十分性の認定に向けた対話が進められている。2018 年 9 月 5 日、欧州委員会はこの十分性認定に向けたドラフトを公開した。この中には、欧州委員会が我が国の法制度をデータ保護の観点から考察した評価が記されている。様々な方面から分析がなされている一方で、通信の秘密に関する分析も含まれている。通信の秘密がプライバシーと関係性を有するものであることは従来から論じられてきたとおりであるが、直接的にプライバシー保護に、あるいはデータ保護に寄与するという点については論ぜられることは稀であった。そういった中で、十分性認定に関する文書の中で通信の秘密に焦点が当てられることは注目に値する。本稿では、ドラフト全体を概観し、通信の秘密とデータ保護について考察を加える。

†1 (株)KDDI 総合研究所
KDDI Research, Inc.

Vol.2018-SPT-31 No.4
Vol.2018-EIP-82 No.4
2018/11/2

2. 第三国または国際機関に対する個人データの移転

GDPR においては、第三国または国際機関に対する個人データの移転について、第 5 章として第 44 条から第 50 条まで関連する規定が設けられている。

2.1 一般原則

第 44 条に第三国または国際機関に対する個人データの移転に関する一般原則が「現に取扱われている又は第三国又は国際機関への移転の後に取扱いを意図した個人データ移転は、その第三国又は国際機関から別の第三国又は国際機関への個人データの転送に関するものを含め、本規則の他の条項に従い、本章に定める要件が管理者及び処理者によって遵守される場合においてのみ、行われる。本章の全ての条項は、本規則によって保証される自然人保護のレベルが低下しないことを確保するために適用される。」とさだめられている。つまり、欧州域外への越境データ移転を行う場合には、規則が定める方法に従う必要があるということが定められている。

2.2 必要な要件

第 45 条に「十分性に基づく移転」、第 46 条に「適切な保護措置に従った移転」、第 47 条に「拘束的企業準則（BCR）」、第 49 条に「特定の状況における例外」が定められている。「特定の状況における例外」には、(a)データ主体との同意に基づく場合、(b)契約の履行のため・契約締結前の措置実施のため、(c)法人との契約のため、(d)公共の利益、(e)訴訟手続き、(f)生命に関する利益保護のため、(g)加盟各国の国内法に従う場合、がそれぞれ定められている。

2.3 十分性の認定

第 45 条の「十分性に基づく移転」では、欧州委員会が当該第三国、当該第三国の地域または特定の部門、国際機関が十分なデータ保護の水準を確保していると決定した場合、当該対象への個人データの移転を個別の許諾無しに行うことができる（第 1 項）。十分性評価においては、(a)当該対象における法制度、(b)執行権限を有する監督機関、(c)国際的な取決め、に基づいて判断される（第 2 項）。欧州委員会は十分な評価をしたのち、実装行為によって決定を行うことができ、この手続きは第 93 条第 2 項による（第 3 項）。欧州委員会は当該対象において、採択された決定が機能することに対して影響を及ぼしうる当該対象内の進展を監視する義務を負う（第 4 項）等が定められている。

2.4 日欧の対話

上記の十分性の認定に向けて、日欧の間では対話が進められてきた。「個人情報の保護に関する法律に係る EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」が設けられる等、国内における制度的担保も進められてきた。

3. Draft adequacy decision - Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan

そのような中で、9 月 5 日、欧州委員会は Draft adequacy decision - Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan（以下「十分性認定に向けたドラフト」）を公開した。

3.1 概要

十分性認定に向けたドラフトにおいては、1 章では、イントロダクションとしてこの文書の背景が説明されている。2 章では、データを取り扱う事業者に課せられる規制について、日本のデータ保護のフレームワーク（2.1）、個人情報保護法の射程（2.2）、安全管理措置・権利と義務（2.3）について触れられている。3 章では、パーソナルデータの日本の行政機関による欧州からのデータ移転に関する分析がなされており、一般的な法的枠組み（3.1）、刑事法の執行を目的とした日本の行政機関によるアクセスと利用（3.2）、国家安全保障を目的とした日本の行政機関によるアクセスと利用（3.3）についてふれられている。通信の秘密については、このうち 3.1 で触れられている。

3.2 通信の秘密の取扱い

通信の秘密については、（116）において、以下のように示されている。（訳は筆者による）

“Importantly, Article 21(2) of the Constitution guarantees the secrecy of all means of communication, with limitations only allowed by legislation on public interest grounds. Article 4 of the Telecommunications Business Act, according to which the secrecy of communications handled by a telecommunications carrier shall not be violated, implements this confidentiality requirement at the level of statutory law. This has been interpreted as prohibiting the disclosure of communications information, unless with the consent of users or if based on one of the explicit exemptions from criminal liability under the Penal Code.”

「重要なのは、憲法第 21 条第 2 項は、公共の利益に関する法律でのみ制限することが許可されており、それ以外のすべての通信手段の秘密を保証することだ。電気通信事業法第 4 条では、電気通信事業者は通信の秘密を侵害してはならないとされており、法令レベルでこの機密保持要件を定めている。 これは、利用者の同意や、刑法上の刑事責任からの明示的免除のいずれかに基づく場合を除いて、通信情報の開示を禁止するものと解釈されている。」

以上のように、憲法第 21 条第 2 項と、その趣旨を反映した電気通信事業法第 4 条における通信の秘密について解説が加えられており、これらの規定が重要な役割を果たして

いることが強調されている。

3.3 Annex2

十分性認定に向けたドラフトの公開後、付属文書（Annex）として、“signed representation”が公開された。これは我が国の法務大臣が、署名入りで欧州委員会宛に送った書状である。2018 年 9 月 18 日付けで、法務大臣に加えて、内閣官房、警察庁、個人情報保護委員会、総務省、公安調査庁、防衛省の代表者が連名している。この書状は欧州委員会から日本政府への要請に応じて、日本国の政府による情報へのアクセスに関する法的枠組みの概要を示したものであることが説明されている。個人情報保護委員会がこの文章に対する欧州側とのカウンターパートになる事も明記されている。

この付属文書では、通信の秘密について以下のように触れられている。（訳は筆者による）

“(2) Limitations with respect to certain areas based on the protections provided in other laws

First, investigative authorities as well as telecommunication carriers holding personal information have a duty to respect the secrecy of communications as guaranteed by Article 21(2) of the Constitution.

Besides, telecommunication carriers have same duty under Article 4 of the Telecommunication Business Act. According to the "Guidelines on Personal Information Protection in Telecommunications Business", which have been issued by the Ministry of Internal Affairs and Communications (MIC) based on the Constitution and the Telecommunication Business Act, in cases where the secrecy of communications is at stake, telecommunication carriers must not disclose personal information regarding the secrecy of communication to third parties, except where they have obtained the individual's consent or if they can rely on one of the "justifiable causes" for non-compliance with the Penal Code. The latter relate to "justifiable acts" (Article 35 of the Penal Code), "Self-Defense" (Article 36 of the Penal Code) and "Averting Present Danger" (Article 37 of the Penal Code). "Justifiable acts" under the Penal Code are only those acts of a telecommunication carrier by which it complies with compulsory measures of the State, which excludes voluntary investigation. Therefore, if the investigative authorities request personal information based on an "enquiry sheet"

(Article 197(2) of Code of Criminal Procedure), a telecommunication carrier is prohibited from disclosing the data.

Second, business operators are bound to refuse requests for voluntary cooperation where the law prohibits them from disclosing personal information. As an example, this includes cases where the operator has a duty to respect the confidentiality of information, for instance pursuant to Article 134 of Penal Code.”

「(2) 他の法律で規定されている保護に基づく一定の領域に関する制限

第一に、捜査当局と個人情報を保有する電気通信事業者は、憲法第 21 条第 2 項によって保証されている通信の秘密を尊重する義務がある。

また、電気通信事業者は、電気通信事業法第 4 条に基づき、同様の義務を負う。総務省が憲法及び電気通信事業法に基づいて発行した「電気通信事業における個人情報保護に関するガイドライン」によれば、通信の秘密について危惧される場合には、電気通信事業者は、個人の同意を得た場合、または刑法における「正当な理由」のいずれかによることができる場合を除き、通信の秘密に関する個人情報を第三者に開示してはならない。後者は、「正当行為」（刑法第 35 条）、「正当防衛」（刑法第 36 条）、「緊急避難」（刑法第 37 条）に関する。刑法上の「正当な行為」は、任意調査を除いた国の義務的措置を遵守する電気通信事業者の行為のみである。したがって、捜査機関が「捜査関係事項照会書」に基づいて個人情報を要求した場合、（刑事訴訟法第 197 条第 2 項）において、電気通信事業者はデータの開示を禁じられている。

第二に、事業者は、個人情報の開示を法律で禁止している場合には、自主的協力の要請を拒否する義務がある。例として、刑法第 134 条に従って、情報の機密性を尊重する義務をオペレータが負う場合が含まれる。」

以上のように、日本政府から、日本が欧州委員会から十分性の認定を受けるのに十分な査証の一つとして、通信の秘密に関する説明がなされていたことが、この付属文書から理解することができる。

4. 十分性認定と通信の秘密

十分性認定と通信の秘密の間にはどのような関係性があるのか、十分性認定に向けたドラフト及び付属文書から、考察を進める。

4.1 十分性認定における憲法第 21 条第 2 項と電子通信事業法の取扱い

前述のとおり十分性認定に向けたドラフトが 9 月 5 日に公開されたが、後に公開された付属文書を見ると、十分性認定に向けたドラフトがこの付属文書に則ったものであることが理解出来る。そもそも、付属文書は日本政府が十分なデータ保護国内で行っている査証として示したものである。それでは、通信の秘密はデータ保護とどのような関係性を有しているのだろうか。これらの文書を手がかりに考察を進める。

付属文書を見ると、該当する章からも明らかであるとおり、日本国の行政機関が濫りに個人情報を取り扱うことがないことの論拠の一つとして、憲法第 21 条第 2 項及び電

気通信事業法第 4 条が示されている。特に捜査機関との関係から、電気通信事業者が、法の定める手続きに則らずに個人情報を捜査機関に提供することはないことが説明されている。これは、特に、個人情報保護委員会が公的分野を所管しないことや、個人情報保護法と行政機関個人情報保護法が別な体系として位置づけられることに対する欧州側の疑念を排除したい狙いがあることから、公的分野における個人情報の保護が多重になされていることを強調しているのではないかと筆者は考える。

一方で、興味深いのが、当然の事ながら、一般論については触れているわけで、「通信の秘密に関する個人情報を第三者に開示してはならない」の第三者は国に限られない。そもそも、総務省のガイドラインも対国家という位置づけで設けられたものではなく、むしろ、民間分野を規制する目的で設けられたことは所与の前提である。国家が国家を自主規制するルールを設けることを否定するわけではないが、ガイドラインの主たる名宛て人が国家で無いことは明白である。つまり、公的分野に限定されず、民間分野も含んだ広い範囲において、通信の秘密がデータ保護に寄与していることをこの説明は示していると言えるのではない。

4.2 従来の通信の秘密に関する解釈との比較

では、従来の議論において、通信の秘密とデータ保護の関係性はどのようなものであったのだろうか。電気通信事業法の議論を中心に概観する。

通信の秘密における「秘密」とは以下のように考えられてきた。「「秘密」とは、知られていない事実であって、他人に知られていないことにつき本人が相当の利益を有すると認められる事実をいう。本人が秘密と考えるもの（主観的秘密）が直ちに法的に保護に値するとはいえず、一般人が通常秘密にしようとする蓋然性（客観的秘密）があることが必要である。なお、通信の内容について、一見それが公知の事実や意味のない内容であっても、当事者にとって特別の意味を有する場合があり、「秘密」でないとは言い切れない。」[4]と伝統的には解釈されている。前半は宴のあと事件に見られるようなプライバシーの権利の要件に近いものを示しつつ、後半で個々の事実評価によらないことが示されている。これは、通信の秘密が「知得」から侵すことに該当することからもわかるように、秘密であるかどうかというような事実評価は不要で、秘密たり得るもの侵すことを電子通信事業法は禁じている。別な文献によれば「通信の秘密には様々な憲法的価値に関わるものが混在し得るが、事業法は、通信の主体が法人か個人か、通信の内容が思想内容に関わるものか否かといった区別をすることなく、一律に通信の検閲禁止と通信の秘密保護を定めている。実務においても、特にこれらの区別を意識することなく、一律の保護が対策がとられてきた。」[6]とされている。

他方で、我が国のデータ保護、つまり個人情報保護に目を向けると、個人情報保護法の目的である「個人の権利利益」の保護については、「プライバシーはその主要なものであるが、それに限られない」［3］とされている。現行の個人情報保護法制定当時に議論を振り返ると、制定に伴って示された付帯決議では「医療、金融・信用、情報通信等、国民から高いレベルでの個人情報の保護が求め荒れている分野について、特に適正な取扱いの厳格な実施を確保する必要がある個人情報を保護するための個別法を早急に検討すること。」とあった。通信の秘密とデータ保護の関係性は皆無であったわけでは無く、むしろ、その後の個別法に関する議論が棚上げにされてきたことが十分性に認定によって明らかになったともいえる。

しかしながら、電気通信事業法に定められた通信の秘密を基準として考えると、加えて、十分性認定に向けたドラフト及び付属文書を踏まえると、むしろ電気通信事業法のような外形判断のみによる一律の保護が、今日に資する側面を肯定できる。通信の秘密が結果的にとはいえ、データ保護に寄与していることが理解出来る。

5. まとめと今後

以上のように、十分性認定に向けたドラフト及び付属文書を通じて、通信の秘密が我が国のデータ保護に資することがわかった。従来の議論においても、通信の秘密が個人情報保護やプライバシー保護に寄与することはふれられていたが、具体的に電気通信事業法側の視点からその必要性が検討されることはなかった。国際的なデータ保護の十分性が指摘される中で、我が国においても個人情報保護法のみならず、従来のデータ保護に寄与する法律を組み合わせることによって総合的なデータ保護の可能性を模索すべきなのでは内だろうか。認定に向けたドラフト及び付属文書によって、そのような可能性が指摘されたのではないだろうか。

参考文献

[1] European Commission - Press release International data flows: Commission launches the adoption of its adequacy decision on Japan 〈http://europa.eu/rapid/press-release_IP-18-5433_en.htm/〉 (参照 2018-10-11).
[2] GDPR（General Data Protection Regulation：一般データ保護規則）〈https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/〉 (参照 2018-10-11).
[3] 園部逸夫, 藤原静雄(編著), 個人情報保護法制研究会(著): 個人情報保護法の解説, ぎょうせい (2018).
[4] 多賀谷一照(編著): 電気通信事業法逐条解説, 財団法人デッキ通信振興会 (2008).
[5] 電気通信法制研究会(編著): 逐条解説電気通信事業法, 第一法規 (1987).
[6] 藤田潔, 髙部豊彦(監), 髙嶋幹夫(著): 実務電気通信事業法, NTT 出版 (2015).