EUの一般データ保護規則（GDPR）
ー国内企業の視点ー

ヤフー株式会社　政策企画本部　政策企画部
主幹／ニューヨーク州弁護士
望月　健太

2018年5月25日

免責事項

- ✓ 本資料は、「ヤフーの公式見解」に関する3ページを除き、**筆者の個人的見解に基づくもの**であり、**ヤフー株式会社の意見や立場を代表するものではありません**。

- ✓ 本資料は、法律的またはその他のアドバイスの提供を目的としたものではありません。本資料の内容（第三者から提供された情報を含む）の正確性･妥当性の確保に努めておりますが、本資料の利用によって利用者等に何らかの損害が生じた場合にも、一切の責任を負うものではありません。

- ✓ 本資料の内容については、予告なしに変更または削除されることがあります。

- ✓ 本免責事項は、予告なしに変更されることがあります。本免責事項が変更された場合、変更後の免責事項に従っていただきます。

ヤフー株式会社の公式見解

「影響範囲を確認しながら継続的に検討中」

適用範囲：考え方のアプローチ（“対象規制”ではなく“行為規制”）

- ✓ EU域内に所在するデータ主体の個人データを持っているからといって、常にGDPRが適用され、GDPRの遵守義務を負う訳ではない。
- ✓ GDPRが適用され遵守義務を負うか否かは、**常に以下を検討する必要**。

【第1段階】どのような個人データの**取扱い**を行っているか？（実体的適用範囲）

① 全部または一部が自動的な手段による個人データの取扱い

② 自動的な手段によるものではないが、個人データがファイリングシステムに含まれる場合

③ 自動的な手段によるものではないが、個人データがファイリングシステムに含まれることを意図している場合

※「取扱い」（第4条2号）：非常に広い定義であり、自動的な手段か否かを問わず、個人データや一連の個人データに対して行われる、あらゆる単一のまたは一連の作業をいう。規定には取扱いの例が細かく規定。

※「ファイリングシステム」（第4条6号）：集約されているか否か、機能的または地理的に拡散されているか否かを問わず、特定の基準に従ってアクセスできる、あらゆる構造化された個人データの集合。

【第2段階】どこで、いかなる形で個人データの**取扱い**を行っているか？（地理的適用範囲）

① EU域内の管理者／処理者の拠点の活動に関連して行われる個人データの取扱い

② EU域内に拠点を有しない管理者／処理者による、EU域内に所在するデータ主体の個人データの取扱いであって、EU域内に所在するデータ主体に対する商品または役務の提供に関連するもの

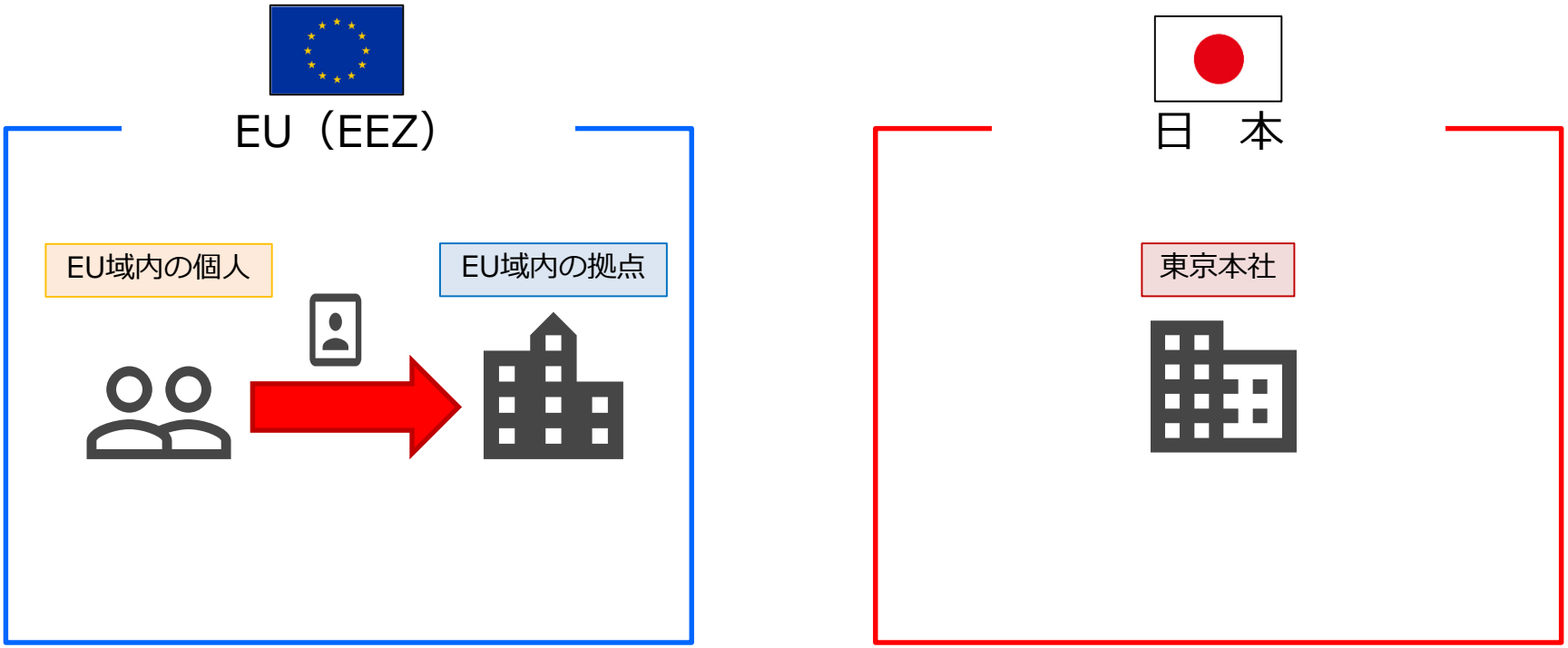
③ EU域内に拠点を有しない管理者／処理者による、EU域内に所在するデータ主体の個人データの取扱いであって、EU域内で行われるデータ主体の行動の監視に関連するもの

域内適用（第3条1項）

- ✓ EU域内の管理者または処理者の**「拠点（establishment）」の活動に関連（“in the context of”）**して行われる個人データの取扱いに適用。

  ※「拠点」の定義に該当するためには、特定の役務を提供するために必要な人的および技術的な資源が恒久的に利用可能であることが求められると解されている（データ保護指令に関する第29条作業部会意見書（WP179））。

- ✓ その取扱いがEU域内または域外で行われるか否かは問わない（前文（22））。

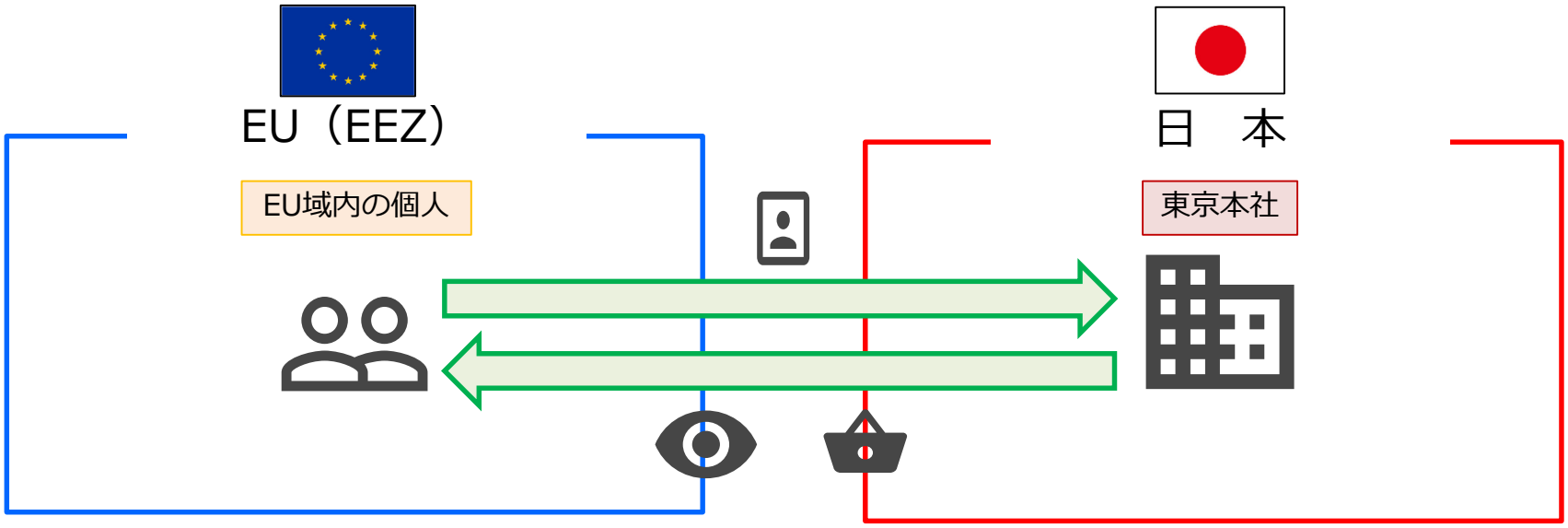


域外適用（第3条2項）

✓ EU域内に拠点を持たない管理者または処理者によるEU域内に所在するデータ主体の個人データの取扱いについても、次の①または②に**関連（”related to”）**している場合、GDPRが域外適用：

①EU域内に所在するデータ主体に対する**商品または役務の提供**
（支払いが請求されるか否かを問わない）

②データ主体のEU域内の**行動のモニタリング**



☆現在、第29条作業部会が、地理的適用範囲（第3条）に関するガイドラインを策定中のため、本規定の解釈についてはこれを待つ必要がある。

域外適用（第3条2項）

① 域外適用その１（第3条2項（a））

EU域内に拠点を持たない管理者／処理者によるEU域内に所在するデータ主体の個人データの取扱いであって、EU域内に所在するデータ主体に対する**商品または役務の提供に関連**するもの（※支払いが請求されるか否かを問わない）

【判断要素（前文（23））】 *これらは例示列挙であって、関連する監督機関が総合的に勘案し判断。

管理者／処理者が、EU域内の1以上の加盟国におけるデータ主体に対して、商品または役務を提供すると**想定していることが明らか**か否か？

- 1以上の加盟国で一般的に使用されている**言語**
- 1以上の加盟国で一般的に使用されている**通貨**
- EU域内の顧客やユーザーへの**言及**

※もっとも、以下の事項のみでは、管理者／処理者の意思を認定するには不十分。

1. EU域内において、管理者、処理者、媒介者のウェブサイトに単にアクセス可能であること
2. 電子メールアドレスや他の連絡先情報に単にアクセス可能であること
3. 管理者が所在する第三国において一般的に使用される言語が使用されていること

域外適用（第3条2項）

① 域外適用その２（第3条2項（b））

EU域内に拠点を持たない管理者／処理者によるEU域内に所在するデータ主体の個人データの取扱いであって、**同データ主体によるEU域内における行動のモニタリングに関連**するもの

【判断プロセス（前文（24））】適用の有無に関し、関連する監督機関が確認すべき事項。

EU域内に所在するデータ主体による、EU域内における何らかの行動を
モニタリング（監視）しているか？

↓

自然人がインターネット上で**追跡**されているか？
（その上で自然人のプロファイリングからなる個人データの処理技術を使用する可能性を含む）

↓ “とりわけ（particularly）” ↓

個人に関する何らかの**決定**を
行うためか？

個人的な嗜好、行動、および言動を
分析または**予測**するためか？

※「モニタリング（監視）」の具体例
①オンライン行動ターゲティング広告、②市の公共交通システムを使った個人の旅行データ（トラベルカード経由の追跡）、③リスク評価目的のプロファイリング・スコアリング（信用評価、保険料の確定、詐欺防止、資金洗浄の発見）、④アプリによる位置情報の取得、⑤ウェアラブル端末を通じた個人の健康データの採取・分析、⑥クラウドサービスが追加のストレージを提供するために個人データの使用状況を把握、⑦cookie等を用いたEU域内の閲覧者のウェブサイトへのアクセス状況の解析・検索内容の評価、等。

執行：課徴金（第83条）

※課徴金は、個別の事案毎に、課徴金以外の執行措置に**加えて**、または**代えて**賦課。課徴金には、**効果性・均衡性・抑止性**の原則があり、個別の事案、そして事前・事後の対応に応じた金額となる。

管理者／処理者による個人データの取扱い

域内適用

【1】　EU域内の「拠点」の活動に関連する場合（第3条1項）

※取扱い自体は必ずしもEU域内で行われる必要はない

○監督機関による課徴金の賦課（域内適用時）

- 各EU加盟国の監督機関が課徴金を賦課する権限を有する（第58条2項(i)）

※EU域内に管理者／処理者の「拠点」がある場合、その「拠点」に対し（を通じて）課徴金を賦課するとみられる。

〔参　考〕

- 監督機関の権限に関する第58条の中で、「代表者」への明示的言及があるものは、情報提供を求める捜査権限に関する1項（a）のみ。
- 第58条2項(j)には、第三国または国際組織の受信者へのデータ流通の停止命令に関する規定があるが、命令の名宛人は明記されていない。

域外適用

【2】　EU域内に「拠点」が存在しない場合（第3条2項）

①EU域内に所在するデータ主体に対する商品または役務の提供に関連する取扱い

または

②データ主体のEU域内の行動のモニタリングに関連する取扱い

- 管理者／処理者は、EU域内の「代表者」を書面で指定する必要（第27条）
- 「代表者」を書面で指定しなかった場合、課徴金の可能性（第83条4項（a））

○監督機関による課徴金の賦課（域外適用時）

- 前提として、管理者／処理者によるGDPRの不遵守の場合には、代表者が執行手続に服するべき（"should" be subject to enforcement proceedings）との規定あり（第27条に関する前文（80））
- 他方、各EU加盟国の監督機関の課徴金賦課権限（第58条2項（i））の規定に「代表者」への明示的言及はないが･･･