欧州の新データプライバシー法に関する最新情報
（2,000万件のデータに関する質問）

※）本資料は、APRC 2017 (9月 at.モンゴル)でMRS代表が行った講演資料を、許諾を得て日本語訳したものです。

Debrah Harding
Managing Director
MRS（英国市場調査協会）

本日のトピックス

- 規制の概要
- GDPR（一般データ保護規則）の重要要素10点
- GDPR施行に備える10の活動
- 質疑応答

文脈理解のために

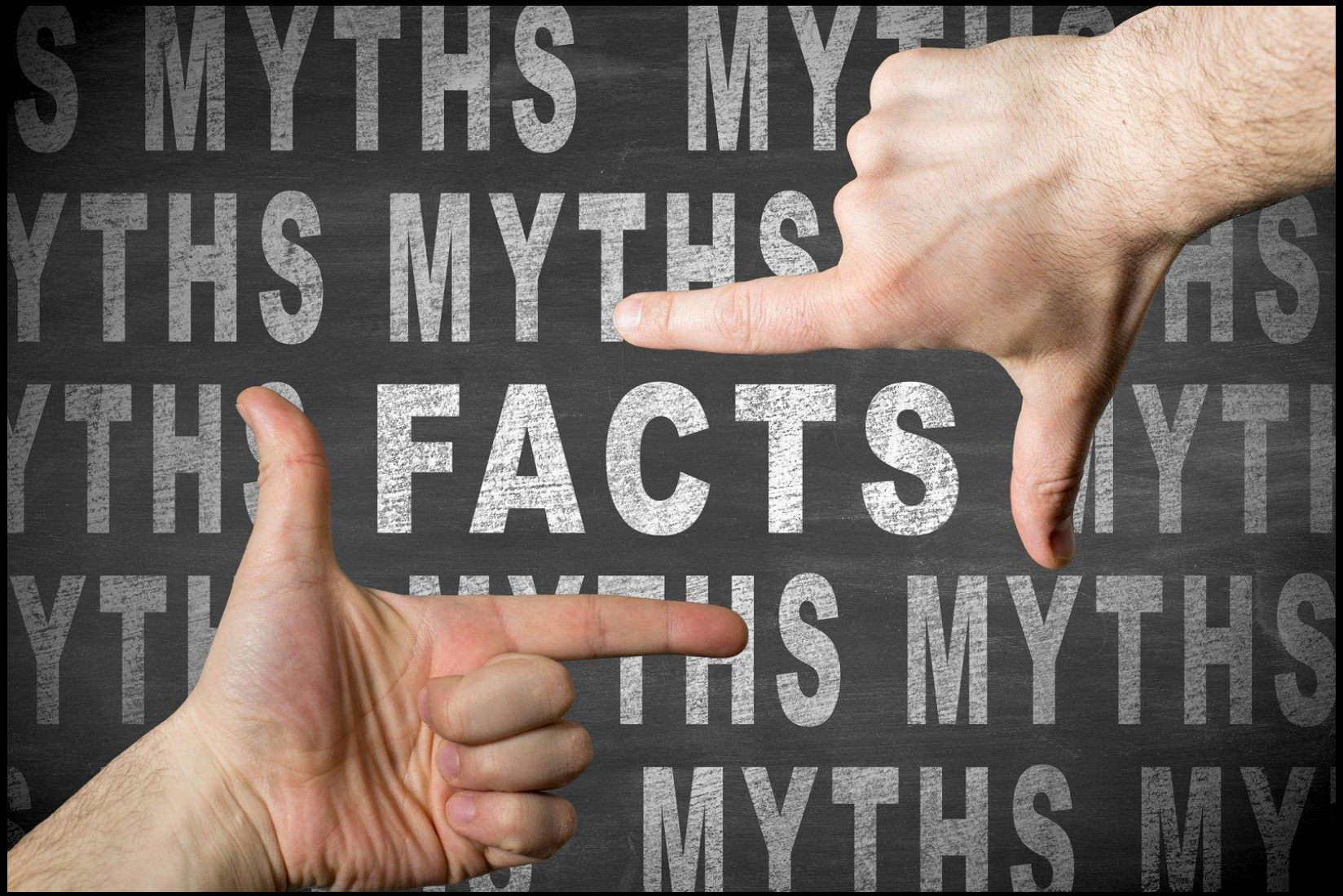
- **2018年5月25日施行**

- **進化的ではあるが、革命的ではない:**

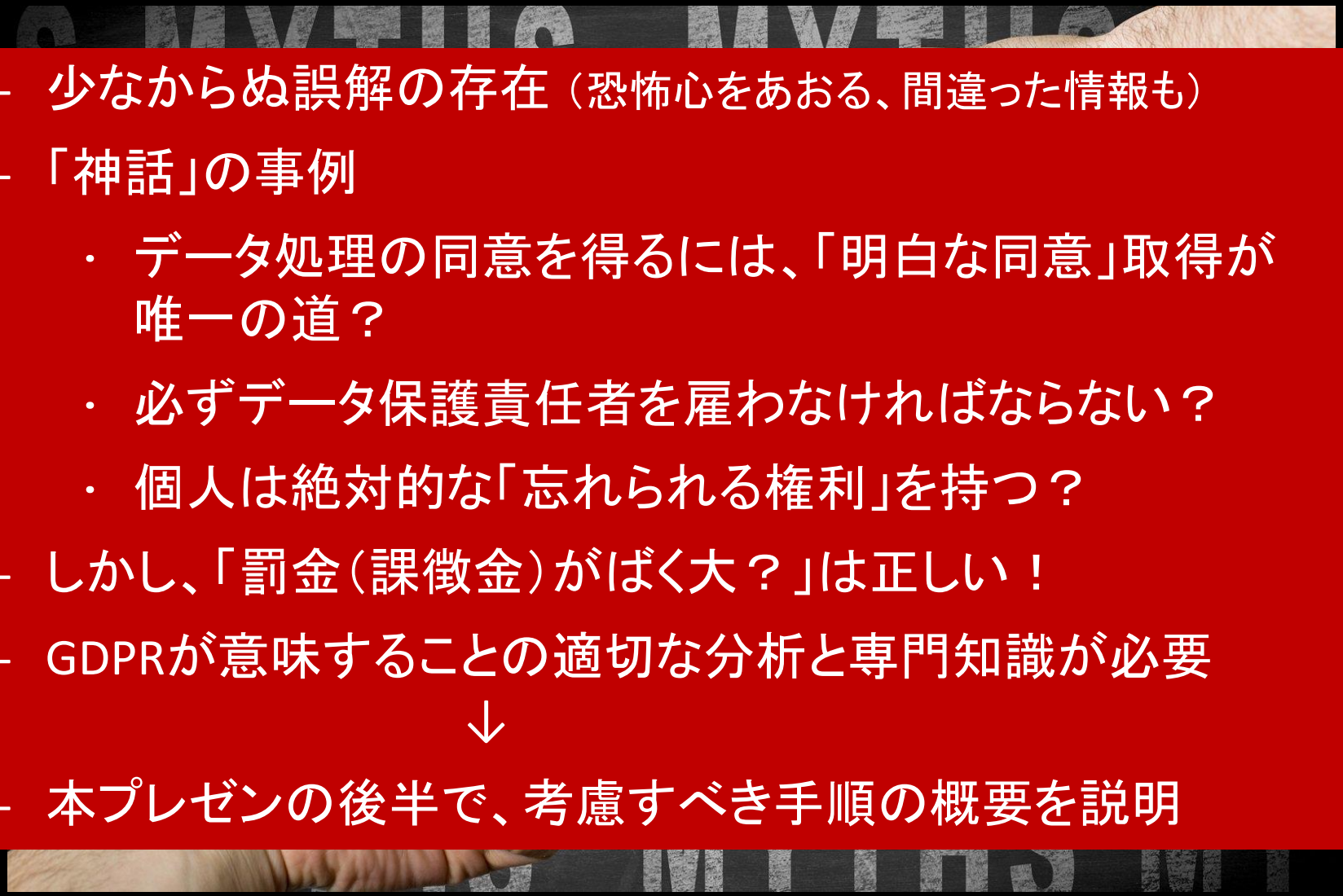
公平性、透明性、正確性、安全性、
最小化、個人の尊重 …
⇒ 基本思想は現行の法規制と変わらない（が…、）

- 個人の権利の（いっそうの）強化
- ビジネスに関する説明責任の増加
- プライバシー優先主義を埋め込むことに焦点をあてた

「神話」と事実



「神話」と事実

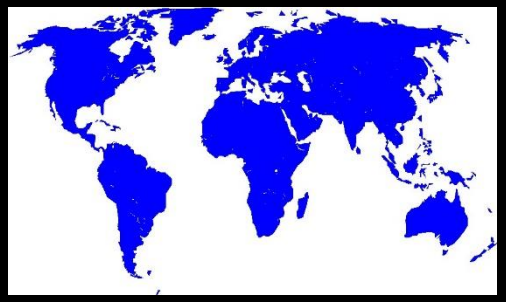


- 少なからぬ誤解の存在（恐怖心をあおる、間違った情報も）
- 「神話」の事例
  - データ処理の同意を得るには、「明白な同意」取得が唯一の道？
  - 必ずデータ保護責任者を雇わなければならない？
  - 個人は絶対的な「忘れられる権利」を持つ？
- しかし、「罰金（課徴金）がばく大？」は正しい！
- GDPRが意味することの適切な分析と専門知識が必要

↓

- 本プレゼンの後半で、考慮すべき手順の概要を説明

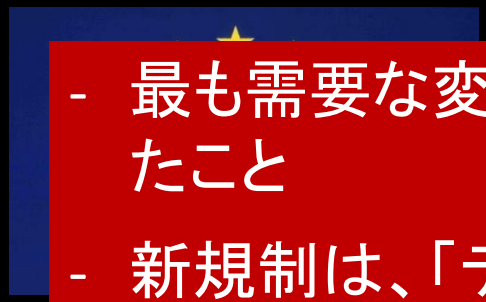
要素1:
適用地域の拡大



注）Brexitの影響？

- 英国政府として、GDPRの施行は承認済み
- 中長期的にはともかく、短期的な影響はない見込み

要素1:
適用地域の拡大



- 最も需要な変更の1つは、EU圏外にも適用対象領域を広げたこと
- 新規制は、「データ主体（＝個人）」の権利を最重視
  ⇒ データのある場所だけでなく、処理される場所にも着目
  - EU域内の個人を対象とするビジネスすべてが対象
  - 市場調査を含む、個人の行動データ収集も対象
- （日本を含む）どの国の会社でも、EU市民が対象ならGDPR規制を遵守しなければならない
- 規制対象となる組織（企業）では、EU内に居住する代表者を任命しなければならない

要素2:
GDPRと国内法の関係

- 現行のプライバシー保護体制は「指針」にとどまる:

  各EU加盟国は独自の法律を持ち、独自の解釈を行っている（行うことができていた）

- GDPRは、全加盟国が採択した規制（＝国内法不要）

  … ただし、加盟国は雇用や調査の領域を含む、特定分野に対する（独自の）法規制を行うことができる

  ⇒ 加盟国ごとの変更については注視していく必要

要素3: 設計とデフォルトによるプライバシー保護

- 哲学的なアプローチ:

「プライバシー（保護）は基本的人権の一種」

- 「設計とデフォルトによるプライバシー保護」は、GDPR の根幹をなす思想:

① 透明性（十分な情報が提供されること）と、
② 説明責任（事業者がデータ保護に責任を負う）
によって担保される

⇒ ITシステム設計、組織の行動原則等に織り込む

要素4:
個人データの定義

- 個人データの定義が拡大された:

  直接的か間接的かを問わず、識別可能な（誰であっても）生きている個人からのデータ

- 個人のものであろう、オンライン上のデータ:

  オンライン上の識別子、デバイスの識別子、クッキーID、IP 識別子など（GDPRの「前文」で特に強調されている）

- 特別なカテゴリーのデータ（機微なデータ）:

  従来の機微な情報に加え、遺伝的および生物学的なデータを含む、今日までに拡張・保持されてきた階層のデータ

要素5: 子 供

- 子供:（現行指針には特に規定がなく、新たに導入される）

  13才未満の子供は、オンラインサービスに関連して個人データの処理を許諾することは決してできない（⇒ ソーシャルメディア使用者は要注意）

  13才～15才までの子供の場合、加盟国が年齢の制限値を引き下げるような立法化を行うのでない限り、親の同意を取得することが一般的なルールとなる

  16才以上の子供は、自身の個人データ処理に同意を与えることがあり得る（＝してもよい）

要素6: 同 意

- 同意: （「同意」と認める条件が厳しくなった）

  （個人は）いつでも同意を取り消す権利を有する

  異なる処理に対しては、別個の同意が得られない限り、（過去の）同意は無効と推定する（ことがルール）

  強制的な、または「オムニバス」への同意の仕組みは無効とみなされる – あらかじめ印の入ったチェックボックスや、行動を伴わない暗示的な同意は無効

  機微なデータについては、明示的な同意が絶対に必要

要素7: 「同意」以外の法的根拠を用いたデータ処理

- データ処理実行のために、以下の法的根拠が必要になる...
  - 契約内容の履行
  - 法的義務の遵守
  - データ主体の致命的（に重要）な利益を守ること
  - 公共の利益に係る業務の実行
  - 正当な利益に属する目的（ダイレクトマーケティング、クライアントや従業員のデータ処理、ネットワークや情報セキュリティの確保、犯罪行為の防止等）

『調査セクターのためのガイダンスノート』（2017年6月 efamro & ESOMAR)を参照

要素8:
さらなるデータ処理

- 新しくデータ処理を行うには、その目的が当初の処理目的と互換性がなければならない：（互換性を判断するには...、）
  - 当初の目的と、提案された新しい目的との関連性
  - データが収集された文脈（特に、データ管理者との関係性）
  - データの性質（特に、機微なデータや犯罪データ）
  - 提案された処理によって起こり得る結果
  - 安全性確保措置の有無 (暗号化や仮名化を含む)

要素9: データの最小化と仮名化

- データの最小化:

  個人データは適切で関連性があり、限定的なものでなければならない
  （調査実施時には必要なデータのみ収集し、分析に使用しないものは最初から収集しない）

- 仮名化: （GDPRで新たに定義された、個人データの一形式）

  追加的な（識別子等の）情報を使用することなしには、特定のデータ主体にさかのぼれないように処理された個人データ（⇒ さまざまな調査等に使用可能）

要素10:
強化された権利と罰金

- 現行の個人の権利は残され、一部は強化された
  強化された権利には、以下が含まれる:

  - 忘れられる権利
  - 新しい組織にデータを移転することを要請する権利
    （＝データを持ち運ぶ権利）
  - 特定のデータ処理に異議を唱える権利
    （例：ダイレクトマーケティング）
  - 自動化された手法による意思決定に異議を唱える権利

要素10:
強化された権利と罰金

2,000万件にのぼる
質問が主に集中

- 監督当局により、違反には罰金（課徴金/制裁金）を科される可能性がある。行政的な罰金には２つの階層がある:

  いくつかの違反行為に対しては、
  1,000万ユーロ または 全世界売上高の2%（の高い方）

  その他の違反行為に対しては、
  2,000万ユーロ または 全世界売上高の4%（の高い方）
  （基本原則の多数に違反し、当局の指示を遵守しなかった場合）

- 罰金は当局による裁量の余地が大きく、「効果的で、金額や量に比例的で、(違反行為を)断念させるように」運用されるとされている

「次」に備える 10のステップ(活動)

1. まずは、GDPRが貴組織に適用されるかどうかを判断する

⇒ 与えるとわかった場合には、以下のような活動に取り組む

2. 情報監査を実施する（二次契約業者を含む）
3. データ収集のための法的根拠を理解する
4. IT に関する契約や取り決めについて見直し、強化する
5. 処理のためのポリシー、プロセス、教育訓練について見直す
6. DPO（データ保護責任者）が必要かどうかを判断する
7. 包括的なプライバシー保護体制を構築する
8. リスクとその影響度が高い領域を特定し、優先順位付けする
9. PIA（プライバシー影響評価）を準備し、実施する
10. データ侵害通知（が行える仕組み）を準備する

「次」に備える 10のステップ(活動)

2. 情報監査では、以下の点を明らかにする…
   - 個人データはどこに保存されているか？
   - それは、どのくらい安全と言えるか？
   - 誰がデータへのアクセス権とコントロール権を持つか？
   - 第三者や他のデータ処理者と共有されているか？
   - 二次契約業者との契約内容は十分と言えるか？

3. データ収集のための法的根拠を理解する
   - 「同意」のみに依拠するか、あるいは他の根拠を使用するか？
   - 「同意」を使用する場合には、「情報の通知」が重要になる

   ⇒ 「公平かつ透明（fair and transparent）」であること
   包括的で、コミュニケーションが容易であること
   （明確に文書化され、アクセス可能であること）

   ⇒ データ処理者の連絡先、処理の目的、法的根拠、データ受信者、転送（の有無）、保管期間、アクセス権…などが含まれるべき

「次」に備える 10のステップ(活動)

4. IT 契約の見直しでは、以下の点を質問する…
   - 現行のシステムや組織で、新しい権利に対応できるか？
   - 個人からのアクセス、ポータビリティ、忘れられる権利、削除等？
   - セキュリティ対策は？（暗号化など？）
   - アクセス制限、合理的な保存期間など？

5. 処理のためのポリシー、プロセス、教育訓練では、
   - スタッフが何をしなければならないか、理解する必要あり

6. DPO（データ保護責任者）は自由に任命でき、
   - 大規模なデータ主体（個人）を定期的・体系的に監視するか、
   - 機微なデータの大規模な処理を監視する
     ⇒ 一般的に、調査機関はこの要件に該当する（＝設置が必要）
   - DPOには高い能力と権限が要求される
     ⇒ 組織内に雇用しなくとも、コンサルタントへの委嘱でOK

「次」に備える 10のステップ(活動)

7. 包括的なプライバシー保護体制は、すべての活動を完結させるために必須となる

8. リスクとその影響度の優先順位付けでは、罰則を考慮
   - 合意取得、機微なデータ、新しい権利へのシステムの互換性など

9. PIA（プライバシー影響評価）は、データフローを確認し、
   - 想定されているデータ処理内容が記述されており、
   - データ主体のリスクと処理の必要性が判断され、
   - リスクを最小化するための措置が講じられているかを評価する

10. データ侵害通知の準備では、内部手順とデータ侵害を検出するプロセスの確立が重要になる

GDPR: 継続的なイニシアティブ

規制当局によるガイドラインは作成途上：ロビー活動継続中

『GDPRのための行動規範』(EFAMRO/ESOMAR)

調査免除のためのロビー活動 (MRS/EFAMRO/ESOMAR)

正当な利益のための作業部会 (MRS/IAF)	**正当な利益のための作業部会** (MRS/DPN)	**規制対応ガイダンス**（MRSから3つのガイドを発行済み） **コンサルテーション** (MRS/EFAMRO/ /A29WP)

※）GDPRの要求水準は確かに現行法よりも高いが、市場調査業界の行動規範や倫理基準に沿ったもの
⇒ ベストプラクティスの進化的定式化と捉えよう！

Any questions?

（日本語訳）