GDPRをきっかけに考えるグローバルなアイデンティティ管理

北野晴人　,CISSP

2018年1月26日

アジェンダ

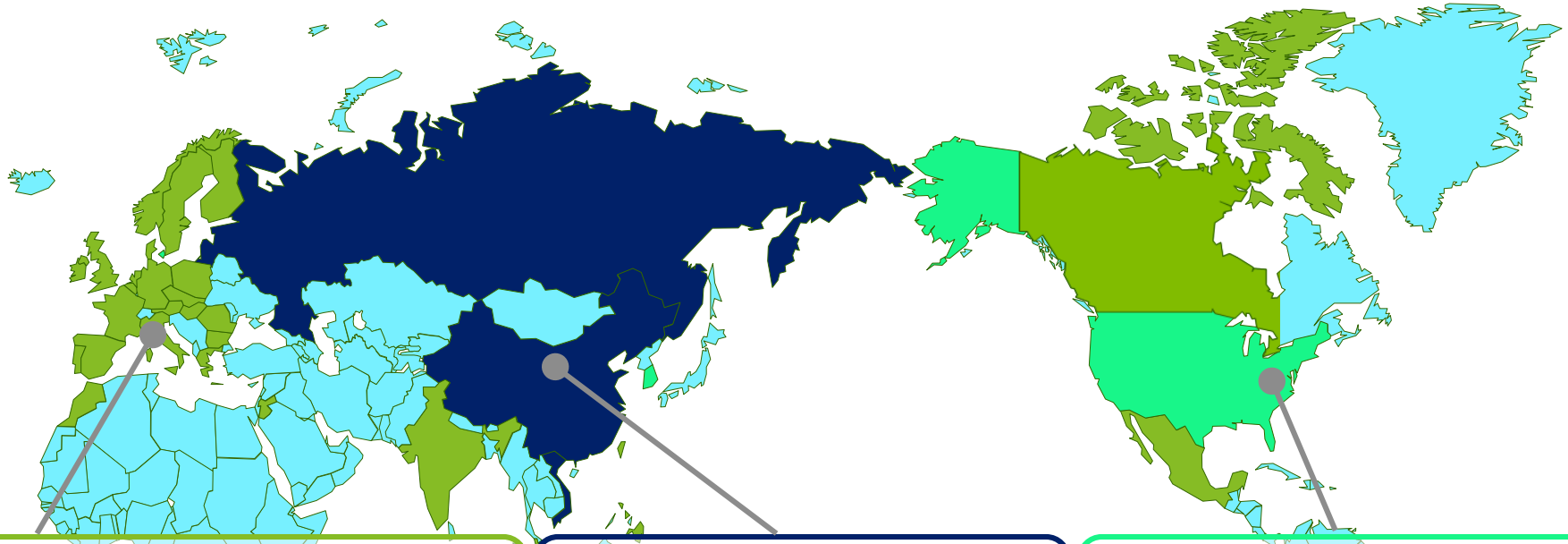
EUデータ保護指令・一般データ保護規則（GDPR）の概要

個人データに対するガバナンスとアイデンティティ管理

EU一般データ保護規則（GDPR）の概要

データの越境移転について規制が強化される傾向があります

越境移転に規制を設けている地域・国



自国・地域の法令で定められたものと同等の保護レベルまたは本人の同意を要求

- ヨーロッパ（EU加盟国およびEEA加盟国）
- 香港
- 台湾
- フィリピン
- シンガポール
- マレーシア
- カナダ（ケベック州を除く）
- メキシコ
- アルゼンチン
- ウルグアイ
- スイス

等

自国の領域内にサーバ等の設置を要求（Data Localization要求）

- ロシア
- 中国
- ベトナム

等

データを第三者へ移転することについて本人の同意を要求

- 韓国

本人より自身に関するデータの第三者への移転の停止要求に応じる必要がある国（Opt-Out）

- 米国（Gramm Leach Bliley Act 金融サービス近代化法）

EU一般データ保護規則（GDPR）は、全11章から構成されています

EU一般データ保護規則の構成

章	タイトル	概要
第1章	一般条項	規則の概要を示した上、適用範囲や用語の定義を規定している。
第2章	原則	個人データ処理に関する原則を規定している。
第3章	データ主体の権利	データ主体が有する権利を規定している。
第4章	管理者と処理者	管理者及び処理者が負う義務を規定している。
第5章	第三国又は国際機関への個人データの移転	いわゆる域外移転に関する規制を規定している。
第6章	独立監督機関	データ保護の権利と自由を保護し、個人データの自由な流通を促進するための機関の設置を規定している。
第7章	連携と一貫性	監督機関の間での連携、管理者及び処理者への対応の一貫性を確保することが規定されている。
第8章	救済、法的責任及び罰則	侵害発生時のデータ主体の救済、管理者及び処理者への罰則が規定されている。
第9章	特定の処理状況における条項	個人データ保護と表現の自由、情報の自由との関係について規定している。
第10章	委任法及び施行法	施行に関する事項を規定している。
第11章	最終規定	

義務の主体、データ種別、操作の観点から用語が定義されています

主な用語の定義

義務の主体	管理者（Controller）	単独若しくは合同で個人データ処理の目的と手段を決定する者。
	処理者（Processor）	管理者に代わり、個人データ処理を行う者。
データ種別	個人データ（Personal Data）	識別された又は識別可能な自然人に関連する全ての情報。
	特別なデータ（Special Category of Data）	人種・民族的出自、政治的見解、宗教又は哲学的信念、労働組合の組合員たる地位、遺伝データ、生体データ、健康又は性生活及び性的嗜好を現す個人データ。
操作	処理（Processing）	自動的手段で行なわれるか否かに関わらず、個人データに対して行なわれる全ての操作又は組単位の操作。
	プロファイリング（Profiling）	自然人に関連する特定の個人的側面を評価するため、特に当該自然人の職務遂行、経済的状況、健康、個人的嗜好、趣味、信頼性、態度、所在地又は行動に関する特定の個人的な側面を評価するための当該個人データの使用により構成される個人データの自動処理のあらゆる形態。

2018年5月25日から新しいルールに基づいた運用が要求されます

GDPRの主なポイント

説明責任

- 管理者は、基本原則に基づいた個人データの処理が求められる。
- 管理者は、原則を遵守していることをデータ保護機関に説明できるようにする。

データ主体の権利の尊重

- 管理者は、以下のデータ主体の権利を尊重する。

✓ 訂正権
✓ 削除権
✓ 制限権
✓ 異議権
✓ 情報の権利
✓ アクセス権
✓ **データポータビリティの権利**
✓ 自動化された個人の判断に関する権利

GDPR

データセキュリティに関する義務

- **個人データの侵害が発生した場合には、監督機関とデータ主体に対して通知しなければならない。**
- 必要に応じてデータ保護影響評価を実施する。

その他の義務

✓ **域外移転に関する対応**
✓ **データ保護責任者の選任**
✓ 代理人の選任
✓ **制裁金** など

義務に違反した場合には、最大で2,000万ユーロ又は前年度全世界売上高の4%のいずれか高い方の制裁金が課されます。

出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に弊社作成

EU域外であってもGDPRの適用対象される場合があります

域外適用

本社がEU域外であっても次の1～4に該当する場合はGDPRが適用されます

1

EU域内に子会社が設立されている場合

- EU域内の子会社は、GDPRが直接適用されるため、GDPRに基づいた個人データの処理が求められます。

2

EU域内で個人データを収集し、日本で処理を行っている場合

- Cookieなどを収集し、日本で処理している場合には、GDPRにおいて「行動の監視」（monitoring）に該当するため、GDPRに基づいた個人データの処理が求められます。

3

EU域内に業務遂行に必要な機器がある場合

- 個人データを保存するサーバなど、業務遂行に必要な機器がEU域内にある場合には、GDPRに基づいた個人データの処理が求められます。

4

EU域内へ日本から直接、商品やサービスを提供している場合

- EU域内の個人も対象として商品・サービスを提供するためWebサイトを設けており、日本から直接、商品・サービスを提供している場合には、GDPRに基づいた個人データの処理が求められます。

出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

違反時には高額な制裁金が課される可能性があります

違反の内容に応じた制裁金

制裁金	違反の内容
企業の全世界年間売上高の2%以下または€1,000万以下のいずれか高い方	• 子供の同意に適用される条件に従わなかった場合 • GDPR要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合 • 義務があるのにEU代表者を選任しない場合 • 責任にもとづいて処理行為の記録を保持しない場合 • 監督機関に協力しない場合 • リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合 • セキュリティ違反を監督機関に通知しなかった場合、データ主体に通知しなかった場合 • データ保護影響評価を行なわなかった場合 • データ保護影響評価によって示されていたにも係わらず処理の前に監督機関に助言を求めなかった場合 • DPO（Data Protection Officer）を選任しなかった場合、またはその職や役務を尊重しなかった場合
企業の全世界年間売上高の4%以下または€2,000万以下のいずれか高い方	• 個人データの処理の原則を遵守しなかった場合 • 適法に個人データを処理しなかった場合 • 同意の条件を遵守しなかった場合 • 特別な個人データの処理の条件を遵守しなかった場合 • データ主体の権利およびその行使の手順を尊重しなかった場合 • 個人データの移転の条件に従わなかった場合 • 監督機関の命令に従わなかった場合

出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

条文だけでなくガイドラインにも留意する必要があります

EU29条作業部会からは、GDPRの遵守にあたりガイドラインが発行されます。

GDPRガイドライン一覧

No.	対象事項	文書名	概要
1	Right to Data Portability （データポータビリティの権利）	Guidelines on the right to “data portability”（WP242）	✓ 本人の請求をもとに、データの開示だけでなく、技術的に可能な場合は会社は個人データを他社へ直接送信する。
2	Data Protection Officers （データ保護責任者）	Guidelines on Data Protection Officers（WP243）	✓ グループ企業は、本人や監督機関、組織内からデータ保護責任者に連絡できる状況であれば、グループに1人の選任でよい。
3	Lead Supervisory Authority （主要な監督機関）	Guidelines for identifying a controller or processor’s lead supervisory authority（WP244）	✓ 複数の国の監督機関から、主要な監督機関を特定する。
4	Notion of high risk, and Data Protection Impact Assessment (DPIA) （リスクの高い処理、データ保護影響評価）	Guidelines on Data Protection Impact Assessment (DPIA)（WP248）	✓ 処理が「本人の権利および自由に対して高いリスクをもたらす可能性」がある場合、DPIAを実施する。
5	Profiling （プロファイリング）	公表予定 （ドラフトは公表済み・パブコメ対応中）	—
6	Data breach Notification （侵害通知）	公表予定 （ドラフトは公表済み・パブコメ対応中）	—
7	Consent （同意）	公表予定 （ドラフトは公表済み・パブコメ対応中	—
8	Transparency （透明性）	公表予定 （ドラフトは公表済み・パブコメ対応中	—
9	Data transfers to third country （第三国へのデータ移転）	公表予定	—
10	Certification （認証）	公表予定	—

公表済みのガイドライン

データ主体にはさまざまな権利が認められています

データ主体の権利

同意の有効性に関する権利	データ主体は、管理者に対して個人データを提供するにあたり、必要な情報の提供を受けることができる（13条、14条）
制限権	データ主体は、管理者に対して個人データの処理を制限することができる（18条）
異議権	データ主体は、管理者又は第三者によって追求される正当な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱えることができる（21条）
削除権	**データ主体は、管理者に対して自己に関する個人データを遅滞なく削除するよう求めることができる（17条）**
アクセス権	データ主体は、自己の個人データへアクセスすることができる（15条）
訂正権	データ主体は、不正確な自己の個人データに関する訂正を管理者に求めることができる（16条）
データポータビリティの権利	**データ主体は自己に関わる個人データを、構造化され、一般的に使用され、機械によって読み取り可能な形式で受け取ることができる（20条）**
自動化された個人の判断に関する権利	データ主体は、自己に対する多大な影響を生じうるプロファイリングを含む自動処理のみに基づいた判断の対象にならないよう求めることができる（22条）

出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

個人データの域外移転には例外的な手続きが必要です

個人データの域外移転の方法（例外条項：十分性認定が得られていない国・地域への移転）

方 法	概 要
明確な同意の取得	✓ **データ主体から**個人データ移転に関する明確な同意を得ます。
拘束的企業準則 **（BCR: Binding Corporate Rules）**	✓ **グループ内で統一された情報管理を実施している場合**に選択できます。 ✓ その情報管理の方法を文書化し、監督機関に申請して承認を得ます。これによりグループ企業を包括した個人データ移転が認められます。 ✓ 監督機関に提出する文書には、SDPC(次項参照）と比べて**情報管理に関する詳細な記載**が求められ、外部専門家の助力が必要になる場合が多いといえます。
標準契約 **(SDPC: Standard Data Protection Clause)** EUデータ保護指令におけるSCC	✓ **所定の契約フォーマットを使用して、監督機関への届出・申請・承認取得等を行います。** ✓ 個別契約を取交わした企業間のみに適用され、その種類は管理者間の契約である①セットⅠ及び②セットⅡのほか、管理者と処理者の間の契約である③CtoPの3種類のフォーマットがあります。
認証 **（Certification）**	✓ EDPB又は監督機関によって承認される基準に基づいて認証されます。 ✓ 認証は3年間有効であり、延長が可能です。 ✓ **今後、認証機関が設置される予定であり、詳細は未定です。**
行動規範 **（Codes of conduct）**	✓ 業界団体がその特質を踏まえ、GDPRの遵守を目的とした行動規範を作成します。 ✓ 監督機関が適切な安全対策を講じているとして行動規範を承認した場合には、行動規範に基づいて行動する企業は、GDPRの要求事項を満たすものとされます。 ✓ **行動規範の作成、遵守状況の監視を行う機関など、未定な部分が多くあります。**

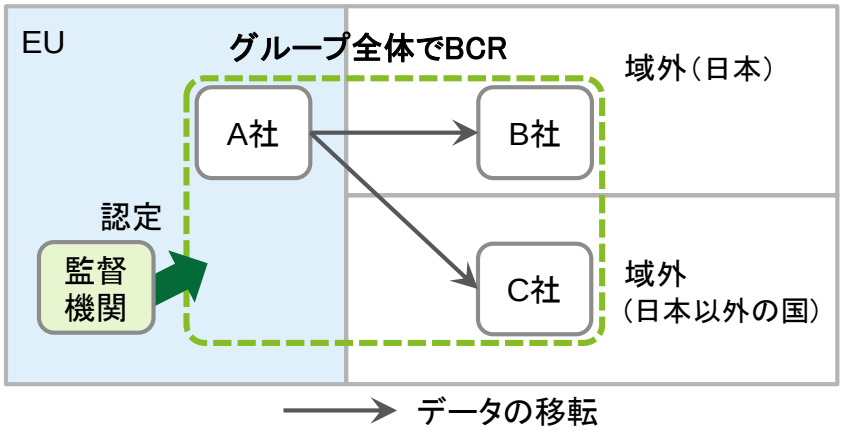
出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

SDPC、BCRなどがこれまで利用されています

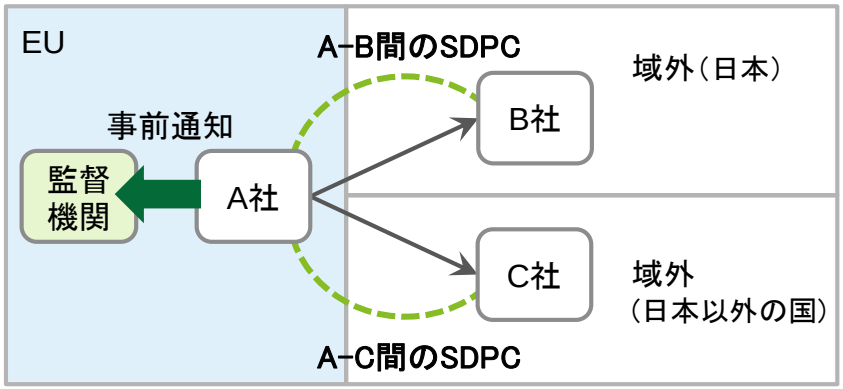
BCRとSDPCの比較

方 法	メリット	デメリット	ポイント
BCR	■ 新しいデータ移転ごとに契約を締結するといった対応の必要がなく、一つのルールによって全グループ企業を拘束することができるので、EU 域外にある多数の企業に対して個人データの移転が可能になります。	■ 監督機関による承認に時間を必要とします。 ■ 相互承認がない国の監督機関については、別途その監督機関に申請が必要になります。	■ データ移転が多数の企業間に行われる場合で、統一的なルールが強制できる場合に適しています。
SDPC	■ モデル契約を締結し、その条項を遵守するだけで、比較的容易にデータの移転を行うことができます。	■ 各企業間において個別に契約を締結する必要があります。	■ **<u>データ移転が少数の企業間で行われる場合に適しています。</u>**

BCRの例



SDPCの例



複数の監督機関から主たる監督機関を特定する必要があります

主たる監督機関（Lead Supervisory Authority）

越境処理の要件	■ 第4条（23）によれば、個人データの越境処理が、EU域内の単一の拠点の個人データの処理であるが、複数加盟国のデータ主体に実質的に影響するか、影響する可能性のある場合に、主たる監督機関を特定する必要があります。
主たる監督機関の特定	■ 主たる監督機関は　、該当する個人データの越境処理活動を管理する主たる拠点、または単一の拠点を管轄する監督機関とされています。 ■ 主たる拠点を確認するためには、まず、EU域内の管理者の統括部門を特定します。GDPRでは、統括部門はEU域内における個人データの処理の目的と手段に関する決定が行なわれる場所であるとされています。

■ 特定の例

銀行はフランクフルトに本社があり、その銀行業務はすべてフランクフルトで統括されていますが、保険部門はウィーンにあります。ウィーンの拠点がすべての保険データ処理活動を決定し、EU全体についてこれらの決定を実施する権限を有する場合、GDPR第4条（16）に見られるように、顧客の所在地を問わず、オーストリアの監督当局は保険業務を目的とした個人データの処理を監督し、ドイツの監督当局（ヘッセン監督当局）は、銀行業務を目的とした個人データの処理を監督します。

“A bank has its corporate headquarters in Frankfurt, and all its banking processing activities are organized from there, but its insurance department is located in Vienna. If the establishment in Vienna has the power to decide on all insurance data processing activity and to implement these decisions for the whole EU, then as foreseen in Art 4(16) of the GDPR, the Austrian supervisory authority would be the lead authority in respect of the cross border processing of personal data for insurance purposes, and the German authorities (Hessen supervisory authority) would supervise the processing of personal data for banking purposes, wherever the clients are located. “

出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

データ保護責任者を任命する必要があります

データ保護責任者（Data Protection Officer）

任命の条件	■ 第37条（1）によれば、以下の場合にDPOの任命を要求しています。 – 処理が公的機関または公的団体によって行われる場合 – 管理者または処理者の主活動がデータ主体の定期的及び体系的監視が大規模に要求される処理活動である場合 – 管理者または処理者の主活動が特別カテゴリのデータまたは有罪判決および犯罪に関連する個人データの大規模な処理である場合 ■ 第37条（6）によれば、DPOの自主的な任命の場合、管理者または処理者の職員（内部DPO）でも、外部者が「サービス契約に基づいて任務を果たす」こともできます。この場合、個人または組織と締結されたサービス契約に基づいてDPOの機能を実行することができますが、GDPR上のDPOではないことを明確にする必要があります。DPOが外部の場合でも、第37条から第39条※のすべての要件がそのようなDPOに適用されます。 ※GDPR 第37条～第39条 第37条　Designation of the data protection officer（データ保護責任者の選任） 第38条　Position of the data protection officer（データ保護責任者の位置付け） 第39条　Tasks of the data protection officer（データ保護責任者の職務）
任命対象	■ 第37条によれば、DPOの任命に関しては、管理者及び処理者の両方に該当します。義務的な任命に関する基準を満たす管理者または処理者が、場合によっては、管理者及び処理者両方がDPOを任命する必要があります。 ■ 「容易にアクセスできる」という条件のもと、グループ企業は単一のDPOを任命することができます。 容易にアクセスできるとは、データ主体、監督当局及び組織内からDPOと連絡することができる状況を指します。

出所：REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

管理者・処理者は、セキュリティに関する義務が課せられています

データセキュリティに関する義務

義務		概要
侵害発生前	リスクに対して適切なセキュリティレベルを確保する技術的かつ組織的措置の実施	• 仮名化、暗号化、システム復元力の確保などの措置の実施、およびこれらの措置の定期的な検査
侵害発生後	差別、個人データ窃盗、詐欺、経済的損失、仮名化の不法解除、レピュテーションの棄損、経済的または社会的損害などの個人の自由および権利にとっての危険性が高い侵害に関する通知	• 不当な遅滞なく、可能な場合には侵害に気づいてから72時間以内に監督機関へ通知する義務 • 不当な遅滞なく、データ主体にその旨を通知する義務 （処理者の場合は管理者へ通知する義務）

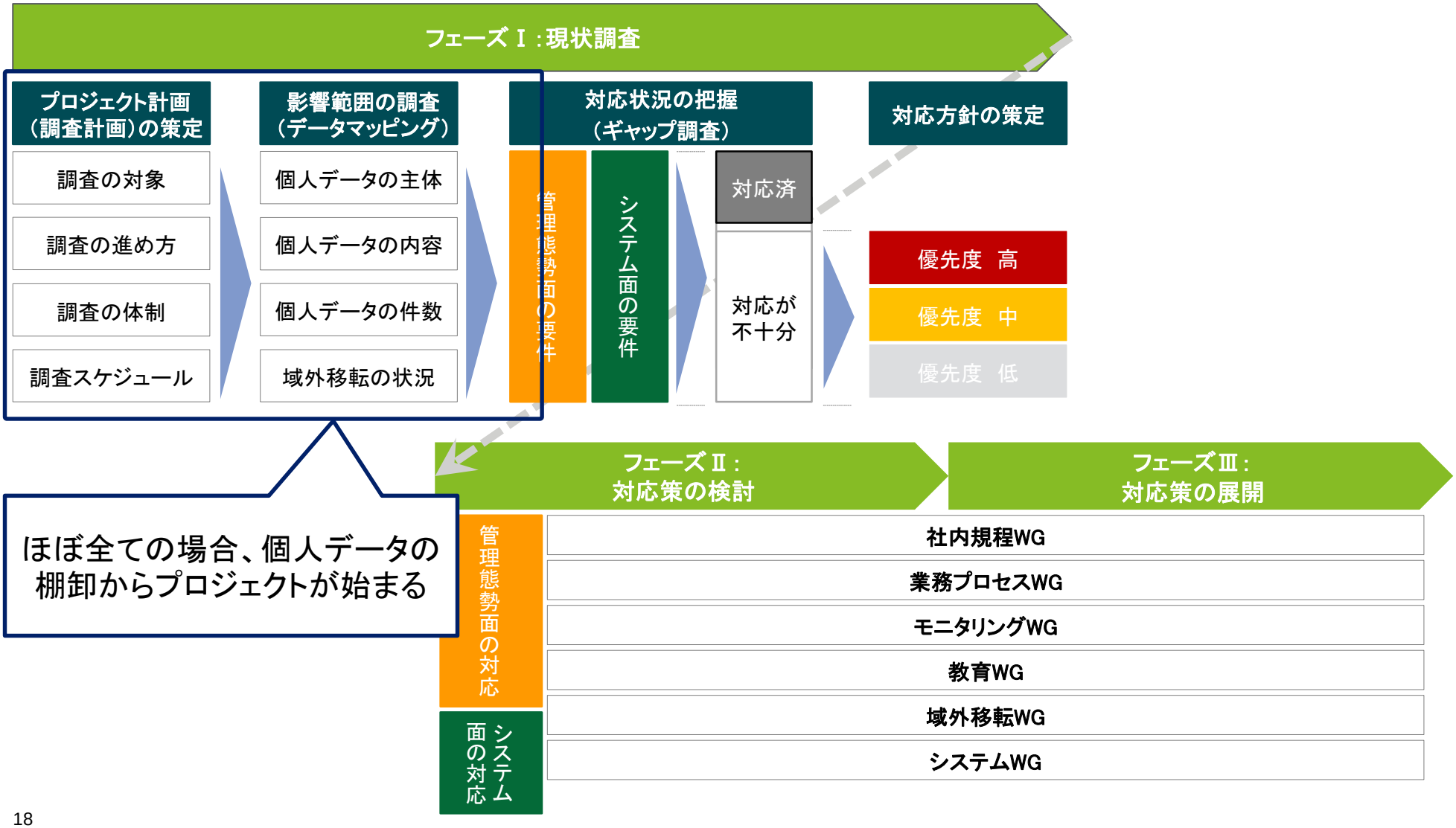
データ保護影響評価

【評価の契機】
新しい技術を使ったデータ処理で、個人の権利や自由に対するリスクが高い場合

【評価に含まれる事項】
- 想定される処理の内容や処理の目的に関する体系的な説明
- 目的に関する処理の必要性および比例性の評価
- データ主体の権利および自由に対するリスク評価
- リスクに対処するための保護措置（セキュリティ措置、個人データ保護のための管理態勢、およびデータ主体ならびに関連するその他の個人の権利および正当な利益を考慮したGDPR遵守の実証を含む）

管理態勢と情報システムの両面での対応を実施する必要がある

管理態勢や情報システムの両面で対応するプロジェクトの進め方の例



まとめ

- GDPRの要求に対応するだけでなく、これをきっかけに個人データの管理を、その後の活用も見据えて見直し、改善すると単なる法制度対応のコストではなく成長のための投資にすることができます
- 個人データの管理・保護と活用を効率的に実現することは、日本企業が今後の成長と国際競争力強化を目指すためには重要になると考えられます
- 個人に関わる多くの情報を活用するときにはプライバシーへの配慮が必要であり、GDPRをそのきっかけにすることは有用です
- アイデンティティ管理は、統合をめざすITの中でセキュリティの要となり、かつ合理化、コスト削減、コンプライアンスなどに有用な基盤となるものです