個人データの越境移転とデータベースを考える

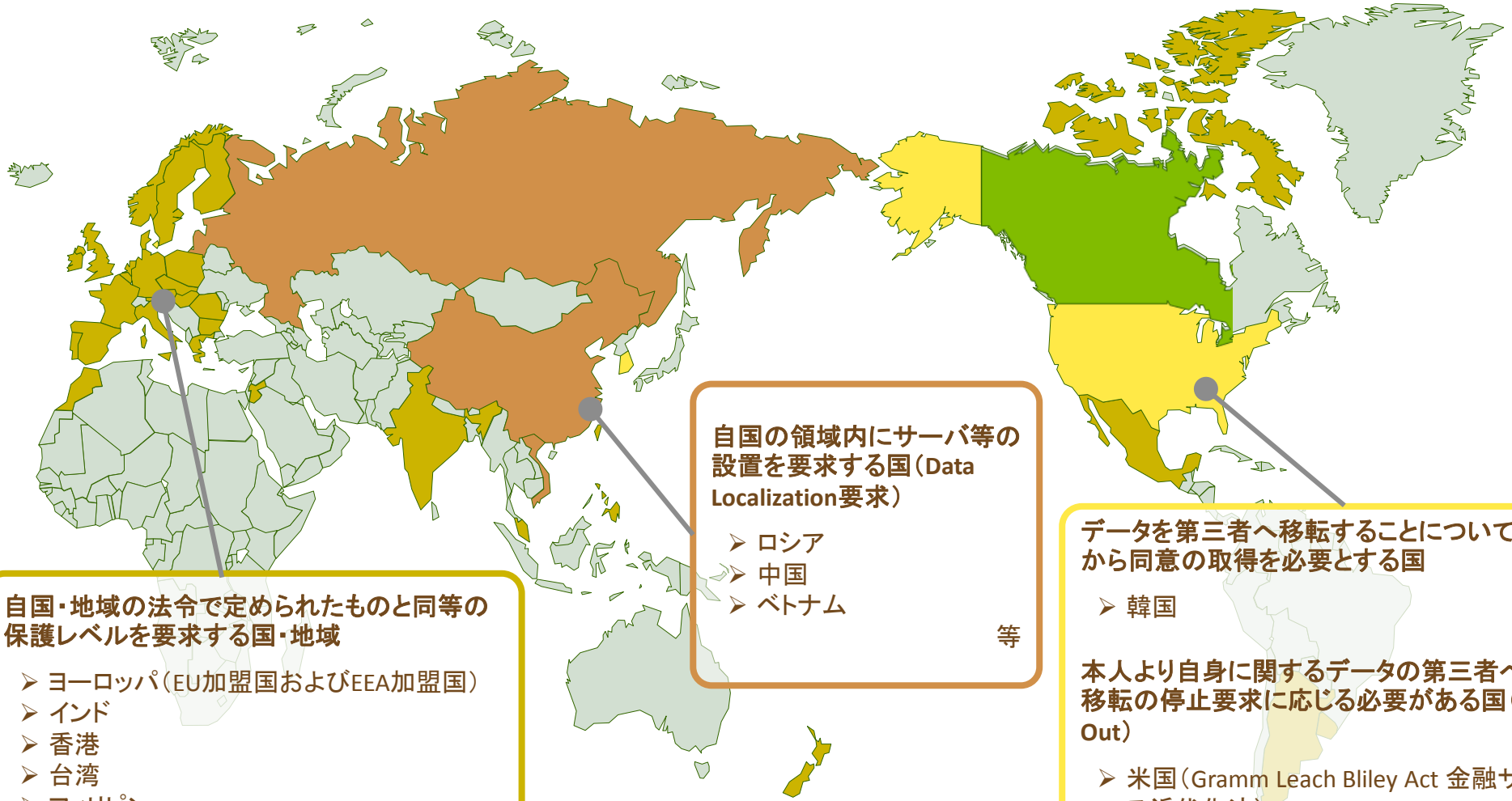
情報セキュリティ大学院大学　客員研究員　　北野晴人　PhD，CISSP-ISSJP

個人情報の活用と越境移転に関する2つのトピックス

- 人事制度のグローバル化のためグローバル人事システムを構築
- 顧客の情報をグローバルに収集・分析し、事業戦略の構築や新サービスに利用

  - 日本でシステムを構築・運用する
  - 米国などにデータセンターを持つクラウドサービスを利用する
  - 欧州に従業者がいる場合、EUからの域外移転が必要になる
  - 日本から個人情報を持ち出す場合にも制約ができた

個人データの越境移転を禁じる国が増えている



自国・地域の法令で定められたものと同等の保護レベルを要求する国・地域

- ヨーロッパ（EU加盟国およびEEA加盟国）
- インド
- 香港
- 台湾
- フィリピン
- シンガポール
- マレーシア

等

自国の領域内にサーバ等の設置を要求する国（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から同意の取得を必要とする国

- 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）

GDPRにおける越境移転の方法

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。
承認された契約	✓ 監督機関により承認された契約条文に基づきます。
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。**
行動規範の遵守 **（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。**

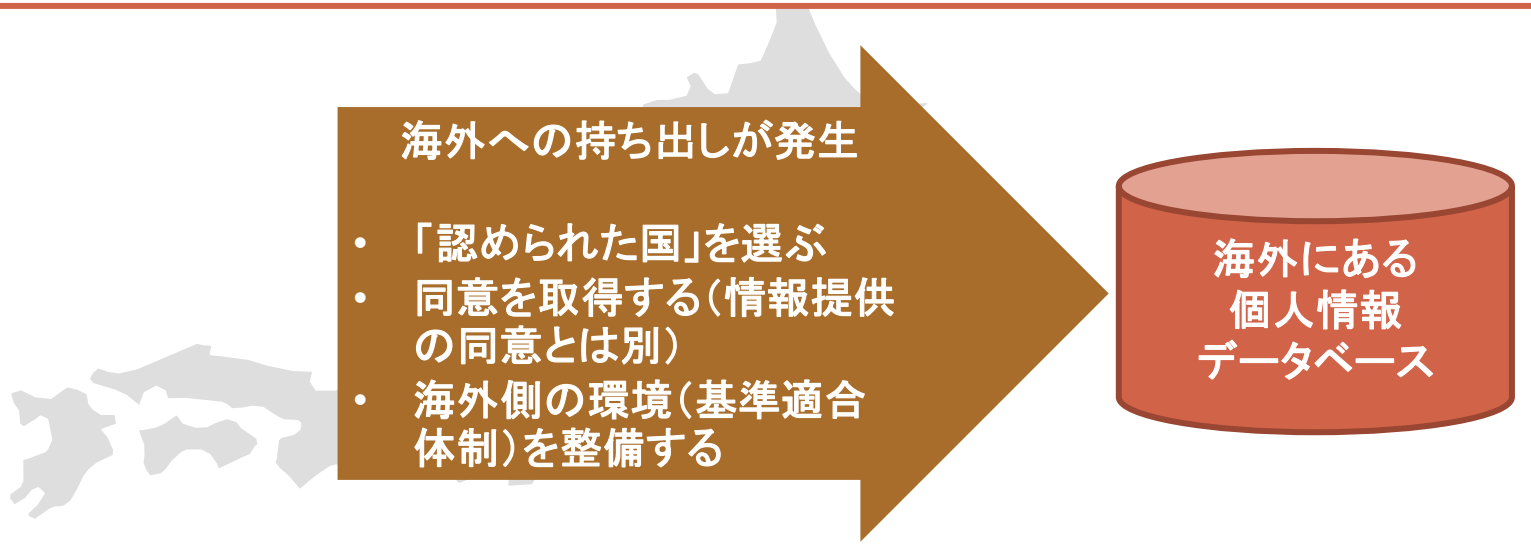
改正個人情報保護法における海外への移転

■ 改正24条（外国にある第三者への提供の制限）

以下の2つの条件どちらも満たさない外国の第三者に個人情報を提供する場合には、「外国の第三者に情報を提供する」ことについて本人からあらかじめ同意を得なければならない、としている（以下2つのどちらかを満たせばよい）。

■ 日本と同等の水準で個人情報が保護されている、と認められた国にある
■ 日本の個人情報取扱事業者と同じような個人情報保護の体制を整備している

※現行法第23条5項各号は除かれていないため委託や共同利用などの場合も適用



データベースをどこに配置するか？（データの流れ）

- データの流れとアクセスのパターンによって、対応の方法を検討します
- システムがオンプレミスでも、クラウドサービス利用でも基本的には同じです

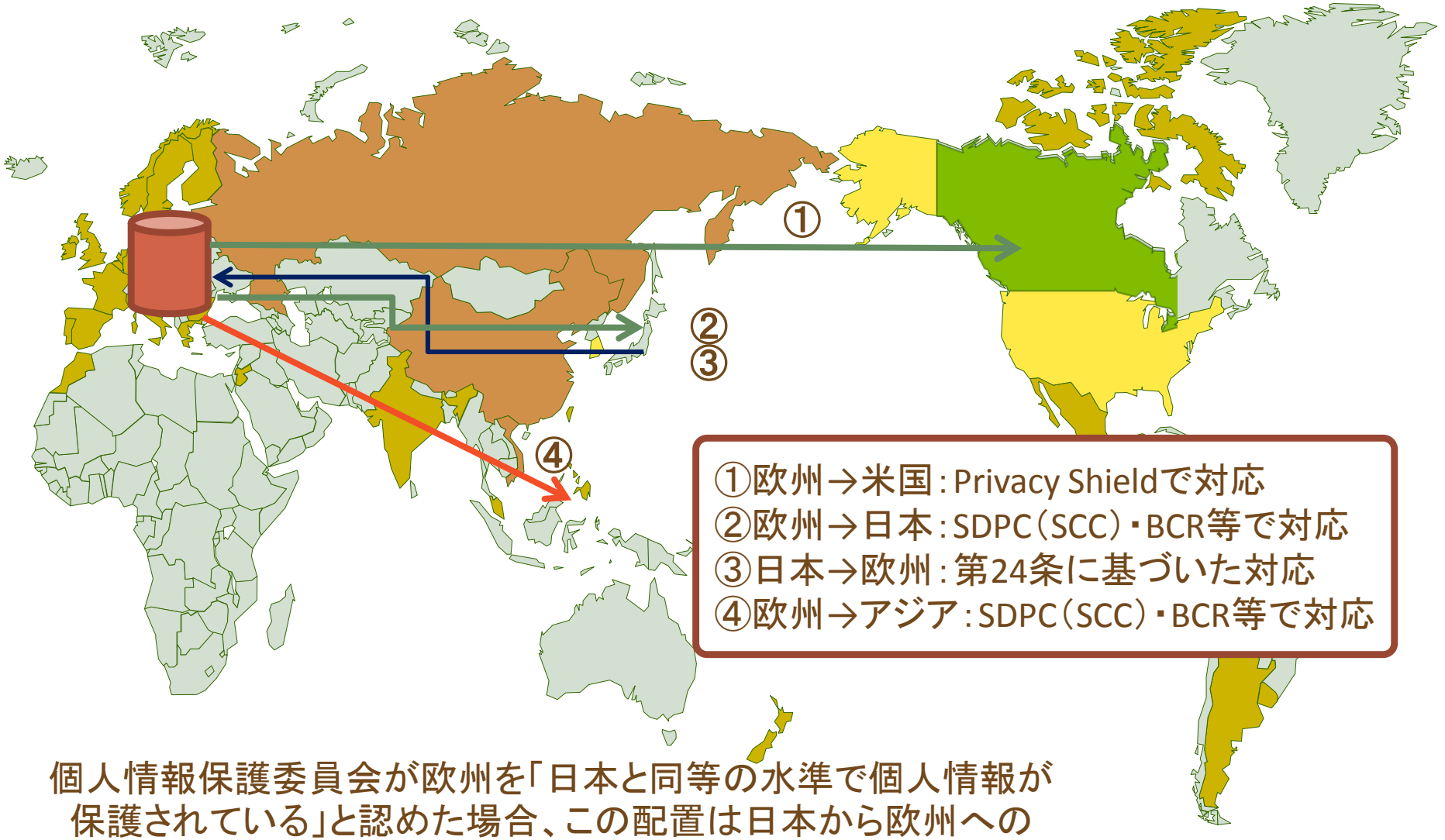
データ移転のパターン

一方向性のデータ移転	欧州から日本にデータを移転し日本側でビッグデータ分析を行い、マーケティングに利用する等
双方向でのデータ移転	日本国内の本社と欧州支社の間で人事情報を共有し相互に情報の閲覧ができるケース等
他拠点間におけるデータ移転	人事情報や顧客情報を複数拠点でグローバル・かつ双方向で閲覧・利用を行う等

データベースをどこに配置するか？（留意点）

- 「この国は規制があるから個人情報を国外に持ち出さないよう、国内にデータベースを配置しよう」は必ずしも良いとは限らない。国外から遠隔保守・運用作業等を行い、管理者権限（DBA）でアクセスするなら、結局個人情報を閲覧することができるため、移転したとみなされる可能性が高い。
- 米国は欧州から個人情報を移転しやすい国のひとつであるが、「Privacy Sheild」があるからといって、米国外の第三国に再移転を認めているわけではない。
- GDPRでは、クラウドベンダーだけでなく保守・運用を委託されているSI企業などもSDPC（SCC）の締結を要求されることがある。
- 法規制があるからという理由で技術的にいびつなシステム構成にするのは本末転倒。
- ロシア、中国など国内にデータベースを置くよう規制している国については別途対応を検討する必要がある。

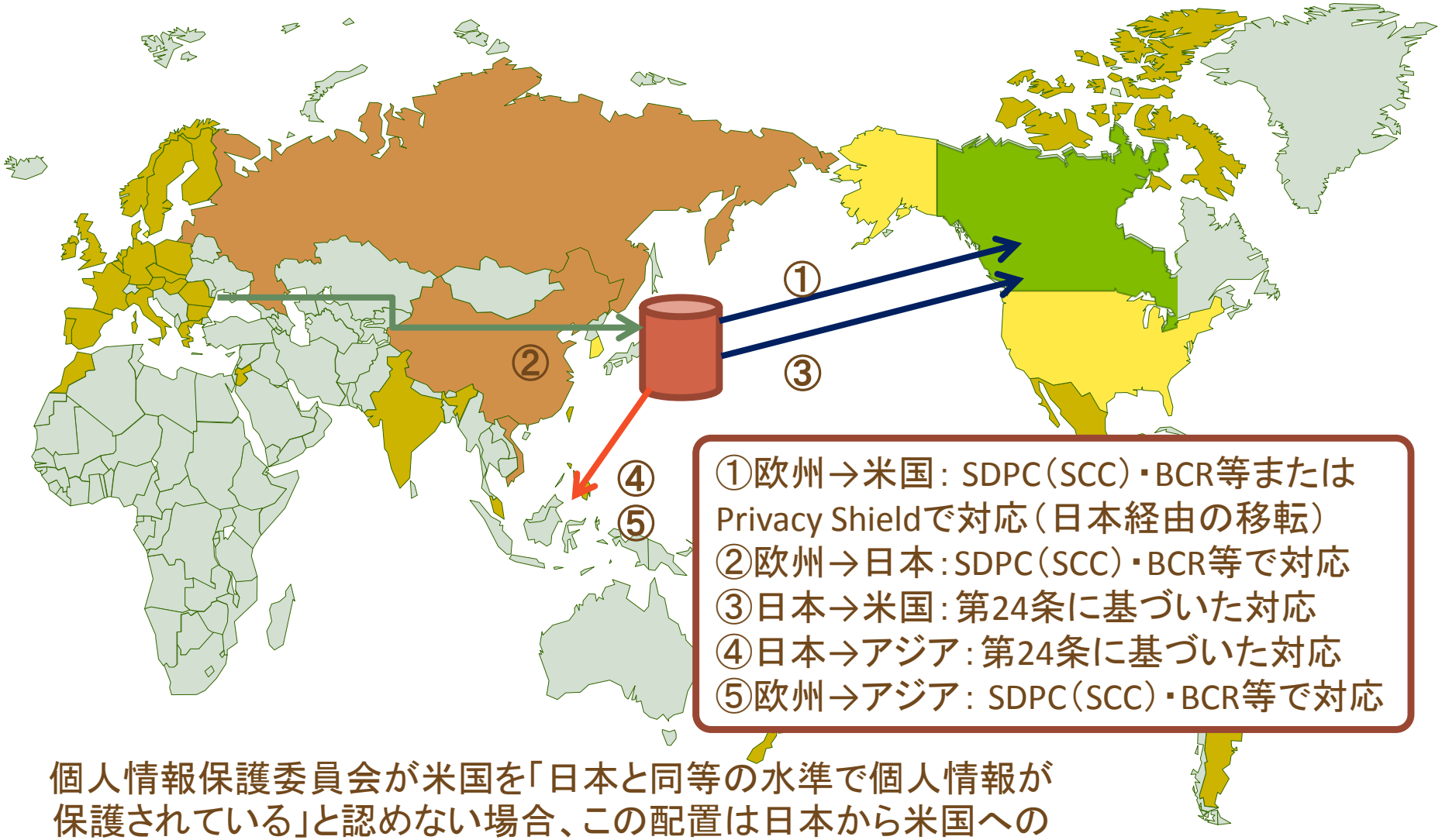
ケース1：欧州に配置（例）



①欧州→米国：Privacy Shieldで対応
②欧州→日本：SDPC（SCC）・BCR等で対応
③日本→欧州：第24条に基づいた対応
④欧州→アジア：SDPC（SCC）・BCR等で対応

個人情報保護委員会が欧州を「日本と同等の水準で個人情報が保護されている」と認めた場合、この配置は日本から欧州への移転の負担を減らすことができる。

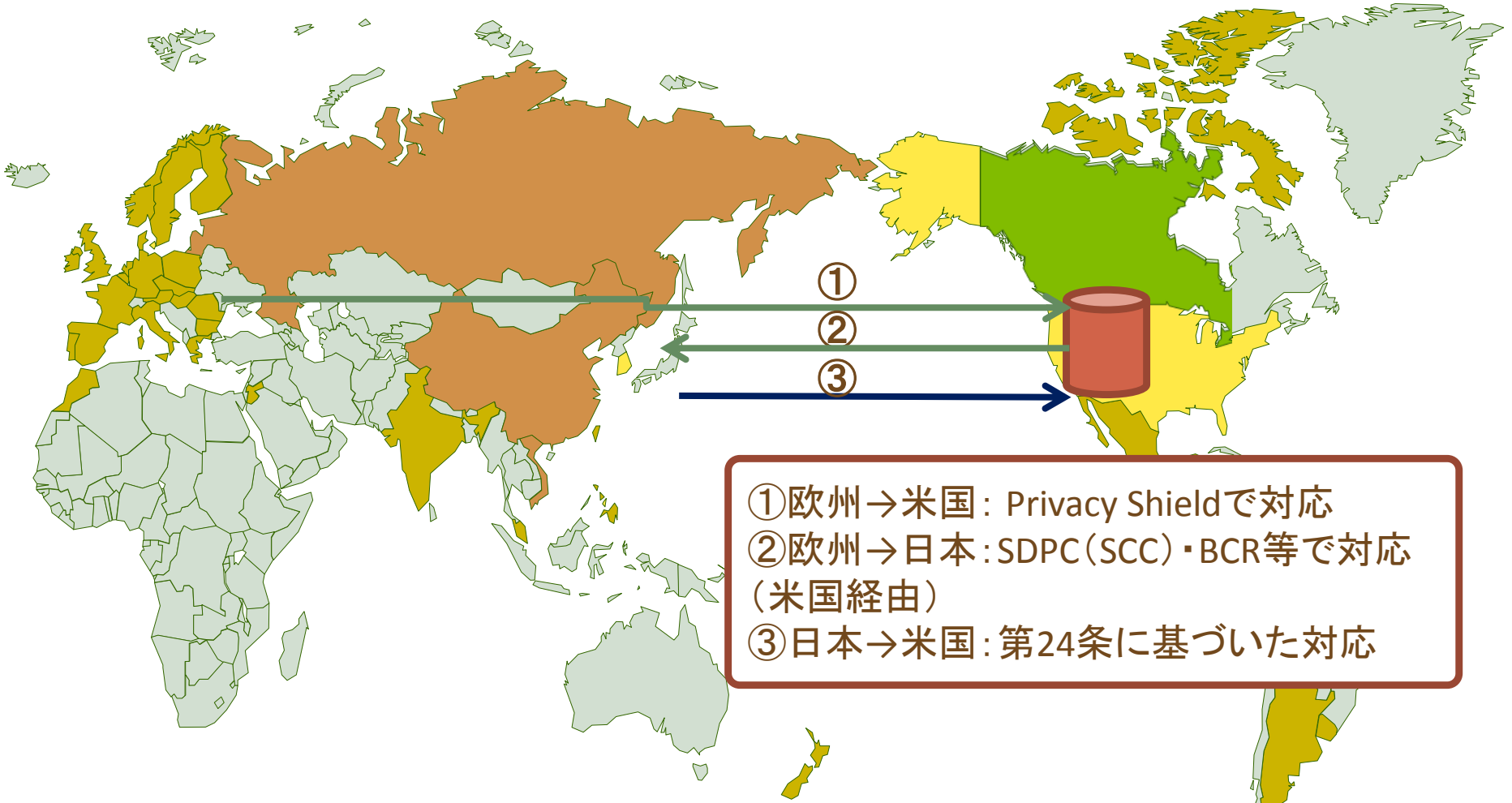
ケース2：日本に配置（例）



①欧州→米国：SDPC（SCC）・BCR等またはPrivacy Shieldで対応（日本経由の移転）
②欧州→日本：SDPC（SCC）・BCR等で対応
③日本→米国：第24条に基づいた対応
④日本→アジア：第24条に基づいた対応
⑤欧州→アジア：SDPC（SCC）・BCR等で対応

個人情報保護委員会が米国を「日本と同等の水準で個人情報が保護されている」と認めない場合、この配置は日本から米国への移転の際に必要なコストが増える。

ケース3：米国に配置（例）



①欧州→米国： Privacy Shieldで対応
②欧州→日本：SDPC（SCC）・BCR等で対応（米国経由）
③日本→米国：第24条に基づいた対応

欧州からPrivacy Shieldを利用して米国に移転した個人情報を日本から閲覧・利用したい場合は、日本・欧州間でSDPC等の対応が必要になる。

海外のクラウドサービスを使う場合の留意点

「①契約での取扱禁止の定め、②適切なアクセス制御が要素として、委託該当性が判断される。そうすると委託に該当しないようにするためには、事業者としては、外国にある第三者たるクラウドサービス事業者に対し、契約上、個人データを取り扱わないことを盛り込んでもらう必要がある。なお、ここでの「個人データを取り扱わない」とは、個人データが含まれるデータについての契約拒否を指すのではなく、個人情報保護法でいう「取り扱い」を行わない、すなわち、個人データを個人データとして扱わないということを示していると　解釈されるべきであろう。しかし外国にある第三者が提供するクラウドサービスの多くは、約款への同意によって利用を始めることが想定されており、約款についての交渉はほとんど不可能である。そうすると、事業者においては、定評あるクラウドサービスを用いようとしても、それが外国にある第三者が運営するものであり、約款の交渉可能性がなければ改正法24条の義務を免れない。」（板倉，2017）[1]

クラウドは委託か？

海外のクラウドサービスを利用する場合、基本的に24条の義務を負う。従って基準適合体制(改正法24条、規則11条各号)を満たさない限り、海外への移転に関する本人の同意が必要になる。

引用文献：[1]　板倉陽一郎,“取引・決済における個人情報保護と改正法の影響”,Law and Technology No.74　pp.41-42,（2017）

越境移転に伴って必要になる体制づくり

規程、ポリシーなどの社内ルール
- 個人情報の定義
- Special category of data
- 明示的な同意の取得　　等

業務プロセスの整備
- 削除要求等への対応
- インシデント発生時72時間以内の通知義務　　等

組織・マネジメントの整備
- データ保護オフィサーの設置
- モニタリング体制の整備　　等

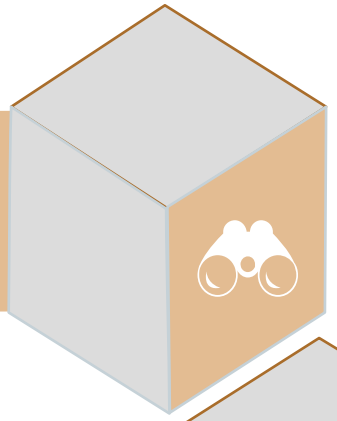
情報システムの対応
- Web画面での説明と同意取得
- 不要な情報の削除や削除要求への対応
- 安全管理　　等

個人情報保護法に基づいて構築した社内体制と海外の法制度の要求事項との間にあるギャップを補正する必要がある。

まとめ

情報活用：

事業を成長させるため積極的に情報を活用しましょう。
リスクをとらずして成長はありません。



情報保護：

新しいチャレンジには新しいリスクが伴います。成長のためにこそ、適切なリスク管理を行いましょう。

説明責任：

過剰投資は必要ありません。しかし海外のステークホルダーに説明できる程度には体制を整えておきましょう。

ご清聴ありがとうございました。