2019年度　東京都
個人情報保護制度説明会

個人情報保護関連の海外の法制度の概要

2019年9月27日

JIPDEC（（一財）日本情報経済社会推進協会）
電子情報利活用研究部　寺田　眞治
Terada-shinji@jipdec.or.jp
（JIPDEC法人番号：1 0104 0500 9403）

本講義の概要

■ 概要

- 主要各国のプライバシー保護制度の概略と個人情報を日本に越境移転する場合の注意点を解説します。
- 政府が掲げる「信頼たるルールの下でデータの自由な流通」について、グローバル視点での位置づけや狙いを概説し、個人情報における国際的な枠組みの構築の動向について解説します。

■ 到達目標

- インバウンド対応やグローバル・サプライチェーン、海外へのサービス提供等において、個人情報を扱う場合の課題への気付きや、実際に対応が必要となった場合の基本的な勘所を把握できることを目標とします。

■ キーワード

- GDPR、中国サイバーセキュリティ法、越境移転、DFFT、CBPR

■ 受講推奨対象

- 一般職員、経営者、管理職、事業開発

アジェンダ

１．　各国のプライバシー保護制度

その個人情報の取扱い方は海外から訴えられるかも!?

2013年に1000万人を超えた訪日外国人が、わずか5年後の2018年に3000万人を突破し、来年は東京オリンピック・パラリンピックを控えることからさらなる急増が予想されています。これに伴って訪日外国人の個人情報を取り扱うことも増えることとなります。

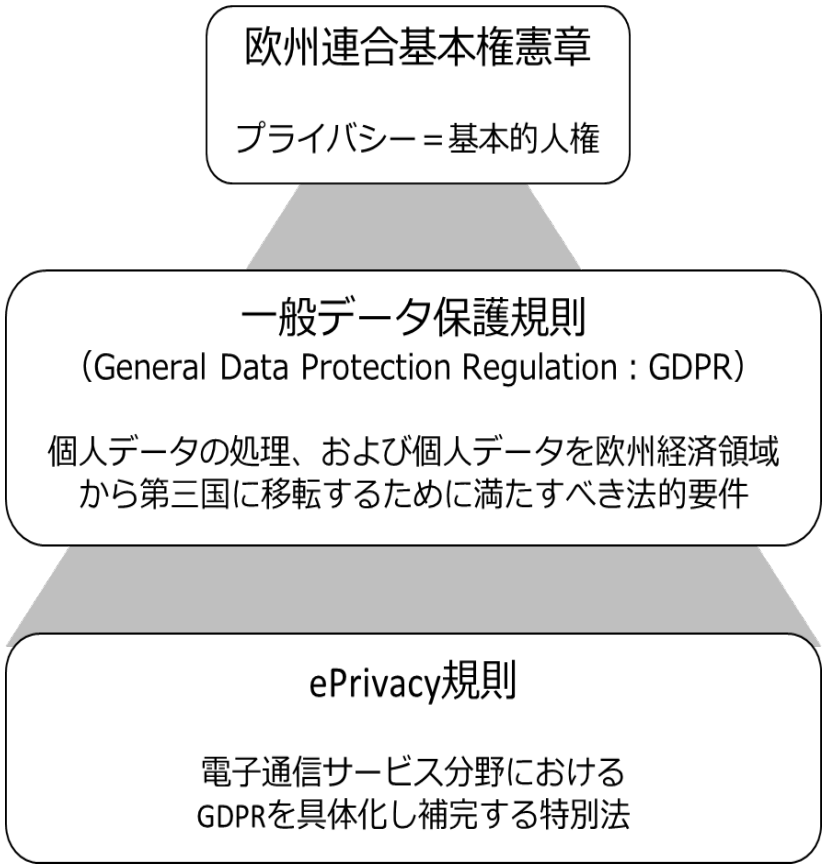
また、製造分野から流通・サービス分野までビジネスのグローバル化が進み、海外での拠点設置や取引も拡大しています。そのため、日本から人員を派遣あるいは現地での採用も増えており、サービス提供の際には現地の個人情報を取り扱うことも珍しくなくなっています。

このように海外との個人情報の流通が増える一方で、各国・地域では「プライバシー保護」や「個人データの越境移転」についての規律が年々厳しくなってきています。

日本の事業者や組織にとってのリスクは、**国や地域によって異なるそれぞれの規律を守らなければ違法であるとされて罰則を課される可能性**があることです。日本の「個人情報保護法」の遵守だけでは、このリスクを避けることができません。

まず、国や地域によってどのような制度があるのかを知ること、個人情報の取扱いや越境移転がある場合に気を付けるべきことを知ること、が重要です。ただしその際に規律だけの解釈に頼ると判断を誤る可能性があります。その背後にある社会的要求や思想、制度の成り立ちや構造を知ることで、規律への対応の勘所が見えてきます。

1）EU　－制度の構造



2018年5月に施行されたGDPRは、EEA※の個人データの取扱いと域外移転を定めた法律で、欧州連合基本権憲章のプライバシーを基本的人権とする考えを具体化したもの。

個人データの定義が広く、およそプライバシーに係る情報は個人データとされているため、結果的にプライバシーに対する保護の領域が広い。

現在、GDPRを補完する**ePrivacy規則**が審議されており、オンライン上の個人データ以外の情報の保護についても強化が検討されている。

※EEA（欧州経済領域）
EU加盟28か国
＋アイスランド、ノルウェー、リヒテンシュタイン

GDPR	ePrivacy規則
送信手段を問わず全ての個人データが対象 **※個人データ＝cokkieを含め個人に関する情報すべて**	**個人データであるか否かを問わず、**電子通信および端末機器上の情報の完全性が対象
個人データ保護の権利を定める	**通信のプライバシーと秘密の権利を定める**
市民に新しい権利を与え、企業に新しい義務を課す	通信を行うアプリやサービスが通信の傍受、録音、聴取または盗聴することができないようにする

1）EU　－GDPRの基本原則（第5条）

個人データ処理の6原則（第1項）

(a)適法性、公正性及び透明性
そのデータ主体との関係において、適法であり、公正であり、かつ、透明性のある態様で取扱われなければならない。

(b)目的の限定
特定され、明確であり、かつ、正当な目的のために収集されるものとし、かつ、その目的に適合しない態様で追加的取扱いをしてはならない。

(c)データの最小化
その個人データが取扱われる目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定されなければならない。

(d)正確性
正確であり、かつ、それが必要な場合、最新の状態に維持されなければならない。その個人データが取扱われる目的を考慮した上で、遅滞なく、不正確な個人データが消去又は訂正されることを確保するための全ての手立てが講じられなければならない。

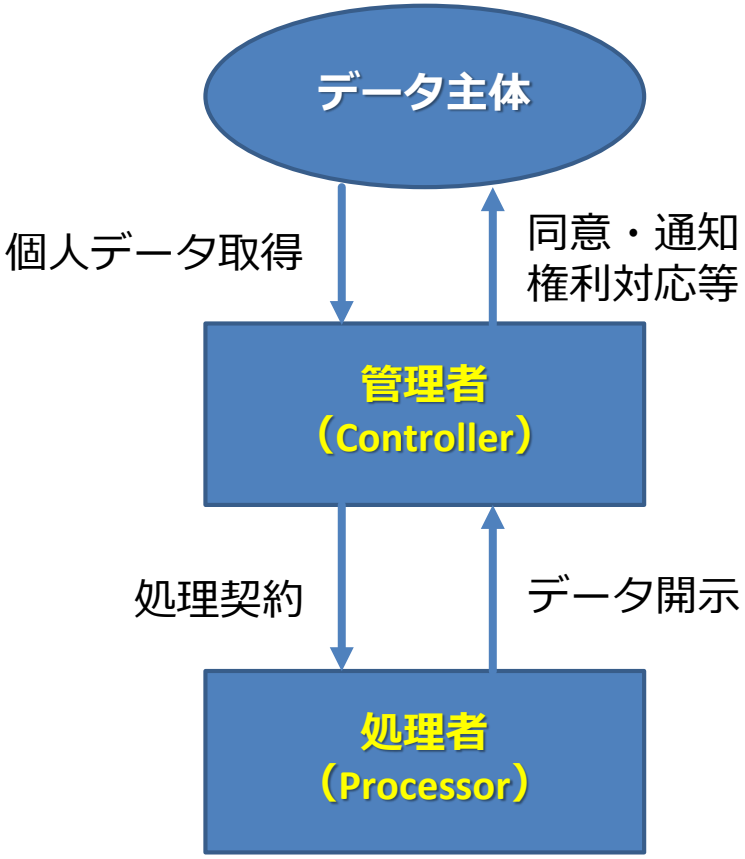
(e)記録保存の制限
その個人データが取扱われる目的のために必要な期間だけ、データ主体の識別を許容する方式が維持されるべきである。

(f)完全性及び機密性
無権限による取扱い若しくは違法な取扱いに対して、並びに、偶発的な喪失、破壊又は損壊に対して、適切な技術上又は組織上の措置を用いて行われる保護を含め、個人データの適切な安全性を確保する態様により、取扱われる。

アカウンタビリティ（第2項）
管理者は、第1項について責任を負い、かつ、同項遵守を証明できるようにしなければならない

※例外：公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のみのために取扱われる個人データ

1）EU　－GDPRの対象事業者



管理者が取得する個人データが属する自然人

単独または共同で個人データ取扱の目的と手段を決定する自然人、法人等
（データ取扱の違法性、GDPR違反に対する責任）

管理者のために管理者を代理して個人データの取扱いを行う自然人、法人等
（管理者による書面の指示のみに従う）

※処理者＝受託事業者ではない。管理者が自ら個人データ取扱を行う場合は管理者と処理者が同一となる。

GDPRは企業や組織の大小ではなく、権利や自由へのリスクの高さを基準とするので、取扱う個人データの種類、規模、処理内容等に応じて必要な対応を考えることが重要。

1）EU　－GDPRの主な注意点

個人データの取扱いが認められる法的根拠

データ主体の同意がある場合
契約履行のため / 法的義務履行のため / データ主体または他の自然人の重大な利益保護のため / 公共の利益のため、または管理者の公的権限の実行のため
管理者または第三者の正当な利益追求のため

データ主体の権利

データ主体が権利を行使してきた場合には、原則として**1か月以内**に対応しなければならない。

（主な権利）アクセス権 / 訂正権 / 削除権 / 忘れられる権利 / データポータビリティ権 / 異議権 / プロファイリングを含む自動化された意思決定に服さない権利

データ侵害の通知義務

原則として**72時間以内**に**所轄監督機関**に通知しなければならない。

データ保護責任者（DPO：Data Protection Officer）の設置

定期的かつ系統的な監視、特別なカテゴリーの個人データの取扱いを大規模に行う場合

データ保護影響評価（DPIA：Data Protection Impact Assessment）の実施

自然人の権利及び自由に対する高いリスクを発生させる恐れがある場合

（例）大規模な：プロファイリング、特別なカテゴリーの個人データ、公共の場での監視

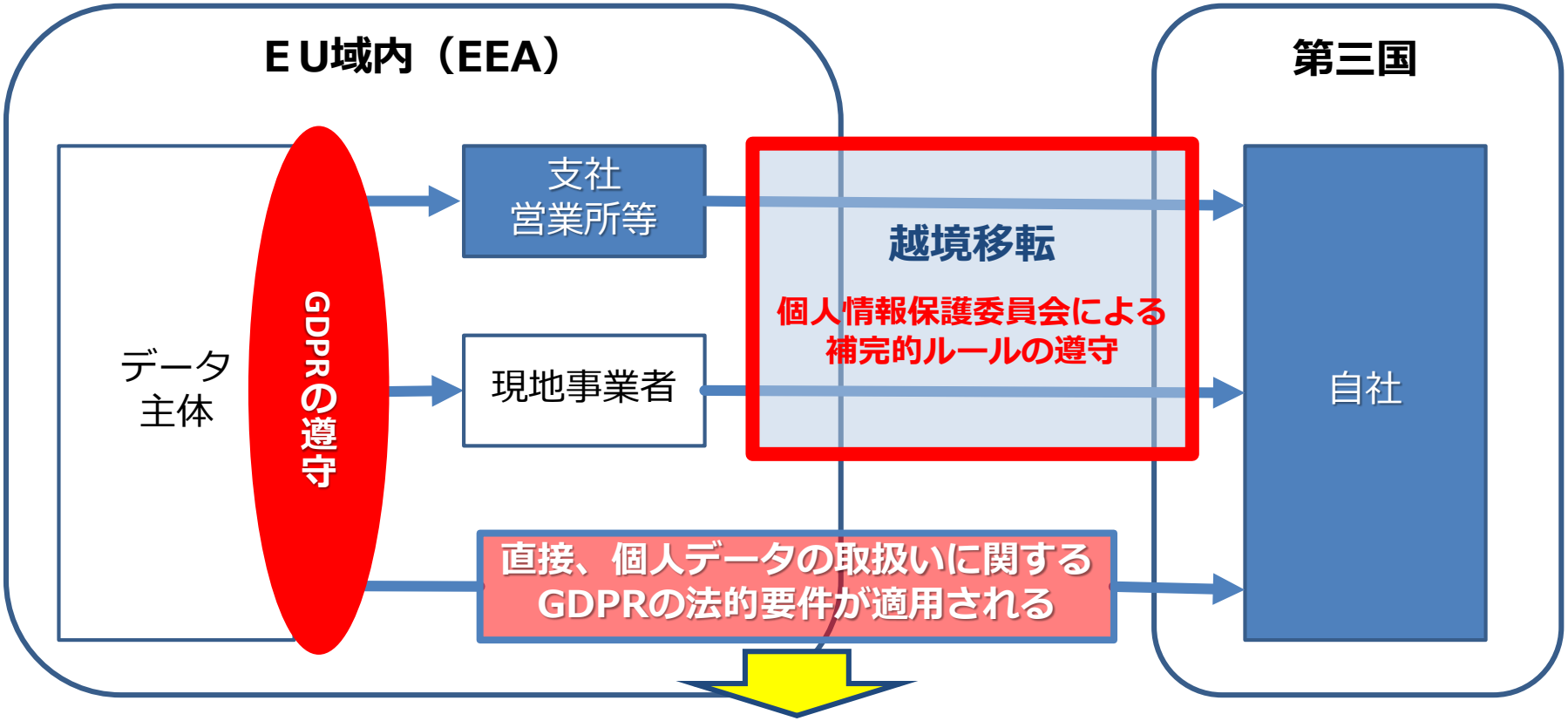
代理人の指定

EU域内に拠点のない管理者または処理者は、書面により、EU域内における代理人を指定する

※データ主体に提供すべき情報や記録義務等についても日本法とは微妙に異なるので注意が必要※

1）EU　－越境移転

EU域内の個人データを取扱う事業者はすべてGDPRの対象



1．有料、無料に関わらず、**EU域内に所在するデータ主体**に対する商品またはサービスの提供に関する個人データの取扱（国籍は問わず現地従業員、他国からの派遣含む）
2．EU域内で行われるデータ主体の**行動の監視**に関する個人データの取扱
（取扱事業者の所在はEU域内、域外を問わない）

1）EU　－越境移転：補完的ルール

GDPRと個人情報保護法との差分を埋めるためのもの

1．GDPRにおける「特別な種類の個人データ」を要配慮個人情報として扱う
→　要配慮個人情報には含まれていない「性生活、性的指向又は労働組合に関する情報」を要配慮個人情報として扱う

2．日本ではGDPRにおける「データ主体の権利」を行使する場合、6か月以上の保有期間となる個人データが対象であるが、GDPRでは取得と同時に行使が可能となる
→　EEAからの個人データは、取得時点で保有個人データとして扱う

3．４．日本では記録義務は第三者提供時にのみ必要となるが、GDPRでは取扱活動すべてについて記録が必要となる
→　EEAからの個人データの移転について利用目的、経緯を確認し記録する

5．十分性認定はEEAと日本の間でのみ有効
→　日本から第三国へ移転する際には、原則として日本法の越境移転の義務に服する

6．日本における匿名加工情報は、GDPRにおいては個人データに該当する
→　EEAからの個人データを匿名加工情報として扱うためには、GDPRにおける匿名化（＝非個人情報）にする
※GDPRにおける匿名化をした場合には、非個人情報として扱ってもよい

補完的とあるが、個人情報保護法への上乗せの規律として遵守する義務がある

2）米国　制度の構造

公的部門：1974年プライバシー法
民間部門：セクトラル方式（分野別）の法令
金融分野：1970年公正信用報告法、1978年金融プライバシー権利法、1999年金融サービス近代化法
通信分野：1934年通信法、1968年総合犯罪防止及び街頭安全法、1986年電子通信プライバシー法、2003年キャン・スパム法
児童保護：1998年児童オンライン・プライバシー保護法(COPPA)
医療分野：1996年HIPAAに基づくプライバシー･ルール及びセキュリティ・ルール、2009年経済及び臨床医療のための健康情報技術法(HITEC Act)に基づく侵害通知義務→2013年総合ルール

FTCの規則制定権限及び執行権限

FTC法第5条は、消費者プライバシー保護の場面でFTCが執行を行う根拠規定であり、現在では連邦プライバシー関連法の主たる法律に位置づけられている。

商取引における又は商取引に影響を及ぼす不公正若しくは欺瞞的な行為又は慣行は、本法により違法と宣言する。

違反行為については、排除措置命令、民事罰、提訴の対象。消費者を騙す実務は「欺瞞的」、データ漏えいの場合は「不公正」。実際は「同意命令」(同意審決)という一種の和解手続によって、審判手続を経ずに解決することが多い。

■最新動向■

2018年夏、**NTIA**（米国商務省電気通信事業局）が**プライバシー基本原則案**を発表しパブコメ実施。
→　基本原則の実現の方法は事業者の自主的な取り組みに委ねるべき。

2018年12月、**NIST**（アメリカ国立標準技術研究所）が民間事業者向け**プライバシー・フレームワーク**を作成中
→　原則はリスクベースアプローチ、アウトカムベースアプローチ、ボランタリー

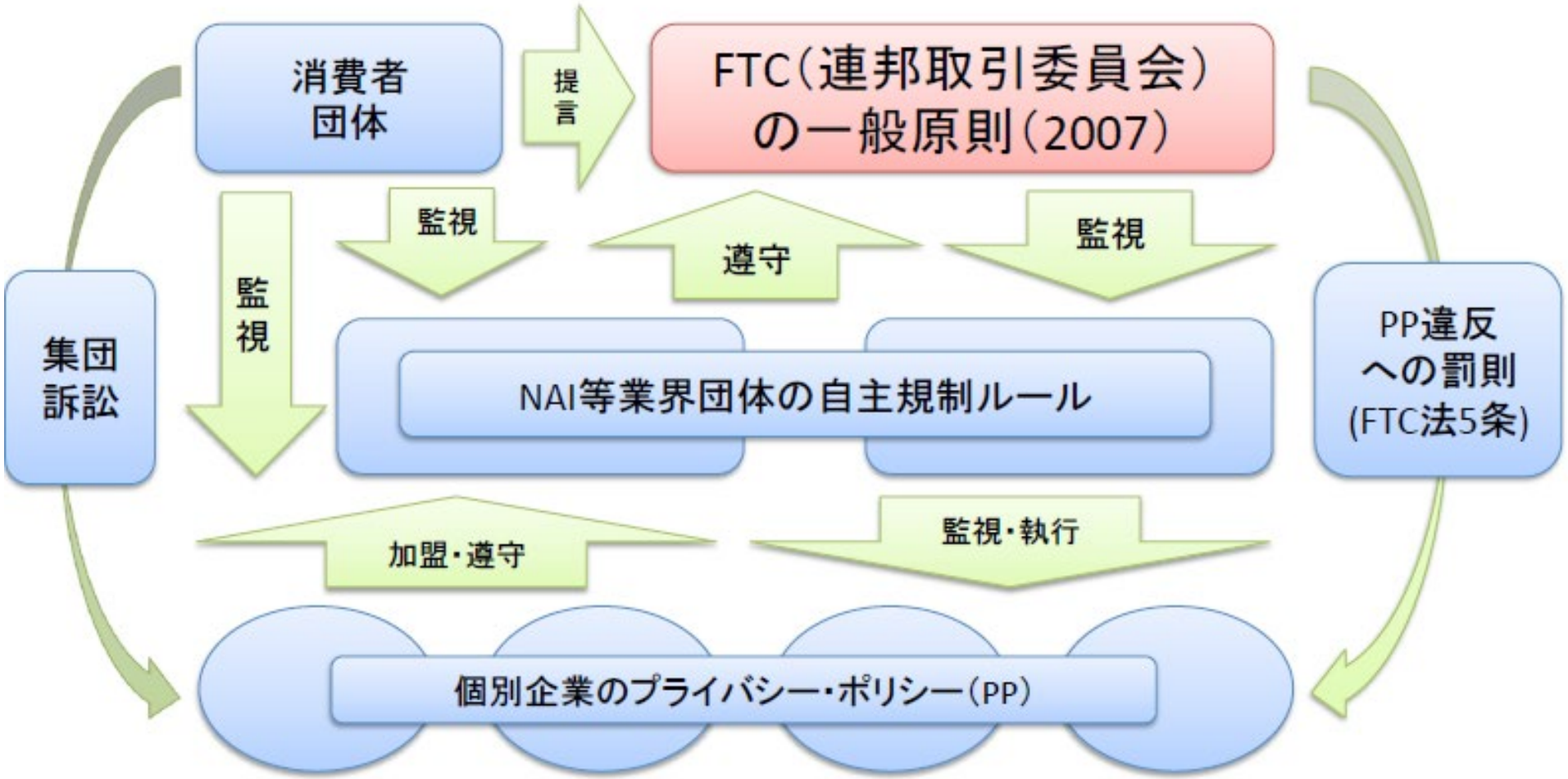
2020年1月　**カリフォルニア消費者プライバシー法**が施行予定
→　アカウンタビリティと消費者の権限を強化（オプトインではない）

プライバシー権をベースとする法制度（連邦法、州法等）による規制
・GDPRに近い考え方
・GAFA、通信事業者等はこれを支持

⇔

自主規制と FTC法第5条に基づく対応
・大半の産業界はこれを支持

2）米国　－規制の特徴

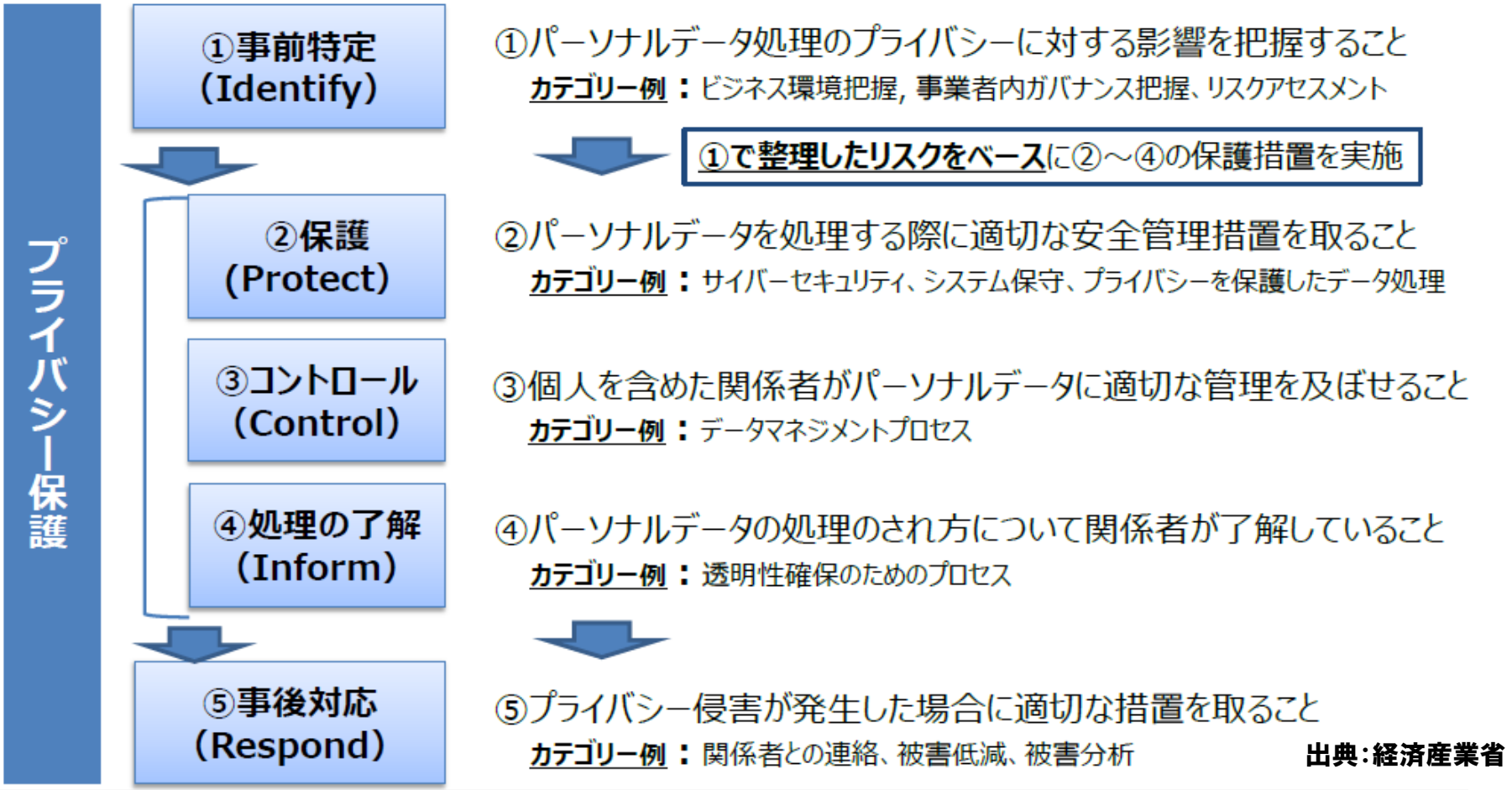


企業が個人情報を取り扱うにもかかわらず**プライバシーポリシーを公表しないこと**、あるいは**プライバシーポリシーに反する行為を行うこと**は「欺瞞的行為」とされる。
強力な消費者団体の存在が、個人情報保護法なしに共同規制として機能させてきた。

2）米国　－NISTのプライバシー・フレームワーク

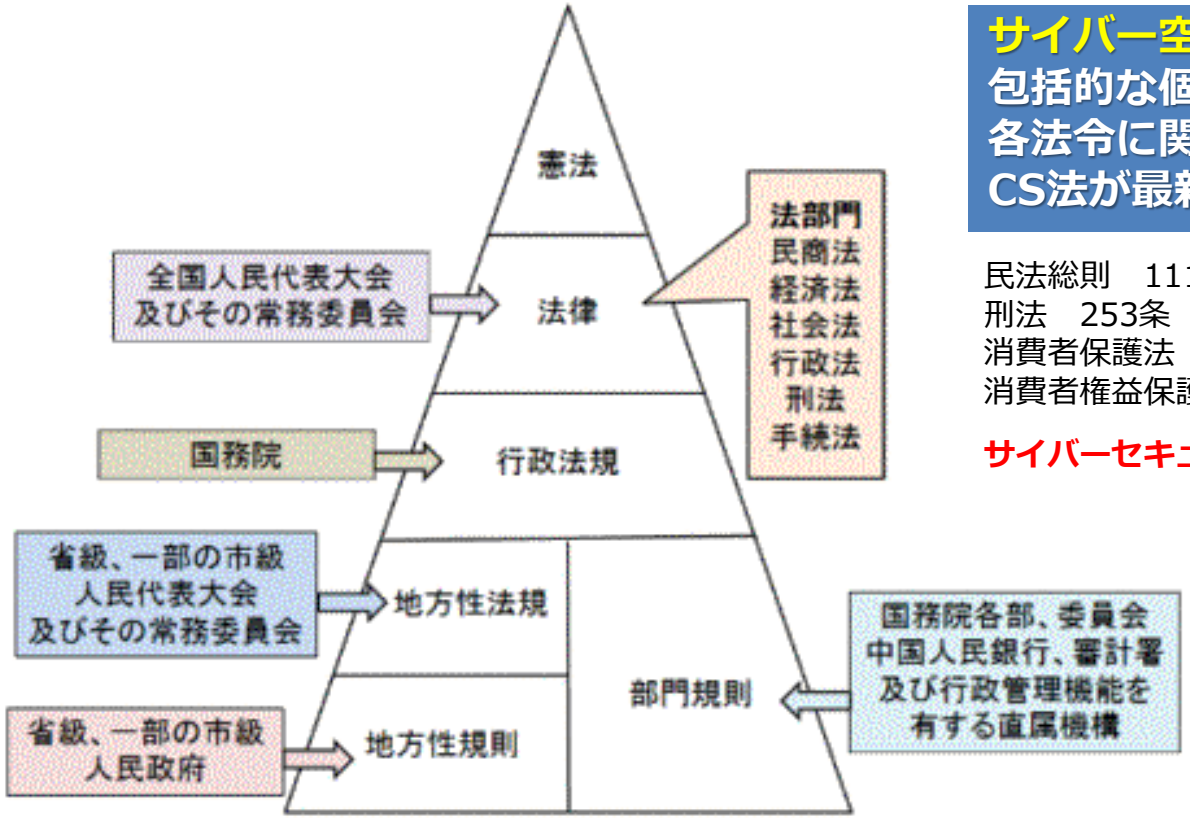
法的な強制力のあるものではなく、プライバシー保護を検討する上でのレファレンス

- プライバシー保護のために事業者が実施すべき事項を5つの機能（function）に分解。
- 機能は、それぞれの機能を実現するための複数の事項（カテゴリー）に更に分解。



出典：経済産業省

3）中国　－制度の構造



広東省情報化促進条例
浙江省公共信用情報管理条例

独自の処罰を規定している地方の条例
曖昧な法規定についての裁判所の解釈
判例の報告書などがあるので注意必要

サイバー空間における国家の安全が目的。
包括的な個人情報保護法は存在しないが、
各法令に関連する規定が散在しており、
CS法が最新かつ最も包括的。

民法総則　111条
刑法　253条
消費者保護法　50条
消費者権益保護法　29条、56条

サイバーセキュリティ法

工業・情報化部
　電気通信及びインターネット利用者の個人情報保護に関する規定
公安部
　パソコン情報システム安全保護条例
　情報安全等級保護管理弁法
国家インターネット情報弁公室（CAC）
　CS法の実施規定と国家基準
　　個人情報保護ガイドライン
　　個人情報セキュリティ規範
その他（金融、電力、信用調査等）

司法解釈「公民個人情報刑事案件の法律適用の若干問題に関する最高人民法院及び最高人民検察院の解釈」
「情報ネットワークを利用して人身権益侵害民事紛争案件審理の法律適用若干問題規定」
その他裁判例

3）中国　－中国CS法（サイバーセキュリティ法）

対象者

ネットワーク製品・サービスの提供者
ネットワーク運営者※
重要インフラ運営者
電子情報送信とアプリダウンロードのサービスプロバイダ

※中国内のあらゆる個人、組織（海外含む）が対象となる

課される義務

国家レベルでの安全確保とデータ保全（国家安全）	一般市民を対象とした個人情報保護（市民保護）
個別企業におけるデータ安全の確保（一般的な情報セキュリティ）	

※**ネットワーク運営者**：ネットワークの所有者、管理者およびネットワークサービス提供者
※企業内のネットワーク所有・管理者（情シス等）も含まれる

2017年6月に施行されたCS法は、個人情報の保護のみを対象としたものではなく、広くオンライン上の情報の保護を目的としている。また、データだけではなく設備や機器、ネットワークの安全性等についても規定されており、位置づけとしては**セキュリティ全般についての基本法**である。

個人情報については、保護すべき重要なデータのひとつとしての位置づけであり、内容はGDPRを意識したものとなっている。ただし中国の政府や公的機関は対象外である。
CS法は原則的な要求仕様であり、詳細については行政法規や国家標準等で順次定められているところである。

個人情報については国家インターネット情報弁公室（CAC）の**「個人情報セキュリティ規範」**が最重要。

3）中国　－個人情報セキュリティ規範

中国において個人情報を取り扱う場合は
GDPR、ISO27000シリーズ　に準拠した対応　＋　**独自の要求仕様**

1．基本的にEUのGDPRに準じており、個人情報支配者（personal data controller：個人、組織に関わらず）を規制対象とするもの。
従って**プロファイリング※、データポータビリティ※**等についても規定されており、中国において個人情報を取り扱う場合には、注意が必要。

2．安全管理措置については、ISO27000シリーズに準じているが、大量の個人センシティブ情報にアクセスする人員は背景調査を行うことといった特殊なものも追加されている。

3．漏えい時の対応についても一般的であるが、本人への告知が明確化されており、また、当局への報告義務についても国家インターネットセキュリティ事件応急プランの関連規定に従うことと定められている。

4．小規模事業者についての言及はないが、専任の個人情報保護責任者と個人情報保護機関を設置する義務は、①主業が個人情報処理にかかり、且つ従業員が200 人以上、又は②50 万人を超える個人情報を処理し、又は12 カ月以内に50 万人の個人情報の処理を予測される組織としている。

とはいえ、「個人情報セキュリティ規範」は国家基準であり法令ではないため、どこまで対応すべきかは未知数。ただし、これに準じていると（原則的には）法令違反には問われないと考えることもできる。ありがちな当局による干渉に対して、隙を作らないという観点では現時点で最も重要な規格である。

※プロファイリング：個人に関するデータを集積・統合・分析等して当該個人の詳細な属性や嗜好等を明らかにすること
データポータビリティ：個人に関するデータを当該個人が取得したり他のサービス等に移転できるようにすること
いずれもGDPRで定義され、日本でも検討されているが、執行にあたって未確定の要素が多く優先度は低いとされている

3）中国　－個人情報の越境移送について

中国で個人情報を取り扱う場合には、現地にデータを保管する必要がある（**データローカライゼーション**）
そのうえで海外に移転する場合には、定められた**安全評価**をしなければならない。

以下のいずれかの場合、業界主管部門または監督部門による安全評価が必要

1．50万人以上の個人情報が含まれる場合
2．情報の容量が1000GBを超える場合
3．核施設、化学生物、国防軍事、人口健康等領域のデータ、大型工事事業、海洋環境及び敏感な地理情報に関するデータ
4．重要情報インフラのシステムの脆弱性、セキュリティ防護等インターネット安全情報
5．重要情報インフラの運営者が個人情報及び重要情報の越境移送
6．その他国家安全及び社会公共利益に影響を与え、業界主管または監督部門が必要と認める場合

その他の場合、ネットワーク運営者が自ら安全評価を行うことができる

【安全評価】

目的評価

データ越境移送の目的（必要性、適法性、正当性）

安全評価

・個人情報の状況（数量、範囲、類型、敏感程度、同意の有無等）
・重要性の状況（数量、範囲、類型及び敏感程度等）
・移送側・受領側の安全保護措置、能力、レベル、対象国のセキュリティ環境等
・越境移送による漏洩、毀損、改ざん、濫用リスク
・越境移送及びデータの集積が国家安全、社会公共利益、個人の適法な利益にもたらすリスク

越境移送同意報告

法　　令：サイバーセキュリティ法
施　行　令：個人情報及び重要データ越境移送安全評価弁法
ガイドライン：情報安全技術･データ越境移送安全評価ガイドライン

４）その他　－アジア各国の動向

シンガポール、韓国はすでに欧米並みの個人情報保護法が制定、施行されている

ベトナム　2019年1月　サイバーセキュリティ法施行
サイバー空間主権主義的なデータローカライゼーション、データ開示規定
（国内でのサーバー設置義務がデータ保存義務に緩和されている）
対応期限は12か月？

マレーシア　域外移転可能国・地域について候補が提案されているが現時点では未承認
日本は含まれている

インド　2018年7月　データ・プライバシー法
2018年10月　インド準備銀行（RBI）は、支払いエコシステム内のすべての
エンティティに対して、すべての支払いシステムデータの国内保存を義務化
2019年2月　国家電子商取引政策の草案
データローカライゼーション+重要個人情報を国内での処理に限定
「インド内で発生するデータはインドの発展のために利用すべき」という思想

タイ　2019年2月　個人情報保護法施行
日本と同様に同意なしでの国外移転の可能な国・地域が指定される予定

プライバシー保護、サイバーセキュリティに関して、包括的な法制度の整備が進展しつつある。
↓
わかりやすくなる反面、概ね規制強化となり、執行リスクも高まることが想定される。
また、越境移転についての強い規制が追加される傾向にあり、対消費者だけでなく
事業者間取引や自社の従業員についても、個人情報を日本で取り扱う際には注意が必要。

5）対応のポイント

各国・地域毎にプライバシー保護の制度は異なります。

→ 現地での個人データの取得や取扱いだけでなく、**海外から個人データを移転する場合の規制に注意！**
（日本から海外へ移転する場合も個人情報保護法を確認のこと）

→ 各国・地域とも制度の刷新や拡充の最中なので、最新の情報のキャッチアップと対応の見直しが重要になります。

→ 各国・地域の制度に一括して適合させる方法は残念ながら存在しません。
- 各国・地域毎に管理するのがベストですが、最も規制が厳しいと考えられるGDPRへの対応をベースに、差分を各国・地域毎に抽出して追加する方法が比較的楽です。
- 世界標準規格であるISO27000シリーズ（ISMS等）の取得も自社における体制の構築や対外的な信頼感の醸成に役立ちます。
- アジア太平洋地域でのデータ流通については、CBPR（次節参照）の取得も検討に値します。

★注意★　実際の対応については、専門家や弁護士と十分に相談してください！

２．データ越境移転の動向

各国・地域毎に対応するしかないのか？

昨年末来、政府は「DFFT（Data Free Flow with Trust）」を提唱し、G20大阪トラックとして宣言しました。これは、国境を越えたデータ流通の促進を目指すものですが、あらためて言及するその背景には阻害要因があることを示唆しています。

阻害の３大要因として、データ保護主義やセキュリティの問題とともにプライバシー保護が挙げられていますが、これらは個別の問題ではなく、深く関連しあっています。前節においてアジアを中心に「データローカライゼーション」が広がっていることに触れましたが、これはプライバシー保護よりも他の要因によるところが大きい施策です。

事業者や組織が世界にその活動の場を広げ、また世界からの多くの訪日外国人を受け入れるうえで、プライバシー保護を確かなものにするためには、各国・地域のデータ流通政策とその動向を把握しておくことも欠かせなくなってきています。

DFFTの実現に向けた様々な動きがある中、プライバシー保護についても具体的な国際連携が進展しており、一定の地域では枠組みが稼働し始めています。この枠組みは、**各国・地域毎に個別に対応することによるコストや手間を削減し、不確実性を低減することに繋がると期待**されています。

1）DFFT　－Data Free Flow with Trustとは

（２０２０年６月２８日）
Ｇ２０大阪サミット デジタル経済に関する首脳特別イベント 安倍総理スピーチ（抜粋）

デジタル化は、各国の経済成長を後押しし、イノベーションを促進し、国際社会が直面している様々な課題を克服する大きな可能性を有しています。しかし、急速に進行するデジタル化の潜在力を最大限活用するには、それに後れを取らない国際的なルールが不可欠であります。中でもデジタル時代の成長のエンジンであるデータ流通、電子商取引に関するルールづくりは、急務であります。膨大なデータが世界を駆けめぐり、イノベーションが経済社会の様々な課題を解決していく。そのような環境をつくり出すには、**データ・フリー・フロー・ウィズ・トラスト、ＤＦＦＴすなわち信頼たるルールの下でデータの自由な流通**を促進しなければなりません。

世界的に拡大する「データ・ローカライゼーション※」や「データ保護主義」への対抗

※データ・ローカライゼーション（Data Localization）：データの国内保存義務化
本来は問題が起きた場合の証拠保全やトレーサビリティ（追跡可能性）確保が目的であり、越境移転禁止ではない。
その一方で、政府等による情報の検閲、改竄、窃取のおそれや遮断の容易化等が指摘されている。

1）DFFT　－実現のための課題

JIPDEC

- データ越境流通において直面している諸課題に対して、**データの自由流通とプライバシー及びセキュリティのバランスを勘案した包括的なアプローチが必要。**
- 実態としては、各国により上記３要素のバランスは異なる。それを前提として、自国民のプライバシーやセキュリティを確保しながら、どのように他国とのデータ流通を確保していくべきか、各国の知恵が求められている。

●プライバシー（個人情報）の保護

- プライバシーの保護は、基本的人権の一つであり、適切に確保していくことが必要。
- 他方、各国の個人情報保護制度を見ると、保護すべき個人情報の範囲や、保護の強度は国により異なる。
- 一部の国では、データを活用した社会統制や検閲強化の動きもみられる。

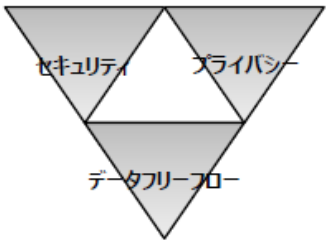
●セキュリティの確保

- 様々な分野で第三者への情報漏洩の問題が顕在化。
- 個人情報はもちろん、重要な産業データ・技術情報、更には重要インフラ等の安全保障上重要な情報もサイバー窃取の危険にさらされている。
- 特に５Ｇ技術が導入されれば、流通する情報量が飛躍的に増大し、情報漏洩の危険も一層拡大するとの指摘も。

●データの自由流通の促進

- 第四次産業革命の第二段階では、質の高いリアルデータを大量に確保することが競争力の鍵。
- そのためには、一国の市場のみに依存していては不十分であり、国境を超えたデータの流通は不可欠。
- 一部の国ではデジタル保護主義的な制度導入の動きも見られる。

○ プライバシー保護やセキュリティの確保は大前提。
○ その範囲内で、可能な国同士で、データの自由流通を促進する仕組み作りが必要。



出典：経済産業省

1） DFFT　－3要素の実態

セキュリティ強靭化の圧力

調達要件への対応

ISO 27000
NIST SP800
IEC 62443
・
・
認証取得必須へ
（国際/業界標準対応）

プライバシー保護強化の潮流

乱立する法・制度への対応

GDPR：最小公倍数的対応
CBPR：広域対応
中国CS法：各国対応
カリフォルニア州法：個別対応

認証取得拡大

DFFT
(Data Free Frow with Trust)

サイバー空間主権主義

※サイバー空間は国家主権の重要部分とする考え方

データの自由流通 vs データの保護主義

1） DFFT　－DFFTとサイバー空間主権主義

イニシアティブ争奪戦
- 米国はサイバーセキュリティの標準化（ISO提案）
- EUは基本的人権としてのプライバシー保護の標準化
  （十分性認定で各国にGDPRに近似の法制度を要求）

US
安全保障

日本
豪州
韓国

EU
権利保護

※経済圏確立のためには
共通の標準化が必要

体制維持
自国産業振興

貿易活性化
安全保障

新興国
Data Localization and/or Data Free Flow

共有
困難

中国
サイバー空間主権主義 with Data Free Flow

共有
困難

独裁国家
サイバー空間主権主義

※支配・被支配的関係でなければ
経済圏確立は困難

標準化戦略の重要性増大
↓
相互認証、Trust Frameworkの確立へ

※Data Localization：データの国内保存義務化（越境移転禁止ではない）

2）国際的なデータ流通の枠組み　－可能性

（個人情報保護委員会資料）

日EU相互認証とUS-EUプライバシーシールドのインターオペラビリティ

✓ US-EUプライバシーシールドの参加企業に対しては、「十分性認定に基づきEU域内から移転された個人データ」を再移転することができるのではないか

CBPRシステムに「何か」を加えた認証方法の構築

✓ CBPRシステムそのものではなく、CBPRシステムを基礎とした新しい枠組みによるGDPRの認証方法とのインターオペラビリティ

OECDプライバシーガイドラインの活用

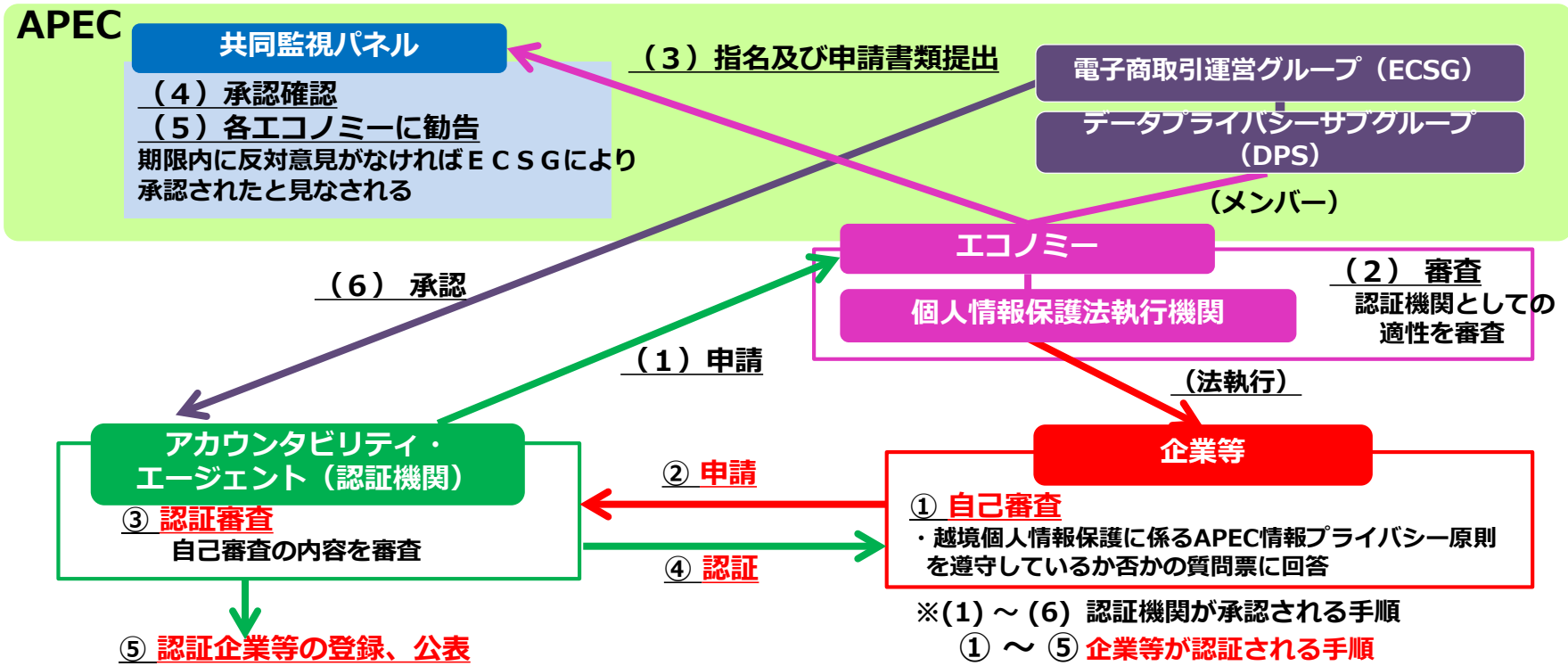
✓ プライバシー保護・個人データ流通に関するグローバルスタンダードとなり得る可能性

2）国際的なデータ流通の枠組み　－CBPR

APEC-越境個人情報保護ルール(CBPR)

- 企業等の越境個人情報保護に係る取組みに関し、APEC情報プライバシー原則への適合性を認証する制度。
- 申請企業等は、自社の越境個人情報保護に関するルール、体制等に関して自己審査を行い、その内容についてあらかじめ認定された中立的な認証機関(アカウンタビリティ・エージェント:民間団体又は政府機関)から認証審査を受ける。（APEC／CBPRシステム）

APEC/CBPRシステムの概念図

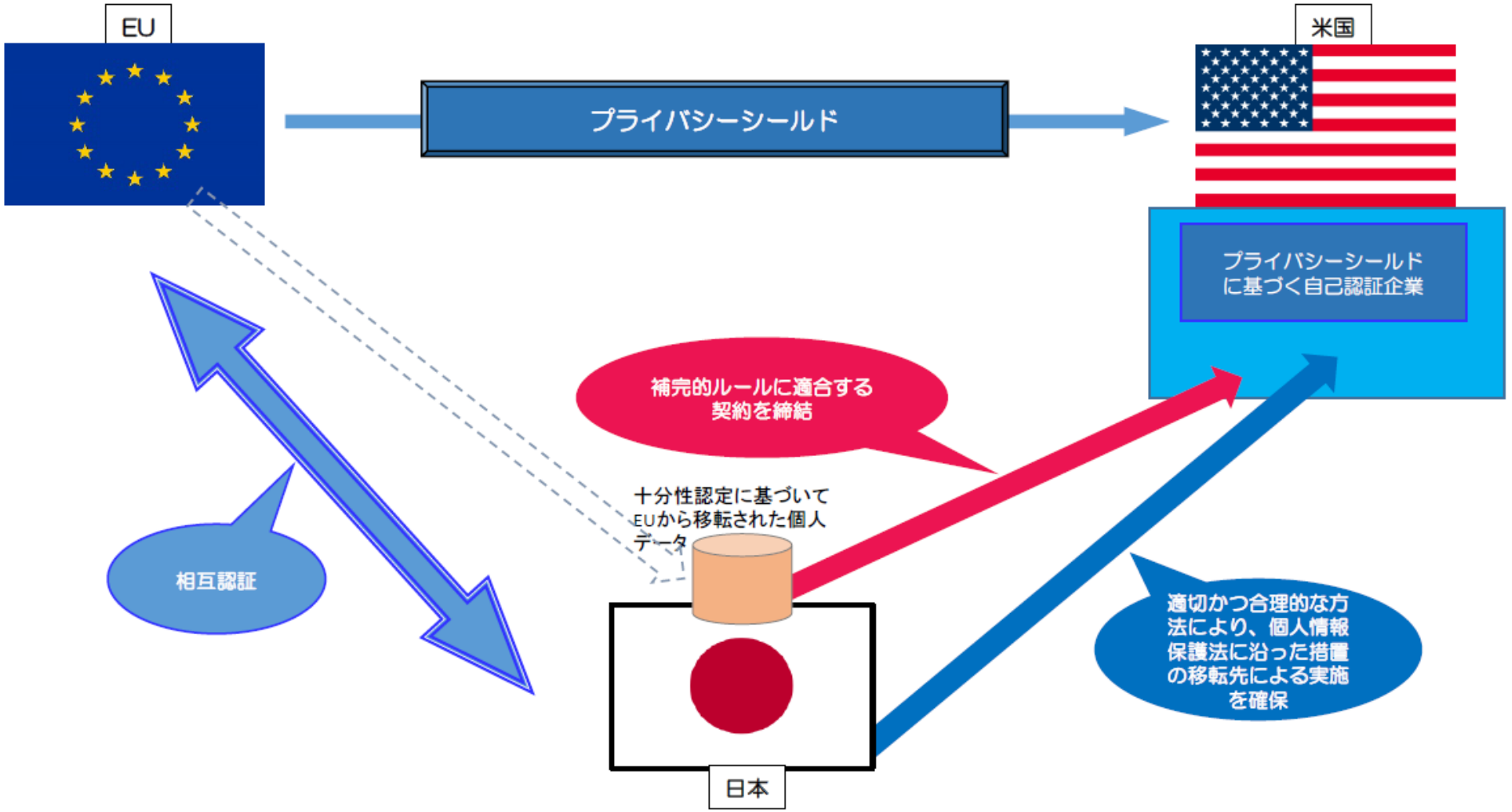


アカウンタビリティ・エージェント：米国（２）、日本（１）、シンガポール（１）
※申請中：韓国、フィリピン

2019年9月15日

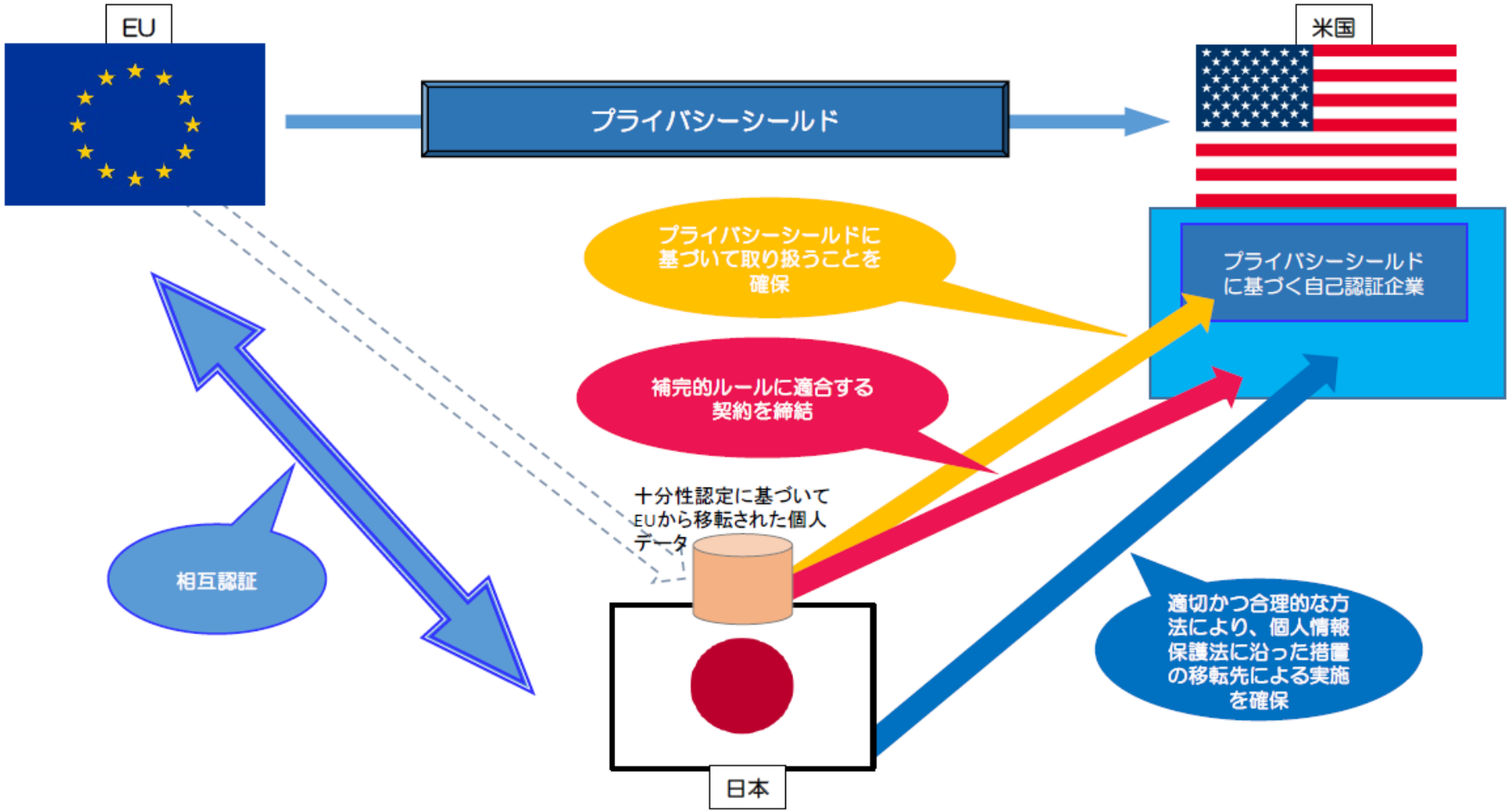
2）国際的なデータ流通の枠組み　－日・米・欧の現状

（個人情報保護委員会資料）



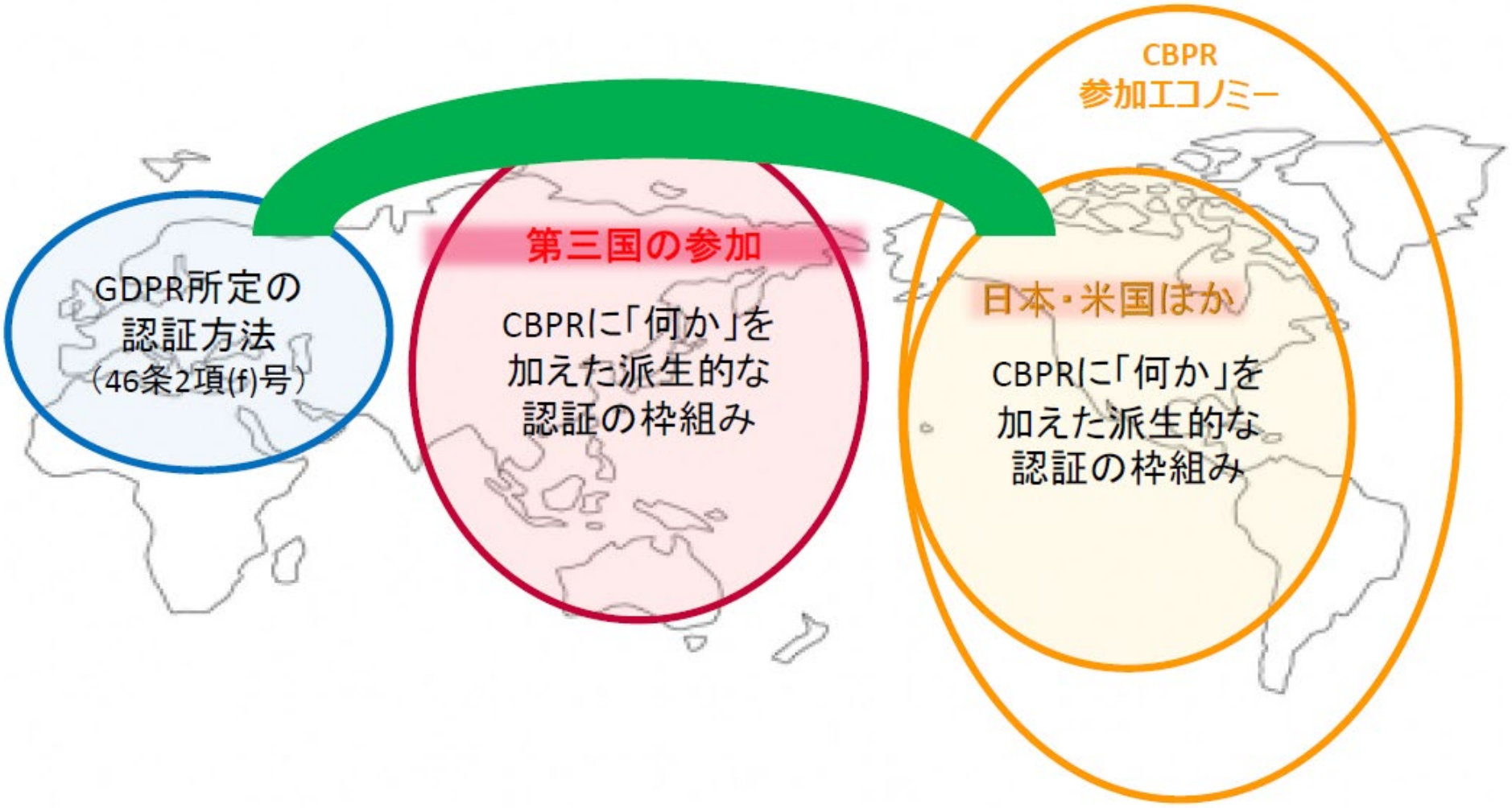
2）国際的なデータ流通の枠組み　－相互運用の可能性

（個人情報保護委員会資料）



2）国際的なデータ流通の枠組み　－グローバル規模でのの可能性

（個人情報保護委員会資料）



プライバシー保護の観点だけではなく、国際的なデータ流通の視点を！

→　本講ではプライバシー保護にフォーカスしていますが、セキュリティについても十分に注意してください！
（問題の多くは個人データの漏洩に関するものです）

→　事業者や組織が利用可能な国際的な枠組みや認証制度については、情報が行き渡っていませんので、個人情報保護委員会や業界団体を活用しましょう！

★注意★　実際の対応については、専門家や弁護士と十分に相談してください！

（ご参考）
個人情報保護からプライバシー保護へ

1）プライバシー　－日本における考え方

1．私生活上の事実、またはそれらしく受け取られるおそれのある事柄であること
2．一般人の感受性を基準として当事者の立場に立った場合、公開を欲しないであろうと認められるべき事柄であること
3．一般の人にまだ知られていない事柄であること

（「宴のあと」裁判　1964年（昭和39年）9月28日　東京地方裁判所）

個人情報に含まれない
プライバシーについては
個人情報保護法の対象外

※電気通信事業法では
「通信の秘密」として
ここに踏み込んでいる
対象者と対象データは限定されている

個別判断が求められるものであり時代によっても変化する。したがって、定義は定性的なものであり定量的ではないため、**個人情報保護法やGDPRのような「DATA」としての形式化は困難。**

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む。）、または個人識別符号が含まれるもの。

（個人情報保護法　第２条１項）

2）プライバシーをとりまく世界の潮流

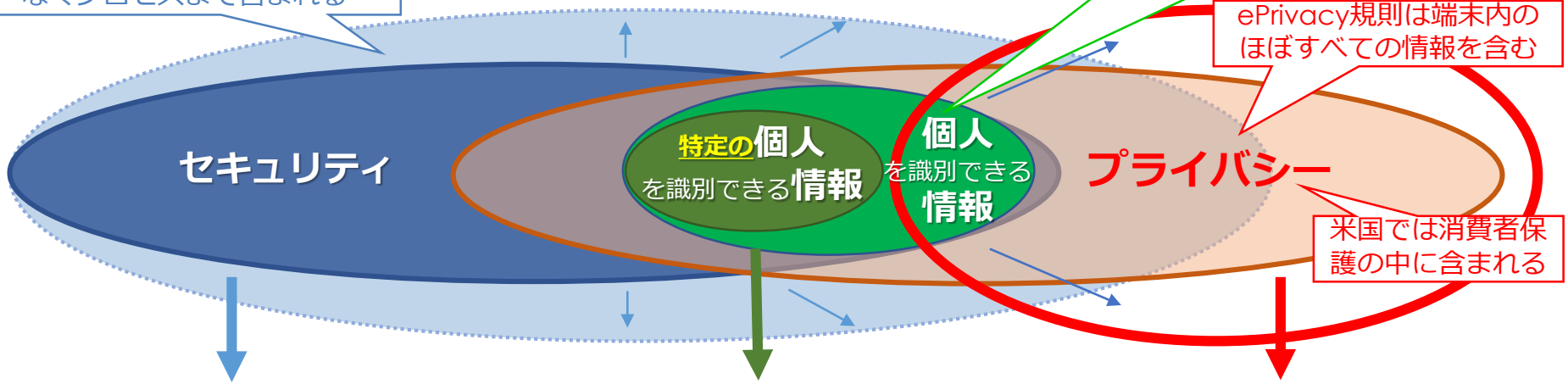
機密性、完全性、可用性の維持
（重要情報・機能・事業・・・）

国によって定義が異なる
日本において法定されているのは個人情報の保護
プライバシー侵害については判例による

リスクベースでのセキュリティ対策は、対象はデータだけではなくプロセスまで含まれる

GDPRはcookieや端末ID等を含む
日本では匿名加工情報が含まれる

ePrivacy規則は端末内のほぼすべての情報を含む



米国では消費者保護の中に含まれる

事業等の態様に加えて
国家安全保障、サプライチェーン
流通する情報全般へと拡大
↓
保護すべき情報の中に
プライバシーに係る情報が含まれ、
処理のプロセスやマネジメントに
ついても言及されている

セキュリティとの関係では
「個人情報保護」に関わる
安全管理措置
↓
管理策が決められる方向性
個人情報の範囲の定義と保護の要件が
拡大する傾向にあり管理策も拡大
※国家の重要情報として政治利用も※

「人」の受容度に依存し、
国家間、時間的変動幅が大きい。
文化、政治体制、経済状況、
治安等多岐に渡る要素からなり
技術進化とサービス普及の
時間軸で変動する。
↓
自主規制、共同規制で対応の方向性

EU：Cyber Security Act
米国：Cyber Security Framework
中国：Cyber Security Law
日本：Cyber Phisycal Security対応Framework

←SET化される方向性→

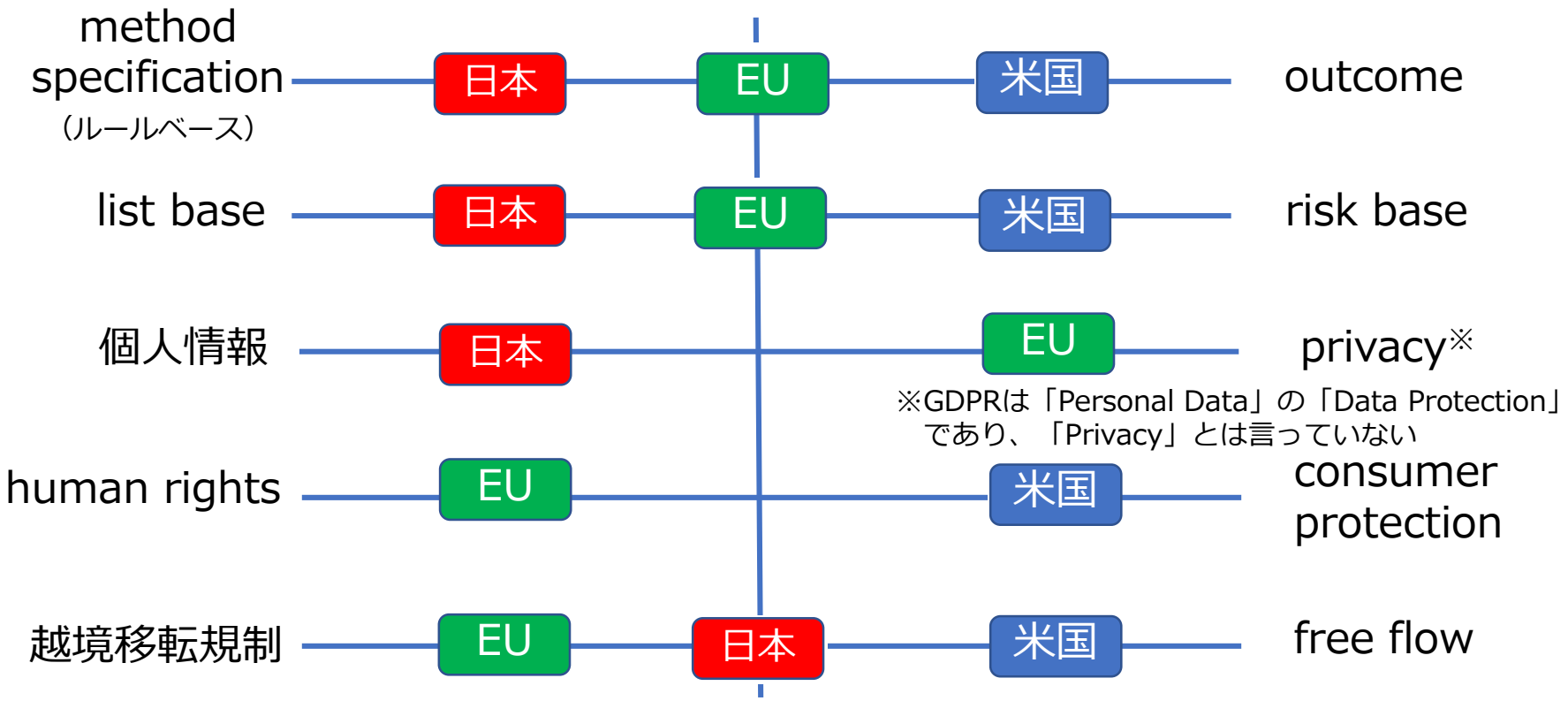
EU：GDPR / ePrivacy Reguration
米国：Privacy Framework / 州法、その他セクター毎
中国：Cyber Security Law /個人情報セキュリティ規範等
日本：個人情報保護法
APEC：Privacy Framework

3）プライバシー関連制度　－主要各国の比較

	原則	根拠法等	法制度（構造）	ガイドライン等	認証等
EU EU	**基本的人権**	欧州連合基本権憲章 ※OECD8原則	GDPR（一次法） ePrivacy規則（補完する二次法） **包括的な整備**	EUと各国の管理当局が発行（EDPB/ENISA/CNIL等）	民間多数(EDPB及び各国認定機関による認証システム構築中)
※アジア太平洋	※域内における貿易及び経済の継続的成長の確保	※APECプライバシーフレームワーク ※OECD8原則	※CPEA（越境執行協力協定）		CBPRシステム
米国 米国	**消費者保護**（不公正または欺瞞的な行為または慣行の禁止）	FTC法（第5条） ・2015年消費者プライバシー権利章典法案/OECD8原則等の影響	セクター毎/州法 ※連邦法提案多数 **適時的**	多様な政府機関（NTIA、NIST：Privacy Framework、SP-800Serieas等）	民間認証
中国	（国家安全）	（中華人民共和国憲法）	サイバーセキュリティ法（個人情報やプライバシーだけではない）	政府各部門、国家インターネット情報弁公室（個人情報安全規範等）	
日本 日本	※個人情報の保護及び適正かつ効果的な活用の促進（個人情報の保護に関する基本方針：閣議決定）	（日本国憲法第13条「すべて国民は、個人として尊重される。」）	個人情報保護法（プライバシーは含まれない、国や自治体も別途） その他事業法 **縦割り傾向**	個人情報保護委員会のガイドライン、認定個人情報保護団体の指針 JIS Q 15001	Pマーク

※APECプライバシーフレームワークは法律ではなく、域内の情報流通を促進するための要件を定めた協定であり、各国のプライバシー保護法を前提としている

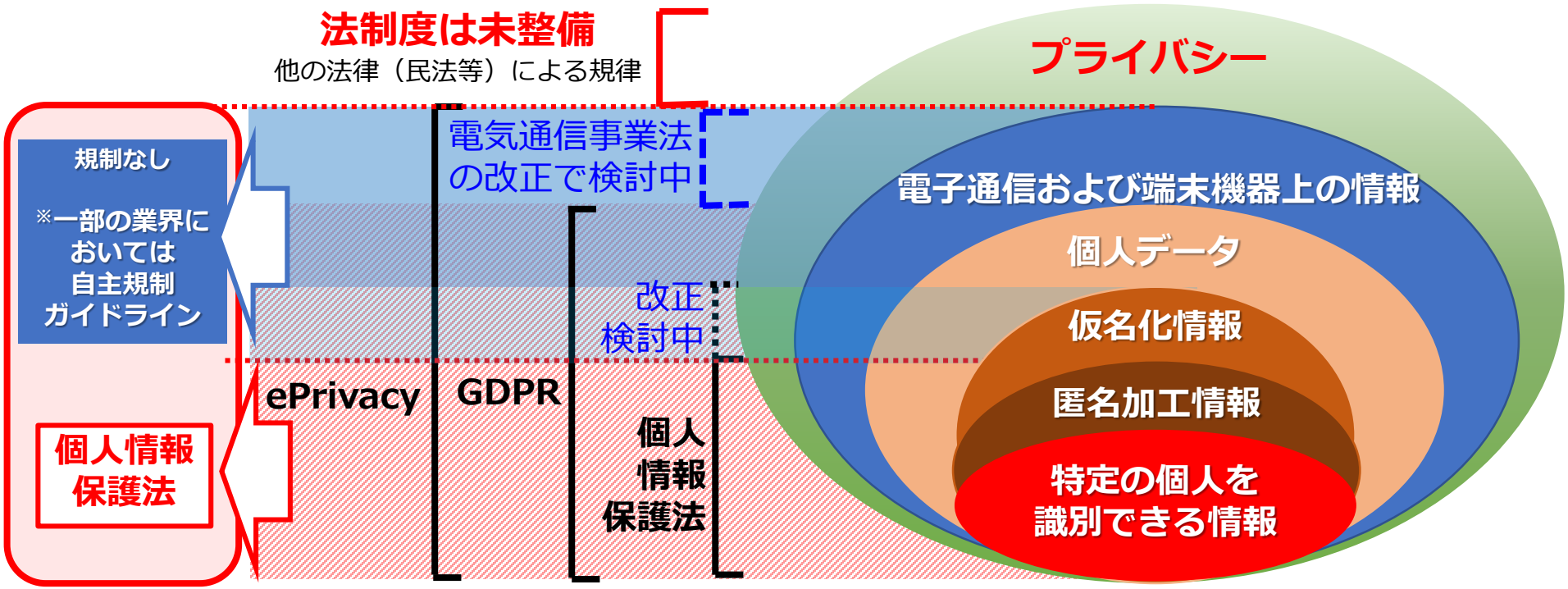
3）プライバシー関連制度　－主要各国の比較



プライバシー保護について個別の規制内容の相違点を解消するためには、それぞれの基本的原則を理解し、根拠や方向性を明らかにし、共有可能なプライバシー保護とはどのようなものであり、その規制の許容水準を見定める必要がある

※完全に自由なPersonal Data流通は、各国のすべての規制を取り込まなければならず、一方で各国ごとに異なる規制に対応することとなると各国ごとの管理が必要になり、いずれも現実的ではない。

3）プライバシー関連制度　－GDPRとの比較

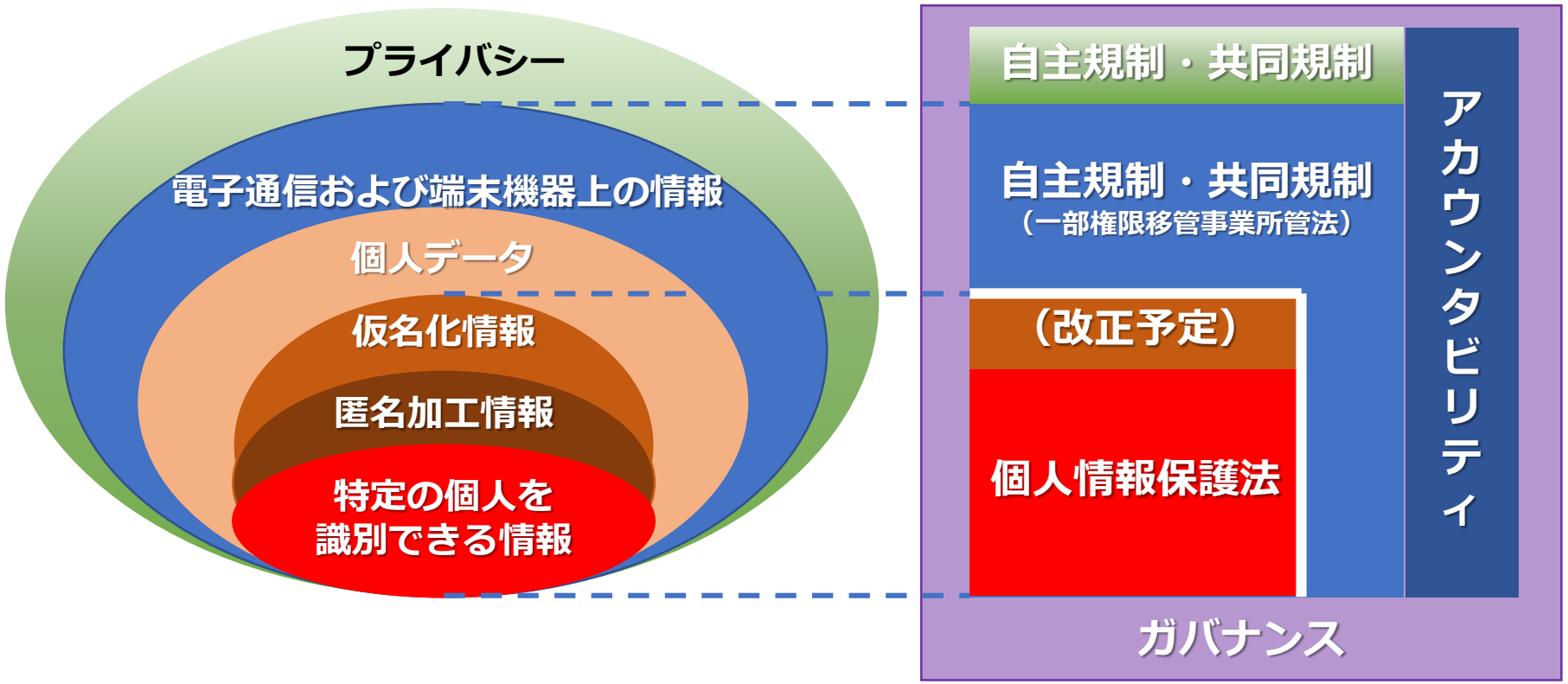


※広告業界におけるcookie等の自主規制
　通信業界における位置情報、端末ID、cookie等のガイドライン

対象とするデータが個人情報保護法よりGDPRのほうが広く、さらにGDPRを補完する法律（ePrivacy規則）により網羅性を拡大している。

※仮名化情報については３年ごと見直しの中で検討中。また、改正の議論がされている電気通信事業法はePrivacy規則に近い。しかしながら、まだGDPRよりは対象が限定されている。（GDPRでは個人を「特定」できなくても対象となる）

4）プライバシー保護への考察



**プライバシー保護に関する自主規制・共同規制の確実な実行を
アカウンタビリティおよびガバナンスの確立により担保することで
個人情報保護法の遵守を信頼（Trust）するという構造を構築できないか？**

プライバシー侵害を引き起こさないための自主規制・共同規制
‖
自主規制・共同規制の遵守はプライバシー侵害を引き起こさない

⇒

個人情報を保護できている
‖
個人情報の遵守

4）プライバシー保護への考察

コンプライアンス

① **個人情報を取得・利用する時のルール**
⇒個人情報を取得した場合は、その利用目的を本人に通知、又は公表すること（あらかじめ利用目的を公表している場合を除く。）
② **個人情報を保管する時のルール**
⇒情報の漏えい等が生じないように安全に管理すること
③ **個人情報を第三者に渡す時のルール**
⇒個人情報を本人以外の第三者に渡すときは、原則として、あらかじめ本人の同意を得ること
④ **個人情報を外国にいる第三者に渡す時のルール**
⑤ **本人から個人情報の開示等を求められた時のルール**
⇒本人からの請求に応じて、個人情報を開示、訂正、利用停止等すること
⑥**匿名加工情報に関するルール**

アカウンタビリティ

個人情報取扱事業者及び匿名加工情報取扱事業者は、上記について責任を負い、かつ、上記の遵守を証明できるようにしなければならない

コーポレート・ガバナンス（内部統制と監査）

個別にルールは決められているが、全体を包括したアカウンタビリティやガバナンスについては明確にされていない。
したがって、この部分を自主規制や共同規制とし、権限の移譲を行うことは可能ではないか？
・直接執行の免除
・違反案件についての是正期間の付与
・減免措置の根拠　等

根拠

認証の取得 PIAの実施

行動規範 CPOの設置

明確な規定なし

罰則等の減免措置

PIA：自主的取り組みと公開
CPO：内部統制（能力認定制度等）

4）プライバシー保護への考察

行動規範
（Code of Conduct／Code of Practice）

一般的には企業理念をステークホルダーに浸透させるためのもの。
https://www.toshiba.co.jp/csr/jp/policy/soc.htm
したがって、プライバシーの文脈での行動規範とは、企業理念に則ったプライバシー保護についてステークホルダーに浸透させるためのものとなる。

CPO（Chief Privacy Officer）

ガバナンス強化のため、事業部門とは独立した（第三者的）な役員クラスであることが重要。

第三者委員会

専門性、ガバナンス確保のため、中立的な専門家による諮問機関。

PIA（Privacy Impact Assessment）

プライバシー保護に関するリスクマネージメントの実行体系。実施・公表によりアカウンタビリティの確保につながる。
→ 企業や事業所単位の認証とは異なり、プロジェクト単位

※その他制度的に検討されていること
コーポレート・ガバナンスコードへの追加
内部監査への追加

基本方針
プライバシーポリシーなど

規律の整備
基本方針のもと
内部規定、マニュアル、社内規定への追加など

組織的安全管理措置
人的安全管理措置
物理的安全管理措置
技術的安全管理措置

整備された規律に基づく具体的な措置

APPENDIX

1）GDPR対応の目標

【全社必須】

1．社内の個人データ保護規定の策定
GDPRの個人データの取扱いの原則の遵守を証明するために必須（アカウンタビリティの原則）

2．プライバシーポリシー（対外）の策定
EEA域内の対象者に対する透明性の確保として必須

3．個人データ侵害通知に関するマニュアルの策定
個人データの侵害があった場合に、データ主体、監督当局等に対する制限時間内の通知のため

4．データ主体の権利行使に対応するマニュアルの策定
情報権、アクセス権、訂正件、削除権、データポータビリティ権、異議権への対応

【必要に応じて】

5．DPO（データ保護責任者）の選任と監督当局への通知
DPOの選任が必要な場合

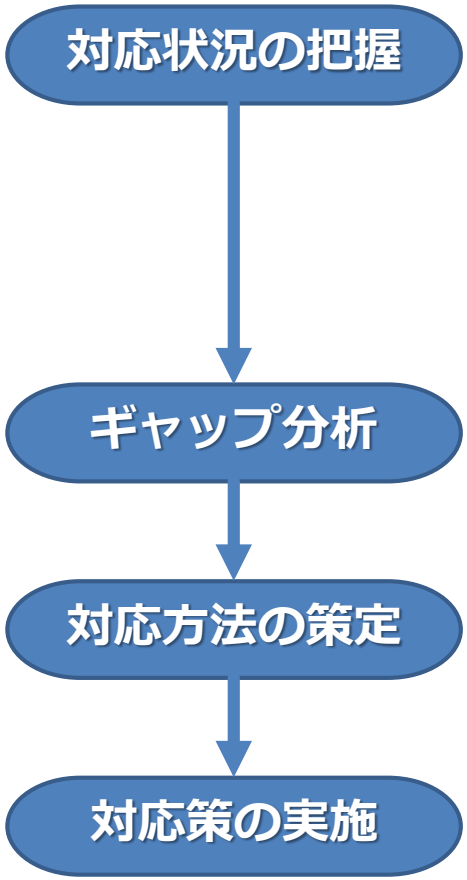
6．管理者⇔処理者、処理者⇔処理者の契約書の整備
処理者がいる場合

7．DPIA（データ保護影響評価）の実行義務の判断
DPIAの実行義務があるか判断し、必要な場合にはDPIAを実施する

8．代理人の指定
EU域内に拠点のない場合

各ドキュメントは当該国の公用語または英語

1）GDPR対応の基本的な流れ



・データ・マッピング
企業グループの本社、子会社、支店などにおいて取扱されるEEA で取得した個人データの取扱の目的、種類(特別カテゴリーの個人データの有無)および量と内容を、各々の本社、子会社、支店などに質問票を送付・回収すること、または、フォローアップのインタビューを行うことで把握する。
・法令、ガイドラインなどにおける要求事項の洗い出し
・資料調査やインタビューによる評価の実施
・評価結果の整理

・要求事項と対応状況を把握した結果を比較
・要求事項との相違を識別し、優先順位付けをする

・現在の対応状況を踏まえて対応方針を検討
・実施に要するコストなどを考慮し、対応方針を策定

・適切な手続き、管理体制、技術面での対応策の実施

JETRO「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）より

2）GDPR対応のガイドライン

Handbook on Security of Personal Data Processing
欧州ネットワーク・情報セキュリティ機関（ENISA）発行：2017年12月

目次

1．データ・マッピング

↓

2．影響の理解および評価
・セキュリティの喪失
・機密性、完全性および可用性の喪失

↓

3．潜在的な脅威の確定および可能性の評価
・ネットワークおよび技術的なリソース
・データ処理業務に関連する処理・手続
・処理業務に関与する様々な当事者および関係者
・処理に関する事業の分野および
・分野毎の脅威発生確率の評価
・脅威の発生に関する評価

↓

4．リスクの評価

↓

5．セキュリティ対策
・技術的対策
・組織的対策

2）GDPR対応のガイドライン

THE CNIL'S GUIDES - 2018 EDITION　SECURITY OF PERSONAL DATA
フランスの情報処理及び自由に関する国家委員会（CNIL）発行：2018年4月

目次

リスクマネジメントの４STEP

個人データの取扱行為及び現状の対策のリスト化
各取扱行為によるリスクの判定
計画された対策の実施とチェック
定期的なセキュリティ監査

体系的に実施されるべき基本的な予防策

各ファクトについて
基本的な予防策
避けるべきこと
追加の措置
がまとめられている

3）参考URL

GDPR関連の仮訳等（個人情報保護委員会）
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

諸外国の個人情報保護制度に係る最新の動向に関する調査研究報告書（個人情報保護委員会
https://www.ppc.go.jp/enforcement/infoprovision/Research/

「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）(2016年11月)
https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html

「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）（2017年8月）
https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html

Handbook on Security of Personal Data Processing（ENISAガイドライン）
https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

THE CNIL'S GUIDES - 2018 EDITION　SECURITY OF PERSONAL DATA
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf

一般財団法人日本情報経済社会推進協会
電子情報利活用研究部　寺田 眞治
terada-shinji@jipdec.or.jp