

2019年度 JIPDECセミナー資料

認定個人情報保護団体の役割

— 認定個人情報保護団体対象事業者であることの意義 —

The logo for JIPDEC, consisting of the letters "JIPDEC" in a bold, black, sans-serif font. A small red dot is positioned above the letter "I".

一般財団法人日本情報経済社会推進協会

認定個人情報保護団体 事務局

(2019年4月5日)

認定個人情報保護団体とは

1. 対象事業者であることの意義
2. 認定個人情報保護団体の位置づけ
3. 認定個人情報保護団体の役割
4. 対象事業者の漏えい等の事故対応
5. 苦情・相談について
6. JIPDEC認定個人情報保護団体の対象事業者になるには

APEC CBPR認証

匿名加工情報について

参考資料

GDPRについて

認定個人情報保護団体とは

1.対象事業者であることの意義

個人情報保護法の改正により、「個人情報取扱事業者」の範囲が拡大しました。さらに、匿名加工情報の作成など、事業者に判断が委ねられる場面が増えています。認定個人情報保護団体は、事業者への個人情報の取扱い等に関する苦情等について第三者的な立場で対応すること等ができるため、認定個人情報保護団体の対象事業者になることは本人と対象事業者の両者にとって有益といえます。

対象事業者のメリット

- 認定個人情報保護団体が第三者機関として関与することで迅速・円滑な苦情の解決が期待できます。
- 認定個人情報保護団体から適切な情報が提供されることによって、適切な個人情報保護の取組が維持できます。
- 個人情報等に関する事故が発生した場合、当協会の監督の下で適切な指導等が行われますので、法律に基づいた立入検査等の権限行使がただちに行われることはありません。
- 個人情報の取扱いや匿名加工情報の作成等、特性に適した方法で扱うための相談ができます。

本人（消費者）のメリット

- 認定個人情報保護団体が第三者機関として関与することで、迅速・円滑な苦情の解決が期待できます。
- 対象事業者の個人情報等の保護のルールが分かって安心です。
- 当協会の監督の下で対象事業者がきちんとルールを守った個人情報等の取扱いが期待できます。

プライバシーマーク制度に基づいて、一般財団法人日本情報経済社会推進協会との間で「プライバシーマーク付与契約」を締結している事業者であれば、当協会の対象事業者となることができます。

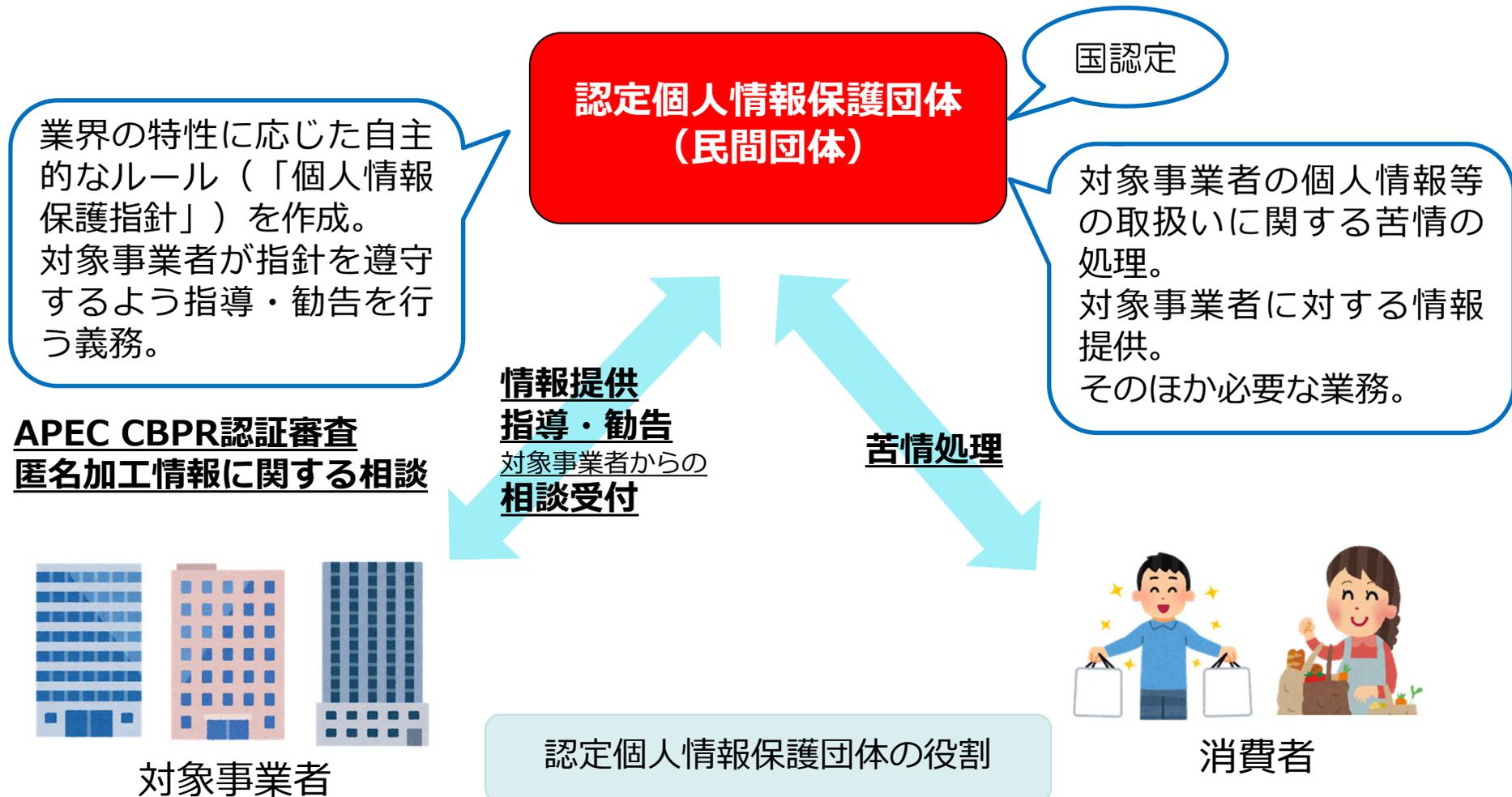
会費について

会費は徴収いたしません。

情報提供業務の一環として研修会等を開催する際には、その都度実費を負担いただく場合があります。

2. 認定個人情報保護団体の位置づけ

事業者の個人情報の適切な取扱いの確保を目的として、個人情報保護委員会から認定を受けた民間団体。
対象事業者への情報提供、個人情報に関する苦情の処理等を行う。



認定個人情報保護団体の業務

1. 対象事業者の個人情報の取扱いに関する苦情の処理。
2. 対象事業者に対する個人情報の適正な取扱いに関する情報の提供。
3. その他、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務。

個人情報保護指針に関する従来の業務

指針を遵守させるための措置を努力義務としていた。

個人情報保護指針の作成についての新たな規定

認定個人情報保護団体は、指針を策定・変更したときは、個人情報保護委員会へ届け出なければならない。

届けられた指針は個人情報保護委員会において公表される。

指針において業界の実状に沿った匿名加工方法を示すなど、その役割の重要性が増すことから、法改正により、指針を遵守させるための措置が義務化された。

3.法改正で強化された認定個人情報保護団体の役割（2）

認定個人情報保護団体は、個人情報保護指針が個人情報保護委員会より公表されたときには、対象事業者に対し、当該個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとらなければならない（53条4項）。

認定個人情報保護団体が、この措置を講ずる義務を怠ると、個人情報保護委員会より報告の徴収や命令を受ける可能性があり（56条、57条）、この命令に従わない場合、認定を取り消される可能性がある（58条1項4号）。

認定個人情報保護団体は、個人情報保護法の趣旨に沿った指針を作成するよう努めなければならない。

この指針を作成する際は、消費者の意見を代表する者その他の関係者の意見を聴くことが求められている（53条1項）。

個人情報保護指針において定める事項

【個人情報について】

- ・ 利用目的の特定
- ・ 安全管理のための措置
- ・ 開示等に応じる手続
- ・ その他の事項

【匿名加工情報について】

- ・ 作成の方法
- ・ 安全管理のための措置
- ・ その他の事項

事業者において個人データの漏えい等の事案が発生した場合等の対応

対象 事案

- ✓ 個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損
- ✓ 加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい
- ✓ これらのおそれ

望ましい対応

- (1) 事業者内部における報告及び被害の拡大防止
- (2) 事実関係の調査及び原因の究明
- (3) 影響範囲の特定
- (4) 再発防止策の検討及び実施
- (5) 影響を受ける可能性のある本人への連絡（事案に応じて）
- (6) 事実関係及び再発防止策等の公表（事案に応じて）

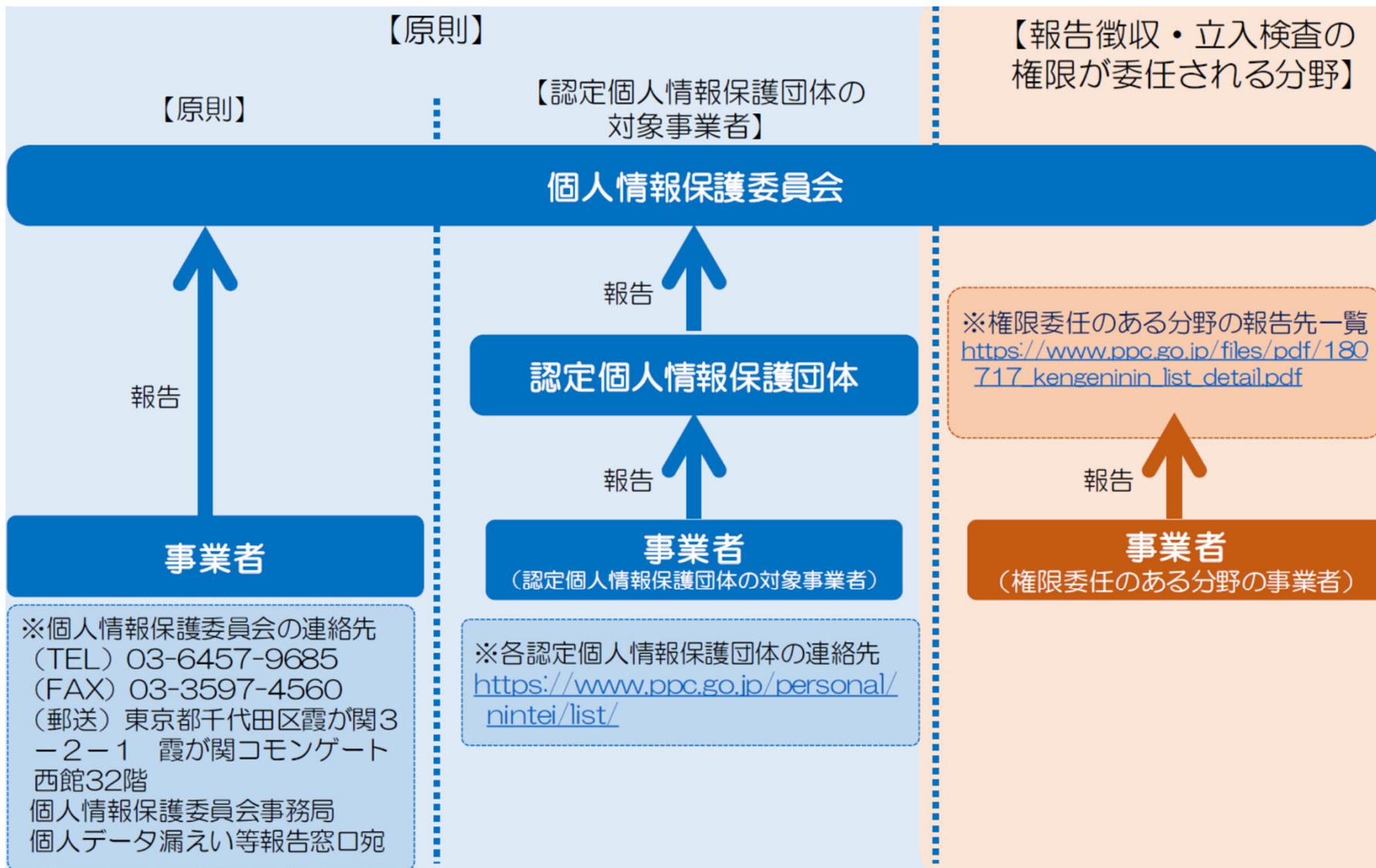
努力義務

個人情報保護委員会等への
速やかな報告

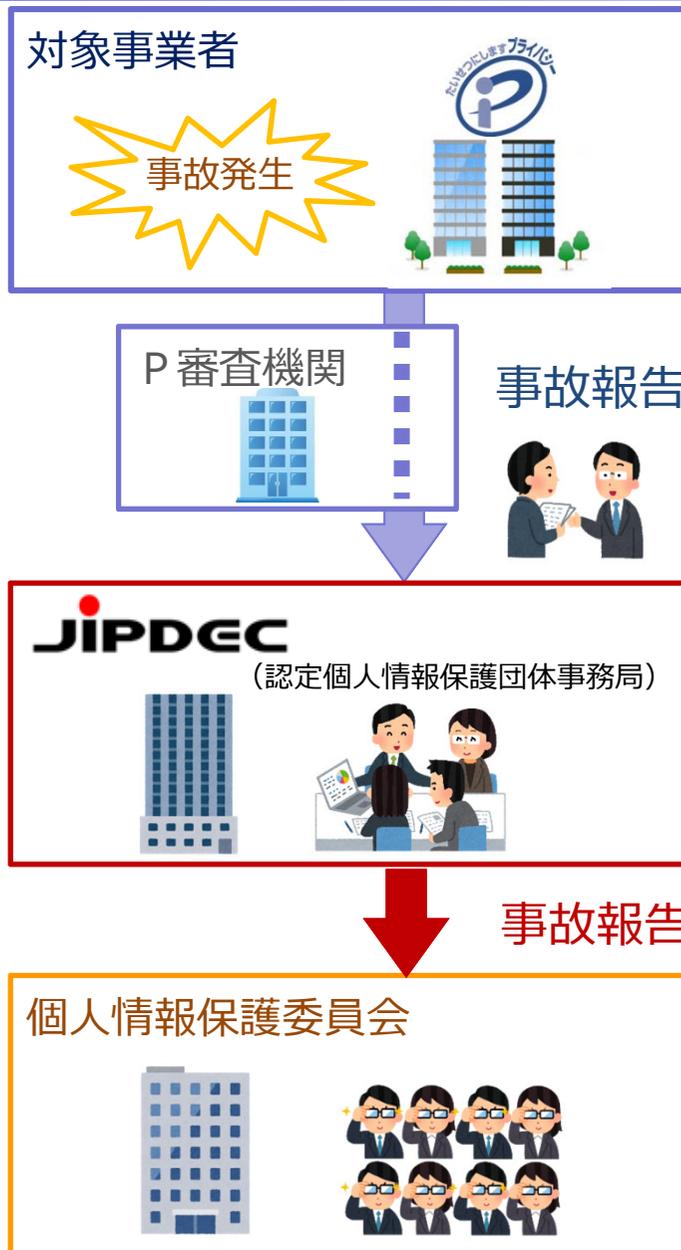
※なお、別途、業法等で監督当局への報告が義務付けられている場合もあるため、注意が必要です。

3.法改正で強化された認定個人情報保護団体の役割（4）

報告先の概要



4.対象事業者の漏えい等の事故対応（1）



① 事故原因調査

② 事故報告書作成・提出

- ✓ 事故の概要
 - ✓ 個人情報の項目・件数
 - ✓ 本人等への対応
 - ✓ 再発防止策の策定 等
- ※ 「様式1」に記入してください。



【注】 認定個人情報保護団体の対象事業者でない場合は、個人情報保護委員会へ直接報告してください。

4.対象事業者の漏えい等の事故対応（2）



すぐに連絡
+
事故報告

助言・連携



速やかに連携
事故報告

適宜連携



①速やかに第一報連絡

JIPDEC
認定個人情報保護団体事務局
TEL:03-5860-7576



②事故原因調査

③事故報告書作成・提出

- ✓ 事故の概要
 - ✓ 個人情報の項目・件数
 - ✓ 本人等への対応
 - ✓ 再発防止策の策定 等
- ※「様式1」に記入してください。



【重大な事故とは】

- 要配慮個人情報¹が漏えいした場合
- 信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合
- 同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合
- 事業者の個人情報を不特定多数の人間が閲覧できる状態になった場合
- 不正アクセスにより大量の情報流出あるいはその可能性がある場合
- 従業員が不正な利益を図る目的で個人データを持ち出した場合
- 当該事案に関して、マスコミに対して報道発表を行う場合、又はマスコミで報道された場合
- インターネットにおいていわゆる「炎上」している場合 等

【注】認定個人情報保護団体の対象事業者でない場合は、個人情報保護委員会へ直接報告してください。

5. 苦情・相談について

(1) 苦情・相談の状況

対象事業者の個人情報の取扱いについて、消費者等からの苦情や相談に応じています（年間150件超）。

(2) 認定個人情報保護団体の表記について

対象事業者は、対象事業者となっている認定個人情報保護団体の名称および苦情の解決の申出先を『本人の知り得る状態』に置くことになっています。

【認定個人情報保護団体の名称、及び苦情の解決の申出先】

認定個人情報保護団体の名称

一般財団法人日本情報経済社会推進協会

苦情の解決の申出先

個人情報保護苦情相談室

〒106-0032 東京都港区六本木一丁目9番9号 六本木ファーストビル内
03-5860-7565 / 0120-700-779（平日9:30~12:00、13:00~16:30）

上記の苦情解決の申出先に対し、消費者が誤って対象事業者の商品やサービスに関する問合せをすることがあります。

これを防止するため、次のような注意書きの併記をお願いします。

【注意書きの例】

➤ 当社の商品・サービスに関する問合せ先ではありません。

➤ 当社の商品・サービスに関する問合せは（*）です。

（*）には、対象事業者の商品・サービスに関する具体的な問合せ先を明記して下さい。

6 .JIPDEC認定個人情報保護団体の対象事業者になるには

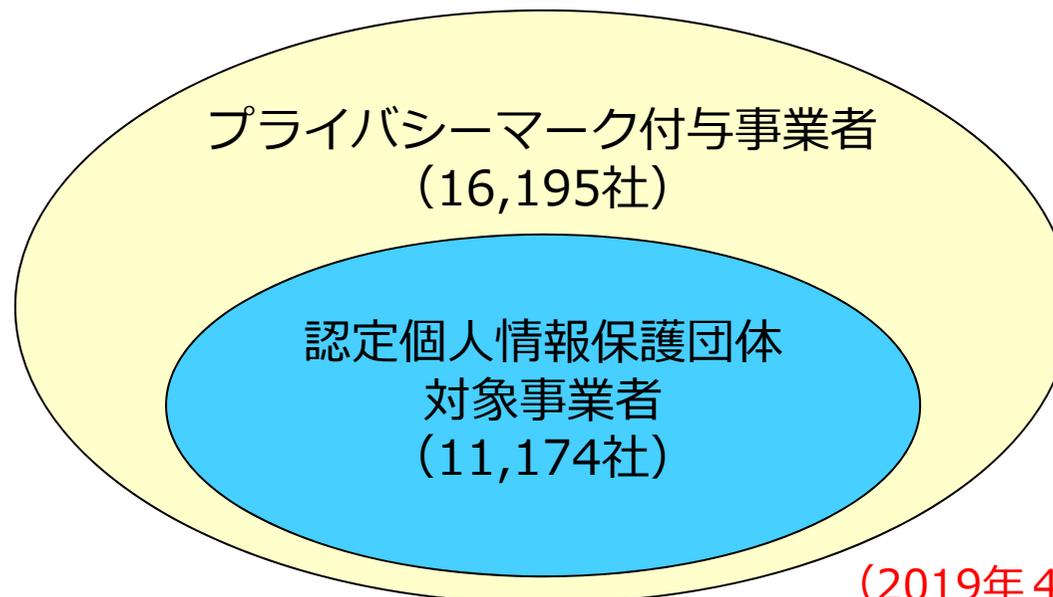
(1) 対象事業者になるには

以下のいずれかの事業者であって、「JIPDEC個人情報保護指針」の遵守ならびに認定個人情報保護団体が行う認定業務（個人情報保護法第51条）の対象となることに同意いただける事業者です。

- ① **当協会が認める第三者認証を受けた事業者**
- ② 電子情報の保護と利活用の推進のため、当協会が認める事業者

(2) 対象事業者になるため手続き（当認定Webページ）

https://www.jipdec.or.jp/protection_org/application.html



(2019年4月1日時点)

APEC CBPR 認証

(1) APEC CBPRシステム

- 企業等の越境個人情報保護に係る取組みに関し、APECプライバシーフレームワークへの適合性を認証する制度。
- APECから認定を受けたアカウントビリティ・エージェント（AA:認証機関）が、自国（エコノミー）の企業等を審査し、認証します。

(2) その背景

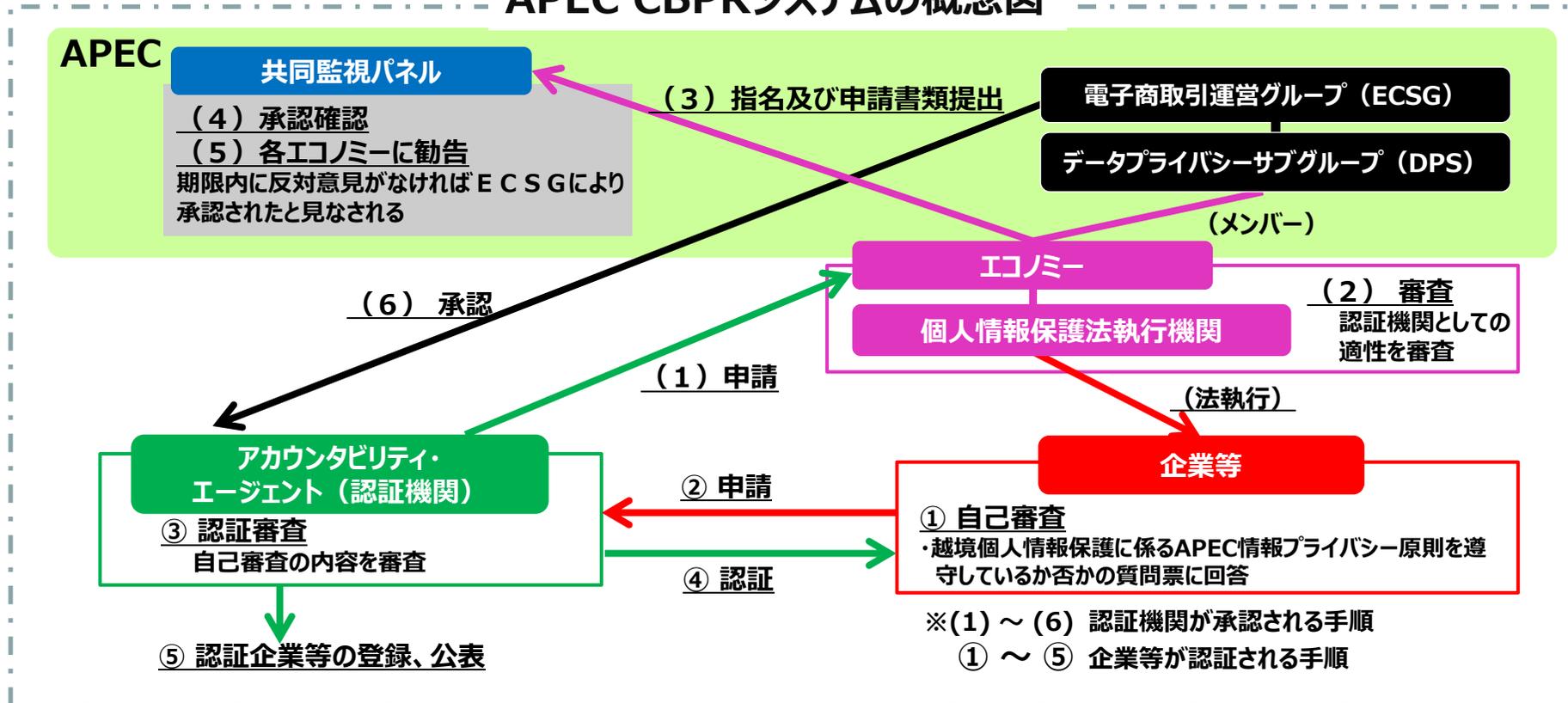
- **APECプライバシーフレームワーク**（2004年10月29日採択）
 - APEC加盟エコノミーにおける整合性のある個人情報保護への取組を促進し、情報流通に対する不要な障害を取り除くことを目的として制定
- **CPEA（越境執行協力協定）**（2009年11月）
 - エコノミー内での情報の取得と管理について、国内の法規や指針を対象に参加国で対応
 - 現在の参加エコノミー：豪州、ニュージーランド、米国、香港、カナダ、日本、韓国、メキシコ、シンガポール
- **CBPR（越境個人情報保護ルール）**（2011年11月）
 - それを運用するための仕組みとして、**CBPRシステム（APEC越境プライバシールールシステム；APEC Cross Border Privacy Rules System（CBPR））**を構築
 - 現在の参加国：米国、メキシコ、日本、カナダ、韓国
 - 現在のAA：TRUST Arc（米国）、JIPDEC（日本）

* APECエコノミーは、21加盟国・地域

APEC CBPR認証 (2)

提供：経済産業省

APEC CBPRシステムの概念図



(3) 認証審査の概要

認証を受けようとする企業等は、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、アカウントビリティ・エージェントは、企業等のAPEC域内のエコノミー間で移転している個人情報の取扱いが、**APECプライバシーフレームワークに従っているかについて審査**を行います。

（4）どのようなことが審査されるのか

国内法の遵守の認証ではなく、越境移転における個人情報の取扱いについて認証される。

項目	確認する内容
通知	APEC通知原則に照らし、①取得される個人情報、移転先、及び利用目的に関する自社のポリシーを本人に必ず理解してもらっているか、②必要最低限の取得になっていることを条件として、本人の個人情報が取得されるタイミング、移転先、及び利用目的を本人に必ず通知しているか。
取得の制限	APEC取得原則に照らし、個人情報の取得がその取得のために表明した目的に確実に限定されているか。
個人情報の利用	APEC利用原則に照らし、個人情報の利用が取得目的及びこれに適合又は関連するその他の目的を達成することに限定されているか。
選択	選択手順に関する規定の条件に照らし、個人情報の取得、利用及び開示に関して本人が必ず選択できるようになっているか。
個人情報の完全性	記録について正確性及び完全性を維持させ、並びに最新化についても維持しているか。
セキュリティ対策	個人がその個人情報を組織に預けるときに、個人情報の紛失、不正なアクセス、不正な破壊、利用、変更若しくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されているか。
アクセス及び訂正	本人がその個人情報にアクセスして、訂正することができることを保証しているか。
説明責任	上記原則の実施方法を遵守することについて確実に説明責任を果たしているか、また、移転後にこの原則に従って個人情報を確実に保護するための合理的な措置を用意しているか。

（5）認証審査の申請手続きについて

https://www.jipdec.or.jp/protection_org/cbpr/index.html

（６）CBPR認証をうける利点

- 取引（対事業者、対消費者）の際に、APECプライバシーフレームワークに適合した個人情報の取扱いを行っていることを示すことを対外的にアピールできる。

- 認証を受けた事業者に対して、APEC域内からの苦情・相談等について、ケースに応じて、AA（認証機関）が調整を行う。
 - 事故などが発生した場合、認証を受けた事業者は、AAとの対応になる。
 - 一方、認証を受けていない事業者は、政府機関（日本では個人情報保護委員会）が直接対応する。

- その他
 - 政府は、国内事業者が個人情報の取扱いを海外の事業者へ委託する際の委託先の監督義務を満たす要件として、CBPR認証を奨励している（次スライド）。

APEC CBPR認証（5）

改正個人情報保護法第24条では、以下に該当する場合「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要は無いとしています。

また、各ケースの内容は委員会規則で定めるとしています。

法第24条のケース	具体的な内容
当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。以下「規則」という。）で定める国にある場合	個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国は、EU（※）が該当する。 https://www.ppc.go.jp/files/pdf/190123_h31iinkaikokuji01.pdf
当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として規則で定める基準に適合する体制を整備している場合	① 第三国の提供事業者がCBPRを取得している場合。 ② 国内の事業者がCBPRを取得している場合は、提供先の第三国の事業者に個人データ処理を委託する場合に限って、その第三国の事業者が適切に個人データを取り扱えるとみなせるとして、個人情報保護委員会が国内事業者のCBPRの取得を奨励
法第23条第1項各号に該当する場合	—

※ 欧州経済領域協定に規定された国

匿名加工情報について

匿名加工情報（第三者提供・目的外利用の本人同意不要）

- 特定の個人を識別することができないよう加工した情報（個人情報として復元できないもの）

個人情報取扱事業者としての義務

- 【作成】加工方法（法定、安全管理）／公表（個人に関する情報の項目、安全管理措置等）／明示（匿名加工情報）／復元の禁止

匿名加工情報取扱事業者としての義務

- 【提供】公表（個人に関する情報の項目、提供方法）／明示（匿名加工情報であること）
- 【識別行為の禁止】再識別化の禁止
- 【安全管理措置等】

個人情報保護委員会の文献以外で参考になるもの

匿名加工情報

『匿名加工情報の適正な加工の方法に関する報告書』（国立情報学研究所、2017）

<http://www.nii.ac.jp/news/release/2017/0221.html>

『匿名加工作成マニュアル』（経済産業省、2016）

<http://www.meti.go.jp/press/2016/08/20160808002/20160808002.html>

『分かりにくい匿名加工情報、JIPDECが事例集で活用促進』（日経BP、2017）

<http://itpro.nikkeibp.co.jp/atcl/column/14/346926/072401068/>

匿名加工情報 (2)

特定の個人を識別することができないよう加工した情報（個人情報として復元できないもの）のイメージ ← **再識別の禁止、復元の禁止**



統計情報

年代	人数	趣味	今居る場所 (メッシュコード)
20	10	映画鑑賞	51340375
30	20	映画鑑賞	51340375
40	5	映画鑑賞	51340375
50	7	映画鑑賞	51340375
.....			

全ての項目に対して、目的制限なく二次利用可能



匿名加工情報

住んでいる地域	年齢	性別	趣味	今居る場所 (緯度経度)
東京都港区芝公園	25	男	映画鑑賞	20 00 00.000,142 00 00.001
東京都港区芝公園	23	男	ドライブ	20 00 00.089,122 00 00.000
東京都港区芝公園	21	女	料理	20 00 00.780,122 00 30.009

- 個人を特定しない情報
- 個人情報に復元されない情報



個人情報

氏名	住所	生年月日	年齢	性別	趣味	今いる場所 (緯度経度)
山田太郎	東京都港区芝公園3-5-8	平成元年1月1日	25	男	映画鑑賞	20 00 00.000, 142 00 00.001
川田二郎	東京都港区芝公園2-5-9	平成4年2月1日	23	男	ドライブ	20 00 00.089, 122 00 00.000
池田花子	東京都港区芝公園6-15-18	平成5年6月14日	21	女	料理	20 00 00.780, 122 00 30.009
.....						

支援策の概要

対象

- 当協会認定個人情報保護団体の対象事業者

方法

- 有識者による検討会を設置し、3～4回程度の検討会を開催します。
- 助言する加工方法や契約時の配慮事項等を報告書にまとめ、ご相談があった対象事業者へお渡しします。

ご用意いただくもの

- 匿名加工情報の利用目的（第三者提供する場合には、提供先の目的）について、概要が分かる資料
- 匿名加工する対象データのサンプル（実データである必要はありません。）
- その他検討している内容が分かるもの

費用について

- 実費のみ（検討会開催費用（謝金等）、データの再識別リスクなどの検証費など）

検討手順

- 3～4回の有識者による検討会を開催（検討期間2～3ヶ月を予定。）
 - ご相談者となる事業者の方にも出席いただきます。

回数	議事
1	利用目的の確認、加工方法、契約時の配慮事項の検討
2	加工方法の確認、再識別リスク等の確認
3	契約時の配慮事項の確認、その他考慮事項の確認

- 審議終了後、報告書を作成し納品。



參考資料

【認定個人情報保護団体 一覧】

43団体 2019年4月1日現在 

一般社団法人全国警備業協会	特定非営利活動法人日本手技療法協会
一般社団法人全日本指定自動車教習所協会連合会	一般社団法人日本個人情報管理協会
日本証券業協会	一般社団法人全日本ギフト用品協会
一般社団法人生命保険協会	一般社団法人日本クレジット協会
一般社団法人日本損害保険協会	公益社団法人東京グラフィックサービス工業会
一般社団法人外国損害保険協会	一般社団法人日本専門店協会
全国銀行個人情報保護協議会	特定非営利活動法人日本個人・医療情報管理協会
一般社団法人信託協会	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
一般社団法人投資信託協会	日本個人情報保護協会
一般社団法人日本投資顧問業協会	一般社団法人結婚相談業サポート協会
日本貸金業協会	一般社団法人日本結婚相手紹介サービス協議会
一般社団法人金融先物取引業協会	株式会社 I B J (日本結婚相談所連盟)
一般財団法人放送セキュリティセンター	ナノライセンス結婚専科システム協議会
一般財団法人日本データ通信協会	大阪毎日新聞販売店事業協同組合
一般財団法人日本情報経済社会推進協会	J E C I A 個人情報保護協会
日本製薬団体連合会	全国こころの会葬祭事業協同組合
公益社団法人全日本病院協会	一般社団法人ビジネスコンプライアンス
一般社団法人モバイル・コンテンツ・フォーラム	一般社団法人医療データベース協会
特定非営利活動法人医療ネットワーク支援センター	特定非営利活動法人検定協議会
一般社団法人全国自動車標板協議会	一般社団法人国際情報セキュリティーマネジメント研究所
公益財団法人日本通信販売協会	一般社団法人中小企業個人情報セキュリティー推進協会
	一般社団法人日本情報システム・ユーザー協会

【法】

個人情報保護に関する法律（平成15年5月30日法律第57号）

最終改正：平成28年5月27日法律第51号

【基本方針】

個人情報保護に関する基本方針（平成16年4月2日閣議決定）

平成30年6月12日一部変更

【政令】

個人情報保護に関する法律施行令（平成15年12月10日政令第507号）

最終改正：平成28年10月5日政令第324号

【規則】

個人情報保護に関する法律施行規則（平成28年10月5日個人情報保護委員会規則第3号）

【補完的ルール】

個人情報保護に関する法律に係るEU域内から充分性認定により移転を受けた個人データの取扱いに関する補完的ルール

【ガイドライン】

個人情報保護に関する法律についてのガイドライン（通則編）

（平成28年11月個人情報保護委員会ガイドライン）

個人情報保護に関する法律についてのガイドライン（外国にある第三者への提供編）

（平成28年11月個人情報保護委員会ガイドライン）

個人情報保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）

（平成28年11月個人情報保護委員会ガイドライン）

個人情報保護に関する法律についてのガイドライン（匿名加工情報編）

（平成28年11月個人情報保護委員会ガイドライン）

【認定個人情報保護団体の定める個人情報保護指針】

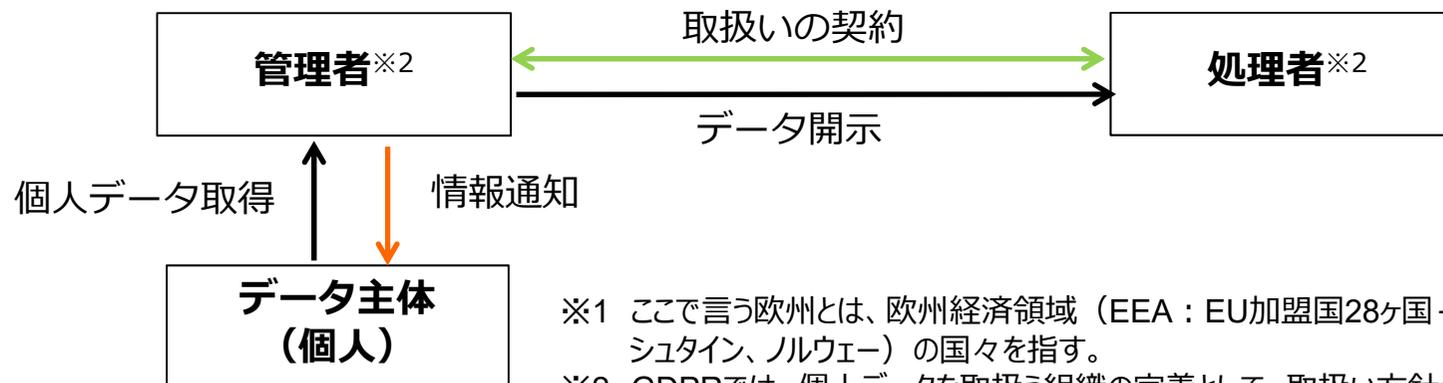
JIPDEC個人情報保護指針（平成29年5月一般財団法人日本情報経済社会推進協会）

GDPRについて

■「個人データ」の「取扱い（処理）」と「移転」に関する法律

- 正式な名称は、「**個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則**」
- 欧州※¹在住者の個人データの取扱いと、欧州在住者の個人データを欧州から第三国に移転するために満たすべき法的要件を規定したものの。
- **原則、移転は禁止されており、例外を法定化している。**

【GDPRにおけるデータ処理の一般的な姿（イメージ）】

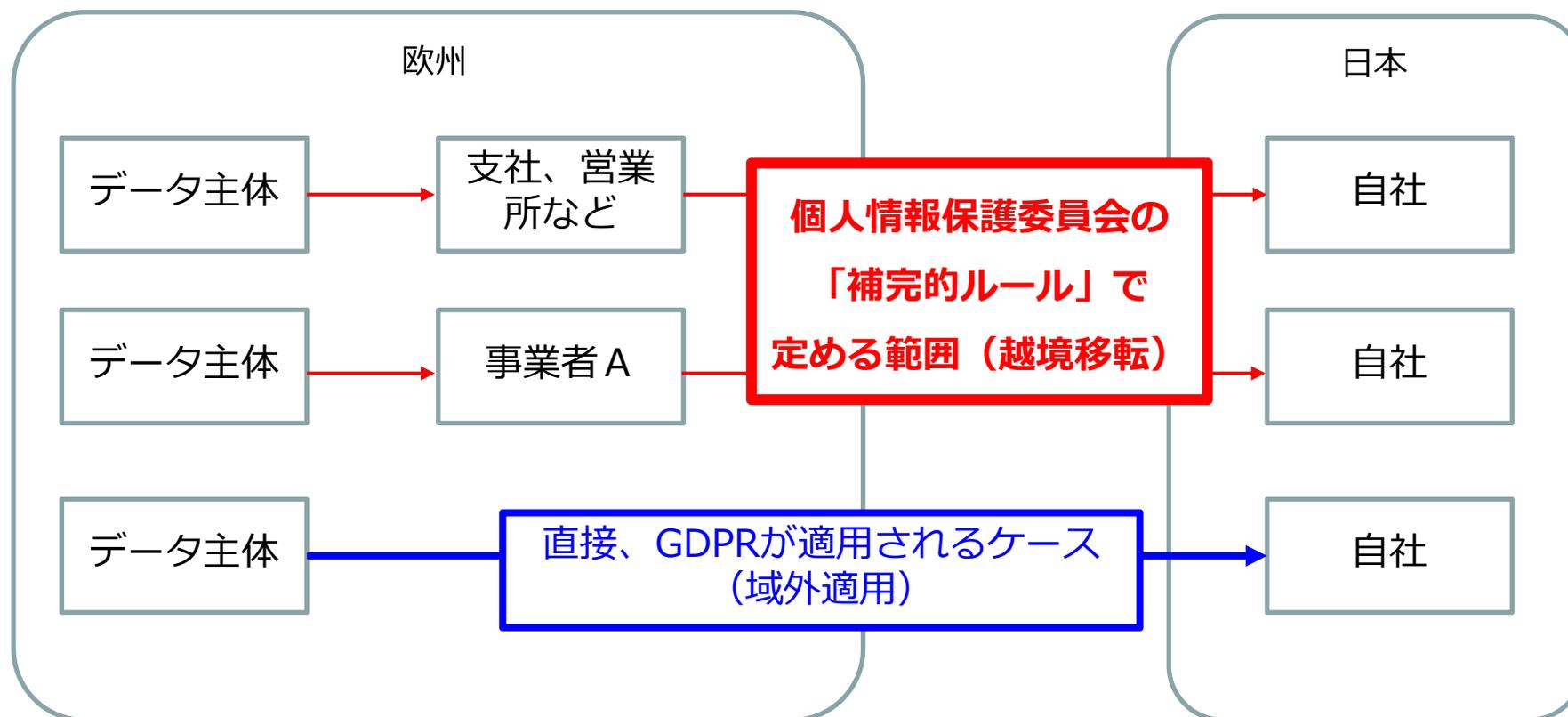


※1 ここで言う欧州とは、欧州経済領域（EEA：EU加盟国28ヶ国＋アイスランド、リヒテンシュタイン、ノルウェー）の国々を指す。

※2 GDPRでは、個人データを取扱う組織の定義として、取扱い方針やルールを定める責任を負う「管理者」と、管理者からの指示や委託を受けて個人データの処理や保管のみを行う「処理者」の2種類がある。もちろん、運用上、管理者と処理者が同一のケースもある。

■ 欧州から個人データを移転する組織※1はすべて対象となる。

- 欧州の組織から個人データの移転を受ける組織は、個人情報保護法の補完的ルール※2に基づき対応を行う。
- 一方で、その対象外になる組織もある。（直接、個人データを取得する組織は、GDPRの直接適用を受ける可能性がある。）



※1 個人情報保護法の対象は「事業者」だが、GDPRは事業者だけでなく自治体や政府などの組織も対象となる。

※2 「個人情報の保護に関する法律に係るEU域内から充分性認定により移転を受けた個人データの取扱いに関する補完的ルール」

- 要配慮個人情報に、性生活・性的志向・労働組合を含める。
 - プライバシーマーク（JISQ15001）の審査において、既に管理すべき対象に入っている。
- 保有個人データ（保有期間に関わらず開示請求の対象となる。）
 - プライバシーマーク（JISQ15001）の審査においては、既に対応している。
- 第三者提供
 - 第三者提供先では、確認記録義務の範囲内で利用する。
- 再移転
 - 移転元と移転先の契約等により、保護水準を同等にする。
- 匿名加工情報
 - 再識別化の可能性を残してはならず、対応表を削除し、連結不可能にしなければならない。

**対象事業者様からの個別相談を
受け付けています。**

(お問合せ先)

〒106-0032

東京都港区六本木一丁目9番9号 六本木ファーストビル内

一般財団法人日本情報経済社会推進協会 (JIPDEC)

認定個人情報保護団体事務局

nintei-inq@tower.jipdec.or.jp

https://www.jipdec.or.jp/protection_org/index.html

ありがとうございました