情報法制研究会第4回シンポジウム　資料

APEC／CBPRシステムの概要

2016年6月12日

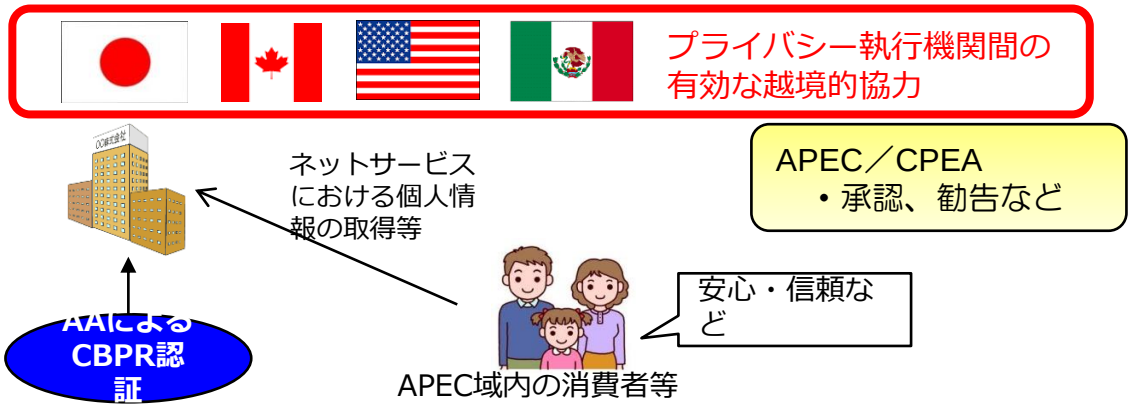
JIPDEC　常務理事
認定個人情報保護団体事務局　事務局長　坂下哲也
sakashita-tetsuya @ jipdec.or.jp
（JIPDEC法人番号：1 0104 0500 9403）

はじめに

- 当協会は、2016年1月、日本で初めてとなる、アジア太平洋経済協力（APEC）のCBPRシステム（Cross Border Privacy Rulesシステム）のアカウンタビリティ・エージェント（Accountability Agent, 略称「AA」）に認定されました。
- APEC／CBPRs（The Cross Border Privacy Rules System：越境個人情報保護ルール；APEC／CBPRシステム）は、日本も参加しているAPECプライバシーフレームワーク（2004年10月採択）の目的である**「適切な情報プライバシー保護策の策定を奨励し、アジア太平洋地域での情報の自由な移動を保証する際の重要な手段」**を具体化するために開始された仕組みです。
- APEC／CBPRの申請を事業者が行うにあたり、当認定個人情報保護団体の対象事業者となっていることが求められます。
  - 具体的には、①当協会が運営する個人情報保護にかかる認証制度の認証事業者、②電子情報の保護と利活用の推進のため当協会内に組織する事業プログラム制度の会員のどちらか一方の要件を満たすことが必要であり、また、当協会認定個人情報保護団体の個人情報保護指針の遵守を同意することが必要です。
- 本紙は、本会で貴重な機会を頂きましたので、APEC／CBPRシステムの概要を御説明する資料です。

APEC（アジア太平洋経済協力機構）の取り組み

- **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。**
  - **参加国は豪州、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**（日本は2011年11月以降、国内の16省庁がプライバシー執行機関として参加）。
    - 事案照会・共同調査・執行活動等のプライバシー保護法の執行に係るプライバシー執行機関間の有効な越境的協力
- **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**
  - **米国、メキシコ、日本、カナダが参加**
    - CPEAに参加しているエコノミーの中で、CBPRへの参加を申請し承認を受けたエコノミーで運用。少なくともAAを一機関を有することが必要。
      - 米：TRUSTe、日本：JIPDEC

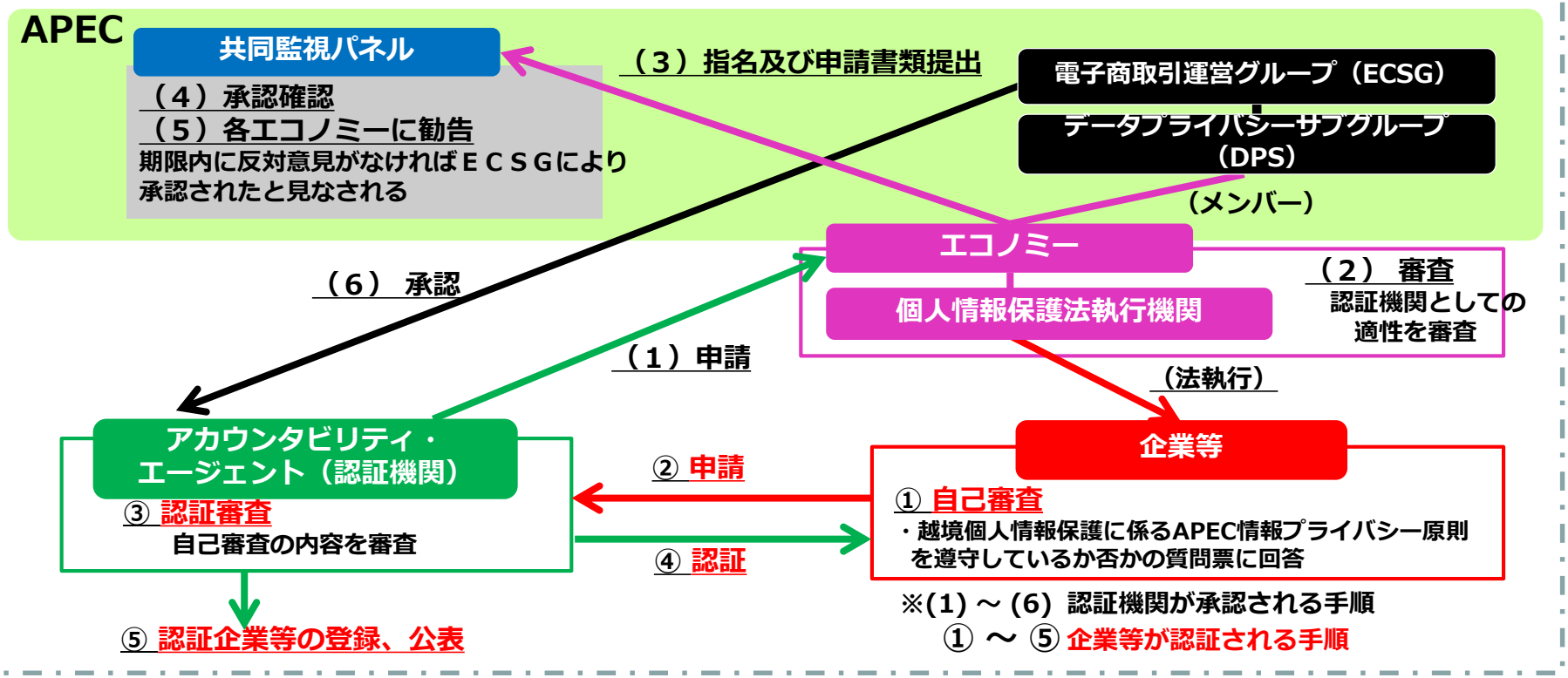


【参考】CBPRの仕組み（提供：経済産業省）

➢ 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）
- 2016年6月現在、現在、米国、メキシコ、日本、カナダがエコノミーとして参加。
- 認証機関としてアメリカのTRUSTe※が認定を取得し、米IBM、Apple、HP等が認証を取得済み。
  ※ウェブサイトにおける個人情報取り扱いに関する認証制度を管理している米国の営利団体

APEC/CBPRシステムの概念図



APEC／CBPRシステムについて

- 事業者を対象に、**APECプライバシー原則に基づく事前質問書**に基づき、以下の点を確認し、認証するものがCBPRシステムです。
  - 個人情報が絡む取引相手の企業等に対して、APECの原則に合致した適切なポリシーと手続を備えており、個人情報を取得する際に必要となる説明をしているか。
  - 消費者に対して、国境を越えて送信される個人情報が保護されることを信頼及び信用できる仕組みをもっているか。
- 認証を受ける事業者が行わなくてはならないこと。
  - 自ら取得又は受領し、他の参加APECエコノミーとの間での越境移転の対象となるすべての個人情報に対して、CBPRの要件に合致したプライバシーポリシー及び手続を実施すること。
  - プライバシーポリシー及び手順は、CBPRの要件の遵守に関して、APEC認定アカウンタビリティエージェントによる評価を受けること。
    - CBPRの認証は**1年更新**（APECでは「再認証」という）です。
- その他
  - CBPRシステムに参加することにより、参加組織の国内の法的義務が置き換えられることはない。
    - ただし、CBPRシステムの認証要件は国内法等で担保されている。
    - なお、CBPRシステムはAPEC域内の個人情報の移転に適用されるものであり、国内法を遵守していることを認証するものではない。

→ この認証を行うため、当事務局では、個人情報保護指針を旧法に基づき改訂。

AAの役割

- アカウンタビリティエージェント（日本の場合、JIPDEC）は、CBPRシステムの認証プロセスである自己評価の審査に対して責任もち、実施する。
  - 申請する組織は、自身のプライバシーポリシー及び手順の策定に責任を負い、関係するアカウンタビリティエージェントによって、そのポリシー及び手順がCBPRシステムの要件を遵守していると認証された場合にのみ、CBPRシステムに参加することができる。
  - 随時、認証を受けた事業者の**モニタリング**を行い、取り扱う個人情報等の変更などがないか確認を行う。（変更届による対応も有。）

- **苦情処理**を行い、また匿名での事例記録及び苦情に関する統計資料をAPECへ提出する。

- なお、モニタリングや苦情処理の結果によっては、追加の調査依頼や認証の一時停止、取り消しなどを行う場合がある。**（ペナルティ）**

ペナルティ

『公表』	『取り消し』	重大	・CBPR認証の申請事項に虚偽の記載があった場合 ・注意、改善指導等の回答期限を過ぎても改善されない場合 ・故意または重大な過失による個人情報の取扱い事件や事故があった場合 ・その他、当会が認証を取り消すべきだと判断した場合	特別審査
	『一時停止』		・故意または重大な過失による個人情報の取扱い事件や事故のおそれがある場合 ・注意、改善指導等の回答期限を過ぎても改善されない場合 ・その他、当会が認証を一時停止すべきだと判断した場合	
非公開	改善指導（勧告）		・中規模な個人情報の取扱い事件や事故があった場合 ・注意等による回答期限を過ぎても改善されない場合 ・その他、当会が判断した場合	
	注意	軽微	・小規模または軽微な個人情報の取扱い事件や事故があった場合 ・その他、当会が判断した場合	調査・依頼
	モニタリング	状況確認	・CBPR認証事業者のWebサイト等における公表事項の査読 ・ニュースや記事等における公表事項の査読	

改善の猶予期間あり

『赤太文字』：AAの義務

※この他に、関係監督官庁への通知（連携）。

申請から登録までの流れ

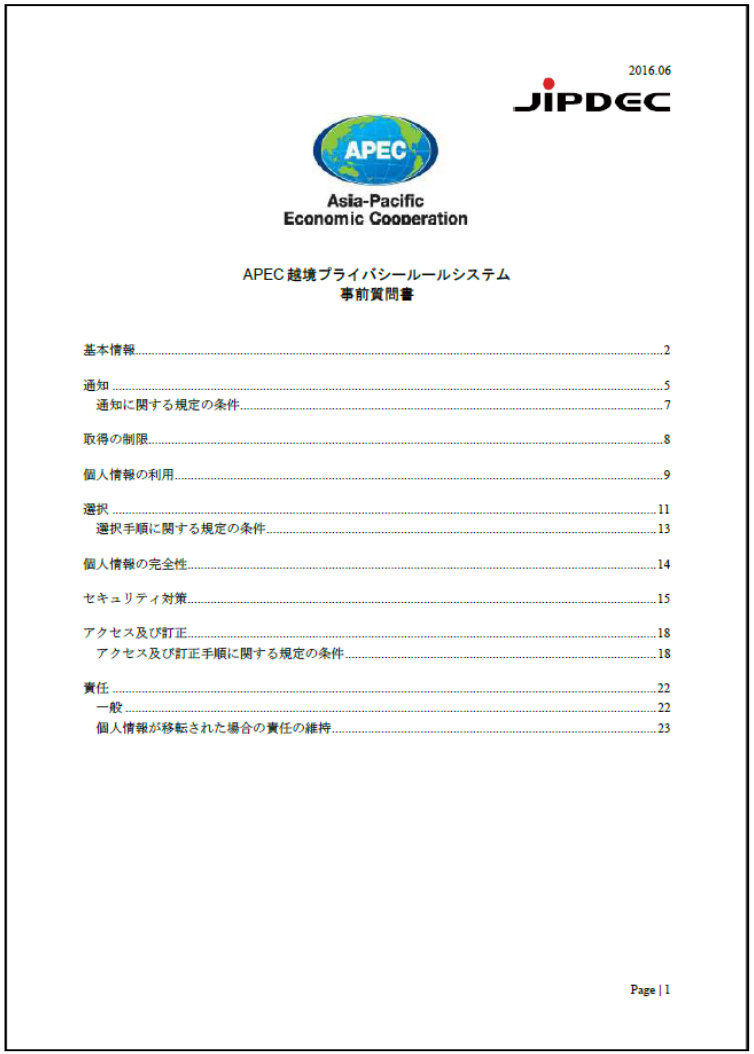
- AAである認定個人情報保護団体の対象事業者となる。
- 申請から登録までの流れ
  - 手順として、**①申請、②審査（文書・現地）、③審査会、④登録**を設定。

手順	申請者の主な提出物	認定個人情報保護団体事務局の対応
申請	1．**事前質問書** 2．申請書	1．書類の確認 2．CBPR規程の順守に関する確認 3．審査料の請求 4．申請申込書受理
審査（文書）	1．規定類（和・英文） 2．対外公表文書（和・英文） 3．審査に必要な内規他（和文）	1．ヒアリング（全体の聞き取り） 2．文書審査
審査（現地）	（立ち合いと説明）	1．申請事業者の運用状況を現地で確認 （主に、セキュリティ等の確認）
審査会		1．審査会を開催し、認証可否を決定 2．認証管理料の請求
登録		1．認証管理料の払い込み確認 2．認証書の発行 3．名称の登録・HP公表

事前質問書の内容（１）

■ 事前質問書は、**APECの原則に照らし**個人情報の取扱いに関する50の質問に対する回答を申請者が記載するもの。
（根拠書類等も必要）

- 質問項目の内容は、国内法と整合性を取るため調整を政府において実施。
  - 国内法の認証ではないがこのスキームに則れば結果的に違法な取扱いはしないという考え。



2016.06

JIPDEC

APEC

Asia-Pacific
Economic Cooperation

APEC越境プライバシールールシステム
事前質問書

Page | 1

事前質問書の内容（２）

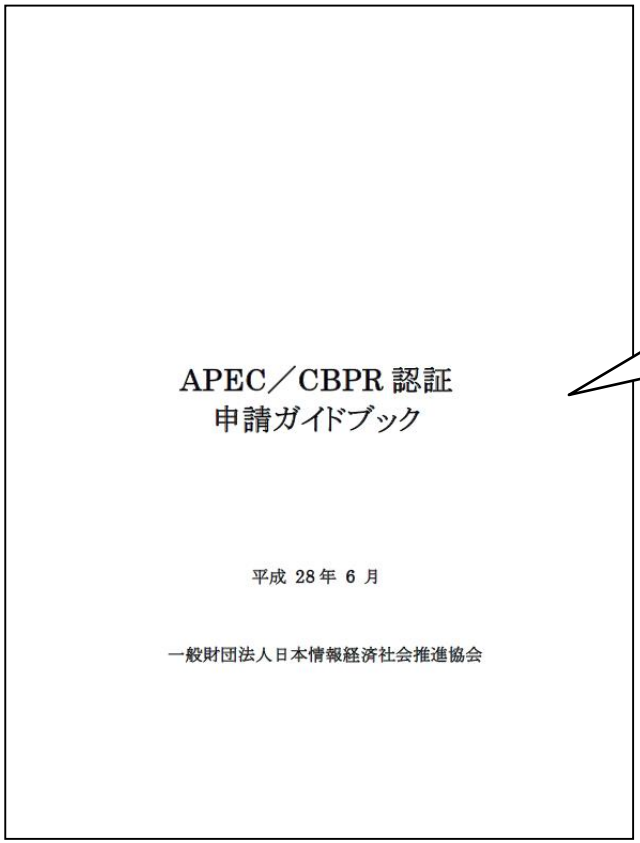
項目	記載内容
基本情報	・組織名称、対象となる組織が管理する組織の一覧、連絡窓口 ・対象となる個人情報の種類（顧客・見込み客、従業員・採用予定者、その他） ・個人情報を取得するエコノミー（APECに参加する国と地域） ・個人情報を移転するエコノミー（同上）

項目	確認する内容
通知	APEC原則（以下、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貴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	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。

相談窓口

■ **CBPRの申請をご検討中の事業者の方に、個別相談に応じています。**
お気軽に御連絡下さい。

- JIPDEC　認定個人情報保護団体事務局
  - E-mail　nintei-inq@tower.jipdec.or.jp
  - Web　http://www.jipdec.or.jp/protection_org/index.html



ダウンロードして
ご利用下さい

今後の展望

- グローバルな展開を行う事業者では、CBPRやBCRなどの認証の取得ニーズが高いことから、相互認証などの検討も進むのではないか。
  - 『EU/BCRとAPEC/CBPRの相互認証は難しい』との指摘もある。
    - “前者は第三者審査を重視し、後者は自主点検の結果を審査するので性格も異なる。“（当協会ヒアリングにおける意見の例）
  - 一方で、HP、メルクが実現している例もあるため、引き続き、経済産業省（改正法施行後は個人情報保護委員会）と調整していきたい。

出典：https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-bcrcbpr-application-process/

出典：
http://www.truste.com/blog/2016/03/22/merck-successfully-concludes-first-apec-based-bcr-approval/

申請お待ちしております。
ありがとうございました。