APEC　CBPR 認証
申請ガイドブック

第 2.3 版

2022 年 8 月

JIPDEC（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

目次

1 はじめに

ビジネスのグローバル化に伴い、個人情報が頻繁に国境を越えて移転する状況になり、越境する個人情報の保護が重要な課題となっています。APEC（アジア太平洋経済協力;Asia-Pacific Economic Cooperation）では、2004 年に APEC プライバシー原則を定め、これに基づく国内個人情報保護制度の策定をこれまで APEC 参エコノミー（国や地域）に勧奨してきました。APEC プライバシーフレームワークに基づき、各国における個人情報保護制度の策定することが各エコノミーに勧奨されました。

また、APEC では個人情報が国境を越えて移転される際に APEC プライバシー原則に基づき保護されるように、APEC 電子商取引運営グループ（ECSG：Electronic Commerce Steering Group）において、APEC 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）が構築されました。

本書は、CBPR 認証申請を検討している事業者を対象に、CBPR 認証申請時に提出すべき資料や質問書等の提出方法を解説しています。本書が、CBPR 認証申請を検討している事業者にとって、申請方法などにおいて正しい理解の一助になることを期待しています。

2 APEC CBPR 認証の概要

APEC CBPR は、越境する個人情報の保護に関する事業者の取組みが APEC プライバシー原則への適合性を認証するものです。申請する事業者は、自社の越境する個人情報の保護に関するルールの整備状況や運用状況、また推進体制等について自己評価を行います。その内容について独立した第三者の認証機関（AA、Accountability Agent）から認証審査を受け、APEC プライバシー原則を遵守していると認められた場合に CBPR 認証が付与されます。日本では、JIPDEC が AA として認定され、2016 年 6 月より CBPR 認証審査の受付を開始しました。

CBPR 認証は、APEC の参加エコノミーから個人情報を越境移転する際に、事業者が APEC プライバシー原則の要求事項を遵守して、プライバシーポリシー等を策定し、日々の実務が実施されているかを認証するものです。各エコノミーの関連法令の遵守を認証するものではありませんが、審査において関連法令等の遵守についても確認を行います。

APEC CBPR は、APEC エコノミー間で越境移転する個人情報の保護のために、事業者が利用できるシンプルかつ透明性のあるシステムの運営示すものです。この認証を取得することによって、事業者は、対外的に以下の点を訴求することができます。

（1） 越境する個人情報を取り扱う際に、取引先などに対して APEC のプライバシー原則に合致した適切なポリシーと手順を備えていること

（2） 消費者に対して越境する個人情報を適切に保護する仕組みを有していること

3 CBPR 認証審査の概要

3.1 CBPR 認証審査の特徴

申請を希望する事業者は、越境する個人情報の保護に関する取り組みについて事前に整備状況と運用状況を自己評価していただきます。審査ではその資料を元に、APEC プライバシーフレームワークに対する準拠状況、維持するための体制に関する適合性・取り組みの妥当性を確認します。具体的には、自己評価の結果を「事前質問書」と「追加質問書」にて自己評価の結果を提示し、根拠文書でそれを説明することが必要になります。

「事前質問書」と「追加質問書」の記載にあたっては、取り組み状況を記載するだけではなく、「なぜそのような取り組みを行っているのか？」、「なぜその取り組みが越境する個人情報の保護に対して妥当と言えるのか？」といった点を明らかにする必要があります。

また審査では、個々の管理策の実施の有無だけではなく、以下の観点より個人情報保護に関するリスクに対して適切な対応を行っているかを確認します。

・取り扱う個人情報を漏れなく認識しているか。
・個人情報の取り扱い状況を認識しているか。
・規定した社内ルールを適切に整備し、日常業務にて十分な運用が行われているか。
・取り扱う個人情報に関するリスクを具体的に認識しているか。
・リスクに対して妥当な対応を行い、妥当であることを説明できているか。

なお、個人情報は広い意味での「個人識別可能情報」で、個人を識別もしくは識別し得る全ての情報とされています。個人情報保護法の個人情報だけではありません。

3.2 CBPR 認証審査で確認すること

申請する事業者が自己評価した内容が適切であるかを、提出された資料をもとに審査員が CBPR 審査を実施します。具体的には、事前質問書（様式 1-2）、追加質問書（様式 1-3）に記載されている回答内容が認証基準に適合していること、回答内容が事業者において適切であるかを、その確証となる根拠文書等を評価します。不足がある場合には、資料提出や改善活動を依頼することになります。

また、その確認にあたっては、以下を実施します。

1. 文書審査
   - 質問書等にて APEC プライバシー原則の遵守状況を確認
   - 根拠文書にて、APEC プライバシー原則に対応のための規程を整備しているかを確認
   - 関連業務において規程等が確実に運用されているかを確認

2. 現地審査

・必要に応じて、上記1を補完するため実際の現場での対応状況を確認

3.3 認証申請書（様式 1-1）

認証申請書では、下記内容を記載し CBPR 認証を受審することを申請します。

・事業者名（和文、英文）
・法人番号
・所在地
・代表者の役職と氏名
・申請担当者の役職と氏名、連絡先
・会社概要（資本金、総売上高、事業の概要、ホームページ URL）
・認定個人情報保護団体に関する同意状況など

なお、申請の際には、「CBPR 認証審査に関する約款」を確認しご承諾頂きます。

3.4 事前質問書（様式 1-2）

事前質問書は、基本情報と 50 の質問項目によって構成されます。記載する内容について、下表に示します。

項目	記載する内容
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・見込客、従業員・採用予定者他）[1] ・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） ・個人情報を移転するエコノミー毎の情報の種類と移転の根拠（一覧表）

基本情報には、対象となる基本情報の対象が誰なのか？どのように取得、処理、移転、保存、破棄されるのか？どの時点でどのように何の目的で越境するのか？等が説明される必要があります。また、関係者とデータの流れについてフロー図などを使ってわかりやすく整理してください。

個人情報を移転するエコノミー毎に、どのような情報を移転するか？どのような根拠で個人情報を移転するか？等を整理してください。

初回審査以外では、前回審査時から.越境個人情報を扱う業務内容の変更の有無を記載し、変更がある場合は変更点を明確にし、業務と個人情報の流れが分かるように記載してください。

[1] 事前質問書の枠内で不足する場合は、「別紙参照」として添付してください。

■APEC プライバシーフレームワーク原則と APEC CBPR 質問表

原則	APEC CBPR 質問表	確認する内容
通知	1～4	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	5～7	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	8～13	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	14～20	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	21～25	記録について正確性及び完全性を維持させ、並びに最新な状態に維持しているか。
セキュリティ対策	26～35	個人がその個人情報を組織に預ける際に、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	36～38	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。
責任	39～50	APEC 原則の実施方法を遵守することについて確実に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。

3.5 追加質問書（様式 1-3）

当協会では、CBPR 認証審査を実施する際の評価基準として独自の「認証基準」を設定しています。これは、APEC CPBR の事前質問表で確認すべき要求事項を補完する位置付けとしています。事業者は認証基準にも適合しているかを事前に自己評価し、事前質問表と合わせて追加質問書（様式 1-3）にも回答が必要となります。

■認証基準
https://www.jipdec.or.jp/project/cbpr/JIPDEC_AOP_CBPR_005.pdf

3.6 根拠文書

申請事業者は、「事前質問書」と「追加質問」に回答すると共に、その根拠となる文書を提出します。審査では、それぞれの質問表に回答された状況について、「根拠文書」に基づいて適切であるかを確認します。

以下では、文書に記載が求められるポイント、申請する事業者が事前に用意することが必要となる文書の例について記載しています。

3.6.1 根拠文書等に記載が求められるポイント

APEC　CBPR 認証は、国内法を遵守することを認証するものではありませんが、この審査において、日本の個人情報保護法の遵守状況についても確認します。CBPR システムは、CPEA（越境プライバシー執行協力：Cross Border Privacy Enforcement Arrangement）に参加しているエコノミーであることから、CBPR 認証を受ける事業者は、関連法令を遵守していなければならないという前提により確認が必要となっています。

APEC CBPR の要求事項に関連した「事前質問書」と「追加質問表」に基づき、確証となる「根拠文書」を提出いただきます。申請する事業者が提出する文書について下表に示します。

対外的に示す文書（プライバシーポリシーなど外部に示す文書）は和文と英文の両者の提出が必要となります。社内文書（マニュアルなど）は和文のみの提出で構いません。また提出される文書には、対外的な公表を行っているウェブサイト等も含みます。

また機微情報や秘密情報が記載されているため、根拠文書が提出困難な場合には、事前送付とはせず、現地審査などで内容確認することも可能です。

3.6.2 根拠文書の例

■規程類

No	提出が求められる文書例
1	プライバシーポリシー（プライバシーステイトメント、個人情報保護方針など）
2	個人情報を特定する手順に関する規程
3	法令、国が定める指針その他の規範の特定、参照及び維持に関する規程
4	個人情報に関するリスクの認識、分析及び対策の手順に関する規程
5	事業者の各部門における個人情報を保護するための権限及び責任の規程
6	緊急事態（個人情報を漏えい、滅失またはき損など）への対応に関する規程
7	個人情報の取得、利用及び提供に関する規程
8	個人情報の適正管理に関する規規程（委託先に関する規程、従業者管理に関する規程、安全管理に関する規程など）
9	本人からの開示等の求めへの対応に関する規程
10	教育に関する規程
11	内部規程の文書管理に関する規程
12	苦情及び相談への対応に関する規程
13	点検や内部監査に関する規程
14	是正処置及び予防処置に関する規程
15	代表者等による見直しに関する規程
16	内部規程の違反に関する罰則規程

■関連文書

No	提出が求められる文書例
17	参照すべき法令、国が定める指針その他の規範の一覧
18	組織図、CBPR 体制
19	システム構成（システム構成図やネットワーク図などシステム仕様の文書）
20	セキュリティポリシー（情報セキュリティ基本方針等）
21	リスク分析及びリスクに対して講ずべき対策の一覧
22	個人情報取得時に本人に通知している文書
23	個人情報を特定し管理する台帳
24	委託先及び提供先の一覧
25	委託先及び提供先を評価選定した記録
26	委託先及び提供先との契約書
27	教育を実施した記録及び教育テキスト
28	監査を実施した記録及び監査チェックリスト

4 CBPR 認証の申請

4.1 CBPR 認証審査の手続き

CBPR 認証審査は、以下の審査手続きにより実施されます。

	手続き	内容
1	申請書類の提出	申請事業者は、「CBPR 認証審査に関する約款」を了承の上、必要な申請書類を提出する。 ■CBPR 認証審査に関する約款 https://www.jipdec.or.jp/project/cbpr/JIPDEC_AOP_CBPR_006.pdf 注）審査手順や審査中止する場合等について
2	事前確認	当協会は、受領した申請書類に基づいて、申請資格を有することを確認する。また受領した資料や越境する個人情報に関する業務について確認（ヒアリング）を行い、その内容に基づいて審査料を見積る。
3	審査料の納付	当協会は、審査料の請求を行う。申請事業者は、見積りを確認し、審査料を納付する。
4	審査	当協会は、文書審査と現地審査を実施する。 1．文書審査：提出された質問表や確証を確認する。 2．現地審査：質問書に回答された運用状況や運営体制などについて現地にて確認する。 ※なお、当協会は、審査において認証基準を満たさないと評価された場合には指摘を行います。申請者事業者が指摘箇所を改善した後に審査を再開する。
5	認証決定の通知	当協会は、審査プロセスを評価した後、その結果により認証の可否を決定する。また認証管理料を請求する。
6	認証管理料の納付、契約締結	申請事業者は認証管理料を納付する。また、申請事業者と当協会間で CBPR 認証に関する契約書（期間は 1 年間）を締結する。
7	公表と通知	当協会は、CBPR 認証事業者であることをホームページで公表し、合わせて APEC 事務局へ通知する。

4.2 申請資格

CBPR 認証審査へ申請するためには、当協会の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必要です。これは、CBPR 認証の審査等を行うアカウンタビリティ・エージェントに係る業務が、個人情報保護法第 47 条第 1 項第 3 号業務として整理されており、認定個人情報保護団体として実施することが要件となっているためです[2]。

当協会以外の認定個人情報保護団体の対象事業者である方は、追加で当協会の認定個人情報保護団体の対象事業者となる必要があります。

なお、当協会が認める認証制度の付与事業者でなくなった場合は、対象事業者として登録を継続することができません。

当協会の認定個人情報保護団体の「対象事業者」となるための手続き、認証制度の付与事業者でなくなった場合の留意事項等は、以下のページを参照してください。

- 「対象事業者になるための申請・変更手続き」ページ
  https://www.jipdec.or.jp/project/protection_org/application.html
- 「認定個人情報保護団体」ページの「対象事業者一覧」
  https://www.jipdec.or.jp/project/protection_org.html

[2] 個人情報保護委員会事務局 Web サイト「APEC CBPR のアカウンタビリティ・エージェントに係る業務について」ページ（ https://www.ppc.go.jp/personalinfo/nintei/procedure/ ）参照

4.3 CBPR 認証の申請書類の提出方法

CBPR 認証の申請時には、以下の資料を提出して頂きます。

（1）認証申請書（様式 1-1）
（2）事前質問書（様式 1-2）
（3）追加質問書（様式 1-3）
（4）根拠文書 … 質問書の回答内容の根拠となる確証等
（5）過去6ケ月の事故等一覧（様式 1-4）
（過去 6 ケ月の間に、個人情報保護委員会/総務省または認定個人情報保護団体等へ報告した事故等。）

正式な資料は電子ファイルとしています。電子ファイルの送付方法は、当協会が利用しているファイル共有サービスや、事前に規定したパスワードつき添付ファイルのメール送付を想定しています。事前に提出先の担当者と申請前に整合させて頂きます。

■提出先

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 CBPR 認証業務グループ
E-mail： cbpr-office @ tower.jipdec.or.jp
※メールアドレスの@の前後の空白を削除してください。

4.4 CBPR 認証取得事業者が再び申請する方法

CBPR 認証取得事業者が再申請する場合には、認証期間の満了日の4ケ月前の日までに、申請書その他必要な書類を提出していただきます。CBPR 認証の再申請にかかる手続は、当協会の定める約款などに従うものといたします。

5 CBPR 認証申請の相談窓口

当協会では、CBPR 認証の申請を検討されている事業者からのご相談に個別にご対応いたします。以下までお気軽にお問合せください。

JIPDEC 認定個人情報保護団体事務局 CBPR 認証業務グループ
E-mail： cbpr-office @ tower.jipdec.or.jp
※メールアドレスの@の前後の空白を削除してください。
URL： https://contact.jipdec.or.jp/m?f=878

6 付録

6.1 審査項目のポイント

以下に、「事前質問表」と「追加質問表」の関係を記載します。

6.1.1 通知(質問1から4)

通知では、個人情報保護方針について本人の理解を確実にするための手順や仕組みがAPEC プライバシー原則に従って実施されるかを確認します。具体的には、①取得される個人情報、移転先、及び利用目的に関するポリシーについて本人にしっかり理解してもらう仕組みが運用されているか、②本人の個人情報が取得されるタイミング、移転先、及び利用目的について本人にしっかりと通知する仕組みが運用されているかを確認します。

なお、通知には適用除外条件(「通知に関する規定の制限条件」)がありますが、これは、APECプライバシー原則に対する適用除外事項を記述しています。国内法との関係においては、必ずしも適用を除外することができない項目も含まれますので、ご注意ください。以下、選択(質問14から20)、アクセスおよび訂正(質問36から38)も同様です。

事前質問表	追加質問表
1.上記の個人情報に適用されるポリシー等を記載した「個人情報に適用される方針やルール(契約書や約款等)に関して明瞭かつ入手しやすい説明書」(以下、「プライバシーステイトメント」という)を提供していますか?「はい」の場合、該当する文書のコピーまたは当該文書へのハイパーリンクを提出してください。 a)このプライバシーステイトメントには、貴社がどのように個人情報を取得するのかが説明されていますか? b)このプライバシーステイトメントには、個人情報が取得される目的が説明されていますか? c)このプライバシーステイトメントでは、個人情報を	**■左記に関して、具体的に説明されていることを確認します。プライバシーポリシーは以下を満たしている必要があります。** *<認証基準:2.1 プライバシーポリシー>* *申請する事業者のプライバシーポリシーは、以下の事項をすべて満たしていること。* *1.個人情報保護の理念を明確にしていること、及びその内容が適切であること。* *2.従業者及び一般の人が容易に入手可能であること。申請する事業者のウェブサイト等に掲載されていること。* *3.APEC プライバシーフレームワークに適合した記述がされていること。* *4.オンライン、オフラインでの取得を問わず、すべての個人情報に適用されていること。* *5.制定年月日(及び最終改訂年月日)を明示していること* *6.公開している個人情報保護方針と規定文書の個人情報保護方針に差異がないこと* *7.個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守することについて記述していること、及びその内容が適切であること。* *8.代表者の氏名を表示していること、及びその内容が適切であること。* *9.個人情報保護方針に関する問合せ先を明示していること* *10.事業の内容及び規模を考慮した適切な個人情報の取得、利用及び*

	第三者が利用できるようにするかどうかについて、またその場合の目的について本人に通知していますか	*提供に関すること(特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い(以下「目的外利用」という。)を行わないこと及びそのための措置を講じることを含む)について記述していること、及びその内容が適切であること。* *11.プライバシーポリシーが、以下の事項を含むこと* *・取得する個人情報の種類* *・個人情報が直接、または第三者または代理人が取得するかの別* *・個人情報の利用目的* *12.個人情報にアクセスまたは訂正するための方法が記載されていること* *13.苦情及び相談への対応に関することについて記述していること、及びその内容が適切であること。* *14.個人情報の漏えい、滅失またはき損の防止及び是正に関することについて記述していること、及びその内容が適切であること。* *15.個人情報保護マネジメントシステムの継続的改善に関することについて記述していること、及びその内容が適切であること。*
	d)このプライバシーステイトメントでは、貴社の名称と所在地(取得した個人情報の取扱いと慣行に関する貴社の連絡窓口情報を含む)について開示していますか？	
	e)このプライバシーステイトメントでは、個人情報の利用と開示に関する情報を本人に提供していますか？	
	f)このプライバシーステイトメントでは、自分の個人情報にアクセスし修正することができますか、また、その方法に関する情報を本人に提供していますか？	
2.個人情報の取得時(直接であるか第三者の代行によるかを問わない)に、そのような情報を取得している旨を通知していますか？		**■左記に関して、具体的に説明されていることを確認します。通知の内容等は以下を満たしている必要があります。** *＜認証基準:3.1a 本人から個人情報を直接書面によって取得する場合＞* *申請する事業者は、本人から直接書面で個人情報を取得する場合、あらかじめ書面で明示のうえ、本人の同意を得ていること。* *1.直接書面により、新規の種類の個人情報を取得する場合、その承認手順を定め、その手順に従い、管理者の承認を得ていること。* *2.本人に対し、取得する手段ごとに手順を定め、以下の a)～h)の必要事項を書面により明示して同意を得るように規定し、その規定に従って運用していること。*
3.個人情報の取得時(直接であるか第三者の代行によるかを問わない)に、個人情報を取得する目的を明らかにしていますか？		
4.個人情報の取得時に、個人情報を第三者に提供する場合があることを本人に通知していますす		

か？	*a)事業者の氏名または名称* *b)個人情報保護管理者（もしくはその代理人）の氏名または職名、所属及び連絡先* *c)利用目的* *d)個人情報を第三者に提供することが予定される場合の事項* *-第三者に提供する目的* *-提供する個人情報の項目* *-提供の手段または方法* *-当該情報の提供を受ける者または提供を受ける者の組織の種類、及び属性* *-個人情報の取扱いに関する契約がある場合はその旨* *e)個人情報の取扱いの委託を行うことが予想される場合には、その旨* *f)開示対象個人情報に係る利用目的の通知、開示、訂正・追加または削除、利用または提供の拒否権に関する場合には、その求めに応じる旨及び問合わせ窓口* *g)本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果* *h)本人が容易に認識できない方法によって個人情報を取得する場合には、その旨* *3.直接書面による取得において、本人の同意を不要とするのは、「個人情報を直接書面以外で取得する場合」の a)から d)、及び「利用に関する措置」の a)から d)のいずれかに該当する場合のみに限定していること。* *4.「個人情報を直接書面以外で取得する場合」の a)から d)、及び「利用に関する措置」の a)から d)を適用する場合の承認手順を定め、その規定に従って管理者の承認を得て運用していること。* *＜認証基準:3.1b 個人情報を直接書面以外で取得する場合＞* *申請する事業者は、直接書面以外の方法で個人情報を取得する場合、あらかじめその利用目的を公表している場合を除き、速やかにその利用目的を、本人に通知するか公表していること。* *1.直接書面以外の方法により、新規の種類の個人情報を取得する場合、その承認手順を定め、その手順に従い、管理者の承認を得ていること。* *2.個人情報を直接書面以外の方法によって取得する場合に、あらかじめその利用目的を公表する手順を規定していること。または取得後に、速やかにその利用目的を本人に通知し、または公表する手順を規定し、い*

	ずれもその規定に従って運用していること。 *3.本人に通知または公表しないのは、以下の a)～d)の場合のみに限定し、その通り運用していること。* *a)利用目的を本人に通知し、または公表することによって本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合。* *b)利用目的を本人に通知し、または公表することによって当該事業者の権利または正当な利益を害するおそれがある場合。* *c)国の機関または地方公共団体が法令の定める事務を遂行することに対して協力する場合であって、利用目的を本人に通知し、または公表することによって当該事務の遂行に支障を及ぼすおそれがある場合。* *d)取得の状況からみて利用目的が明らかであると認められる場合* *4.上記 a)～d)を適用する場合の承認手順を規定し、その規定に従って運用していること。* *5.上記 d)に該当する場合、適用を限定するよう規定し、その規定に従って運用していること。*

6.1.2 取得の制限（質問5から7）

取得の制限では、①合法かつ公正なものである点、②情報取得は必ず取得時に明記した具体的な目的に限定したものとしている点、③情報取得は当該目的に関連したもので、且つ当該目的の遂行に応じたものである点を審査します。

事前質問表		追加質問表
5.個人情報はどのように入手していますか？	a)当人から直接。「はい」の場合、具体的に説明してください。 b)第三者が代行による。「はい」の場合、具体的に説明してください。 c)その他。「はい」の場合、具体的に説明してください。	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:1.2 個人情報の特定＞* *申請する事業者は、自らの事業の用に供する個人情報及び取得方法を特定するための手順を確立し、かつ、維持していること。* *1.各個人情報を特定する手順が明確であること。* *2.手順に従い、個人情報を特定し、管理者の承認を得ていること。* *3.個人情報を取得する方法を明らかにしておくこと* *4.個人情報を特定した台帳等を作成していること。* *5.個人情報管理台帳等の更新及び定期的な見直しに関する手順が明確であること。* *6.手順に従い、個人情報を管理する台帳等の更新及び定期的見直しを実施していること。*
6.個人情報の取得（直接であるか		**■左記に関して、具体的に説明されていることを確認します。個人情報**

第三者の代行によるかを問わない)は、取得目的、又は取得目的に関連する他の目的の達成に関する個人情報に限定されていますか？	**の取得は以下を満たしている必要があります。** *＜認証基準:1.3　利用目的の特定＞* *申請する事業者は、個人情報を取得するに当たって、その利用目的をできる限り特定し、その目的の範囲内で利用すること。* *1.個人情報の取得に当たっては、利用目的をできる限り特定しその目的達成に必要な限度において行わなければならない旨を規定し、その規定に従って運用していること。* *2.利用目的の特定に関する手順を定め、利用目的を特定にあたっては管理者の承認を得ていること。* *3.事業者内で個人情報を取り扱う従業者は、その利用目的を明確に認識していること。*
7.個人情報の取得に適用される管轄権の要件に合わせて、適法かつ公正な手段で個人情報を取得していますか？(直接であるか第三者の代行によるかを問わない)？	**■左記に関して、具体的に説明されていることを確認します。個人情報の取得は以下を満たしている必要があります。** *＜認証基準:3.1　適正な取得＞* *申請する事業者は、適法、かつ、公正な手段によって個人情報を取得すること。* *1.個人情報の取得は、適法、かつ、公正な手段により行わなければならない旨を規定し、その規程に従って運用していること。* *2.受託を含め、本人以外から個人情報を取得する場合、提供元または委託元が個人情報を適正に取り扱っていることを確認するよう規定し、その手順に従い提供元または委託元の個人情報の取扱いについて確認していること。* *＜認証基準:3.1c　要配慮個人情報の取得＞* *申請する事業者は、要配慮個人情報を取得する場合，あらかじめ書面による本人の同意を得ること。* *要配慮個人情報を取得する際，書面による本人の同意を得ることを要しないときは，以下の場合に限定していること。* *a) 法令に基づく場合* *b) 人の生命，身体または財産の保護のために必要がある場合であって，本人の同意を得ることが困難であるとき* *c) 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって，本人の同意を得ることが困難であるとき*

	d) 国の機関若しくは地方公共団体またはその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって，本人の同意を得ることによって当該事務の遂行に支障を及ぼすおそれがあるとき *e) その他，個人情報取扱事業者の義務などの適用除外とされている者及び個人情報保護委員会規則で定めた者によって公開された要配慮個人情報，または政令で定められた要配慮個人情報であるとき*

6.1.3 個人情報の利用（質問8から13）

個人情報の利用では、個人情報は具体的な取得目的に限定して利用する点について審査します。

APEC 取得の原則に従って個人情報を利用する例として、効果的かつ効率的に人材管理を行うための管理台帳、第三者による従業員の給与処理などが考えられます。

事前質問表	追加質問表
8.プライバシーステイトメントまたは取得時に出した通知に特定した通り取得する（直接であれ第三者の代行であれ）個人情報の利用は、当該情報の取得目的またはその他の矛盾のない関連する目的に限定されていますか？	**■左記に関して、具体的に説明されていることを確認します。個人情報の利用は以下を満たしている必要があります。** *＜認証基準:4.1 利用に関する措置＞* *申請する事業者は、特定した利用目的の達成の範囲内で個人情報を利用すること。* *特定した利用目的以外の目的で利用する場合、本人から直接書面で個人情報を取得するときと同等以上の内容を本人に通知し、本人の同意を得ること。*
9.質問 8 の回答が「いいえ」の場合、以下のいずれかの状況において、関連のない目的で集めた個人情報を利用していますか？下欄に説明してください。	*1.特定した利用目的の達成に必要な範囲内で個人情報を利用しなければならない旨を明確に規定し、その規定に従って運用していること。* *2.利用目的を変更する場合の承認手順を規定し、その規定に従って運用していること。* *3.利用目的を変更する場合、「本人から個人情報を直接書面によって取得する場合」の a)～f)に示す事項またはそれと同等以上の内容の事項を本人に通知して同意を得る手順を規定し、その規定に従って運用していること。* *4.目的外利用で本人の同意を必要としないのは、以下 a)～d)の場合のみに限定して規定し、その通り運用していること。* *a)法令に基づく場合* *b)人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき*

	c)公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき *d)国の機関または地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることによって当該業務の遂行に支障を及ぼすおそれがあるとき* *5.上記の a)～d)を適用する場合の承認手順を規定し、その規定に従って運用していること。* *6.目的外利用に該当するかどうか判断に迷う場合、管理者の判断を求めるよう規定し、その規定に従って運用していること。* *＜認証基準:4.1a　本人にアクセスする場合の措置＞* *申請する事業者は、個人情報を利用して本人にアクセスする場合には、本人に対して直接書面で個人情報を取得するときと同等以上の内容及び取得方法を通知し、本人に同意を得ること。* *1.本人にアクセスすることについての承認手順を規定し、その規定に従って運用していること。* *2.本人に対し、「本人から個人情報を直接書面によって取得する場合」の a)～f)に示す事項またはそれと同等以上の内容の事項，及び取得方法を通知し、本人の同意を得る手順を規定し、その規定に従って運用していること。* *3.本人に通知する書面が、「本人から個人情報を直接書面によって取得する場合」の a)～f)に示す事項またはそれと同等以上の内容の事項及び取得方法を満たしていること。* *4.本人の同意を必要としないのは、以下の a)～e)の場合のみであるように規定し、その規定に従って運用していること。* *a)個人情報の取扱いの全部または一部を委託された場合であって、当該個人情報を、その利用目的の達成に必要な範囲内で取り扱うとき* *b)合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する事業者が、既に本人から直接書面で個人情報を取得するときの a)～f)に示す事項またはそれと同等以上の内容の事項を明示または通知し、本人の同意を得ている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき* *c)個人情報が特定の者との間で共同して利用され、共同利用者が、既に「本人から個人情報を直接書面によって取得する場合」の a)～f)に示す事項またはそれと同等以上の内容の事項を明示または通知し、本人の*

	同意を得ている場合であって、次に示す事項またはそれと同等以上の内容の事項を、あらかじめ、本人に通知し、または本人が容易に知り得る状態に置いているとき *-共同して利用すること* *-共同して利用される個人情報の項目* *-共同して利用する者の範囲* *-共同して利用する者の利用目的* *-共同して利用する個人情報の管理について責任を有する者の氏名、名称* *-取得方法* *d)「個人情報を直接書面以外で取得する場合」d)に該当するため、利用目的などを本人に明示、通知または公表することなく取得した個人情報を利用して、本人にアクセスするとき* *e)「利用に関する措置」の a)～d)のいずれかに該当する場合* *5.上記の a)～e)を適用する場合の承認手順を規定し、その規定に従って運用していること。* *6.上記の d)を適用する場合、その手順を規定し、その規定に従って運用していること。*
10.（直接であれ第三者の代行であれ）取得する個人情報を他の個人情報取得者に開示していますか？ 11.個人情報を個人情報処理業者に転送していますか？ 12.質問 10 または 11 への回答が「はい」の場合、その開示または転送は、取得目的またはその他の矛盾のない関連した目的を果たすために行われたものですか？ 13.質問 12 の回答が「いいえ」の場合、または適切な場合は、その開示や転送は以下の状況のいずれかにおいて行われていますか？	**■左記に関して、具体的に説明されていることを確認します。個人情報の開示等は以下を満たしている必要があります。** *＜認証基準:4.2 提供についての措置＞* *申請する事業者は、個人情報を第三者に提供する場合には、あらかじめ、本人に対して、取得方法及び「本人から個人情報を直接書面によって取得する場合」の a)～d)と同等以上の内容を通知し、本人の同意を得ること。* *1.第三者に提供する場合、承認手順を規定し、その規定に従って運用していること。* *2.第三者に提供する場合、あらかじめ本人に対し、取得方法及び「本人から個人情報を直接書面によって取得する場合」の a)～d)の事項またはそれと同等以上の内容の事項を通知し本人の同意を得る手順を規定し、その規定に従って運用していること。* *3.特定した利用目的の達成に必要な範囲で個人情報を提供しており、以下を明らかにしていること* *・第三者へ提供するデータの種類* *・提供されるデータの種類ごとに対応する利用目的*

	・データを提供することにより利用目的がどのように達成されるのか *4.本人の同意を必要としないのは、法令に基づく場合に限定されていること* *＜認証基準:8.5 個人情報の提供の手続き＞* *申請する事業者は、法令に基づき個人情報の提供を行う場合の手順をあらかじめ定めていること。*

6.1.4 選択（質問14から20）

個人情報の取得、利用、開示に関連して本人に選択権を必ず与えていることを審査します。APEC 原則では、明らかに同意が示唆されている場合や、選択権を行使できる仕組みを提供する必要がない場合があることを「選択に関する規定の制限条件」として想定しています。これに該当する場合には、申請者は根拠を示す必要があります。

事前質問表	追加質問表
14.個人情報の取得に関連して本人が選択できる方法を提供していますか？	**■左記に関して、具体的に説明されていることを確認します。本人が選択できる方法は以下を満たしている必要があります。** *＜認証基準:5.1 本人の選択肢＞* *申請する事業者は、個人情報の取得、利用、提供に関連して、本人に必ず選択肢を与えていること。* *1.申請する事業者は、取得、利用、提供の各局面において、個人に選択権を与えていること* *2.個人が，個人情報の取得時に選択権を行使することができること* *3.本人が選択権を行使する仕組みが整備され使用可能であること* *4.選択権を行使する仕組みを明瞭かつ気が付きやすい方法で提供していること* *5.選択権を行使する仕組みを明瞭かつ理解しやすい言葉遣いで表現していること* *6.選択権を行使する仕組みは本人が容易に行うことができる方法であること* *7.選択権を行使する仕組みが個人の求めに対し，迅速に対応していること。*
15.個人情報の利用に関連して本人が選択できる方法を提供していますか？	
16.個人情報の開示に関連して個人が選択できる方法を提供していますか？	
17.個人情報の取得（質問 14）、利用（質問15）、開示（質問16）を制限する権限を与える選択肢を個人に提供している場合、それは明瞭かつはっきりとした形で表示または提供されていますか？	
18.個人情報の取得（質問 14）、利用（質問15）、開示（質問16）を制限する権限を与える選択肢を個人に提供している場合、それは明瞭な表現ですぐ分かるようになっていますか？	
19.個人情報の取得（質問 14）、	

利用(質問15)、開示(質問16)を制限する権限を与える選択肢を個人に提供している場合、その選択は簡単に利用でき手頃なものですか？	
20.必要に応じて、効果的かつ迅速に希望が通るようにするどのような方法が用意されていますか？下欄または必要に応じて添付資料として説明を添えてください。	

6.1.5 個人情報の完全性(質問21から25)

個人情報の完全性では、個人情報管理者[3]が記録を正確、完全かつ最新に保管していることを審査します。

事前質問表	追加質問表
21.保管している個人情報が、利用目的に必要な限りにおいて、最新、正確、必要最低限なものであることを検証する措置を講じていますか？	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:5.2 正確性の確保＞* *申請する事業者は、利用目的の範囲内において、個人情報を正確かつ最新の状態で管理すること。*
22.利用目的上必要な限りにおいて、不正確、不十分で、古くなった個人情報を修正する方法を用意していますか？	*1. 個人情報の入力時の照合・確認の手続の整備* *(1)個人情報を入力する際の作業責任者を明確化していること* *(2)入力した個人情報の照合及び確認の手順を明確化していること* *(3)定めた手順により照合及び確認作業を実施していること*
23.不正確、不完全、または古くなった情報が利用目的に影響すると思われ、当該情報の転送後に修正がなされた場合、その修正について、当該個人情報の転送先である処理業者等に連絡をしていますか？	*2. 訂正の手続の整備* *(1)個人情報を訂正する際の作業責任者を明確化していること* *(2)個人情報の誤りや不整合を発見する手順を明確化していること* *(3)訂正した個人情報の照合及び確認の手順を明確化していること* *(4)定めた手順により訂正作業を実施していること*
24.不正確、不完全、または古くなった情報が使用目的に影響す	*3. 個人情報が正確かつ最新であることを検証する手順の整備* *(1)個人情報が正確かつ最新であることを検証する作業責任者を明確化していること*

[3] 個人情報の収集、保管、処理及び利用を行う個人又は組織のことです。ここでは、申請事業者のことを指しています。

ると思われ、情報の開示後に修正が行われた場合、その修正について個人情報の転送先であるその他の第三者に伝えていますか？	*(2)個人情報が正確かつ最新であることを検証し、必要に応じて訂正する手順を明確化していること* *(3)定めた手順により作業を実施していること* *4. 記録事項の更新* *(1)作業実施記録を維持する責任者を明確化していること*
25.不正確、不完全、または古くなった情報に気づいた場合は連絡をするよう、委託や共同利用等を行う事業者に求めていますか？	*(2)作業実施記録を更新する手順を明確化していること* *(3)作業記録を保管する手順を明確化していること* *(4)定めた手順により記録事項の更新を実施していること* *5. 保存期間の設定* *(1)保存期間を設定する責任者を明確化していること* *(2)保存期間を設定する基準を明確化していること* *(3)定めた手順により保存期間を設定していること* *6. 委託先への訂正等の連絡* *(1)委託先へ個人情報の訂正等について連絡をしていること* *7. 委託先における訂正等手続きの整備* *(1)委託先に個人情報の訂正等の連絡を行った際に、委託先が訂正等を行うための手順を確認していること* *8. 委託先への確認手続きの整備* *(1)個人情報を取り扱う委託先が個人情報の訂正等に気が付いた際は、申請する事業者に連絡をすることを規定していること*

6.1.6 セキュリティ対策（質問26から35）

セキュリティ対策では、個人が自分の情報を申請事業者へ付託する場合に、事業者が事業者のリスク分析に基づき、当該情報の紛失、不正なアクセスまたは開示、その他の不正な利用から保護するための妥当な安全管理措置を必ず実施することを審査します。攻撃、侵入、その他のセキュリティ障害を検出、防止、対応するための措置により検出された脆弱性をリスク分析にフィードバックするとともに、採用した安全保護策の効果を検証することが求められます。

安全管理措置の実施は、事業者のリスク分析が基となります。リスク分析では、個人情報の取扱い状況、採用済みの安全管理措置、前述の攻撃、侵入、その他のセキュリティ障害を検出、防止、対応するための措置及びその効果を試すためのテストから得られる情報を踏まえて、事業者の置かれた状況や、取り扱う個人情報等に関する具体的なリスクを特定することが求められます。

なお、「認証基準」に安全管理措置の一覧が定められており、これはすべての事業者が最低限満たすべき措置を列挙したものです。審査において、「認証基準」の措置が講じられていることのみを確認するものではありません。

事前質問表	追加質問表
26.情報セキュリティ方針を実装し	**■左記に関して、具体的に説明されていることを確認します。説明では**

ていますか？	**以下を満たしていることを証明する必要があります。** *＜認証基準:1.5 リスクの認識、分析、対策＞* *申請する事業者は、個人情報の取扱いについて、個人情報保護リスクを特定し、分析し、必要な対策を講じる手段を確立し維持していること。* *1.個人情報保護リスクを特定し、分析し、必要な手順を確立し，かつ，維持するよう規定していること。* *2.個人情報保護リスクを特定し、分析し、リスクに応じた対策を講じられていること。* *3.リスク対策は事業者の代表者の承認を得て決定していること。* *4.講じることとした対策は、規定に反映させていること。* *5.定期的な見直し、及び必要に応じた随時の見直しの手順が明確であり、その手順に従い、リスクの見直しを実施していること。* *＜認証基準:1.7 緊急事態＞* *申請する事業者は、緊急事態を特定する手順及びその対応の手順を確立、実施、維持すること。* *その手順は、個人情報が漏えい、滅失またはき損した場合に想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とするものとしていること。* *1.緊急事態を特定するための手順、それらにどのように対応するかの手順を定め、その手順に従って実施していること。* *2.個人情報が漏えい、滅失またはき損をした場合に想定される経済的な不利益及び社会的な信用の失墜，本人への影響などのおそれを考慮し、その影響を最小限とするための手順を定めており、その手順に従った措置を実施していること。* *3.漏えい，滅失またはき損が発生した個人情報の内容を本人に速やかに通知し，または本人が容易に知り得る状態に置く手順を定め、その手順に従った措置を実施していること。* *4.二次被害の防止，類似事案の発生回避などの観点から、可能な限り事実関係，発生原因及び対応策を，遅滞なく公表する手順を定め、その手順に従った措置を実施していること。* *5.緊急事態発生の場合の事実関係、発生原因及び対応策を関係機関（報告すべき利害関係を有している機関）に直ちに報告する手順を定めていること。*
27.個人情報を、情報の紛失または不正なアクセス、破壊、利用、修正または開示またはその他の悪用のリスクから保護するために実施している、物理的、技術的、運営上の安全保護策について説明してください。	
28.質問 27 に対応して特定した安全保護策が、脅かされる危害の可能性と程度、情報の機密性、また保管状況に鑑みてなぜ適当なのか説明してください。	
29.従業員に個人情報のセキュリティの維持の重要性についてどのように認識させているか説明してください（定期的な研修や監督など）	
30.次のような手段で、迫る危害の可能性と程度、情報の機密性、保管状況に適した安全保護策を実施していますか？ a)従業員の研修や管理その他の安全保護策 b)ネットワークやソフトウェア設計、および情報処理、保存、転送、廃棄などの、情報システムや情報管理 c)攻撃、侵入、その他のセキュリティ障害の検出、防止、対応 d)物理的セキュリティ	
31.個人情報の安全な処分のための方針を実施していますか？	
32.攻撃、侵入、その他のセキュリ	

ティ障害を検出、防止、対応するための措置を実施していますか？	*＜認証基準:6.1　安全管理措置＞* *申請する事業者は、その取り扱う個人情報のリスクに応じて、漏えい、滅失またはき損の防止その他の個人情報の安全管理のために必要、かつ、適切な措置を講じること。*
33.上記質問 32 でふれた安全保護策の効果を試すためのプロセスが用意されていますか？	*＜認証基準:6.3　リスク対応及び安全管理措置の構築＞* *申請者の事業規模、事業の内容及び個人情報の種類に応じて妥当な対応を行っていること。当該対応は、個人情報の種類、機密性に応じた妥当な措置を講じなければならない。当該措置は、個人情報の機密性、危害の可能性と程度、個人情報の保管状況に適したものでなければならない* *1.申請者が策定し，実施している物理的、技術的、人的、組織的安全管理措置が、特定したリスクに対し，必要かつ適切であること。* *2.現状で実施し得る対策を講じたうえで、未対応部分を残留リスクとして把握し、管理していること。* *3.リスク分析及びリスク対応の実施に関する監査を定期的に実施していること。* *＜認証基準:6.5　定期的な見直し＞* *申請者は、リスクの特定及び分析、リスク評価及びリスク対応について定期的に見直し，見直しの結果に応じた修正を行っていること*
34.リスク評価または第三者認証を利用していますか？	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:6.2　個人情報に関するリスクの特定，分析及び評価＞* *申請者は、事業活動の内容と範囲、当該申請者が収集する個人情報の種類及び個人情報の保管、取り扱い状況に関連したリスクを特定，分析及び評価していること* *1.個人情報に関する取り扱い（個人情報の取得・入力，移送・送信，利用・加工，保管・バックアップ，消去・廃棄を含むがこれに限らない）に関するリスクを具体的に特定していること* *2.個人情報を保護するために採用している、組織的，人的，技術的，物理的安全管理措置を具体的に特定していること* *3.攻撃、侵入、その他のセキュリティ障害を検出、防止、対応するための*

		措置を講じ、その効果を試すためのテストを定期的に実施していること *4.安全管理措置が別紙 1 を充足していること* *5.個人情報の保護に影響を及ぼす具体的なリスクについて、分析を行っていること* *6.申請者は、リスク評価を適切に行わなければならない。申請者は，法令で別段の定めがある場合を除き、リスクを受容してはならない。*
35.個人情報の転送先である処理業者、代理人、請負業者、その他のサービス業者に、以下の手段により、当該情報の紛失、または不正なアクセス、破壊、利用、修正、または開示その他の不正な利用から保護するよう求めていますか？		**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:6.4　委託先の監督＞* *申請者は、個人情報に関するリスクの特定及び分析，リスク評価並びにリスク対応を委託先に求めていること* *1.委託先が，個人情報に関するリスクの特定及び分析，リスク評価並びにリスク対応を行うよう，必要な措置を講じていること(委託先との間の契約の締結を含む)。* *2.委託先が、個人情報またはセキュリティの侵害に気が付いた場合は、申請者に連絡することを求めていること* *3.個人情報またはセキュリティの侵害に対する修正対応を委託先に求めていること*
	a)提供された情報やサービスの機密性に対応した情報セキュリティプログラムを実施する。	
	b)申請者の顧客の個人情報のプライバシーまたはセキュリティの侵害に気づいた場合は速やかに通知する。	
	c)プライバシーの侵害または機密保持違反につながったセキュリティ障害の修正対応のための措置を速やかに講じる。	

6.1.7 アクセス及び訂正(質問36から38)

アクセス及び訂正では、本人が必ず自分の情報にアクセスし修正することができることを審査します。この項目では、①情報への直接のアクセスの提供を防ぐセキュリティ要件、②アクセスの提供前に身分の十分な証明を求めること(本人確認等)も含みます。また、情報にアクセスし修正する権限を提供する手順(情報開示等)では、情報の内容やその他の要因により異なる場合を想定し、状況に応じて、記録を変更、差し止め(非公表)、または削除することが不可能・非現実的、または不要な場合も想定し、アクセスと修正の要請を拒否する対応についても許容しています(アク

セス及び訂正に関する規定の制限条件）が、申請する事業者がその条件に相当する場合は、その旨を説明していることを審査します。アクセス要請を拒否するときは、その判断を下した理由及び拒否に異議を唱える方法について、要請した本人に説明していることが求められます。

事前質問表	追加質問表
36.要請に応じて、要請者に関する個人情報を保有しているか確認していますか？	**■左記に関して、方針と手順が具体的に説明されていることを確認します。方針と手順には以下を含む必要があります。** *＜認証基準:7.1　個人情報についての事項の公表＞* *申請する事業者は、個人情報について、当該申請者が本人から求められる開示、内容の訂正、追加または削除、利用の停止（以下、「開示等」という。）の求めに応じることができる権限を有するもの（開示等の対象個人情報という。）に関して本人の知り得る状態（本人の求めに応じて遅延なく回答する場合を含む）に置いていること。* *1.以下の a)～f)の事項について本人の知り得る状態に置く具体的な手順を規定し、その規定に従って運用していること。* *a)申請者の名称及び苦情の解決の申出先* *b)個人情報保護管理者（もしくはその代理人）の氏名又は職名、所属及び連絡先* *c)すべての越境個人情報の利用目的* *d)個人情報の取扱いに関する苦情の申し出先* *e))認定個人情報保護団体の名称及び苦情の解決の申し出先* *f)開示等の求めに応じる手続き* *＜認証基準:7.2　個人情報に関する権利＞* *申請する事業者は、開示等の対象個人情報について、当該申請者が本人から求められる開示等に関して、本人から要請を受けた場合は、遅滞なく応じること。* *1.開示等の対象個人情報について、この認証基準に沿って開示の求め等に応じる旨を規定し、その規定に従って運用していること。* *2.開示等の対象に漏れがないこと。* *3.例外事項が適用される場合の承認手順を規定し、その規定に従って運用していること。* *＜認証基準:7.3　個人情報に関する権利に対する手続＞* *申請する事業者は、開示等の対象個人情報の開示等の求めに応じる手*
37.要請があった場合、保管する個人情報の本人に当該情報へのアクセスを認めていますか？「はい」の場合、以下の質問37.a)-.e)に回答し、アクセス要請を受け取り対応するための方針と手順について説明してください。「いいえ」の場合、質問 38 に進んでください。	
a)あなたはアクセスを要請してきた人の身元を確認する措置を講じていますか？	
b)あなたは、アクセス要請があった場合、適当な期間内にアクセスを認めていますか？	
c)情報は基本的に理解しやすい妥当な方法で伝えられていますか（読みやすいフォーマットなど）？	
d)情報は、個人との通常の対話形式にあった方法で提供されていますか（電子メール、同一言語	

	など）？	*続として、以下の事項を定めていること。*
	e)アクセスの提供は有料ですか？「はい」の場合、料金設定基準とどのようにして法外ではない額に設定しているか説明してください。	*本人からの開示等の求めに応じる手続は、簡潔で使いやすく、明確で見つけやすく提示されおり、また、本人に過度な負担を課することがないよう配慮されていること* *a)開示等の求めの申し出先* *b)開示等の求めに際して提出すべき書面の様式その他の開示等の求めの方式*
38.情報の正確さについて個人が異議を唱え、それを修正、完成、改正、または削除させることを認めていますか？以下に関する申請者の方針と手順について説明し、質問 38.a)-e)に回答してください。		*c)開示等の求めをする者が、本人又は代理人であることの確認の方法* *d)開示、訂正、追加又は削除の場合の手数料の徴収方* *e)開示等の求めに応じる合理的な期間* *＜認証基準:7.4 個人情報についての利用目的の通知＞* *申請する事業者は、本人から開示等の対象個人情報について、利用目的の通知を求められた場合、遅滞なくこれに応じること。*
	a)アクセス及び修正方法は明瞭かつ明確に表現されていますか？	*1.本人から利用目的の通知を求められた場合、遅滞なくこれに応じるよう規定し、その規定に従って運用していること。* *2.本人への回答内容（求めに応じない場合を含む）に関する承認手順を定め、手順を明確に記述していること。* *＜認証基準:7.5 個人情報の開示＞* *申請する事業者は、本人から開示等の対象個人情報の開示を求められた場合、該当する法律がある場合を除き、本人に遅延なく、当該開示等の対象個人情報を書面で開示すること。* *1.本人から，当該本人が識別される開示等の対象個人情報の開示を求められた場合に、法令の規定により特別の手続が定められている場合を除き、遅滞なくこれに応じるよう規定し、その規定に従って運用していること。* *2.本人への回答内容（求めに応じない場合を含む）に関する承認手順を定め、手順を明確に記述し、その手順に従って行う本人への回答内容について管理者の承認を得ていること。* *3.開示の求めに応じることを拒否する場合、拒否する理由を本人に説明し、必要に応じて異議を唱えるための適切な連絡先情報を提供すること。*
	b)個人情報が不完全または不正確であることを本人が実証した場合、要請のあった修正、追加、または適宜、削除を行っていますか？	
	c)修正または削除の要請があってから適当な期間内にその修正や削除を行っていますか？	
	d)修正された個人情報の写しを本人に送ったり、データが修正または削除されたという確認を出す等していますか？	
	e)アクセスや修正が拒否された場合、なぜ拒否されたのかを、拒否に対する今後の問い合わせに	

	関する連絡先情報と供に、説明していますか？	*＜認証基準:7.6　個人情報の訂正、追加または削除＞* *申請する事業者は、本人から開示等の対象個人情報の内容が事実でないことを理由に、訂正、追加又は削除を求められた場合、根拠となる法令がある場合を除き、利用目的の範囲内に置いて、遅滞なく必要な調査を行い、訂正等を行うこと。* *1.本人から，当該本人が識別される開示等の対象個人情報の訂正等を求められた場合に、法令の規定により特別の手続が定められている場合を除き，利用目的の達成に必要な範囲内において，遅滞なく必要な調査を行い，その結果に基づいて，当該開示等の対象個人情報の訂正等を行わなければならない旨を規定し、その規定に従って運用していること。* *2.訂正等の結果を合理的な期間内に回答すること。* *3.本人への回答内容（求めに応じない場合を含む）に関する承認手順を定め、手順を明確に記述し、その手順に従って行う本人への回答内容について管理者の承認を得ていること。* *4.訂正を実施しない場合、訂正をしない理由を本人に通知し、必要に応じて異議を唱えるための適切な連絡先情報を提供していること。* *＜認証基準:7.7　個人情報の利用、または提供の拒否＞* *申請する事業者は、1.3 に違反して個人情報が取り扱われる場合又は 3.1 若しくは 3.1c を理由として個人情報の取得がなされたことを理由として本人から個人情報の利用の停止又は消去を求められた場合，及び 4.2 に違反して個人情報の提供がなされたことを理由として本人から第三者への提供の停止を求められた場合で，請求に理由があることが明らかとなった場合には、法令の根拠がある場合を除き，個人情報の利用の停止，消去又は第三者提供の停止（以下，「利用停止等」という。）を行うものとする。申請する事業者は、当該措置を講じた後は、遅滞なくその旨を本人に通知すること。* *1.本人から、当該本人が識別される開示等の対象個人情報の利用停止等を求められた場合、これに応じる旨を規定し、その規定に従って運用していること。* *2.措置を講じた後は、遅滞なくその旨を本人に通知しなければならない旨を規定し、その規定に従って運用していること。* *3.本人への回答内容（求めに応じない場合を含む）に関する承認手順を*

		定め、手順を明確に記述し、その手順に従って行う本人への回答内容について管理者の承認を得ていること。 *4.利用停止等の求めを拒否する場合、拒否する理由を本人に説明し、必要に応じて異議を唱えるための適切な連絡先情報を提供すること。*

6.1.8 責任（質問39から50）

責任では、APEC 情報プライバシー原則を遵守するための措置が講じられているか、苦情等への対応がなされているか、また委託などにより個人情報の転送を行っている場合には委託先が申請事業者の求める要件を遵守するように合理的な措置を講じているか等の審査を行います。

事前質問表	追加質問表
39.APEC 情報プライバシー原則に従うためにどんな措置を講じていますか？該当するものにすべてチェックし説明してください。	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:1.1 プライバシー原則の遵守＞* *申請する事業者は、他の参加エコノミーに越境移転させる目的で収集または受領したすべての個人情報(以下個人情報という)についてAPECプライバシー原則に継続して対策し実行しなくてはならない。* *対応と実行は以下の項目が含まれていなくてはならない* *・プライバシーポリシーとステートメント* *・内部指針または方針* *・契約* *・法令、該当する業界または部門の規定類の遵守* *・自主規制による規範または規則の遵守* *＜認証基準:1.4 法令、国が定める指針、その他の規範＞* *申請する事業者は、個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し参照できる手順と運用を確立していること。* *1.個人情報の取扱いに関する法令，国が定める指針その他の規範を特定し、参照し、維持する手順を定めていること。* *2.参照すべき法令、指針、規範を定めた手順に従って特定し、管理者の承認を得て必要に応じて更新していること。* *3.参照すべき法令、指針、規範が適切であること。* *4.参照すべき法令、指針、規範が、必要に応じ参照できること。且つ海外からの要求等を処理する適切な手順を含めること。*

	＜認証基準:1.6　内部規程＞ *申請する事業者は、下記の 1.から 15.に相当する具体的に規定すること。* *これらの規定は、社内の正式手続きを経たうえで定められ、従業者が参照可能な状態であること。* *1.個人情報を特定する手順に関する規定* *2.法令、国が定める指針その他の規範の特定、参照及び維持に関する規定* *3.個人情報に関するリスクの認識、分析及び対策の手順に関する規定* *4.事業者の各部門及び階層における個人情報を保護するための権限及び責任に関する規定* *5.緊急事態（個人情報が漏えい、滅失またはき損をした場合）への準備及び対応に関する規定* *6.個人情報の取得、利用及び提供に関する規定* *7.個人情報の適正管理に関する規定* *8.本人からの開示等の求めへの対応に関する規定* *9.教育に関する規定* *10.個人情報保護マネジメントシステム文書の管理に関する規定* *11.苦情及び相談への対応に関する規定* *12.点検に関する規定* *13.是正処置及び予防処置に関する規定* *14.代表者による見直しに関する規定* *15.内部規程の違反に関する罰則規定* **■左記に関して、以下についても具体的に説明されていることを確認します。** *＜認証基準:9.1　内部監査＞* *申請する事業者は、個人情報保護管理システムの認証基準の要件への適合状況、及び個人情報保護管理システムの運用状況について定期的に内部監査を実施していること。* *内部監査に関する以下の条件が満たされていること。* *1.申請する事業者は、認証基準の要件およびその運用状況への適合に関する内部監査を実施するための規則を制定し、監査計画に従って実施すること。*

	2.適合性および運用状況に関する内部監査は、事業体のすべてのセクションで実施されていること。 *3.申請する事業者の代表者が、個人情報保護監査責任者としての地位と客観性を有する事業体内の人を任命するための規則を制定し、それに応じて事業が行われていること。* *4.申請する事業者は、個人情報保護監査責任者が内部監査を指示し、監査報告書を作成し、それを事業体の代表者に提出するための規則を制定し、それに応じて事業が行われていること。* *5.申請する事業者は、内部監査の客観性と公平性を確保するための規則を制定し、どの監査員も所属するセクションを監査せず、それに応じて事業が行われること。* *監査計画とその実施に関する責任と権限を決定するための手順が確立され、ビジネスがそれに応じて実施されること。* *＜認証基準:9.2 内部監査計画書＞* *申請する事業者は、個人情報保護マネジメントシステムを確実に実施するために必要な教育、監査などの計画の立案、文書化、維持をすること。* *1.代表者の承認のもと教育計画書を作成するよう規定し、適切に作成していること。* *2.代表者の承認のもと監査計画書を作成するよう規定し、適切に作成していること。* *＜認証基準:9.3 是正処置、予防処置＞* *申請する事業者は、不適合に対する是正処置及び予防処置を確実に実施するための責任及び権限を定める手順を確立し実施し、維持すること。* *その手順には、次の事項を必ず含めること。* *a)不適合の内容を確認する。* *b)不適合の原因を特定し、是正処置及び予防処置を立案する。* *c)期限を定め、立案された処置を実施する。* *d)実施された是正処置及び予防処置の結果を記録する。* *e)実施された是正処置及び予防処置の有効性をレビューする。*
40.上記措置に対する組織全体	**■左記に関して、具体的に説明されていることを確認します。説明では**

の遵守について責任を持つ担当者がいますか？	**以下を満たしていることを証明する必要があります。** *＜認証基準:8.1　資源、役割、責任、権限＞* *申請する事業者の代表者は、個人情報保護マネジメントシステムを確立、実施、維持、改善するために、不可欠な資源を用意していること。* *1.各担当者の役割・権限を明確に定め、文書化していること。* *2.各担当者の役割、責任及び権限を明確に定めていること。* *3.個人情報保護管理者と個人情報保護監査責任者は同一人物でないこと。* *個人情報保護管理者は、代表者によって内部から指名していること。* *個人情報保護監査責任者は、代表者により内部から指名され、会社法上の監査役が体制の一部を占めていないこと。* *4.各担当者の役割・権限を周知させていること* *5.個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない旨を規定し、実際に報告していること。*
41.プライバシー関連の苦情の受付、調査、対応に関わる手順を用意していますか？ 42.苦情申立てに適時に対応するための手順を用意していますか？	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:8.2　苦情・相談の対応＞* *申請する事業者は、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順・体制を確立し、維持すること。*
43.「はい」の場合、その対応では、苦情に関連した救済措置の説明もしていますか？具体的に説明してください。	*1.個人情報の取扱い及び個人情報保護マネジメントシステムに関して，本人からの苦情及び相談を受け付けて，適切，かつ，迅速な対応を行う手順を定めていること。* *2.苦情の申し出先が、本人にとって明確であること。* *3.規定した手順に従って受け付け、対応していること。* *4.受け付ける手順が有効に運用されており、対応が迅速であること。* *5.本人に回答する対応内容について承認手順を規定し、その規定に従って運用し、対応内容について管理者の承認を得ていること。* *6.苦情や相談の内容及び対応結果を代表者に報告する手順を規定し、その規定に従って代表者に報告していること。*
44.プライバシー関連の苦情への対応方法をはじめ、プライバシーに関する方針や手順に関して社	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:8.3　従業者の管理＞*

員を教育する手順を用意していますか？	*申請する事業者は、従業者に個人情報を取り扱わせるに当たって、当該個人情報の安全管理措置が図られるよう、当該従業者に対し必要かつ適切な監督を行うこと。* *1.従業者に対し必要かつ適切な監督を行わなければならない旨をこの認証基準に沿って規定し、従業者に対し必要かつ適切な監督を行っていること。* *2.従業者との雇用契約時または委託契約時に、個人情報の非開示契約を締結するように規定し、その規定に従って運用していること。* *3.雇用契約または委託契約等を締結する場合、非開示条項は、契約終了後も一定期間有効とするよう規定し、その規定に従って運用していること。* *4.個人情報保護マネジメントシステムに違反した場合の措置に関する措置を規定し、その規定に従って運用していること。* *5.ビデオ及びオンラインによる従業者のモニタリングを実施する場合、その措置の実施について規定し、その規定に従って運用していること。* *6.モニタリングの実施に関する責任者とその権限を規定し、その規定に従って運用していること。* *7.あらかじめモニタリングの実施について定めた社内規程を策定し、事前に社内に徹底していること、及びモニタリングの実施状況について、適正に行われているか監査または確認を行っていること。* *＜認証基準:8.4　従業者の教育＞* *申請する事業者は、従業者に定期的に適切な教育を行わなければならないこと、並びに、従業者に、関連する各部門及び階層においてそれぞれ必要な事項を理解させる手順を確立、維持すること。* *1.すべての従業者に定期的に個人情報保護に関する適切な教育を実施するよう規定し、教育計画書に従い教育を実施していること。* *2.すべての従業者に個人情報保護に関する適切な教育を受講していること。* *3.規定または教育計画書、少なくとも以下の a)～f)の内容を含めていること。* *a)個人情報に関する方針や手順* *b)APEC の情報プライバシー原則に従うことの重要性及び利点*

	c)APEC の情報プライバシー原則に従うための役割及び責任 *d)APEC の情報プライバシー原則に違反した際に予想される結果* *e)苦情及び相談への対応* *f)法令に基づき個人情報の提供を行う場合の手続* *4.教材に上記の a)～f)の内容を含めていること。* *5.受講者の理解度確認を実施する手順を規定し、その規定に従って運用していること。* *6.教育の計画及び実施，結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を規定し、その規定に従って運用していること。*
45.個人情報の開示が求められる場合をはじめ、裁判所またはその他政府の召喚令状、捜査令状や命令に対応するための手順を用意していますか？	■左記に関して、具体的に説明されていることを確認します。 *＜認証基準:1.4　法令、国が定める指針、その他の規範＞* *申請する事業者は、個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し参照できる手順と運用を確立していること。* *1.個人情報の取扱いに関する法令，国が定める指針その他の規範を特定し、参照し、維持する手順を定めていること。* *2.参照すべき法令、指針、規範を定めた手順に従って特定し、管理者の承認を得て必要に応じて更新していること。* *3.参照すべき法令、指針、規範が適切であること。* *4.参照すべき法令、指針、規範が、必要に応じ参照できること。且つ海外からの要求等を処理する適切な手順を含めること。*
46.代行して個人情報を処理する、処理業者、代理人、請負業者、またはその他のサービス提供者に関して、各個人に対するあなたの義務が必ず果たされるようにするための方法を用意していますか？（該当するものを全てチェック） 47.上記の契約では一般に個人情報の処理業者、代理人、請負業者またはその他のサービス業者に以下の行為を義務付けていますか？（該当するものを全てチェック）	**■左記に関して、具体的に説明されていることを確認します。説明では以下を満たしていることを証明する必要があります。** *＜認証基準:8.6　委託先の管理＞* *申請する事業者は、個人情報の取扱いに関して委託する場合は、委託先選定の基準を確立したうえで、十分な個人情報の保護水準を満たしている者を選定すること。* *また、委託する個人情報の安全管理が図られるよう、委託先に対して必要かつ適切な監督を行うこと。* *1.委託先の選定基準を定める手順及び見直しの手順を規定し、その規定に従って具体的で運用可能な委託先選定基準を確立していること。* *2.必要に応じて委託先選定基準の見直しを実施していること。* *3.委託先選定基準により委託先を評価（定期的な再評価を含む）するよう規定し、その規定に従って運用していること。*

48.個人情報の処理業者、代理人、請負業者、その他のサービス業者に、指示または契約や合意に従わせるために監査の提出を義務付けていますか？	*4.すべての委託先を認識していること。* *5.委託先の義務が確実に果たされるため、下記の a)～i)の内容を含む、メカニズム(委託先との契約を含む。)を規定し、その規定に従って運用していること。* *a)申請者のプライバシーステートメントに明記されているプライバシー方針や実務ルールに実質的に類似したプライバシールールを実施すること* *b)申請者の個人情報の取り扱いに関する指示に従うこと* *c)委託者及び受託者の責任の明確化* *d)個人情報の安全管理に関する事項* *e)申請者の同意がない限り再委託を制限する事項* *f)個人情報の取扱状況に関する委託者への報告の内容及び頻度* *g)契約内容が遵守されていることを委託者が確認できる事項* *h)契約内容が遵守されなかった場合の措置* *i)事件・事故が発生した場合の報告・連絡に関する事項* *6.指示または合意、契約の遵守のために、委託先に対して定期的な自己評価の提出を義務付けていること* *7.指示または合意、契約の遵守のために、委託先の定期的なモニタリングまたは抜き打ち検査を実施していること* *8.当該契約書などの書面を個人情報の保有期間にわたって保存する手順を規定し、その規定に従って運用していること。*
49.指示または合意や契約に従わせるために、処理業者、代理人、請負業者、またはその他のサービス業者の定期的な検査やモニタリングを行っていますか？	
50.CBPR を確実に遵守させるための事前評価及び方法が、個人情報の処理業者、代理人、請負業者、その他のサービス業者に難しいという場合であっても、個人情報を開示していますか？	

【第 2 版　改訂履歴】

第 2 版	2021 年 2 月改訂	－
第 2.1 版	2021 年 12 月改訂	「4.2　申請資格」における、対象事業者となるための手続及び、「4.3　CBPR　認証の申請書類の提出方法」における電子ファイルでの申請に係る内容を中心に加筆
第 2.2 版	2022 年 5 月改訂	「4.3　CBPR　認証の申請書類の提出方法」に「(5)過去 6 カ月の事故等一覧」を追加
第 2.3 版	2022 年 8 月改訂	「4.2　申請資格」の対象事業者について加筆 「4.4 CBPR 認証取得事業者が再び申請する方法」を追加

APEC CBPR 認証
申請ガイドブック
2.3 版　 2022 年 8 月 30 日発行

発行　　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

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
TEL03－5860－7576