2019 年 4 月 7 日版

APEC 越境プライバシールール（CBPR）システムに申請する事業者のための認証基準

一般財団法人日本情報経済社会推進協会

■APEC プライバシーフレームワークへの準拠状況の確認

この審査基準は APEC Cross-Border Privacy Rules System Policies, Rules And Guidelines に基づく
申請者は越境する個人情報（個人を識別もしくは識別し得る全ての情報）保護リスク対応のために以下の管理策を決定しなければならない。

項番	項目	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
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。
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。
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。
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。

項番	項目	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
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。
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

項番	項目	基準
		の内容が適切であること。
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。
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。 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。
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。

項番	項目	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
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。 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。
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

項番	項目	基準
		- 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。
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
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。
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。 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 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 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 (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 (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

項番	項目	基準
		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	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。
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。
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。
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
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
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、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）の氏名または職名、所属及び連絡先 c) 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

項番	項目	基準
7.2	個人情報に関する権利	申請する事業者は、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。）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。
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続として、以下の事項を定めていること。 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 c) 開示等の求めをする者が、本人または代理人であることの確認の方法 d) 開示、訂正、追加また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
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。 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。
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，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。
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、追加また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。

項番	項目	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または 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また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，消去また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。
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。
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。 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。
8.3	従業者の管理	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。

項番	項目	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。
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。
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。 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。

■APEC プライバシーフレームワークに準拠、維持するための体制の確認

申請者は上記 APEC プライバシーフレームワークに準拠し、維持するための体制を構築・維持しなければならない。

項番	項目	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。
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。
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。

JIPDEC

別紙 1

安全管理措置一覧

基準
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、滅失又はき損の防止その他の個人情報の安全管理措置のために必要、かつ、適切な措置を講じること。 Ⅰ．物理的安全管理措置として講じなければならない事項 (1) 入退館（室）管理の実施 a) 建物、室、サーバー室、個人情報の取扱い場所への入退を制限していること。 b) 建物、室、サーバー室、個人情報の取扱い場所への入退の記録を取り、保管していること。 c) 建物、室、サーバー室、個人情報の取扱い場所への入退の記録を定期的にチェックしていること。 (2) 盗難等の防止 a) 離席時に個人情報を記した書類、媒体、携帯可能なコンピュータ等を机上に放置していないこと。 b) 個人情報を取り扱うコンピュータの操作において、離席時は、パスワード付きスクリーンセーバーの起動又はログオフを実施していること。 c) 個人情報を記録した媒体（紙、外部記録媒体）は施錠保管していること。 d) 個人情報を記録した媒体の保管場所の鍵は特定者が管理していること。 e) 個人情報を記録した媒体（紙、外部記録媒体）の廃棄は、再利用できない措置を講じていること。 f) 個人情報を記録した携帯可能なコンピュータ等について、盗難防止措置を講じていること。 g) 携帯可能なコンピュータやUSBメモリ、CD-ROM等の外部記録媒体の利用についてルールを定め、それを遵守していること。 h) 個人情報を取り扱う情報システムの操作マニュアルを机上に放置していないこと。 (3) 機器・装置等の物理的な保護 a) 個人情報を取り扱う機器・装置等について、安全管理上の脅威（盗難、破壊、破損等）や環境上の脅威（漏水、火災、停電、地震等）から物理的に保護する装置を導入していること。

Ⅱ．技術的安全管理措置として講じなければならない事項

(1) 個人情報へのアクセスにおける識別と認証

a) 個人情報へのアクセスにおいて、識別情報（ID、パスワード等）による認証を実施していること。

b) 個人情報を格納した情報システムについて、デフォルトの設定を適切に変更していること。

c) 識別情報の発行・更新・廃棄は、ルールに従っていること。

d) 識別情報を平文で記録していないこと

e) 識別情報の設定及び利用は、ルールに従っていること。

f) 個人情報へのアクセス権限を有する従業者が使用できる端末又はアドレス等について制限していること。

(2) 個人情報へのアクセス制御

a) 個人情報にアクセスできる従業者の数は必要最小限にしていること

b) 個人情報にアクセスできる識別情報を共用していないこと。

c) 従業者に付与するアクセス権限は必要最小限にしていること。

d) 個人情報を格納した情報システムの同時利用者数を制限していること。

e) 個人情報を格納した情報システムの利用時間を制限していること。

f) 個人情報を格納した情報システムを無権限アクセスから保護していること。

g) 個人情報にアクセス可能なアプリケーションの無権限利用を防止していること。

h) 個人情報を取り扱う情報システムに導入したアクセス制御機能の有効性を検証していること。

(3) 個人情報へのアクセス権限の管理

a) 個人情報にアクセスできる者を許可する権限の管理を適切かつ定期的に実施していること。

b) 個人情報を取り扱う情報システムへのアクセスは必要最小限であるよう制御していること。

(4) 個人情報へのアクセスの記録

a) 個人情報へのアクセスや操作の成功と失敗の記録を取得し、保管していること。

b) 取得した記録について、漏えい、滅失及びき損から適切に保護していること。

(5) 個人情報を取り扱う情報システムに関する不正ソフトウェア対策

a) ウイルス対策ソフトウェアを導入していること。

b) OS やアプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆるセキュリティパッチ）を適用していること。

c) 不正ソフトウェア対策の有効性・安定性を確認していること。

d) 個人情報にアクセスできる端末にファイル交換ソフトウェア（Winny、Share、Cabos 等）をインストールしていないこと。

(6) 個人情報の移送・通信時の対策

a) 個人情報の受渡しには授受の記録を残していること。

b） 個人情報を媒体で移送するときに紛失・盗難が生じた際の対策を講じていること

c） 盗聴される可能性のあるネットワーク（例えばインターネットや無線 LAN 等）で個人情報を送信する際に、個人情報の暗号化又はパスワードロック等の秘匿化の措置を講じていること。

(7) 個人情報を取り扱う情報システムの動作確認時の対策

a） 情報システムの動作確認時のテストデータとして個人情報を利用していないこと。

b） 情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことを検証していること。

(8) 個人情報を取り扱う情報システムの監視

a） 個人情報を取り扱う情報システムの使用状況を定期的にチェックしていること。

b） 個人情報へのアクセス状況（操作内容を含む。）を定期的にチェックしていること。