2017 年 04 月 05 日制定
2020 年 11 月 30 日改正

（第２版）

個人情報保護法等適合性評価サービスについて

■　目　次

１．個人情報保護法等適合性評価サービスの概要

１．１　評価サービスとは

個人情報保護法等適合性評価サービス（以下、「評価サービス」という。）とは、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（以下、「保護法等」という。）に適合した個人情報保護管理システムを構築し、個人情報を適切に保護している事業者を、NPO 法人 日本情報システム・コンサルタント協会（以下、「当協会」という。）が第三者の立場で客観的に評価して『個人情報保護法等適合性評価確認書（以下、「評価確認書」という。)』を交付するサービスです。

No.	主要な保護法等
1	個人情報の保護に関する法律（個人情報保護法）
2	行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法）
3	個人情報の保護に関する法律についてのガイドライン〔通則編〕
4	個人情報の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〕
5	個人情報の保護に関する法律についてのガイドライン〔仮名加工情報・匿名加工情報編〕
6	個人情報の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］
7	特定個人情報の適正な取扱いに関する ガイドライン〔事業者編〕

図表１－１　主要な保護法等

１．２　評価サービス誕生の背景

（１）番号法の施行と個人情報保護法の改正

番号法が施行され、個人番号及び特定個人情報の適正な取扱いとその保護が全ての事業者に義務付けられました。また、個人情報保護法の改正によって、従来個人情報保護と無縁だった中小規模事業者も、今後は対応に取組まざるを得ない状況になりました。中小規模事業者が適正な取組みを行わずに、個人情報の漏えい事件・事故を起こした場合には、個人情報保護法違反になってしまいます。

（２）個人情報のデジタル化

コンピューターによる個人情報の管理が一般的となり、事業者は過去には考えられないほどの大量の個人情報をデジタル化して所有するようになりました。デジタル化された個人情報は、複製が容易なため紙媒体を利用していた時代よりも漏えいの危険性が飛躍的に高くなっています。不適正な個人情報の管理・取扱いを起因とする大量の個人情報の漏えい・滅失・毀損によって、個人のプライバシー等の権利利益の侵害、並びに事業者が社会的信用・信頼の失墜及び経済的損失を被ることを防ぐために、個人情報への安全管理措置が必要とされています。

（３）個人情報保護への国民意識の高まり

日々報道される個人情報の漏えい事件・事故を見聞きする中で、個人情報を提供する際に、提供した個人情報が適正に管理・取扱いをされているかを気にする人が増えています。確実に個人情報保護への国民の意識は高まっています。個人のプライバシーを守ろうとする事業者でないと、生き残れない社会になってきていると言っても過言ではないでしょう。

上記の懸念事項に対応するためには、事業者において個人情報の適正な取扱いと個人情報保護のための対策が的確に行われているかを第三者として審査する仕組み、つまり評価サービスが必要と思われます。

当協会はこの分野の専門家を多く抱えており、NPO 法人として評価サービスの根幹を理解してもらうための啓発活動と同時に当該審査事業にも取組んでいくことで、社会的責任をはたしていくことを目指したいと考えています。

１．３　評価サービスの目的と狙い

（１）目的

評価サービスの対象事業者から独立した当協会が、第三者の立場で客観的に評価することで、保護法等に適合した個人情報保護管理システム（以下、「PCS [注1]」という。）を構築して、個人情報を適切に保護している事業者であることを、担保します。

注１：PCS（Personal information protection Control System）とは、事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための、個人情報保護に係る方針の文書化、計画・準備、実施・運用、確認・評価、及び是正・改善を含む、管理の仕組みをいいます。

（２）狙い

個人情報の適正な取得、利用、及び提供、並びに個人情報の漏えい・滅失・毀損を防止することで、個人のプライバシー等の権利利益の侵害を未然に防止します。

１．４　取得のメリット

評価サービスを通じて、次の効果が期待できます。

（１）保護法等に準拠した PCS を構築して個人情報を適切に保護している事業者であることを対外的に強くアピールすることができ、利害関係者（顧客、取引先、従業者など）からの信頼を獲得することができます。

（２）改正個人情報の施行によって、全ての事業者に委託先における個人データの取扱い監督義務が生じました。当協会から評価確認書の交付を受けることで、同業他社との差別化を図ることができます。

（３）個人情報の漏えいは外部からの侵入者ではなく、内部からがほとんどを占めています。従業者の個人情報保護に対する意識を向上させることで、個人情報の漏えい事件・事故の発生を未然に防ぐことができます。

（４）PCS の構築・維持によって、個人情報の保護だけでなく、業務情報のセキュリティを強化することができます。

（５）個人情報保護に必要な内部規程が整備されることによって、短期間（3 ヵ月から 6 ヵ月以内）でプライバシーマーク（以下、「P マーク」という。）[注2]を取得することが可能になります。

注２：一定の要件を満たした事業者などの団体に対し、一般財団法人 日本情報経済社会推進協会（JIPDEC）が使用を許諾する登録商標です。P マークの取得によって、顧客からの更なる信用・信頼を獲得し、受注拡大・利益確保に貢献することが期待されます。

１．５　評価確認書交付の対象と単位

評価サービスの対象は、国内に活動拠点を持つ事業者です。また、評価確認書の発行は、法人単位となります。

少なくとも次の条件を満たしている事業者であって、実際の事業活動の場で個人情報の保護を推進している必要があります。

（１）当協会が定めた『個人情報保護管理システム - 要求事項)』（以下、「PCS - 要求事項」という。）に準拠した PCS の文書を定め、実施可能な体制が整備されていること。

（２）事業者自らが、PCS の文書のレビューを完了していること。

１．６　評価確認書の有効期間

新規審査後に交付する評価確認書の有効期間は、1 年間です。次回の更新審査後から交付する評価確認書の有効期間は、3 年間です。

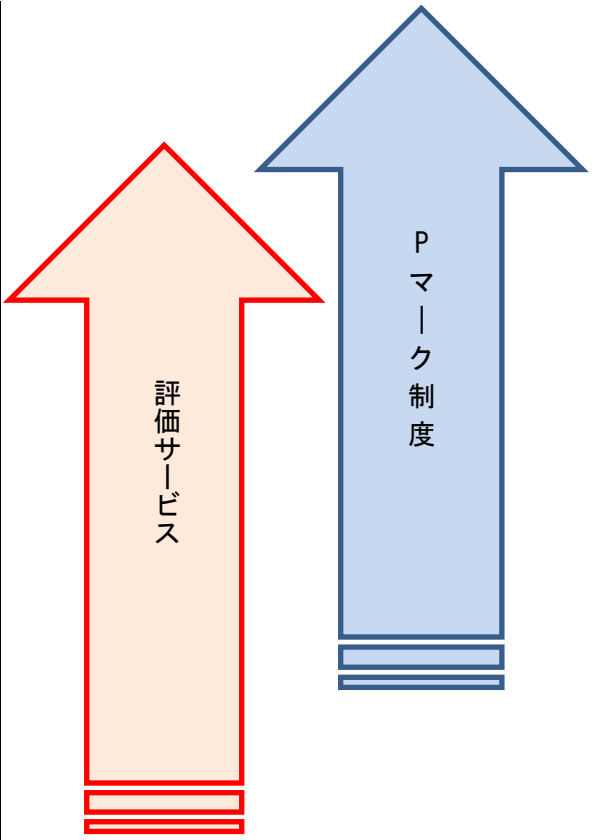
１．７　プライバシーマーク制度との違い

JIPDEC のプライバシーマーク制度（以下、「P マーク制度」という。）と当協会の評価サービスとでは、次の相違があります。

（１）成熟度目標

P マーク制度の成熟度目標はレベル 5 ですが、評価サービスの成熟度目標はレベル 4 となっています。P マーク制度に比べ、目標が低く設定されています。

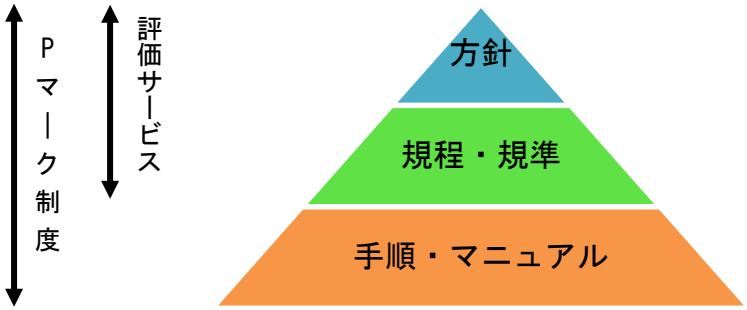
レベル５	マネジメントシステムの原則に従って PDCA サイクルをスパイラル的に廻し、個人情報保護の最適化が図られている。
レベル４	PCS - 要求事項に従って個人情報保護の計画・準備、実施・運用、及び確認・評価を行い、適宜に是正・改善を行っている。
レベル３	個人情報保護に係る内部規程を策定し、当該文書に従って個人情報保護を組織的に実施・運用している。
レベル２	個人情報保護に係る内部規程が策定されておらず、個人情報保護の実施・運用は従業者に一任している。
レベル１	個人情報保護の必要性・重要性に気付いているが、その対策は場当たり的なものとなっている。
レベル０	個人情報保護の必要性・重要性に全く気付いておらず、何の対策も講じていない。



図表１－２　成熟度目標

（２）文書

Ｐマーク制度は、個人情報保護に係る文書として方針・規程・手順の策定を要件としています。評価サービスは、個人情報保護に係る文書として手順の策定を要件としていません。Ｐマーク制度に比べ、文書作成の負荷が軽減されています。



図表１－３　マネジメント文書の体系

（３）準備期間

Ｐマーク制度は、Ｐマークの取得準備期間として概ね３ヵ月～6 ヵ月を要します。一方、評価サービスは、評価確認書の取得準備期間として概ね 2～3 ヵ月を要します。Ｐマーク制度に比べ、短期間で評価確認書を取得できます。

（４）費用（消費税込み）

Ｐマーク制度は、Ｐマークの新規交付に 314,288 円～1,257,144 円、更新に 230,478 円～942,858 円かかります。一方、評価サービスは、評価確認書の新規交付に 55,000 円～121,000 円、更新に 44,000 円～82,500 円かかります。Ｐマーク制度に比べ、リーズナブルな価格設定となっています。

（５）従業員数

Ｐマーク制度は、個人情報保護の内部監査を必須要件としているため、従業員数は最低でも個人情報保護管理者と内部監査責任者の２名となっていいます。一方、評価サービスは、個人情報保護の内部監査を必須要件としていないため、従業員数は１名でも問題ありません。したがって、一人親方でも、評価サービスの審査を受けることができます。

（６）リスクアセスメント及びリスク対策

Ｐマーク制度は、全ての事業者に個人情報の取扱いの各局面における詳細なリスクアセスメントを行い必要なリスク対策を講じ、かつ、年１回及び適宜にそれらを見直すことを求めています。一方、評価サービスは、簡易なリスクアセスメントを行い必要なリスク対策を講じ、かつ、定期的（少なくとも３年に１回）及び適宜に見直すことを求めています。Ｐマーク制度に比べ、リスクアセスメント及びリスク対策の負荷が軽減されています。

（７）審査技法

Ｐマーク制度は、内部規程への準拠性審査の技法として、事業者の現場に赴き、記録の閲覧、関係者への質問（対面インタビュー）、現場の観察などを用いています。一方、評価サービスは、内部規程への準拠性審査の技法として、遠隔審査による記録の閲覧、関係者への質問（オンラインインタビュー）などを行います。したがって、事業所へ赴いての現地審査は行いません。事業者の審査への負担が軽減されます。

２．評価サービスの費用

評価サービスに係る費用は、事業者規模（業種、従業者数で判定）によって異なります。

２．１　料金表

単位：円（消費税抜き）

種別	新規審査の時			更新審査の時		
事業者規模	小規模	中規模	大規模	小規模	中規模	大規模
審査料[注１注２]	45,000	75,000	105,000	25,000	40,000	60,000
交付登録料	5,000	5,000	5,000	15,000	15,000	15,000
合　計	50,000	80,000	110,000	40,000	55,000	75,000

図表２－１　料金表

２．２　審査料

評価サービスの審査に係る費用として必要です。審査料には、審査関係事務、適合状況審査、運用状況審査、報告書作成などの各費用を含みます。交付適格性審査の申請後に当協会からご請求いたします。

注１：当協会が認定した文書の雛形（記録様式を含む。）を使用して申請した事業者に対しての審査料金です。当協会が認定した文書の雛形を使用せず、自社独自で考案した文書で申請した事業者に対しては、新規申請時に、小、中、大事業者それぞれに、10 万円、15 万円、20 万円の追加料金が発生します。

注２：当協会が認定した組織が主催する、個人情報保護に係る研修の修了事業者につきましては、文書審査に要する時間が削減されるため、新規時の審査料を所定の 20%割引とします。

２．３　交付登録料

当協会からの交付適格決定の通知送付後に、ご請求いたします。

２．４　事業者規模

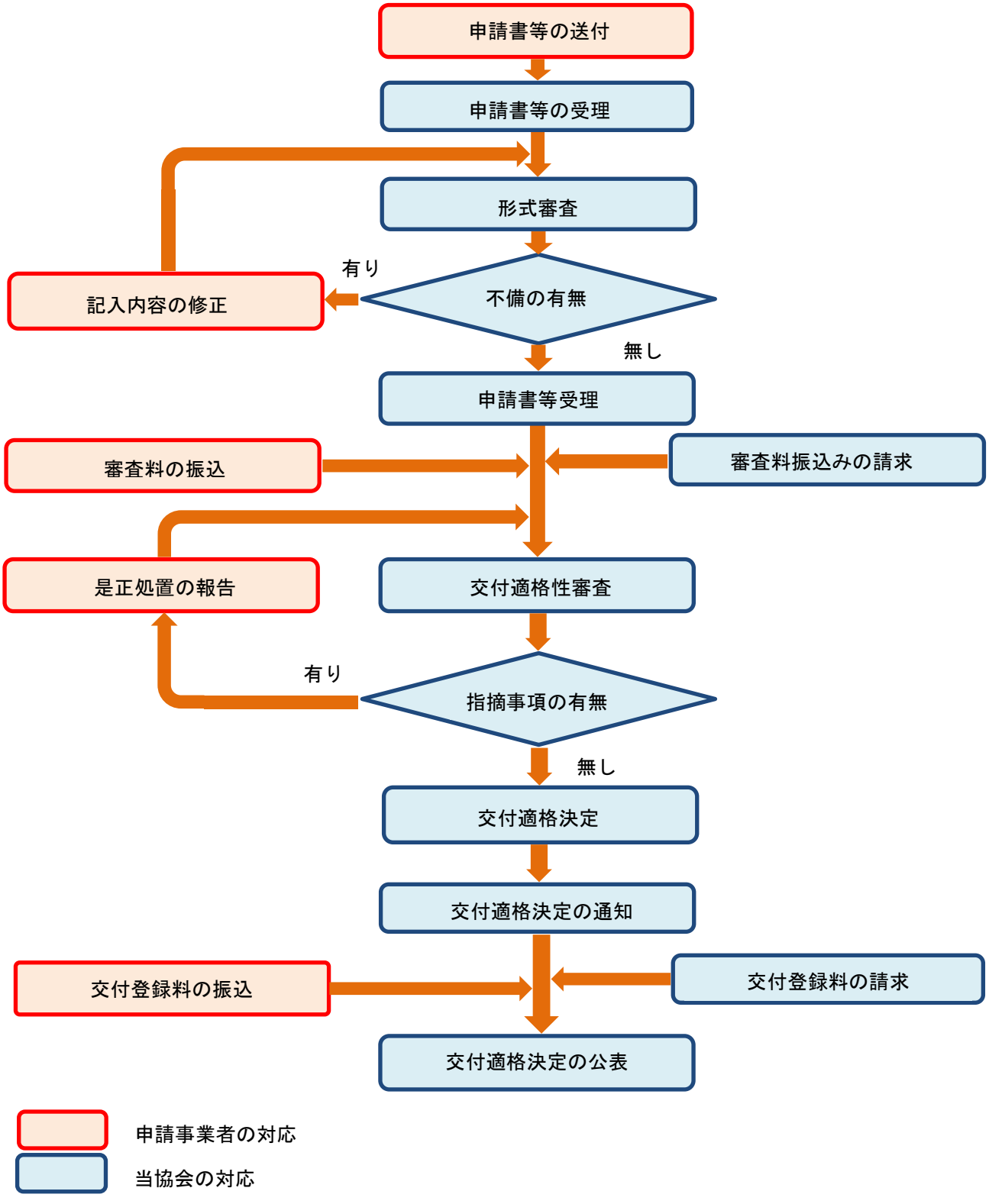
業種と従業者数のみで判定します。

業種分類	従業者数		
	小規模	中規模	大規模
製造業・その他	1～20 人	21～100 人	101 人～
卸売業	1～10 人	11～100 人	101 人～
小売業	1～5 人	6～100 人	101 人～
サービス業	1～10 人	11～100 人	101 人～

図表２－２　事業者規模判定表

３．審査の申請から交付適格決定の公表までの流れ

交付適格性審査の申請から交付適格決定の公表までの流れを、次図に示します。



図表３－１　審査の申請から交付適格決定の公表までの流れ

４．交付適格性審査の申請

４．１　申請手続

当協会への申請に必要な書類は、次表の通りです。

No.	申請書等
0	審査申請書等チェックリスト（申請-00）
1	審査申請書（申請-01）
2	申請事業者の会社概要（申請-02）
3	個人情報を取扱う業務の概要（申請-03）
4	全事業所の所在地及び業務内容（申請-04）
5	個人情報保護管理システムの運用体制（申請-05）
6	文書（規程・記録様式）一覧（申請-06）
7	個人情報保護管理システム - 要求事項との対応表（申請-07）
8	教育実施サマリー（申請-08）【全従業者に実施した教育実施状況】
9	内部監査実施サマリー（申請-09）【全部門に実施した監査実施状況がある場合】
１０	マネジメントレビュー実施サマリー（申請-10）
１１	会社パンフレット（ある場合）
１２	個人情報保護管理システム文書一式（申請-06、申請-07 に記入した内部規程・記録様式の全て。記録様式は、記入済みサンプルのコピー（2～3 枚））

図表３－１　申請書等の一覧

※　各申請書に記載された【記入上の注意】は、提出する際に削除してください。

※　ご提出の際は、申請書等を№0～№12 の順に A4 サイズ・2 つ穴にてファイルに綴じてください。各書類には、インデックスを付けてください。

※　申請後、申請書等の内容に変更があった場合は、当該申請書等に係る変更報告書（様式は自由）、変更のあった申請書等をご提出ください。

４．２　申請方法

申請書等を作成し、簡易書留、宅急便など、配送記録が残る手段を利用してご送付ください。なお、申請書は「PCS に関する問合せ先」（E-mail ユーザ名：pcs-assess、ドメイン名 jisca.jp）に、ご請求ください。

４．３　申請窓口

特定非営利活動法人 日本情報システム・コンサルタント協会（当協会）
- 〒110-0015　東京都台東区東上野３－２６－３
- TEL：　03-3839-1677（代表）
- E-mail：（ユーザ名：jisca22、ドメイン名 jisca.jp）
- URL：　https://jisca.jp/jis/
- 受付時間 10：00～17：00（土、日、祝日休み）

※　上記以外のお電話や直接ご持参しての申請はお受け致しかねますので、その旨ご了承賜りますようお願いします。

４．４　申請受理

申請書等の不足及び記入内容について、不備がないかを確認します。

問題がなければ、申請を受理し、『申請書等受領書』と『審査料請求書』を送付いたしますので、指定の口座にお振込みをお願いいたします。お預かりした書類をもとに、「5. 交付適格性審査と交付適格決定」に進みます。

申請書等が全て揃っていない場合、問題がある等の場合は、申請書等を申請事業者の費用負担で返却させて頂きます。

４．５　更新申請

（１）更新申請対象の事業者

現に評価確認書の交付を受けている事業者で、評価確認書の有効期間の満了を迎える事業者です。

（２）更新申請の受付期間

評価確認書の有効期間の満了日 6 ヵ月前の日から満了日 3 ヵ月前の日までです。

【更新申請の受付期間の例】

有効期間の満了日：令和 2（2020）年 1 月 10 日の場合
更新申請受付期間：令和 1（2019）年 7 月 10 日 ～ 令和 1 年（2019）年 10 月 10 日

※　有効期間、受付期間は事業者ごとに異なります。

※　上記の原則に沿って確定した更新申請の受付期間の最終日が、土曜日、日曜日、祝祭日などに当たる場合は、直後の営業日まで延長して受付けます。

５．交付適格性審査と交付適格決定

５．１　適合状況審査（文書審査）

受理された内部規程について、PCS - 要求事項に適合（合致）しているかどうかの適合状況の審査を行います。審査において発見された不適合につきましては、申請事業者に書面（指摘事項文書）で通知します。

申請事業者は、指摘事項文書に記載された不適合を、原則として運用状況審査の前に是正しなければなりません。

５．２　運用状況審査（準拠性審査）

実際の業務における個人情報の取扱いが、PCS - 要求事項と適合した内部規程に準じて行われているかの運用状況の審査をリモート（遠隔）で行います。審査において発見された不適合につきましては、申請事業者に書面（指摘事項文書）で通知します。

申請事業者は、指摘事項文書に記載された不適合を、指摘事項文書の発効日から 2 ヵ月以内に是正し、当協会に報告しなければなりません。

当協会は、申請事業者からの是正処置の報告において、不適合と指摘した事項の是正が確認できない場合は、再度不適合の指摘を行います。

申請事業者は、すべての不適合を、初回の指摘事項文書の発効日から 4 カ月以内に是正しなければなりません。

５．３　交付適格決定

（１）交付適格決定の通知

交付適格性審査において不適合が全くない場合、又は指摘した全ての不適合が 4 か月以内に解消された場合は、申請事業者を交付適格決定とします。指摘した全ての不適合が 4 か月以内に解消されない場合は、申請事業者を交付適格の否認とします。

（２）評価確認書の交付及び登録の公表

交付適格決定後、『交付登録料請求書』を送付いたしますので、指定の口座にお振込みをお願いいたします。

当協会は、交付登録料の振込確認後、速やかに当該事業者に対して評価確認書を交付します。また、所定の登録簿に交付適格決定を受けた事業者に関わる事項を記載して、当協会のホームページ上で公表いたします。

５．４　評価確認書交付の取消し

当協会は、評価確認書の交付を受けていながら個人情報の不適切な取扱いを行った結果、個人情報の漏えい、滅失又は毀損、保護法等の違反など、個人情報に関わる重大な事件・事故が発生した事業者に対して、評価確認書交付の取消しを行うことがあります。

６．PCS の構築手順

PCS は、次の手順で構築することができます。

Step01	個人情報保護の目的と方針を定め文書化する
Step02	PCS 構築のための組織を編成する
Step03	PCS 構築の作業計画を立案する
Step04	個人情報保護の目的と方針を組織内に周知する
Step05	保護対象となる個人情報を特定する
Step06	個人情報の取扱いに関する法令等を特定する
Step07	個人情報保護リスクを特定し、分析・評価し、必要な対策を決定する
Step08	PCS 構築に必要な経営資源を確保する
Step09	PCS に係る内部規程を策定する
Step10	PCS を周知するための教育を実施する
Step11	PCS の試行運用を開始する
Step12	PCS の試行運用状況を点検・評価する
Step13	PCS の試行運用で明らかになった不具合を是正する

図表６－１　PCS の構築手順