

個人情報保護法等適合性評価サービス

■ 目 次

1. 個人情報保護法等適合性評価制度の概要	2
1. 1 個人情報保護法等適合性評価制度とは	
1. 2 適合性評価制度誕生の背景	
1. 3 適合性評価制度の目的と狙い	
1. 4 取得のメリット	
1. 5 交付の対象・単位	
1. 6 有効期間	
1. 7 プライバシーマーク制度との違い	
2. 費用	7
2. 1 料金表	
2. 2 審査料	
2. 3 確認書交付登録料	
2. 4 事業者規模	
3. 申請・審査	8
3. 1 申請	
3. 1. 1 申請の流れ	
3. 1. 2 申請の手続き	

1. 個人情報保護法等適合性評価制度の概要

1. 1 個人情報保護法等適合性評価制度とは

個人情報保護法等適合性評価制度（以下、「適合性評価制度」という。）とは、個人情報について、個人情報の取扱い・保護に関する法令、国が定める指針、その他の規範（以下、「法令等」という。）に適合した個人情報保護管理システムを構築して体制を整備している事業者を、NPO 法人 日本情報システム・コンサルタント協会（以下、「JISCA」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、「適合性評価確認書」という。）』を交付する制度です。

No.	主要な法令等
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	個人データの漏えい等の事案が発生した場合等の対応について
6	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 主要な法令等

1. 2 適合性評価制度誕生の背景

（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すべ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、個人情報漏えい事件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、複写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、滅失又は毀損によって、事業者が社会的信用の失墜や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その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・認定する仕組み、つまり適合性評価制度が必要と思われます。

JISCA はこの分野の専門家を多く抱えており、NPO 法人として適合性評価制度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 適合性評価制度の目的と狙い

(1) 目的

適合性評価制度の対象事業者から独立した JISCA が、第三者の立場で客観的に評価することで、法令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。）を構築して体制を整備している事業者であることを、担保します。

注1：PCS（Privacy 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システムをいいます。

(2) 狙い

個人情報を取扱う事業者の順守すべき事項、及び個人データの取扱プロセスにおけるリスクを軽減させる適切かつ有効な安全管理策を定め、これらを順守して個人データの取扱いを適正に行うこととで、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

適合性評価を通じて、次の効果が期待できます。

- (1) 法令等に準拠した PCS を構築して体制を整備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、従業者等）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り、すべ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。JISCA から適合性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) 個人データ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、個人データの漏えい事件・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、個人データの保護だけでなく、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文書類が整備されることによって、短期間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 交付の対象・単位

適合性評価制度の対象は、国内に活動拠点を持つ事業者です。また、適合性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) JISCA が規定する『個人情報保護管理システム - 要求事項』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 有効期間

一回の審査による適合性評価確認書の有効期間は、3年間です。適合性評価確認書の交付後、1年毎に記録のサンプル、並びに新規制定及び改定した文書の審査（以下、「維持確認審査」という。）の手続きと3年後の維持更新の手続きによって、3年間の延長を行うことができます。

維持確認審査時に提出する記録のサンプルは、次の通りです。なお、④～⑦の記録は、実施した場合に限ります。

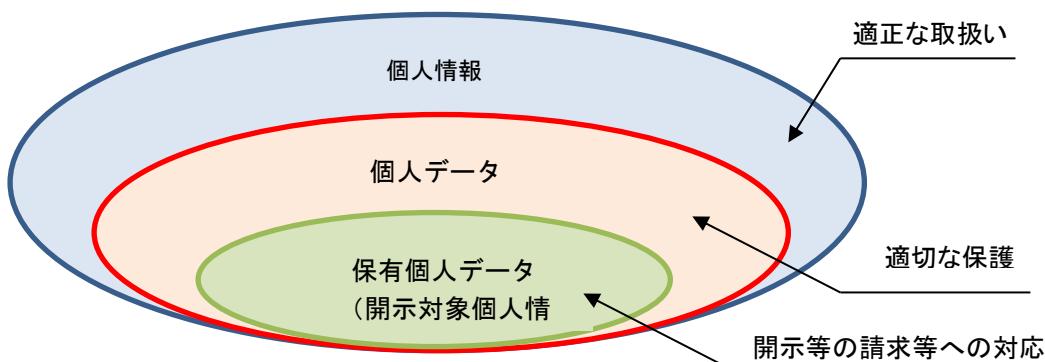
- ① PCS 年間計画
- ② 定期教育の計画及び結果報告
- ③ 運用の確認（自己点検）の報告
- ④ 重要な個人データの取扱記録
- ⑤ 委託先の再評価
- ⑥ 内部監査の計画及び結果報告
- ⑦ マネジメントレビュー

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 JISCA の適合性評価制度とでは、次の相違があります。

（1）保護の対象

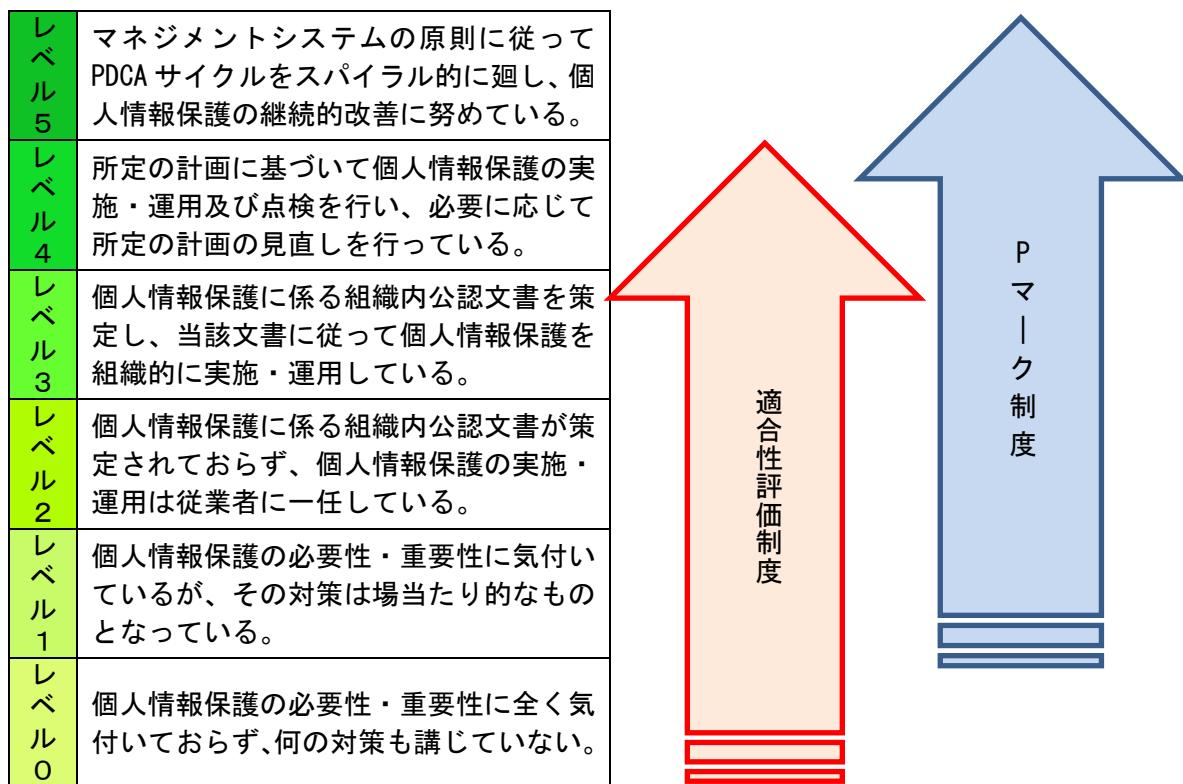
P マーク制度は、個人情報を保護の対象とし、法令等よりも高い保護レベルを要求しています。適合性評価制度は、個人データを保護の対象とし、法令等と同じ保護レベルを要求しています。個人情報の取扱いについても、法令等と同じレベルです。



図表 1-2 適合性評価制度の保護対象の構成

(2) 認定基準

Pマーク制度の認定基準は成熟度レベル5ですが、適合性評価制度の認定基準は成熟度レベル4となっています。Pマーク制度に比べ、ハードルが低く設定されています。

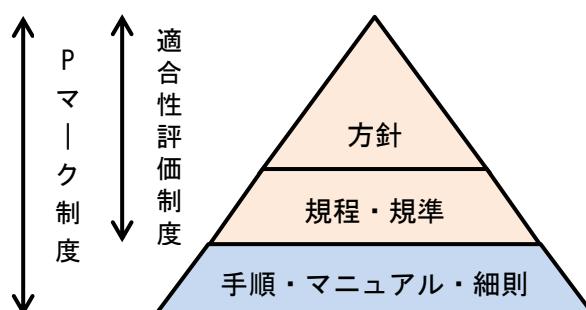


図表1-3 制度の認定基準

(3) 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。適合性評価制度は、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。

ただし、適合性評価確認書の交付を受けた事業者が、個人情報保護管理システムを継続して適切に維持改善していることを確認するために、1年毎に維持確認審査が必要です。



図表1-4 マネジメント文書の体系

(4) 準備期間

適合性評価制度は、適合性評価確認書の取得準備期間として概ね1~3ヶ月を要します。Pマーク制度に比べ、短期間で適合性評価確認書を取得できます。

(5) 費用（消費税込み）

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。

(6) 従業員数

Pマーク制度は、個人情報保護の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監査責任者の2名となっていきます。適合性評価制度は、個人情報保護の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、適合性評価制度の審査を受けることができます。

(7) リスク分析・評価

Pマーク制度は、全ての事業者に個人情報の取扱いの局面におけるリスクの分析・評価を求めています。適合性評価制度は、一定要件を満たす事業者に限定して、個人データの取扱いの局面におけるリスクの分析・評価を求めています。

(8) 審査技法

Pマーク制度は、事業者が規定した文書への準拠性審査の技法として、記録の閲覧、関係者への質問（対面インタビュー）、現場の観察を用いています。適合性評価制度は、事業者が規定した文書への準拠性審査の技法として、送付されたサンプル記録の閲覧と必要に応じたメール又は電話による関係者への質問を用います。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. 費用

適合性評価制度における文書審査と適合性評価確認書の交付にかかる料金は、業種、従業者数などによって異なります。

2. 1 料金表

単位：円（消費税抜き）

種別	新規の時			維持・更新の時		
	S 規模	M 規模	L 規模	S 規模	M 規模	L 規模
審査料 ^{注1注2注3}	45,000	75,000	105,000	25,000	40,000	60,000
確認書交付登録料 ^{注4}	15,000	15,000	15,000	15,000	15,000	15,000
合計	60,000	90,000	120,000	40,000	55,000	75,000

図表 2-1 料金表

2. 2 審査料

適合性評価制度の審査に係わる費用として必要です。審査料には、審査関係事務、文書審査、報告書作成などの各費用を含みます。申請後に JISCA からご請求いたします。

注 1： JISCA が認定した文書（記録を含む）の雛形を使用して申請した事業者に対しての審査料金です。JISCA 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、S、M、L 事業者それぞれ、3 万円、5 万円、7 万円の追加料金が発生します。

注 2： JISCA 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いては、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。

注 3： 新規時の審査料には、2 年度分の維持確認審査に係る料金が含まれています。

注 4： 適合性評価確認書が交付される場合（新規申請、更新申請）のみ、必要となります。1 年毎に行う維持確認審査には必要ありません。

2. 3 確認書交付登録料

JISCA からの交付適格決定通知後、ご請求いたします。

2. 4 事業者規模

従業者数と業種のみで判定します。

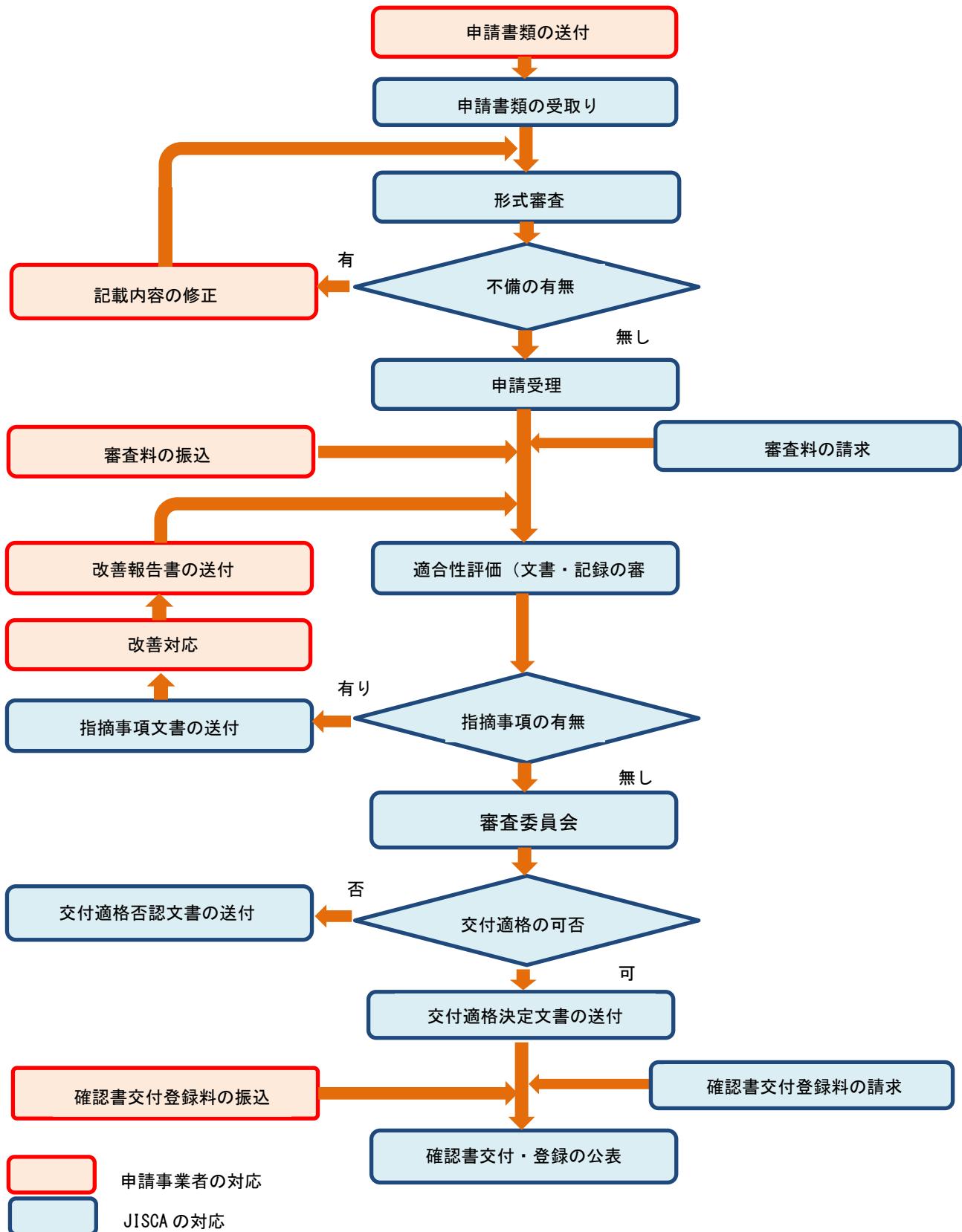
業種分類	従業者数		
	S 規模	M 規模	L 規模
製造業・その他	1～20 人	21～100 人	101 人～
卸売業	1～10 人	11～100 人	101 人～
小売業	1～5 人	6～100 人	101 人～
サービス業	1～10 人	11～100 人	101 人～

図表 2-2 事業者規模判定表

3. 申請・審査

3. 1 申請

3. 1. 1 申請の流れ



3. 1. 2 申請の手続き

JISCAへの申請に必要な書類は、下記の通りです。

No.	申請書類
1	個人情報保護法等適合性評価確認書交付審査申請書（様式-1）
2	会社概要（様式-2）
3	個人情報を取扱う業務の概要（様式-3）
4	全ての事業所の所在地及び業務内容（様式-4）
5	個人情報保護体制（様式-5）
6	個人情報保護管理システム（PCS）文書（内部規程・様式）の一覧（様式-6）
7	個人情報保護管理システム（PCS）要求事項との対応表（様式-7）
8	教育実施サマリー（様式-8）【全ての従業者に実施した教育実施状況】
9	監査実施サマリー（様式-9）【全ての部門に実施した監査実施状況がある場合】
10	事業者の代表者による見直し実施サマリー（様式-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（PCS）文書（内部規程・様式）一式（様式-6、様式-7に記載の内部規程・様式の全て。様式類は記入済みのサンプルのコピー（1～3枚））
13	個人データの取扱いの局面におけるリスク分析表（様式-11）【リスクが高い事業者のみ】

図表3-1 適合性評価申請書類一覧

※ 次に示す事項のいずれかに該当する事業者は、個人データが漏えい、滅失又は毀損した場合のリスクが高いと判断されるため、『リスク分析表』の提出が必要です。

- ① 事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が10,000を超える事業者
- ② 個人番号利用事務実施者
- ③ 委託を受けて個人データを取扱う事業者
- ④ 委託に基づいて個人番号関係事務又は個人番号利用事務を業務として行う事業者
- ⑤ 金融分野の事業者

※サービス内容や申請手続きの詳細は、下記にお問合せください

E-mail : kjht-ad@jisca.jp