# 適　合　証　明　書

下記の「受託者の条件」各項について、以下のとおり適合することを証明いたします。

日　　付：　　年　　月　　日
住　　所：
会 社 名：
代表者氏名：
社 員 数：（　　）人

Ⅰ　業務内容

| 項 | 受託者の条件 | 合否 | 合否判定の根拠となる事由 |
|---|---|---|---|
| 1 | 国際標準化機構が認証するＩＳＯ２７００１、一般財団法人日本情報経済社会推進協会が認定する「プライバシーマーク」又は「ＩＳＭＳ」を取得していること。 | | 「ＩＳＯ２７００１」、「プライバシーマーク」又は「ＩＳＭＳ」を取得していることを証明する書類を添付 |
| 2 | データプリント業務及び BPO 業務において ISO9001 の認証資格を取得していること。 | | 資格を取得していることが分かる書類を提出すること。 |
| 3 | 直近 2 年間の、各期 1 年間における決算について、債務超過になっていないこと。 | | 株式上場会社は金融商品取引法上の直近 2 年間の財務諸表、非上場会社は直近 2 年間の貸借対照表及び損益計算書を提出すること。 |
| 4 | 直近 2 年間に金融機関またはゆうちょ銀行から委託を受け、以下の全ての業務の事務局運営または本件仕様書と同様の実績があること。<br>・アンケート等の回答集約業務<br>・アンケート等の WEB 回答システムの構築<br>・抽選業務 | | 実績を証明できる書類の提出。（様式適宜） |
| 5 | データ処理業務を専門に行うための独立した施設を有すること。 | | その施設を証する書類を提出すること。（様式適宜） |
| 6 | 業務の受託・遂行にあたり社内ルールが定められており、業務遂行の体制が整備され統合的な管理が行えること。また、必要に応じ適宜見直しが行われていること。 | | 業務遂行体制、社内ルール及び必要に応じ適宜見直しが行われたことが確認できる書類を提出すること。（様式適宜） |
| 7 | ６の社内ルールについて、研修等により、業務処理を行う社員に徹底されていること。 | | 研修内容等、社員に対する周知・徹底が実施されていることが確認できる書類を提出すること（様式適宜） |
| 8 | 各拠点ごとに事業継続マネジメントシステム（ＢＣＭＳ）の国際規格ＩＳＯ２２３０１を取得しており、リスク管理体制（緊急時の製造等）を整備しており、緊急時のバックア | | 資格を取得していることがわかる書類を証明する書類または事業継続体制が整備されていることを証明する社内規定等の写しまたは BCP 及び継続的な見直し、運用等に |

| | | | |
|---|---|---|---|
| | *ップ施設を有すること。取得していない場合は、緊急時の事業継続体制が確立されており、効果的・効率的に運用できる仕組みが整備されていること。* | | *関する説明資料、及び機器の故障時や停電時又は災害時などの緊急時における緊急時対応計画書を提出すること。（様式適宜）* |
| *9* | *業務受託・遂行にあたり、自社又はグループ会社敷地内（日本国内）で完結すること。* | | *作業拠点の所在地を明記した資料（様式適宜）* |
| *10* | *業務遂行のためのルールが業務処理担当者に徹底される体制となっていること。また、その徹底状況が十分なこと。* | | *社内教育体制、研修の実施状況等がわかる書類を添付* |

Ⅱ　個人データの取扱いの全部又は一部を委託する場合

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 1 | セキュリティ管理を適切に行うため、委託業務を行う要員に対し、委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、その遵守状況を確認するルールを整備しているか。 | |
| 2 | セキュリティ管理状況及び、委託した業務が適切に遂行されているかを確認するため、委託業務の内容または作業の範囲に応じて、委託契約に基づき遂行状況を確認できる委託業務の管理体制を整備しているか。 | |
| 3 | 勘定系システムにおいて共同センターを利用する場合、緊急事態の発生時に迅速な初動対応が取れるよう、適切な安全対策を講じているか。 | |
| 4 | 個人データの安全管理に係る基本方針を策定し、以下の事項を定めているか。<br>（１）事業者の名称<br>（２）安全管理措置に関する質問及び苦情処理の窓口<br>（３）個人データの安全管理に関する宣言<br>（４）基本方針の継続的改善の宣言<br>（５）関係法令遵守の宣言 | |
| 5 ① | システムの安全対策を適切に実施するために、組織体制、関係者の役割及び管理すべき事項を明確にした規程類（セキュリティポリシー等）を策定し、適宜見直しているか。<br>※ セキュリティポリシーには、個人情報の取扱い及びその法令遵守に関する内容が盛り込まれていること | |
| 5 ② | 個人データの安全管理における以下の各管理段階に係る取扱規程を定めているか。<br>（１）取得・入力段階<br>（２）利用・加工段階<br>（３）保管・保存段階<br>（４）移送・送信段階<br>（５）消去・破棄段階<br>（６）漏えい事案等への対応の段階<br>※ 記憶装置等の故障等により、機器・部品を交換する場合、データ消去も含めた十分な管理を行うこと。 | |
| 5 ③ | 個人データの取扱状況の点検及び監査に関する規定が整備されているか。 | |
| 5 ④ | （受託業務を再委託する場合）受託業務に係る再委託に係る規程が整備されているか。 | |

| 項 | 受　託　者　の　条　件 | | 合・否 |
|---|---|---|---|
| 6 | ① | セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限及び責任について定めているか。 | |
| | ② | データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備しているか。<br>また、データ保管場所の固有のリスク（データ保管場所が海外の場合、適用される法令等）を考慮し、データ管理を行っているか。 | |
| 7 | ① | 個人データの安全管理に係る業務遂行の総責任者である個人データ管理責任者を設置しているか。 | |
| | ② | 個人データを取扱う各部署における個人データ管理者を設置しているか。 | |
| | ③ | 個人データ管理責任者は、次に掲げる業務を行っているか。<br>（１）個人データの安全管理に関する規程及び再委託先の選定基準の承認及び周知<br>（２）個人データ管理者及び「本人確認に関する情報」の管理者の任命<br>（３）個人データ管理者からの報告徴収及び助言・指導<br>（４）個人データの安全管理に関する教育・研修の企画<br>（５）その他個人情報取扱事業者全体における個人データの安全管理に関すること | |
| | ④ | 委託業務を所管する部署の個人データ管理者は、次に掲げる業務を行っているか。<br>（１）個人データの取扱者の指定及び変更等の管理<br>（２）個人データの利用申請の承認及び記録簿の管理<br>（３）個人データを取り扱う保管媒体の設置場所の指定及び変更等<br>（４）個人データの管理区分及び権限についての設定及び変更の管理<br>（５）個人データの取扱状況の把握<br>（６）再委託先における個人データの取扱状況等の監督<br>（７）個人データの安全管理に関する教育・研修の実施<br>（８）個人データ管理責任者に対する報告<br>（９）適用される国内外の法令等の遵守<br>（10）その他所管部署における個人データの安全管理に関すること | |
| 8 | ① | 個人データの安全管理に係る取扱規程に従った体制を整備し、運用を行っているか。 | |
| | ② | 取扱規程に規定する事項の遵守状況の記録及び確認を行っているか。 | |
| 9 | 次に掲げる事項を含む台帳を整備しているか。<br>（１）取得項目<br>（２）利用目的<br>（３）保管場所・保管方法・保管期限<br>（４）管理部署<br>（５）アクセス制限の状況 | | |
| 10 | ① | 個人データを取扱う部署が自ら行う点検体制を整備し、点検を実施しているか。<br>（１）個人データ取扱部署の点検責任者・点検担当者の選任<br>（２）点検計画の策定による体制整備<br>（３）定期的及び臨時の点検の実施<br>（４）点検の実施後において、規程違反事項等を把握したときは、その改善 | |
| | ② | 当該部署以外の者による監査体制を整備し、監査を実施しているか。<br>（１）個人データ取扱部署以外からの監査責任者・監査担当者の選任<br>（２）監査計画の策定による監査体制整備<br>（３）定期的及び臨時の監査の実施<br>（４）監査の実施後において、規程違反事項等を把握したときは、その改善 | |

| 項 | 受　託　者　の　条　件 | | 合・否 |
|---|---|---|---|
| 11 | ① | 漏えい事案等に対応する次に掲げる体制を整備しているか。<br>（１）対応部署<br>（２）漏えい事案等の影響・原因等に関する調整体制<br>（３）再発防止策・事後対策の検討体制<br>（４）自社内外への報告体制 | |
| | ② | 委託業務に係る漏えい事案等発生時に、委託元に対する速やかな報告を実施する体制を整備しているか。 | |
| | ③ | 使用するハードウェア及びソフトウェアについて、適切に管理・使用するための管理方法を明確にし、その内容を、テレワーク勤務者に周知徹底しているか。<br>（１）テレワークに使用する端末は、会社が許可したものに限ること<br>（２）テレワーク端末を家族と共用しないこと<br>（３）不特定多数の部外者が使用する端末をテレワークに使用しないこと<br>（４）テレワーク端末は、適切に管理し、盗難・紛失防止に努めること<br>（５）テレワーク端末で業務上利用可能と定められたアプリケーション、クラウドサービス等のみを業務に使用すること<br>（６）テレワーク端末へのインストールが許可されたアプリケーションについて、定められた場所（公式アプリケーションストア、アプリケーション提供企業の公式ホームページ等）からのみインストールすること | |
| 12 | ① | 従業者との間で採用時等に個人データの非開示契約等を締結しているか | |
| | ② | 従業者との個人データの非開示契約等の締結に際しては、以下の措置を講じているか<br>（１） 当該従業者との、業務上知り得た秘密に関する守秘義務を含む非開示契約の締結<br>（２） 非開示契約等の締結における非開示契約等の十分な説明、非開示契約等の書面を管理・保管する部署の明確化<br>（３）派遣社員を従事させる場合の、派遣社員本人との契約・覚書・念書等（電子的手段を含む）による守秘義務の規定<br>（４）従業者でなくなった後における非開示義務の遵守に関する非開示契約での規定。非開示義務に反した場合の責任の規定 | |
| | ③ | 就業規則等に、次に掲げる事項を定めているか<br>（１）個人データの取扱に関する従業者の役割・責任<br>（２）非開示契約違反時の懲戒処分 | |
| 13 | 従業者の役割・責任等の明確化のため、次に掲げる措置を講じているか<br>（１）各管理段階における個人データの取扱いに関する従業者の役割・責任の明確化<br>（２）個人データの管理区分及びアクセス権限の設定<br>（３）必要に応じた規程等の見直し | | |
| 14 | ① | 従業者へ次に掲げる措置を講じているか。<br>（１）従業者に対する採用時の教育及び定期的な教育・訓練<br>（２）個人データ管理責任者及び個人データ管理者に対する教育・訓練<br>（３）個人データの安全管理に係る就業規則等に違反した場合の懲戒処分の周知<br>（４）従業者に対する教育・訓練の評価及び定期的な見直し | |
| | ② | 従業者に対する教育・訓練の評価および定期的な見直しに当たって以下の事項に留意しているか。<br>（１）教育・研修担当部署の明確化<br>（２）教育・研修を計画的に実施できる体制の整備<br>（３）教育・研修の計画的な実施、実施状況の確認、新入社員や中途採用者が確実 | |

| 項 | 受　託　者　の　条　件 | | 合・否 |
|---|---|---|---|
| | | に教育・研修を受けられる体制の整備<br>（４）教育・研修が関連法令、自主ルールおよび内部規程等を従業者に対し周知徹底できる内容であること | |
| 15 | 個人データの利用者の識別・認証に関し、次に掲げる措置を講じているか。また、個人情報を取り扱う情報システムを利用する場合は、ユーザーＩＤ、パスワード、磁気・ＩＣカード等により、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する仕組みとなっているか。その他、サービスの内容及びリスク特性に応じて、多要素認証や多段階認証を検討しているか。<br>（１）本人確認機能の整備<br>（２）本人確認に関する情報の不正使用防止機能の整備<br>（３）本人確認に関する情報が他人に知らされないための対策<br>（４）本人確認要素(パスワード、トークンやIDカードなど認証機器、指紋などの身体情報、など)の配布時の適切な本人確認および、安全な経路での配布<br>（５）本人確認要素の紛失時や流出時の即時利用権限停止 | | |
| 16 | 個人データの管理に関し、次に掲げる措置を講じているか。<br>（１）従業者の役割・責任に応じた管理区分及びアクセス権限の設定<br>（２）アクセス権限所有者を特定し、漏えい等の発生に備えアクセスした者の範囲が把握できるような対応の実施<br>（３）事業者内部における権限外者に対するアクセス制御<br>（４）外部からの不正アクセスの防止措置<br>（５）アクセス可能な通信経路の限定<br>（６）外部ネットワークからの不正侵入防止機能の整備<br>（７）インターネットと接続する場合はファイアウォール等を設置し外部からの個人データへの不正アクセスから保護する措置をとること<br>（８）不正アクセスの監視機能の整備<br>（９）ファイアウォールにて不要なポートへの通信を閉塞すること | | |
| 17 | 個人データへのアクセス制限に関し、次に掲げる措置を講じているか。<br>（１）従業者に対する個人データへのアクセス権限の適切な付与及び見直し<br>（２）アクセス権限の付与方法の明定（アクセス権限の承認者及び認定作業者の明確化）<br>（３）アクセス権限の付与方法の明定（管理簿等によるアクセス権限の登録、変更、抹消記録の管理）<br>（４）アクセス権限の付与方法の明定（担当者の役割に応じたアクセス権限が適切に付与されているかの定期的な見直し）<br>（５）個人データへのアクセス権限を付与する従業者数を必要最小限に限定すること<br>（６）従業者に付与するアクセス権限を最小限に限定すること<br>（７）導入するパッケージソフト、アプリケーションソフト等について、納入前に既に登録されているアクセス権限を抹消すること<br>（８）アクセス権限を抹消できない場合は、当該アクセス権が設定されているIDを、管理台帳等を用いて管理し、管理者による適切な管理を実施すること<br>（９）（特権ＩＤを設定する場合）<br>従業者を限定し特別に留意すること<br>外部からアクセス可能な場合、限られた環境からのみアクセス可能とする等、対策を講じていること（デバイス認証やアクセス経路の限定等） | | |
| 18 | ① | 個人データの漏えい、き損等防止に関し、次に掲げる措置により個人データの保護策を講じているか。<br>（１）ファイルの不正コピーや盗難の際にも個人データの内容が分からないようにするための蓄積データの漏えい防止措置<br>（２）データ伝送時に盗聴された場合にもデータの内容が分からないようにするた | |

| 項 | 受 託 者 の 条 件 | | 合・否 |
|---|---|---|---|
| | | めの伝送データ漏えい防止策<br>（３）コンピュータウイルス等不正プログラムへの防御対策<br>（４）ウイルス対策ソフトウェアの導入、適用状況を一元的に管理する仕組みの構築<br>（５）ウイルス等の不正プログラムの検知対策<br>（６）ウイルス対策ソフトウェアのパターンファイル、検知ロジックを最新化する仕組みの構築<br>（７）ウイルス対策ソフトウェアのパターンファイル、検知ロジックが最新化されていることの定期的な確認<br>（８）上記（６）（７）を一元的に管理する仕組みの構築<br>上記（１）、（２）について、暗号化の仕様（暗号化対象項目、暗号化方式、暗号鍵の管理態勢等）を把握し、個人データの暗号化もれが無いようにすること。<br>なお、次に掲げる顧客の重要情報の暗号鍵は、ゆうちょ銀行が管理できるようにすること。<br>ア　暗証番号<br>イ　認証情報<br>ウ　クレジットカード情報（クレジットカード番号、セキュリティコード、暗証番号、有効期限）<br>エ　生体認証情報<br>オ　その他（本籍地等センシティブ情報） | |
| | ② | 次に掲げる措置により障害発生時の技術的対応・復旧手続の整備の措置を講じているか。<br>（１）不正アクセスの発生に備えた対応・復旧手続の整備<br>（２）コンピュータウイルス等不正プログラムによる被害時の対策<br>（３）リカバリ機能の整備 | |
| | ③ | テレワークを実施する場合は、テレワーク端末へのデータ保存・保管において、データの保護対策を講じているか | |
| 19 | 個人データへのアクセスを記録するとともに、当該記録の分析・保存を行っているか。<br>（１）ネットワークによるアクセス制御機能の整備<br>（２）アクセス制御機能の有効性の検証<br>（３）個人データへのアクセス及び個人データの取扱う情報システムの稼動状況についての記録・分析（例：ログインとログオフの状況、不正なアクセス要求、システムによって失効とされたIDなど）<br>（４）取得した記録についての漏えい防止等の観点からの適正な完全管理措置の実施<br>（５）取得した記録についての、特に漏えいリスクの高い時間帯（例：休日や深夜時間帯等）におけるアクセス頻度の高いケースについての定期的な分析の実施 | | |
| 20 | 個人データを取扱う情報システムの稼動状況を記録するとともに、当該記録の分析・保存を行っているか。<br>※ログ（システムログ、業務ログ、操作ログ等）の取得範囲・取得頻度・保存期間について、ゆうちょ銀行と予め確認、合意しておくこと。 | | |
| 21 | ① | 個人データを取り扱う情報システムの利用状況及び個人データへのアクセス状況を監視しているか。<br>また、サイバー攻撃に対するリスクの洗い出しと影響度の評価を行うための対応を考慮しているか。（TLPT の実施等） | |
| | ② | 上記①の監視状況についての点検及び監査を行っているか。 | |
| | ③ | セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策を行っているか。 | |

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 22 | 外国において個人データを取り扱う場合（外部事業者の運営するサーバに個人データを保存する場合を含む。再委託先での取扱いを含む）又は基準適合体制を整備していることを根拠として外国にある再委託先等に個人データを提供する場合、以下の内容について確認し、措置を講じているか。<br>※以下の内容については、ゆうちょ銀行と予め確認、合意しておくこと。<br>（１）委託する個人データを取り扱う外国の名称<br>（２）個人データの安全管理措置に影響を及ぼすおそれのある制度の有無・内容<br>（３）個人データの安全管理のために講じた措置 | |

Ⅲ　特定個人情報の取扱いの全部又は一部を委託する場合

| 項 | 受　託　者　の　条　件 | | 合・否 |
|---|---|---|---|
| 1 | 特定個人情報の安全管理に係る基本方針を策定し、以下の事項を定めているか。<br>（１）事業者の名称<br>（２）関係法令・ガイドライン等の遵守<br>（３）安全管理措置に関する事項<br>（４）質問及び苦情処理の窓口 | | |
| 2 | 以下の管理段階ごとに、特定個人情報の取扱方法、責任者・事務取扱担当者及びその任務等について取扱規程等を定めているか。<br>（１）取得段階<br>（２）利用段階<br>（３）保存段階<br>（４）提供段階<br>（５）削除・廃棄段階 | | |
| 3 | ① | 特定個人情報を取り扱う事務における責任者を設置し、その責任を明確化しているか | |
| | ② | 特定個人情報を取り扱う事務を行う担当者（事務取扱担当者）及び担当者の役割を明確化しているか | |
| | ③ | 事務取扱担当者が取り扱う特定個人情報の範囲は明確化されているか | |
| | ④ | 事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制は整備されているか | |
| | ⑤ | 情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制は整備されているか。 | |
| | ⑥ | 特定個人情報を複数の部署で取り扱う場合、各部署の任務分担及び責任が明確化されているか。 | |
| 4 | 取扱規程等に基づく運用を行うとともに、その状況を確認するため、次に掲げるような手法により、システムログ又は利用実績を記録しているか。<br>≪例示≫<br>（１）特定個人情報ファイルの利用・出力状況の記録<br>（２）書類・媒体等の持ち運びの記録<br>（３）特定個人情報ファイルの削除・廃棄記録<br>（４）削除・廃棄を再委託した場合、これを証明する記録等<br>（５）特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録 | | |
| 5 | 次に掲げるような事項を含む台帳を整備しているか。<br>≪例示≫<br>（１）特定個人情報ファイルの種類、名称<br>（２）責任者、取扱部署<br>（３）利用目的<br>（４）削除・廃棄状況<br>（５）アクセス権を有する者 | | |
| 6 | 情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備しているか。<br>≪例示≫<br>（１）事実関係の調査及び原因の究明<br>（２）再発防止策の検討及び決定<br>（３）委託元への速やかな報告 | | |

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 7 | 次に掲げるような手法により、特定個人情報の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組んでいるか。<br>≪例示≫<br>（１）特定個人情報の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する等<br>（２）外部の主体による他の監査活動と合わせて、監査を実施する等 | |
| 8 | 特定個人情報が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行っているか。 | |
| 9 | 次に掲げるような手法により、事務取扱担当者に、特定個人情報の適正な取扱いを周知徹底するとともに適切な教育を行っているか。<br>≪例示≫<br>（１）特定個人情報の取扱いに関する留意事項等について、従業者に定期的な研修等を行う等<br>（２）特定個人情報についての秘密保持に関する事項を就業規則等に盛り込む等 | |
| 10 | 特定個人情報の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（管理区域）及び特定個人情報を取り扱う事務を実施する区域（取扱区域）を明確に、次に掲げるような手法により、物理的な安全管理措置を講じているか。<br>≪例示≫<br>（１）管理区域について、入退室管理（ＩＣカード、ナンバーキー等による入退室管理システムの設置等）及び持ち込む機器の制限を行う<br>（２）取扱区域について、壁又は間仕切り等の設置及び座席配置の工夫を行う | |
| 11 | 管理区域及び取扱区域における特定個人情報を取り扱う機器、電子記録媒体及び書類等の盗難又は紛失等を防止するために、次に掲げるような手法により、物理的安全管理措置を講じているか。<br>≪例示≫<br>（１）特定個人情報を取り扱う機器、電子記録媒体又は書類等を、施錠できるキャビネット・書庫等に保管する等<br>（２）特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する | |
| 12 | 特定個人情報が記録された電子記録媒体又は書類等を持ち運ぶ場合、次に掲げるような手法により、容易に個人番号が判明しないよう安全な方策を講じているか。<br>※ 持ち運ぶ…特定個人情報を管理区域又は取扱区域の外へ移動させること<br>≪例示≫<br>（１）特定個人情報が記録された電子記録媒体を安全に持ち運ぶ方法としては、持ち運ぶデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等（ただし、行政機関等に法定調書等をデータで提出する際は、行政機関等が指定する提出方法に従うこと）<br>（２）特定個人情報が記載された書類等を安全に持ち運ぶ方法としては、封緘、目隠しシールの貼付、追跡可能な移送手段の利用等 | |

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 13 | 個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、次に掲げるような手法により、個人番号をできるだけ速やかに復元不可能な手法で削除又は廃棄する。個人番号若しくは特定個人情報ファイルを削除する場合、又は電子記録媒体等を廃棄する場合は、削除又は廃棄した記録を保存することとしているか。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認することとしているか。<br>≪例示≫<br>（１）特定個人情報が記載された書類等を廃棄する場合、焼却又は溶解、復元不可能な程度に細断可能なシュレッダーの利用、個人番号部分を復元不可能な程度にマスキングすること等の復元不可能な手段を採用する<br>（２）特定個人情報が記録された機器及び電子記録媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する等<br>（３）特定個人情報を取り扱う情報システム又は機器において、特定個人情報ファイルの中の個人番号又は一部の特定個人情報を削除する場合、容易に復元できない手段を採用する等<br>（４）特定個人情報を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する等<br>（５）個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める | |
| 14 | 情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するため、次に掲げるような手法により、適切なアクセス制御を行っているか。<br>≪例示≫<br>（１）個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する<br>（２）特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する<br>（３）ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を、事務取扱担当者に限定する | |
| 15 | 特定個人情報を取り扱う情報システムは、次に掲げるような手法により、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する仕組みとなっているか。また、サービスの内容及びリスク特性に応じて、多要素認証や多段階認証を検討しているか。<br>≪例示≫<br>（１）ユーザーＩＤ、パスワード、磁気・ＩＣカード等<br>（２）本人確認要素（パスワード、トークンや ID カードなど認証機器、指紋などの身体情報、など）の配布時の適切な本人確認および、安全な経路での配布<br>（３）本人確認要素の紛失時や流出時の即時利用権限停止 | |

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 16 | 次に掲げるような手法により、情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しているか。<br>≪例示≫<br>（１）情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する等<br>（２）情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する等<br>（３）導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する等<br>（４）機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする等<br>（５）ログ等の分析を定期的に行い、不正アクセス等を検知する等<br>（６）ウイルス対策ソフトウェアのパターンファイル、検知ロジックを最新化する仕組みを構築する等<br>（７）ウイルス対策ソフトウェアのパターンファイル、検知ロジックが最新化されていることを定期的に確認する等<br>（８）上記（６）（７）を一元的に管理する仕組みを構築等<br>（９）ファイアウォールにて不要なポートへの通信を閉塞すること | |
| 17 | 特定個人情報をインターネット等により外部に送信する場合、次に掲げる方法等により、通信経路における情報漏えい等及び情報システムに保存されている特定個人情報の情報漏えい等を防止するため以下の措置を講じているか。<br>（１）通信経路における情報漏えい等の防止策としては、通信経路の暗号化等<br>（２）情報システムに保存されている特定個人情報の情報漏えい等の防止策としては、データの暗号化及びパスワードによる保護等 | |

Ⅳ　委託先システム等当行以外が管理するシステム及び端末において個人データを取扱う場合
（当行が委託する顧客の個人データを、受託者等が管理するシステム及び端末を用いて取扱い、保管等する場合には以下項番に適合することを証明。なお、「受託者等が管理する」とは、再委託先や受託者が契約する受託者以外の外部サービス等も含むこととする）

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 1 | サイバーセキュリティについて各部署の役割・責任が明確化されているか。<br>≪合否判定の根拠となる事由≫<br>サイバー攻撃に対する未然防止措置や発生後のシステム対応、当行への報告等について受託者社内の各部署がどのような役割・責任を担っているかが記載された資料の提出 | |
| 2 | サイバーセキュリティについて経営陣に遵守状況が報告され、積極的に関与しているか。<br>≪合否判定の根拠となる事由≫<br>・サイバーセキュリティについて経営陣に遵守状況が報告され、積極的に関与していること<br>・サイバー攻撃に対し、金銭の支払いは厳に慎むべきとの姿勢であること<br>※資料の提出は不要 | |
| 3 | サイバーセキュリティについて、内部監査または外部監査を実施しているか。<br>≪合否判定の根拠となる事由≫<br>監査（予定）日、監査（予定）の概要が分かる資料の提出<br>※未実施の場合は、履行開始前の実施が必須 | |

| 項 | 受　託　者　の　条　件 | 合・否 |
|---|---|---|
| 4 | サイバーセキュリティの観点からリスクの洗い出し及び影響度の評価が行われ、適切に管理されているか。<br>≪合否判定の根拠となる事由≫<br>　サイバーセキュリティに対して、想定されるリスク及びその影響度の評価が記載された資料の提出 | |
| 5 | サイバーセキュリティに関する脅威や脆弱性等の情報を収集する体制があり、影響確認及びパッチ適用等の対処、台帳等による管理を行っているか。また、情報の収集にあたり専門機関等との情報共有を行う場合、情報を適切に管理するための共有方針、共有プロセスを定めているか。<br>≪合否判定の根拠となる事由≫<br>　脅威や脆弱性等の情報を収集、影響確認を行い、速やかに対処する体制があること<br>※資料の提出は不要 | |
| 6 | 従業者に対し、目にとまりやすい方法でサイバーセキュリティについての教育・周知を行っているか。<br>≪合否判定の根拠となる事由≫<br>　実施（予定）日、実施（予定）概要が分かる資料の提出<br>≪教育内容の例≫<br>〈標的型攻撃メール〉<br>　・攻撃の概要と対処方法（不審なメールの特徴、開封時の留意点、ウイルス感染した場合の報連相等）<br>〈不正アクセス〉<br>　・攻撃の概要と対処方法（発生した場合の報連相等）<br>※未実施の場合は、履行開始前の実施が必須 | |
| 受託者の管理する既存システム等を使用する場合（委託業務に新たなシステム構築を含まない場合） | | |
| 社外からのメールが受信できる端末を使用する場合（当行が委託する顧客の個人データを保有するシステムにアクセス可能なメール利用端末も含む） | | |
| 7 | 通信を監視し、不審なメール等を検知・遮断する機能があるか。<br>≪合否判定の根拠となる事由≫<br>　不審なメール等を自動的に検知・遮断する機能（以下の例を参照）を記載して提出<br>≪検知・遮断する機能の例≫<br>　・メール送信元のアドレス等で遮断するフィルタリング機能　等 | |
| 8 | 侵入されることを前提とした被害発生時の対処フローが整備されているか。<br>≪合否判定の根拠となる事由≫<br>　対処フローが文書化されていること<br>※資料の提出は不要 | |
| 9 | 電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針が明確にされているか。<br>≪合否判定の根拠となる事由≫<br>　運用方針が文書化されていること<br>※資料の提出は不要 | |
| 10 | 業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、不正使用防止対策が講じられているか。<br>≪合否判定の根拠となる事由≫<br>　不正使用防止策を記載して提出<br>≪不正使用防止策の例≫<br>　メールフィルタリング機能の導入、ホワイトリスト方式によるホームページの閲覧制限　等 | |

| 項 | | 受　託　者　の　条　件 | 合・否 |
|---|---|---|---|
| | インターネットに接続するシステムを使用する場合 | | |
| | 11 | 通信を監視し、不審な通信を検知・遮断、またはDLP等によるセキュリティ対策を講じることが可能か。<br>≪合否判定の根拠となる事由≫<br>　不審な通信を検知・遮断する機器等の名称（以下の例を参照）、または講じているDLP等のセキュリティ対策を記載して提出<br>≪検知・遮断する機器等の例≫<br>　・FW、IDS/IPS、WAF | |
| | 12 | セキュリティ診断を実施しているか。<br>≪合否判定の根拠となる事由≫<br>　実施（予定）日、実施（予定）診断項目が分かる資料の提出<br>≪診断項目の例≫<br>　・ネットワーク診断、Webアプリケーション診断、サーバ構成診断、ペネトレ―ションテスト<br>※未実施の場合は、履行開始前の実施が必須 | |
| | 13 | 不正アクセス等を検知、監視する体制及び被害発生時の対処フローが整備されているか。<br>≪合否判定の根拠となる事由≫<br>　対処フローが文書化されていること<br>※資料の提出は不要 | |
| | 14 | クラウドサービス契約のように他社とリソースを共有する場合、他社のシステムへのサイバー攻撃が、当該システムに与えるリスクを認識しているか。<br>≪合否判定の根拠となる事由≫<br>　どのようなリスクがあるか認識していること<br>※資料の提出は不要 | |
| | 15 | 不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、ネットワーク構成情報を適切に管理しているか。<br>また、外部ネットワークからアクセス可能な機器へのセキュリティパッチの適用やファイアウォールにおける不要なポートの閉塞等の対応を実施し、感染を防止しているか。<br>≪合否判定の根拠となる事由≫<br>　・通信経路、通信関連機器等を最小限とし、ネットワーク構成情報を適切に管理していること<br>　・外部ネットワークからアクセス可能な機器へのセキュリティパッチの適用やファイアウォールにおける不要なポートの閉塞等の対応を実施し、感染を防止していること<br>※資料の提出は不要 | |

（注１）「合・否」判定にあたっては、「〇」又は「×」を記入し、該当しない場合には「－」を記入してください。また、現在未措置でも、履行を開始するまでに措置する場合には、「実施予定日」を記載してください。
（注２）証明書類の添付を必要とする場合は、「合・否」欄に添付書類名を記述してください。
（注３）受託者には責任者等の管理体制、個人情報の管理状況について、必要に応じて書面で提出をしていただく場合があります。
（注４）提出した内容に虚偽があることが判明した場合又は報告について、書類の提出を当社から求められたにもかかわらず提出がなされない場合には、契約条項に違反したものとみなし契約の解除を行います。
（注５）本件に係る諸経費は提出者の負担とします。

（注６）実施予定日を資料に書く場合、例えば、委託業務の実施が数か月以上先の場合等、中長期の準備が許される場合は、予定日ではなく、予定月でも構いません。

（注７）例等として挙げているのは、受託者において証明内容を捉えやすいよう当行が想定している一般的な例を示しているものであり、これに限定する意図ではありません。

（注８）当証明書における用語の定義は以下のとおりとします。

| 用語 | 定義 |
|---|---|
| サイバー攻撃 | システムやネットワークへの不正侵入等を行い、情報の改ざん・破壊・窃取、サービスの安定稼働を妨害する等を行うこと。 |
| サイバーセキュリティ | サイバー攻撃等からシステムやネットワークの安全を確保すること。 |
| 標的型攻撃メール | 特定の組織や個人を狙い、情報の詐取等を目的に攻撃者が送信する電子メール。受信者が添付ファイルを開封、または電子メールの中に書かれたURLを受信者がクリックすることによりウイルスがダウンロードされることで攻撃が開始される。 |
| 脆弱性 | サーバ等のハードウェアの設定やアプリケーション、OS等のソフトウェアのセキュリティ上の不備・欠陥のことであり、情報の改ざん・破壊・窃取、システムの破壊等を行う攻撃に悪用される。 |