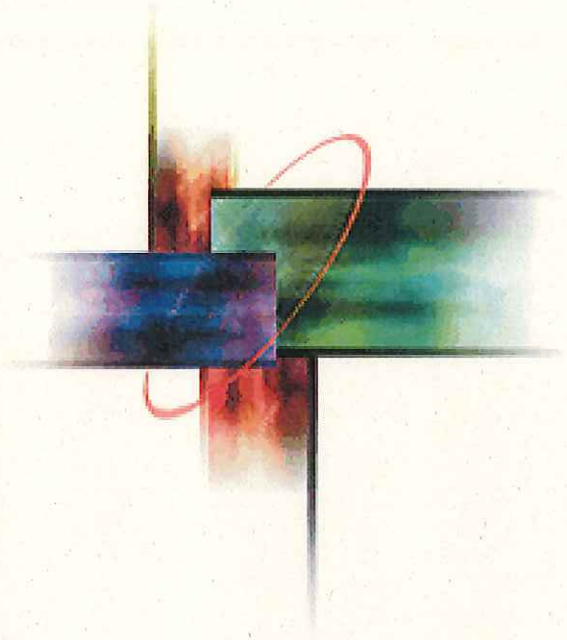
第36回社会保障審議会年金事業管理部会
平　成　３　０　年　６　月　４　日

資料1－3

別添資料
1－2



日本年金機構 御中

「委託業務における情報持ち出し可能性に関する調査」の評価業務 報告書

平成 30 年 5 月 11 日

ＴＩＳ株式会社

目　次

はじめに

本書は、日本年金機構（以降「機構」という。）から提示された「委託業務における情報持ち出し可能性に関する調査」の評価業務 調達仕様書に基づき、評価業務を実施した結果報告書である。

日本アイ・ビー・エム株式会社（以降「日本ＩＢＭ」という。）が行った調査は、機構の「扶養親族等申告書・個人番号申出書データ入力及び画像化業務」受託事業者が、機構との契約で再委託禁止とされていた主体的業務を、機構に無断で海外の事業者に再委託していた事象の発見を受け、再委託先事業者へ渡った情報の範囲、受託事業者および再委託先事業者による情報の持出し有無を調べる調査であったが、日本ＩＢＭの調査開始時点において、すでに再委託業務は終了しており、再委託期間に遡った調査に必要なログ取得などが十分に行うことができない状況であったと推察される。また、海外にある再委託先事業者に対する調査については、再委託先事業者は機構と直接の契約関係にはなっておらず、第三者としての調査協力であり、情報の取扱いに係わる情報セキュリティ体制と関係作業の運用実態の調査範囲には、制約があったものと考えられる。

本評価結果の報告は、日本ＩＢＭが調査にあたり機構からどのような事前情報の提供を受け、調査目的ならびに調査対象、調査方法を決定したのかといった、調査プロセスの適切性をまず評価し、その後、調査対象機器や調査対象機器ごとの調査技法について妥当性の評価を行ったものである。

また、本報告書において斜体字にて表記された文章は、日本ＩＢＭが作成した「株式会社 SAY 企画委託業務における情報持ち出し可能性に関する調査結果報告書（以降「調査結果報告書」という。）」から引用を行っている。

なお、本報告書には、今回の評価対象範囲における情報セキュリティ上の潜在的なリスクに関する内容が含まれているため、取扱いには注意が必要と考える。

1. 本業務における評価結果

当社は、日本ＩＢＭが作成した調査結果報告書の評価を行い、以下の結論を得た。

1.1. 調査対象範囲について

日本ＩＢＭの調査対象範囲は、個人情報保護マネジメントシステム（JIS Q 15001:2017）に定義されている個人情報のライフサイクルに基づく取扱場所、取扱機器等について評価人が整理した内容および機構と日本ＩＢＭの調査における役割分担、調査時点および機構と再委託先事業者との関係を考慮すると、調査目的達成のために必要な範囲として妥当であると評価できる。

○日本ＩＢＭの調査対象範囲(P10 表 3.2-4)
- 受託事業者　　：業務状況確認、ファイルサーバー、管理サーバー、業務用 PC、画像切り出しに関わる運用状況
- 再委託先事業者：セキュリティ管理体制の確認、セキュリティ管理の実施の確認、情報の管理、情報セキュリティへの対応

1.2. 調査方法について

日本ＩＢＭが選定した調査方法について、評価人は「情報セキュリティ監査手続ガイドラインを利用した監査手続策定の手引（経済産業省）」において示されている監査技法に照らし、調査対象ごとに適切な調査方法が選定されており、調査時点および機構と再委託先事業者との関係を考慮すると、調査目的に対して有効であると評価できる。

○日本ＩＢＭの調査方法（P12 表 3.3-1、表 3.3-2）

1)受託事業者に対する調査方法の確認

表 3.3-1　受託事業者に対する調査方法の確認

調査対象	調査方法	評価結果
業務状況確認	*調査人によるヒアリング*	有効※1
ファイルサーバー運用状況 *管理サーバー運用状況*	*調査人によるヒアリング* *調査人による目視確認*	有効
ファイルサーバーログ状況 *管理サーバーログ状況*	*調査人によるヒアリング* *調査人による目視確認* *管理サーバーから Security イベントログを抽出し、調査*	有効 ※2
ファイルサーバー設定状況	*ヒアリング* *調査人による目視確認*	有効
画像切り出しに関わる運用状況	*調査人によるヒアリング* *実機および実データを使用した再現テストの実施および調査人による立ち会い* *調査人による目視確認*	有効
業務用 PC	*情報取り出しの有無を分析可能な以下の情報を取得。* *・ログ* *・設定*	有効

※1 情報セキュリティ監査では、ヒアリングによる「業務状況確認」を確実なものとするために作業手順書や業務フローとの照らし合わせを行うことがあるが、今回はファイルサーバーや業務 PC の調査のための状況把握が目的であるため、評価人は、前述の照らし合わせが無くとも良いと考える。

※2 ログ調査に用いるログ情報の正確性を確認するために、調査人が想定する内容がログに記録される設定となっていることを再実施により確認（実機を用いて異常系の操作を実施し、ログが記録されることを確認）する技法もあるが、

評価人は、調査人が実機に変更を加えることなく調査を行うために選択した技法は妥当であると考える。

2)再委託先事業者に対する調査方法の確認

表 3.3-2　再委託先事業者に対する調査方法の確認

調査対象	調査方法	評価結果
セキュリティ管理体制の確認	*調査人による運用規程に関するヒアリング* *調査人による規定文書の目視確認および表紙写真*	有効
セキュリティ管理の実施の確認	*調査人によるヒアリング* *調査人による作業部屋の目視確認と可能な限りの写真撮影（作業部屋など）*	有効
情報の管理	*調査人による作業運用手順と人的な対応のヒアリング* *調査人による作業運用手順文書の確認*	有効
情報セキュリティへの対応（設定と事件/事故対応）	*調査人によるネットワーク機器に関するヒアリング* *調査人によるネットワーク機器設定の目視確認* *ネットワーク機器設定画面キャプチャ* *ネットワーク機器の写真*	有効

1.3. 調査の結果について

日本ＩＢＭの調査については、上記 1.1 および 1.2 のとおり、調査対象範囲および調査方法は妥当および有効であると評価できることから、その調査結果から日本ＩＢＭが導き出した以下の結論については、評価人が確認した範囲においては、信頼性があると評価できる。

- *受託事業者および再委託先事業者から情報の流出は生じていないと判断した。*
- *受託事業者から中国の再委託先事業者に送付されていた情報は、「氏名とフリガナ」のみであった。*

○日本ＩＢＭの調査目的の達成度（P24）

評価人は、調査を取り巻く環境を考慮すると、日本ＩＢＭの調査対象の選定、調査方法の選定、調査結果には一定の妥当性、有効性があり、日本ＩＢＭは最大限取り得る技法をもって調査を行っており、「*情報の持ち出しが生じている可能性を評価すること*」という調査目的は達成されていると評価した。

評価人が確認した範囲においては、日本ＩＢＭが導き出した「*受託事業者から中国の再委託先事業者に送付されていた情報は、「氏名とフリガナ」のみであった。*」との結論については、信頼性があると評価できる。

2. 評価の実施方針

当社は、「委託業務における情報持ち出し可能性に関する調査の評価業務 調達仕様書（平成 30 年 4 月）」に基づき、以下のとおり評価を実施した。

2.1. 本評価業務の範囲

2.1.1. 評価業務の目的・範囲

「扶養親族等申告書・個人番号申出書データ入力及び画像化業務」の受託事業者において、機構との契約で再委託禁止とされていた主体的業務を、機構に無断で海外の事業者に再委託していたことが確認されたことを受け、機構は、日本ＩＢＭに受託事業者及び再委託先事業者における情報持ち出し可能性に関する調査を委託した。

本業務は、日本ＩＢＭが取りまとめた調査結果報告書の内容を確認し、調査対象の選定や調査方法が、調査目的や調査環境等に照らし、合理的であるか客観的な評価を行うことを目的とする。

2.1.2. 評価実施体制

本業務の実施体制を下表に示す。評価人はいずれも情報セキュリティ監査の経験を有しており、評価人１は独立行政法人における最高情報セキュリティアドバイザーの経験、複数の独立行政法人における情報セキュリティインシデント対応支援の経験を有している。

表 2.1-1　評価実施体制

所属組織	評価人	役職
TIS 株式会社 サービス事業統括本部 プラットフォームサービス事業部 エンタープライズセキュリティサービス部	評価人１	フェロー
	評価人２	主任
	評価人３	主任補

2.1.3. 評価の方法

評価人は、日本ＩＢＭが受託事業者および再委託先事業者に対して実施した調査について、ISO/IEC 27001 等の関連する基準やガイドラインとの整合性、本調査における調査目的と調査人の役割および調査人が保有する専門的知見を勘案し、調査結果報告書に記載されている調査対象、調査方法および調査人が導き出した結論（調査結果）の妥当性を評価する。

2.1.4. 評価の制限

評価人が評価にあたって確認した文書は以下のとおりである。なお、記載以外の文書・記録その他の証跡については評価時点に確認できなかったことから評価していない。

株式会社 SAY 企画委託業務における情報持ち出し可能性に関する調査結果報告書
（文書番号：AA17031401-089PF0）
付録１：現地調査項目と確認結果
付録２：現地調査のエビデンス写真

3. 評価の詳細

3.1. 調査プロセスの適切性

3.1.1. 機構からの情報提供

評価人は機構へのヒアリングにより、日本ＩＢＭに対し機構が以下の情報提供を行ったことを確認した。

1) 機構監査部が実施した業務監査に日本ＩＢＭも同行し情報を共有

2) 受託事業者の運用仕様書、ネットワーク構成図等の事前開示

3) 日本ＩＢＭへの調査依頼に至った経緯の説明資料

3.1.2. 調査目的や調査範囲の決定等に係る諸プロセスの迅速性、柔軟性

評価人は機構へのヒアリングにより、前項に示した機構からの情報提供内容を踏まえて日本ＩＢＭと機構が調査前に調査目的、調査範囲の合意を取り交わしたこと、現地での調査中に知りえた運用実態に応じて、調査対象の特定や調査方法の選択を行ったことを確認した。

評価人は、本調査にあたっては、限られた期間の中での合意形成が必要であり、受託事業者および再委託先事業者の情報取扱い環境が現地に赴かなければ不明確である状況の中で調査遂行が求められる状況であったことから、事前の合意形成は迅速に行う必要があり、現地での柔軟な対応が行わなければならなかったと評価した。

3.1.3. 現地調査開始までの準備プロセスの適切性

評価人は機構へのヒアリングおよび日本ＩＢＭの調査結果報告書に基づき、日本ＩＢＭが現地調査開始前に作業の正確性の担保および調査人による作業のばらつき防止するために、以下の準備を行っていることから、日本ＩＢＭが実施した準備プロセスは適切であると評価した。

1) 受託事業者の全業務 PC の調査にあたって必要となる保全用デバイスの構成作業
   - 保全用スクリプトの検証と調整および保全作業の計画と手順の確認

2) 再委託先事業者へのヒアリングに用いる調査チェックリストの作成

3.2. 日本ＩＢＭによる調査対象範囲の妥当性

3.2.1. 調査対象選定の合理性の評価にあたっての整理

日本ＩＢＭが実施した調査は「*情報持ち出し可能性に関する調査*」であり、ここでの「情報」とは「個人情報」である。そこで、評価人は、個人情報を事業の用に供している、あらゆる種類、規模の事業者に適用できる個人情報保護マネジメントシステム（JIS Q 15001:2017）を用いて、受託事業者および再委託先事業者における個人情報のライフサイクルを明らかにし、評価人として調査が必要と思われるライフサイクルの局面ごとに取扱場所、取扱機器等を整理することにした。

3.2.2. 評価人の想定する調査対象範囲

評価人は、委託先事故発生時におけるインシデント対応において、機構と外部専門家の役割は以下のとおりと捉えている。

表 3.2-1　委託先事故発生時の機構と外部専門家における役割分担

主体者	役割	分類
機構	受託事業者に機構が要求した事項に対する遵守状況の確認	組織面 業務面
外部専門家	機構が行う上記確認において専門的な知識・技術が必要となる範囲の確認支援	技術面

本調査にあたり、外部専門家である日本ＩＢＭは、「受託事業者の遵守状況の確認において専門的な知識・技術が必要となる範囲」を確認する役割を担っていたと考えられる。

そこで、評価人は、受託事業者および再委託先事業者における個人情報のライフサイクルの局面ごとに取り扱われる個人情報の形態（紙媒体・電子データ）と、個人情報の取り扱いに使用される機器を洗い出し、「受託事業者の遵守状況の確認において専門的な知識・技術が必要となる範囲」の想定を行った。

評価人が行った洗い出しの結果を「表 3.2-2　受託事業者における個人情報のライフサイクル」「表 3.2-3　再委託先事業者における個人情報のライフサイクル」に整理し、評価人が想定した調査対象範囲を赤枠破線で囲む。

表 3.2-2　受託事業者における個人情報のライフサイクル

ライフサイクル	形態	使用機器
取得・入力	紙媒体	－
	電子データ	スキャナ・OCR 業務用 PC
移送・送信	紙媒体	－
	電子データ(送信)	ファイルサーバー 社員用 PC クラウドストレージ

ライフサイクル	形態	使用機器
	電子データ(移送・納品)	外付け HDD DVD-R
利用・加工	紙媒体	スキャナ
	電子データ	スキャナ・OCR 業務用 PC ファイルサーバー 作業員用 PC 社員用 PC
保管・バックアップ	紙媒体	－
	電子データ	ファイルサーバー
消去・廃棄	紙媒体	－

表 3.2-3　再委託先事業者における個人情報のライフサイクル

ライフサイクル	形態	使用機器
取得・入力	紙媒体	－
	電子データ	クラウドストレージ 情報受け渡し専用 PC
移送・送信	紙媒体	－
	電子データ(送信・納品)	情報受け渡し専用 PC クラウドストレージ
	電子データ(移送)	－
利用・加工	紙媒体	－
	電子データ	サーバー 作業 PC
保管・バックアップ	紙媒体	－
	電子データ	サーバー
消去・廃棄	－	－

3.2.3. 日本ＩＢＭの調査対象範囲の評価

1) 評価人が想定した調査対象範囲と日本ＩＢＭの調査対象範囲の比較

評価人は、前項で整理した評価人の想定した調査対象範囲と、日本ＩＢＭの調査対象範囲を照らし合わせた。その結果について、「表 3.2-4　調査対象範囲の比較」に示すとおり、評価人の想定した調査対象範囲と日本ＩＢＭの調査対象範囲との差異を確認した。

差異となっている部分を赤枠破線で囲む。

表 3.2-4　調査対象範囲の比較

	評価人が想定した調査対象範囲	日本ＩＢＭの調査対象範囲	差異
受託事業者	運用状況の確認	*業務状況確認*	無
	ファイルサーバー	*ファイルサーバー（設定状況、運用状況、ログ状況）*	無
	—	*管理サーバー（設定状況、運用状況、ログ状況）*【差異①】	有
	クラウドストレージ【差異②】	—	有
	スキャナ【差異③】	—	有
	スキャナ・OCR 業務用 PC	*業務用 PC*	無
	社員用 PC	*画像切り出しに関わる運用状況* *業務用 PC*	無
	作業員用 PC	*業務用 PC*	無
	外付け HDD【差異④】	—	有
	DVD-R【差異⑤】	—	有
再委託先事業者	運用状況の確認	*セキュリティ管理体制の確認* *セキュリティ管理の実施の確認* *情報の管理* *情報セキュリティへの対応（設定と事件/事故対応）*	無
	サーバー【差異⑥] クラウドストレージ 情報受け渡し専用 PC 作業 PC	—	有

2) 差異の要因と評価

調査対象範囲の比較の結果、差異が生じている部分について、その要因と評価人の評価を以下にまとめる。

差異①：評価人が作成した「表 3.2-2　受託事業者における個人情報のライフサイクル」は、個人情報の取扱い場面から調査対象機器を想定したものであり、直接個人情報を取扱うことがない Windows ドメインコントローラーおよび Active Directory サービスを提供する管理サーバーは、評価人の想定した調査対象範囲に入っていなかった。ただし、個人情報を直接取扱うことがない機器であっても、スキャナ・OCR 業務用 PC や社員用 PC、作業員用 PC などのアクセス制御や PC 利用状況を把握するために必要なものであることから調査対象として、妥当である。

差異②：クラウドストレージは、再委託先事業者が契約主体となり、日本ＩＢＭの調査実施時点では、受託事業者と再委託先事業者間の業務委託は既に終了していたため日本ＩＢＭの調査対象範囲に含まれていなかったと考えられる。そのため、

日本ＩＢＭの調査実施時点において、クラウドストレージは調査を行うことができないことから、調査対象範囲に含まれていないことはやむを得ない。

差異③：スキャナは紙媒体に記載されている文字情報を画像データに変換するために使用する専用機器であり、スキャナ本体にデータ保存を行っていないことを機構が確認を行っていることを機構へのヒアリングにより確認したことから、日本ＩＢＭの調査対象範囲に含まれていないことは妥当である。

差異④：外付け HDD は、電子記録媒体としての管理状況を機構が確認を行っていることを機構へのヒアリングにより確認したことから、日本ＩＢＭの調査対象範囲に含まれていないことは妥当である。

差異⑤：DVD-R は、電子記録媒体としての管理状況を機構が確認を行っていることを機構へのヒアリングにより確認したことから、日本ＩＢＭの調査対象範囲に含まれていないことは妥当である。

差異⑥：再委託先事業者は機構と直接の契約関係にはなっておらず、第三者としての調査協力であり、情報の取扱いに係わる情報セキュリティ体制と関係作業の運用実態の調査の範囲に制約があるため日本ＩＢＭの調査対象範囲に含まれていなかったと考えられる。再委託先事業者に対する強制的な調査は行えないことから、日本ＩＢＭの調査対象範囲にサーバー、クラウドストレージ、情報受け渡し専用 PC、作業 PC を含めていないことはやむを得ない。
なお、日本ＩＢＭは運用状況についてヒアリングにより確認を行うことで、サーバー等についても一定の調査を行っていることを調査結果報告書にて確認している。

さらに、機構へのヒアリングによって日本ＩＢＭに対する調査依頼の内容を確認し、機構の調査依頼対象範囲と日本ＩＢＭの調査対象選定範囲に差異がないことを確認した。

3) 評価人の出した結論

前項に記載の通り、評価人が想定した調査対象範囲と日本ＩＢＭの調査対象範囲で差異が生じている調査対象は、調査の必要があり調査対象としたもの、機構で確認が行われている、もしくは機構と再委託先事業者との関係から調査対象に含めていないものであることから、日本ＩＢＭの調査対象範囲は、妥当と評価できる。

3.3. 日本ＩＢＭによる調査方法の有効性

3.3.1. 評価対象ごとの調査方法の選定

評価人は、日本ＩＢＭが実施した「情報持ち出し可能性に関する調査」に用いた調査方法の評価にあたり、「情報セキュリティ監査手続ガイドラインを利用した監査手続策定の手引（経済産業省）」の「1.3 監査手続の選択(※)」を参照し、調査対象に対する調査方法の有効性を評価した。

※「情報セキュリティ監査手続ガイドラインを利用した監査手続策定の手引（経済産業省）」では、監査技法の種類として、閲覧（レビュー）、観察（視察）、質問（ヒアリング）、再実施が適宜選択されると記載されている。

1) 受託事業者に対する調査方法の確認

表 3.3-1　受託事業者に対する調査方法の確認

調査対象	調査方法	評価結果
業務状況確認	*調査人によるヒアリング*	有　効 ※1
ファイルサーバー運用状況 *管理サーバー運用状況*	*調査人によるヒアリング* *調査人による目視確認*	有　効
ファイルサーバーログ状況 *管理サーバーログ状況*	*調査人によるヒアリング* *調査人による目視確認* *管理サーバーから Security イベントログを抽出し、調査*	有　効 ※2
ファイルサーバー設定状況	*ヒアリング* *調査人による目視確認*	有　効
画像切り出しに関わる運用状況	*調査人によるヒアリング* *実機および実データを使用した再現テストの実施および調査人による立ち会い* *調査人による目視確認*	有　効
業務用 PC	*情報取り出しの有無を分析可能な以下の情報を取得。* *・ログ* *・設定*	有　効

※1 情報セキュリティ監査では、ヒアリングによる「業務状況確認」を確実なものとするために作業手順書や業務フローとの照らし合わせを行うことがあるが、今回はファイルサーバーや業務 PC の調査のための状況把握が目的であるため、評価人は、前述の照らし合わせが無くとも良いと考える。

※2 ログ調査に用いるログ情報の正確性を確認するために、調査人が想定する内容がログに記録される設定となっていることを再実施により確認（実機を用いて異常系の操作を実施し、ログが記録されることを確認）する技法もあるが、評価人は、調査人が実機に変更を加えることなく調査を行うために選択した技法は妥当であると考える。

2) 再委託先事業者に対する調査方法の確認

表 3.3-2　再委託先事業者に対する調査方法の確認

調査対象	調査方法	評価結果
セキュリティ管理体制の確認	*調査人による運用規程に関するヒアリング* *調査人による規定文書の目視確認および表紙写真*	有　効
セキュリティ管理の実施の確認	*調査人によるヒアリング* *調査人による作業部屋の目視確認と可能な限りの写真撮影（作業部屋など）*	有　効

調査対象	調査方法	評価結果
情報の管理	*調査人による作業運用手順と人的な対応のヒアリング* *調査人による作業運用手順文書の確認*	有　効
情報セキュリティへの対応(設定と事件/事故対応)	*調査人によるネットワーク機器に関するヒアリング* *調査人によるネットワーク機器設定の目視確認* *ネットワーク機器設定画面キャプチャ* *ネットワーク機器の写真*	有　効

3) 評価人が出した結論

評価人は、日本ＩＢMが選定した調査対象に対する調査方法は、調査目的に対して有効であると評価した。

3.4. 「扶養親族等申告書･個人番号申出書」関連情報を保管するサーバーおよびネットワーク関連の調査結果の妥当性

3.4.1. 運用状況のヒアリング（調査結果報告書 P6～P7）

1) 日本ＩＢMの調査結果

評価人は、日本ＩＢMの調査結果報告書に記載のある運用状況のヒアリングにおいて日本ＩＢMが実施した調査結果を確認した。

① 「扶養親族等申告書・個人番号申出書」の「氏名とフリガナ」情報のみを再委託先事業者に処理を再委託している。

② 「氏名とフリガナ」はシステムにより切り出し処理している。

③ 再委託先事業者に「氏名とフリガナ」情報を送る際、通常はケーブルを外して切断しているインターネットを一時的に接続し実施している。

④ 業務PCへのUSB禁止ソフトの導入が進んでいない。

⑤ 業務PCへの操作ログ取得ソフトの導入が進んでいない。

2) 評価人の出した結論

日本ＩＢMは、複数人（受託事業者の経営者およびIT管理者）に対してヒアリングを行って調査結果を得ており、供述の一貫性および後述する処理の再実施などの結果による裏付けを行っている。また、機構が別途実施した受託事業者の経営者およびIT管理者へのヒアリングでも同一の結果を得ていることから、評価人は、日本ＩＢMが実施したヒアリング内容結果に対する一定の信頼性は担保できていると評価できる。

3.4.2. ファイルサーバー上での関連情報の保存状況調査（調査結果報告書 P8～P12）

1) 日本ＩＢMの調査結果

評価人は、日本ＩＢMの調査結果報告書に記載のあるファイルサーバー上での関連情報の保存状況調査において日本ＩＢMが実施した調査結果を確認した。

① 全てのサーバーは施錠できる隔離されたサーバー室に設置されており、鍵を所有する IT 管理者以外が直接サーバーからデーターを持ち出すことは難しい環境であると判断した。

② 受託事業者のファイルサーバー上に保存されたファイルおよびシステムにより生成された再委託先事業者に渡すためのファイルの内容を目視により確認した結果、再委託先に送付された情報は「扶養親族等申告書・個人番号申出書」から切り出された「氏名とフリガナ」のみ含まれているファイルであることを確認した。

2) 評価人の出した結論

受託事業者におけるサーバー室の施錠管理について、評価人は直接現況を確認することは出来ないが、日本ＩＢMの調査結果報告書の「*サーバーは常に施錠された専用の部屋に設置されている。鍵は IT 管理者が管理している。*」という記載から、鍵を所有する IT 管理者以外が直接サーバーから情報を持ち出す可能性は低いとの判断は妥当であると評価した。

日本ＩＢMが行った目視確認の結果は、調査結果報告書内に画面のスクリーンショットを用いて示されており、一定の信頼性は担保できていると評価できる。

評価人は、日本ＩＢMが実施した以下に記載する切り出し処理の再実施について、切り出し処理におけるデータ加工の手順と結果は、一貫性があると評価した。

① 実際に処理された「ロット」「区分」を使用した動作検証を行った

② ZIP 圧縮ファイルが「FTP」ディレクトリに生成されることを確認した

③ 集約されたファイルはすべて「氏名とフリガナ」のみの画像化ファイルであることを確認した

また、2017 年 12 月 18 日に生成されたファイルと同一のファイル名の画像化ファイルを確認した際に内容が一致していることを確認していることから、切り出し処理するシステムが再委託先事業者への作業依頼時（少なくとも 2017 年 12 月 18 日時点）に利用されていることの確からしさがあると評価した。

3.4.3. 管理サーバーおよびネットワーク関連ログによるアクセス実態調査（調査結果報告書 P12～P14)

1) 日本ＩＢMの調査結果

評価人は、日本ＩＢMの調査結果報告書に記載のある管理サーバーおよびネットワーク関連ログによるアクセス実態調査において日本ＩＢMが実施した調査結果を確認した。

① 管理サーバーの調査対象ログ（Security ログ）の保存期間が「*約 5 日間（1 月 10 日時点では平成 30 年 1 月 5 日 14 時 9 分 44 秒から同月 10 月日 13 時 25 分 06 秒までの間のログのみ）*」であること。

② *ルーターのアクセスログの保存期間は「1 日間（1 月 10 日時点のログのみ）」*であること。

③ 業務 PC から情報持ち出しする可能性を否定するには、全業務 PC の調査を必要とする。

2) 評価人の出した結論

受託事業者の業務 PC による情報持ち出しの可能性を否定するには、機構が受託事業者へ「扶養親族等申告書・個人番号申出書」の預託を開始した平成 29 年 10 月 2 日に遡ってのログ調査が必要となる。

しかし、日本ＩＢＭが受託事業者への調査を行った平成 30 年 1 月 10 日、12 日時点では、前述のとおり管理サーバー、ルーターのログで確認できる期間はそれぞれ約 5 日間、1 日間と限られた期間であったため、当該ログを調査しても業務 PC による情報持ち出しの可能性を否定することはできない。

このことから、評価人は日本ＩＢＭの「全業務 PC の調査が必要である」との判断は妥当であると評価した。

3.4.4. サーバーおよびネットワーク関連設定状況の確認（調査結果報告書 P14）

1) 日本ＩＢＭの調査結果

評価人は、日本ＩＢＭの調査結果報告書に記載のあるサーバーおよびネットワーク関連設定状況の確認において日本ＩＢＭが実施した調査結果を確認した。

①「扶養親族等申告書・個人番号申出書」画像化ファイルが保存されているファイルサーバー上のフォルダは、受託事業者のユーザーID を持つ職員および作業員全員がアクセス可能な状態となっており、適切な制限がかけられていない。

2) 評価人の出した結論

評価人は、日本ＩＢＭが「扶養親族等申告書・個人番号申出書」画像情報が保存されているディレクトリの権限設定を確認（*Everyone に対して「フルコントロール」が付与*）していることから、日本ＩＢＭの「*適切な制限がかけられていない*」との判断は適切であると評価した。

3.5. 「扶養親族等申告書･個人番号申出書データ入力及び画像化業務」を実際に行う作業 PC を含む全業務 PC の調査結果の妥当性

3.5.1. 全業務 PC から収集した情報（調査結果報告書 P14～P16）

1) 日本ＩＢＭが収集した情報

評価人は、日本ＩＢＭは、Web アクセス履歴およびUSB 外部媒体使用履歴に関する調査にあたり、全業務 PC から「表 3.5-1　日本ＩＢＭが収集した PC 調査用情報」に記載の情報について収集を行っていることを確認した。

表 3.5-1　日本ＩＢＭが収集した PC 調査用情報

データカテゴリ	データ詳細	調査目的
レジストリ	*Windows¥System32¥config¥SAM* *Windows¥System32¥config¥SOFTWARE* *Windows¥System32¥config¥SYSTEM* *Windows¥System32¥config¥SECURITY*	*PC 基本情報の確認* *Web アクセス履歴に関する調査* *USB 外部記憶媒体利用履歴に関する調査*

データカテゴリ	データ詳細	調査目的
デバイスとドライバインストールログ	*Windows¥INF¥setupapi.dev.log*	*USB 外部記憶媒体利用履歴に関する調査*
ユーザーに係わる全ての情報	*Users¥**	*PC 基本情報の確認* *Web アクセス履歴に関する調査*
イベントログ	*Windows¥System32¥winevt¥Logs¥**	*USB 外部記憶媒体利用履歴に関する調査*

2) 評価人の出した結論

日本ＩＢＭの調査結果報告書では、他者に知られることなく持ち出しを行う手法として、「*Web 経由での情報送信*」と「*USB 外部記憶媒体の利用*」の 2 種類の手法が多いとしている。なお、日本ＩＢＭは調査において「*PC 基本情報の確認*」を実施していることから、初期導入以降に追加でインストールされたソフトウェアおよび Users フォルダ配下の情報を調査し、「Web 経由での情報送信」と「USB 外部記憶媒体の利用」以外の持ち出し手法に対しても確認は行っていた、と評価できる。

3.5.2. Web アクセス履歴に関する調査（調査結果報告書 P16～P17）

1) 日本ＩＢＭの調査結果

評価人は、日本ＩＢＭの調査結果報告書に記載のある全業務 PC を対象とした Web アクセス履歴に関する調査において日本ＩＢＭが実施した調査結果を確認した。

① 全ての PC には、OS のインストール日から情報取得日平成 30 年 2 月 10 日までの間の Web アクセス履歴が存在していないことから、Web 経由の情報持ち出し行為は存在しなかった。

2) 評価人の出した結論

評価人は、日本ＩＢＭが Web アクセスに使用するブラウザを特定し、ブラウザごとに閲覧履歴そのものとユーザーが閲覧履歴消去を実施しても削除できないファイルなどを調査し、全業務 PC に当該ファイルそのものが存在していないことをもって、Web アクセス行為自体がなかったと結論付けたプロセスについて、妥当であると評価した。

3.5.3. USB 外部媒体使用履歴に関する調査（調査結果報告書 P17）

1) 日本ＩＢＭの調査結果

評価人は、日本ＩＢＭの調査結果報告書に記載のある全業務 PC を対象とした USB 外部媒体使用履歴に関する調査において日本ＩＢＭが実施した調査結果を確認した。

① 全ての PC の USB 外部装置使用履歴を調査した結果、受託事業者社員による正規業務であることが確認できた。このことから USB 外部記憶媒体による情報持ち出し行為はなかったと判断した。

日本ＩＢＭは、調査対象である全業務 PC100 台のうち 53 台の PC に USB 外部装置の使用履歴が存在していることを確認し、存在した使用履歴について絞り込み作業を実施し、確認できた USB 外部装置の使用記録数 332 件において情報持ち出しの疑いがなく、問題ないと判断している。

2) 評価人の出した結論

評価人は、日本ＩＢＭが 332 件の使用履歴に対し「表 3.5-2　日本ＩＢＭが実施したＵＳＢ外部記憶媒体履歴の絞り込み作業の評価」の要素で類型化した上で、それぞれの類型ごとに運用状況や機構での調査状況等を勘案し、絞り込み作業を行った手法は、日本ＩＢＭの外部専門家としての知見が反映されたものである、と評価した。

日本ＩＢＭが実施した絞り込み作業における個別の評価結果について、以下に記載を行う。

表 3.5-2　日本ＩＢＭが実施したＵＳＢ外部記憶媒体履歴の絞り込み作業の評価

No.	評価項目	評価基準	該当する使用記録数	該当しない使用記録数	評価結果
1	*USB 外部装置の記録*	—	*332*	—	—
2	*実際に使用された USB 外部装置の記録*	*PC に接続された USB 外部装置で OS に外部ドライブ等として認識されていない場合は、実際には使用されておらずユーザーID に結び付かない。このためユーザーID が記録されない。ユーザーID がない記録を除外*	*296*	*36*	妥　当
3	*DVD 使用以外の記録*	*ヒアリングにより、社員用 PC とスキャナ PC 上での DVD 操作は納品業務であることが確認できたため、除外*	*218*	*78*	次ページ①にコメント記載
4	*OCR 業務以外の記録*	*sec_ocr、set_rej は OCR ソフトウェアが利用するユーザーID。通常のユーザーのような GUI、コマンドなどの操作はできないため、USB 外部記憶媒体の操作も不可能。情報持ち出しを示すファイル操作の記録も存在していない。そのためこの 2 つのユーザーID が関連する使用記録は除外*	*43*	*175*	妥　当
5	*help_td ユーザーID 以外の記録*	*help_td は社員用 PC 上で業務管理などを行うユーザーID であることを確認できたため、help_td が関連する使用記録は除外*	*42*	*1*	次ページ②にコメント記載
6	*平成 29 年 10 月 1 日以降の記録*	*受託事業者の戸田サテライトオフィスにおいての作業が平成 29 年 10 月からのため平成 29 年 9 月 30 日以前の使用は除外*	*30*	*12*	妥　当
7	*情報持ち出しの振る舞いと同様もしくは近い利用パターンを示す記録*	*「複数のユーザーID が同一の USB 外部記憶媒体を使用している記録」もしくは「特定のユーザーID が複数の USB 外部記憶媒体を複数の PC に対して利用している記録」は情報持ち出しの振る舞いに合致しないので除外*	*1*	*29*	次ページ③にコメント記載

No.	評価項目	評価基準	該当する使用記録数	該当しない使用記録数	評価結果
8	*対象PC上のログから不審な振る舞いと判断した記録*	*1台のPCのみで、他では利用されていないUSB外部記憶媒体を使用したユーザーIDの履歴が1つだけ存在した。当該履歴を確認するため、イベントログ、ファイルの情報、削除済みファイルなどの調査を実施し、問題のないことを確定*	*0*	*1*	本ページ④にコメント記載

評価人は、日本ＩＢＭが実施したUSB外部記憶媒体履歴の絞り込み手順を確認し、「*OSに外部ドライブ等として認識されていない使用記録*」「*通常のユーザーのようなGUI、コマンドなどの操作はできないOCRソフトウェアが利用するユーザーIDの使用記録*」「*受託事業者の戸田サテライトオフィスにおいての作業開始前（平成29年9月30日以前）の使用記録*」の除外について、妥当であると評価した。

なお、「表 3.5-2　日本ＩＢＭが実施したＵＳＢ外部記憶媒体履歴の絞り込み作業の評価」の赤枠破線で囲んだ箇所については、以下のとおり評価を行った。

① 「*社員用PCとスキャナPC上でのDVD操作の記録*」は、作業履歴との突合確認が望ましいが、機構による受託事業者への業務監査にて突き合わせにより不自然な作業がない、と判断していることを機構へのヒアリングにて確認したため、日本ＩＢＭの評価は妥当であると評価した。

② 「*業務管理などを行うユーザーIDであるhelp_tdが関連する使用記録*」については、作業履歴との突合確認が望ましいが、機構が実施した業務監査にて、当該ユーザーIDは受託事業者の戸田サテライトオフィスにおける業務管理などを行うユーザーIDであり正規業務であることの確認を行っていることを機構へのヒアリングにて確認したため、日本ＩＢＭの判断は妥当であると評価した。

③ 日本ＩＢＭの知見に基づく「*複数のユーザーIDが同一のUSB外部記憶媒体を使用している記録*」もしくは「*特定のユーザーIDが複数のUSB外部記憶媒体を複数のPCに対して利用している記録*」は情報持ち出しの振る舞いではない、との判断について客観的な統計や数値による評価は困難ではあるが、実際のUSB外部記憶媒体の利用現場において違和感を覚える判断ではない、と評価した。

④ 「*1台のPCのみで、他では利用されていないUSB外部記憶媒体を使用したユーザーIDの履歴*」について、日本ＩＢＭは当該履歴について「*当該履歴を確認するため、イベントログ、ファイルの情報、削除済みファイルなどの調査を実施し、*」外部専門家としての知見と責任に基づき総合的に判断を行っており、客観的な評価は困難ではあるが、一定の信頼性をおける判断である、と評価した。

3.6. 再委託先事業者に対する調査結果の妥当性

3.6.1. 管理規程（調査結果報告書 P21～P23、P30）

1) 日本ＩＢＭの調査結果

評価人は、日本ＩＢＭの調査結果報告書に記載のある再委託先事業者の管理規程の内容について日本ＩＢＭが実施した調査結果を確認した。

① 情報を保護するための一定の基準が必要な日本のプライバシーマークと同等のPIPAを遵守した、十分な管理規程が用意され、適切に運用されていると判断した。

2) 評価人の出した結論

日本ＩＢＭの調査結果報告書には、再委託先事業者が取得した中国の個人情報保護認定資格 PIPA（Personal Information Protection Assessment）の資格証書の写しが記載されている。

また「*PIPA は 2008 年 6 月 30 日から 2016 年 9 月 30 日まで日本のプライバシーマーク（P マーク）と相互承認を実施している。相互承認終了後も PIPA の審査レベルは相互承認実施時と同じレベルを維持し変更されていない*」、「*PIPA に審査レベルが変わっていないことを確認済み*」との記載があるが、現在の日本のプライバシーマークは「JIS Q 15001：2017（個人情報保護マネジメントシステム－要求事項）」を審査基準としている。ただし、プライバシーマーク審査基準の改訂は 2018 年 3 月 16 日であり、日本ＩＢＭ調査時点においては、日本国内において JIS Q 15001：2017 による認証の実績がないことから、日本ＩＢＭ調査時点において、PIPA が「*日本のプライバシーマークと同等*」であるとの判断は妥当であると評価した。

なお、評価人は再委託先事業者の管理規程や運用の現況について直接の確認は行っていないが、PIPA が日本のプライバシーマークと同等の審査レベルを維持しているのであれば、管理規程の整備と管理規程に基づく適切な運用が認証の条件となると考えられる。そのため、日本ＩＢＭの「*十分な管理規程が用意され、適切に運用されていると判断*」は妥当であると評価した。

3.6.2. 業務の実態（調査結果報告書 P24～P25、P30）

1) 日本ＩＢＭの調査結果

評価人は、日本ＩＢＭの調査結果報告書に記載のある再委託先事業者の業務の実態について日本ＩＢＭが実施した調査結果を確認した。

① 作業員の行動は適切に制限されると同時に十分な監視が行われており、情報の持ち出しが困難な環境であると判断した。

2) 評価人の出した結論

評価人は、日本ＩＢＭが確認した再委託先事業者における作業員の行動への制限と監視の状況について、「表 3.6-1　再委託先事業者における作業員への行動の制限と監視」を用いて整理を行い、再委託先事業者において作業員の行動が、物理的区画、ネットワーク、サーバー、フォルダ、データ、クラウドサービス、端末、媒体、においてそれぞれ制限と監視がされていることから「*情報の持ち出しが困難な環境である*」との日本ＩＢＭの判断は妥当であると評価した。

表 3.6-1 再委託先事業者における作業員への行動の制限と監視

No.	対象	制限方法※	監視方法※
1	物理区画	・カードと入室キーで作業室への立ち入りを制御している（2.7.1、2.7.2） ・サーバー室は[redacted]のみがアクセスできる（2.7.2） ・カードのストラップの色で分けている。オレンジは社員で、青は訪問者である。（2.7.3） ・私用物はロッカールームに置いている。（2.7.5） ・印刷は禁止している。（2.7.6）	・監視カメラがあり、映像は[redacted]保管する（2.7.4） ・カードで入退室および出勤記録を管理している。記録データは削除しておらず、[redacted]データが残っている（2.7.4）
2	ネットワーク	・サーバ室にある専用 PC からデータ授受を行っている。FireWall にて専用 PC 以外接続できないようにアクセス制御されている。（2.3.4.1） ・[redacted]でインターネットにアクセスする IP アドレスを制御している。（2.9.1） ・[redacted]でインターネットへのアクセスが許可されている IP アドレスの通信を制御している。（2.9.1） ・ルータやファイアウォールのアクセス制御は適切に実装されている。（2.9.1.2）	・ログは[redacted]保管している。（2.9.1） ・（ルータやファイアウォールのアクセス制御を）[redacted]に確認している。（2.9.1.3）
3	サーバー	・情報を保存するサーバーへのアクセス制限を実施し、業務上情報を知る必要がある人のみがアクセスできる仕組みがある。（2.8.3）	・情報へのアクセス者の記録（ログ）を取得し、一定の期間適切に保管している。アクセス記録を[redacted]（2.8.4）
4	フォルダ	・案件毎に作業グループを指定している。（2.3.2.1） ・案件毎に専用フォルダにデータを保存する。（2.3.2.1） ・内部専用 FTP サーバーから業務データが自動的に担当作業グループに配布される。（2.3.2.1） ・案件毎に[redacted]し、その案件の専用フォルダのみへのアクセス権限を付与している。（2.3.2.1） ・フォルダの共有を使用していない。（2.3.2.1）	・独自開発の作業管理システムでログを保存している。（2.3.2.3）
5	データ	・年金機構様の情報は専属グループで処理されており、他の顧客のデータと混在することはない。（2.1.6）	・情報へのアクセス者の記録（ログ）を取得し、一定の期間適切に保管している。アクセス記録を[redacted]（2.8.4）
6	情報システム	・[redacted]しており、ユーザーID の共有は禁止されている（2.8.1.1）	・情報へのアクセス者の記録（ログ）を取得し、一定の期間適切に保管している。アクセス記録を[redacted]（2.8.4）

No.	対象	制限方法※	監視方法※
7	クラウドサービス	・案件毎に外部 FTP サービス業者[redacted]に FTP のログオン ID とパスワードを発行してもらっている。（2.9.4.4） ・外部 FTP サービスを利用してデータを授受する際パスワードを付けて保護されている。（2.9.4.4）	・外部 FTP サービス業者[redacted]のサーバーでは過去 28 日分（7 日×4 回分）のログが保存されている。（2.3.4.3）
8	端末	・カードと入室キーで作業室への立ち入りを制御している（2.7.1、2.7.2） ・サーバー室は[redacted]のみがアクセスできる（2.7.2） ・カードのストラップの色で分けている。オレンジは社員で、青は訪問者である。（2.7.3） ・PC 起動時に ID とパスワードが要求される（2.9.4.3） ・PC にて[redacted]放置した場合、画面がロックされるように設置されている。（2.9.4.3） ・ファイル交換ソフトのインストール・使用を禁止している。（2.10.3）	・監視カメラがあり、映像は[redacted]保管する（2.7.4） ・カードで入退室および出勤記録を管理している。記録データは削除しておらず[redacted]データが残っている（2.7.4） ・PC、記憶媒体には盗難防止対策を施していないが代替策として、監視カメラが設置されており、かつ、PC には情報を保管していない（2.9.4.2）
9	媒体	・USB メモリなどの外部記憶媒体の使用は禁止されている。具体的には[redacted]でマウスとキーボード以外のすべての USB デバイスの接続を禁止している。（2.5.2）	・PC、記憶媒体には盗難防止対策を施していないが代替策として、監視カメラが設置されており、かつ、PC には情報を保管していない（2.9.4.2）

※制御方法、監視方法の () 内は、「付録 1：現地調査項目と確認結果」にて当該制御について確認を行っている項目の番号

3.6.3. 情報の取り扱い実態（調査結果報告書 P26～P30）

1) 日本ＩＢＭの調査結果

評価人は、日本ＩＢＭの調査結果報告書に記載のある情報の取り扱い実態について日本ＩＢＭが実施した調査結果を確認した。

① 再委託先事業者が受託事業者と情報のやり取りを実施する際には、専任担当者による作業、限定した PC の利用および接続制限が行われている。作業段階においても作業システムによる制御により情報への自由なアクセスが制限されている。情報の取り扱い段階においても持ち出しが困難になるように管理されている。

2) 評価人の出した結論

評価人は、日本ＩＢＭが確認した再委託先事業者における情報の取り扱い実態の状況について、「表 3.6-2　再委託先事業者における情報の取り扱い実態の整理」を用いて整理を行い、再委託先事業者における情報の取り扱い実態について、情報のライフサイクルごとに登場する機器の利用制限および接続制限が行われていることから、「*持ち出しが困難になるように管理されている*」との日本ＩＢＭの判断は妥当であると評価した。

表 3.6-2　再委託先事業者における情報の取り扱い実態の整理

No.	情報のライフサイクル	情報を取扱う機器	日本ＩＢＭが確認した取扱い実態
1	情報の取得	・クラウドストレージ	・受託事業者と再委託先事業者の間の情報の受け渡しには、クラウドストレージサービスを使用している。受け渡すファイルはパスワードが付与され保護されている。 ・今回のデータ授受を実施していた期間は、10 月中旬から 12 月 25 日までであることをヒアリングで確認した。
		・ファイアウォール	・クラウドストレージサービスには、情報受け渡し PC 以外は接続できないよう、再委託先事業者所有のファイアウォールによるアクセス制御が行われている
		・情報受け渡し PC	・情報授受の際には情報受け渡し専用 PC のみを使用している。 ・情報受け渡しは専任者が実施し、専用のユーザーID とパスワードを使ってクラウドストレージサービスに接続していた。 ・情報受け渡し専用 PC は一切のネットワークから切断された状態で運用されている。 ・クラウドストレージ間で情報授受が必要な場合は、ケーブルをファイアウォールに接続している。授受終了後はケーブルを抜線している。 ・受領した情報を作業者に渡す際には、情報受け渡し PC を内部ネットワークに接続し、サーバーへ保存している。終了後ケーブルは抜線される。
2	情報の送信	・クラウドストレージ	・受託事業者と再委託先事業者の間の情報の受け渡しには、クラウドストレージサービスを使用している。受け渡すファイルはパスワードが付与され保護されている。 ・今回のデータ授受を実施していた期間は、10 月中旬から 12 月 25 日までであることをヒアリングで確認した。
		・ファイアウォール	・クラウドストレージサービスには、情報受け渡し PC 以外は接続できないよう、再委託先事業者所有のファイアウォールによるアクセス制御が行われている
		・情報受け渡し PC	・情報授受の際には情報受け渡し専用 PC のみを使用している。 ・情報受け渡しは専任者が実施し、専用のユーザーID とパスワードを使ってクラウドストレージサービスに接続していた。 ・情報受け渡し専用 PC は一切のネットワークから切断された状態で運用されている。 ・クラウドストレージ間で情報授受が必要な場合は、ケーブルをファイアウォールに接続している。授受終了後はケーブルを抜線している。 ・受領した情報を作業者に渡す際には、情報受け渡し PC を内部ネットワークに接続し、サーバーへ保存している。終了後ケーブルは抜線される。
3	情報の利用	・サーバー （作業管理システム）	・受託事業者から受領した情報を処理するグループは専任であり、他の業務の情報と誤って混在することがないよう、分離されている。 ・加えて権限のない情報にはアクセスできないようアクセス制御が施されている。

No.	情報のライフサイクル	情報を取扱う機器	日本ＩＢＭが確認した取扱い実態
		・作業 PC	*・作業対象情報は、作業管理システムを用い、内部専用サーバーから FTP で自動的に担当グループに配布されており、それ以外の手法でのファイル共有は実施されていない。* *・配付及び作業は専用アプリケーションで実施され、作業者による作業終了後、アプリケーションが作業対象情報の削除を実施するため、作業 PC には作業した情報は保管できない。*
4	保管・バックアップ	・サーバー（作業管理システム）	*・受託事業者から受領した情報を処理するグループは専任であり、他の業務の情報と誤って混在することがないよう、分離されている。* *・加えて権限のない情報にはアクセスできないようアクセス制御が施されている。*
5	消去・廃棄	・クラウドストレージサービス	*・受領した情報は、受領後、クラウドストレージから削除している。*
		・情報受け渡し PC	*・データ消去の専用ソフトウェアでデータを消去している。*
		・サーバー（作業管理システム）	*・データ消去の専用ソフトウェアでデータを消去している。*
		・作業 PC	*・作業室内の作業 PC には作業した情報が保管できないよう制御されている。* *・配付及び作業は専用アプリケーションで実施され、作業者による作業終了後、アプリケーションが作業対象情報の削除を実施するため、作業 PC には作業した情報は保管できない。* *・加えて処理完了後、担当グループの情報を直ちに削除していた。*

3.7. 調査目的の達成度

評価人は、調査結果報告書の「*2.調査目的*」において、調査目的が「*情報取り扱い実態を確認することで、情報の持ち出しが生じている可能性を評価すること*」であることを確認し、日本ＩＢＭが実施した調査における調査目的の達成度の評価を行った。

3.7.1. 情報の取り扱い実態の確認（調査結果報告書 P32～P33）

日本ＩＢＭは、受託事業者および再委託先事業者における情報の取扱い実態を確認するために IT 管理者へのヒアリングを行い、調査対象となっている IT 機器を用いた情報の取扱いについて手順等の聞き取りを行った後、実際のデータ(情報)受渡方法、データ加工方法、データ保管方法などを IT 機器に残された記録などを用いて、可能な限り実査にて調査を行っている。また調査中に知り得た運用実態に応じて、調査対象である全業務 PC の Web アクセス履歴、USB 外部媒体使用履歴の評価等を行っている。評価人は、機構が期待する外部専門家としての知見にもとづく専門性の高い調査が行われ、「*情報取り扱い実態を確認する*」という調査目的は達成されていると評価した。

これにより、評価人が確認した範囲においては、日本ＩＢＭが導き出した「*受託事業者および再委託先事業者から情報の流出は生じていないと判断した*」との結論について、信頼性があると評価できる。

3.7.2. 情報の持ち出しが生じている可能性の評価（調査結果報告書 P32～P33）

日本ＩＢＭは、受託事業者および再委託先事業者における情報の持ち出しが生じている可能性について、以下のとおり確認を行っている。

1) 受託事業者および再委託先事業者における情報の持ち出しに関する調査結果

① 受託事業者のサーバー設備は施錠された部屋で運用されており、鍵を所有する IT 管理者以外の直接アクセスは制限されており、ファイルサーバーから直接情報の持ち出しの可能性は非常に低い。

②（受託事業者への調査において）全ての業務 PC を確認した結果、Web 経由および USB 外部記憶媒体経由での情報持ち出しは生じていない。

③ 再委託事業者では、セキュリティ管理規程が整備され、維持および運用が実施されて管理されている。作業者による情報の持ち出しが困難になるように環境が整備されている。

2) 受託事業者から再委託先事業者に受け渡された情報に関する調査結果

① 受託事業者は、「扶養親族等申告書・個人番号申出書」をスキャンした画像化ファイルから「氏名とフリガナ」の画像化ファイルを切り出し処理するシステムにより、自動的に必要なファイルを集約した受け渡しファイルを生成し、継続的に使用していたことをヒアリングで確認した。

② 受託事業者のファイルサーバーには、扶養親族等申告書・個人番号申出書全体を画像化したファイル①と「氏名とフリガナ」部分を切り出した画像化ファイル②の 2 種類が保存されていた。保存されていた全体の画像化ファイルに該当するロットと区分を対象に、「氏名とフリガナ」を切り出すシステムの動作検証を実施した。この動作検証で生成されたファイル③の内容を比較したところ、②と③の内容が一致した。③のファイルは、再委託先事業者に送付するための専用フォルダに作成された。

③（受託事業者への調査において）確認を行った「扶養親族等申告書・個人番号申出書」全体を画像化したファイルは 12 月 12 日に、「氏名とフリガナ」部分を切り出した画像化ファイルは 12 月 18 日に生成されたものであった。

④ 貴機構が平成 30 年 2 月 16 日に再委託先事業者から受託事業者が受領したファイルを確認したところ、「氏名とフリガナ」しか含まれていなかった。

⑤ 再委託先事業者が使用している作業者用マニュアルには、入力作業用の画面が示されており、「氏名とフリガナ」部分の入力作業および、作業者 2 名による入力結果のコンペア作業が記載されている。これは受託事業者から受領した運用マニュアル中の業務フロー概要図に表記されている「氏名ヨミ、漢字」部分の処理手順と同一であった。

⑥（再委託先事業者への調査において）「氏名とフリガナ」部分の入力作業は 10 月中旬から 12 月 25 日に実施していたことをヒアリングで確認した。

評価人は、調査を取り巻く環境を考慮すると、日本ＩＢＭの調査対象の選定、調査方法の選定、調査結果には一定の妥当性、有効性があり、日本ＩＢＭは最大限取り得る技法をもって調査を行っており、「*情報の持ち出しが生じている可能性を評価すること*」という調査目的は達成されていると評価した。

これにより、評価人が確認した範囲においては、日本ＩＢＭが導き出した「*受託事業者から中国の再委託先事業者に送付されていた情報は、「氏名とフリガナ」のみであった。*」との結論については、信頼性があると評価できる。

以　上