資料１－２

公 表 資 料

株式会社 NTT マーケティングアクト ProCX 及び NTT ビジネスソリューションズ株式会社に対する個人情報の保護に関する法律に基づく行政上の対応について（詳細資料）

令和６年１月●日
個人情報保護委員会

第１　事案の概要等

１　株式会社 NTT マーケティングアクト ProCX（以下「ProCX 社」という。）は、西日本電信電話株式会社（以下「NTT 西日本」という。）が 100%出資する子会社であり、コールセンター事業等を行っている。ProCX 社は、多数の民間事業者及び地方公共団体等（以下「本件委託元」という。）から委託を受け、商品販売等や健康診断等の行政上の通知に係るコールセンター業務（以下「コールセンター業務」という。）を行っており、同業務において、本件委託元の多数の顧客又は住民等に関する個人データ及び保有個人情報（以下「個人データ等」という。）を取り扱っていた。

２　ProCX 社は、NTT ビジネスソリューションズ株式会社（NTT 西日本が 100%出資する子会社であり、情報システムの開発・運用等 IT サービス事業を行っている会社。以下「BS 社」という。）との間で、コールセンター業務で用いるシステムの利用に関するサービス利用契約（以下「コールセンターサービス利用契約」という。）を締結していた。BS 社は、同契約に基づき、ProCX 社に対し、コールセンター業務における業務実績を管理するシステム（以下「コールセンター業務用システム」という。）を提供し、同システムの保守運用を行っていた。ProCX 社は、コールセンターにおける架電の対象となる本件委託元の顧客又は住民等の個人情報等が記載されたリスト（以下「サービス対象者リスト」という。）を、BS 社が提供するコールセンター業務用システムに保存し、ProCX 社の従業者がコールセンター業務を行っていた。

３　本件は、2013 年７月頃から 2023 年２月頃にかけて、BS 社内においてコールセンター業務用システムの保守運用業務に従事していた従業者（派遣会社から BS 社に労働者派遣されていた派遣社員。以下「Ｘ」という。）が、本件委託元の顧客又は住民等に関する個人データ等合計約 928 万人分[1]を不正に持ち出し、漏えいが発生した事案である。

４　個人情報保護委員会（以下「当委員会」という。）は、2023 年 10 月 20 日、ProCX 社及び BS 社に対し、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」

[1] BS 社が行った調査により、現時点において、ログ等から不正に持ち出されたことが確認されている個人データ等の本人数であり、その委託元は民間事業者 30 社、独立行政法人１機関及び地方公共団体 38 団体とされているが、詳細について BS 社において更に確認中である。

という。）第146条第１項に基づく報告徴収を行った。これについて、両社から同年11月10日、報告書を受領し、以降、同報告書の内容を精査するとともに、関係者へのヒアリングを行う等の調査を実施した。

第２　事実関係

１　本件事案に係る業務概要

(1)　ProCX社の業務内容

ProCX社は、本件委託元である民間事業者[2]、独立行政法人及び地方公共団体[3]との間で、テレマーケティング業務委託契約書を締結し、全国に40ある拠点において、コールセンター業務を実施していた。コールセンターでは、ProCX社のコールセンター管理者（以下「コールセンター管理者」という。）が、サービス対象者リストをコールセンター業務用システムへアップロードし、本件委託元の顧客又は住民等である対象者に対し、オペレーターが順次架電等[4]する業務を行っていた。

(2)　BS社の業務内容

BS社は、ProCX社との間で締結したコールセンターサービス利用契約に基づき、前記第１の２のとおり、ProCX社に対し、サービス対象者リストや業務実績等を管理するコールセンター業務用システムを提供し、さらに、コールセンター業務用システムの保守運用や、コールセンター業務用システムの利用に関する技術的なサポート業務を行っていた。

(3)　ProCX社及びBS社における個人情報の取扱いに係る規律

ProCX社及びBS社は、NTT西日本グループで統一された基準である「情報セキュリティマネジメント規程」及び「情報セキュリティ規則ICT編・一般業務編」（以下あわせて「NTT西日本グループ管理規程」という。）等[5]に従って、個人情報を取り扱うこととしていた。

ProCX社における個人データ等の取扱いについては、NTT西日本グループ管理規程等に加え、本件委託元との契約書で明記された個人情報の保護に関する取り決めに従うこととなっており、業務完了時には、サービス対象者リストは、速やかに廃棄する旨が定められていた。

---

[2] 民間事業者からの業務委託では、対象顧客の連絡先に対してテレマーケティング等のための架電業務を行っていた。

[3] 独立行政法人及び地方公共団体からの業務委託では、対象住民の連絡先に対して健康診断未受診者や税料金未納付者等への通知連絡業務等を行っていた。

[4] 架電のほか、一部契約においては顧客からの問合せに対応する業務も担っていた。

[5] 加えて、ProCX社は、個人情報等の取扱いに関して、「個人情報・特定個人情報保護安全管理対策規程」を規定していた。

また、BS 社については、NTT 西日本グループ管理規程に加え、コールセンターサービス利用契約において秘密保持に関する取り決め[6]が明記されていた。

２　本件事案発生の経緯

(1)　Ｘが従事していた業務内容

Ｘは、派遣会社に派遣労働者として雇用され、派遣会社と BS 社との間で締結された「労働者派遣に関する基本契約」及び「労働者派遣個別契約」（以下あわせて「労働者派遣契約」という。）に基づき、2008 年６月[7]から 2023 年７月[8]までの間、BS 社において、コールセンター業務用システムの保守運用業務等に従事していた。

BS 社と派遣会社は、労働者派遣契約において、派遣労働者の守秘義務等を規定し、BS 社従業者が遵守すべき NTT 西日本グループ管理規程の遵守を、Ｘのような派遣労働者に対して義務付けていた。

(2)　BS 社における個人データ等の取扱状況について

BS 社は、コールセンター業務用システムの保守運用に当たって、グループ企業が運営するデータセンター内に業務システムサーバ（以下「PDS サーバ」という。）を設置し、当該サーバ内に ProCX 社が本件委託元から取扱いを委託された個人データ等を保存していた。

BS 社において、コールセンター業務用システムの保守運用業務を担当する者（Ｘを含む。以下「保守運用担当者」という。）は、BS 社内の保守拠点において、PDS サーバにアクセス可能な保守端末を利用し、保守運用業務を行っていた。保守運用担当者は、ProCX 社においてサービス対象者リストを適切にダウンロードできない場合等のトラブル対応を行うため、個人データ等を取り扱う業務を担っており、具体的には以下の態様で個人データ等の取扱いを行っていた。

ア　トラブル対応のサポートを行う必要があったため、Ｘを含む４人の保守運用担当者に対して、コールセンター業務用システム上の全てのサービス対象者リストを委託元ごとに閲覧及びダウンロードする権限（以下「システム管理者アカウント」という。）が付与されていた。

---

[6] コールセンターサービス利用契約書において、BS 社は、契約に関して知り得た秘密に関する情報を、ProCX 社の書面による承諾なしに、コールセンター業務用システムのサービス提供以外の目的に使用してはならず、第三者に漏えいしてはならない旨が規定されていた。

[7] 2008 年６月１日から 2020 年６月末日までは BS 社の前身である株式会社エヌ・ティ・ティネオメイトに派遣されていた。

[8] Ｘが BS 社で業務を行ったのは 2023 年７月 10 日が最後であり、2023 年７月 25 日付けで派遣会社を退職している。

イ　システム管理者アカウントは個人単位に付与されていたものではなく、アカウントを４人で共用する状態であった。

ウ　PDS サーバは閉域網内に設置されていたため、保守運用担当者がシステム管理者アカウントを用いて作業を行うためには、通常は、BS 社内の保守拠点に設置された保守端末で作業を行う必要があった。

エ　Ｘは、ProCX 社のコールセンターオペレーター向けに在宅オプションの利用に必要なアカウント ID 及びパスワードを払い出す業務に携わっていたため、オペレーター向けのリモートアクセスの仕組みを利用した上で、システム管理者アカウントを用いることで、BS 社内の保守拠点以外からも個人データ等にアクセスできた可能性があった。

オ　保守運用担当者は、システム障害時等に、外部業者に原因調査を依頼するため、PDS サーバ内のデータを持ち出す業務があり、容量の大きなデータの受け渡し等を行う場合に USB メモリを保守端末に接続利用していた。

カ　USB メモリの利用に関しては、指紋認証機能付き USB メモリ以外の外部記録媒体の使用を防止する技術的な措置がとられておらず、また、「事前に承認」を得ることなく個人判断で利用することを物理的又は技術的に防止する措置はとられていなかった。

(3)　Ｘによる個人データ等の持ち出しの方法

ProCX 社及び BS 社の回答によれば、Ｘの個人データ等の持ち出しは以下の方法があり得るとしている（資料１－３参照）。

ア　保守運用担当者であったＸは、業務上付与されていたシステム管理者アカウントを用いて、PDS サーバにアクセスし、サーバ内の個人データ等をダウンロードすることが可能な状況にあった[9]。

イ　Ｘは、BS 社から貸与された保守業務用端末に、個人データ等をダウンロードし、保守拠点に持ち込んだ私物の USB メモリに個人データ等を書き出し、保守拠点の外へ不正に持ち出した。

ウ　Ｘは、前記(2)エの方法（オペレーター向けのリモートアクセスの仕組みを利用することで、BS 社内の保守拠点以外から個人データ等にアクセス）を用いて、保守拠点以外から、個人データ等をダウンロードし、私物の USB メモリに個人データ等を書き出した。

３　本件漏えい等事態の発覚の端緒

コールセンター業務を ProCX 社に委託していた本件委託元のうちの１社（以下「A

[9] 本件において PDS サーバから個人情報のダウンロードが行われた事実については、ログ分析が BS 社によって行われており、窃取目的と思われるログが確認されている。

社」という。）は、2022 年１月頃から同年３月頃に、同社の顧客から、「不審な投資の勧誘電話があり、Ａ社から自身の個人情報が流出しているのではないか。」との問合せを複数回受け、顧客情報の漏えいの可能性が高いと認識した。そこで、社内調査並びにＢ県警への相談及び捜査依頼を行った。しかしながら、社内調査ではＡ社からの漏えいの事実は確認されなかったため、2022 年４月、大量に個人データ等の取扱いを委託する外部企業からの漏えいの疑いがあるとして、コールセンター業務の委託先であった ProCX 社に調査を依頼した。

これに対し、ProCX 社は、BS 社と共に調査（以下「過去調査」という。）を実施したが、2022 年７月に、Ａ社に対し、個人データ等の漏えいは確認されなかった旨を報告している。

その後、Ａ社からの捜査依頼を受けたＢ県警により、BS 社に対して捜査が実施されたことを発端として、ProCX 社は、Ｘによる個人データ等の持ち出しを認め、2023 年８月７日、Ａ社に対し、個人データ等の漏えいがあった事実について報告を行うとともに、その他の委託元に対しても順次報告を行っている。

第３　法律上の問題点について

１　ProCX 社－安全管理措置（法第 23 条）の不備

(1)　組織的安全管理措置（取扱状況の把握及び安全管理措置の見直し）

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）（以下「ガイドライン」という。）において、個人情報取扱事業者は、個人データ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まなければならないと規定されている（10-3(5) 取扱状況の把握及び安全管理措置の見直し）。

ProCX 社は、Ａ社からの調査依頼に対し、2022 年４月から同年７月に BS 社も協力の上で実施した過去調査において、前記第２の３のとおり、個人データ等の漏えいは確認できなかった旨を報告した。しかしながら、実際は、Ｘによる不正な持ち出しが過去調査以前のみならず、それ以降も行われていたことからすれば、ProCX 社における個人データ等の取扱状況の把握や安全管理措置の見直しは不十分であったと言わざるを得ない。

以上のとおり、ProCX 社には、組織的安全管理措置の不備が認められる。

(2)　人的安全管理措置（従業者の教育）

ガイドラインにおいて、個人情報取扱事業者は、従業者に個人データ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わなければならないと規定されている（10-4　従業者の教育）。

この点、ProCX 社においてはコールセンターの管理者・従業者に対して年１回定期的な研修を一般的なセキュリティ知識が記載された資料を用いて実施していたものの、大量の個人データや保有個人情報を取り扱うコールセンター業務における研修

内容としては不十分であった。

また、多くの委託元らの顧客又は住民等に関する個人データ等が入力され管理されるコールセンター業務用システムの保守運用を行うBS社に対し、後述のように委託元としての十分な監督を行うことができなかったことからすると、ProCX社における教育研修は、適切な情報セキュリティの確保及び個人データ等の適正な取扱いの重要性に関する認識を醸成するところまでには到底至っていなかったものと認められ、大量の個人情報を取り扱うコールセンター業務を行う企業としての教育研修体制は不十分であったと言わざるを得ない。

以上から、ProCX社においては、人的安全管理措置の不備が認められる。

(3) 小括

以上のことから、ProCX社において、組織的安全管理措置及び人的安全管理措置に不備が認められ、本件事案発生当時の同社の取扱いは、個人データの安全管理のために必要かつ適切な措置を求める法第23条の規定に違反する。

2 BS社－安全管理措置（法第23条）の不備

(1) 組織的安全管理措置

ア 個人データの取扱いに係る規律に従った運用の状況について

ガイドラインにおいて、個人情報取扱事業者は、あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならないと規定されている（10-3(2)個人データの取扱いに係る規律に従った運用）。

BS社では、前記第２の１(3)のとおり、あらかじめ整備されたNTT西日本グループ管理規程等が存在し、個人データの安全な取扱いの確保について取り組むための事項が規定されていたところ、BS社は、当時の従業者の遵守状況としては、一定程度これらの規律に従った運用がなされていた旨を回答している。

しかしながら、BS社においては、実際、Ｘによって規程に従わないUSBメモリの利用が行われていた。また、定期的な自主点検や監査が行われていたと回答しているものの、Ｘによる個人データ等の不正な持ち出しを発見することはできなかった。また、NTT西日本グループ管理規程等においては、定期的又は必要に応じたアクセス記録等の分析・監視が必要であるとされていたが、実際にはアクセスログの分析・監視はされていなかった。

イ 個人データの取扱状況の把握及び安全管理措置の見直しが十分でなかったこと

ガイドラインにおいて、個人情報取扱事業者は、個人データ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まなければならないと規定されている（10-3(5) 取扱状況の把握及び安全管理措置の見直し）。

しかしながら、BS社においては、以下のとおり、個人データの取扱状況の把握ができておらず、安全管理措置の評価、見直し及び改善などの取組も十分に行われ

ていなかった。

（ア） 監査等

BS 社では、前記アのとおり、記録されたアクセスログの分析・監視が実施されておらず、また、社内の監査担当により監査は実施していたものの、前記アのような取扱状況であることを監査により検知・是正できておらず、本件事案を未然に防止するには内容が不十分なものであったと言わざるを得ない。

（イ） Ａ社から ProCX 社に依頼された過去調査の対応

Ａ社から ProCX 社に対する調査依頼について、BS 社も協力の上で過去調査を実施した。しかし、前記１(1)のとおり、BS 社においてもＸによる持ち出し等は確認されず、Ａ社に対し、個人データ等の漏えいは確認できなかった旨を報告することとなった。

ウ　以上のとおり、BS 社には、組織的安全管理措置の不備が認められる。

(2) 人的安全管理措置（従業者の教育）

ガイドラインにおいて、個人情報取扱事業者は、従業者に、個人データ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わなければならないと規定されている（10-4 従業者の教育）。

しかしながら、BS 社は、派遣社員であるＸを含む従業者に、年１回研修等の取組を実施していたが、本件事案におけるＸの不適切な取扱いを質せず、漏えいを防止するに至らなかったことからすると、その取組は、BS 社の従業者が適切な情報セキュリティの確保や個人データ等の適正な取扱いの重要性に関する認識を醸成するには不十分な内容であったと言わざるを得ない。

以上のとおり、BS 社には、人的安全管理措置の不備が認められる。

(3) 物理的安全管理措置（個人データを取り扱う区域の管理）

ガイドラインにおいて、個人情報取扱事業者は、個人情報データベース等を取り扱うサーバ等の重要な情報システムを管理する区域及びその他の個人データを取り扱う事務を実施する区域について、それぞれ適切な管理を行わなければならないと規定されている（10-5(1)個人データを取り扱う区域の管理）。

しかしながら、BS 社では、個人情報データベース等を取り扱うサーバに接続可能な保守拠点においては、入退室の管理や監視カメラの設置を行うにとどまり、USB メモリ等の外部記録媒体の持ち込みについてチェック及び制限は行わず、入室者の判断で自由に持ち込めるよう運用していた。このため、Ｘを含む従業者は、私物 USB メモリを保守拠点内に持ち込み及び持ち出すことが可能な状態となっていた。

以上のとおり、BS 社には、物理的安全管理措置の不備が認められる。

(4) 技術的安全管理措置

ア　システム管理者アカウントのアクセス制御が適切になされていなかったこと

ガイドラインにおいて、個人情報取扱事業者は、担当者及び取り扱う個人情報デ

ータベース等の範囲を限定するために、適切なアクセス制御を行わなければならないと規定されている（10-6(1)アクセス制御）。

しかしながら、BS 社では、PDS サーバに保存する個人データ等にアクセス可能であるシステム管理者アカウントの ID 及びパスワードについて、保守運用担当者４名全員が単独作業にて常時利用できる状態であった。

イ　システム管理者のアカウントの共用によりアクセス者の識別と認証が適切に行われていなかったこと

ガイドラインにおいて、個人情報取扱事業者は、個人データを取り扱う情報システムを使用する従業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しなければならないと規定されている（10-6(2)アクセス者の識別と認証）。

しかしながら、BS 社では、前記第２の２(2)イのとおり、保守運用担当者複数名の従業者がシステム管理者アカウントを用いた個人データ等の取扱いを伴う作業を行っていたにもかかわらず、システム管理者アカウントを共用して業務を行っていた。そのため、本件事案のような特定の従業者の不適切な取扱いがあった場合にも、誰が不適切な操作を行っているか、また、１人の保守運用担当者が業務上必要な頻度以上にデータベースにアクセスしていないかなどについて、ログから判別できなかったものであり、アクセス者の識別と認証に問題があった。

ウ　情報システムの使用に伴う漏えい等の防止のための措置が不十分であったこと

ガイドラインにおいて、個人情報取扱事業者は、情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならないと規定されている（10-6(4)情報システムの使用に伴う漏えい等の防止）。

しかしながら、BS 社においては、以下のとおり、情報システムの使用に伴う個人データの漏えい等を防止するための措置が十分に講じられていなかった。

（ア）　保守端末等への個人データ等のダウンロード

BS 社では、PDS サーバに保存された個人データ等を、保守端末及びコールセンター管理者が業務で利用する端末にダウンロード可能としていた。

（イ）　私物 USB メモリの接続制限

前記(ア)の保守端末等については、業務上必要である登録された USB メモリ以外の接続を制限するなどの措置がとられておらず、私物 USB メモリを接続可能であり、保守端末等にダウンロードした個人データ等を外部へ持ち出すことが可能な状態であった。また、USB メモリが保守端末等に接続されたことを即時あるいは事後的に検知する仕組みも導入されていなかった。

エ　以上から、BS 社には、技術的安全管理措置の不備が認められる。

(5)　小括

以上のことから、BS 社において、組織的安全管理措置、人的安全管理措置、物理

的安全管理措置及び技術的安全管理措置に不備が認められ、本件事案発生当時の同社の取扱いは、個人データの安全管理のために必要かつ適切な措置を求める法第 23 条の規定に違反する。

3　ProCX 社－委託先の監督（法第 25 条）の不備

(1)　BS 社に対する個人データ等の取扱いの委託

ガイドライン 3-4-4 では、「個人データの取扱いの委託」とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱いを行わせることと示している。

ProCX 社と BS 社との間のコールセンターサービス利用契約に基づき、BS 社は、サービス対象者リスト等の個人データ等を保守運用のために必要な範囲で閲覧、入出力、削除することができ、実際に ProCX 社からの指示に基づき個人データ等を取り扱う業務を行っていた。したがって、ProCX 社は、BS 社に対し個人データ等の取扱いを委託していたものと認められる。

(2)　BS 社に対する監督

法第 25 条において、個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならないと規定されている。さらに、ガイドラインにおいて、委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元及び委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むこととされ（3-4-4(2) 委託契約の締結）、委託先における委託された個人データの取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することとされている（3-4-4(3) 委託先における個人データ取扱状況の把握）。

ア　ProCX 社と BS 社との間において、個人データ等の取扱いに関する取り決めがなされていなかったこと

ProCX 社と BS 社との間で締結されたコールセンターサービス利用契約においては、BS 社の個人データ等の取扱いに関する安全管理措置の実施状況を確認するための取り決めについて明記がないにもかかわらず、前記(1)のとおり、実態として個人データ等の取扱いを委託していた。

さらに、ProCX 社は、コールセンター業務の履行に当たり、一部の本件委託元との契約において、事前に委託元に再委託することを申請し、承諾を得た場合に限り、第三者に個人情報の処理を委託してもよいと規定していたにもかかわらず、委託元に報告することなく、BS 社に個人データ等を取り扱わせていた。

イ　委託先であるBS社における個人データ等の取扱状況の把握が不十分であったこと

ProCX社は、本件委託元の大量の個人データ等をコールセンター業務用システムで管理し、その保守運用としてBS社に指示し個人データ等を取り扱う業務を行わせていたにもかかわらず、定期的な監査や委託の内容等の見直しの検討を行っておらず、BS社における個人データ等の取扱状況を適切に把握していなかった。

(3)　小括

以上のことから、ProCX社において、委託先であるBS社に対する必要かつ適切な監督が十分になされていなかったことが認められ、本件事案発生当時の同社の取扱いは、法第25条の規定に違反する。

第４　再発防止策

１　ProCX社－安全管理措置（法第23条）

(1)　組織的安全管理措置（過去調査の対応）

ProCX社は、Ａ社から調査を依頼された際、十分な調査を行わなかった理由について、当委員会の法第146条第１項に基づく報告徴収への回答となる2023年11月10日付け報告書において、社外の専門家の関与の下、当時の調査担当者への事情聴取等の検証を進めていると説明しており、漏えいに繋がる端緒まで調査が至らなかったのかについて、回答していない。これに対し、当委員会は、当該報告徴収[10]に十分回答できていないことを同年12月７日に指摘するとともに、改めて当時の調査が適切であったか否かについて確認したところ、不適切な調査報告が行われていたことは確認できているものの、不適切な調査報告が行われた経緯・要因の解明には至っておらず、2024年２月を目処に社外の専門家による経緯調査を進め、不適切な調査報告に至った経緯・要因を明らかにするとのみ回答しており、現在もなお、不適切な調査の経緯や要因を明らかにしていない。

Ａ社の依頼に基づく過去調査から１年６か月が経過し、また、Ｂ県警のBS社に対する捜査実施後、Ａ社に対して漏えいの事実を報告してから５か月が経過する現在においても、BS社が不適切な調査報告が行われた経緯・要因を解明できない状況であることは、BS社の組織的安全管理措置について、個人データ等の取扱状況の把握及び安全管理措置の見直しの点で不備があることを改めて示すものである。

以上から、ProCX社の組織的安全管理措置については不備があり、法第23条の違反状態が現在も続いているものと認められる。

(2)　人的安全管理措置（従業者の教育）

---

[10] 法第182条第１項において、個人情報取扱事業者は、法第146条第１項に対して正当な理由なく報告若しくは資料提出をしない場合には罰則が課されている。

ProCX 社は、本件事案を受けて、2023 年 12 月７日、８日、個人データ等を取り扱う業務にあたる担当者へ講じた再発防止策について周知を行い従業者への教育を行っている。

この点、ProCX 社が講じた本再発防止策は、一定の改善が認められるものであるが、更なる従業者への教育の充実が図られることも期待した上で、今後、確実に実施されることを注視する必要がある。

２　BS 社－安全管理措置（法第 23 条）

(1)　組織的安全管理措置

ア　USB メモリの利用

BS 社は、2023 年７月 18 日、保守端末に保存された情報の USB メモリへの書き出しを不可とする対処を行っている。加えて、BS 社は、USB メモリの利用はシステム障害時等のやむを得ない場面に限定することを改めて徹底するとともに、事前登録された指紋認証機能付きの USB メモリのみ利用可能とし、さらに、管理職のみが利用可能な専用端末でのみ USB メモリが接続可能とする技術的な対応を行っている。また、USB メモリへのデータ書き出し作業を行う場合は、作業者を管理職に限定し、当該作業時に別の管理職による監視をあわせて行うよう運用している。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

イ　システム管理者アカウントのアクセス制限

BS 社は、2023 年８月９日、PDS サーバに保存する個人データ等にアクセス可能であるシステム管理者アカウントの ID 及びパスワードについて、保守運用担当者のうち２名の個人データ等を取り扱う役割を担う者に限定して権限付与することに運用を変更した。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

ウ　自主点検及びログの分析

BS 社は、2023 年 10 月 25 日、定期的な自主点検及びログの分析が行われるよう、自主点検及び分析の担当者、分析結果を監視する担当者について詳細な運用ルールを定め、同日以降、週次で自主点検及びログの分析を行っている。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、他部署や外部主体による実務に即した監査等が行われることによって、より高い実効性が確保されることも期待した上で、今後、確実に実施されることを注視する必要がある。

エ　個人データの取扱状況の把握及び安全管理措置の見直し（過去調査の対応）

前記第３の２(1)イのとおり、BS 社は、ProCX 社と共に実施した過去調査当時、

十分な調査が行われなかった点について、現在もなお、その経緯及び理由を明らかにできていない。

この点、BS 社の組織的安全管理措置は、個人データ等の取扱状況の把握及び安全管理措置の見直しの点について、ProCX 社と同様にいまだ不備があり、法第 23 条の違反状態が現在も続いているものと認められる。

(2) 人的安全管理措置（従業者の教育）

BS 社は、本件事案を受けて、2023 年 12 月７日、８日、個人データ等を取り扱う業務にあたる担当者へ講じた再発防止策について周知を行い従業者への教育を行っている。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、更なる従業者への教育の充実が図られることも期待した上で、今後、確実に実施されることを注視する必要がある。

(3) 物理的安全管理措置（保守拠点への USB メモリの持ち込み）

BS 社は、保守拠点への入室に際し、ルール及び実際の運用の双方において、USB メモリ等の外部記録媒体の持ち込みがチェック及び制限されていないことについて、不適切な外部記録媒体の利用を牽制するため監視カメラに記録を取っているものの、保守拠点内の作業には外部から PC 端末等の媒体を持ち込む必要があるとの理由から、現時点でも USB メモリ等の外部記録媒体の持ち込みに関してチェック及び制限を実施していない。

この点、BS 社は、後記(4)エ私物 USB メモリの接続制限を行う再発防止策により、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

(4) 技術的安全管理措置

ア システム管理者アカウントのアクセス制御

BS 社は、前記(1)イのとおり、再発防止策を講じている。

イ システム管理者アカウントの共用

BS 社は、共用していたシステム管理者アカウントは速やかに使用停止し、2023 年８月９日に個人データ等を取り扱う役割を担う者２名に個人単位でアカウントの払い出しを行い、その後、他人とのアカウント共用禁止を従業者に通知した。また、今後個人単位のアカウントについて、多要素認証を導入することを検討している。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

ウ 保守端末への個人データ等のダウンロード

BS 社は、2023 年８月５日、保守端末と PDS サーバとの間に中継サーバを設置することで、保守端末からはデータの閲覧のみを行うよう技術的な対策を行ってい

る。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

エ　私物 USB メモリの接続制限

BS 社は、2023 年 7 月 18 日、保守端末に保存された情報を USB メモリ等の外部記録媒体へ書き出すことができないよう技術的な対策を実施した。加えて、同年 10 月 16 日、未登録の USB メモリ等の外部記録媒体が接続された場合は、即時に管理職へアラートが発報されるよう内部不正監視システムを導入した。

この点、BS 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

3　ProCX 社ー委託先の監督（法第 25 条）

(1)　ProCX 社と BS 社との取り決め

ProCX 社は、コールセンターサービス利用契約を補完する目的で、2023 年 10 月 19 日、BS 社との間で「お客様情報の取扱いに関する覚書」を締結し、BS 社の個人データ等の取扱いに関する安全管理措置の実施状況を確認する取り決めを定めた。

この点、ProCX 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、取り決めの内容が適切であるか等、確実に実施されることを注視する必要がある。

なお、ガイドライン 3-4-4(3)においては、「委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データの取扱方法等について、委託先から事前報告を受け又は承認を行うこと、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第 23 条に基づく安全管理措置を講ずることを十分に確認することが望ましい」と示している。本件において、委託関係が生じたコールセンター業務の大量かつ様々な顧客層の個人情報を取り扱う特性を鑑みると前記ガイドラインのとおり可能な限り対応することが望まれるものであり、特に、ProCX 社が本件委託元に対し再委託の報告を行う必要があることを取り決めていたにもかかわらず、個人データ等の取扱いを再委託することを本件委託元に対して報告していない場合には、この点が、法上において、委託元が適切に監督を行う義務を果たすために重要な点であることからすれば、早急に再委託について報告して承認を得ることが望ましい。

(2)　定期的な監査等

ProCX 社は、2023 年 10 月 19 日、BS 社に対して、個人データ等の取扱いに関する作業管理簿、ログ等について提出することを求め、同年 10 月 31 日、ProCX 社の責任者において確認を行っており、同日以降、週次で BS 社の個人データ等の取扱いに関

するログ分析結果の確認を行っている。

この点、ProCX 社が講じた本再発防止策は、一定の改善が認められるものであるが、今後、確実に実施されることを注視する必要がある。

第５　当委員会の対応

１　事案の重大性について

本件事案は、判明しているだけでも約 928 万人分と大量の個人データ等が長期にわたり漏えいした事案である。また、Ｘにより持ち出された大量の個人データ等が名簿業者に売却された可能性が高く、民間事業者 30 社、独立行政法人１機関及び地方公共団体 38 団体の多数の委託元に関わるコールセンター業務で取り扱われた個人データ等に影響があったもので、当該個人データ等の性質として、企業の商品購入履歴があること又は地方公共団体の住民であること等から推測することにより、年齢、性別、利用企業及び行動範囲等で分類し、嗜好性又は経済状況といった特徴を分析され、悪用されることが懸念される。

このような本件事案の重大性、影響を受けた個人データ等の量及びその性質を考慮した上で、適切な権限行使を行う必要がある。

２　指導及び勧告について

(1)　ProCX 社

ア　法第 148 条第１項に基づく勧告

本件では、個人データ等の不正な持ち出しが 2013 年から 2023 年までの間という長期間にわたって反復的に行われており、個人データ等の数も判明しているものだけで約 928 万人分と多数にのぼっている。また、ProCX 社については、前記第４の１(1)で述べたとおり、過去調査における不適切な調査報告の経緯及び原因を未だに明らかにできていないため当委員会への報告もできていない状態であり、自社における個人データ等の取扱状況を把握するための組織体制が、現状においても十分でない。ProCX 社が現在においても、多数の個人情報取扱事業者及び行政機関等から、個人データや保有個人情報の取扱いを委託され、コールセンター業務を実施していることからすると、この状態を放置しておくことは、個人の権利利益を侵害するおそれが高い。したがって、法第 148 条第１項に基づき、法第 23 条の規定違反（組織的安全管理措置の不備）を是正するために必要な措置として、当該違反行為を是正するために必要な措置をとるよう勧告する。

イ　法第 147 条に基づく指導

その他に確認された法第 23 条が求める安全管理措置及び法第 25 条が求める委託先の監督の不備については、問題点を改善するよう指導する。

ウ　法第 146 条第１項に基づく報告等の求め

過去調査における不適切な調査報告に至った経緯及び原因について、関係資料を添付の上、2024年２月29日までに報告するよう求め、前記の勧告及び指導に対するその後の確実な再発防止策の実施状況について、関係資料を添付の上、同年３月29日までに報告するよう求める。

(2) BS社

ア　法第148条第１項に基づく勧告

BS社に対しては、前記第４の２で述べたとおり、ProCX社と同様、過去調査における不適切な調査報告の経緯及び原因を未だに明らかとすることができず、自社における個人データ等の取扱状況の把握を行うための組織体制が現状においても十分でない。

BS社がProCX社から委託を受けて、現在においても、多数の個人データ等を取り扱い、業務を継続していることからすると、この状態を放置しておくことは、個人の権利利益を侵害するおそれが高い。したがって、法第148条第１項に基づき、法第23条の規定違反（組織的安全管理措置のうち個人データの取扱状況の把握及び安全管理措置の見直し）を是正するために必要な措置として、当該違反行為を是正するために必要な措置をとるよう勧告する。

イ　法第147条に基づく指導

その他に確認された法第23条が求める安全管理措置の不備については、問題点を改善するよう指導する。

ウ　法第146条第１項に基づく報告等の求め

過去調査における不適切な調査報告に至った経緯及び原因について、関係資料を添付の上、2024年２月29日までに報告するよう求め、前記の勧告及び指導に対するその後の確実な再発防止策の実施状況について、関係資料を添付の上、同年３月29日までに報告するよう求める。

３　本件委託元及び流出先等の調査継続について

本件委託元におけるProCX社及びBS社に対する個人データ等の取扱いに関する監督について問題点がなかったか、確認が必要であるが、本件委託元は計69団体と多岐に渡り、委託していた個人データ等の多寡も様々であることから、今後も継続して調査し、個人データ等の取扱状況や監督上の問題点が認められた場合は、権限行使を含めた必要な対応を検討する。

また、Ｘが本件事案によって持ち出した大量の個人情報を売却したとされる名簿業者に対しても、今後も継続して調査し、法第27条第２項の規定に基づく届出を行っている事業者か否かを確認するとともに、不適正に取得した個人データ等の利用状況について確認し、権限行使も含めた必要な対応を検討する。

４　注意喚起

本件においては、コールセンター業務を運営又は受託している事業者が、安全管理措置、従業者の監督及び委託先の監督について適切な対応を行っているか、コールセンター業務受託事業者の業務の参考となる内容も含めて、資料１－４のとおりコールセンター業務受託事業者へ注意喚起を行う。

以　上