公表資料

個人情報保護委員会
Personal Information Protection Commission

News Release

株式会社 NTT マーケティングアクト ProCX 等における不正持ち出し事案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

令和６年９月 11 日

個人情報保護委員会は、本日、株式会社 NTT マーケティングアクト ProCX 等における不正持ち出し事案に対する個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づく行政上の対応について、以下資料のとおり、取りまとめましたので、お知らせいたします。

【連絡先】
個人情報保護委員会事務局
監視・監督室
電話：03-6457-9680（代）

株式会社NTTマーケティングアクトProCX等における不正持ち出し事案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
【概 要 資 料】

令和６年９月11日
個人情報保護委員会

第１　事案の概要

１　株式会社NTTマーケティングアクトProCX（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。以下「ProCX社」という。）は、多数の民間事業者及び地方公共団体等から委託を受け、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。）を行っている。

２　本件は、平成25年７月頃から令和５年２月頃にかけて、ProCX社のコールセンター業務に関するシステムの提供及び保守運用を行っている 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。以下「BS社」という。）の元従業者（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、委託元である民間事業者30社、独立行政法人１機関及び地方公共団体38団体（以下まとめて「本件委託元」という。）の顧客又は住民等に関する個人データ等合計約928万人分を不正に持ち出したことにより漏えいが発生し、Xが名簿業者に売却した事案である。

第２　ProCX社及びBS社に対する対応状況

１　これまでの経緯

⑴　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社」という。）は、令和４年１月から３月に、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、県警察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、令和４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ところ、ProCX社は、BS社と共に調査（以下「本件過去調査」という。）を実施したが、同年７月に、A社に対し、個人データの漏えいは確認されなかった旨を報告している。

⑵　個人情報保護委員会（以下「当委員会」という。）は、令和５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」という。）第 146 条第１項の規定により、漏えい事態の詳細、両社の安全管理措置の実施状況、本件過去調査等について報告等を求め、これについて、同年 11 月 10 日、両社から報告書を受領した。しかしながら、同報告書では、ProCX 社及び BS 社は、本件過去調査において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及び原因の解明には至っていないとして、明らかにしなかった。

⑶　当委員会は、令和６年１月 24 日、ProCX 社及び BS 社に対し、本件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ことは、両社の組織的安全管理措置（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）について不備があり、法第 23 条に違反していると認定し、法第 148 条第１項の規定により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した。また、その他に確認された ProCX 社及び BS 社の安全管理措置等の不備については、問題点を改善するよう法第 147 条の規定により指導を行った。

⑷　ProCX 社及び BS 社は、当委員会に対し、令和６年２月 29 日に、本件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関する報告書を提出し、同年３月 29 日に、再発防止策の実施状況に関する報告書を提出した。

２　勧告に対する是正状況

ProCX 社及び BS 社は、当委員会が、本件過去調査においてＡ社に事実とは異なる内容を回答した経緯及び原因を調査し、問題点を明らかにするよう勧告したことに対し、令和６年２月 29 日付け報告書において、本件過去調査を検証し、複数の問題点があったものの、漏えいに繋がる端緒を意図的に隠蔽したものではなかったと結論付けている。また、発覚した複数の問題点についても、両社は、NTT 西日本が設置した調査委員会からの再発防止策の提言を受け、計画どおり同再発防止策を実施しており、ProCX 社及び BS 社における勧告に係る措置は現時点において一定の取組が認められるものである。

詳細は、別紙１「当委員会からの勧告等に対する是正状況の概要」参照。

３　指導に対する改善状況

ProCX 社は、当委員会からの人的安全管理措置（従業者の教育）及び委託先の監督（ProCX 社と BS 社との取り決め）の不備に関する指導に対して、再発防止策を実施しており、改善が認められた。

BS 社は、当委員会からの組織的安全管理措置（自主点検及びログの分析）、人的安全管理措置（従業者の教育）、物理的安全管理措置（USB メモリの利用）及び技術的安全管理措置（システム管理者アカウントのアクセス制御・システム管理者アカウントの共用・保守端末への個人データのダウンロード）の不備に関する指導に対して、再発防止

策を実施しており、改善が認められた。

詳細は、別紙１「当委員会からの勧告等に対する是正状況の概要」参照。

第３　本件委託元に対する対応状況

１　これまでの経緯

当委員会は、令和６年４月 26 日から同年５月 10 日にかけて、本件委託元に対し、法第 146 条第１項又は法第 156 条の規定により報告等を求め、本件委託元による ProCX 社及び BS 社に対する監督状況を調査してきた。

２　本件委託元への対応

調査の結果、事案発生当時の本件委託元には、ProCX 社との間の委託契約書における取り決め及び ProCX 社の個人データ取扱状況の把握について、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）及び個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）で求める委託先の監督措置と比較し、不十分な点があることが判明した。

本件事案におけるＸによる不正持ち出しは、所属組織である BS 社においても長年気付けずにいたものであるため、本件委託元による委託先の監督措置の不備が原因で不正持ち出しの未発覚に至ったとまではいえないものの、本件事案による気付きを個人データの取扱いの委託を行う委託元全般に注意喚起することにより、委託先の取扱実態も含めて適切に監督を行うことへの意識を高めてもらえることに期待する。

詳細は、別紙２「委託元に対する調査結果について」参照。

第４　名簿業者に対する対応状況

１　これまでの経緯

Ｘが持ち出した個人データの提供先について情報収集に努めてきたところ、岡山県警察及び ProCX 社からの情報提供、令和６年５月 23 日に開かれた岡山地方裁判所津山支部での公判時のＸの供述等により、持ち出した個人データが株式会社中央ビジネスサービス及びネクストステージ合同会社に売却されたことが明らかとなったため、当委員会は、同年６月 19 日に株式会社中央ビジネスサービス、同月 20 日にネクストステージ合同会社に対し、法第 146 条第１項の規定による立入検査を行った。

２　名簿業者への対応

当委員会は、株式会社中央ビジネスサービス及びネクストステージ合同会社に対する立入検査を実施し、両社共に、Ｘから個人データを取得していた事実を確認した。

また、当委員会は、両社に対し、Ｘから取得した個人データの削除を求めたところ、両社は既に消去済みである旨を説明し、当委員会において両社の個人情報データベー

ス等から当該データの残存を確認することはできなかった。

両社には、Xからの個人データの取得、提供等に関して法違反が認められたため、以下のとおりの対応を実施した。

⑴　株式会社中央ビジネスサービス

ア　以下のとおり、法違反が認められたため、法第 147 条の規定による指導及び法第 146 条第１項の規定による報告等の求めを実施することとし、今後１年間、３か月ごとに、個人データの第三者提供を受けた状況及び個人データの第三者提供をした状況を報告させることによって、株式会社中央ビジネスサービスの法遵守状況を注視していくこととする。

①　不適正取得（法第 20 条第１項の規定違反）

Xから大量の個人データを取得するに当たり、Xによる個人データの提供が法第 27 条第１項の規定に違反すること（第三者提供についての本人同意を得ていない等）を知り、又は容易に知ることができるにもかかわらず、Xから個人データの提供を受けて個人情報を取得していた行為は、法第 20 条第１項の規定に違反する。

②　第三者提供を受ける際の確認義務（法第 30 条第１項第２号）違反

Xから個人データの提供を受けるに際し、Xから当該個人データの取得の経緯の確認を行っていなかった。

イ　当委員会が法第 146 条第１項の規定により実施した報告等の求めに対し、虚偽の報告をした事実が確認されたため、刑事告発を実施する。

⑵　ネクストステージ合同会社

以下のとおり、法違反が認められたため、法第 147 条の規定による指導及び法第 146 条第１項の規定による報告等の求めを実施することとし、今後１年間、３か月ごとに、個人データの第三者提供を受けた状況及び個人データの第三者提供をした状況を報告させることによって、ネクストステージ合同会社の法遵守状況を注視していくこととする。

①　不適正取得（平成 27 年改正法[1]第 17 条第１項の規定違反）

Xから大量の個人データを取得するに当たり、Xによる個人データの提供が平成 27 年改正法第 23 条第１項の規定に違反すること（第三者提供についての本人同意を得ていない等）を知り、又は容易に知ることができるにもかかわらず、Xから個人データの提供を受けて個人情報を取得していた行為は、平成 27 年改正法第 17 条第１項の規定に違反する。

②　第三者提供の制限（法第 27 条第１項）違反

令和４年４月以降、法第 27 条第２項本文の規定（オプトアウト規定）によ

[1] 個人情報の保護に関する法律及び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の一部を改正する法律（平成 27 年９月９日法律第 65 号）により改正された個人情報の保護に関する法律をいう。

り、Xから法 20 条第１項の規定に違反して取得した個人データを第三者に提供することは禁止されており（同項ただし書[2]）、本人同意を得ることなく当該個人データを第三者に提供していた行為は、法第 27 条第１項の規定に違反する。

③　第三者提供を受ける際の確認義務（平成 27 年改正法第 26 条第１項第２号）違反

Xから個人データの提供を受けるに際し、Xから当該個人データの取得の経緯の確認を行っていなかった。

⑶　詳細は、別紙３「株式会社中央ビジネスサービス及びネクストステージ合同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」参照。

以　上

[2] 令和４年４月１日に追加施行された。

当委員会からの勧告等に対する是正状況の概要

別紙１

□ 勧告に対する是正状況

株式会社NTTマーケティングアクトProCX（以下「ProCX社」という。）及び NTTビジネスソリューションズ株式会社（以下「BS社」という。）の是正状況

１．令和４年４月、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社」という。）がProCX社に調査を依頼し、これに対し、ProCX社がBS社と共に実施した調査（以下「本件過去調査」という。）に関する検証

(1)本件過去調査の経緯

本件過去調査は、ProCX社社長、ProCX社担当部長（BS社兼務）、ProCX社担当課長及びBS社担当課長２名の計５名が関与し、ProCX社及びBS社は、Ａ社に対して、令和４年４月15日から同年７月15日にかけて、複数回の回答を提出した。

それらの回答においては、ProCX社及びBS社からＡ社の顧客情報が流出していないかについて、エクスポートログの十分な調査がなされず、短期間で表面的にログの確認を行っただけで、ProCX社及びBS社において個人データの漏えいは確認されなかったものと結論付けられていた。また、エクスポートログの一部改変、USBポートの設置状況と暗号化ソフトの導入状況に関する虚偽回答、Ａ社からのシステム管理者体制変更の依頼に対する虚偽回答、データ消去状況に関する虚偽回答及びシステム保守作業体制に関する虚偽回答も含まれていた。

ProCX社及びBS社は、顧客であるＡ社の依頼であるにもかかわらず、本件過去調査を軽視し、調査を行うためのシステム及びセキュリティの仕様を理解した人員を調査に加えず、Ａ社との取引を継続したい又はＡ社からの追加質問を回避したいといった意図を優先し、十分な調査を行わず、虚偽回答を含むＡ社への回答を行った。

(2)本件過去調査の問題点

令和６年２月29日付け報告書によれば、ProCX社の担当者においては、BS社に対して個人データの取扱いを委託しているとの認識がなかったこと、本件過去調査の司令塔的役割を果たす人物の不在、顧客企業であるＡ社と対話する姿勢の欠如及び規程に基づく適切なエスカレーションがなかったことといった問題点があり、BS社においても、長年システム運用保守従事者による情報漏えいを想定した情報セキュリティ体制が敷かれていなかったこと及び規程に基づく適切なエスカレーションがなかったことといった問題点があった。

なお、本件過去調査の当時、ProCX社及びBS社の調査担当者らが、内部からの情報漏えいの事実を認識しつつ、積極的かつ意図的に隠蔽したといった形跡は確認されなかった。

□ 勧告に対する是正状況（続き）

ProCX社及びBS社の是正状況

２．組織的安全管理措置に関するProCX社の再発防止策の実施状況

ProCX社は、西日本電信電話株式会社（以下「NTT西日本」という。）と協働し、本件で問題となったコールセンター業務用システム（以下「本件システム」という。）、顧客情報を保有する全てのシステム及び機密性の観点の重要度が「高」と分類されているシステムについて、詳細な点検項目を設定の上、令和５年９月及び10月並びに令和６年１月に点検を実施した。ProCX社は、この点検を通じて、個人情報の取扱状況を把握するとともに、コンタクトセンターで使用する端末について、個人端末の接続が適切に制限されていないこと等のシステム上の不備を発見した。

これを受けて、ProCX社は、システム的な対処及び運用面での対処を実施し、又は実施することを決定し、具体的には、以下のような対応をとった。

(1)リスクの視える化に関する措置
- ProCX社保有の全システムについて、内部不正による顧客情報流出の未然防止等の観点も含めたリスクの把握・視える化を実施（「リスク管理データベース」の作成）した。
- ProCX社コールセンターにて運営する全業務に対し、内部不正による顧客情報流出の未然防止等の観点も含めたリスクアセスメントシートの活用によるリスクの可視化を実施した。

(2)リスク箇所の最小化に関する措置
- 外部脅威にさらされるリスクを最小限のものとするため、従来はシステムごとにネットワークを構築し対策していた外部脅威について、各ネットワークを１つの閉域網内に集約するとともに、高度なマルウェア等によるサイバー攻撃に対する備えとしてEDR（※）を導入することで、早期の攻撃検知、防御及び駆除が可能となるよう対策を推進（業務用ネットワークの集約）している。
- 物理的な端末識別子による接続端末の管理を行い、未承認端末のアクセス制限を行い、利用が許可されていない端末のネットワークへの接続防止対策を推進している。
- ログ収集と点検を集中管制できるよう、資産管理システムを導入（監査ログの集中管理）した。
- 統合アカウント管理のためのシステムを導入し、利用されているアカウントを特定し、アカウントの集中管理を実現した。
- コールセンターにおけるUSBメモリを利用した個人情報の取扱いについて、顧客企業のルールにより指定されたものを除き撤廃（USBメモリの利用制限）した。

(3)監視の高度化・点検の徹底に関する措置
- EDR等のエンドポイント管理技術を導入し、異常行動の検知の高度化（通常では想定されない時間帯でのアクセスや禁止されたサイトへのアクセス等の自動検知等）による個人データ流出の未然防止及び追跡が可能な仕組みとすることで、内部不正及び外部脅威への監視強化に向けた対策を推進している。

(4)情報セキュリティ推進体制の強化
- NTT西日本と協働し、コールセンター運営の実態を踏まえ、事業部門が策定した各対策が適切に設計・運営されているかをモニタリング・監視する専担部門を新設することにより牽制機能を強化した。
- 全社横断的に情報システムに求める統一的なセキュリティ要件を定め、情報セキュリティマネジメントシステムを設計、構築、運用及び保守する仕組みを新設することにより、安全管理措置の実装を強化した。
- 事業部門及び管理部門に対する監督・是正権限を有する内部監査部門として実施した監査結果を取締役会に直接報告する体制に見直すことで、より実効的に情報セキュリティに関するガバナンスを確保する組織体制を構築した。
- エスカレーションの必要性の浸透、手順の明確化、研修等を通じてエスカレーションの徹底を図っていくべく、ビジネスリスクマネジメントマニュアルに基づき、派遣社員等を含む全従業者に対し、エスカレーションルールの再徹底を指示した。

（※）EDR（Endpoint Detection and Response）：PC等のエンドポイントの不審な挙動を検知・防御する仕組み

□ 勧告に対する是正状況（続き）

ProCX社及びBS社の是正状況

３．組織的安全管理措置に関するBS社の再発防止策の実施状況

BS社もProCX社と同様に、安全管理措置の見直しとして、本件システムにおけるシステム的な対処及び運用面での対処を速やかに実施した。併せて、NTT西日本と協働し、顧客情報を保有する全てのシステム及び機密性の観点の重要度が「高」と分類されているシステムについて点検を実施した。BS社は、これらの点検を通じて個人情報の取扱状況を把握するとともに、不備事項については運用対処を含む是正措置として、以下のような対応をとった。

(1)リスクの視える化に関する措置
- 本件システムを含むBS社保有の全システムについて、内部不正による顧客情報流出の未然防止等の観点も含めたリスクの把握・視える化を実施（「リスク管理データベース」の作成）した。
- 上記に基づき、システムごとのセキュリティリスク状況を評価し、適切に把握している。

(2)リスク箇所の最小化に関する措置

本件システムについて、以下の対処を実施した。
- 使用を許可されていない私有USBメモリ等の外部記録媒体の接続防止措置
- 中継サーバの設置による保守端末への顧客データのダウンロードの禁止（個人データは閲覧するのみに制限）
- 保守拠点における保守端末からのインターネットアクセス接続の無効化（ウェブメール等の使用を制限）
- 保守拠点における私有端末によるシステムへのアクセス無効化
- BS社のシステム保守担当者へ本件システムからの個人データのダウンロード権限を与えない保守等運用形態への変更
- 統合アカウント管理のためのシステムの導入によるアカウントの集中管理
- ProCX社との契約内容を変更し、本件システムの保守業務において、原則、個人データを取り扱わないこととする運用に変更

(3)監視の高度化・点検の徹底に関する措置

本件システムについて、以下の対処を実施した。
- USB接続時に、複数の管理監督者によって不正利用でないことをリアルタイムに監視するため、複数の管理監督者へ接続アラームメールが発出される仕組みを導入した。
- USBメモリの利用が必要な際、専用端末（管理監督者のみ利用可能）に限定し、さらに、複数の管理監督者が承認しないと実施不可能な仕組みを導入した。
- USBメモリの利用記録簿の記載をルール化したうえで、利用記録簿と作業ログとの突合による定期チェック等を実施している。
- 保守作業環境へセキュリティカメラを設置し、物理的な監視を実施している。
- 個人データ閲覧で利用する中継サーバに対する振る舞い検知を実施するためEDRを導入し、各種保守作業時のアクセスには、正当なアクセス権を有する者であることを識別するため多要素認証を導入した。

(4)情報セキュリティ推進体制の強化
- 本件システムの担当部署にセキュリティ担当者を段階的に増員した（令和６年４月～７月）。
- BS社の管理部門強化として、BS社における情報セキュリティに関する推進者の明確化、BS社独自システムへの適正な対処等の課題解決促進に向け「セキュリティ＆トラスト推進室」を新たに設置した（令和６年７月）。
- 情報セキュリティに関する監査項目を追加し、事業部門及び管理部門のガバナンスが正しく機能しているか等の監査強化を図る等、NTT西日本の内部監査部と連携し、BS社における内部監査機能の拡充を実施する。
- エスカレーションの必要性の浸透、手順の明確化、研修等を通じてエスカレーションの徹底を図っていくべく、ビジネスリスクマネジメントマニュアルに基づき、派遣社員等を含む全従業者に対し、エスカレーションルールの再徹底を指示した。

□ その他指導事項に対するProCX社の改善状況

	指導事項	再発防止策の実施状況
１．人的安全管理措置（従業者の教育）		
	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、一般的なセキュリティ知識が記載された資料を用いて年１回定期的な研修を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、委託元の顧客又は住民等に関する多くの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、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。	ProCX社は、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事業者として、あらためて社長自ら、情報セキュリティが事業の根幹であること、一人一人が「自分ごと」として顧客情報管理の徹底に取り組むことを従業者にメッセージ発信するとともに、各エリアでのタウンホールミーティングを行い、直接、従業者の意識醸成を図るとともに意見交換を実施した。 また、令和５年12月７日及び８日に、個人データを取り扱う業務に当たる従業者に対し、再発防止策を周知し従業者教育を実施した。 さらに、当委員会からの指導を受けて、令和６年３月29日までに取締役を含む管理者170名に対し、委託先管理及び本件不正持ち出し事案の振り返りを含む情報セキュリティ対策の在り方について、リスクマネジメント強化研修を複数回実施し、令和６年８月にはProCX社への転入管理者及び新任管理者に対しても同様に研修を実施した。 加えて、コールセンター業務に携わるセンター所長、ジョブマネージャー、SV（コールセンター管理者）といった役職者及びこれらの役割を担う従業者に対して、本件事案の振り返りを含む今後の情報セキュリティ対策の在り方について、映像教材を作成し受講させる等のコールセンター業務従事者に特化した研修を令和６年３月末までに実施した。 今後においても、これらリスクマネジメント強化研修及びコールセンター業務従事者に特化した研修について、年間を通じ継続して実施することで、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事業者としての研修体制の充実に取り組むこととしている。
２．委託先の監督（ProCX社とBS社との取り決め）		
	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、実態として個人データの取扱いを委託していた。 また、ProCX社は、コールセンター業務の履行に当たり、一部の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社に個人データを取り扱わせていた。 さらに、ProCX社は、委託元の大量の個人データ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の取扱状況を適切に把握していなかった。	ProCX社は、BS社に対して令和５年10月19日、BS社との間で個人情報取扱いに関する覚書を締結し、BS社の個人データ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ProCX社の立入検査権限や報告要求権限等を定めた。 また、当委員会からの指導を受けて、令和６年１月26日、同覚書を改訂し、システムバックアップ、セキュリティ上の問題への対処及びサービスの故障発生等の場面を除き、BS社が個人データを取り扱わないこととした。 くわえて、BS社における物理的・技術的安全管理措置の履行状況を確認するため立入点検を行い、BS社において適切に対処されていることを確認した。

□ その他指導事項に対するBS社の改善状況

	指導事項	再発防止策の実施状況
１．組織的安全管理措置（自主点検及びログの分析）		
	BS社においては、実際、不正持ち出し行為者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、同行為者による個人データ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。	本件システムにおいて、作業記録簿の記載をルール化した上で、作業記録簿と作業ログとの突合による定期チェック等を実施している。 ※ 本件システム以外の一部システムにおいては、作業記録簿と作業ログとの突合による定期チェックの実施や振る舞い検知アラートに基づくヒアリング調査等を実施した。特権ID操作ログの定期チェックによる内部不正監視の強化についても今後導入を検討中としている。 ※ NTT西日本が新たな情報セキュリティ推進部署を立ち上げ、BS社を含むNTT西日本グループ各社の事業部署を集中的に監査するとともに、BS社を含むNTT西日本グループ各社の監査部署を支援する新体制を構築した。NTT西日本の情報セキュリティ推進部署による支援の下、BS社の監査部署が、BS社の事業部署に対し、定期的に監査を実施する予定としている。
２．人的安全管理措置（従業者の教育）		
	BS社は、従業者に、年１回研修等の取組を実施していたが、本件事案における不正持ち出し行為者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。	BS社は、令和５年12月７日及び８日、個人データを取り扱う業務に当たる従業者に対し、再発防止策を周知し従業者教育を行った。さらに、当委員会からの指導を受けて、令和６年２月29日、本件不正持ち出しが発生した部署の全従業者を対象に、再発防止策の徹底に関する意識付けを実施した。 令和６年度は、BS社の全社員を対象に「タウンホールミーティング」を実施し、社員の意識醸成を図っている。また、NTT西日本グループ全体で年に一回実施している全従業者向け研修に加え、NTT西日本グループ全体において、データ書き出し権限を保有する実務者層や、システム運用管理のマネジメント層に対し、階層別に、個人情報の適正な取扱いに係る研修を予定しており、令和６年６月に、管理者としての業務マネジメントにおいて必要な情報セキュリティ知識の習得を目的とした転入管理者向けの研修を実施した。
３．物理的安全管理措置（USBメモリの利用）		
	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、私有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。また、保守端末については、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、私有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。	BS社は、本件システムにおいて、令和５年７月18日、保守端末に保存されたデータを、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（外部記録媒体への書き込みアクセス権をシステム上、拒否する設定）を実施している。 ただし、BS社の保守運用業務では、外部の協力会社による故障原因調査等を行う場合に、保守端末に保存されたデータをUSBメモリ等によって外部送信用端末へ移さなければならないことがある。そこで、やむを得ずデータをUSBメモリに書き出す必要があるときは、管理監督者のみが利用可能な専用端末に限ってUSBメモリへのデータ書き出しを行えることとし、さらに、専用端末へのUSBメモリ接続時には複数の管理監督者に対しメール通知が発出されること、データ書き出しを行うためには操作する管理監督者とは別の管理監督者のクロスチェックを必須とすること、作業を終えた後はUSBメモリ内のデータを即時に削除する運用とした。

□ その他指導事項に対するBS社の改善状況（続き）

	指導事項	再発防止策の実施状況
４．技術的安全管理措置（システム管理者アカウントのアクセス制御）		
	BS社では、本件システムに保存する個人データ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。	BS社では、本件システムにおいて、顧客データのダウンロードが可能なシステム管理者アカウントについて、共用アカウントの利用を停止した上で、業務上必要な最小限の範囲である担当者２名に対し、個人単位のアカウントを付与した。 さらに、ProCX社と協議し、令和６年１月26日以降は、BS社がシステム管理者アカウントを用いて行っていたProCX社コールセンター管理者からの問合せに伴い個人データをダウンロードする業務を、ProCX社が自ら行うこととし、業務分担を変更した。これにより、BS社がシステム管理者アカウントを用いる業務上の必要性が生じないようにした上で、同年２月２日、BS社従業者に付与していたシステム管理者アカウントについて削除した。
５．技術的安全管理措置（システム管理者アカウントの共用）		
	BS社では、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。	前記４のとおり、本件システムにおいて、BS社による本件システムからの顧客データのダウンロードが可能なシステム管理者アカウントの利用は廃止され、以降、ProCX社においてコールセンター管理者からの問合せの対応窓口を設置し、アカウントを共用せず、窓口担当者に適切にアカウントを付与する運用とした。
６．技術的安全管理措置（保守端末への個人データのダウンロード）		
	BS社では、本件システムに保存された個人データを、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。	BS社は、令和５年８月５日、保守端末と本件システム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ダウンロードを不可とし、閲覧のみ可能となるよう技術的な対策を行っており、当委員会からの指導を受けた以降も同対策を継続している。

別紙２

委託元に対する調査結果について

第１　本件委託元の回答内容

１　株式会社 NTT マーケティングアクト ProCX（以下「ProCX 社」という。）との間の委託契約書における取決め

⑴　委託契約書における個人情報の取扱いに関する安全管理条項の有無

（評価対象団体数：60 団体[1]）

個人情報を含むデータの授受における安全管理措置に関する条項		ProCX 社における個人情報の保管についての安全管理措置に関する条項		委託業務終了時の個人情報の廃棄についての安全管理措置に関する条項	
あり	49 団体、82%	あり	53 団体、88%	あり	51 団体、85%
なし	11 団体、18%	なし	７団体、12%	なし	９団体、15%

なお、本件委託元のうち７団体（全て民間事業者）では、ProCX 社との契約において、上記３つの安全管理条項が、いずれも「なし」となっていた。

⑵　再委託の禁止又は制限に関する条項の有無

（評価対象団体数：60 団体）

あり　　＝　58 団体、97%

なし　　＝　２団体、３％（全て民間事業者）

⑶　契約の締結時又は役務提供時、個人情報の取扱いの再委託があるかについての確認の有無

（評価対象団体数：57 団体[2]）

あり　　＝　24 団体、42%

なし　　＝　33 団体、58%

⑷　上記⑶で、再委託があるかについて確認を行っている場合の確認方法

（評価対象団体数：24 団体）

書面　　＝　17 団体、71%

口頭　　＝　７団体、29%

---

[1] 本件委託元 69 団体のうち、現時点で契約書類等が不存在であり全項目に対して回答不能とした９団体を⑴・⑵・⑶・⑷及び２⑴・⑵の項目の集計から除外した。

[2] 60 団体のうち、契約中の作業状況を把握するための記録が確認できず回答不能とした３団体を⑶・⑷及び２⑴・⑵の項目の集計から除外した。

２　委託先の個人データ取扱状況の把握

⑴　ProCX 社の個人データ取扱状況の把握

本件委託元における委託先である ProCX 社における個人データ取扱状況の把握の実施状況は、次のとおりであった。

（評価対象団体数：56 団体[3]）

契約の締結時等に、ProCX 社に対して、個人情報の取扱いに関する規律の確認を要求する		契約の役務提供時に、書面で報告を受けるなどProCX 社における個人情報の取扱状況を把握する		契約の役務提供時に、ProCX 社の執務環境を実地確認等し、ProCX 社における個人情報の取扱状況を把握する	
あり	31 団体、55％	あり	33 団体、59％	あり	22 団体、39％
なし	25 団体、45％	なし	23 団体、41％	なし	34 団体、61％

なお、本件委託元のうち 14 団体（民間事業者が６社、地方公共団体が８団体）では、ProCX 社への上記３つの監督状況が、いずれも「なし」となっていた。

⑵　NTT ビジネスソリューションズ株式会社（以下「BS 社」という。）への監督について

（評価対象団体数：57 団体）

本件委託元は、いずれも、ProCX 社との契約締結時又は ProCX 社の役務提供時に、ProCX 社が BS 社に個人データ等の取扱いを再委託することについて説明を受けておらず、BS 社による個人データの取扱いを把握する機会がなかったため、監督することができなかったという回答結果であった。

第２　調査結果に対する評価

１　本件委託元による ProCX 社に対する監督

⑴　調査の結果、ProCX 社との間の委託契約書に安全管理条項の記載がない団体が７団体（全て民間事業者）あり、ProCX 社における個人データ取扱状況の把握が行われていない団体が 14 団体（民間事業者が６社、地方公共団体が８団体）あることが判明した。詳細は、下記の一覧表のとおりである。

[3] 57 団体のうち、一切の契約書類及び記録が保存年限経過済みのため残っておらず回答不能とした１団体を２⑴の項目の集計から除外した。

【 民間事業者 】

事業者名	不正持ち出しの影響を受けた本人数	委託期間	委託契約書の安全管理条項なし[4]	ProCX 社への監督なし[5]
B社	約 231,000 人	平成 27 年３月～平成 29 年３月	全てなし	あり
C社	約 88,000 人	平成 25 年 12 月～令和３年２月	全てなし	全てなし
D社	約 63,000 人	平成 27 年５月～同年７月	全てなし	全てなし
E社	約 61,000 人	平成 28 年１月～令和５年３月	全てなし	あり
F社	約 39,000 人	平成 27 年３月～同年５月	全てなし	あり
G社	約 26,000 人	平成 27 年３月～同年 10 月	全てなし	全てなし
H社	約 16,000 人	平成 29 年９月～令和４年 11 月	あり	全てなし
I 社	約 12,000 人	平成 27 年 12 月～平成 28 年３月	全てなし	全てなし
J 社	約 4,000 人	平成 30 年 10 月～平成 31 年２月	あり	全てなし

【 地方公共団体 】

K団体	約 28,000 人	平成 28 年８月～平成 29 年 12 月	あり	全てなし
L団体	約 3,000 人	令和２年 10 月～令和３年３月	あり	全てなし
M団体	約 3,000 人	平成 27 年７月～平成 28 年３月	あり	全てなし
N団体	約 2,000 人	平成 29 年６月～平成 30 年 12 月	あり	全てなし
O団体	約 2,000 人	平成 28 年～令和元年	あり	全てなし
P団体	約 2,000 人	平成 27 年～平成 30 年	あり	全てなし
Q団体	約 2,000 人	平成 26 年６月～平成 28 年 12 月	あり	全てなし
R団体	約 2,000 人	平成 29 年６月～同年８月	あり	全てなし

[4] 「個人情報を含むデータの授受における安全管理措置に関する条項」、「ProCX 社における個人情報の保管についての安全管理措置に関する条項」、「委託業務終了時の個人情報の廃棄についての安全管理措置に関する条項」の全ての項目について「なし」と回答したもの。

[5] 「契約の締結時等に、ProCX 社に対して、個人情報の取扱いに関する規律の確認を要求していたか」、「契約の役務提供時に、書面で報告を受けるなど ProCX 社における個人情報の取扱状況を把握していたか」、「契約の役務提供時に、ProCX 社の執務環境を実地確認等し、ProCX 社における個人情報の取扱状況を把握していたか」という全ての項目に「なし」と回答したもの。

⑵　民間事業者については、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。

また、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。）3-4-4 において、委託先の監督について、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に起因するリスクに応じて、(1)適切な委託先の選定、(2)委託契約の締結、(3)委託先における個人データ取扱状況の把握という必要かつ適切な措置を講じなければならないとされている。

委託契約の締結（ガイドライン 3-4-4(2)）では、委託契約書には、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、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が望ましいされているところ、例えば、本件のような他社のコールセンターにおける個人データの取扱いに関する取決めとして、①個人情報を含むデータの授受における安全管理措置に関する条項、②委託先における個人情報の保管についての安全管理措置に関する条項、③委託業務終了時の個人情報の廃棄についての安全管理措置に関する条項を委託契約書に盛り込むことが考えられる。

また、委託先における個人データ取扱状況の把握（3-4-4(3)）では、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が望ましいとされているところ、例えば、今回のような物理的に自社と離れた場所における個人データの取扱状況を適切に把握するための措置として、①契約の締結時等に、委託先に対して、個人情報の取扱いに関する規律の策定又は提出を求める、②契約の役務提供時に委託先から個人情報の取扱状況を書面で報告を受ける、③契約の役務提供時に、委託先の執務環境を実地確認等して個人情報の取扱状況を把握する等の対応を行うことが考えられる。

⑶　地方公共団体等については、法第 66 条において、行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならないと規定されている。さらに、個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）（以下「事務対応ガイド」という。）において、行政機関等が保有個人情報の取扱いを委託する場合は、行政機関等として講ずべき安全管理措置として、サイバーセキュリティに関する対策の基

準等を参考に委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準や委託先の選定基準を整備するとともに、委託先との契約において安全管理措置のために必要な条項を盛り込んだ上で、定期的な監査を行う等、委託先に対して必要かつ適切な監督を行わなければならない（事務対応ガイド 4-3-1-1(3) 委託先の監督）とされている。

今回はほとんどの団体が委託契約書に安全管理条項を盛り込むといった形式面での措置は行えていたものの、定期的な監査を行う等の契約後の実態的な取扱いを監督するための措置が不十分であった団体が見受けられたため、保有個人情報の取扱いを外部に委託する地方公共団体において、委託先における取扱状況の把握に努める必要がある。

２　本件委託元による BS 社に対する監督

本件では、ProCX 社は BS 社へコールセンター業務自体の業務再委託を行っていなかったとの理由から、BS 社への個人データの取扱いの再委託に当たらないと安易に判断し、委託元に対して、BS 社がシステムの保守運用上で個人データを取り扱っていることを知らせていなかった。また、本件委託元からの回答にあるとおり、そのことから、全ての本件委託元において BS 社の個人データの取扱いを把握することができず、委託元が ProCX 社を通じる等して BS 社を監督するに至らなかったものである。

この点、ProCX 社及び BS 社が、法を適切に理解し、委託元への説明を尽くす必要があることはもちろんのこと、委託元においても、ProCX 社が利用するシステムの保守運用状況、それに伴うアクセス権限の付与状況等から個人データの取扱いの有無を確認することで BS 社による個人データの取扱いの存在を把握できる可能性があったものであり、委託元においても、自らが委託した個人データが委託先でどのように取り扱われているか具体的に確認する姿勢が重要となる。

以　上

別紙３

株式会社中央ビジネスサービス及びネクストステージ合同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

第１　事案の概要等

１　事案について

多数の委託元（民間事業者、地方公共団体及び独立行政法人）から委託を受けてコールセンター業務を行っていた株式会社NTTマーケティングアクトProCX(以下「ProCX社」という。）が、NTT ビジネスソリューションズ株式会社（以下「BS 社」という。）にコールセンター業務で用いるシステムの保守運用を委託していたところ、BS 社に所属していた派遣社員（以下「X」という。）が、個人データ合計約 928 万人分を不正に持ち出し、その一部を株式会社中央ビジネスサービス（以下「中央ビジネス」という。）[1]及びネクストステージ合同会社（以下「ネクストステージ」という。）[2]へ売却していた事案である。

２　時系列

日時	経緯
令和５年１月17日	Xが、中央ビジネスに対し、BS 社から持ち出した個人データ約３万人分をメールで送信
令和５年１月18日	中央ビジネスが、Xに対し、上記個人データの購入代金を振込入金
令和５年８月３日	中央ビジネスが、当委員会からの報告等の求め（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」という。）第 146 条第１項）に対し、「（令和４年４月１日～令和５年６月 30 日の期間、第三者から個人データの提供を受けた件数について、回答欄に記載すること。）０」と回答
令和６年６月19日	当委員会が、中央ビジネスに対する立入検査（法第 146 条第１項）を実施
令和６年６月20日	当委員会が、ネクストステージに対する立入検査（法第 146 条第１項）を実施

第２　立入検査で判明した事実関係の概要等

１　中央ビジネス

⑴　中央ビジネスは、平成 28 年から令和５年１月までの間、Xから個人データを取得しており、Xから取得した個人データの合計数は約 650 万人分である。

⑵　中央ビジネスは、Xから個人データを取得するに際し、初回取得時のみ、口頭で「盗品ではない」旨を確認したにとどまり、それ以上にXが個人データを取得した経緯等を確認したことはなかった。

⑶　中央ビジネスは、令和４年３月 31 日までの間、Xから取得した個人データを第三者に提供していた。しかし、同年４月１日以降、中央ビジネスが、Xから取得した個人データを第三者に提供していた事実は確認できなかった。

⑷　中央ビジネスは、Xとの１回の取引において、平均約 10 万件の個人データを取得していた。

---

[1] オプトアウト届出番号 2021-100103。法人番号 9011001052896。
[2] オプトアウト届出番号 2022-100174。法人番号 6010003022002。

⑸　中央ビジネスは、令和５年１月 20 日、Ｘから取得した個人データ等を保存していたPC を岡山県警察に押収され、その後、同個人データ等を削除した上で、中央ビジネスに PC が還付された。

なお、中央ビジネスは、前記 PC の他に、Ｘから取得した個人データ等のバックアップを保管していたが、中央ビジネスは、「バックアップのうち、Ｘから購入した個人データについては全て削除した。」旨を述べており、立入検査時（令和６年６月 19 日）に、Ｘから購入した個人データと思われるデータを発見するには至らなかった。

２　ネクストステージ

⑴　ネクストステージは、令和元年９月 19 日、同年 10 月７日、同年 11 月 15 日、令和２年３月 10 日、同年４月 30 日及び同年７月８日の合計６回にわたり、Ｘから個人データを取得していた。

⑵　ネクストステージは、Ｘから個人データを取得するに際し、Ｘから「提供する個人情報は、不正に取得したものではない。」「個人情報保護法に従い適正に入手したものである。」旨の定型文言をメールで送信させるにとどまり、それ以上に、Ｘに対し、Ｘが当該個人データを取得した経緯等を具体的に確認することはしていなかった。

⑶　ネクストステージは、令和６年２月 29 日までの間、Ｘから取得した個人データを含む全データから、特定の条件で抽出した個人データを、第三者に提供していた。

⑷　ネクストステージは、令和６年２月 29 日、Ｘから取得した個人データを削除した。なお、当委員会は、立入検査時（令和６年６月 20 日）に、ネクストステージが同個人データを削除した痕跡を確認した。

第３　法律上の問題点について

１　中央ビジネス

⑴　不適正取得（法第 20 条第１項違反）[3]

ア　法第 20 条第１項において、個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならないと規定されている。

「不正の手段」には、「偽り」のほかにも、不適法な又は適正性を欠く方法や手続も含まれるところ、第三者が個人データの提供について本人の同意を得ておらず、当該第三者による個人データの提供が法第 27 条第１項の規定に違反することを知り、又は容易に知ることができるにもかかわらず、当該第三者から個人データの提

[3] 平成 28 年～平成 29 年５月 29 日までの取得行為は、平成 15 年５月 30 日に公布された個人情報の保護に関する法律（以下「平成 15 年公布法」という。）第 17 条違反。平成 29 年５月 30 日～令和４年３月 31 日までの取得行為は、個人情報の保護に関する法律及び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の一部を改正する法律（平成 27 年法律第 65 号）により改正された個人情報の保護に関する法律（以下「平成 27 年改正法」という。）第 17 条第１項違反。令和４年４月１日以降の取得行為は、デジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律第 37 号）により改正された個人情報の保護に関する法律（以下「令和３年改正法」という。）第 20 条第１項違反。

供を受けて個人情報を取得することは、法第 20 条第１項違反となる[4]。

イ　本件において、中央ビジネスは、Ｘから個人データを取得するに当たり、Ｘの職業や個人データの取得の経緯、第三者提供についての本人同意の有無等を一切確認しないまま、漫然と１回当たり平均約 10 万件、合計約 650 万件という大量の個人情報を取得していた。

この点、中央ビジネスは、個人データの売買をその主たる業務とし、第三者に個人データを売却する際には、法第 27 条第１項の規定により第三者提供についての本人同意を得ることはせず、法第 27 条第２項本文の規定による個人データの提供を行う個人情報取扱事業者（以下、「オプトアウト届出事業者」という。）であり、多人数の本人全員から第三者提供についての同意を得ることが極めて困難であることは、当事者として十分に認識していたはずである。

したがって、本件においても、中央ビジネスは、Ｘから大量の個人データを取得しており、Ｘが第三者提供についての本人同意を得ることなく個人データの提供をしようとしていることは当然に想定することができ、中央ビジネスは、Ｘに本人同意の証跡の提出を求める等の方法によって、Ｘが本人同意を得ていないことを容易に知ることができた。

なお、個人データの提供についての本人の同意を得ていなくとも、Ｘがオプトアウト届出事業者として個人データの第三者提供を行っていた場合は、法第 27 条第１項違反には該当しないが[5]、Ｘがオプトアウト届出事業者ではないことは、当委員会のウェブサイトにより容易に確認することができ、中央ビジネスにおいても、Ｘがオプトアウト届出事業者であるとは認識していなかった。

したがって、中央ビジネスは、法第 27 条第１項に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、Ｘから個人情報を取得していたといえ、かかる取得行為は法第 20 条第１項の規定に違反する。

⑵　第三者提供を受ける際の確認義務違反

法第 30 条第１項[6]において、個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、当該第三者による当該個人データの取得の経緯について確認を行わなければならないこととされ、個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号。以下「規則」という。）第 22 条第２項[7]において、「法第 30 条第１項の規定による同項第

---

[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（通則編）3-3-1【個人情報取扱事業者が不正の手段により個人情報を取得している事例】事例 5）法第 27 条第１項に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、個人情報を取得する場合。

[5] 本件個人データの提供が、法第 27 条第１項各号に該当しないことは明らかである。

[6] 平成 29 年５月 30 日～令和４年３月 31 日までは、平成 27 年改正法第 26 条第１項。令和４年４月１日以降は、令和３年改正法第 30 条第１項。

[7] 平成 29 年５月 30 日～令和４年３月 31 日までは、平成 28 年 10 月５日に公布された規則第 15 条第２項。令和４年４月１日以降は、令和３年個人情報保護委員会規則第４号により改正された規則第 22 条第２項。

２号に掲げる事項の確認を行う方法は、個人データを提供する第三者から当該第三者による当該個人データの取得の経緯を示す契約書その他の書面の提示を受ける方法その他の適切な方法とする。」と規定されている。

また、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）3-1-2 において、「『取得の経緯』の具体的な内容は、個人データの内容、第三者提供の態様などにより異なり得るが、基本的には、取得先の別（顧客としての本人、従業員としての本人、他の個人情報取扱事業者、家族・友人等の私人、いわゆる公開情報等）、取得行為の態様（本人から直接取得したか、有償で取得したか、いわゆる公開情報から取得したか、紹介により取得したか、私人として取得したものか等）などを確認しなければならない。」と規定されている。

本件において、中央ビジネスは、Ｘから個人データを取得するに際し、初回購入時に、口頭で「盗品ではない」という旨を確認したにとどまり、それ以上にＸが個人データを取得した経緯（取得先の別、取得行為の態様等）を確認していなかったのであるから、「当該第三者による当該個人データの取得の経緯」を確認したとはいえず、法第 30 条第１項第２号の規定に違反する。

⑶　報告等の求め（法第 146 条第１項）に対する虚偽報告（法第 182 条第１号、法第 184 条第１項第２号）

ア　当委員会は、令和５年２月から同年３月にかけて、「オプトアウト届出事業者に対する実態調査」を実施し、同調査に未回答、回答不十分であった等の理由から別途調査が必要であると判断した 24 事業者に対し、同年７月、法第 146 条第１項の規定により報告等の求めを実施した。

イ　中央ビジネスは、前記報告等の求めを実施した事業者の一つである（当委員会は、令和５年７月 27 日、中央ビジネスに対し、法第 146 条第１項の規定により報告等の求めを実施した）。

ウ　これについて、中央ビジネスは、令和５年８月３日、当委員会に対し、「令和４年４月１日～令和５年６月 30 日の期間、第三者から個人データの提供を受けた件数について、回答欄に記載すること。※提供を受けたデータの数や提供を受けたデータに含まれる個人情報の数ではなく、提供行為を受けた件数を記載すること。なお、上記期間に個人データの提供を受けた実績が無い場合は、回答欄に０と記載すること。」という設問に対する回答欄に、「０」と記載して報告した。

エ　中央ビジネスは、明確に判明しているものとして、少なくとも令和５年１月 17 日には、Ｘから個人データを取得していたのであるから、前記ウの回答は、明らかに虚偽の報告である。したがって、同報告を行った中央ビジネスの取締役の行為は法第 182 条第１号に該当し、また、中央ビジネスは両罰規定である法第 184 条第１項第２号に該当する。

2　ネクストステージ

⑴　不適正取得（平成 27 年改正法第 17 条第１項違反）

ア　前記１⑴アのとおり、第三者が個人データの提供について本人の同意を得ておらず、当該第三者による個人データの提供が平成 27 年改正法第 23 条第１項の規定に違反することを知り、又は容易に知ることができるにもかかわらず、当該第三者から当該提供を受けて個人情報を取得することは、平成 27 年改正法第 17 条第１項違反となる。

イ　本件において、ネクストステージは、Ｘから個人データを取得するにあたり、Ｘの職業や個人データの取得の経緯、第三者提供についての本人同意の有無等を一切確認しておらず、「Ｘがネクストステージに提供する個人情報は、不正に取得したものではないこと、また、個人情報保護法に従い適正に入手したものである。」旨の定型文を、Ｘにメールで送信させるのみで、漫然と１回当たり少なくとも数万件という大量の個人データを取得していた。

また、ネクストステージは、中央ビジネスと同様に、個人データの売買をその主たる業務としているところ、第三者に個人データを売却する際には、平成 27 年改正法第 23 条第１項の規定により第三者提供についての本人同意を得ることはせず、オプトアウト規定により個人データの提供を行うオプトアウト届出事業者であり、多人数の本人全員から第三者提供についての同意を得ることが極めて困難であることは、当事者として十分に認識していたはずである。

したがって、本件においても、ネクストステージは、Ｘから大量の個人データを取得するに当たり、Ｘが第三者提供についての本人同意を得ることなく個人データの提供をしようとしていることは当然に想定できるものであり、中央ビジネスは、Ｘに本人同意の証跡の提出を求める等の方法によって、Ｘが本人同意を得ていないことを容易に知ることができたといえる。

なお、個人データの提供についての本人の同意を得ていなくとも、Ｘがオプトアウト届出事業者として個人データの第三者提供を行っていた場合は、平成 27 年改正法第 23 条第１項違反には該当しないが、Ｘがオプトアウト届出事業者事業者ではないことは、当委員会のウェブサイトにより容易に確認することができ、ネクストステージにおいても、Ｘがオプトアウト届出事業者であるとは認識していなかった。

したがって、ネクストステージは、平成 27 年改正法第 23 条第１項に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、Ｘから個人情報を取得していたといえ、かかる取得行為は平成 27 年改正法第 17 条第１項の規定に違反する。

⑵　第三者提供の制限（法第 27 条第１項）違反

法第 27 条第１項は、個人情報取扱事業者は、同項各号に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならないと規定す

るところ、その例外として、同条第２項本文では、オプトアウト届出事業者による、本人の同意を得ない個人データの第三者提供について規定している。

しかしながら、同項ただし書では、「第三者に提供される個人データが・・・法第 20 条第１項の規定に違反して取得されたもの・・・である場合は、この限りでない。」と規定され、オプトアウト届出事業者による第三者提供であっても、法第 20 条第１項の規定に違反して取得された個人データについては、本人同意を得ずに第三者提供することはできない。

本件において、ネクストステージは、オプトアウト届出事業者であるところ、前記⑴のとおり、法第 27 条第２項ただし書の規定が施行された令和４年４月１日以降、法第 20 条第１項の規定に違反してＸから取得した個人データを、本人の同意なく第三者に提供している。したがって、当該提供行為は、法第 27 条第２項本文に該当しない第三者提供であるから、このように本人の同意のない提供行為は、法第 27 条第１項の規定に違反する。

⑶　第三者提供を受ける際の確認義務（平成 27 年改正法第 26 条第１項第２号）違反

ア　前記１⑵のとおり、個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、当該第三者による当該個人データの取得の経緯を確認しなれければならない（平成 27 年改正法第 26 条第１項第２号)。

イ　本件において、ネクストステージは、Ｘから個人データを購入するに際し、Ｘに「提供する個人情報は、不正に取得したものではない。」「個人情報保護法に従い適正に入手したものである。」旨の定型文をメールで送信させるにとどまり、当該個人データの取得の経緯を具体的に確認することはしていなかったのであるから、平成 27 年改正法第 26 条第１項第２号の規定に違反する。

以　上