当委員会からの勧告等に対する是正状況の概要

資料２－２

公表資料

□ 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。