株式会社NTTドコモ及び株式会社NTTネクシアにおける再発防止策の実施状況

資料１

公表資料

- 個人情報保護委員会（以下「当委員会」という。）は、株式会社NTTドコモ（以下「ドコモ社」という。）における顧客情報の流出事案に関して、ドコモ社及び同社の個人データの取扱いの委託先である株式会社NTTネクシア（以下「ネクシア社」という。）に対し、令和６年２月15日に指導を行い、同年３月15日までに再発防止策の実施状況について報告するよう求めていた。
- 今回、ドコモ社及びネクシア社から報告を受けた再発防止策の実施状況に関して、現時点において一定の取組が認められるものであった。
- 当委員会としては、今後も、再発防止策が確実に実施されることを、引き続き注視していく。

□ ドコモ社の再発防止策の実施状況

	指導事項	再発防止策の実施状況
１．物理的安全管理措置		
	ドコモ社では、情報管理規程で定めるところにより、顧客の個人データを取り扱う場合はインターネット及びメールの利用が制限された専用のPCを利用することとし、インターネット及びメールを利用するPCとは取扱区域を分けて管理するルールであった。 しかし、電話営業用の顧客情報管理（以下「本件業務」という。）のために業務上使用するPCは、個人データを取り扱うにもかかわらずインターネット及びメール利用の制限がなされておらず、当時の物理的安全管理措置（個人データを取り扱う区域の管理）は十分な状態とはいえなかった。	■個人データを取り扱う区域の管理 令和５年５月、外部インターネットから分離した個人データを取り扱う専用PCを配備し、専用PCは、パーティションで区切られた専用エリア内でのみ利用可能とした。さらに、同月、個人データの取扱いが業務上必要な作業者のみに専用PCへのアクセス権限を付与し、専用エリアへの入退室には生体認証を導入した。 ■専用PC及び専用エリアの利用に関する運用 令和５年５月以降、専用PCを用いて個人データを取り扱う作業を実施する場合、作業者は事前申請を行い、上司承認の元で作業を行うよう運用を変更した。また、月に１度、事前申請の内容と専用PCのアクセスログ及び専用エリアの入退室ログとの突合を行い、不正利用防止の対策を講じている。
２．技術的安全管理措置		
	ドコモ社では、個人データの漏えい等を防止するための措置として、本件業務も含めて、ネットワーク監視を行っており、ネクシア社の派遣社員であった者（以下「Ｘ」という。）がクラウドサービスへアップロードした操作についても発生当日に検知し、当日中にＸへの聴取と対象端末のネットワークからの切断を行っていたことからすれば、一定の処置を講じていたといえる。 しかし、本件業務に関するネットワーク環境についてみると、外部インターネットへのアクセス規制については、一部のサイトを接続不可と定めるブラックリスト方式で運用されており、ファイル共有サービス等のクラウドサービスも含めて、業務上不必要なサイトには接続できない設定とはしていなかったものであり、大量の顧客個人データを取り扱っているシステムであるにもかかわらず、漏えい等の防止の措置が十分ではなかった。	■インターネットアクセスの制御見直し 令和５年４月、外部インターネットへのアクセス制御をブラックリスト方式からホワイトリスト方式に変更し、外部ストレージ等の業務上不必要な通信を制限するよう見直した。ホワイトリスト方式のアクセス制御について、新たに業務上やむを得ず外部インターネットへのアクセスが必要となった場合のみ、管理者による承認の元でホワイトリストへの追加を行い、アクセス制御の状況について管理簿にて適切な管理が行えているか確認している。 ■顧客情報の暗号化 令和５年９月、ファイルシステム及びデータベースに保存していた個人データの暗号化対策を完了した。 ■データの外部送信手段の制限 令和５年５月、個人データを取り扱う専用PCが外部インターネットから分離されたため、専用PCからデータを送信することが不可能となったことに伴い、業務上必要な個人データの受渡しを行う場合は、管理者立会いの元、専用HDD等の環境のみとするよう、手段を制限して行っている。

□ ドコモ社の再発防止策の実施状況（続き）

	指導事項	再発防止策の実施状況
３．組織的安全管理措置		
	ドコモ社は、物理的安全管理措置及び技術的安全管理措置が一部不十分な状況に対して、追加的運用ルールを規定し運用していたところ、本件業務における同運用確保のための取組では、日次で行わせる自主点検の結果を月次で確認することで、確実に徹底されていることを確認することとしていた。 しかし、上記取組では、自主点検において虚偽の申告が含まれないことを前提としているため、意図的に追加的運用ルールに反したＸの取扱いは是正できず、また、自主点検結果の月次の確認では、いつ行われるか予測できない私的なインターネット接続を即時で検知できないものである。したがって、ドコモ社においては、個人データの取扱いに係る規律に従った運用に問題があり、組織的安全管理措置の不備があったものと言わざるを得ない。	■ルールの周知徹底 令和５年４月、従業者及び委託先に対して、個人情報取扱いルールの再周知を実施し、同月、ネクシア社従業者に対して、個人情報の保護及び情報セキュリティに関する研修を実施した。さらに、同年５月、全ての従業者を対象として、個人情報の保護及び情報セキュリティに関するeラーニング研修を受講させ、理解度テストを実施した。 今後も、年に１度、全ての従業者に対する個人情報の保護及び情報セキュリティに関する研修を継続して実施する。 ■点検・監査 令和５年７月、社内の個人データの取扱いのある全部署及び全委託先に対して、アカウント管理、インターネット接続制限及びデータ暗号化等の本件漏えい事態の問題点について自己点検を行わせ、情報セキュリティ部による点検内容の確認及び必要な是正措置を行った。 ■組織体制の強化 令和５年11月より、専門的な情報・意見を収集し、検討する仕組みとして情報セキュリティマネジメント検討会を設置し、情報セキュリティへの不適合事項及びリスクへの対策について、主管部署一任とせず、役員を交えて不適合事項に対する対策の進捗や取組状況を確認する体制とした。
４．委託先の監督		
	ドコモ社は、物理的安全管理措置及び技術的安全管理措置が一部不十分な状況でありながら、ネクシア社に対し、大量の個人データの取扱いを委託しているにもかかわらず、自ら又は外部の主体による監査を実施することはなく、ネクシア社の自主点検に任せ、月次で結果報告を受け取るだけであった。その結果として、Ｘの不適切な行為を発見できず、本件漏えいのおそれの発生を未然に防ぐことができなかったものといえる。 また、Ｘの不適切な行為を自主点検により発見することができなかった理由として、ドコモ社は、Ｘが自主点検をすり抜けるという手口を使っていたことが要因である旨を回答している。 しかしながら、ドコモ社がネクシア社に行わせていた自主点検は、従業者にデータを削除したことを自己申告させ、他の従業者がデスクトップ上に不要なデータが残っていないかどうかを確認するという簡易な方法にとどまっており、本件のように意図的にデータ削除せず、自身しか把握していないデスクトップ以外の場所に保存した場合は、発見され得ないことは容易に想定可能であるから、点検項目や点検の方法が不十分であったといえる。したがって、その報告を月次で受領し確認するだけであったドコモ社の委託元としての監督は、不十分であったと言わざるを得ない。	■全てのPCの総点検 令和５年５～６月、個人データを取り扱う全てのPC（委託先に貸与したPCに限らず、従業者が利用するものも含む。）において、PC上に個人データが残存していないか総点検を実施した。 ■委託先への実地監査 令和５年６月、個人データを取り扱う業務を委託している委託先企業に対して、抜き打ちにて、個人データが残存していないか等の取扱状況を実地で監査した。 ■貸与PCのチェック機能の導入（予定） 令和６年８月、ドコモ社が委託先へ貸与するPCに対し、使用量及びファイル保存状況等を遠隔監視する機能を導入する予定である。

□ ネクシア社の再発防止策の実施状況

	指導事項	再発防止策の実施状況
１．組織的安全管理措置		
	ネクシア社では、自主点検は実施していたものの、他部署等による監査は実施しておらず、大量の個人データの取扱いがある本件業務において、Ｘが本件 PC 内に作業データを日常的に残しており、また、私的なインターネット接続を是正できなかったことを踏まえると、個人データの取扱状況の把握や安全管理措置の評価等が不十分であったと言わざるを得ず、組織的安全管理措置の不備が認められる。	■組織体制の整備 令和６年１月、コーポレートガバナンス体制の見直しとして、リスクマネジメント室を新設し、内部監査室を社長直結組織に変更した。リスクマネジメント室は事業部門に対してモニタリングを行い、個人情報の取扱いやセキュリティ対策状況をチェックし、必要に応じてアドバイスを行い、内部監査室は独立した立場から業務運営やリスク管理の適切性及び実効性を検証・評価する。 ■グループ会社での監査 親会社である東日本電信電話株式会社と連携し、ネクシア社の受託業務における個人情報の保護及びセキュリティ対策に対する現場調査を実施した。 ■内部監査の強化 令和５年11月より、年に１回実施する内部監査において、私的なインターネット接続、USBメモリの使用禁止、外部ストレージへの不正持ち出し防止対策等の遵守状況に関する監査項目を追加し、内部監査を実施している。
２．人的安全管理措置		
	ネクシア社では、派遣社員であるＸを含む従業者に、情報セキュリティ遵守のため機密保持に関する誓約書を提出させ、また、情報セキュリティ研修の実施を行っていたものの、情報セキュリティ研修では、一般的な情報セキュリティの考え方及び法の令和２年改正部分を紹介するにとどまっており、大量の顧客データを管理する事業者における研修としては十分とはいえず、結果としてＸによる本件漏えいのおそれの発生を防止するに至らなかった。 したがって、ネクシア社における従業者の教育は、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ず、人的安全管理措置の不備が認められる。	■経営トップからのメッセージ発信 令和５年７月及び同年11月、個人情報の保護及び個人データの適切な取扱いの重要性等に関して、ネクシア社社長から全従業者に対し、メッセージを発信した。 ■教育研修の充実 令和５年８月、全従業者を対象に、本件事案における教訓を中心として緊急情報セキュリティ研修を実施した。 令和６年３月に実施した研修においても、情報セキュリティの研修教材に加え、不正持ち出し事例を追加し、カリキュラムを充実させるとともに、研修後の理解度テストを実施した。 ■コンプライアンスチェックの徹底 令和６年２月以降、従業者に対して、個人情報の保護の重要性を認識させることを目的とし、新規採用者にコンプライアンス遵守に関する確認書の提出を求め、一定数以上の顧客情報を取り扱う従業者には、年に１回、同確認書の提出を求め、必要に応じて面談を実施している。
３．その他		
	上記当委員会からの指導事項に対するものではないが、対応策の実効性を担保する観点から、ネクシア社において右記の改善策が実施されている。	■情報システムの使用に伴う漏えい等の防止 本件事案発覚後、速やかに、全受託業務を対象にシステム及びネットワークに関する実態調査を実施した。調査後、本件事案と同様の事象が発生するリスクのあるシステムに対し、業務に関係のないインターネット接続制限（UTMの設置等）を行い、私的なインターネット接続が行えない環境を構築済みである。