公表資料

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

News Release

株式会社 NTT ドコモ及び株式会社 NTT ネクシア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２月 15 日

個人情報保護委員会は、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）に基づき、株式会社 NTT ドコモ及び株式会社 NTT ネクシアに対し、令和６年２月 15 日に個人情報保護法第 147 条に基づく指導等を行いましたので、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 ドコモ及び株式会社 NTT ネクシア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２月 15 日
個人情報保護委員会

個人情報保護委員会（以下「当委員会」という。）は、令和６年２月 15 日、株式会社 NTT ドコモ（以下「ドコモ社」という。）及び株式会社 NTT ネクシア（以下「ネクシア社」という。）における個人情報等の取扱いについて、両社に対し、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 147 条に基づく指導等を行った。

１．事案の概要

ドコモ社は、自社インターネットサービス等に関する事業について、サービス・商品の提案等を行うため、個人データを取り扱っている。

ドコモ社は、これらの事業に関し、ネクシア社に対し、電話営業用の顧客情報管理（以下「本件業務」という。）を含む業務を委託していたところ、ネクシア社の派遣社員であった者（以下「X」という。）が、令和５年３月 30 日、顧客情報管理のために業務上使用する PC（以下「本件 PC」という。）から、個人契約するクラウドサービスに無断でアクセスし、合計約 596 万人分の個人データ[1]（以下「本件個人データ」という。）を同クラウドサービスへアップロードすることにより、外部に流出させ、漏えいのおそれ[2]が発生した。

２．事案発生に至った原因

(1) 基準不適合事項

本件業務は、令和４年７月、ドコモ社が株式会社 NTT ぷらら（以下「ぷらら社」という。）を吸収合併したことにより、ドコモ社が事業を承継したものであるところ、本件業務に関するネットワーク等の執務環境（本件 PC を含む。）については、以下の①及び②のような、ドコモ社が定めた情報管理規程に一部適合しない事項（以下「基準不適合事項」という。）が存在した。

① 顧客情報を取り扱う場合は専用の PC を利用し、顧客情報を取り扱う PC においてはインターネット及びメールの利用が制限される必要があるが、これらの制限が実施されていなかった。

② 顧客情報（ファイルシステム及びデータベース）の暗号化が必要であるところ、これが行われていなかった。

---

[1] インターネット接続サービスの営業対象者に関する氏名・住所・電話番号・回線 ID 等の約 165 万人分、映像配信サービスの営業対象者に関する氏名・住所・電話番号・メールアドレス・生年月日・回線 ID 等の約 431 万人分。

[2] ドコモ社が行ったXに対する聞き取りによると、Xは、自ら作成したツールのソースコードをノウハウとして持ち出したかったものであり、当該個人データについて外部の第三者への提供は行っていないと説明している。

(2) 追加的運用ルール

ドコモ社は、この基準不適合事項について、速やかに技術的な対応を行うことが困難であると判断した。そこで、ドコモ社は、本件業務を行う際は、以下に例示したような、ぷらら社における運用ルール（以下「追加的運用ルール」という。）に従うことを条件とし、令和４年 12 月までの時限的例外措置として、基準不適合事項を許容することとした。

- PC で実施した作業データは、当日中に全て削除すること
- 業務上不要な私的インターネット接続の禁止
- 社外へのデータ送信時の手動暗号化徹底
- 追加的運用ルールの遵守状況について定期的に自主点検を行うこと

さらに、ドコモ社は、その後、基準不適合事項への技術的な対応に時間を要すること等が判明したことから、追加的運用ルール遵守を条件に基準不適合事項を許容する期限を令和５年５月まで延長した。

(3) 本件漏えいのおそれの発生に至ったＸの取扱い

Ｘは、本件業務にてデータ管理ツールを開発するにあたり、個人データが含まれた同ツールを本件 PC 内の自身しか把握していない保存場所[3]にコピー保存の上で開発作業を実施していたところ、当日作業の終了時に至っても、本件 PC 上の同ツールを削除していなかった。さらに、Ｘは、業務上の必要性がないにもかかわらず、クラウドサービスに個人アカウントでログイン[4]し、本件個人データをアップロードした。

(4) 小括

このように、ドコモ社及びネクシア社においては、大量の顧客の個人データを取り扱っていたにもかかわらず、ドコモ社がぷらら社を吸収合併した後、半年以上も、基準不適合事項のリスクが存在する状況下で、追加的運用ルールが徹底されず、本件漏えいのおそれが発生した。

３．法律上の問題点

(1) ドコモ社

法第 23 条は、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データ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。」と規定しており、法第 25 条は、「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。」と規定している。

しかしながら、ドコモ社では、個人情報等の取扱いについて、以下の問題点が認められた。

---

[3] ドコモ社によるとＸはデータ管理ツールの保存場所をドコモ社及びネクシア社の誰にも伝えていなかったとされる。

[4] ドコモ社によるとＸはクラウドサービスへのアクセスの際に Web ブラウザのプライベートモード（インターネットの閲覧履歴を自動で削除し、端末上に記録しない特殊な方法）を用いていたとされる。

ア　物理的安全管理措置（個人データを取り扱う区域の管理）

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、本件 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。

イ　技術的安全管理措置（情報システムの使用に伴う漏えい等の防止）

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、Ｘ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。

ウ　組織的安全管理措置（個人データの取扱いに係る規律に従った運用）の不備

ドコモ社は、前記ア及びイの物理的安全管理措置及び技術的安全管理措置に関する問題点について、前記２．(2)のとおり、組織的安全管理措置の徹底により総合的なリスクを低減させる方針を決定したものであるから、この決定に従った運用が実際に徹底されることが重要である。

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。

エ　委託先の監督の不備（委託先における個人データの取扱状況の把握）

ドコモ社は、ネクシア社に対し、本件業務に関して、追加的運用ルールを遵守するよう周知していた。また、ネクシア社は、日次で、本人及び第三者にて業務終了時作業データの削除確認等を行い、その結果を管理簿に記録するという自主点検を実施し、この結果について、月次でドコモ社へ提出していた。

しかしながら、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。

(2) ネクシア社

法第 23 条は、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データ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。」と規定している。しかしながら、ネクシア社では、個人情報等の取扱いについて、以下の問題点が認められた。

ア　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）

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。

イ　人的安全管理措置（従業者の教育）

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。

４．指導等の内容

(1) ドコモ社

・　法第 23 条、法第 25 条及び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）に基づき、必要かつ適切な措置を講ずること。

・　既に策定した再発防止策を確実に実施するとともに、爾後、適切に運用し、継続的に個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。
・　法第 146 条第１項に基づき、再発防止策の実施状況について、関係資料を提出の上、令和６年３月 15 日までに報告するよう求める。

(2) ネクシア社

・　法第 23 条及び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）に基づき、必要かつ適切な措置を講ずること。
・　既に策定した再発防止策を確実に実施するとともに、爾後、適切に運用し、継続的に個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。
・　法第 146 条第１項に基づき、再発防止策の実施状況について、関係資料を提出の上、令和６年３月 15 日までに報告するよう求める。

以　上