資料14－4

NTT西日本

第14回 利用者情報に関するワーキンググループ

NTT西日本における業務委託契約時のお客様情報の取り扱い等について

西日本電信電話株式会社

2024年11月12日

はじめに

- 当社子会社である株式会社NTTマーケティングアクトProCX（以下、ProCX）およびNTTビジネスソリューションズ株式会社（以下、BS）からのお客さま情報漏えいについて、NTT西日本グループに関係する全ての皆さまに多大なご迷惑とご心配をおかけしましたことを、改めて深くお詫び申し上げます。

- 当該事案は、当社（NTT西日本）からProCXへアウトバウンドテレマーケティング業務を委託し、ProCXはその業務において、BSが提供するコールセンタシステムを利用する中で発生させてしまったものです。
契約形態は、正しくは当社とProCX間は業務委託、ProCXとBS間はサービス利用契約＋個人データ取扱い委託ですが、従来から、業務委託の場合は個人データの取扱い委託に該当する認識があった一方で、業務委託ではない外部サービスを利用する場合には、個人データの取扱い委託には該当しないと誤認していました。

- そのため、外部サービス利用に伴うProCXからBSへの個人データの取扱い委託について、ProCXから当社へ報告するよう求めておらず、個人データをBSにおいて取扱っている事実を把握できておりませんでした。

- この点を踏まえ、外部サービス利用時においても、個人データの取扱い委託となる場合には安全管理措置を講じる必要がある旨を契約書に明記する等、法に則ったルールにあらためるとともに、委託先事業者の皆様には、改正後のルールを反映した契約に変更いただき、適宜必要な措置を講じていただくよう対応を進めているところです。

- NTT西日本グループとして、今後同様の事案を再び発生させることがないよう、大切なお客さまの情報を取り扱う会社としての自覚を新たに、委託先管理の取組みを一過性のものではなく継続的に実施していくことを通じて、セキュリティファーストカンパニーとなることをめざします。

委託先に対する監督（全体像）

- 委託契約締結前、委託契約締結時、委託契約締結後において、それぞれ個人データの取扱い委託先に対する監督を実施することとしています。

- 今回の漏洩事案を踏まえ、業務の委託にはあたらない外部サービス利用時においても、個人データ取扱い委託となる場合があり、その場合には安全管理措置を講じる必要がある旨を契約書に明記する等、法に則ったルールにあらためました。

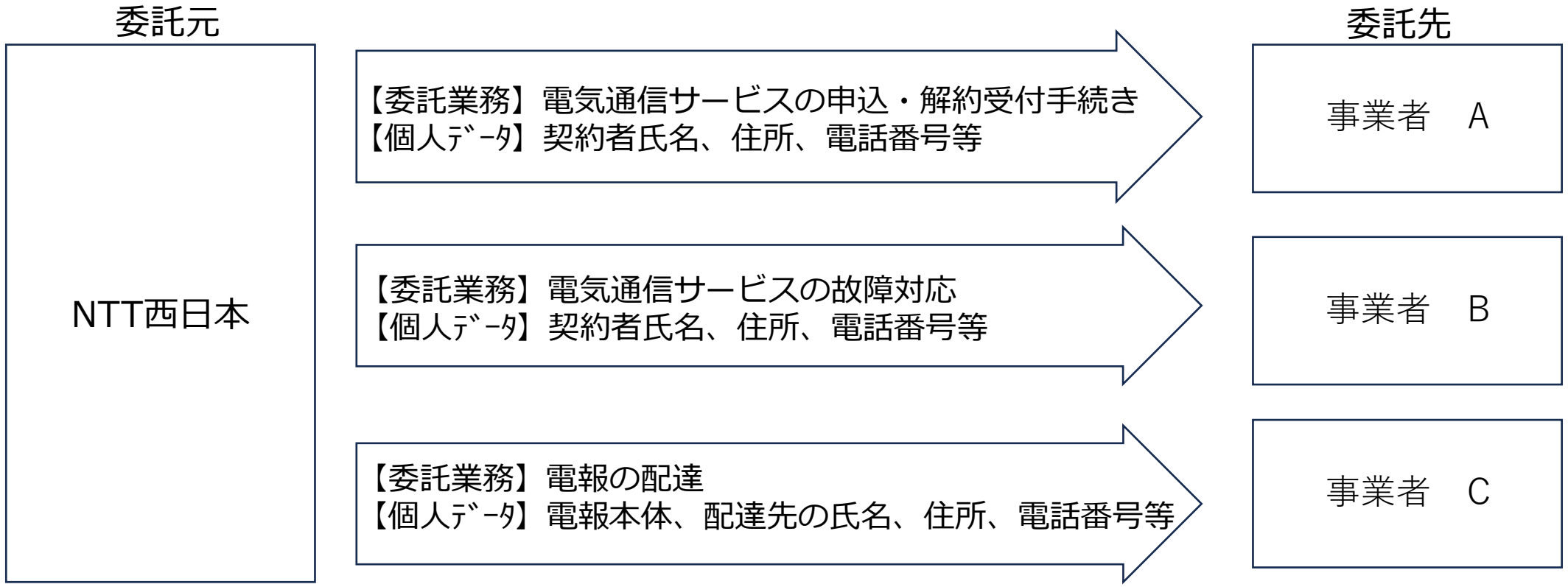
時期	委託契約締結前	委託契約締結時	委託契約締結後
実施事項	委託先の選定	契約書の締結	個人データの取扱いの委託先における個人データの取扱状況の把握
個人データの取り扱い委託先に対する当社監督事項	委託先が当社が要求する安全管理阻止を履行できる委託先かどうか、委託契約締結前にチェック	当社が要求する安全管理措置実施を義務付ける契約書を締結	当社が要求する安全管理措置を実行できているか、契約締結後にチェック

代表的な委託業務

Q1-1:個人データの取扱いの委託（再委託）について、どのような情報を、どのような事業者に委託しているのか、代表的なものを可能な範囲で記載すること。

- 代表的な個人データの取扱いの委託業務、取扱う個人データは以下の通りです

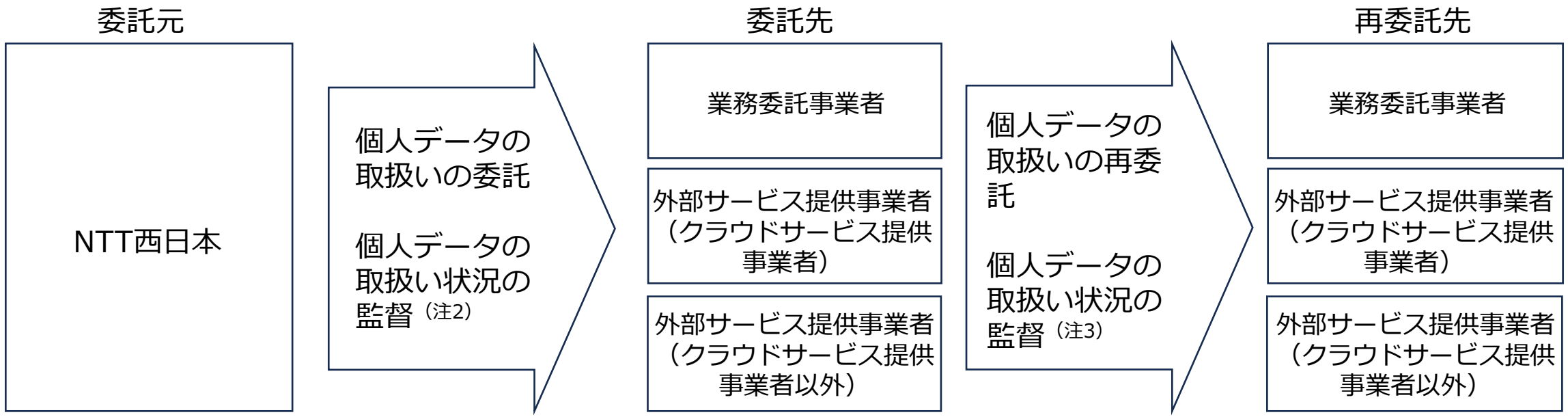
（個人データの取り扱い委託例）



委託先との間の契約形態・外部サービス利用に対する認識

Q1-2：個人データの委託（再委託）について、委託先との間の契約形態にはどのような種別があるか
Q2-1：個人データを取り扱う情報システムに外部サービスを活用する場合において、当該外部サービスの提供者が当該個人データを取り扱う場合、個人情報保護法上の委託に該当するものとして扱っているか、等

- 委託先との契約形態については、業務委託、外部サービス利用（クラウドサービス、クラウドサービス以外）の種別があります。
- 当社は、個人データ取り扱いの委託先（再委託先）のうち、業務委託先に対しては、従来より個人データの取扱い状況を監督しておりましたが、**外部サービス提供事業者（注1）に対しての対応は不十分でした。今回の漏洩事案を受け、外部サービス提供事業者への個人データの取扱い状況の監督を強化しています**。



（注１）個人情報を取り扱っていないと想定されるクラウドサービス提供事業者は委託先管理対象とはしておりません。（「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ　Q7-53、7-54参照）
（注２）安全管理措置等、契約上どのように担保されているかは6頁に記載
（注３）委託先が再委託先の履行状況を調査・確認するほか、当社がその調査内容を確認しています。

委託先の選定

Q2-5：個人データの取扱いを委託する場合において、委託先（再委託先を含む）の選定にあたり、個人データを適切に取り扱うための安全管理措置が講じられているかについて確認を行っているか。確認を行っている場合、具体的にどのような項目を、どのような方法で確認しているか、等

- 契約締結前に、当社が要求する安全管理措置を履行できる委託先かどうかについて、以下の通りチェックすることとしています。

チェック概要	具体的チェック方法
契約締結前に、委託先が当社が要求する安全管理措置を履行できる委託先かどうかチェック	・契約締結前に、委託先事業者における個人データの取扱いにかかる、**情報管理体制、研修、事業所環境、アクセス権管理、外部脅威対策、越境移転確認、事故対応等**の項目を遵守しているか、チェックシートを用いて確認を行うこととしています。 ・**研修に関する確認**については、お客様情報管理に関する研修を少なくとも年１回実施を求めることとしています。 そのうえで、下記について確認を行っています。 ・個人情報保護規則等にて情報管理研修の実施に関する規定を盛り込んでいること ・研修実施計画書・カリキュラム・受講者名簿等・研修の実績を提示できるようにしていること ・研修内容は情報管理についての基本事項を盛り込んだ適切な内容であるようにしていること

契約書の締結（１）

Q2-7-1：個人データの取扱いに係る委託契約（再委託契約を含む）において、安全管理措置の実施、秘密保持、再委託の条件、再委託先の監督等に関する事項を定めているか。

- 個人データの取扱いに係る委託契約書において、安全管理措置の実施、秘密保持、再委託の条件、再委託先の監督等に関する事項を以下の通り定めています。

覚書記載項目	覚書記載項目（詳細）
安全管理措置	お客様情報保護のために必要な組織的・人的・物理的・技術的・外的環境把握に係る安全管理措置の遵守
秘密保持	業務遂行にあたり委託先が知り得た情報の守秘義務の遵守
再委託の条件	当社の書面による事前同意が必要
再委託先の監督	委託先が再委託先の履行状況を調査・確認し、その調査結果を当社が報告を受け把握する

契約書の締結（２）

Q2-7-2：自社の個人データの取扱いを委託している場合において、2-7-1のとおり委託契約（再委託契約を含む）に定めた事項について、契約書締結以外の方法により実運用上行っている措置はあるか。
Q2-8　：個人データの取扱いの委託先が再委託を行う場合、委託先に対してどのような対応を行っているか（再委託を承諾する基準等の再委託条件、委託先による再委託先の管理監督の実施状況の把握方法等）。

- 自社の個人データの取扱いを委託している場合において、委託契約（再委託契約を含む）に定めた事項について、契約書締結以外の方法により実運用上行っている措置として、以下の措置を実施しています。

項目	実運用上行っている措置
契約書締結以外の方法により実運用上行っている措置	委託先事業者における個人データの取扱いにかかる、情報管理体制、研修、事業所環境、アクセス権管理、外部脅威対策、越境移転確認、事故対応等の項目を遵守しているか、ヒアリング等により確認を行うこととしています。

- 個人データの取扱いの委託先が再委託を行う場合の、委託先に対する対応は、以下の通りです。

項目	実運用上行っている措置
再委託を承諾する基準等の再委託条件	当社の事前の書面による同意を必要としている・当社が委託先と締結する覚書と同等の内容の覚書を委託先と再委託先で締結することを義務付けている
委託先による再委託先の管理監督の実施状況の把握方法	当社は、委託先及び再委託先に対して、定期的に個人データ管理の履行状況の報告を求めることができ、また、事務所等に立入り、直接調査・報告を求めることができるとしている

個人データの取扱いの委託先における個人データの取扱状況の把握

Q2-9　：個人データの取扱いの委託先（再委託先を含む）における個人データの取扱状況について、どのように把握し、監督を行っているか。
Q2-10：個人データの取扱いの委託先（再委託先を含む）における個人データの取扱いの監査・点検の内容、方法及び頻度

- 個人データの取扱いの委託先（再委託先を含む）における個人データの取扱状況については、以下の通り把握、監督を行っています。

把握項目	把握方法
当社による委託先の個人データの取扱状況の把握・監督方法	・定期的に個人データ管理の各種対応の履行状況の確認をしており、事務所等に立入点検を実施している （点検項目は委託先選定時のチェック項目と同様）
委託先による再委託先の監督	・委託先が再委託先の履行状況を調査・確認
当社による再委託先の監督	・再委託にあたり、当社の事前の書面による同意を必要としている ・当社が委託先と締結する覚書と同等の内容の覚書を委託先と再委託先で締結することを義務付けている ・定期的に個人データ管理の各種対応の履行状況の報告を求めることができ、また、事務所等に立入り、直接調査・報告を求めることができるとしている

- 個人データの取扱いの委託先（再委託先を含む）における個人データの取扱いの監査・点検の内容、方法及び頻度
  - ・委託先による個人データ管理の各種対応の履行状況に関する報告書により確認を行っており、加えて、少なくとも年１回事務所等への立ち入り点検を実施しました。
  - ・委託先による再委託先の個人データ管理の各種対応の履行状況を、少なくとも年1回調査・確認しています。

委託先への物理的・技術的安全管理措置

Q3-1、3-2：委託先（再委託先を含む。）において、外部からの不正アクセスによる個人データの漏えい、及び内部からの不正な持ち出しによる個人データの漏えいを防ぐため、どのような安全管理措置を講じているか。

- 外部からの不正アクセス、および内部からの不正な持ち出しによる個人データの漏えいを防ぐため、委託先と個人データの取扱いの委託に関する契約書を締結し、外部からの不正アクセスを防止するための安全管理措置の遵守を義務づけるとともに、立ち入り点検により順守状況の把握・確認を行うこととしています。
- 今回の漏洩事案を踏まえ、既存の全ての委託先に対しても、変更した契約書の締結及び追加の安全管理措置の実施を進めております。
- 業務委託先に当社システムをご使用頂く場合、当社にて当該システムの安全管理措置を施したうえで、業務委託先にご使用頂いています。

目的	項目	遵守内容
外部からの不正アクセス防止	個人データにアクセスする場合の従業員の認証等	従業員の認証を実施すること
内部からの不正持ち出しの防止	許可されていない外部ストレージへのアクセスが可能となっていないか	許可されていない外部ストレージへのアクセスが可能とならない措置を実施すること
	保守作業端末にダウンロードが可能になっていないか	保守作業端末から情報が取り出せないような措置を実施すること
	保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていないか	保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能にならない措置を実施すること
	セキュリティリスクが大きいと想定される振る舞いを即時に検知できているか	即時振る舞い検知が可能となるような措置等を実施すること
	各種ログ等の定期的なチェックは十分か	定期的なログチェックを実施すること

委託に関する利用者へのご説明、漏洩発生後の対応

Q3-3：個人データの取扱いを外部へ委託することについて、利用者に対してどのような説明を行っているか。
Q3-4：漏えいの発生後の対応として、漏えいした情報がインターネット上に流通していないかを検知したり、作業者の記録を保存し漏えいの発生原因を特定したりすることができるよう、措置を行っているか。

- 個人データの取扱いを外部へ委託することに対する利用者へのご説明については、当社プライバシーポリシーにおいて、「個人情報（以下略）等の取扱いを外部に委託する場合には、守秘義務契約の締結等により委託先においても適正に取り扱われるよう管理、監督します。」と記載し、公式HP上で公開しています。
- 漏えいの発生後の対応として、インターネット上に情報が漏洩していないかのモニタリング実施、ログ等による漏えいの発生原因を調査するフォレンジックを行っています。

当社プライバシーポリシー抜粋
（https://www.ntt-west.co.jp/share/privacy.html#privacy01）

西日本電信電話株式会社（以下「NTT西日本」といいます。）は、個人情報、特定利用者情報及び特定個人情報等の保護に対する社会的要請を十分に認識し、個人情報、特定利用者情報及び特定個人情報等の適正な取扱いを推進していくことが、公共性を有する電気通信事業者としての重大な社会的責務と考えております。
NTT西日本は、このような責務を十分果たしていくとともに、安心・安全なサービスを提供し、皆様に信頼される企業であり続けるため、「NTTグループ情報セキュリティポリシー」及び以下の基本的な方針に従い、全社を挙げて個人情報、特定利用者情報及び特定個人情報等の保護に努めてまいります。

(1) NTT西日本は、個人情報、特定利用者情報及び特定個人情報等の保護に関連する法令等※1の規定に従って個人情報、特定利用者情報及び特定個人情報等の適正な取扱いを行っていくなど、コンプライアンス（法令遵守）の徹底に努めてまいります。
(2) NTT西日本は、個人情報、特定利用者情報及び特定個人情報等の利用目的を明確に定めるとともに、その利用目的の達成に必要な範囲内で適正に個人情報、特定利用者情報及び特定個人情報等を取扱います。 また、個人情報、特定利用者情報及び特定個人情報等を正確かつ最新の内容に保つよう努めます。
(3) NTT西日本は、個人情報、特定利用者情報及び特定個人情報等の適正な管理のため、個人情報及び特定個人情報等保護を推進する委員会、及び特定利用者情報統括管理者を置くとともに各組織に個人情報、特定利用者情報及び特定個人情報等の保護に関する責任者並びに事務取扱担当者を配置する等の責任体制を整備します。
(4) NTT西日本は、個人情報、特定利用者情報及び特定個人情報等を取り扱う業務に従事する者に対して必要な教育研修等を実施するとともに適切な監督を行います。
また、個人情報、特定利用者情報及び特定個人情報等の取扱いを外部に委託する場合には、守秘義務契約の締結等により委託先においても適正に取り扱われるよう管理、監督します。
(5) NTT西日本は、個人情報、特定利用者情報及び特定個人情報等の安全性の確保のため、各種の基準・ガイドライン等を参照しつつ、必要な安全管理措置を講じます。