データマッピング・ツールキット
（個人情報保護法関係）

2022 年 10 月

個人情報保護委員会事務局

データマッピング・ツールキットの構成

IT 技術の進展に伴い個人情報等の取扱いが増加している中で、事業者が取得する個人情報を適切に管理していく必要性が高まっています。こうした中で、事業者の自主的な取組みの一つとして、データマッピングによる管理手法が注目されています。

データマッピング・ツールキット（以下「本ツールキット」といいます。）は、多数のデータを保有している等の事業者が、当該データを適切に管理するための自主的な取組みとして、データマッピングを開始する際の一助となることを目的とするものです。

導入初期は本ツールキットを参考にしながら、更新の都度、項目等の見直しを行い、事業者にあった方法を構築することが期待されます。また、最初から本ツールキットのデータマッピングをすべて行うことを目指すのではなく、基本的な項目だけを選別してデータマッピングする等のスモールスタートを目指すことも考えられます。

本ツールキットは、以下の構成になっています。

章立	項目	備考
第１章	データマッピングの意義等	● データマッピングの意義や手順（準備、表作成、確認・対応、更新）等が記載されています。
第２章	データマッピング表の項目等	● データマッピング表の項目例が記載されています。 ● 記載例は別紙１です。
第３章	データマッピング表の確認・対応	● 第１章に記載されたデータマッピングの手順である「確認・対応」を詳細に説明しています。 ● データマッピング表の確認の際に利用できるチェックリストが別紙２及び別紙３です。

第１章　データマッピングの意義等

1. データマッピングとは

データマッピングとは、事業者が取り扱うデータを事業者全体で整理して、取扱状況等を可視化する作業のことを言います。具体的には、別紙１のようなデータマッピング表を作成する等して可視化します。

2. データマッピングの意義

データマッピングによって、事業者全体としてどのようなデータを取り扱っているのかを把握し、

① 個人情報保護法（以下「法」といいます。）を含む当該データに適用される法令の遵守状況の確認

② 当該データの取扱状況等に起因するリスクに応じた必要な対応の実施

等を行うことができます。

なお、個人データについてデータマッピングする場合には、法第 23 条の定める個人データの安全管理措置の一つの手法となります（ガイドライン（通則編）10－３(3)）[1]。具体的には、データマッピングは、個人データの項目、責任者・取扱部署等をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とするものであり、安全管理措置の一つである、組織的安全管理措置の「個人データの取扱状況を確認する手段の整備」の一つの手法です[2]。

3. データマッピング手順

データマッピングの手順としては、以下のような手順が考えられます。

＜手順の概要＞

準備

- データマッピングの責任者・担当部署（事務局）の決定
- データマッピングの目的の設定
- データマッピングする項目及び対象とするデータの範囲の設定
- データマッピング表のフォーマットの作成
- データマッピング表の記入者の決定

---

[1] https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

[2] その他にも、安全管理措置の内容を決定する際の参考資料や、本人からデータについて問い合わせを受けた時の回答の参考資料となります（法第 32 条、法第 28 条３項も参照）。また、いわゆる個人情報管理台帳を作成している事業者においては、これとは別にデータマッピング表を作成するのではなく、本ツールキットも参考に個人情報管理台帳の改善を行うことが考えられます。

- 記入者によるデータマッピング表の記入
- データマッピング担当部署による記入の正確性の確認

- データマッピングの目的に沿ったデータマッピング表の確認・必要な対応（是正）

- データマッピング表の随時又は定期的な更新

(1)データマッピングの準備

ア　データマッピング責任者・担当部署（事務局）の決定

データマッピングの責任者・担当部署（事務局）を決定し、当該責任者・担当部署（事務局）がデータマッピングを取りまとめることにより、事業者内で統一的な考え方の下、データマッピングを行うことができます（担当部署としては、総務部門、法務部門、データ保護部門等が考えられます。）。

また、データマッピングのためには各部門の協力が不可欠です。そのため、データマッピング責任者は、各部門に対して実効的な協力要請ができる権限を有する者（役員等）であることが望ましいです。

イ　データマッピングの目的の設定

データマッピングにより、事業者全体でデータを一元管理して法令の遵守状況の確認やリスクへの対応を行うことができます。もっとも、遵守を確認する法令（さらには、法令の規制のうち、どの規制について重点的に確認するか）や、特定しようとするリスクを定めることにより、データマッピングする項目やデータの範囲を定めることができます。そのため、データマッピングの目的（データマッピングで遵守を確認しようとする法令、特定しようとするリスク）を設定する必要があります。

具体的な目的例	データマッピングする項目等
個人情報保護法全般を遵守しているかを確認するため	【データマッピングの範囲】 個人情報保護法の適用を受ける情報を含むデータ

	【データマッピングの中心となる項目】 個人情報保護法の遵守の確認のために必要な項目
個人情報保護法の規制のうち、個人データの越境移転規制等[3]を中心に確認するため	【データマッピングの範囲】 個人情報保護法の適用を受ける情報を含むデータ 【データマッピングの中心となる項目】 個人情報保護法のうち、越境移転規制等の遵守の確認のために必要な項目
保管しているデータの内容に応じた適切なセキュリティが施されているか確認するため	【データマッピングの範囲】 全てのデータ 【データマッピングの中心となる項目】 データの内容、保管態様、利用・アクセス範囲、施されているセキュリティ等

ウ　データマッピングする項目及び対象とするデータの範囲の設定

データマッピングの目的に応じて、データマッピングする項目及び対象とするデータの範囲[4]を設定します。

なお、本ツールキットでは、データマッピングの目的を、「個人情報保護法の規制のうち、個人データの越境移転規制等を中心に確認するため」として、対象となるデータの範囲を、個人情報保護法の適用を受ける情報を含むデータとする場合の項目例を第２章でご説明します。

エ　データマッピング表のフォーマットの作成

データマッピング項目を記載するためのフォーマット（データマッピング表）を作成します。フォーマットは表計算ソフトやデータマッピングツール等を用いて作成することが考えられます。

なお、データマッピングとしては、データベース単位で行う[5]、プロジェクト単位で行う[6]等の方法が考えられます。

---

[3] 具体的には、外国にある第三者への提供の制限（法第 28 条）並びに「外国において個人データを取り扱う場合」において必要な外的環境の把握（ガイドライン（通則編）10－７）及び保有個人データに関する事項の公表等（法第 32 条第１項）です。

[4] データマッピングの範囲を個人情報に限定しても、事業者が取り扱う個人情報のすべてをデータマッピングするためには多大なコストが必要になります。そのため、リスクやコスト等も考慮して、データマッピングをする範囲を決定する必要があります。

[5] 本ツールキットにおいては、この方法を前提にしています。

[6] あるプロジェクトで使用するデータについて、当該プロジェクトにおける取扱いをデータマッピング表に記入する等です。

オ　データマッピング表の記入者の決定

データマッピング表の各項目の記入者を決定します。項目の記入の難易度等に応じて、同じデータであっても、項目によって記入者を分けることも考えられます。

(2)データマッピング表の作成

ア　記入者によるデータマッピング表の記入

データマッピング表の記入者には、データマッピングの意義、目的、対象となるデータの範囲等について十分に理解してもらう必要があります。そのため、以下のような工夫をすることが考えられます。

- データマッピング表の記入者を対象とした説明会を開催する[7]。
- データマッピング表の記入者に具体的な記入方法を記載したマニュアル等を配布する。
- データマッピング表の記入者にデータマッピングについて説明する際には理解が難しい法律概念を使用するのではなく、平易な言葉で説明する。
- 事業者における個人データの取扱状況等に応じて、データマッピングする項目に該当する事例や具体的な記載例等を示す。
- データマッピング表の記載欄をプルダウン方式として、負担を減らす。

イ　データマッピング担当部署による記入の正確性の確認

データマッピング担当部署は、記入者が記入したデータマッピング表について、正しい理解に基づいて記入されているか等を確認する必要があります。

また、データマッピングの分量が多い場合は、担当部署の負担軽減のため、担当部署と記入者の間に、例えば部門別にとりまとめ担当者を決定して、形式面等を含めて２段階で確認することが考えられます。

(3)データマッピング表の確認・対応

作成したデータマッピング表を、データマッピングの目的に沿って確認し、必要な対応（是正）をする必要があります。詳細は第３章をご参照ください。

(4)データマッピング表の随時又は定期的な更新

事業者全体における最新のデータの取扱状況等を把握するため、以下のタイミングでデータマッピング表を更新することが望ましいです。

---

[7] 個人情報保護委員会が公表している資料等もご参照ください。
https://www.ppc.go.jp/news/publicinfo/

・記載事項に変更が生じた場合（随時）
・データを使用したサービスの仕様を変更する場合
・法改正があった場合
・定期的（半年に１回程度）

特に、事業の企画・設計段階で、当該事業において取り扱う予定のデータについてデータマッピング表に記入することで、予定している取扱いが法令を遵守しているのかを検討して事前に是正するとともに、洗い出された管理体制等のリスクに応じた対応をとることができます。

★ データマッピング表への取扱条件の記入について

データの取扱いを開始する前に、データのリスク等に応じて取扱条件を決めておき、その条件をデータマッピング表に記入することが考えられます。

例えば、顧客から取得したデータＡについて、取扱いを開始する前に、

① 自らデータＡの分析ができないため、データ分析についての委託は認めるが、データ分析以外の委託は認めない
② データＡは第三者への提供について本人から同意を得ているが、外国にある第三者に提供することについて本人から同意を得ていないため、外国にある第三者への提供を禁止する

との取扱条件を決めて、それをデータマッピング表に記入します。その上で、データを取り扱う場合にはデータマッピング表を事前に確認することとしておけば、記載された取扱条件に従って取り扱うことができます。

（例）

	取扱条件		
	委託	第三者提供	外国にある第三者への提供
データＡ	分析のみ可	可	不可

第２章　データマッピング表の項目等

本ツールキットでは、データマッピングの目的を「個人情報保護法の規制のうち、個人データの越境移転規制等を中心に確認するため」とする場合のデータマッピングの項目例を示しています。別紙１に記載例が示されていますので、それもあわせてご参照ください。

★　個人情報保護法の適用を受ける情報は顧客情報や取引先情報だけ？

個人情報保護法の適用を受ける情報は、事業者が顧客、取引先等から取得したものだけではなく、例えば、以下のものも含まれます。

- 委託元から委託に伴って提供を受けたもの
- 他の事業者から購入等することによって取得したもの
- 社員（離職者も含む）や求人応募者から取得したもの
- 取引先からもらった法人の情報であっても、担当者名等が記載されているもの

1. 基本項目

データの基本項目を把握するために、下記の項目についてデータマッピングを行います。

	項目	項目の記載例
①	データの名称	電子データに付している名称や紙媒体の表紙等に記載されている名称
②	取扱部署	事業者内でデータの管理責任を負っている部署名
③	責任者	データの管理責任を負っている者の氏名又は役職名
④	人数	データに含まれる個人に係る人数（概数でも可）
⑤	データの項目	データに含まれる情報の概要[8]
⑥	利用目的	データの利用目的
⑦	データの分類	下記の分類のうち、データに含まれる情報の分類名 ＜分類[9]＞ 個人情報、個人データ（保有個人データ）、仮名加工

[8] データの項目については、項目例を示し、その項目例に該当する項目がデータ内に含まれていれば、その項目名を記載させることが考えられます。なお、記載する項目例においては要配慮個人情報や個人識別符号を列挙しておくことが考えられます。

[9] それぞれの情報の定義等については、ガイドライン（通則編）2-1、2-2、2-6、2-7 及びガイドライン（仮名加工情報・匿名加工情報編）2-1-1、3-1-1 を参照してください。

		情報（個人情報である仮名加工情報、個人情報でない仮名加工情報）、匿名加工情報、個人関連情報
⑧	要配慮個人情報の有無	要配慮個人情報[10]を含むデータであるか
⑨	データの本人	データの本人の氏名・名称又は属性
⑩	データの取得方法	データの取得方法（本人から直接取得、本人以外の者からの取得（取引先からの取得等）等）
⑪	第三者提供の同意の有無	第三者提供の同意を得ているか

2. 事業者内での取扱い

事業者内における保管状況等を明らかにするために、下記の項目についてデータマッピングを行います。

(1)保管についての基本項目

	項目	項目の記載例
⑫	データの保存形態	データの保存形態（電子データ、紙媒体等）
⑬	データの保管場所	自社保管（自社キャビネット、自社 USB、自社所有サーバ等）、自社契約のクラウドで保管、委託先で保管等
⑭	保存期間	法律又は事業者内で定められた保存期間

(2)従業者[11]の利用・アクセス

	項目	項目の記載例
⑮	利用･アクセスできる従業者	事業者内でデータを利用･アクセスできる従業者の範囲（氏名又は属性）
⑯	従業者がいる国	上記の従業者がいる国名[12]

[10] 要配慮個人情報についてはガイドライン（通則編）2-3 を参照してください。

[11] 「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者等をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれます。

[12] 外国支店に常駐していたり、外国に居住してテレワークを行う等により、外国からデータを利用・アクセスする者がいる場合には、その者がいる国・地域名を記載します（以下、「国」には地域も含みます。）。

(3)事業者がデータについて利用しているクラウド[13]

上記⑬において自社契約のクラウドと記載された場合に記載します。

	項目	項目の記載例
⑰	クラウド事業者名	データについて利用しているクラウドを運営するクラウド事業者名
⑱	クラウド事業者の本店所在国	上記クラウド事業者の本店所在国名
⑲	サーバ所在国	データが保存されているサーバ所在国名
⑳	契約書情報	上記クラウド事業者と締結している契約書の情報（事業者内で契約書に付している管理番号や契約書に記載されている締結年月日・契約書の標題等）

(4) 自社保管の場合の保管国

上記⑬において自社保管と記載された場合に記載します。

	項目	項目の記載例
㉑	保管国	データが印刷された紙媒体やデータが保存されている USB・サーバ等の所在国名

3. 「委託先（再委託先を含む）での取扱い」（事業者が利用しているクラウド事業者を除く）

委託先及び再委託先の事業者がどのような管理を行っているか等を明らかにするために、委託がなされている場合には、下記の項目についてデータマッピングを行います。

(1)委託先の基本項目

	項目	項目の記載例
㉒	委託先	委託先の氏名・名称 ※例えば以下のものが委託に該当する。 ・データの集計、データの解析、データの取得等のデータの内容に関与する委託 ・データを取り扱う情報システム（ハードウェア、

[13] クラウド事業者には、いわゆる、SaaS、IaaS、PaaS 等のサービス形態があり、また、事業者が複数のクラウド事業者と契約を締結していたり、事業者が直接契約しているクラウド事業者において他のクラウド事業者を利用している場合（クラウド事業者が他のクラウド事業者の IaaS を利用して SaaS を提供している場合等）もありますので、契約形態に応じて漏れなくデータマッピングを行う必要があります。

		ソフトウェアを含む）の保守
㉓	委託先の本店所在国	委託先の本店所在国名
㉔	契約書情報	上記委託先と締結している契約書の情報
㉕	委託の目的・範囲	委託契約書に記載の委託の目的、範囲
㉖	再委託の有無	再委託を行っているか

(2)委託先の保管等についての基本項目

	項目	項目の記載例
㉗	データの保存形態	データの保存形態（電子データ、紙媒体等）
㉘	データの保管場所	委託先が保管（委託先キャビネット、委託先 USB、委託先所有サーバ等）、委託先が契約するクラウドで保管、再委託先で保管等

(3)委託先の従業者の利用・アクセス

	項目	項目の記載例
㉙	利用･アクセスできる従業者	委託先の事業者内でデータを利用･アクセスできる委託先の従業者の範囲（氏名又は属性） ※以下のような場合には、これに該当する。 ・事業者（委託元）の契約するサーバに保存されているデータについて、委託先、再委託先の従業者に対してデータ利用・アクセスを認める場合 ・委託先、再委託先が委託先・再委託先の契約するサーバにデータを保存し、委託先、再委託先の従業者に対してデータ利用･アクセスを認める場合
㉚	従業者がいる国	上記の従業者がいる国名

(4)委託先が委託をしたデータについて利用しているクラウド

上記㉘において委託先が契約するクラウドと記載された場合に記載します。

	項目	項目の記載例
㉛	クラウド事業者名	データについて利用しているクラウドを運営するクラウド事業者名
㉜	クラウド事業者の本店所在国	上記クラウド事業者の本店所在国名
㉝	サーバ所在国	事業者のデータが保存されているサーバ所在国名

(5)委託先保管の場合の保管国

上記㉘において委託先保管と記載された場合に記載します。

	項目	項目の記載例
㉞	保管国	データが印刷された紙媒体やデータが保存されているUSB・サーバ等の所在国名

4. 「第三者（親会社・子会社等のグループ会社を含む）への提供」（事業者が利用しているクラウド事業者及び委託先・再委託先を除く）

データの第三者（事業者以外の者であり、親会社・子会社等のグループ会社を含む）への提供の実態等を把握するために、下記の項目についてデータマッピングを行います。

	項目	項目の記載例
㉟	提供先	データの提供先の第三者の氏名・名称
㊱	提供先属性	上記提供先の業種等の属性
㊲	提供先の本店所在国	提供先の本店所在国名[14]
㊳	契約書情報	提供先の第三者と締結している契約書の情報

★ 「提供」とは物理的に渡すことだけ？

ここでの「提供」とは、自己以外の者が利用可能な状態に置くことをいいます。そのため、物理的に提供されていない場合であってもデータを利用できる状態にあれば（利用する権限が与えられていれば)、「提供」に当たります。

（提供にあたる例）

- データを紙に印刷して持ち帰ったり、データを記憶媒体に保存して持ち帰ることを認めている。
- データを紙に印刷してその紙を第三者に見せている。
- データをサーバに保存した上で、サーバに保存してあるデータへのアクセス権限を認めている。
- API連携等により、データを利用することを認めている。

5. その他の項目

上記のデータマッピング表の項目はあくまで一例にすぎません。そのため、データマッピングの目的等を踏まえて、項目の追加・削除をしてください。な

[14] データが国内のサーバに保存されていたとしても、提供先が外国にある場合には記載してください。

お、データマッピング表に追加する項目としては、以下の項目が考えられます。

基本項目	● データの取得時期 ● 利用目的の本人への周知方法（本人に明示して同意を得ている、ホームページに公表している等） ● 匿名加工情報や仮名加工情報への加工の有無
事業者内での取扱い	● 使用しているクラウドのサービス名 ● データを保管しているシステム名 ● 事業者内のセキュリティ分類 ● 事業者内で講じている安全管理措置の内容（アクセス制御の有無や暗号化の状態等） ● 廃棄の時期、廃棄方法 ● 他のデータとの突合の有無（他社から受け取った Cookie 情報等のデータを突合しているか）[15]
委託先での取扱い	● 委託先への監査の実施時期 ● 委託先への監査の結果
第三者への提供	● 事業者以外の者に対する提供の根拠条文（法第 27 条１項柱書、同条１項各号、同条５項各号、法第 28 条） ● 共同利用に関する事項（共同利用の実施の有無、共同利用先） ● 越境移転のための本人同意にあたっての参考情報の提供の有無（法第 28 条２項）
その他	● データに適用されるルールの概要 ● 社内基準による PIA[16]実施対象データか否か ● データマッピング表の記入者、記入日

[15] Cookie 等の個人関連情報を個人データと突合するために取得する場合には、個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の本人の同意を得ること等が必要です（法第 31 条参照）。

[16] PIA とは、個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法です。PIA については、個人情報保護委員会が公表している「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点」をご参照ください。

第３章　データマッピング表の確認・対応

1. 概要

データマッピングは、データマッピング表の作成自体が目的ではなく、作成したデータマッピング表を、データマッピングの目的に沿って確認し、必要な対応（是正）をする必要があります。

2. 個人情報保護法を含むデータに適用される法令の遵守状況の確認

データマッピング表を用いて、個人情報保護法を含むデータに適用される法令の遵守状況の確認を行います。

個人情報保護法の遵守状況については、例えば、データマッピング表の項目の「利用目的」を参照して法第 17 条（利用目的の特定）を遵守しているか、「事業者内での取扱い」の項目を参照して利用・アクセス範囲を適切に限定しているか（法第 23 条に基づいて安全管理措置が適切に講じられているか）等について確認することができます。

個人情報を含むデータの国境を越えた流通が増加していること等から、本ツールキットにおいては、以下の越境移転規制等について確認するべき点とともに、確認を補助するためのチェックリストを添付しています。

(1)外国にある第三者に個人データを提供する場合のルール（法第 28 条）

個人情報保護法においては、個人データの第三者提供に関して法第 27 条（第三者提供の制限）が定められていますが、個人データの「外国にある第三者への提供」については、法第 28 条（外国にある第三者への提供の制限）が定められています。

法第 28 条の適用を受ける場合には、法第 27 条による国内における第三者への個人データの提供と異なり、参考情報を提供した上で、あらかじめ外国にある第三者に提供する旨の本人の同意を得る等の規律があり、これを遵守しなければなりません。この規律を遵守しているかの確認を補助するための「チェックリスト（外国にある第三者への提供）」（別紙２）も参考にして、確認を行ってください。

(2)外国において個人データを取り扱う場合のルール

外国において個人データを取り扱う場合には、法第 23 条に基づき、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じるとともに、法第 32 条に基づき、講じた安全管理措置の内容として当該外国の名称等を公表等する必要があります。

この規律を遵守しているかの確認を補助するための「チェックリスト（外国において取り扱う場合）」（別紙３）も参考にして、確認を行ってください。

3. データの取扱状況等に起因するリスクに応じた必要な対応の実施

データマッピング表を用いて、データの取扱状況等に起因するリスクを特定し、必要な対応を実施します。

データマッピング表で特定されるリスクとその対応としては、例えば、以下のようなものがあります。

(1)データの内容におけるリスク

例えば、要配慮個人情報を含むデータや膨大なデータについて漏えい等が生じた場合には本人及び事業者にとって重大な損害リスクがあります。

そのため、データマッピング表の「データの項目」や「要配慮個人情報の有無」を参照して、データの内容を評価するとともに、事業者内や委託先において必要な対応（セキュリティやアクセス制御等）がとられているかを確認する必要があります。

(2)保管におけるリスク

例えば、事業者にとって重要なデータを紙媒体でしか保管していない場合には紛失等のリスクがあり、また、事業者内のデータを一つのクラウドに保管しているような場合にはそのクラウドから漏えい等が生じた場合には多くのデータが漏えい等するリスクがあります。

そのため、データマッピング表の「事業者内での取扱い」や「委託先(再委託先を含む)での取扱い」等の項目を参照して、保管のリスクを評価するとともに、事業者内や委託先において必要な対応（セキュリティやアクセス制御等）がとられているかを確認する必要があります。

(3)利用におけるリスク

例えば、事業者内で利用する場合や第三者に提供する場合等、それぞれの取扱いに応じて適切に利用しなければ、法令違反のリスクがあります。

そのため、データマッピング表の「利用目的」や「第三者提供の同意の有無」等の項目を参照して、法令を遵守しているか等について確認する必要があります。

以上