

データマッピング・ ツールキット



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、p.3以降に示す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。



■ 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)）。

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。

データマッピングの手順

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
（次ページ以降で紹介）
- 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

表作成

- 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

確認・対応

- 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）

更新

- データマッピング表の随時または定期的な更新

■ データマッピング表の項目

次頁以降で示す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。なお、個人情報保護委員会が用意したデータマッピング・ツールキットに含まれる項目以外に、データマッピング表に追加が考えられる項目としては、以下のような項目が考えられます。

データマッピング表に追加する項目の一例

基本項目	<input type="checkbox"/> データの取得時期 <input type="checkbox"/> 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) <input type="checkbox"/> 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	<input type="checkbox"/> 使用しているクラウドのサービス名 <input type="checkbox"/> データを保管しているシステム名 <input type="checkbox"/> 事業者内のセキュリティ分類 <input type="checkbox"/> 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) <input type="checkbox"/> 廃棄の時期、廃棄方法 <input type="checkbox"/> 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)
委託先での取扱い	<input type="checkbox"/> 委託先への監査の実施時期 <input type="checkbox"/> 委託先への監査の結果
第三者への提供	<input type="checkbox"/> 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) <input type="checkbox"/> 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) <input type="checkbox"/> 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	<input type="checkbox"/> データに適用されるルールの概要 <input type="checkbox"/> 社内基準によるPIA実施対象データか否か <input type="checkbox"/> データマッピング表の記入者、記入日

データマッピング表の項目と記入例 (基本項目)

基本項目					
データの名称	取扱部署	責任者	人数	データの項目	利用目的
①	②	③	④	⑤	⑥
2019年～2020年に各種キャンペーンで取得した顧客情報	事業開発部	事業開発部 総務課長	10,000人	住所(市町村まで)、購買履歴(購入日、購入物)	当社の新規事業の開発

※ 事例として、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を示しています。

	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
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> 個人情報、個人データ(保有個人データ)、仮名加工情報(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

データの分類	要配慮個人情報の有無	データの本人	データの取得方法	第三者提供の同意の有無
⑦	⑧	⑨	⑩	⑪
仮名加工情報 (個人情報である 仮名加工情報)	含まない	顧客	本人から直接取得したデータを仮名加工	—

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更新 【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

データマッピング表の項目と記入例（事業者内での取扱い）

事業者内での取扱い				
保管についての基本項目			従業員の利用・アクセス	
データの保存形態	データの保管場所	保存期間	利用・アクセスができる従業員	従業員がいる国
⑫	⑬	⑭	⑮	⑯
電子データ	自社保有サーバ	10年	全社員	日本

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	保管期間	法律又は事業者内で定められた保存期間

（２）従業員の利用・アクセス

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

（３）事業者がデータについて利用しているクラウド

上記⑬において自社契約のクラウドと記載された場合のみ

	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）

事業者がデータについて利用しているクラウド				自社保管の場合の保管国
クラウド事業者名	クラウド事業者の本店所在国	サーバ所在国	契約書情報	保管国
⑰	⑱	⑲	⑳	㉑
クラウド事業者名	クラウド事業者の本店所在国	サーバ所在国	契約書情報	保管国

(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のみ

	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

参考 「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もデータマッピングを行います。

- | | |
|----------------------|--------------------------------|
| (1) 委託先の基本項目 | (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 |
| (2) 委託先の保管等についての基本項目 | (5) 委託先保管の場合の保管国 |
| (3) 委託先の従業者の利用・アクセス | |

参考 「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、「提供先」、「提供先の属性(業種等)」、「提供先の本店所在地」、「契約書情報」等の項目についてもデータマッピングを行います。

データマッピング表の作成以後に行うこと

■ 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。

■ 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い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。

- 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は是正するとともに、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い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い条件を決めておき、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い条件を決めて、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すれば、記載された取扱い条件に従って取り扱うことができます。

(例)

	取扱い条件		
	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

データマッピング・ツールキットのテンプレートは
個人情報保護委員会HPからダウンロードできます。

個人情報保護委員会>個人情報保護等>民間の自主的取組(PIA・データマッピング等)
https://www.ppc.go.jp/personalinfo/independent_effort/

