JIPDECセミナー
「個人情報のクラウド保管 実務における対応ポイント」講演資料

講演資料01
「クラウドを利用する際に遵守すべき個人情報保護法のルール」

本資料は、2023年9月5日（火）開催、JIPDECセミナーで配布した資料です。セミナーお申込み者様限定での配布となりますので、WEB、SNS等への掲載、転載はご遠慮ください。

また、本セミナー（資料）は、プライバシーマークの構築運用指針を解説するものではありません。

2023.09.05

クラウドを利用する際に遵守すべき
個人情報保護法のルール

令和５年９月

クラウドを利用する際に遵守すべき個人情報保護法のルール

クラウドを利用する場合の留意点

①個人データの第三者への「提供」（個人データの第三者提供）に該当するか。

②「個人データの第三者提供」に該当した場合の個人情報保護法上のルール（外国のクラウド提供事業者を利用する場合を中心として）

③クラウドを利用する場合の安全管理措置（外的環境の把握を含む）

④安全管理措置の公表等

クラウド事業者への個人データの第三者提供

- 「個人データの第三者提供」に該当する場合には法27条・法28条のルールを遵守しなければならない。
- クラウド事業者に対する「提供」があるかは、クラウド事業者において個人データを「取り扱うこととなっているのかどうか」が判断基準となる。

クラウドサービスを提供する事業者において個人データを取り扱うこととなっているか

※ 取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等

YES

クラウド事業者に対する「**提供**」に該当する

※ **法27条・法28条のルールを遵守しなければならない**

NO

クラウド事業者に対する「**提供**」に該当しない

※ **「提供」に該当しなくとも安全管理措置は必要**

クラウド事業者への第三者提供に該当する場合の留意点

- 外国にあるクラウド事業者（外国にある第三者）に個人データを第三者提供する場合には、法28条のルールを遵守しなければならない。

法28条のルール

原則：本人に対して情報提供をした上で、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得なければならない（法28条1項・法28条2項）。

例外：①外国にある第三者が我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している国（EU及び英国）に所在する場合
⇒法27条のルールを遵守しなければならない。

②外国にある第三者が個人情報取扱事業者が講ずべきこととされている措置に相当する措置（相当措置）を継続的に講ずるために必要なものとして委員会規則で定める基準に適合する体制（基準適合体制）を整備している場合
⇒法27条及び法28条3項のルールを遵守しなければならない。

③法２７条１項各号に該当する場合（法令に基づく場合等）

クラウド事業者への第三者提供に該当する場合の留意点

本人同意の要否のまとめ

日本にあるクラウド事業者

外国にあるクラウド事業者

提供先が①EU又は英国、
②基準適合体制の場合

法27条が適用

法28条1項・2項が適用

原則：同意が必要。
例外：法27条1項各号、法27条2項（オプトアウト）、法27条5項各号（**委託**、事業承継、共同利用）

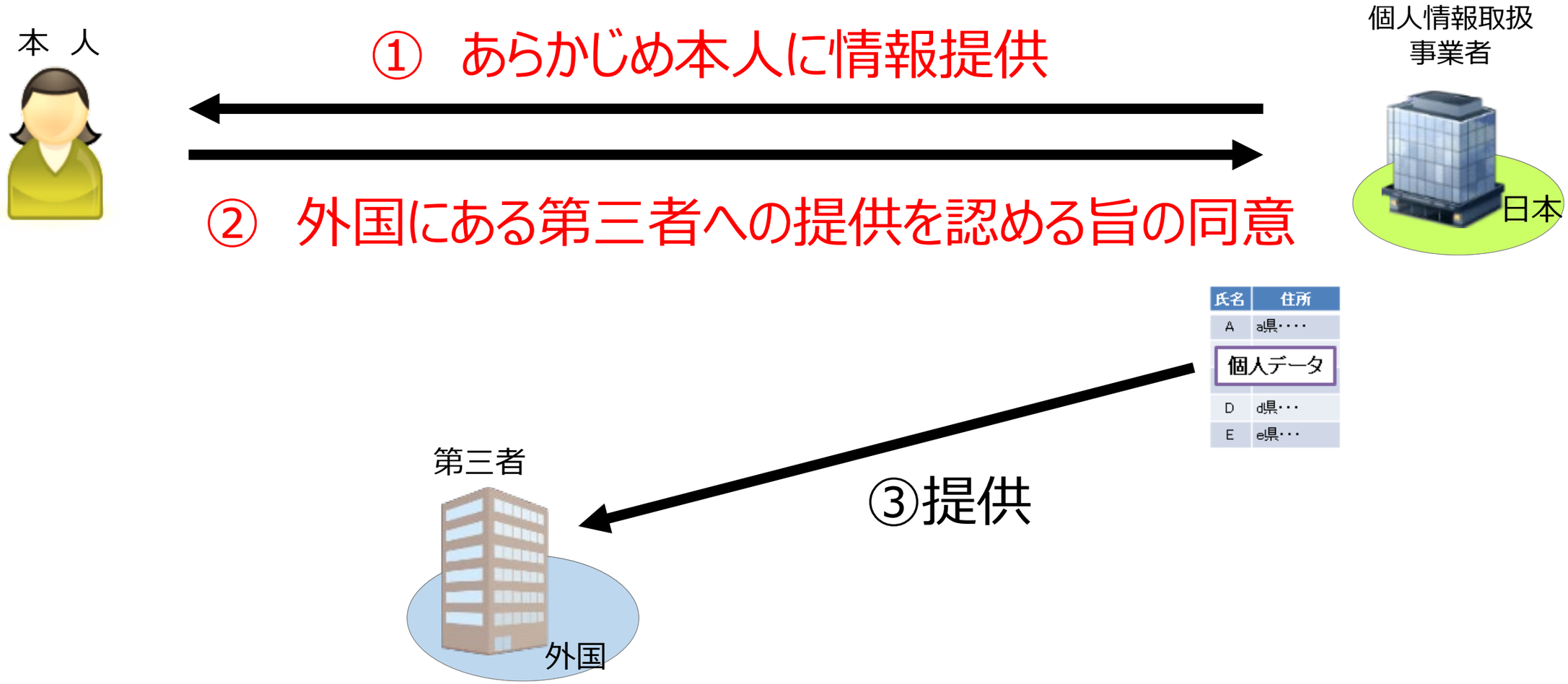
※「委託」と整理できる場合には同意は不要

原則：本人に情報を提供した上で外国にある第三者への提供を認める旨の同意が必要。
例外：法28条1項が準用する法27条1項各号

※法28条の場合には「委託」であっても同意を得なければならない。

クラウド事業者への第三者提供に該当する場合の留意点

- 法28条1項・2項により個人データを提供する場合には情報提供をした上で、外国にある第三者への提供を認める旨の同意を得なければならない。



上記①の情報提供については、本人が確実に認識できると考えられる適切な方法により、以下の事項について情報提供する必要があります。

- ○ 第三者（提供先）が所在する外国の名称
- ○ 適切かつ合理的な方法により得られた上記外国における個人情報保護制度
- ○ 第三者（提供先）が講ずる個人情報保護のための措置

（参考）外国制度に係る情報提供

●個人情報保護委員会では、<u>調査対象とする国又は地域の個人情報の保護に関する制度</u>と<u>我が国の個人情報保護法との間の本質的な差異</u>の把握に資する一定の情報を公表しています。

URL：https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/

（１）調査対象の国又は地域（50音順）右記のとおり。
（※１）「ADGM」は、Abu Dhabi Global Market を指す。
（※２）「DHC」は、Dubai Healthcare City を指す。
（※３）「DIFC」は、Dubai International Financial Centre を指す。

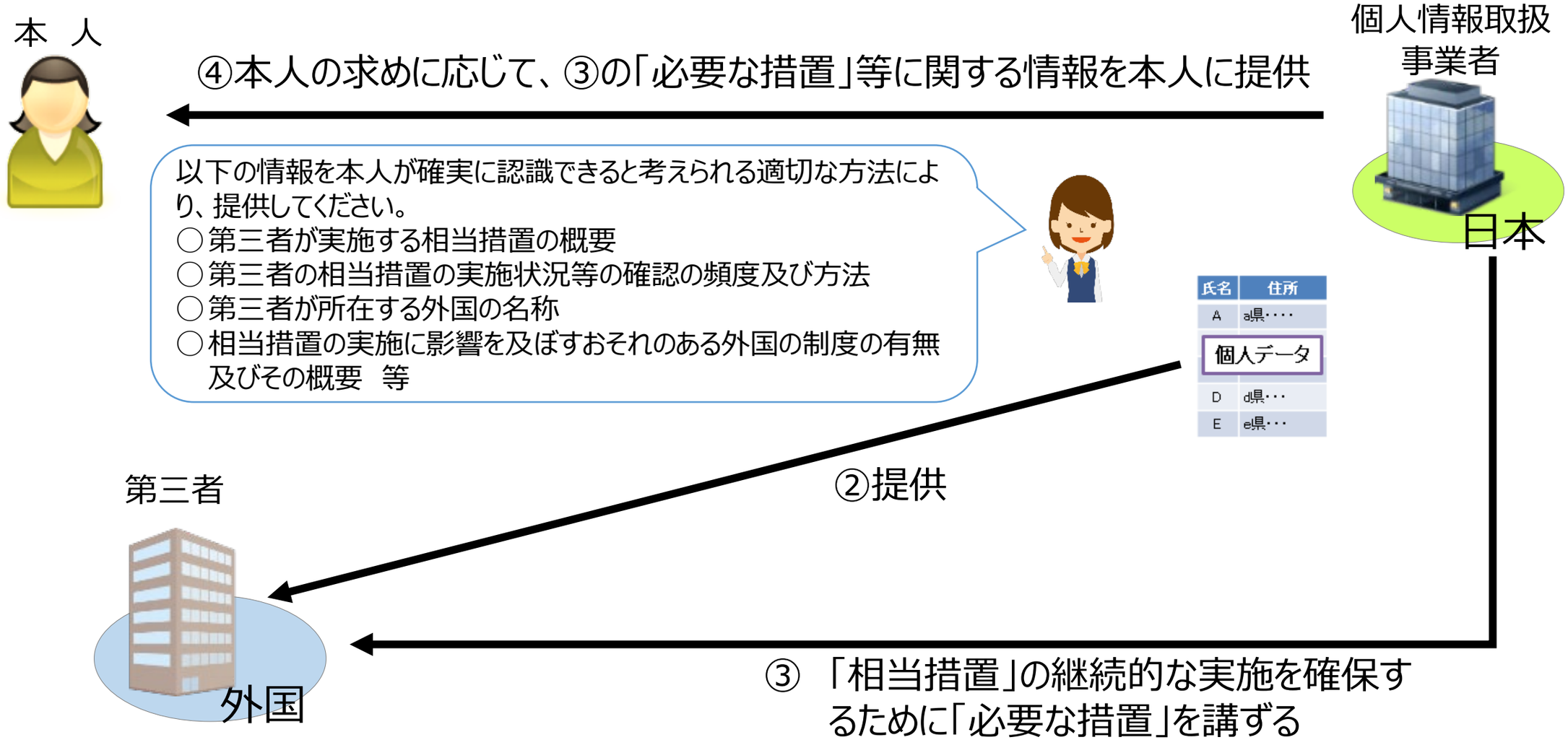
（２）調査項目
① 個人情報の保護に関する法制度の有無
② 個人情報の保護に関する制度についての指標となり得る情報の有無
③ OECD プライバシーガイドライン８原則（※４）に対応する個人情報の取扱いに係る義務又は本人の権利に関する規定の有無
④ その他本人の権利利益に重大な影響を及ぼすおそれのある制度の有無及びその概要

（※４）OECDが1980年9月に採択した「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」に記述されている、「収集制限の原則」「データ内容の原則」「目的明確化の原則」「利用制限の原則」「安全保護の原則」「公開の原則」「個人参加の原則」「責任の原則」を指す。

1	アメリカ合衆国（連邦）	2	アメリカ合衆国（イリノイ州）	3	アメリカ合衆国（カリフォルニア州）
4	アメリカ合衆国（ニューヨーク州）	5	アラブ首長国連邦（連邦）	6	アラブ首長国連邦（ADGM）（※１）
7	アラブ首長国連邦（DHC）（※２）	8	アラブ首長国連邦（DIFC）（※３）	9	イスラエル国
10	インド	11	インドネシア共和国	12	ウクライナ
13	オーストラリア連邦	14	カタール国	15	カナダ
16	カンボジア王国	17	コスタリカ共和国	18	シンガポール共和国
19	スイス連邦	20	タイ王国	21	大韓民国
22	台湾	23	中華人民共和国	24	チュニジア共和国
25	トルコ共和国	26	ニュージーランド	27	パナマ共和国
28	フィリピン共和国	29	ブラジル連邦共和国	30	ベトナム社会主義共和国
31	ペルー共和国	32	香港	33	マレーシア
34	南アフリカ共和国	35	ミャンマー連邦共和国	36	メキシコ合衆国
37	モロッコ王国	38	モンゴル国	39	ラオス人民民主共和国
40	ロシア連邦				

クラウド事業者への第三者提供に該当する場合の留意点

- 基準適合体制を整えた第三者に個人データを提供する場合であっても、法27条に従って提供しなければならない。
- 上記の場合には、さらに法28条3項に基づく情報提供と「必要な措置」を講じなければならない。

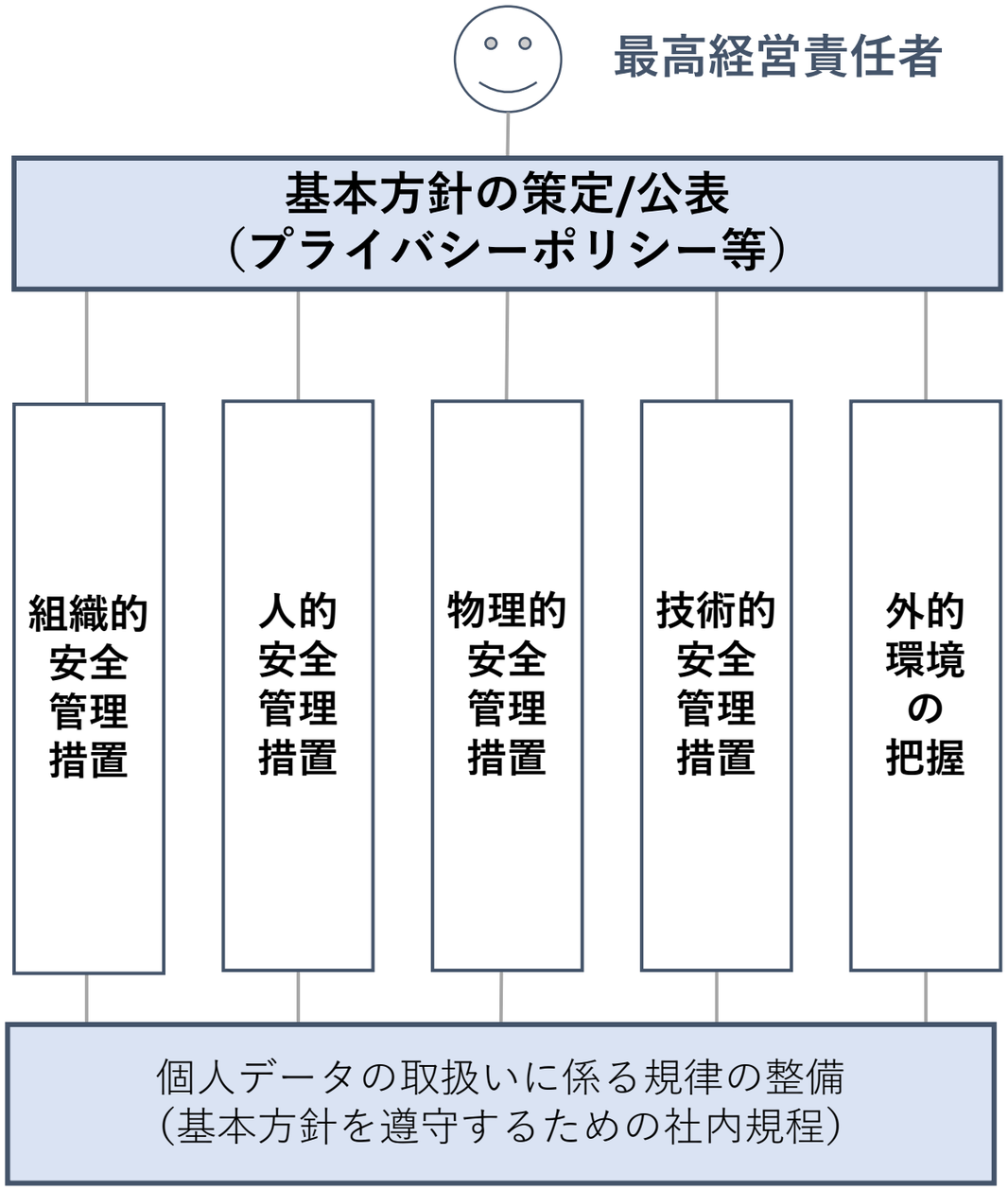


① 「相当措置」を継続的に講ずるために個人情報保護委員会が定める基準に適合する体制を整備

「必要な措置」とは以下の措置です。
○第三者の相当措置の実施状況等を定期的に確認
○第三者の相当措置の実施に支障が生じたときは一定の措置
○第三者の相当措置の継続的な実施の確保が困難となったときは提供を停止

クラウドを利用する場合の安全管理措置（外的環境の把握を含む）

- クラウド事業者に対して「提供」していない場合でも、個人データに対して安全管理措置を講じなければならない。
- クラウド事業者に対して「提供」している場合、委託であれば安全管理措置を講じるとともに、委託先の監督をしなければならない。



1. 組織的安全管理措置
(1) 組織体制の整備
(2) 個人データの取扱いに係る規律に従った運用
(3) 個人データの取扱状況を確認する手段の整備
(4) 漏えい等事案に対応する体制の整備
(5) 取扱状況の把握及び安全管理措置の見直し

2.人的安全管理措置
(1) 従業者の教育

3.物理織的安全管理措置
(1) 個人データを取り扱う区域の管理
(2) 機器及び電子媒体等の盗難等の防止
(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止
(4) 個人データの削除及び機器、電子媒体等の廃棄

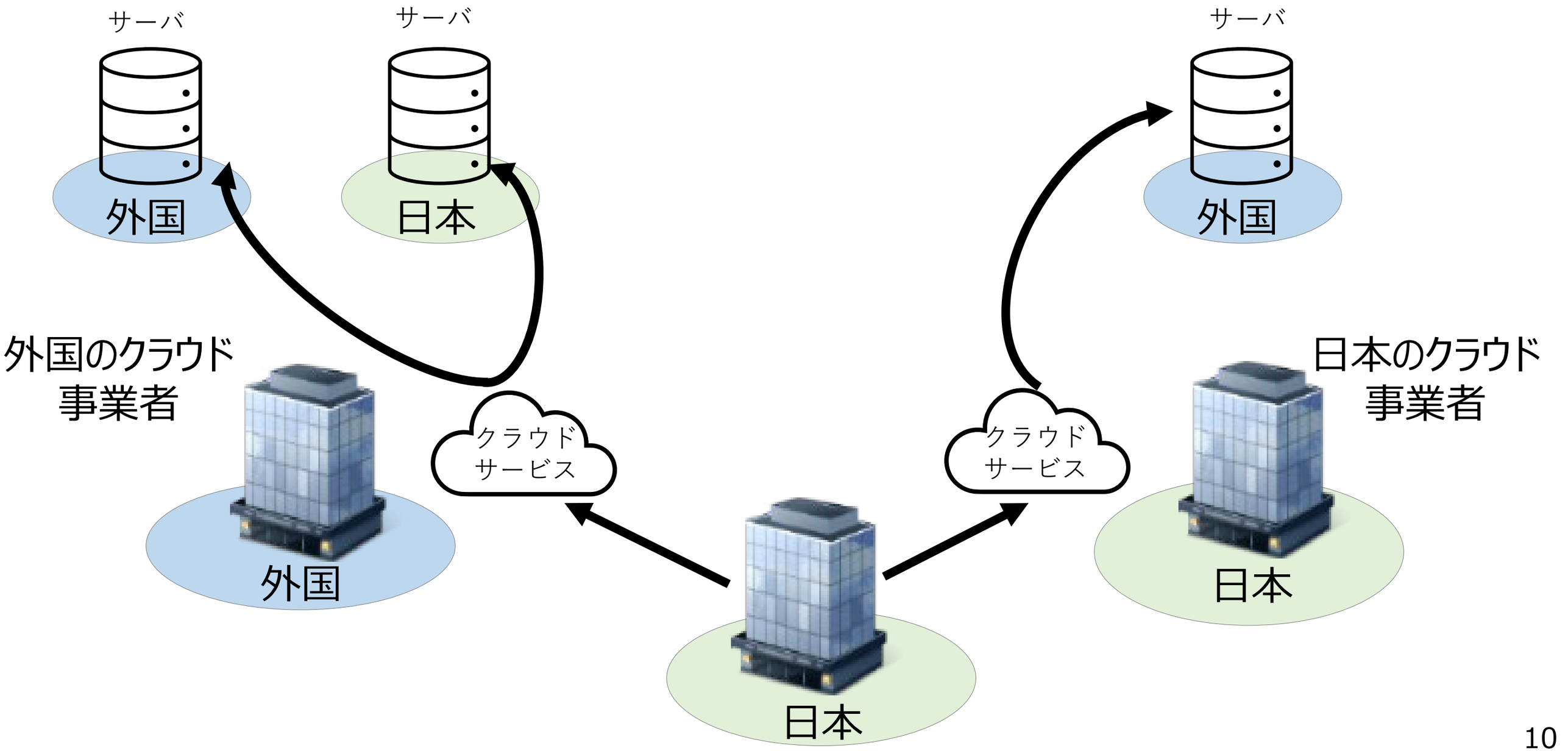
4.技術織的安全管理措置
(1) アクセス制御
(2) アクセス者の識別と認証
(3) 外部からの不正アクセス等の防止
(4) 情報システムの使用に伴う漏えい等の防止

5.外的環境の把握
外国において個人データを取り扱う場合、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、安全管理を実施

クラウドを利用する場合の安全管理措置（外的環境の把握を含む）

- クラウドを利用する場合において、「外国において個人データを取り扱う場合」とは、外国のクラウド事業者が提供するサービスを利用する場合や、サーバが外国にある場合等である。

「外国において個人データを取り扱う場合」



クラウドを利用する場合の安全管理措置の公表等

- 外国において個人データを取り扱う場合には「保有個人データの公表等」（法32条1項）として、個人データを取り扱う外国の名称の公表等をしなければならない（本人の求めに応じて遅滞なく回答することでも可）。

「公表等」するべき事項

①個人情報取扱事業者の氏名又は名称等
②全ての保有個人データの利用目的
③保有個人データの開示等の請求に応じる手続等
④保有個人データの安全管理のために講じた措置

外国で取り扱う場合には、④として、以下の事項を公表等
- ○　個人データを取り扱う外国の名称（サーバ設置国等）
- ○　外国の制度等を把握した上で講じた安全管理措置の内容

⑤保有個人データの取扱いに関する苦情の申出先　（認定個人情報保護団体の対象事業者である場合は、その団体の名称等を含む。）

JIPDEC