

スマートビルサービス提供に係る
ビルデータおよびパーソナルデータ管理・取扱手順

2025 年 5 月 30 日

目次

1. 総則	3
(1) 目的	3
(2) スマートビルサービスの概要	3
(3) 適用範囲	3
2. 用語の定義	3
(1) 本手順書における定義	3
3. 体制および責任	5
(1) 体制および責任	5
4. データ利活用に関する手続き	5
(1) データ利活用における原則	5
(2) データ利活用プロセスの適用条件	6
5. スマートビルサービス提供に係る企画	7
(1) 企画起案	7
6. 企画および取扱いデータの審査	11
(1) 企画評価	11
(2) リスク審査	14
7. データ取得	16
(1) データ取得	16
(2) 取得データの確認	19
8. データ利用	25
(1) データ利用前準備	25
(2) サービス提供／学内利用	26
(3) データ提供（委託・第三者提供・共同利用）	28
(4) サービス提供／学内利用終了	31
9. その他	32
(1) 企画変更手順	32
(2) 苦情問合せ	33

1. 総則

(1) 目的

学校法人立命館（以下、「本法人」という）は「立命館大学・エコシステム形成」に向けて、「立命館大学・大阪いばらきキャンパス」において、人々が多様な目的の下に集う複数のビル（教職員のオフィス、飲食店等の商業施設、市民交流型の施設、地域の商工会議所、災害時に地域住民が避難する防災公園等）が属する当キャンパスを「社会の縮図」として活用し、都市におけるサービス（利用者目線でのビルに求められる機能）を俯瞰的に整備する取り組みを推進している。

本法人は、ビルに係るサービス運営に係るデータを適正かつ効果的に利活用するための具体的な取扱い手順を定めることにより、利用者目線のきめ細やかなビル設備管理や個々の利用者に応じたサービス創出を推進するとともに、関連法令の遵守の下、サービス利用者のプライバシーを尊重したうえで安心・安全なデータ利活用を実現することを目的とする。

(2) スマートビルサービスの概要

ビルは社会活動の拠点として、オフィス、商業施設等の産業・経済の場や、研究施設を含む教育・文化的な人材交流の場であるとともに、非常時の防災・災害の場に至るまで、デジタル社会における地域経済の発展を担うものであり、その使途や利用ニーズはますます多様化している。

ビルの利用においても、ビル利用者から求められる、あるいはビル管理運営業務の効率化やビルの価値を向上させるために、ビル管理者から提供されるサービス（以下、「スマートビルサービス」とする）もビル利用者および管理者目線のきめ細やかなものが求められている。例えば、ビルサービス利用者に係る行動データと物理アセットの紐づけを試みることによる、利用者の行動予測による事前空調スタンバイや、必要な場所や時間に限定した照明コントロール等の設備コントロールが挙げられる。

これらのスマートビルサービス提供においては、ビル OS と IoT 基盤のデータ連携を促進することで、新たな協調領域を創出し、アプリケーション領域における参入障壁を下げ、新しいビジネスモデルの創出とビルの価値の継続的な向上へつながると考えられる。また、スマートビルサービスの利用を促進する一方で、ビルサービス利用者のプライバシーやセキュリティを確保しつつ、その活用を最大化するために、ビルや IoT 基盤から取得されるデータに対して適切なデータ管理と活用についてのガバナンスの整備が重要である。

(3) 適用範囲

① 対象組織

本法人、本法人が設置する学校、外部委託先および外部事業者を対象とする。

② 対象業務

立命館スマートビル運営に係るデータ・パーソナルデータを取扱う業務を対象とする。

2. 用語の定義

(1) 本手順書における定義

① データ

本法人のスマートビルサービスにおいて収集、保管、利活用されるデータをいう。

② スマートビルサービス

スマートビルサービス全体を指し、データを取得するためのカメラ、センサー等のビル設備、データを収集・蓄積するためのデータプラットフォーム、およびデータを提供するためのアプリやサービス等を含む。

③ 教職員等

本法人の役員および本法人と雇用関係にある者またはあつた者、教職員の指示を受けて業務に従事する学生、派遣労働者等をいう。

④ データ提供者

本法人のスマートビルサービスで利活用するデータを提供する一般市民、学生および教

職員等をいう。

⑤ データ利用者

本法人のスマートビルサービスにおいて提供されるデータを利活用する一般市民、学生および教職員等をいう。

⑥ データ提供事業者

本法人のスマートビルサービスで利活用するデータを提供する事業者をいう。本法人からスマートビルサービスに関する委託を受けデータを提供する事業者を含む。

⑦ データ利用事業者

本法人のスマートビルサービスにおいて提供されるデータを利活用する事業者をいう。本法人からスマートビルサービスに関する委託を受けデータを利活用する事業者を含む。

⑧ 個人情報

次のいずれかに該当する情報をいう。

- a. 生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等（文書、図画もしくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。）で作られる記録をいう。以下同じ。）に記載され、もしくは記録され、または音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
- b. 個人識別符号が含まれるものをいう。

⑨ 個人データ

「個人情報データベース等」を構成する個人情報をいう。「個人情報データベース等」とは特定の個人情報を、コンピュータを用いて検索することができるように体系的に構成した個人情報を含む情報の集合体、またはコンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則（例えば五十音順、生年月日順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態においているものをいう。

⑩ パーソナルデータ

個人が識別できるかどうかによらない、個人に関する情報全般をいう。個人の属性情報、移動・行動・購買履歴、カメラやセンサー等から収集された個人情報を含む。

⑪ 仮名加工情報

次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報をいう。

- (i) 第2条9項（ア）に該当する個人情報、当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）
- (ii) 第2条9号（イ）に該当する個人情報、当該個人情報に含まれる個人情報識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

⑫ 匿名加工情報

次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であつて、当該情報を復元することできないようにしたものをいう。

- (i) 第2条9項（ア）に該当する個人情報、当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

- (ii) 第2条9号(イ)に該当する個人情報 当該個人情報に含まれる個人情報識別符号の全部を削除すること(当該個人情報識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。)

3. 体制および責任

(1) 体制および責任

立命館スマートビル運営推進・管理体制について、「図3-1 立命館スマートビルサービス運営推進・管理体制図」に示す。各責任者・担当者の責任および権限は、『立命館スマートビルサービスに係るデータ取扱いガイドライン』の第3章に準ずる。

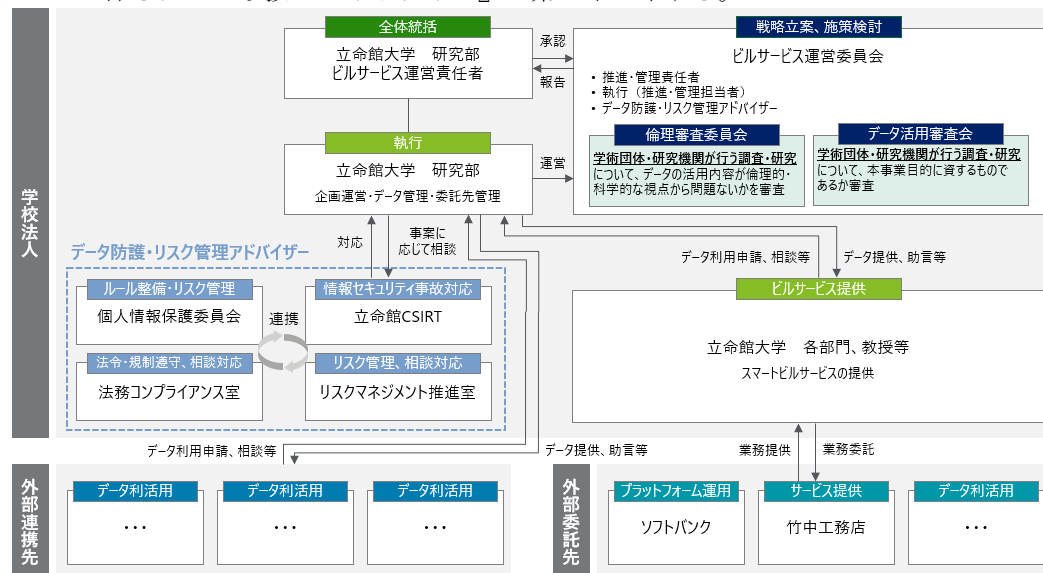


図3-1 立命館スマートビルサービス運営推進・管理体制図

4. データ利活用に関する手続き

(1) データ利活用における原則

立命館大学におけるビルサービス提供組織あるいは外部のビルサービス提供者（以下、ビルサービス提供者）は、原則として「立命館スマートビルサービスに係るデータ取扱いポリシー」に従ってスマートビルサービスに関連するデータを取扱い、ビルサービス関連データを提供する本人（以下、「本人」とする）の意向を最大限配慮して運用する。

① データの取得

スマートビルサービスの提供にあたってパーソナルデータを取得する際は、あらかじめビル利用者に利用目的を通知・公表し、必要に応じて本人より同意を取得したうえで、データを取得する。

② データの利用目的

ビル利用者から取得したデータは明示した利用目的以外に使用することではなく、データの利用目的を変更する必要がある場合には、その旨を事前に通知または公表する。

③ データの利用・分析

AI等の先端技術を用いてデータ分析する場合には、ビル利用者および本人のプライバシーを侵害したり、問題のある結果を導出したりすることのないよう、法的・倫理的・社会的影響の観点からリスクを評価したうえでスマートビルサービスを提供する。

④ データの提供、共有

スマートビルサービスの提供にあたっては、ビル利用者のプライバシーを尊重したうえで、『立命館スマートビルに係るデータ取扱いガイドライン』に従いデータを取扱う。なお、当該データに個人データが含まれる場合には、個人情報保護法等の関連する法令に従って適切に対応する。

⑤ 委託事業者の義務

本法人は、スマートビルサービスに関して、パーソナルデータの取扱いの全部または一部を委託する場合には、委託先を適切に監督するとともに、委託先に対して個人情報保護法等の関連する法令に従った取扱いを義務付ける。

⑥ 保有個人データの開示請求等

本法人は、本人またはその代理人からスマートビルサービスで保有する個人データの開示、内容の訂正、追加、削除、利用の停止または第三者への提供の停止等の請求があった場合には、適切に対応する。

⑦ データの安全管理措置

スマートビルサービスを通じてビル利用者から取得したパーソナルデータについて、紛失、破壊、改ざんおよび漏えい等を防止するため、不正アクセス対策、コンピュータウイルス対策等適切な情報セキュリティ対策を講じるとともに、その運用状況を監視する。

(2) データ利活用プロセスの適用条件

ビルサービス提供者は、スマートビルサービスの提供が、利用者目線のきめ細やかなビル設備管理や個々の利用者に応じたサービス創出の推進に貢献すること、および本人の権利を侵害せず不利益を与えないことを担保するため、ビルサービス提供に関わるデータの利活用に際して、以下のプロセスを適用する。

① データ利活用プロセス

ビルサービス提供者は、データ利用の際、「図 4-1. データ利活用プロセスの全体像」に従って運用する。

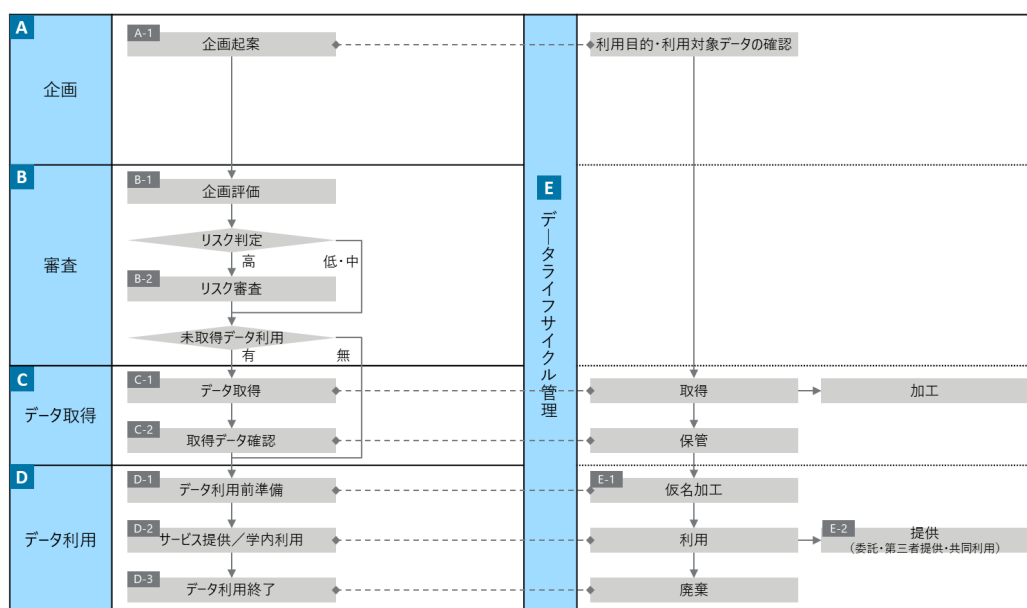


図 4-1. データ利活用プロセスの全体像

(i) スマートビルサービス企画

- ・ スマートビルサービス提供に関する企画の起案
- ・ 企画における法令・倫理・セキュリティリスクに対するリスクアセスメントチェックシートを用いた自己評価
- ・ 新規取得が必要なデータに関する取得計画の立案

(ii) 企画審査

- ・ スマートビルサービス企画書およびリスクアセスメントチェックシートの記載内容に基づく、法令・倫理・セキュリティリスクおよび取扱いデータに関するリスク判定
- ・ リスクに応じたフィードバックおよび適切な形式でのリスク審査

(必要に応じて外部有識者等のリソースを活用)

(iii) データ取得

- a. ビルデータ
 - ・ データ取得に際して、利用目的の通知または公表
- b. パーソナルデータ
 - ・ データ取得の新規取得（第三者提供は受けない）
 - ・ 本人よりデータを直接取得する場合における利用目的の通知または公表、同意取得
- c. 両データ共通
 - ・ データ取得後、承認済みの「データ利用計画・申請書」に則り、取得したデータの仕様・構造・形式の整理およびデータカタログ登録用の申請書作成

(iv) データ利用

- ・ データの提供
- ・ データ利用状況・結果の報告
- ・ データ利用結果の共有
- ・ 仮名加工の要否検討および必要に応じた実施
- ・ 第三者への提供の要否検討および必要に応じた実施
- ・ 利用済みデータの廃棄要否検討および必要に応じた実施

② 適用条件

本手順書においては、スマートビルサービスの新規企画およびサービス提供における手順を対象としているため、すべての企画が適用対象となる。

ビルサービス提供元は、以下いずれかに所属する。

- ・ 立命館大学ビルサービス提供組織
 - 立命館大学内（ビルサービス責任者・ビルサービス提供者）
 - 立命館大学による外部委託先
- ・ 学外組織とのデータの共同利用
- ・ 学外組織によるデータの利用

なお、企画変更時の手順については、「9(1)企画変更手順」を参照されたい。

5. スマートビルサービス提供に係る企画

(1) 企画起案

ビルサービス提供者は、スマートビルサービス提供開始にあたり、当該サービスが利用者本人の権利を侵害せず不利益を与えないことや、企画および利用予定データに係るリスクを整理・評価するため、「図 5-1. A-1（立命大学）：企画／企画起案」「図 5-2. A-1（外部事業者）：企画／企画起案」のフローに沿って企画起案およびビルサービス提供者自身による自己評価（リスクアセスメント）を行う。

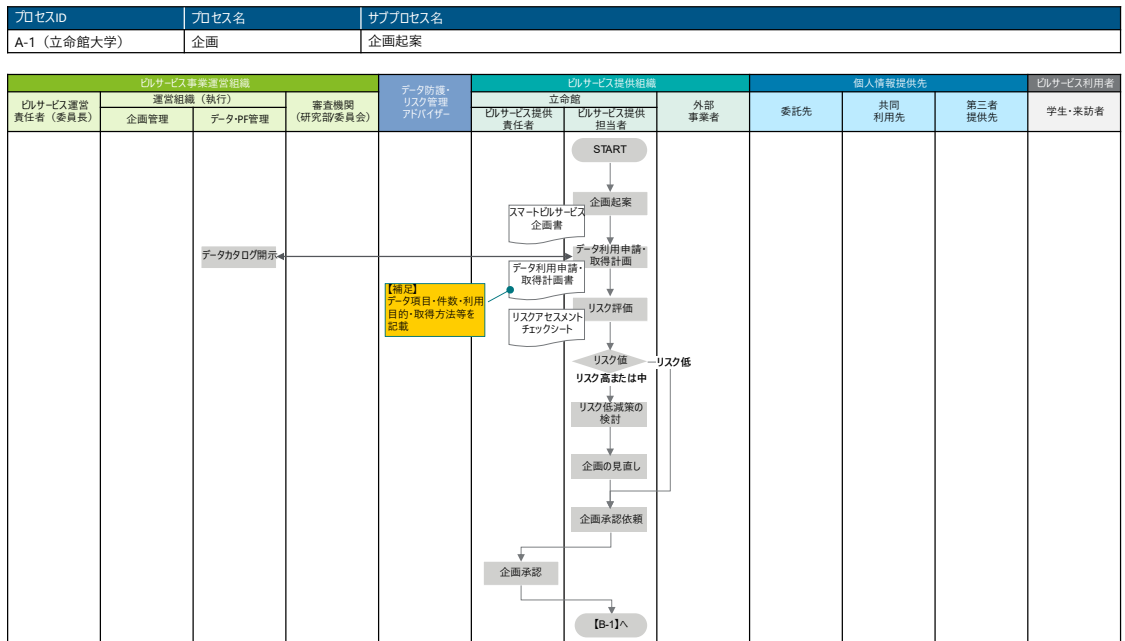


図 5-1. A-1 (立命大学) : 企画／企画起案

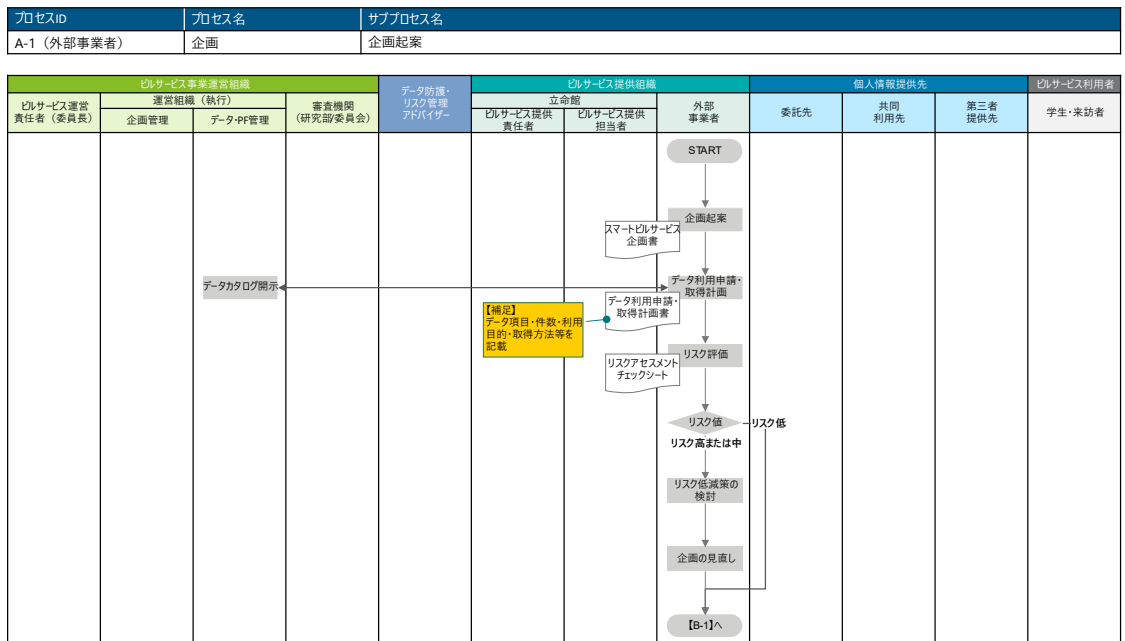


図 5-2. A-1 (外部事業者) : 企画／企画起案

① 企画起案

ビルサービス提供者は、スマートビルサービス提供開始にあたり様式『スマートビルサービス企画書』を用いて、利用目的や分析に必要なビルデータの種類・項目、利用方法等の情報を記載し、企画起案を行う。

『スマートビルサービス企画書』に記載する情報は、「表 5-1. スマートビルサービス企画書記載事項」とする。

なお、スマートビルサービス提供に関する上程書等に「表 5-1. スマートビルサービス企画書記載事項」の情報を含む場合、当該文書を添付することで『スマートビルサービス企画書』を代替できるものとする。

表 5-1. スマートビルサービス企画書記載事項

No.	項目	記載内容
1	企画名称	企画内容を一言で表したもの（簡潔かつ内容が想像できる記載に）
2	企画の背景・問題	企画検討に至った背景や解決したい問題とその中で重要となる原因（直接的に対処すべき問題）を記載。 3 の目的・目標を裏付けるため、内部環境・外部環境（規制・潮流等）を踏まえて企画内容の必要性を支持する情報として記載。 研究で新たな発見を目指している場合等直接的な問題が紐づきにくい場合であっても、当企画で取り組む課題が適切であることや企画実行のモチベーションを説明する内容となっていること。
3	当企画の目的・目標	当企画におけるゴール。企画実施後に目指すべき姿があればその内容も記載。 可能ならば定量的な数値目標を入れる。
4	データ利活用企画内容詳細	企画実施内容の詳細。 企画における実施内容と、具体的にどこからどのようなデータを取ってどこでどのように利用するか、それによってどのような価値を創出するのかについて記載する。 営業秘密に係るような、データ分析における詳細な手法等についての記載は不要だが、実施予定の作業概要（データがどのように使われるか）について分かるようにする。
5	必要データと利用方法	4 の内容から考えられる、必要なデータとその利用方法（利用範囲）を表形式で記載。 必要データを特定するために立命館データプラットフォームのデータカタログを確認することができる。
6	スケジュール	データ利活用に関するスケジュール（プロジェクト・スケジュール）。
7	リビングラボ	リビングラボを利用する場合は、使用期間および使用予定人数（常駐予定者人数）について記載。
8	期待効果	取り組み（プロジェクト）による期待効果。可能なら定量的に記載。

② データ利用申請・取得計画書

ビルサービス提供者は、立命館データプラットフォームに利活用対象となるデータが既に有る場合は、当該データの利用許諾を得ることで利用可能である。一方で、立命館データプラットフォームに利活用対象となるデータが無い場合は、新たにデータ取得する必要がある。

運営組織（執行）へデータカタログの開示を依頼し、利活用予定データの有無を確認し、「表 5-2. データ利用申請書・取得計画書記載事項」に則り『データ利用申請・取得計画書』を作成する。

表 5-2. データ利用申請書・取得計画書記載事項

No.	項目	記載内容
1	データ利用対象	データ利用対象の情報を記載する。
2	利用目的	データの利用目的を記載する。
3	利用期間	データの利用開始日および終了日を記載する。
4	仮名加工の要否	立命館データプラットフォーム上の仮名化されたデータを利用するか否か、あるいは研究利用のため、仮名加工を施して学内に限定しデータを利用するか否かを記載する。

No.	項目	記載内容
		る。 なお、仮名化されたデータを利用することで個人を識別することができなくなるため、以下の個人情報保護法への対応が不要となる。 ・ 利用目的変更について本人への通知が不要 ・ 学外への漏えい等のインシデント発生時に、監督機関および本人への報告が不要 ・ 保有個人データに関する事項の公表や、保有個人データの開示・訂正等・利用停止等への対応が不要
5	データ項目	本企画に必要なデータ項目を記載する。
未取得データを利活用する場合		
6	データの取得方法	データ項目ごとに取得方法を記載する
7	要配慮個人情報の有無／要配慮個人情報に該当する項目	要配慮個人情報に該当するか否かを記載する。 要配慮個人情報とは次のいずれかに該当する事項を指す。 ・ 思想、信条および宗教に関する事項 ・ 人種、民族、門地、本籍（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項 ・ 勤労者の団結権、団体交渉およびその他団体行動の行為に関する事項 ・ 集団示威行為への参加、請願権の行使およびその他の政治的権利行使に関する事項 ・ 医療上の個人情報に関する事項 上記以外の法律、条例、業界ごとの個人情報保護に関するガイドライン等で取得を禁じる旨の定めがある事項
8	データ件数	想定されるデータ取得件数を記載する。
9	第三者への提供有無／提供データにおける個人情報の有無／提供先／第三者への提供理由	新たに取得したデータを第三者へ提供する場合（業務委託または共同利用）は、提供先、第三者への提供理由および提供データに個人情報が含まれるか否かを記載する。

(i) 利用目的の確認

利用データに個人情報が含まれる場合、当該個人情報の利用目的を本人に通知または公表せずに利用すると法令違反により罰則を受ける可能性がある。

なお、カメラ等からの画像情報の取得等、ビルデータの取得方法によっては個人情報を利用していると受け取られることもあり得るため、個人情報に限らず利用目的の通知および公表を実施する必要がある。

利用目的の通知および公表方法等に関しては、後述の「データ取得」のプロセスに準じて対応すること。

③ リスク評価・リスク低減策の検討

利用データについて、法令・倫理的・セキュリティの観点から適切に利活用されないと、法令違反による罰則や社会的バッシング等、本法人として不利益を被る可能性がある。例えば、大阪駅一帯にある商業ビル・公共空間において、監視カメラから取得する画像データと顔識別技術を基に人の流れを解析する実証が計画されていたが、JR大阪駅と駅ビルの利用者は通勤経路等を変えない限り実証実験への参加を拒否できず、プライバシー侵害に関する懸念が高まったため、延期になった事例がある。このようなリスクを低減するため、事前に企画内容および利用予定データに関して法令・倫理的・セキュリティリスク評価を実施し、識別されたリスクを低減する必要がある。

本リスク評価は、データの利用およびビルサービスの提供を阻むものではなく、事前にリスクを識別し、識別したリスクに対して適切なリスク低減措置を行うことで安全にデータ

利用およびスマートビルサービスの提供をすることを目的としている。

ビルサービス提供者は、様式『リスクアセスメントチェックシート』を用いて、『スマートビルサービス企画書』および『データ利用申請・取得計画書』の記載内容に基づき、以下の観点でリスクを評価する。

【法令リスク】

- ・ 現行の法令に違反するリスク

【倫理的リスク】

- ・ 社会において依拠すべき規範に反するリスク
- ・ 社会が受け入れずバッシングを受けるリスク

【セキュリティリスク】

- ・ 個人情報が漏えいするリスク

ビルサービス提供者は、自動判定されたリスク評価結果に基づき、以下のプロセスにおいてリスク低減策を検討する。

(i) リスク評価結果が「低」の場合

想定されるリスクは限定的もしくはその影響は小さいと考えられる、または後続プロセスでリスク低減を行うことが想定される。したがって、リスク低減策の検討は省略可能とする。

ビルサービス提供者は、「6(1)①企画承認依頼」に進む。

(ii) リスク評価結果が「高」または「中」の場合

想定されるリスクの影響が大きいと考えられるため、リスク低減策を検討する必要がある。

したがって、ビルサービス提供者は、『リスクアセスメントチェックシート』の回答についてリスク「高」または「中」と判定された各リスクに対して、「リスク低減策の例」を参考にリスク低減策を検討するとともに、必要に応じて企画を見直す。

ビルサービス提供者は、検討結果を『リスクアセスメントチェックシート』に記入し、「6(1)①企画承認依頼」に進む。

④ 企画承認依頼・企画承認

当法人がスマートビルサービスを提供する場合は、当該サービスを提供する学部または部門において、ビルサービス提供担当者は、様式『リスクアセスメントチェックシート』を用いて、『スマートビルサービス企画書』および『データ利用申請・取得計画書』をビルサービス提供責任者へ提出し、企画承認を依頼する。

ビルサービス提供責任者は、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を閲覧し、利用者本人の権利等を侵害せず不利益を与えるリスクが存在しないこと、また、適切なリスク低減策が検討されていることを確認し、企画承認または否認を行う。

6. 企画および取扱いデータの審査

(1) 企画評価

ビルサービス提供者は、「図 6-1. B-1：審査／企画評価」のフローに沿って、スマートビルサービスの企画、当該サービス提供にあたってのリスク、および利用予定データ等をビルサービス事業運営組織に対して説明し、承認を得る。

[illegible]

図 6-1. B-1 : 審査／企画評価

① 企画承認依頼

ビルサービス提供者は、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を運営組織（執行）へ提出し、企画承認を依頼する。

② 企画案受付・ヒアリング

運営組織（執行）は、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』における記述に基づき内容を確認するとともに、必要に応じてビルサービス提供者へヒアリングし、以下の情報を収集する。

【ヒアリング事項（例）】

- ・ スマートビルサービスの詳細
- ・ スマートビルサービスにて取扱うビルデータ（特に、映像等の個人データに該当する可能性があるもの）および目的
- ・ スマートビルサービスにて取扱う機微情報（項目単位）および目的
- ・ リスク低減策の実現方法
- ・ スマートビルサービス提供に係るスケジュール 等

③ 企画案評価

運営組織（執行）は、ヒアリング結果に基づき『データ利活用企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を更新し、適切なリスク低減策が検討されていることを以下の観点で評価する。

【リスク低減策の適切性を判断する観点】

- ・ リスク低減策（例：ビルサービス利用者に丁寧に説明する、相談窓口を記載する等）により、リスクが許容される範囲になること
- ・ データ利用開始までに対策が完了すること
- ・ 対策コストが過剰に掛からないこと 等

(i) リスク評価結果が「低」の場合／リスク低減策によってリスクが「低」まで低減されていると判断した場合

ビルサービス運営責任者に企画の承認を依頼する。したがって、「0リスク審査」は省略可能とする。運営組織（執行）は、「6(1)④エラー! 参照元が見つかりません。エラー

ー! 参照元が見つかりません。」に進む。

- (ii) リスク評価結果が「高」または「中」の場合／リスク低減策が妥当でなく、リスクが「高」または「中」のままであると判断した場合

想定される法令・倫理的・セキュリティリスクにより、利用者本人の権利等を侵害し不利益を与えるとともに、本法人の評判を著しく損なう可能性があるため、検討したリスク低減策が適切であるか本法人の審査機関によるリスク審査を受ける。

ビルサービス提供者および運営組織（執行）は、「6(2)リスク審査」に進む。

		データ		
		リスク高	リスク中	リスク低
(例)		個人情報	未取得ビルデータ	格納済みビルデータ
企画	リスク高	リスク審査委員会による審査の実施および承認 委員会	リスク審査委員会による審査の実施および承認 メール閲覧	リスク審査委員会による審査の実施および承認 メール閲覧
	リスク中	リスク審査委員会による審査の実施および承認 メール閲覧	リスク審査委員会による承認	リスク審査委員会による承認
	リスク低	リスク審査委員会による審査の実施および承認 メール閲覧	リスク審査委員会による承認	ビルサービス運営責任者による承認

図 6-2. リスク評価結果の考え方

表 6-1. リスク評価結果に基づき実施すべきプロセス

リスク判定	リスク低減策の要否	企画段階において必要なプロセス	
高	必要 (審査機関に相談)	4(1) 4(2) 4(3)	ビルサービス利用者や社会に対して影響が大きいと考えられるため、「4(2)リスク審査」に進み、リスク審査委員会においてリスク許容可否について確認する。 審査機関の審査結果に基づき、運営組織（執行）からリスクが許容されないと判断された場合は、ビルサービス提供者にてリスク低減策あるいは企画内容・取扱いデータ等の見直しを実施し、運営組織（執行）へ再審査を依頼する。
中	必要 (審査機関に相談)	4(1) 4(2) 4(3)	ビルサービス利用者や社会に対して影響が大きいと考えられるため、「4(2)リスク審査」に進み、メール閲覧にてリスク許容可否について確認する。 審査機関の審査結果に基づき、運営組織（執行）からリスクが許容されないと判断された場合は、ビルサービス提供者にてリスク低減策あるいは企画内容・取扱いデータ等の見直しを実施し、運営組織（執行）へ再審査を依頼する。

リスク判定	リスク低減策の要否	企画段階において必要なプロセス	
低	必要 (ビルサービス提供者にて検討)	4(1)	ビルサービス運営責任者による企画承認の後、利活用予定のデータ種別に応じて「7 データ取得」あるいは「8 データ利用」に進む。

④ 企画案報告

運営組織（執行）は、ビルサービス運営責任者に『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を共有する。

⑤ 企画承認

ビルサービス運営責任者は、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を閲覧し、利用者本人の権利等を侵害せず不利益を与えるリスクが存在しないこと、また、適切なリスク低減策が検討されていることを以下の観点で確認し、企画承認または否認を行う。

【リスク低減策の適切性を判断する観点】

- ・ リスク低減策（例：カメラ等から画像データを取得する際は、個人を特定できないよう加工したうえでデータを利用し、その旨と利用目的を予め通知・公表する、相談窓口を記載する等）により、リスク許容される範囲になること
- ・ データ利用開始までに対策が完了すること
- ・ 対策コストが過度に掛からないこと 等

⑥ 企画案に対するフィードバック

データの利用目的および提供サービスに対する効果予測、スケジュール、コスト面等に課題を識別した際は「6(1)⑥エラー! 参照元が見つかりません。」において、運営組織（執行）からサービス提供者に対して助言する。

ビルサービス提供者は、未取得データの利用有無を確認し、未取得データを利用する場合は「7 データ取得」へ、未取得データを利用しない場合は「8 データ利用」へ進む。

(2) リスク審査

「6(1)③企画案評価」の結果がリスク「高」または「中」の場合は、本人の権利等を侵害し不利益を与えるとともに、本法人の評判を著しく損なう可能性があるため、「

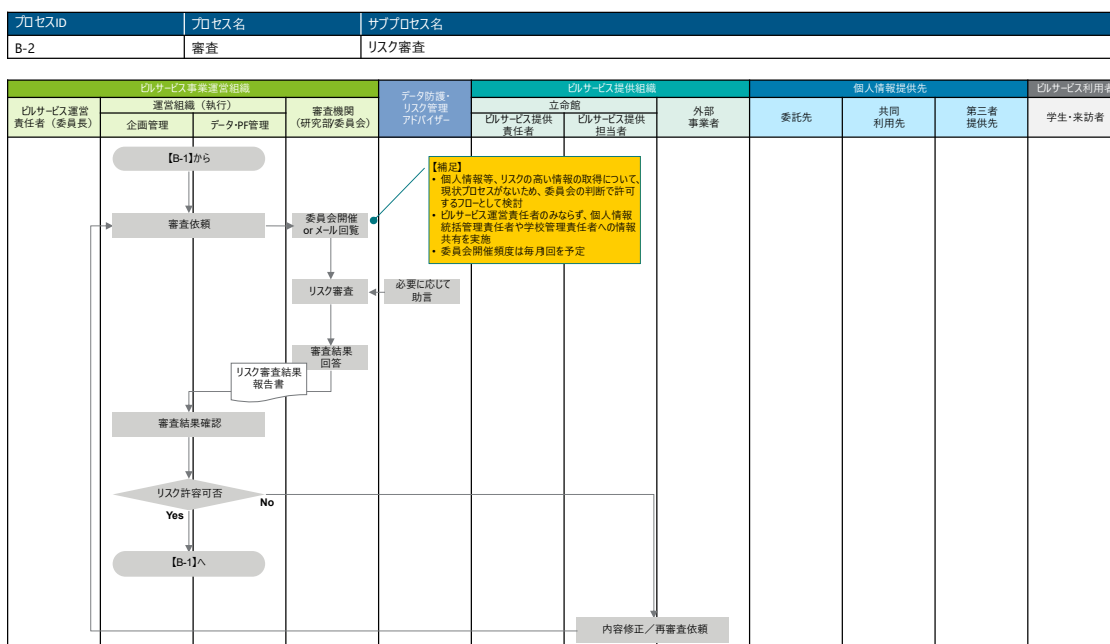


図 6-3. B-2 : 審査／リスク審査エラー! 参照元が見つかりません。」のフローに沿って企画評価を行う。

なお、リスク「低」の場合は、当該プロセスは省略可能とする。

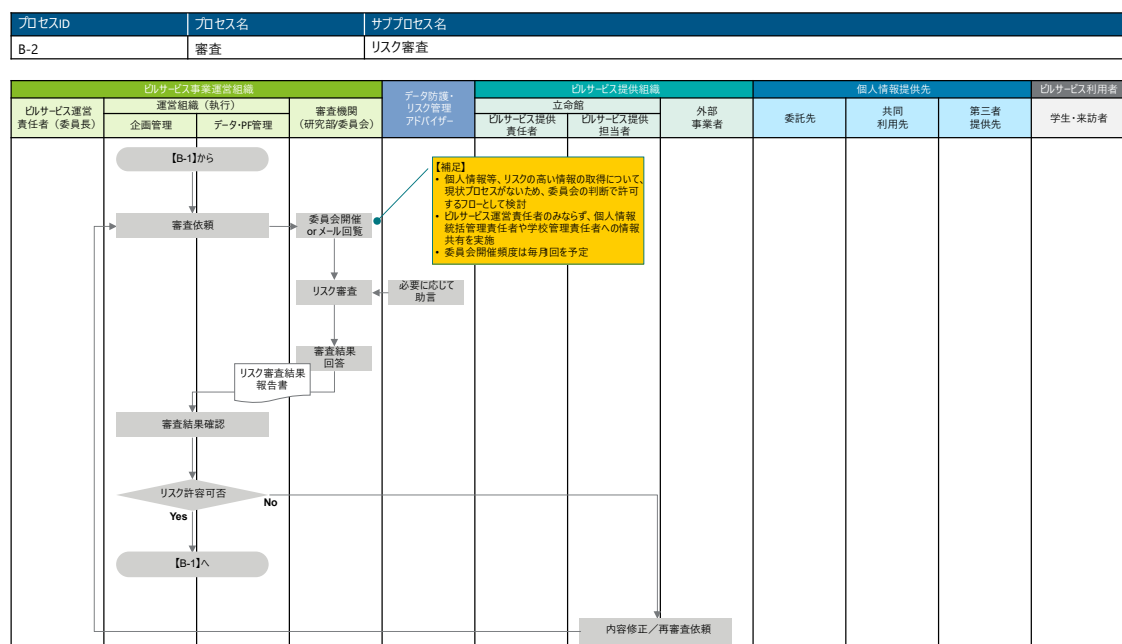


図 6-3. B-2 : 審査／リスク審査

① 審査依頼

運営組織（執行）は、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』の内容に基づき、法令・倫理・セキュリティリスクに応じて法人内の審査機関にリスク審査を依頼する。

法令・倫理・セキュリティリスクが多岐に渡る、またはリスクが非常に高いと判断された場合、データ防護・リスク管理アドバイザーとして外部の有識者によるリスク審査および助言を依頼する。

なお、リスク審査の開催方法は、リスク値に応じて以下の通り実施する。

(i) リスク「高」の場合

リスク審査委員会を開催する。

運営組織（執行）はデータ防護・リスク管理アドバイザーに対して、リスク審査委員会の開催を通知し、開催日程の調整を行う。

(ii) リスク「中」の場合

リスク審査をメール回覧により行う。

運営組織（執行）はデータ防護・リスク管理アドバイザーに対して、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を送付する。

		データ		
		リスク高	リスク中	リスク低
(例)		個人情報	未取得ビルデータ	格納済みビルデータ
企画	リスク高	リスクが顕在化したときに事業に与える影響度が高いと考えられる場合 リスク審査委員会による審査の実施および承認 委員会	リスク審査委員会による審査の実施および承認 メール回答	リスク審査委員会による審査の実施および承認 メール回答
	リスク中	リスクが顕在化したときに事業に与える影響が一定程度あると考えられる場合 リスク審査委員会による審査の実施および承認 メール回答	リスク審査委員会による承認	リスク審査委員会による承認
	リスク低	データの取得や第三者提供に際して、各手順が明確に定義され、それらを遵守することが前提となる場合 リスク審査委員会による審査の実施および承認 メール回答	リスク審査委員会による承認	ビルサービス運営責任者による承認

図 6-4. リスク評価結果に基づくリスク審査方法

② リスク審査・審査結果回答

審査機関およびデータ防護・リスク管理アドバイザーは、『スマートビルサービス企画書』、『データ利用申請・取得計画書』および『リスクアセスメントチェックシート』を確認し、想定されるリスクの許容可否や追加のリスク軽減措置の要否、データ利活用の中止勧告要否等を検討する。

審査機関およびデータ防護・リスク管理アドバイザーは、審査結果を『リスク審査結果報告書』に記入し、運営組織（執行）へ回付する。

③ 審査結果確認

運営組織（執行）は『リスク審査結果報告書』に記載の審査結果を確認し、リスク許容可否により以下のプロセスを実施する。

(i) リスクが許容できると判断した場合

運営組織（執行）は、「6(1)④企画案報告」に進む。

(ii) リスクが許容できないと判断した場合

運営組織（執行）は、ビルサービス提供者へ『リスク審査結果報告書』を回付し、企画内容の修正を依頼する。

ビルサービス提供者は企画内容を修正したうえで、運営組織（執行）へ再審査を依頼し、運営組織（執行）は「6(2)①審査依頼」にて再度審査機関へリスク審査を依頼する。

7. データ取得

(1) データ取得

スマートビルサービス提供に際してデータを取得する場合、利用目的の通知または公表を行う必要がある。なお、利活用するデータに要配慮個人情報が含まれる場合、または個人情報を第三者に提供する場合は本人の同意を取得する必要がある。

ビルサービス提供者は、データの取得に際し適切な対応を行うため、「図 7-1. C-1：データ取得／データ取得」のフローに沿ってデータ取得を行う。

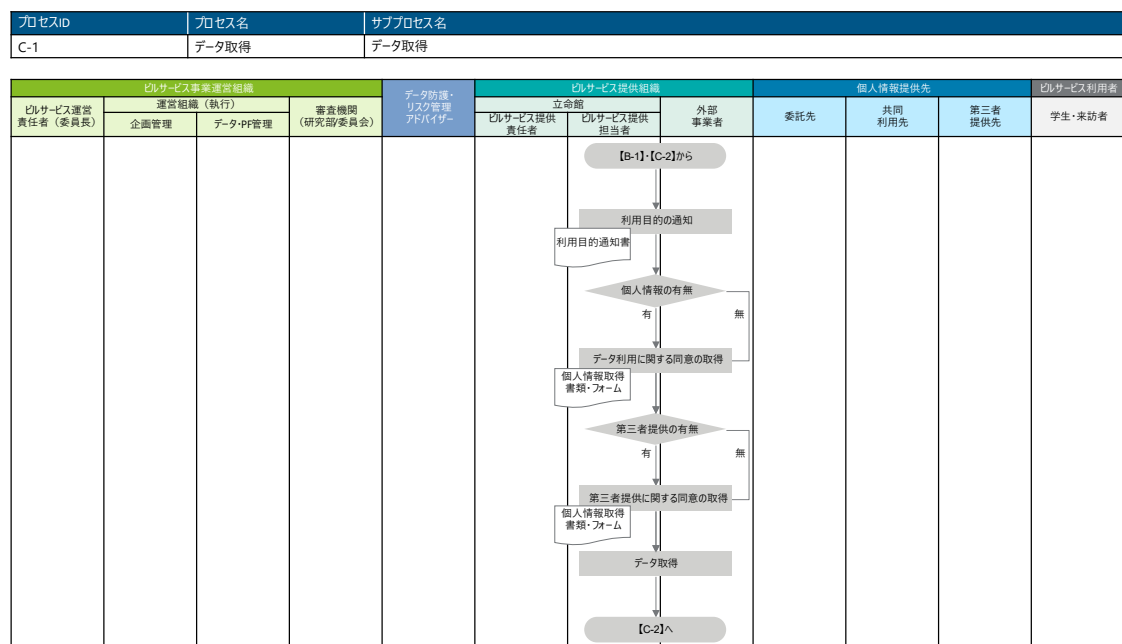


図 7-1. C-1：データ取得／データ取得

① 利用目的等の通知

ビルサービス提供者は、スマートビルサービスの提供に際して『利用目的通知書（ひな型）』を用いて、ビル利用者およびサービス利用者本人にデータの利用目的等を通知する。データの利用目的等の記載にあたっては、本人に利用目的等の情報を明確かつ分かり易い表現で記載することが求められるため、箇条書き等を用いて要点を記載することや、曖昧な表現を避けて端的に記載する。

なお、利用目的等の通知は、以下に例示する方法等により行う。

(i) ウェブサイトやスマートフォンのアプリケーション等

ビルサービス提供者は、スマートビルサービスを提供するウェブサイトやスマートフォンのアプリケーション上で利用目的を明記する、もしくはトップページやユーザー登録画面等から1クリックでプライバシーポリシーが掲載された画面に遷移・表示できるようにすることで、データの利用目的等を通知する。

(ii) 書面（対面・電子メール）

ビルサービス提供者は、スマートビルサービスを紹介する書面等を用いて、本人にデータの利用目的等を通知する。利用目的等の記載にあたっては、本人に利用目的等の情報を明確かつ分かり易い表現で示すことが求められるため、利用目的等を通知するために必要十分なスペースを用意して当該情報を記載するものとし、記載スペースに制限がある場合は極端に小さな文字で記載する等の対応はせず、書面にQRコードを掲載することでスマートフォン等から利用目的等が掲載されたウェブサイトを開覧できるようにする。

(iii) ポスター等

ビルサービス提供者は、例えばカメラ等を用いて顔の画像を取得する場合は、スマートビルサービスを利用しない対象も含めて広くデータ取得状況と利用目的を通知・公表する必要があるため、ポスター掲示等にて利用目的等を通知し、ビル利用者が確認できるようにする。

② データ利用に関する同意の取得

ビルサービス提供者は、ビルサービス利用者の個人情報を利活用する、または当該個人情報を第三者に提供する場合、ビルサービス利用者本人の積極的な意思表示による同意を取得する必要がある。積極的な意思表示による同意とは「はい」と「いいえ」の選択肢があり、かつ本人の意思で「はい」を選択した証拠が残る方法で同意を取得する方法を指す。

同意の取得方法について、以下に想定ケースを例示する。

(i) ウェブサイトやスマートフォンのアプリケーション等

ビルサービス提供者は、スマートビルサービスを提供するウェブサイトやスマートフォンのアプリケーション上で本人の「同意する」意思を確実に確認できるようにデータの登録・変更画面に同意を示すチェックボックスを用意し、本人がチェックすることにより同意を取得する。

(ii) 書面（対面）

ビルサービス提供者は、本人の「同意する」意思を確実に確認できるように書面に同意を示すチェックボックス、もしくは署名欄を設けることにより本人の同意を取得する。

なお、第三者提供に係る同意を取得する際は、ビルサービス利用者に以下の内容を知ること。

- ・ 第三者提供における目的
- ・ 第三者提供先
- ・ 第三者提供する個人情報の種別
- ・ 第三者提供する個人データの項目 等

③ データ取得

ビルサービス提供者は、ビルデータ、および本人の同意に基づき個人情報等を取得する。

(i) ビルデータ

ビルサービス提供者は、センサーやカメラ等を用いてビルデータを取得する。ビルデータの取得にあたっては、センサーやカメラ等の機器を複数設置する場合や、機器の不具合によりデータが取得できない場合等の取扱いについて、どのように取扱うがあらかじめ取り決める。

- a. 複数の機器を用いてデータを取得する場合、同一性が一定割合以上認められなければリリースしない等の要件を設ける
- b. 機器の不具合によりデータが欠落している場合、その間のデータを破棄する、または平均値で補足する等のルールを定める
- c. 機器自体の不具合や機器の設置ミス、機器の性能不足により、データの正確性や完全性が担保できていないケースがあるため、機器自体の不具合や設置ミスが原因で正確性が担保できないことが想定されるため、定期的に機器の校正をする
- d. 当初同メーカーの機器を設置していても、機器を増やしたり、交換が発生したりする場合に異なるメーカーの機器を設置することが考えられるため、交換後の機器にて取得するデータ形式や取得頻度が標準に適合しているか確認する

(ii) 個人情報

ビルサービス提供者は、スマートビルサービスを提供するウェブサイトやスマートフォンのアプリケーションや書面を用いて、本人の同意を取得したうえで個人情報等を取得する。

なお、センサーやカメラ等を用いて個人を識別する場合は、ビルデータの取扱方法に加えて、以下について考慮する。

- a. カメラで撮影したデータで個人の移動情報を分析する場合、異なる場所に設置している2台のカメラにおいて、個人の同一性が認められなければ正確な移動情報が把握できないため、同一性が一定割合以上認められなければリリースしない等の要件を設ける
- b. データの「一貫性」について、提供するスマートビルサービスによっては日付が変わっても対象者を追跡し個人を特定する必要があると考えられるため、同一性が一定割合以上認められなければリリースしない等の要件を設ける

(iii) 第三者からの取得による、その他データ

ビルサービス提供者は、立命館大学に入居する事業者、茨木市および近隣の商業施設等の第三者より、イベント情報や災害情報等の非パーソナルデータの提供を受ける場合は、データ授受に係る契約を締結したうえでデータを取得する。

ビルサービス提供者は、「7(2)取得データの確認」に進む。

(2) 取得データの確認

ビルサービス提供者は、「**図 7-2. C-2：データ取得／取得データ確認**」のフローに沿って、取得データの適切性を質・量の観点から確認する。

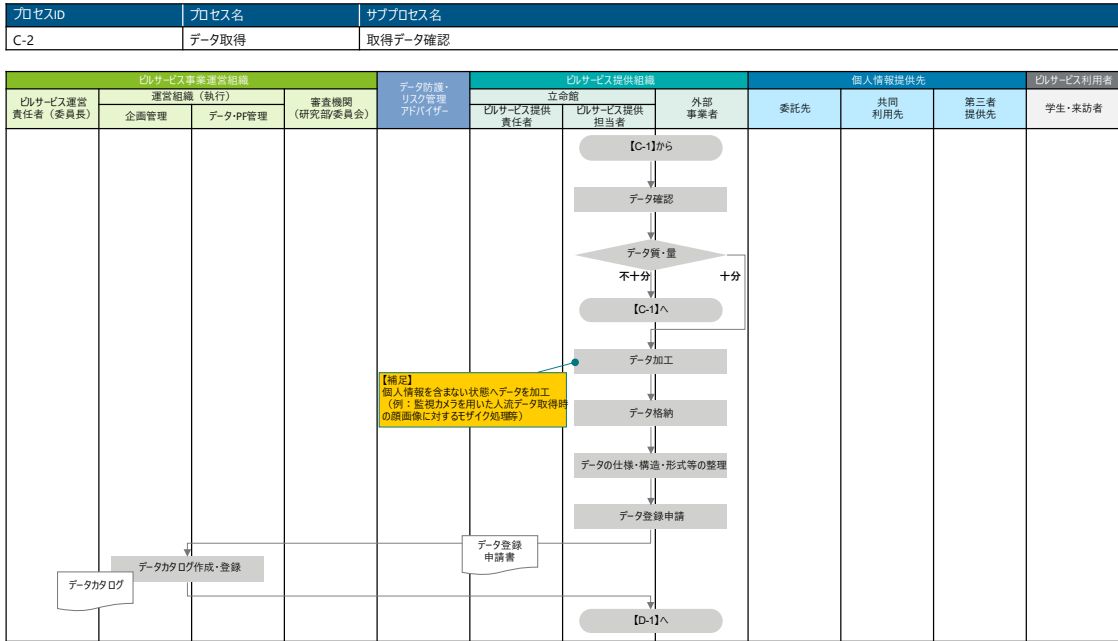


図 7-2. C-2 : データ取得／取得データ確認

① データ確認

ビルサービス提供者は、データ利用にあたり、データ更新・共有のタイミングを事前に定め、不備を検出して修正する仕組みを整備する。データ品質を継続的に担保し、立命館データ連携プラットフォーム上で安定してスマートビルサービスを提供するために、データ品質、サービス品質および管理プロセスの評価を定期的実施し、品質の改善を図る。

データの品質の確認における観点を「表 7-1. データの品質管理」に示す。

表 7-1. データの品質管理

分類	評価の観点	品質不備の例
正確性	・書式が正しいか ・誤字脱字等はないか ・意味的な誤りはないか ・データに誤りはないか	・「同上」、「〃」等の記述がある ・日付や数字が記述されるべき欄に「不明」等数字以外の文字列が記述されている ・住所が記述されるべき欄に電話番号が記述されている ・フリガナ欄にカタカナとひらがなが混在している
完全性	・用途に応じて必要な項目が網羅されているか ・必須項目に空欄が含まれていないか	・重要なデータ項目が定義されていない ・データが取得できないという理由で必須項目に空欄がある
整合性・一貫性	・データセット内でデータに矛盾はないか ・データセット間でデータに矛盾はないか	・住所コードと住所が一致しない ・外部参照に間違いがある ・各項目の個別の値を集計した合計値と、元々データに含まれていた合計値が一致しない
信憑性	・データの出所が明示されているか ・データの更新日が明示されているか ・改ざん防止策が施してあるか	・特定のデータ作成者やデータ計測機器によるデータの誤りが複数発見された ・データがいつ作成されたものか分からない ・データの出典や収集方法が不明
最新性	・公開データの更新サイクルは元データの更新サイクルに対して適切か ・データは収集時から十分に短い期間で公開されているか ・ファイル等で提供される場合は、最終更新日時及び最新版の所在が明記されている等、更新版の有無が確認できるようになっているか	・データが更新されていない（データが古くなった場合は、データの公開を終了することを検討する必要がある） ・各年で取りまとめているデータの公開に半年近くかかる ・ダウンロードしたファイルの更新版の有無が確認できない ・最新のデータにおいて住所だけ古いまま掲載されている（例：東京市）
アクセス性	・ファイルで提供している場合、データの使用权を持つ全ての人が利用できるようになっているか ・ソフトウェアを通して提供している場合、そのソフトウェアは ISO/IEC 40500 に準拠しているか。 ・使用している文字セット（常用漢字等）は正しいか。	・特殊なファイル形式で公開されている ・常用漢字が定められているにも関わらず、それ以外の漢字がフリガナを伴わず使用されている ・環境依存の文字が使用されている
標準適合性	・データの書式は標準に準拠しているか ・使用している文字セットは正しいか ・選択項目に、指定された選択肢以外のデータが入っていないか	・年月日が西暦ではなく和暦で表記されている（例：R2.4.1） ・環境依存の文字やユーザー定義文字が使用されている ・都道府県名が略称で表記されている（例：「東京都」と表記すべきところを「東京」と表記）
機密性	・データにアクセスできるのは、アクセスを許可された者に限定されているか	・データを提供しているソフトウェアに脆弱性がある ・データ管理ツールにおいて共有範囲

分類	評価の観点	品質不備の例
	・利用者を制限する場合、暗号化やハッキング対策等が行われているか	が誤って設定されている
効率性	・データの内容に重複等がないか ・データは効率的に処理できるようになっているか ・コードを効果的に使用しているか ・データに一貫性はあるか	・データに全角と半角が混在する等、データとデータを結び付ける際に正規化が必要となる ・住所とビル名が別データ項目になっていない等、データ活用するために分離処理が必要になる ・表計算ソフトで作成されたデータに余分な罫線やスペースが入っている ・他のデータと結合しやすくするためのIDやコードが入っていない
精度	・データの精度は適正に設定されているか ・データの精度がそろっているか ・データの精度が示されているか	・各データが、小数点以下切捨て、小数点以下2桁まで記録等、精度にばらつきがあり、単純に加算できない ・許容誤差範囲が異なるデータが混在している ・正確な位置を特定する必要のあるデータにおいて、緯度経度の値が粗すぎる
来歴	・外部データが明確になっているか ・データの変更の際に、変更者、変更日等を記録しているか	・外部データの出所が明確になっていない ・いつ、誰が変更したかが分からない ・データの変更箇所や変更方法（例：機械処理なのか人手なのか）が不明
理解性	・データ全体及びその各項目が意味するものを利用者が理解できるようになっているか ・データ全体や必要に応じてその各項目にメタデータが提供されているか	・データの説明がなく、データが意味するものを正確に理解できない ・住所が本店所在地なのか、事業所所在地なのか判断できない ・記述されているコードや略称の意味する内容が不明
可用性	・必要な時にいつでもデータにアクセスできるようになっているか ・データを公開するシステムは常時稼働しているか	・頻繁にシステムが停止する ・データ公開システムにアクセス可能な時間帯が限定されている
移植性	・標準的なフォーマットで出力できないソフトウェアに依存していないか ・データを管理するシステムから標準的な形式によりデータをエクスポートすることができるか	・ソフトウェア固有のフォーマットでしか出力できない
回復性	・データのバックアップが保存されているか ・システム障害が発生した場合であっても、継続してデータを提供するバックアップシステムが存在するか	・バックアップされないディスク上のみデータが保存されている ・特定のサーバーのみからしかデータが取得できない

(i) データの質・量が十分である場合

ビルサービス提供者は、「7(2)②データ加工」に進む。

(ii) データの質・量が不十分である場合

ビルサービス提供者は、再度データを取得するため、「7(1)データ取得」を再度実施する。

② データ加工

ビルサービス提供者は、取得したデータに個人情報者が含まれており、かつビルサービス利用者本人から利用目的に対する同意を取得していない場合、監視カメラを用いた人流データ取得に際してモザイク処理を施す等、データプラットフォームへの格納に際して個人情報を含まない状態へ加工する。

なお、ビルデータに係る個人情報の考え方を「

表 7-2. ビルデータに係る個人情報」に示す。

表 7-2. ビルデータに係る個人情報

分類	説明	個人情報	考え方
特微量データ	「特微量データ」とは、画像から個人の目、鼻、口の位置関係等の特徴を抽出し、数値化するという処理方法によって得られたデータのことをいう。 「特微量データ」は、顔認証データともいう。顔の画像そのものではなく、数値化したデータも「個人識別符号」にあたるため、「個人情報」にあたる。	該当	個人の特徴を抽出した「特微量データ」は個人情報にあたるため、第三者提供する場合には同意が必要となる。「特微量データ」の第三者提供の必要性については、慎重に検討する必要がある。
属性情報	「属性情報」とは、画像から抽出した個人の容貌を元に AI が推定した性別・年齢等をデータにしたものをいう。「属性情報」だけでは、個人を特定できないため、「個人情報」にはあたらない。 ただし、抽出元の画像と「属性情報」が容易に照合できる場合、個人を特定できるようになるため、この場合には「個人情報」にあたることになる。	非該当 ※ただし容易に照合できない場合	性別・年齢等の「属性情報」に加工した場合、本人の同意なく第三者提供や利用目的の変更を行うことができる。ただし、抽出元の画像と「属性情報」が容易に照合できる場合、個人情報に該当するため、留意が必要である。
カウントデータ	「カウントデータ」とは、人の形のみを判別して、その数を計測する処理方法により得られたデータのことをいう。人数をカウントするだけのため、特定の個人を識別することはできないデータとなる。そのため「個人情報」にはあたらない。	非該当	人数をカウントするためだけの「カウントデータ」に加工した場合、本人の同意なく第三者提供や利用目的の変更を行うことができる。
動線データ	「動線データ」とは、個人がどのように移動したかを示すデータである。どこにいたかという座標値を時系列にそって蓄積することで生成される。「動線データ」だけでは、個人を特定することはできないため、「個人情報」にはあたらない。 ただし、個人の移動経路の確	非該当 ※ただし容易に照合できない場合	個人の移動データである「動線データ」に加工した場合、本人の同意なく第三者提供や利用目的の変更を行うことができる。 ただし、「動線データ」と「特微量データ」を紐づけている場合、容易に照合して個人を特定でき個人情報に該当するため、留意が必要であ

分類	説明	個人情報	考え方
	認のために「動線データ」と「特微量データ」を紐づけている場合には、これらを容易に照合して個人を特定できるようになるため、「個人情報」にあたる。		る。
同時性データ	「同時性データ」とは、個人単体の位置・動線データだけではなく、当該データが示す場所に誰と一緒に居たか（複数人の同時性）を示すデータである。 「動線データ」だけでは「個人情報」にはあたらないが、一緒に居た他個人が特定でき、かつ当該個人を推察できる場合は「個人情報」にあたる可能性がある。	非該当 ※ただし他個人が特定できない場合	特定の本人の個人情報を活用する場合、複数人の同時性（誰と一緒に居たか）についても個人情報になり得るため、留意が必要である。
処理済みデータ	「処理済みデータ」とは、画像にモザイク処理等を施して、個人を特定できないようにする処理をしたデータのことをいう。処理済みデータも個人を特定できないため、「個人情報」にはあたりません。 ただし、人の歩き方は「個人識別符号」として「個人情報」にあたるため、顔にしかモザイク処理をしないとといった不十分な処理や、復元が可能な処理がなされていた場合は、「個人情報」にあたる可能性がある。	非該当 ※ただし容易に照合できない場合	画像にモザイク処理を施すことにより、個人を特定できないように加工した「処理済みデータ」の場合、本人の同意なく第三者提供や利用目的の変更を行うことができる。 ただし、歩き方が判別できる等、個人が特定できるような不十分な加工である場合、個人情報に該当するため、留意が必要である。

③ データ格納

ビルサービス提供者は、運営組織（執行）が指定したデータ格納先に取得したデータを格納する。

なお、取得したデータの原本は「学校法人立命館情報システムの利用および運用管理に関わる基本規程」をはじめとする規程・ガイドラインに従って適切に保管する。

④ データの仕様・構造・形式等の整理

ビルサービス提供者は、取得したデータをデータカタログとして登録・管理・公開するために、「表 7-3. 整理するデータの情報」に従って当該データの情報を整理する。

表 7-3. 整理するデータの情報

No.	項目	内容
データ概要		
1	データのタイトル	データに関するタイトル
2	データのキーワード	データカタログ上で検索するためのキーワード
3	データ概要	データに関する概要説明
4	データ作成日	データの作成日

No.	項目	内容
5	データの公開期間	立命館データプラットフォームにおけるデータの公開期間
6	データ更新可否	今後のデータの更新想定
7	データオーナー	データの所有者および第三者利用に関する承認者
8	データ問合せ先	データに関する問合せ先
データ仕様		
9	データ分類	データに関する分類
10	利用目的	データの利用目的
11	データ対象者	データの提供者（例：学生本人）
12	データ対象期間	データの取得対象期間
13	データ項目	データの項目（例：学籍番号）
14	データ構造	データの構造（例：半角数字 10 桁）
15	データ形式	データの保存・提供形式（例：CSV 形式）
16	データ件数	データの件数
17	データの取得条件	カメラやセンサーにてデータを収集した際の環境や条件ならびにデータの諸元
18	補足情報	上記以外の補足情報

⑤ データ登録申請

ビルサービス提供者は、様式『データ登録申請書』を作成し、運営組織（執行）へ提出する。『データ登録申請書』に記載する情報は、「表 7-3. 整理するデータの情報」および「表 7-4. データ登録申請書記載事項」とする。

表 7-4. データ登録申請書記載事項

No.	項目	記載内容
コンプライアンス・セキュリティ対応		
1	仮名加工の可否	立命館データプラットフォームにデータを格納する際、仮名加工を行うか否かを記載する。原則として、学生および学外の個人情報を含むデータについては仮名加工を施すこと。 なお、データを仮名加工することで、個人を識別することができなくなるため、以下の個人情報保護法への対応が不要となる。 ・ 利用目的変更について本人への通知が不要 ・ 学外への漏えい等のインシデント発生時に、監督機関および本人への報告が不要 ・ 保有個人データに関する事項の公表や、保有個人データの開示・訂正等・利用停止等への対応が不要
2	開示範囲	立命館データプラットフォームにデータを格納するにあたり、データカタログに公開する利用条件を記載する。 【利用条件の種類】 ・ 条件を設けず利用を許可する ・ 指定する条件を満たした場合に限り利用を許可する（指定する条件の詳細について記載すること） ・ 利用を許可しない
3	学外への開示可否	学外への第三者への開示・提供可否（本人同意を取得済か否か）
4	秘密保持義務	秘密保持契約等の締結有無
5	準拠法	データの提供者に紐づく、準拠すべき法令
6	注意事項	上記以外の注意事項

⑥ データカタログ登録

運営組織（執行）は、『データ登録申請書』を閲覧し、申請内容に基づきデータカタロ

グへの登録を行う。

8. データ利用

(1) データ利用前準備

運営組織（執行）およびビルサービス提供者は、データ利用前の準備に際し適切な対応を行うため、「図 8-1.D-1：データ利用／データ利用前準備」のフローに沿ってデータ利用前準備を行う。

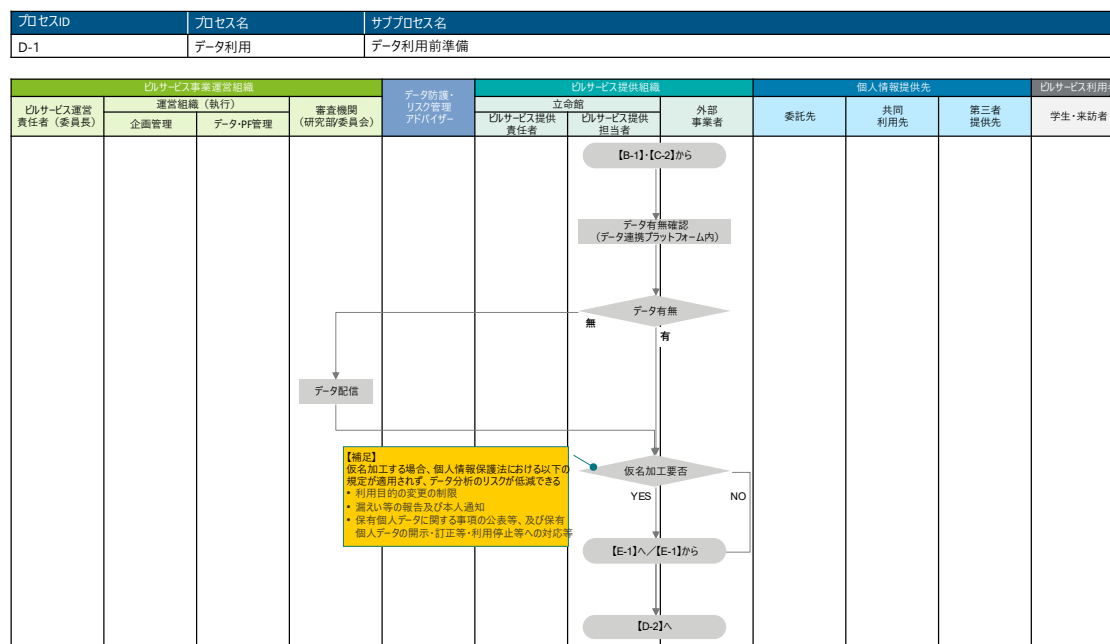


図 8-1.D-1：データ利用／データ利用前準備

① データ有無確認

スマートビルサービスの提供においてデータを活用するにあたり、当該データがプラットフォームへ格納されているかを予め確認し、データが無ければ運営組織（執行）へデータの配信を依頼する。運営組織（執行）は『データ利用計画・申請書』または『データ登録申請書』を閲覧し、申請内容に基づいて承認済みのスマートビルサービス提供に必要なデータをプラットフォームに格納する。

なお、利活用するデータに個人情報者が含まれており、かつビルサービス利用者本人から利用目的に対する同意を取得している場合であっても、情報漏えい時におけるリスク低減等を目的として仮名加工を施すことが望ましいため、仮名加工の要否を判断するプロセスを経たうえでデータ利用を開始する。

(i) 仮名加工を行う場合

ビルサービス提供者ならびに運営組織（執行）は、「8(1)②仮名加工」に進む。

(ii) 仮名加工を行わない場合

ビルサービス提供者は、「8(2)サービス提供／学内利用」に進む。

② 仮名加工

運営組織（執行）は、対象となるデータについて、以下の基準に従い、「図 8-2.E-1：データライフサイクル管理／仮名加工」のフローに沿って仮名加工を行う。

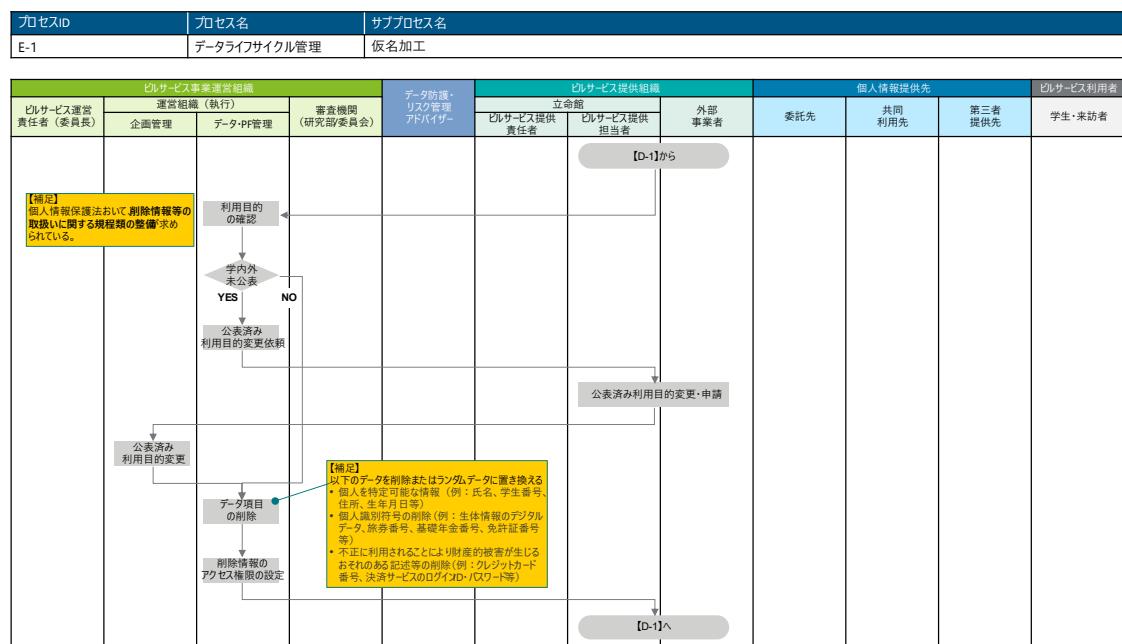


図 8-2.E-1 : データライフサイクル管理／仮名加工

(i) 特定の個人を識別することができる記述等の削除

スマートビルサービス提供のために取得するデータには、学生の氏名や学籍番号、学部、所属サークル、性別等の様々な個人に関する情報が含まれる可能性がある。また、氏名のようにその情報単体で特定の個人を識別することができるものや、所属サークル、学部のように複数の情報を組合せることで特定の個人を識別することができるものがある。このような特定の個人を識別できるデータにビルデータを含む場合は、全部またはその一部を削除、または他の記述等に置き換えることで特定の個人を識別することができないように加工する。

なお、他の記述等に置き換える場合は、置き換え前の情報に復元できないように不規則な方法を用いて変換する。例えば、学籍番号の情報を置き換える場合は、学年のみに置き換えて元の情報よりも抽象化することが考えられる。また、学籍番号そのものを他IDに置き換える場合は、ランダムな文字列や数字になるように変換する。

(ii) 個人識別符号の削除

スマートビルサービス提供のために収集するデータに個人識別符号を含む場合は、当該個人識別符号単体で特定の個人を識別できるため、当該個人識別符号の全部を削除、または他の記述等に置き換えることで、特定の個人を識別できないように加工する。

なお、他の記述等に置き換える場合は、置き換え前の情報に復元できないように不規則な方法を用いて変換する。

(iii) 不正利用により財産的被害が生じるおそれがある情報の削除

スマートビルサービス提供のために収集するデータに不正利用により個人の財産的被害が生じるおそれがあるデータを含む場合は、該情報が漏えいした場合に本人に不利益を及ぼす可能性が高いため、当該情報の全部を削除、または他の記述等へ置き換える。

なお、他の記述等に置き換える場合は、置き換え前の情報に復元できないように不規則な方法を用いて変換する。例えば、口座番号等を削除することが考えられる。

(2) サービス提供／学内利用

ビルサービス提供者は、運営組織（執行）の助言を受けながら「図 8-3.D-2（立命館）：データ利用／サービス提供／学内利用」のフローに沿ってサービス提供を行い、サービス提供結果評価・報告を実施する。

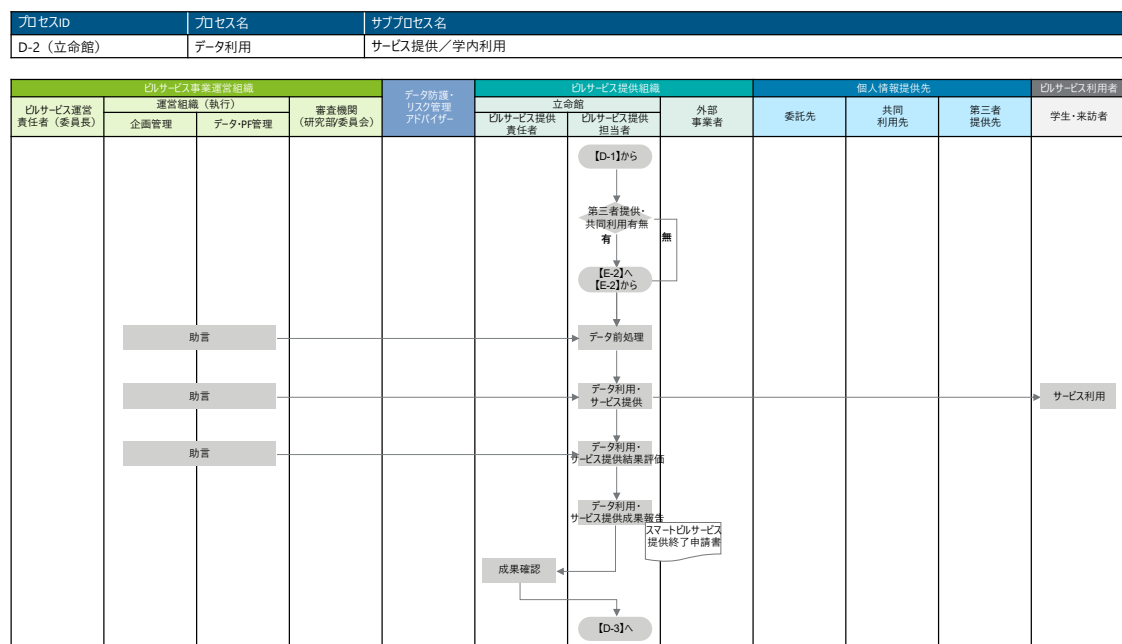


図 8-3.D-2 (立命館) : データ利用／サービス提供／学内利用

なお、ビルサービス提供者のうち、外部事業者に該当する事業者については、データの第三者提供および共同利用は原則として行わない想定のため、「図 8-4.D-2 (外部事業者) : データ利用／サービス提供／学内利用」のフローに沿ってサービス提供を行い、サービス提供結果評価を実施する。

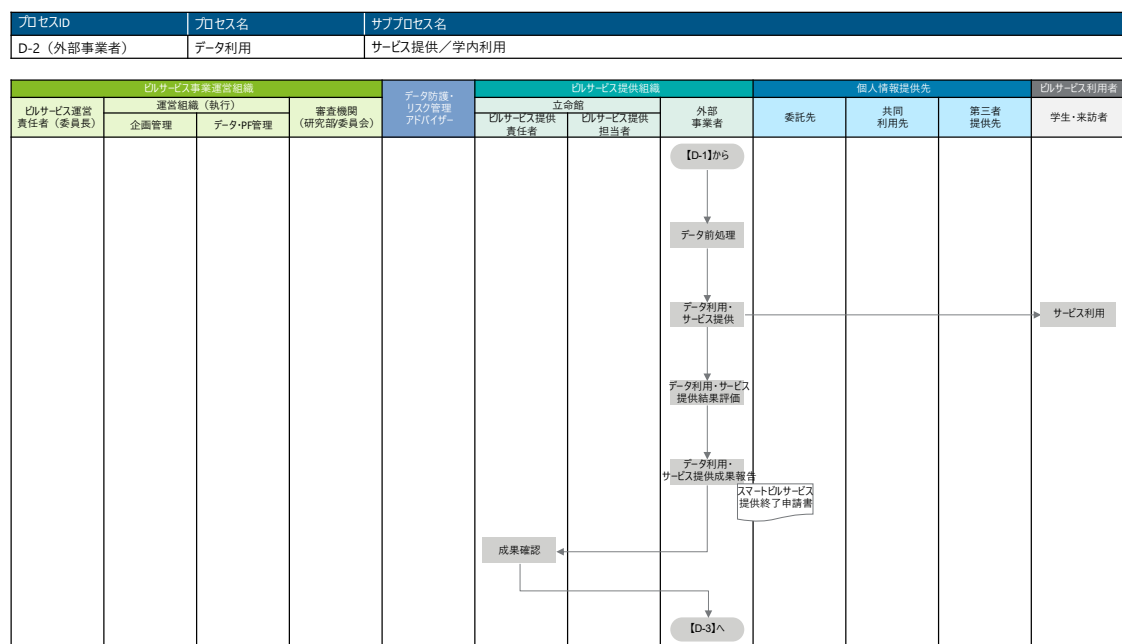


図 8-4.D-2 (外部事業者) : データ利用／サービス提供／学内利用

① 第三者への提供有無 (※立命館のみ対象)

ビルサービス提供者は、スマートビルサービス関連データの第三者への提供有無を確認する。

(i) 第三者へ提供する場合

第三者へデータを提供する場合には以下のプロセスを実施する。

- a. 業務委託を行う場合
ビルサービス提供者は、「エラー! 参照元が見つかりません。①データ提供（委託）」に進む。
 - b. 第三者提供を行う場合
ビルサービス提供者は、「8(3)②データ提供（第三者提供）」に進む。
 - c. 共同利用を行う場合
ビルサービス提供者は、「8(3)③データ提供（共同利用）」に進む。
- (ii) 第三者へ提供しない場合
ビルサービス提供者は、「8(2)②エラー! 参照元が見つかりません。データ前処理（※立命館、外部事業者ともに対象）エラー! 参照元が見つかりません。」に進む。
- ② データ前処理（※立命館、外部事業者ともに対象）
ビルサービス提供者は、運営組織（執行）の助言に基づき、データクレンジングやデータ統合、データ変換を行う。
- (i) データクレンジング
利活用対象となるビルデータについて、データ欠損やエラー等が含まれている可能性があるため、当該データの一部を取り除いたり、利活用対象データの中央値にて補正したりする。
 - (ii) データ統合
利活用対象となるビルデータについて、複数のデータから構成される場合は様々な条件下で取得されており、データの粒度が異なる可能性がある。そのため、データ統合により、一貫性の取れたデータを作成する。
 - (iii) データ変換
利活用対象となるビルデータについて、必要に応じてデータを指定のフォーマットに変換する。例えば、数値データを決められた範囲（例：0～1）に変換する。
- ③ データ利用・サービス提供（※立命館、外部事業者ともに対象）
ビルサービス提供者は、運営組織（執行）や外部の専門家等の助言に基づき、データ特性やデータ利用の目的に応じた手法を用いてデータの利活用し、サービス提供を行う。

(3) データ提供（委託・第三者提供・共同利用）

ビルサービス提供者は、ビルデータの第三者への提供形態に応じて、各フローに則り対応する。

- ① データ提供（委託）
ビルサービス提供者は、委託先の選定にあたり、委託先において適切な安全管理措置が整備されていること、および個人情報を法律に従って適切に取扱うための措置が規定されていることを確認したうえで、「発注業務マニュアル」に従ってビルサービスに係る業務を委託する。
- ② データ提供（第三者提供）
ビルサービス提供者は、「図 8-5.E-2（立命館）：データライフサイクル管理／提供（第三者提供）」のフローに沿ってビルデータの第三者提供を行う。

ビルサービス事業運営組織				データ防護・ リスク管理 アドバイザー	ビルサービス提供組織		個人情報提供先			ビルサービス利用者 学生・来訪者
ビルサービス運営 責任者（委員長）	運営組織（執行）		審査機関 (研究部/委員会)		立命館		委託先	共同 利用先	第三者 提供先	
	企画管理	データ・PF管理			ビルサービス提供 責任者	ビルサービス提供 担当者				
						[D-2]から ↓ 個人情報を含むか YES ↓ 第三者提供に係る 事項の公表 ↓ 本人同意の 取得済み確認 ↓ 第三者提供に関する 申請				
						第三者提供 申請書				

図 8-5.E-2 (立命館) : データライフサイクル管理/提供 (第三者提供)

(i) 第三者提供に係る事項の通知および本人同意の取得済み確認

ビルサービス提供者は、第三者提供を予定しているビルデータに個人情報が含まれる場合、当該個人情報を第三者提供することを本人に通知または公表したうえで、本人同意を取得する必要がある。ビルサービス提供者は、「7(1)②データ利用に関する同意の取得」にて、第三者提供にて必要な情報を通知したうえで本人同意の取得済みであることを確認する。

なお、取得済み、かつ本人同意が未取得の個人情報を第三者提供する場合は、当該個人情報を取得した本人に再度接触したうえで、第三者提供に係る本人同意を取得しなければならない。

(ii) 第三者提供に関する申請

ビルサービス提供者は、第三者提供先や提供するデータ、第三者提供に係る法令要件の遵守状況を整理するために、第三者提供に係る情報を取り纏めた『第三者提供申請書』を作成し、運営組織（執行）へ提出する。

(iii) 第三者提供に関する申請の受領・承認

運営組織（執行）は、ビルサービス提供者より提出された『第三者提供申請書』を確認したうえで、ビルサービス運営責任者に承認を依頼する。ビルサービス運営責任者は、『第三者提供申請書』に記載された第三者提供先が適切であることや、個人情報保護法で要求される対応が完了していることを確認したうえで、第三者提供を承認する。

(iv) 契約書作成

運営組織（執行）より第三者提供の承認を受けたビルサービス提供者は、『発注業務マニュアル』に従って、ビルデータに含まれる個人情報適切に取扱う旨を含む契約書を作成する。

(v) 契約書レビュー

ビルサービス提供者は、『発注業務マニュアル』および『規程・契約書点検手続きマニュアル』に従って、作成した契約書についてビルサービス提供責任者よりレビューを受け、必要に応じて内容の修正をする。

(vi) 契約締結

契約締結手続き完了後、ビルサービス提供者は、契約書の写しを保管する。

(vii) データ提供

(viii) 第三者提供の記録作成

- ・ 第三者の氏名または名称（不特定多数に対して提供した場合にはその旨）
- ・ 第三者の連絡先
- ・ 個人情報によって識別される本人の氏名の一覧
- ・ 第三者提供される個人情報の項目（例：氏名、住所等）
- ・ 第三者提供される個人情報の件数
- ・ 本人の同意を取得していること

データ利活用担当者は、「**図 8-6.E-2：データライフサイクル管理／提供（共同利用）**」フローに沿ってビルデータ利活用に係る共同利用を行う。

図 8-6.E-2：データライフサイクル管理／提供（共同利用）

ビルサービス提供者は、共同利用を予定しているビルデータに個人情報が含まれる場合、共同利用先とビルデータの取扱いに関する体制、役割分担および手続き等について協議・合意する。

- ・ 共同利用先
- ・ 共同利用先における個人情報取扱責任者、問い合わせ担当者および連絡先
- ・ 共同利用するデータの取扱いに関する事項
- ・ 共同利用終了後におけるデータの返還、消去、廃棄に関する事項
- ・ 個人情報漏えい等のインシデント防止・発生に関する事項
- ・ 共同利用するデータの取扱いに関する事項が遵守されなかった場合の措置 等

30

ビルサービス提供者は、当該個人情報を利用することについて本人に通知または公表する必要がある。ビルサービス提供者は、共同利用先と協議・合意した共同利用における事項について、スマートビルサービスを提供するウェブサイトやスマートフォンのアプリケーション上や、書面を用いて本人に通知または公表する。

- (iii) 共同利用に関する申請
ビルサービス提供者は、共同利用先や提供するデータ、共同利用に係る法令要件の遵守状況を整理するために、共同利用に係る情報を取り纏めた『共同利用申請書』を作成し、運営組織（執行）へ提出する。
- (iv) 共同利用に関する申請の受領・承認
運営組織（執行）は、ビルサービス提供者より提出された『共同利用申請書』を確認したうえで、ビルサービス運営責任者に承認を依頼する。ビルサービス運営責任者は、『共同利用申請書』に記載された共同利用先が適切であることや、個人情報保護法で要求される対応が完了していることを確認したうえで、共同利用を承認する。
- (v) 契約書作成
運営組織（執行）より共同利用の承認を受けたビルサービス提供者は、『発注業務マニュアル』に従って、ビルデータに含まれる個人情報を適切に取扱う旨を含む契約書を作成する。
- (vi) 契約書レビュー
ビルサービス提供者は、『発注業務マニュアル』および『規程・契約書点検手続きマニュアル』に従って、作成した契約書についてビルサービス提供責任者よりレビューを受け、必要に応じて内容の修正をする。
- (vii) 契約書締結
契約締結手続き完了後、ビルサービス提供者は、契約書写しを保管する。
- (viii) データ提供
ビルサービス提供者は、共同利用先にビルデータを提供する。

(4) サービス提供／学内利用終了
ビルサービス提供者は、「図 8-7.D-3：サービス提供／学内利用終了」のフローに沿って運営組織（執行）にサービス提供・学内利用終了に関する報告を行う。

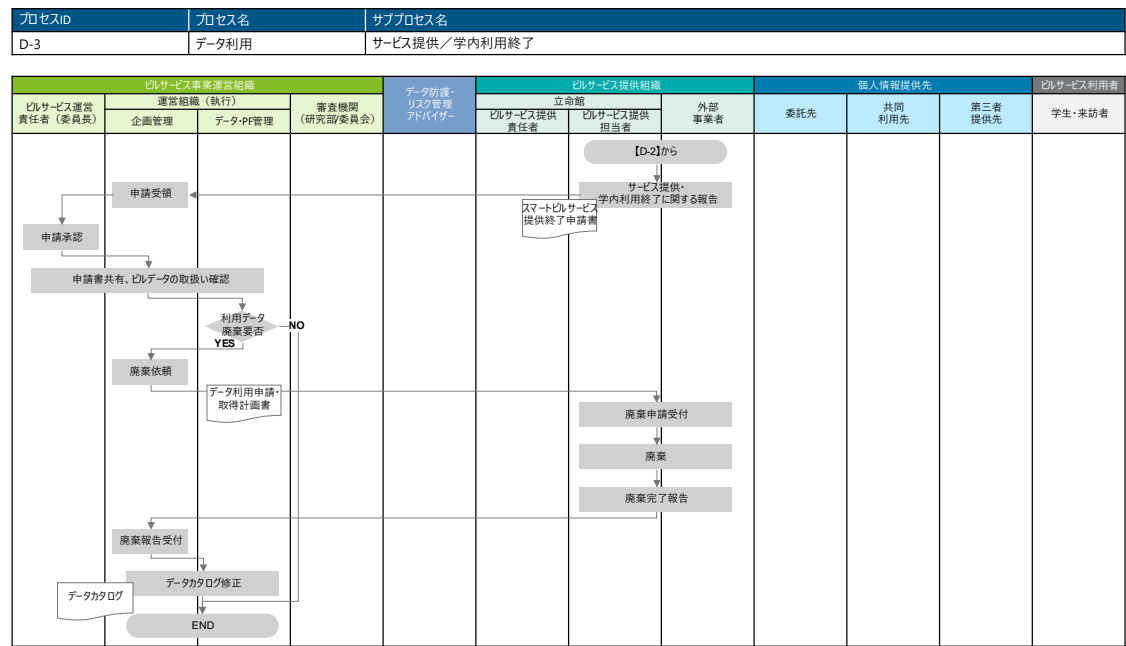


図 8-7.D-3：サービス提供／学内利用終了

① サービス提供・学内利用終了に関する報告

ビルサービス提供者は、ビルサービスの提供を終了するにあたり、ビルサービス提供を終了する背景や理由、終了予定日および取得したビルデータの取扱い等の情報を取り纏めた『スマートビルサービス提供終了申請書』を作成し、運営組織（執行）へ提出する。

② ビルサービス提供終了に関する申請の受領・承認

運営組織（執行）は、ビルサービス提供者より提出された『ビルサービス提供終了申請書』を確認したうえで、ビルサービス運営責任者に承認を依頼する。ビルサービス運営責任者は、『ビルサービス提供終了申請書』に記載された内容を確認・承認する。

③ ビルデータの廃棄依頼

運営組織（執行）は、『ビルサービス提供終了申請書』に記載されたビルデータの取扱いを確認し、ビルデータの廃棄要否を確認する。ビルデータの廃棄が必要と判断された場合、ビルサービス提供者に対して『データ利用申請・取得計画書概要』におけるデータの廃棄に係る記述を更新・交付し、個人情報を含むビルデータについて廃棄を依頼する。

なお、立命館大学として研究目的等のために当該データを利用する必要性が認められ、かつ個人情報が含まれている場合は、個人を識別できないようにデータを加工することにより当該データを継続利用できるものとする。

④ ビルデータの廃棄・報告

ビルサービス提供者は、データの廃棄について更新された『データ利用申請・取得計画書概要』に則って適切にデータを廃棄し、廃棄が完了したら運営組織（執行）へ報告する。

⑤ データカタログ修正

運営組織（執行）は、ビルサービス提供者からのビルデータの廃棄完了報告を受け、データカタログを修正する。

9. その他

(1) 企画変更手順

ビルサービス提供者は、提供中のスマートビルサービスの企画を変更する場合は、「表 5-1. スマートビルサービスの企画変更に係る手続き」に従って必要な手続きを実施する。

表 5-1. スマートビルサービスの企画変更に係る手続き

変更内容	必要な手続き	備考
利用目的の追加・変更を伴う提供サービスの変更	5. スマートビルサービス提供に係る企画 6. 企画および取扱いデータの審査 7. データ取得（必要に応じて実施）	利用目的の変更を伴う、提供サービスの追加変更となるため、新規サービス提供と同等に取扱う
利用目的の追加・変更を伴わない提供サービスの変更	特になし	サービスの提供対象や範囲、時間帯の変更等、サービス提供に係るリスクに影響しないものを想定
AI 等の新規技術の採用	5. スマートビルサービス提供に係る企画 6. 企画および取扱いデータの審査	新規技術の採用に伴うリスクを評価する
データ項目の追加・変更	5. スマートビルサービス提供に係る企画 6. 企画および取扱いデータの審査 7. データ取得	データ項目の追加に伴うリスクを評価する

委託先の開始	8(3)① データ提供（委託）	—
第三者提供先の追加・変更	8(3)② データ提供（第三者提供）	取得済みの個人情報に係る第三者提供となるため、当該個人情報を取得した本人に再度接触したうえで、第三者提供に係る本人同意を取得しなければならない
共同利用の開始	8(3)③ データ提供（共同利用）	—

(2) 苦情問合せ

ビルサービス提供者は、スマートビルサービス提供においてビルサービス利用者より苦情等の問合せがあった場合は、適切に対応する。

① ビルサービス提供に関する問合せ

ビルサービス提供者は、スマートビルサービス提供における連絡先を公表し、ビルサービス利用者からの苦情等の問合せに適切に対応するとともに、必要に応じて運営組織（執行）に報告する。

② ビルデータに含まれる個人情報に関する問合せ

ビルサービス提供者は、ビルデータに含まれる個人情報に関する問い合わせがあった場合は、前項の手順に従うほか、『学校法人立命館個人情報保護規程』における「第6章 公表、開示、訂正、利用停止等」に従って対応するものとする。

なお、スマートビルサービスの特性として、カメラ等で取得した顔の画像を含む個人情報の開示、訂正、利用停止等請求があった場合は、開示や訂正、削除等により第三者のプライバシーが侵害されるケースや犯罪捜査に影響を与えるケース等を除き、法令に基づき適切に対応する必要があるため、留意すること。