O-024

パーソナルデータの利活用と規制を両立させる情報ガバナンスの考察
The Consideration of the Information Governance to achieve both the Utilization and the Regulation of the Personal Data

北村 浩†
Hiroshi Kitamura

1. はじめに

IoT や自動走行に係るサービスにおいて、ヒト（利用者）～モノ（デバイス）～コト（行動）の一体化された活動に伴って収集・利活用の対象となるビッグデータの管理指針を定めることは急務だと考えられることから、本稿においてデータの利活用と規制のガバナンスを図るルール化を考察する。その中で、ヒトの活動により参照・更新が伴う IoT 事業のパーソナルデータの所有・利用において、ステークホルダーの間の合意形成をいかに図り、利活用と規制を調和させるのかは、IoT を推進するための課題になる。2017 年 5 月末に個人情報保護法が改正・施行されて、パーソナルデータ利活用の環境が整備されてきたが、利活用と規制の合意ルールは必ずしも形成されておらず、両立を図るために、情報管理と法的規制を融合した研究が十分行われているとは言い難い。パーソナルデータの利活用と規制のルールの可視化を進めることで、IoT サービスの平時と紛争等の有事の両方で、ステークホルダーがいかにアカウンタビリティを発揮するためかを研究する意義は大きい。

2. クラウトサービス下の越境データ

データの管理において、パーソナルデータを扱う事業者が、米国・英国等のクラウドサービス下を物理システムの拠点とする場合、当該地域の法的規制に支配される管理則を準備する必要性が生じる。予測可能な不測事態は、データ管理に係る損害として、電子媒体の物理損失、エラー時の手順のミス、それらに伴うサービスの継続の中断のような運用上の障害に加えて、データに係る所有者・提供者・利用者等のステークホルダーの有事の際のデータの漏洩や流出のような社会的損害への波及を十分考慮した基盤的なマネジメントシステムの未整備という状況が考えられる。これらを管理するためのシステム化をいかに講じるかが、事業者の責務だと考えられる。クラウドサービス下のデータを運用コストの安い海外データセンターの別の事業者に委託すると、当該地域への越境データとしての管理負担が増加するのが通常である。パーソナルデータに係る IoT サービスの有事に至る過程で、損害が波及して漏洩や流出のような社会的なものへ波及し、データのステークホルダーを巻き込む有事が進み訴訟への展開が予測されると、審理前の手続きとして、米国・英国等の先進国は、当該地域の行政機関・裁判所から事案の eDiscovery(電子情報開示)の情報開示要求という手続きが発生し、事案に関係したかもしれないデータの開示を行うことで、事業者がいかにアカウンタビリティを発揮し説明するのか、また、いかにパーソナルデータの所有・利用のステークホルダーの間の合意形成を図り、利活用と規制を調和させたサービス継続に努めるのかについて、組織の取り組み方針と詳細な実施手順等の責務がいかに実行するかが問われる。

IoT サービス事業に係るデータを物理的に越境した拠点で管理されることを前提に、パーソナルデータの情報ガバナンスを本稿では考察する。 IoT サービスに係るデータの多くは、クラウドサービスを運用する海外データセンターに設置された情報システムで管理される。IoT サービスにおいて、サービス提供者(事業者)とサービス利用者の間で取り交わす利用に際して、利用者は所有するテータを事業者に提供する。例えば、利用開始に伴って顧客プロフィールの登録、利用取引の都度生じる注文情報や蓄積された履歴記録等の安全措置について、事業者に委任する手続きの後、サービスの利用規約等の定められた管理基準に則って運用し、その中で、外部企業に委託する業務があれば、当該管理基準と同等の運用を行う旨、委託業務契約を結び、以降は管理・監査が適宜実施され、一定の管理水準で運用を維持することが事業者の責務となる。事業者は、利用者からの提供データについて保護すべき安全保護の施策を講じて、データに係るリスクの軽減、不測事態の際においてもリスクが二次的に波及することの未然防止を図る局所化の考慮が相応に施されているが、事業者と利用の間でどの程度のサービス提供が保証されるのかというサービス合意の形成を示す SLA(Service Level Agreement)が利用規約や契約に明示的に条文化されない限り、事業者はベストエフォートサービスの維持に努めるものの、当該合意は実質的に、事業の費用対効果に見合うサービス水準で内部管理が行われるに過ぎず、万全の安全措置が保証されるには至らない。 利用者から事業者への提供データとして、B2C サービスでは個人に係る情報(パーソナルデータ)を、B2B サービスでは営業秘密(顧客情報、商談(案件)情報、取引等の商談履歴、技術上の機密情報など)に一定水準で管理する情報ガバナンスを構築する役割を事業者が果たすことが、管理上極めて重要になる。

データの係る有事において、物理データの所在地の行政機関・裁判所から事業者へのデータ開示要求時においても、利活用の継続と規制に係る保護をいかに実現するのか、越境状態のパーソナルデータの管理をいかに行うのかの指針を考察する。前述の eDiscovery は、米国・英国等での事業における紛争時に生じる訴訟の審理前のステークホルダー対象の情報開示要求に係る義務手続きであり、日本にはない法務手続きであるが、日本の事業者が当該制度を運用する海外地域で有事に係る際は不可避の手続きである。当局からのデータの要求先(事業者)は、要求元(当局)に適正な開示を行って、誠実な対応を遂行して早期の和解を促進する役割の遂行が、当該地域では社会的に定着している。

3. データとカストディアンの管理責任

有事事案が当事者間の紛争に展開すると、eDiscovery という訴訟の審理前に行われる、事案のステークホルダーに係る電子情報の開示手続きである。事案に係るデータが米

国・英国等の先進国地域のクラウドサービス下に物理的な越境データとして配置される場合、規制当局から情報開示の義務を負うデータの要求先となる事業者は、事案の概観を示す関係者の間の関係等を示す証拠データを提出する。 eDiscovery の過程において、事案のステークホルダーは、カストディアン(Custodian、事案に係るデータの管理者)と定義づけられ、証拠データの開示要求の手続きが行政機関や裁判所により進められる。 情報開示の要求時に、事案に係るデータ管理(所有または利用)者がカストディアンとして指名され、対象データの識別、事案における重要度の判定、カストディアン間の関係性を可視的に図示するカストディアンマップが規制当局に提出される。 日本の事業者(プライマリ事業者)が、利用者からの提供データを海外のクラウド事業者(セカンダリ事業者)に委託して越境データとして運用する場合、両者はカストディアンとして認められ、また、事業者と提携する別の事業者(セカンダリ事業者)がデータを共有する場合、その事業者もカストディアンとして、当局からの情報開示の要求先の対象に含まれる。

デバイス利用の IoT サービスにおける、パーソナルデータ漏洩という有事においては、利用者からの提供データだけでなく、当該データに家族や知人のデータが関係付けられ、IoT サービスのアプリケーションが当該データを利用して稼働するのであれば、カストディアンとして、漏洩した一連の物理データを管理する事業者と共にデータ漏洩事案の責任を分担するステークホルダーに係る概観について、可視化を行うカストディアンマップに関係者の名前が列挙され、eDiscovery の手続きが進む。 また、IoT サービスの利用に伴って、商談情報、取引履歴等ライフログが、顧客プロフィールと照合可能な配置の場合は、 両者を照合する機会が生じた際には、特定の個人の識別が容易になる。このようなシステム環境下での有事は、個人とライフログが関係付けられ、たとえ行動データの提供者が個人情報を開示していない状況でも、データ管理者のサービス事業者等が意図的に照合可能な状況下にあれば、個人情報が追跡可能になる。また、事業者（データの管理者兼所有者）と関係先である別の事業者（データの利用者兼共有者）の間の有事においては、この管理・所有と利用に係る事業者は、eDiscovery のカストディアンとして、応分負担を担うステークホルダーと定められる。 パーソナルデータの漏洩、ライフログと顧客プロフィールによる個人の識別の容易照合性での個人情報が追跡可能の両方の場合、eDiscovery のプロセスでは、ステークホルダーとして、事業に係る電子情報の管理者であるカストディアンのすべてを対象に、規制当局から開示要求の手続きが進められる。 その際、候補データの事案との関係やカストディアン間の関係を可視化されたカストディアンマップのような証拠を提出する義務が事業者に生じる。

サービス提供者(事業者)は、サービス利用者から提供されたデータの中で保護すべきデータのリスクの軽減や局所化を図る管理策を講じているが、当該データについて、関係先である別の事業者がデータ共有を行う場合、責任の分担に際して、どのように可視化を図るのかについては、基準が必要になる。 eDiscovery の手続きにおいて、組織単独のデータ管理でも、他の事業者との分担に基づくデータ管理でも、規制当局等から開示要求が生じた際、候補データについて、所有と利用の分担を定めた上で、カストディアンマップを行政機関・裁判所に提出する。 通常、IoT サービスは複数の要素技術を実装する機器やアプリケーション等のソフトウェアを複数の事業者によるものを最終事業者が統合して提供することが多いため、IoT サービスに伴う有事の原因が、個別の要素技術、またはそれらが複合する技術のうち、何に帰結するのかについては、問題判別を要する。 責任の内訳としての自責と他責の配分については、マルチステークホルダーを前提に、事案の候補データについて、複数のカストディアンの共有データの記録管理の可視化が重要な課題になる。日本国内のみで、IoT サービスの構成要素であるデータやソフトウェアの接続、他ネットワークとの連携を行う場合でも、有事の責任の分担について、事業者各ステークホルダーの責任の割合、利用者への影響度の具体化を図ることは、越境データの考慮が前提の場合、eDiscovery の手続きへの対応が必要になるため、情報ガバナンスの指針の備えが必要になる。

4. eDiscovery 前提のデータ共有ルールの再考

パーソナルデータについて、IoT 利用者のデバイスからの収集データ、その後の流通データ等を、Observed data(観測データ)のヒトの属性を有するライフログ(ヒトの行為に係る記録(行動履歴))として、個人の行動にもとづくデータを対象に考察を進める。 パーソナルデータの利活用による IoT サービス事業における、 eDiscovery の開示手続きの施策を考案するために、事業者は、データ管理者の責務であるカストディアンとして利用者との合意形成を図り、共有データの管理ポリシーを実装して、データの所有と利用に係る権利の分担ルールを考えることが必要である。 この分担は、データの主管理者である事業者と、共有する関係先の別の事業者の責任の応分負担を示す。 そのために、IoT サービスの利用者、パーソナルデータの提供元であるデータの所有者に、所有・利用の権利を定める視点を導入する。

本稿は、パーソナルデータの所有・利用のルール化をいかに行うかの問題提起を示した。IoT サービス事業のシステム基盤において、パーソナルデータの所有権を曖昧にしたままで、データ管理者であるカストディアンとしての事業者の共有データの帰属先や責任に係る分担を明示せずに、IoT サービス事業が展開されると、データに係る有事の際に、データを共有するカストディアンの間において責任をいかに分け合うのかについて、問題が顕在化する。 一般に、ネットワークサービスを支援する情報システムの管理を考えると、データ利用の権利(アクセス権)はシステム管理者による権限付与を行うことから明らかであるが、データ所有の権利(オーナーシップ)は不明瞭な場合が多いと考えられる。 IoT サービスの利用において、個人のライフログの例として、小売事業での消費者の行動(照会・注文・決済等)は、個人主体のデータの利用であるが、利用対象のデータの帰属先には記名式の所有権の有無や共有対象は必ずしも明らかではない。 例えば、ヒトの行為に係る記録(行動履歴)として、注文・決済等のライフログは、消費者プライマリのデータであり、ステークホルダーのどこのだれとデータ共有を行うかについては不明瞭であり、行動に係る事業者の所属業界の慣習的な暗黙ルールにこれまで依存してきた。 実際に、注文データは利用者と注文先の事業者の共有データとして、また、決済データは利用者と小売事業者および決済機関の金融事業者の共有データとしてそれ

ぞれ扱われてきた。 利用者と事業者の間で、ライフログに係るデータの帰属先を明示的に合意する手続きはないが、データに係る有事が発生することを前提に、責任に係る分担の中身を定めることは可能である。 越境データに係る有事には、カストディアンが所有と利用で共有するデータについて、eDiscovery の開示要求の対象になることから、所有と利用に係る個人・法人のすべてが要求先になり得るため、データの所有と利用に係る権利の分担ルールを定めた情報ガバナンスを考察することが極めて重要になる。 業界の慣習に依存するデータの開示ポリシーなき現況において、共有データについて情報漏洩等の問題が生じると、利用者を中心とするステークホルダーからの苦情や規制当局からの調査や紛争手続きの問題が顕在化した後のオプトアウト手続き、組織の監査業務、さらには訴訟に波及する場合には、IoT サービスのアプリケーション実施に伴うデータの追跡等が行われ、データの Chain of Custody(CoC: 証拠保全の連続性)の検証手続きまで影響が及ぶことが考えられる。

5. eDiscovery 手続きのデータ要件

eDiscovery 前提のデータ共有ルールを再考し、情報ガバナンスを構築することを提言する。この情報ガバナンスは、有事の発生以前の予防法務対策として、情報管理の体系化を構築することで、海外での紛争を念頭において、訴訟ホールド(Litigation Hold)の手続きに対応するデータマネジメントを必須とする。これは、有事の発生以前の時点の予兆が検知される時点において、一定の潜在的な問題を認識できて、不測の事態の発生が起こり得ることを合理的に予測できる時点において、有事につながり得るデータを証拠の候補として保全を開始し、また、将来予測される情報開示要求の発生を想定して、データに係る説明責任を果たすための情報開示のマネジメントシステムの仕組みを構築し、組織の情報管理のルール化と運用を推奨する eDiscovery の理念に基づく手続きが実現できるシステム化を示す。訴訟ホールドは、事案に係るデータ証拠の候補となるデータの保全を行うが、証拠データとして保全の必要な最早時点の静態データ(スナップショットデータ)を取得するシステム的な手続きが可能である。データを管理する事業者は、事案と係るデータ候補を eDiscovery のための証拠保全とし、どのように管理・運用するのかという指針を定め、日常の運用において妥当性を検証し、明文化された手順にもとづいて、提出可能な証拠データを管理する法的な義務を負う。

訴訟ホールドのためには、Chain of Custody が示す証拠保全の連続性というデータマネジメントの要件が必要になる。米国・英国等の法務手続きにおいては、証拠データの提出形式が厳密に定められている。eDiscovery の手続きにおいて、Contents(データ本体)と、Metadat(メタデータ)の両方の保全・開示を行う原則がある。メタデータは、コンテンツのことを記述するデータであり、コンテンツを説明する情報を含み、コンテンツとは区別された管理が必要とされる。米国機関によると、eDiscovery 手続きでの証拠データについて、データ本体の形式およびメタデータの要求事項が示されている。国際規格の ISO15489-1(Information and documentation -- Records management -- Part 1: Concepts and principles)において、メタデータをデータの定義記録コンテキスト(背景・状況・説明)、内容、構造およびある期間記録管理(履歴管理)の記述データとの定義がある。メタデータの必要性は、eDiscovery 手続きにおける 5W1H の情報として、パーソナルデータのライフログを補足する情報が提供できる点にある。すなわち、「いつどこでだれが何をどのように行った」の記録を示す証拠データが必要であり、いつ(タイムスタンプ)、どこで(IoT サービスのクラウドサービスに接続されたネットワーク識別)、だれが(IoT デバイスを利用するヒトや IoT アプリケーション)、何を(アプリケーション機能)、どのように(アクセス履歴)に係るデータ保全を担保することが、eDiscovery のプロセス後に考えられる紛争対応の手続きに重要になるためである。

IoT サービス事業に係るデータについて、そのオーナーシップが、越境テータとして物理分散システム環境に配置されるため、訴訟を前提に統合されたデータマネジネントでのルール整備を図ることが、eDiscovery への対応につながる。IoT システムの構成要素である処理データやログについては、管理主体の事業者が個別管理下のクラウドサービス運用を行っているが、考慮を要する。クラウドサービスの形態としては、パブリッククラウド、プライベートクラウド、その両者を組み合わせたハイブリッドクラウド等の商用サービスの提供が一般である。利用者のコスト負担、事業者の管理負担それぞれの軽減を図るために、パブリッククラウドでのサービス稼働が多いと考えられるが、次の点に注目して対策を講じることが必要である。 パブリッククラウドは、専用システムとしての利用契約を結ばない限り、他の事業者とのシステム資源を共有するため、データのコンテンツ(本体)には専用スペースが割り振られるが、それ以外は、共有となることが考えられ、CoC を担保する証拠データの保全が極めて難しくなるのである。 具体的には、ログデータとメタデータについては、他との共有が通常運用から生じることが考えられ、CoC の要件が最初から満たされないため、eDiscovery に対応不可のパブリッククラウド自体を計画せず、プライベートクラウド、または、それを含むハイブリッドクラウドの利用を前提にサービス稼働のシステム環境が計画されるべきである。

訴訟ホールドは、その予兆が発生した時点、または、その以前に、将来的な不測の事態の発生が合理的に予測可能と判断できる時点で、証拠データの保全が担保されることを示す。保全は、データを担保することに留まらず、訴訟ホールド後のデータアクセス全般を抑制し、対象データを強制的に利用の凍結を可能にする。eDiscovery プロセスと当該データは、事案のステークホルダーに公明正大に開示されるべきという理念の下、カストデイアンには保全義務が生じる。その際、どの時点でどのような範囲でのデータ保全に着手するのかが重要である。例えば、同業他社での予兆検知の情報を得た時、顧客から苦情が来た時、不具合の社内報告があった時、メディア報道に向けた動きがあった時に、訴訟ホールドに着手するのか判断を迫られるが、タイミングを見誤るとデータ保全が遅れ、eDiscovery プロセスの遅延を導き、予測不能な責任問題へ影響が拡大することが懸念される。具体的には、規制当局の行政調査や裁判所の司法手続きの中で、不利な推定、手続き上の制裁、課徴金を受ける等の負担を受け、アカウンタビリティを発揮する機会を逸することで、事業者は社会的な信頼を失うことも考えられ、以降の対応コストが指数関数的に増加する事案が多い。事業者が抱える経営リスクの予防法務の対策に、早期事案評価(ECA: Early Case Assessment) という方

法論の適用により、有事を概観する効果的な意思決定において、事案に係るデータの可視性を判断することも可能である。

6. データの所有選択・利用選択の指針

パーソナルデータについて、IoT サービス事業では、利用者からの収集・流通データを対象に、クラウドサービス下に実装されたアプリケーションにより、サービスに係る処理・制御が行われる。 パーソナルデータの共有(所有・利用)アクセスについて、所有情報選択権と利用情報選択権の考え方を適用し、データの所有者と利用者の間の合意形成のためのルール化を図り、それにもとづく情報ガバナンスの管理ポリシーをいかに定めて実装するのかが重要になる。 パーソナルデータの所有と利用の共有形態では、データを管理ポリシー上の開示対象の場合、所有または利用の選択権を行使でき、所有情報選択権と利用情報選択権として定め、どのデータを所有または利用するのか、だれとだれが共有するのか、どんな条件を定めるのか等を明示する。データの所有と利用の共有システム環境を構成する場合、所有については、一次生成の情報源として定め、その生成の直接的な関係者に認められる情報所有行為として所有権が定められる。所有情報選択権は、所有データのうち、他への開示を可能にし、対象として、不特定者向けの開放データ、事前定義された特定者向けの静的データ、アクセス時に共有可と判定する動的データ、に分類される。また、利用については、それまでの所有と関係なく、その直接的、または二次的に認められる情報利用行為として利用権が定められる。利用情報選択権は、データ所有者により開示されている前述 3 種のデータのうち、静的データと動的データを対象にして、所有データとのマッチングが、静的または動的に行われる。 マッチングの概観については、アクセスの可否、可能な場合はアクセス対象のデータ項目・種別(コンテンツとメタデータ)・アクセス種別(参照･編集や更新の権限付与の程度)等を定める。

7. おわりに

今後、有事の事案に係るステークホルダー間の合意形成を支援するデータマネジネントを実装するための指針を明らかにすることが重要である。IoT サービスの利用データについて、データ管理者であるカストディアンとしての事業者の共有データの帰属先や責任に係る分担を明示し、個人主体となるデータの利用においても、ライフログ等の対象データの帰属先に記名式の所有権の有無や共有対象について、利用者と事業者の間の合意形成を図るルール整備と手続き化を目指して、有事の発生を前提に、責任分担を示す基準を定めることは可能である。

IoT サービス事業はグローバル市場であり、複数の技術の統合に伴って、情報ガバナンスの具体化のために、管理ポリシー、管理規範・基準、運用手順、データのアクセス手法、情報プラットフォームの構築等により、有事の問題判別を容易に実現することが期待される。

参考文献

[1] A.Phillips, R. Godfrey, C. Steuart, and C. Brown, E-discovery: An Introduction to Digital Evidence, pp.2-18, August 2013.

[2] Brackett, M.(1994). Data Sharing Using A Common Data Architecture, John Wiley. A.Phillips, R. Godfrey, C. Steuart, and C. Brown, E-discovery: An Introduction to Digital Evidence, pp.2-18, August 2013.

[3] A.Phillips, R. Godfrey, C. Steuart, and C. Brown, E-discovery: An Introduction to Digital Evidence, pp.2-18, August 2013.

[4] EDRM: Electronic Discovery Refence Model https://www.edrm.net/frameworks-and-standards/edrm-model/

[5] Cohasset Associates , ARMA International and AIIM 2013 | 2014 Information Governance Benchmarking Survey, pp.19-29, December 2014.

[6] Federal Trade Commission, Bureau of Competition Production Guide, https://www.ftc.gov/sites/default/files/attachments/bc-production-guide/bcproductionguide.pdf , pp.1-8, January, 2012

[7] Amelia, P., Ronald, G., Christopher, S., and Christine, B. (2013). E-discovery: An Introduction to Digital Evidence, Delmar Publishing, 2-18.

[8] Cohasset Associates (2014). ARMA International and AIIM 2013|2014 Information Governance Benchmarking Survey, 19-29

[9] ISO 15489-1:2016, Information and documentation – Records management -- Part 1: Concepts and principles https://www.iso.org/standard/62542.html

[10] 佐藤 一郎 (2016). ビッグデータと個人情報保護法：データシェアリングにおけるパーソナルデータの取り扱い,科学技術振興機構ジャーナル『情報管理』, 58(11), 828-835.

[11] 北村 浩 (2017). eDiscovery(電子情報開示)手続きを考慮した自動運転車のクロスボーダー・リスクの可視化システム要件, 電子情報通信学会 IEICE Technical Report, 7-12.

[12] 北村 浩 (2018). パーソナルデータの管理リスクの可視化を指向する IoT サービス事業の考察, サービス学会・年次大会発表.