様式 1-4-2 (2022-1)

令和４年度研究開発成果概要書

採 択 番 号　　22004
研究開発課題名　データ連携・利活用による地域課題解決のための実証型研究開発（第３回）
副　　題　　情報銀行による匿名化データサービスと地域永続化実証

（１）研究開発の目的

これまで、代表研究責任者らは街区に IoT 機器やセンサを設置し、その情報をもとにデータの二次利用サービスを提供してきた。その基本は、代表研究責任者が構築した Authorized Stream Contents Analysis (ASCA)と呼ぶ技術を利用したエッジコンピューティングノード(以下エッジと呼称)、および、その ASCA エッジを含む情報インフラ基盤である。ASCA は、例えば REST over https や MQTT over SSL といった通信下であっても、クラウドと結託して入手した共有鍵を用いて暗号を復号し、gzip 展開および chunk デコードを行いつつ、コンテキストスイッチ機構と高度なコンテキストキャッシュ管理により TCP ストリームを低コストで再構築、さらに直接ストリームの中から必要な情報を正規表現などにより抜き出し、その情報抽出や改変を行うことを可能とする。ASCA を用いれば、ゲートウェイやエッジにおいて透明アドオンと呼ぶサービス提供手法が実現できる。透明とはネットワーク透過性(Network Transparency)を備える状態を意味し、IoT などエンドデバイスからクラウドを見た時、その間には何も存在しないように見えることを意味する。エッジにおける透明アドオンとは、端末に何ら機能拡張や変更、更新を伴わずに、端末にない機能をエッジで自由に追加しつつ、もともとの機能を維持することを意味する。つまり、ASCA によりエッジにおいてネットワーク透過にプロトコル変換、データ変換、セキュリティ向上などを実現可能となる。図 1 はゲートウェイやエッジといったネットワーク階層における透明アドオンにより、ネットワーク途中で情報取得およびサービス提供を行うイメージ図である。

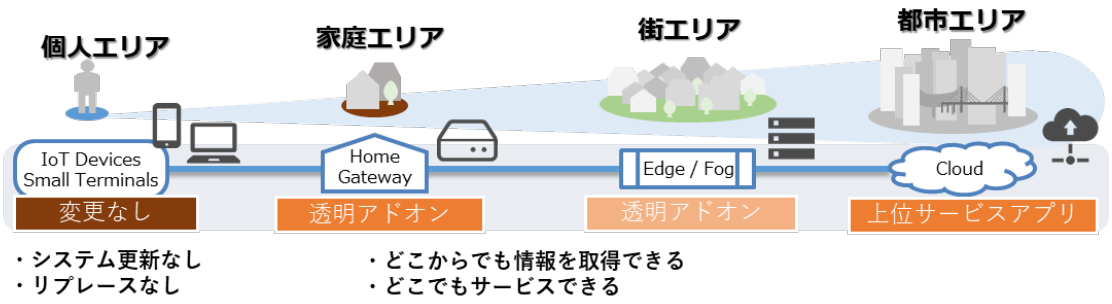


図 1 透明アドオンによるネットワーク途中での情報取得・サービス提供のイメージ

エッジはクラウドの処理をエンドユーザに近い場所で提供するため、低遅延サービスを提供できるという指摘がしばしばなされる。しかしながら、クラウドはエッジと比較して計算リソースが潤沢にあり機械学習など膨大な計算を比較的短時間に処理することができる。従って、エッジ処理による処理時間増加と通信遅延低減のトレードオフを議論しなければ、単純にエッジだから低遅延とはならない。つまり、すべてのアプリケーションがエッジにより、低遅延化の恩恵を受けるわけではない。透明アドオンこそが、エッジの大きなメリットであると考え、実際に透明アドオンを実現するスマートコミュニティ向け情報通信プラットフォームおよび関連インフラを構築し、UDCMi において運用した。その運用によって、その先にある将来の社会的問題が明らかになった。その解決手段の構築が本研究の核心である。

・解決するべき課題

個人情報の提供と二次利用において、エッジでの透明匿名化と透明電子透かしは、データ漏えいの際に効力を発揮するが、EU による一般データ保護規則(GDPR)などは、漏えい以前のデータの流通やデータの保持すらも制限する内容を含む。これは、個人の権利を守る以外にも、個人情報を用いたサービスを EU 外の企業が担うことを規制するという側面も垣間見える。これはつまり、国家間でのデータ管理競争や、情報産業における経済活動の掌握競争ともいえる。透明電子透かし技術は漏えいの抑止力となりえるが、データが漏えいして明るみになった場合に効力を発揮するため、漏えいに至るデータ流通や、データの保存そのものを監視、制限することはできない。データの流通を検出してこれを制限すれば保持すらできなくなるため、流通の検出手法が必要となる。同様の問題は地方自治体にも存在し、代表研究責任者がさいたま市と共に、将来の情報インフラが解決するべき問題として、これまでも協議を重ねてきた。場合によっては地方自治体の存続にも関わりかねない深刻な問題が見えてきた。

個人情報やプライベートな情報の漏えいに対する感覚や判断について、地域的特徴が存在する。すなわち、地域住民間では、プライバシの問題とならない場合でも、地域外では問題となることを意味する。言い換えれば、地域では、個人情報など、その地域内に留めて外部から秘匿されるべき情報が存在し、これらは、地域に留めて外部からアクセスできなくする、もしくは匿名化し、電子透かしを入れてから公開することで情報を守ることができる。これを情報のカプセル化と呼ぶ。同様に、あるスマートコミュニティサービスを展開する場合、個人に近いほど、平文データ(未処理の情報で個人情報やプライベートな情報が含まれる可能性がある情報)を扱い、プライベートな情報を利用した個人特化型サービスが求められる。ネットワーク階層を上がるにつれ、対象は個人から、住戸、街区、都市へとなるが、それにつれ、各個人の情報ではなく、全体としての大まかな情報が重要となる。つまり、情報の匿名化度合いに地域性が存在する。その他、要求計算コストや通信スループットなども同様に地域性が存在する。図 2 は代表研究責任者が IEEE P2413 および IEEE-SA Smart Grid Vision Project Document において提出した図を再構成した図であり、この地域性を元に、様々なスマートコミュニティサービスを適所にマッピングしている。この図において、例えばプライベートな情報を扱う場合は、クラウドではなくエッジで処理するべきと判断される。

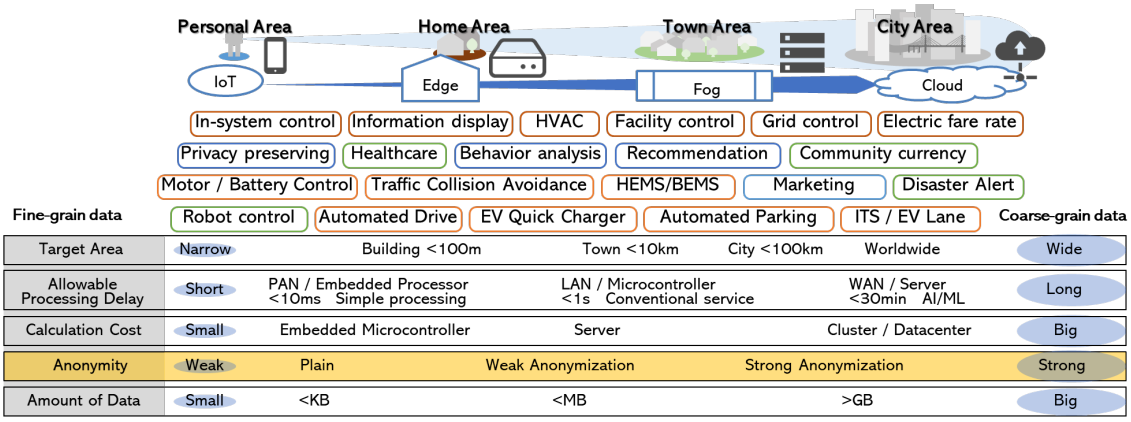


図 2 ネットワーク階層とスマートコミュニティサービスの適材適所実行

図 3 は、同様に IEEE-SA Smart Grid Vision Project Document で記述した図を基に、Wi-Fi および BLE ドメインについて追記した図である。各ドメイン内での情報把握が可能になる。なお、本研究における実証実験では、この規模の実験を行えないため、地域に独自の Wi-Fi 無線網および BLE 無線網を設置し、それらのステーション、さらにはステーションを束ねるハブに ASCA エッジを併設した環境を構築する。これを実証実験環境とする。図 3 のように、PON における同一 OLT の接

続範囲や、無線通信のサービス範囲は、その地域性を利用する上で効率が良いことがわかる。情報のカプセル化を達成するために、各エンドデバイスが、データをどこに送るかを把握して匿名化の手法や基準、つまり匿名化の強度を切り替えるのは非現実的である。透明アドオンを利用し、透明な情報のカプセル化を行えば、比較的容易に対応できると考える。将来、PON では NTT の局内の OLT を起点とする 50 軒程度の共通接続された近隣グループ、移動体通信網などの基地局を中心としたセル内端末群を基本とするグループを対象としたサービスの構築が想定できる。

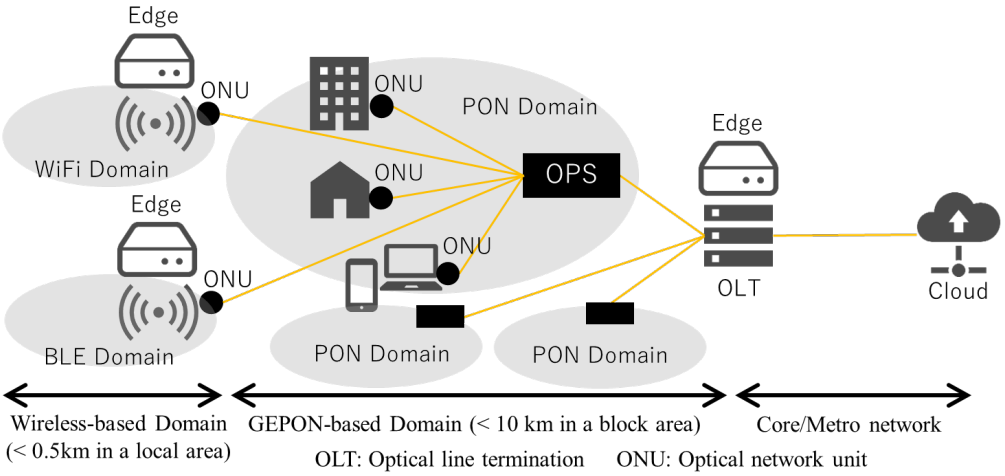


図３ エッジコンピューティングノードによる処理ドメイン

これらの、課題に対する対応策と目的および研究内容は次のとおりである。

地方自治体は地域住民の情報の重要性を認識し、その情報を利用して関連する将来の問題を予見し、かつその対応策を事前に見出すべきであり、この対応策の構築が、Society5.0 実現の重要課題の一つといえる。ここまで述べた課題に対する本研究の対応策は、次の(i)インフラ・サービスの永続化、(ii)情報匿名化の理解、(iii)匿名化データの利用許諾に整理できる。以下、順に説明する。

代表研究責任者らはさいたま市と共に、地域密着型の情報銀行を用いた現在および未来社会における問題解決や永続的な地域自治の維持について議論している。現時点の情報銀行運用は、地域住民の個人情報を含む様々なデータを Opt-In で取得、管理運用し、このデータを地域住民サービスへと転化して提供し、地域産業発展にも貢献するという形態である。すなわち、そのサービス提供によって得られた対価を情報提供者に還元しつつ自己運用資金とすることを前提にしている。この形態を応用すれば、上記の将来の情報インフラが解決するべき問題を含む、様々な社会問題を解決できる可能性がある。

前提として、先に示した実証実験環境により、街区にエッジノードが分散配置されている状況を想定する。そのエッジノードに実装された ASCA によりエンドデバイスから流れるパケットを再構築し、パケットに分割されていない元の情報、つまりストリームを獲得する。このストリームを用いて情報の流れを検出し情報銀行で管理する。この管理された情報群を用いれば、地域外からのデータアクセスや、地域内の関連行動を把握することができる。このデータアクセスの把握や域内行動の把握を元に、例えば、該当する情報の利用を制限する、該当する情報の利用に対する対価を得る、当該商業活動に対する課税の負担額を決定するなどの対応が可能となる。域外に対しても、透明な情報のカプセル化を実施すれば、外部からは匿名化された情報のみ取得できる。また、なにかしらの対価を支払った場合に透明アドオンにより緩い匿名化を行うことや、安全のため暗号化した平文データを提供

することも可能である。

なお、本研究は、既存デバイスへの変更を避け、末端デバイスコストの増大を防ぐこと、つまり導入や運用上の障壁の低減を図る仕組みの構築を前提としており、極端なケースでの情報取得漏れや、鍵共有を拒否するクラウドへの完全な対応は想定していない。これらは地方自治体による政策との両輪で対応し、技術的進歩と共に解決を図るべきと考える。購買情報、EV 充電・走行情報など、クラウドへのデータ搬出があれば、これを検出し、後述する秘密計算を用いて、秘密裏に情報銀行で管理することができる。この仕組みに従えば、経済の中心になりつつある情報通信インフラにおけるデータ流通に対して、受益者負担の原則を適用することが可能となり、先に述べた収益化や課税の問題に対して一石を投じることができると考える。すなわち、情報銀行運用および提供する㈠インフラ・サービスの永続化に通じ、地方自治の永続化にも寄与する。

次に、㈡情報匿名化への理解と㈢匿名化データの利用許諾について述べる。情報銀行を地域で運用する目的の一つは、様々な情報を保有し、有用な情報に加工し、安全に情報の二次利用サービスを提供すること、そして収集した情報の価値を高めると共に地域産業に貢献し、提供者に利益を還元することである。個人情報が含まれるため、基本的には Opt-In による情報収集と提供が行われる。しかしながら、この方法では、新たなサービスを提供するたびに Opt-In を取り直す必要があり、利用者の手続きが煩雑となる。改正個人情報保護法では、適切な情報匿名化を行うことで、同意を得ずともデータの二次利用が可能になると定められており、その匿名化のガイドラインも別途示されている。しかしながら、実際に取得したデータの二次利用を行う際には、データの利用者の立場に立ち、新しい概念である匿名化に対して使用者が抱く不安や、匿名化基準の誤用などの心配を払拭しなければならない。また、匿名化データの活用に対する信頼も獲得しなければならない。そこで、㈡情報匿名化への理解と㈢匿名化データの利用許諾という観点で、理解しやすい運用を可能とし、利用者の信頼を得ることで、データ利用の活性化を促す。

㈡情報匿名化への理解とは、匿名化という新しい技術について、シンプルでわかりやすい、統一された安全度合いとしての匿名化基準を与え、利用者がその匿名化基準を理解し、比較を易化することである。加えて、インセンティブやロイヤリティ、サービスの質との比較判断を行いやすくすることである。利用者は匿名化基準を知ることで、異なる基準で匿名化された異なるデータ間の価値を比較できるようになる。一般に、データの形式の違いや利用目的の違いによって異なる匿名化手法が適用されるが、そのような場合でも匿名化度合いを比較できる技術が求められる。これは、情報銀行をあえて情報信託銀行と呼ぶならば、その価値の明確化と提示は、信託銀行が投入資産や投資先の違いによる統一化された価値を明確化するのと同様、当然のことである。

しかしながら、様々な匿名化における新手法が提案されている一方で、匿名化度合いが客観的かつ明確に与えられていない提案も少なくない。単に匿名化した情報と平文データとが異なるという結果では、どのようなケースかつどのような確率で個人が特定されるかという指標が不明瞭であることを意味する。これは説明可能な匿名化ではないため実利用に耐えない。基準が明確で説明可能な匿名化が求められている。

㈢匿名化データの利用許諾とは、匿名化手法や匿名化基準といった個別の配布条件を、情報提供者自らが自由に選ぶことができるようにすることを意味する。これには、利用者の負担をなるべく軽減した形で、柔軟かつ多角的な Opt-In、Opt-Out の実施が必要となる。通常の信託銀行においても、預かった資産を運用する上で、その運用手続きのたびに預金主の許諾を取るような運用は受け入れがたい。情報信託銀行も同様に、正しく匿名化された情報を自由に運用でき、かつ、情報提供主がいつ

でも運用状況を監視、管理できれば、情報信託銀行と情報提供主の双方の利便性が向上する。

ここで、(iii)匿名化データの利用許諾に関して、現状での対応について述べる。現在、さいたま市では、代表研究責任者が提案した Vendor and Consumer Relationship Management (VCRM)による運用が行われている。VCRM は一般的な Consumer Relationship Management (CRM)と、近年注目されている Vendor Relationship Management (VRM)を包括的に管理する仕組みである。CRM は、サービス提供者が、顧客を契約や利用料徴収など、サービス提供契約を管理し、それに基づいて実際にサービス提供を行う仕組みを意味する。VRM は、顧客がサービス提供者に対してどの情報をどのように渡すかといった、サービス提供の主体や仕方を管理する仕組みを意味する。VCRM の構造を図４に示す。VCRM により、サービス提供者とサービス利用者は一つの Relationship という管理エントリにより、その契約、利用料、データの提供方法、付随する処理などの情報が保持され関連付けられる。Relationship の構築は Opt-In、その変更は Opt-Out と見做すことができ、理想的には全ての情報取引について Relationship を管理する。つまり、データ提供者は常に提供するデータをどのサービス提供者のどのサービスが利用しているかを知り、また制御でき、それぞれについて、例えば匿名化基準を変更したり、利用できるデータに制限を与えたりすることができる。

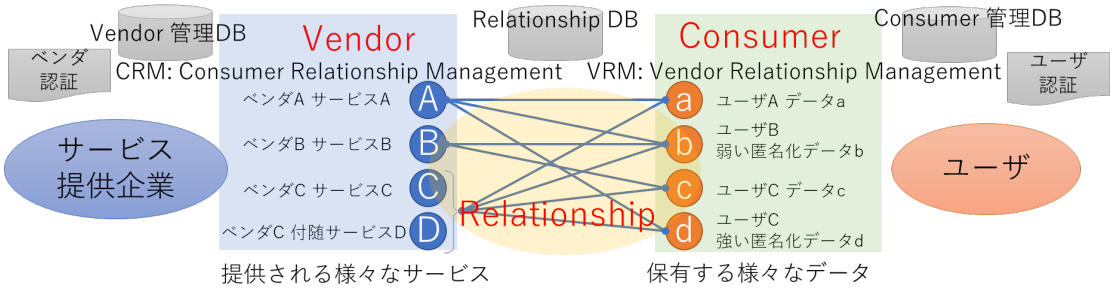


図４ VCRM のアーキテクチャ

サービス提供企業は、提供されるデータの質や価値を評価し、それに従ってサービス提供時の品質保証や、利用料金もしくは、提供ロイヤリティの決定を行うことができる。つまり、この匿名化基準は、情報銀行におけるデータのプライシングに影響する。平文データは個人情報がそのまま残留するが、価値は最も高い。匿名化度合いが増すに従いデータがオリジナルの状態から乖離していくため個人情報の残留率は低下し個人の特定が困難になるが、価値は低下する。さらに、情報銀行のユーザでありデータ提供者にとっても、データの価値と価格バランスを見ながら匿名化基準を選ぶことができるようになる。このように、VCRM は情報銀行が備えるべき基本機能である。本研究では、VCRM の管理情報を更新し、機能追加して課題解決を図る。ここで、本研究で構築するシステムの全体像を図５に示す。エッジが果たすべき役割の一つが、サービス提供遅延の低減にあることから、情報銀行のデータストレージを介してデータを取得する以外にも、データフィルタにおいて適切な匿名化などの処理を ASCA で行い、そのままサービスアプリケーションに投入するパスも想定する。この場合も、VCRM の制約に従って動作することで、全体の管理において齟齬なく運用できる。

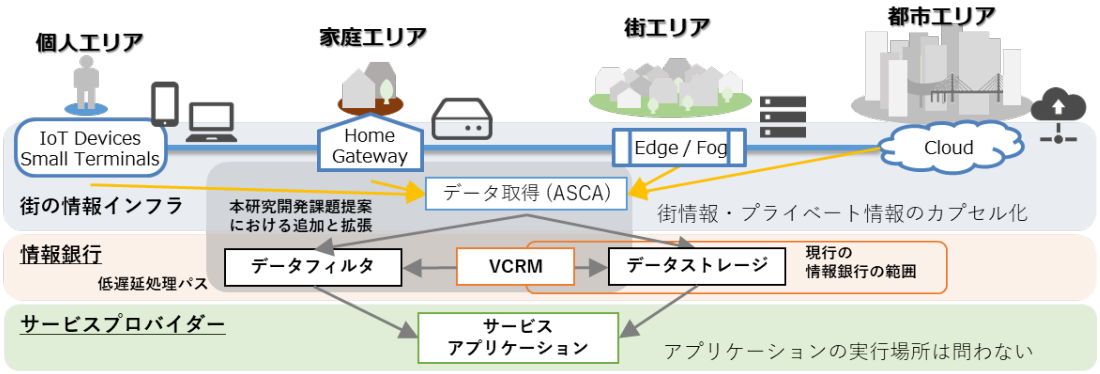


図５ 構築システムの全体像

この(ii)情報匿名化への理解と(iii)匿名化データの利用許諾を達成することで、情報銀行の利用者である地域住民との相互の理解や信頼に結び付くと考える。以下、具体的な実施内容を述べる。

以上より、到達目標および実施内容を次のように定める。

VCRM と周辺情報インフラとの融合による情報銀行機能の強化を図るための本研究における到達目標としての３つの研究開発要素は以下のとおりである。

(1) 情報取得を集約しフローとして管理する仕組みの構築
(2) 情報を公開し利用を促進させるために必要な情報匿名化処理
(3) 情報を秘匿し特定の利用を達成するために必要な秘密計算処理

(1)の内容が(iii)匿名化データの利用許諾における新しい概念の導入に寄与し、(2)の内容が(ii)情報匿名化への理解につながる統一的な指標の導入に寄与する。(3)の内容が安全な匿名化処理の実現やアカウンティング管理を可能とすることから、情報銀行運用の幅を広げ、必須インフラへの昇華につながり、結果として(i)インフラ・サービスの永続化に寄与する。なお、情報通信インフラが絡む経済活動における受益者負担の徹底など、地方自治の安定運用を可能とする地域社会制度改革は、本研究の評価項目や到達目標ではなく、長期的観点での当該研究分野の最終目標である。(iii)の匿名化された情報を利用する際の許諾を司る仕組みを構築し、また、その上で(ii)の共通の評価基準を持たせることで相互比較可能とし、その仕組みを内包した情報銀行による、地域サービスの提供という短期的観点が、本研究における研究開発期間内の評価項目であり到達目標である。以下、(1)、(2)、(3)の各実施内容と到達目標を述べる。なお、各項目について実証フェーズが存在するが、これについては最後にまとめて記述する。また、ここに記した内容を元に、後述する「3. 研究開発計画」における具体的な研究開発項目を設定する。

（２）研究開発期間
令和２年度から令和４年度（３年間）

（３）受託者
学校法人慶應義塾＜代表研究者＞
フェリカポケットマーケティング株式会社
学校法人早稲田大学（令和２年度から令和３年度まで）

（４）研究開発予算（契約額）
令和２年度から令和４年度までの総額 30 百万円（令和４年度 10 百万円）

※百万円未満切り上げ

（5）研究開発項目と担当

以下、法人名について以下の略称を用いる
学校法人慶應義塾：慶應
フェリカポケットマーケティング株式会社：FPM
学校法人早稲田大学：早大

研究開発項目１　情報取得集約・フロー管理機構の構築
研究開発項目 1-1　情報検出・集約・流通把握と VCRM 統合（慶應）
研究開発項目 1-2　情報検出・集約・流通把握の実証（慶應）

研究開発項目２　情報公開・利用を促進する情報匿名化処理の構築
研究開発項目 2-1　位置・多次元・テキスト情報匿名化（慶應）
研究開発項目 2-2　匿名化サービス提供実証（FPM）

研究開発項目３　匿名・会計利用を達成する秘密計算処理の構築
研究開発項目 3-1　秘密計算を用いた情報銀行機能の拡張
（令和３年度まで早大、令和４年度は慶應）
研究開発項目 3-2　秘密計算サービス提供実証（FPM）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	8	1
	その他研究発表	44	18
	標準化提案・採択	152	55
	プレスリリース・報道	0	0
	展示会	9	2
	受賞・表彰	0	0

（7）具体的な実施内容と最終成果

研究開発項目１　情報取得集約・フロー管理機構の構築

研究開発項目 1-1　情報検出・集約・流通把握と VCRM 統合

個人情報の扱いに対する不安を取り除くため、情報のカプセル化を実現した。この機能は、エッジがドメインを出入りする情報を掌握し、ノードの不足機能を補足・機能追加する仕組みである透明アドオンを利用して実装された。

研究開発項目 1-2　情報検出・集約・流通把握の実証

統一インフラの構築においては、フロー管理、すなわち情報流通管理として、透明アドオンによるフローセンサでフロー・情報を解析し、情報流通におけるコンプライアンスをチェックする機構を構築した。このフロー管理や情報のカプセル化など、エッジの機能を多用するが、結果的にエッジの負荷が増大し運用が困難となることも想定される。そこで、エッジを分散配置した環境を想定し、そのエッジ間の負荷分散も透明に行う柔軟な負荷分散手法を構築した。これは、ダイナミックなプロセス・データマイグレーションとフロー制御を組み合わせて実現される。また、完全独自な仕組みではなく、都市 OS としてしばしば利用される FIWARE を拡張した。クラウド中央集権的 FIWARE は個人情報

の扱いにおいて不利であり、この問題が解決される。

研究開発項目３　匿名・会計利用を達成する秘密計算処理の構築

研究開発項目 3-1　秘密計算を用いた情報銀行機能の拡張

匿名化について、ドメイン内秘密・ドメイン外分散暗号を利用し平文情報を渡さずに比較的低コストに DP または k 匿名化する技術を構築した。さらに、多次元情報の匿名化は従来困難であり、アプリケーションに即してそれぞれ検討する必要があるが、位置・時間の連続である経路情報、文章情報など多次元情報の匿名化手法を構築した。加えて、匿名化したからといって安全というわけではなく、その利用には、個人情報保護で必要な誰が、どの目的でだれに情報を提供したのかを明らかにし、関連する利用規約事項を遵守させる必要がある。そこで、匿名化の多様性を利用して、これらの情報を匿名化の際に透かし込む技術を構築した。これは、いわば、情報に色を塗って区別することを意味し、情報のカラーリングを達成した。

研究開発項目 2-2　匿名化サービス提供実証

API を提供し構築インフラと連携可能とした。統一インフラの構築をはかり、サービス提供・移動を自由化した。各地方自治体が個別のインフラを作るのはコストがかかるが、都市 OS として著名な FIWARE を基本とし、不足機能を実装した。また、情報共有の基本であるオプトイン・オプトアウトをデータだけでなく、フローについても管理・設定可能とし、情報流通監視・制御など技術的に管理運用する仕組みを構築した。法的制約を人為的解決だけで達成することは困難である。技術面でのサポートを可能とし情報管理対応を易化した。

研究開発項目３　匿名・会計利用を達成する秘密計算処理の構築

研究開発項目 3-1　秘密計算を用いた情報銀行機能の拡張

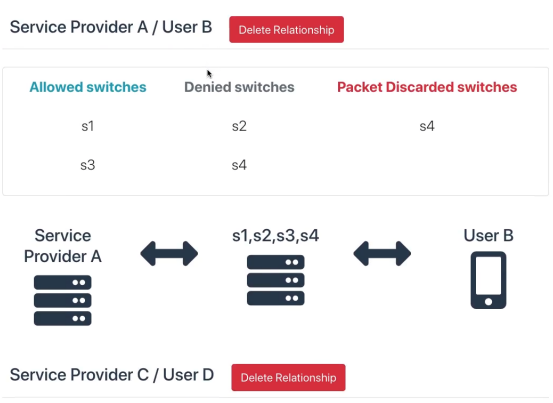
以上の技術構築により、個人情報の取り扱いを易化した。情報のカプセル化で重要情報を外部に渡さなくともよく、外部に出す場合も匿名化されるため不用意に情報が漏えいされることを阻止し、専門技術である暗号化をアウトソーシングする際でも、生データを渡さなくともよい技術を構築した。さらに、GDPR など法令対応を技術で緩和した。例えばシートベルト着用義務に対して未着用警告を搭載したのと同様に、許可されない個人情報交換に対して警告が可能であり、安心してデータ流通を行うことが可能となる。また、仮に情報が漏えいしてもこれを検知でき、正しく対応できる。

研究開発項目 3-2　秘密計算サービス提供実証

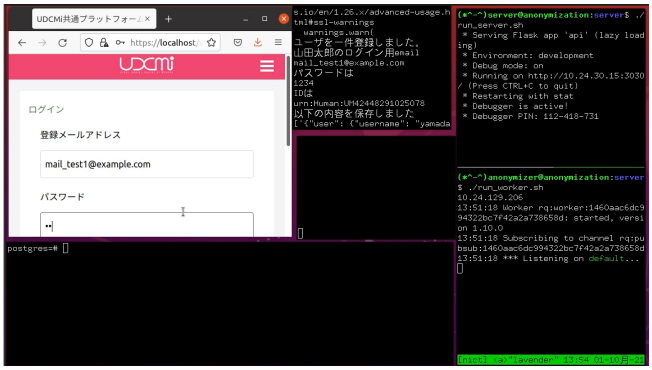
実際にデモシステムを構築し、実データを投入したオペレーション評価を行った。当該評価によりスループットの確認や全体動作の確認を行うことができた。

まず、柔軟な負荷分散およびフロー管理として、次の図に示すように、複数の域内 IoT ノード、ここではスマートメータ情報をエッジにおいて匿名化しつつ情報のカプセル化を達成しながら集約し、これらのフローを VCRM で管理するとともに、各エッジ処理の制御を行うデモ画面（画面 1）である。実際の情報流通は、専用のオペレーション画面を利用して確認・制御を行うことができる（画面 2）。また、情報を提供し、サービスベンダーがこれを利用、レコメンドサービスをユーザに提供する際の全体のオペレーションと、ユーザおよびベンダーからみた操作画面の一覧を画面３に示す。左上に web オペレーション画面、その下にフロー管理テーブルのエントリを管理する DBMS のログ画面、中央上が FIWARE のオペレーション画面、その下がエッジノードのコンテナ実行ログ、右側上が匿名化サービスエッジの実行画面（上下２つ存在）を表している（画面３）。電力レコメンドアプリや購買アプリを実装した（画面４）。レコメンデーションサービスとして、新たに No-Code/Low-Code で匿名化機能付きレコメンドアプリを設計可能なツールを実装（画面 5）、匿名化によるサービス品質と利益を勘案可能な機能を搭載した。また、実運用されているスーパーリージョナルアプリ「よむすび」と連携させた（画面 6）。使用感アンケートでユーザ・サービス提供者共に良好な結果を得た。

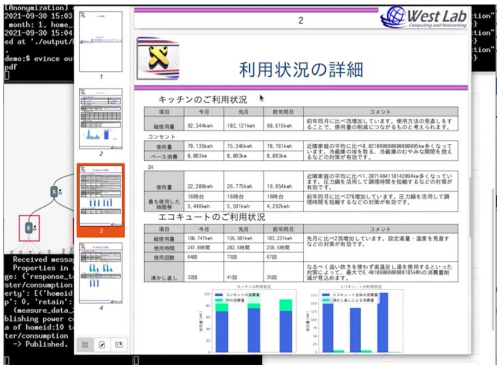
画面１



画面２

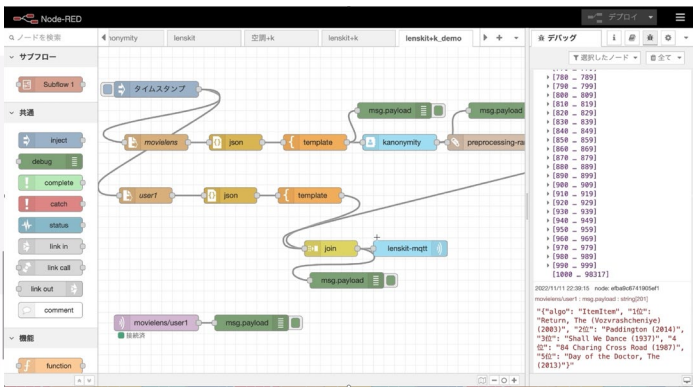


画面３



画面４

画面５



画面６

（8）研究開発成果の展開・普及等に向けた計画・展望

⑴ 上記技術標準化 WG の活動を継続し、AdCOM 投票を終えた IEEE SA P1451.0 については最終承認待ち、IEEE SA P1451.1.6 についても最終ドラフト執筆、間もなく AdCOM 投票へと進む。これまで検討していた UDCMi に限らず、高松市なども検討を進めたが、おもてなし ICT 協議会によりその他複数の地方自治体を巻き込んだサービス実装が計画されている。

⑵ 様々なアプリケーションが想定されているが、新たにスマートアグリ応用の利用検討が進められている。営農情報などはプライベートな情報でありながら、その共有は生産品質や量の獲得に重要となるためである。

⑶ 既に実証は進められているが、今後も継続して実証し、FPM に限らず、ソフトバンクといった企業との連携も進んでおり、今後提案インフラの展開が進められる。