「マルチメディア，分散，協調とモバイル
(DICOMO2016)シンポジウム」 平成28年7月

来歴情報を用いた複数システム間でのデータ追跡に関する一提案

毛 かい毅[1] 伊藤 俊夫[1] 金子 雄[1]

概要： ICT の浸透に伴い，企業の壁を超えたデータの共有によるサービス連携が注目を集めている．しかし，企業が保有するデータの中には，個人情報や機密情報が含まれる場合がある．こうしたセンシティブな情報を，複数の企業のシステム間で安心かつ安全に流通させるために，情報の漏えいや不正利用などを防ぐ対策が必要になる．同時に，情報漏えいが発生した場合の流出元や流出経路，影響範囲を素早く特定できる仕組みを築く必要もある．本論文では，複数の企業のシステムに跨ったデータ交換における，データのトレーサビリティを提供するためのシステムを提案する．提案システムは，システム間で共有するデータを常に暗号化し，暗号化のための鍵をデータ操作前後のハッシュ値や操作ログなどの来歴情報から生成することによって，各システムにおけるデータの操作履歴をトレース情報として強制的に記録できる．記録された一連のトレース情報に基づき，「データ配布における派生経路の追跡」と「データ流出における流出元の特定」を実現する．

A Proposal for Tracing Data Across Multiple Systems using Provenance

KAIYI MAO[1] TOSHIO ITO[1] YU KANEKO[1]

1. はじめに

近年，IT インフラの充実やクラウドサービスの普及に伴い，様々な業界のあらゆる情報が電子化され，社会全体に蓄積されるデータの総量が飛躍的に増大している．米国の調査会社 IDC の報告[1]によると，世界中のデータ量は 2 年ごとに倍増し，2020 年には 44 兆ギガバイトに達すると予想されている．そこで，多くの企業は，自社のシステムに眠っている膨大なデータに着目し，それらを活用したイノベーションに期待している．日本においても企業の国際競争力を確保するため，この数年で国を挙げてデータの活用を推進している．その活動の一つに，分野や企業の壁を超えたデータの共有によるサービス連携への取り組みがある[2]．例えば，鉄道会社と IT 会社が連携し，交通系 IC カードの乗降履歴を，駅におけるエリアマーケティングに活用するサービスが検討されている．

一方，企業が保有するデータの中には，個人情報やパーソナルデータなど機密性の高い情報が含まれる．パーソナルデータとは，個人情報に限らず，位置情報や購買履歴など個人識別性のない情報も含まれた「個人に関する情報」を指すとされている[3]．パーソナルデータは顧客から直接に得られるデータであるため，価値の高いデータとも言われている．近年，ヘルスケア情報や電力利用情報も，重要なパーソナルデータとして，企業間連携により活用される可能性が高まっている．

しかし，企業において，こうしたセンシティブな情報が含まれたデータを共有する際に，以下の 2 つのリスクが存在すると考えられる．

- 法令違反のリスク

昨年改正された個人情報保護法によって，パーソナルデータから，個人を特定ができないように個人情報を匿名化することで，本人の同意なしの第三者提供や目的外利用ができるように緩和された．しかし，不十分な匿名加工や，外部情報との突き合わせにより，個人が特定される可能性が高いと指摘されている[4]．この場合，個人情報保護法に抵触する危険性があり，結局，匿名化にも関わらず，事前の本人同意を取得せざるを得なくなる．

- 風評被害のリスク

個人情報漏えいなどのセキュリティ事故が発生している今，プライバシー保護に対する意識が社会全体に浸透しつつある．パーソナルデータを扱う企業に対し，社会的責任を厳しく問う傾向が強まっており，法律を超えた対応を求めるケースも存在すると指摘されている[5]．一度，情報の漏えいに関わってしまうと，風評の被害に遭う危険性がある．

こうした背景から，企業はデータの活用について依然として躊躇している．上記のリスクに対応するには，技術

1 株式会社 東芝 研究開発センター

を通じてデータ提供者の安心感と納得感を得ることが重要である．センシティブな情報を，複数の企業のシステム間で安心かつ安全に流通させるために，情報の漏えいや不正利用などを防ぐ対策や，情報漏えいが発生した場合の流出元や流出経路，影響範囲を素早く特定できる仕組みが必要であると考えられる．

本論文では，複数の企業のシステムに跨ったデータ交換における，データのトレーサビリティを提供するための方法を提案する．以降，2 章で複数システム間データ追跡の問題と課題を説明する．3 章で提案システムの詳細について説明する．4 章でデータ共有の事例に基づき，提案システムの実用性について考察する．5 章で関連研究について述べ，最後に 6 章でまとめる．

2. 複数システム間データ追跡の問題と課題

前述のように，複数の企業のシステム間のデータ共有において，データの提供者の，情報の漏えいや不正利用などのリスクに対する不安が高まっている．この一因は，データの流れを正確に把握できないためだと考えられる．特に，複数のシステムに跨って，データが二次利用，三次利用されるような場合においては，このような問題が益々複雑になり，企業間のデータ共有に支障をきたす恐れがある．

我々が想定した複数の企業間のデータ共有のシナリオを図 1 に示す．

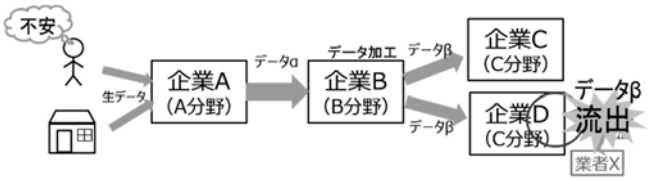

図 1：複数の企業間のデータ共有のシナリオ

1. 企業 A が生データを取集し，その一部（データ α）を企業 B に提供する．
2. 企業 B がデータ α をデータ β に加工し，企業 C と企業 D に提供する．
3. 企業 C と企業 D のどちらかがデータ β を業者 X に不正流出する．

こうしたシナリオにおいて，データの提供者は以下のような不安を抱くと考えられる．

- 自分のデータがどんな形で加工され，誰に渡され，どういう目的で利用されるかがわからない．
- データの不正流出が判明した場合，自分が関わっているかどうかがわからない．

データ共有に関わる企業らは，データ提供者の信頼を得るために，データの流れを正確に説明できる必要がある．しかし，各システムの運用者が異なる場合，自分のシステムから離れたデータを追跡するのは困難である．

そこで，我々は，「運用者が異なる複数のシステムに跨るデータ共有」を行う状況において，データの提供者を安心させるために，以下の 2 つの課題を解決するシステムを提案する．

課題 1：データ配布における派生経路の追跡

課題 2：データ流出における流出元の特定および流出経路の遡及

3. 提案手法

3.1 コンセプト

本提案のコンセプトは，システム間で共有するデータを常に暗号化し，暗号化のための鍵を来歴情報に関連付けることで，各システムにおけるデータの送信，編集，削除等の操作履歴を確実に記録することである．データの来歴情報とは，データの完全性やデータの起源を証明可能な操作履歴の記録である．

3.2 システム構成

本提案のシステムを用いてデータ配布（送信）の例を図 2 に示す．

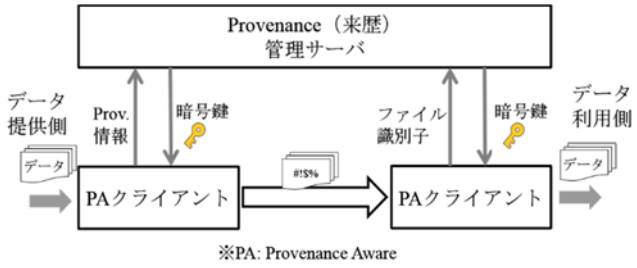

図 2：データ追跡に関わるシステム構成

提案システムは，来歴情報を管理するサーバと，来歴情報を提供する複数の PA（Provenance Aware）クライアントで構成される．来歴管理サーバは，PA クライアントから送られてきた来歴情報を用いて，暗号鍵を生成する．PA クライアントは，この暗号鍵でデータを暗号化して配布する．データを利用する際は，暗号鍵を来歴管理サーバから取得して，データを復号する．

3.2.1 来歴管理サーバの概要

来歴管理サーバは，サーバ上で実行するアプリケーションであり， PA クライアントの認証，PA クライアントから来歴情報を収集，収集した来歴情報を DB に蓄積などの機能を備える．

PA クライアントの認証とは，PA クライアントのなりすましなどを防ぐために，来歴管理サーバと通信する各 PA クライアントの真性を確認することである．認証の手法は，既存技術の利用を想定する．例えば，ID とパスワードや電子証明書，セキュリテトークンによる認証手法がある．来歴情報の信頼性を担保するため，強い認証方式の採用が望ましい．

来歴管理サーバは，PA クライアントとの通信によって，来歴情報の収集や，暗号鍵の配布を行う．来歴管理サーバと各 PA クライアント間の通信経路は，広域ネットワーク

を想定する．来歴情報や暗号鍵の改ざんや盗聴を防ぐために，通信経路の信頼性が要求される．本提案では，既存のネットワークセキュリティ技術，例えば，TLS 等により通信経路の信頼性を確保する．

また，来歴管理サーバは，来歴情報の解析，来歴情報から暗号鍵の生成，来歴情報に基づいたデータ追跡なども行う．これらの来歴情報の処理の詳細は，3.3.5 節で説明する．

来歴情報を蓄積する DB（来歴記録用 DB）では，PA クライアントから送られてきたすべての来歴情報を記録する．来歴管理サーバは，一つの来歴情報の記録に対して，一つの管理 ID を付与する．また，各来歴情報の有効/無効/処理中などの状態を示す状態フラグを管理する．本提案において，来歴記録用 DB はリレーショナルデータベース（RDB）の利用を想定する．

3.2.2 PA クライアントの概要

PA クライアントは，パソコンなどのデバイス上で実行するアプリケーションであり，データの操作や暗号化処理，来歴情報の生成および送信を担う．なお，PA クライアントは，データを利用する各システムに導入することを想定する．

PA クライアントは，PA クライアントで行われる各種のデータ操作に基づき，来歴情報を生成して来歴管理サーバに送信する．来歴管理サーバとの通信経路の安全性は，前述の TLS などの既存技術で担保される．

PA クライアントは，来歴管理サーバから受信した暗号鍵を用いてデータを暗号化/復号化する．暗号方式は，例えば，共通鍵暗号の AES を利用する．また，暗号化したデータのハッシュ値を算出する．ハッシュアルゴリズムは例えば MD5 を利用する．

PA クライアントは，データを操作するためのインタフェースを備える．データの送信，表示，編集，削除などの操作が可能である．

3.2.3 来歴情報の構成

来歴情報は XML 形式で記述される．来歴情報の構成を図 3 に示す．

```
<Provenance>
        <org_pa>
                PA_CLIENT_1
        </org_pa>
        <mod_pa>
                PA_CLIENT_1
        </mod_pa>
        <org_hash>
                1024748A371533F0B703578531FF8
         </org_hash>
        <mod_hash>
                0CC01B3FC6A9196EC78524DAD4C1C450
        </mod_hash>
        <mod_time>
                2015-12-01 00:00:00
        </mod_time>
        <op_type>
                MODIFY
        </op_type>
</Provenance>
```

図 3：来歴情報の構成

来歴情報の各要素を簡単に説明する．

- org_pa：操作前の PA クライアント ID
- mod_pa：操作後前の PA クライアント ID
- org_hash：操作前のデータのハッシュ値
- mod_hash：操作後のデータのハッシュ値
- mod_time：操作の時刻
- op_type：操作の種類（SEND/MODIFY/DELETE 等）

3.3 動作詳細

提案システムは，データの送信（配布），表示，編集，削除等の操作に対して，来歴管理サーバと PA クライアントが連携し，来歴情報の交換および記録を行う．その後，記録された一連の来歴情報に含まれたトレース情報に基づき，データの追跡を実現する．以下，データ操作別に，提案システムの動作ついて説明する．

3.3.1 データ送信動作

図 4 のシーケンス図に，提案システムにおけるデータ送信動作を示す．

送信側 PA クライアントは，データ送信の前に，今回の送信に関する来歴情報（送信元クライアント ID，送信先クライアント ID，送信前データのハッシュ値，操作種類，操作時刻など）を来歴管理サーバに送る．来歴管理サーバは，後述の「暗号鍵生成処理」に基づき，暗号鍵を生成し，PA クライアントに送付する．PA クライアントは，この鍵を用いてデータを暗号化し，暗号化したデータのハッシュ値を来歴管理サーバに通知する．来歴管理サーバは，後述の「操作後データ関連付け処理」に基づき，上記のハッシュ値を来歴情報に関連付け，来歴記録用 DB に記録する．

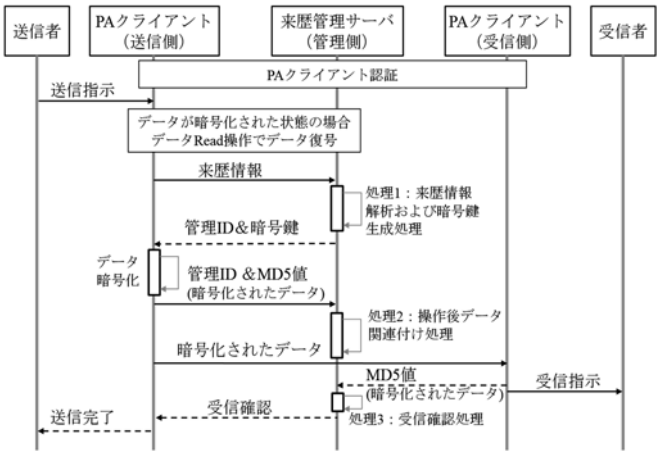

図 4：データ送信のシーケンス

この一連の処理が完了した後に，送信側 PA クライアントは，暗号化されたデータを受信側 PA クライアントに送信する．受信側 PA クライアントは，後述の「受信確認処理」に基づき，受信確認を行う．

こうした処理によって，データ送信に関する来歴情報を記録することができる．また，送信するたびに，来歴情報が変わり，暗号鍵も変わる．暗号化されたデータのハッシュ値が判明すれば，データ配布のルートの確認ができる．

3.3.2 データ表示動作

図 5 のシーケンス図に，提案システムにおけるデータ表示の動作を示す．

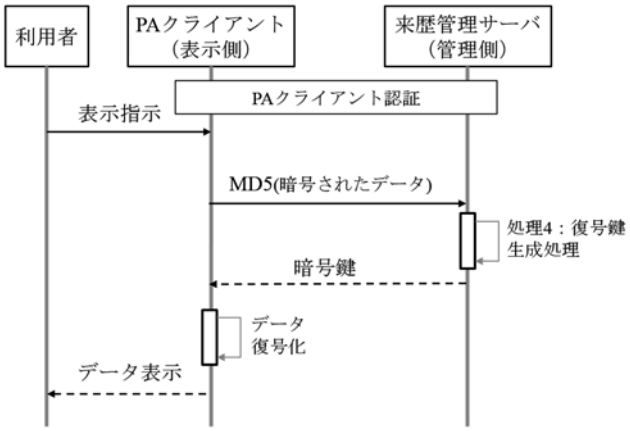

図 5：データ表示のシーケンス

表示側 PA クライアントは，暗号化されたデータのハッシュ値を来歴管理サーバに送る．来歴管理サーバは，後述の「復号鍵生成処理」に基づき，暗号化鍵を生成し，PA クライアントに送付する．PA クライアントは，この鍵を用いてデータを復号化して表示する．

3.3.3 データ編集動作

図 6 のシーケンス図に，提案システムにおけるデータ編集動作を示す．

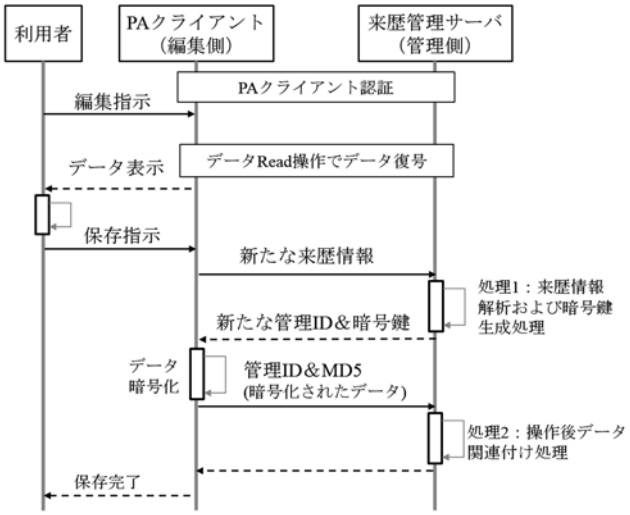

図 6：データ編集のシーケンス

編集側 PA クライアントは，編集を完了する後に，今回の編集に関する来歴情報（編集クライアント ID，編集前のデータハッシュ値，操作種類，操作時刻など）を来歴管理サーバに送る．来歴管理サーバは，後述の「暗号鍵生成処理」に基づき，新たな暗号鍵を生成し，PA クライアントに送付する．PA クライアントは，この鍵を用いて編集後のデータを暗号化し，暗号化したデータのハッシュ値を来歴管理サーバに通知する．来歴管理サーバは，後述の「操作後データ関連付け処理」に基づき，上記のハッシュ値を来歴情報に関連付け，来歴記録用 DB に記録する．

こうした処理によって，データ編集に関する来歴情報を記録することができる．また，編集前後の来歴情報を関連付けることによって，加工されたデータの追跡も可能になる．

なお，データの新規作成や，データのサブセットの取得などの操作は，データ編集と見なし，このシーケンスに準拠する．

3.3.4 データ削除動作

図 7 のシーケンス図に，提案システムにおけるデータ削除動作を示す．

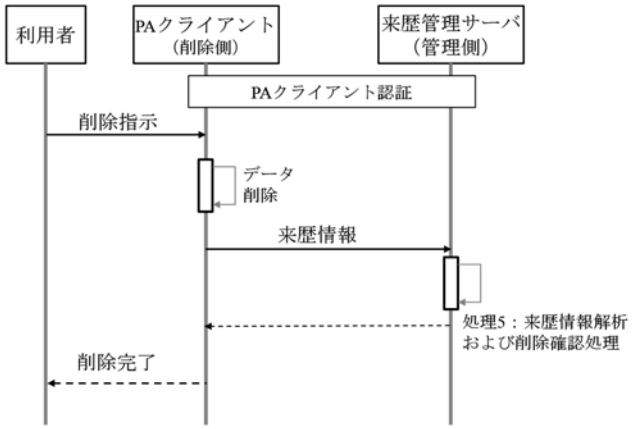

図 7：データ削除のシーケンス

削除側 PA クライアントは，データ削除した後に，今回の削除に関する来歴情報（削除クライアント ID，削除前のデータハッシュ値，操作種類，操作時刻など）を来歴管理サーバに送る．来歴管理サーバは，後述の「削除確認処理」に基づき，来歴情報を来歴記録用 DB に記録し，削除確認を行う．

こうした処理によって，データ削除に関する来歴情報を記録することができる．また，削除前後の来歴情報を関連付けることによって，削除されたデータの追跡も可能になる．

3.3.5 各サブルーチン処理

- 暗号鍵生成処理

PA クライアントから受信された来歴情報を解析し，管理 ID を割り付けて来歴記録用 DB に保存する．保存した来歴情報の状態フラグを「処理中」に設定する．そして，CMAC などの認証アルゴリズムを用いて，来歴情報から固定長の暗号鍵を生成する．本処理で生成された暗号鍵と来歴情報の管理 ID を PA クライアントに送信する．

- 操作後データ関連付け処理

PA クライアントから今回の操作に関する来歴情報管理 ID と，操作後のデータのハッシュ値を受信する．管理 ID で上記の「暗号鍵生成処理」で記録した来歴情報記録を検索し，操作後のデータのハッシュ値を追記する．こうした関連付けによって，来歴情報から操作前後のデータを確認できるようになる．

なお，来歴情報記録の状態フラグについて，操作種類が送信の場合，「処理中」のままで受信確認を待つ．操作種類

が編集の場合，「有効」に設定する．

- 受信確認処理

PA クライアントから受信データ（暗号された状態）のハッシュ値を受信する．ハッシュ値で来歴情報記録を検索し，受信側 PA クライアントの真性を確認した上で，来歴情報記録の状態を未確定から有効に設定する．本処理が完了後，送信側 PA クライアントに受信確認の指示を送信する．

- 復号鍵生成処理

PA クライアントから表示データ（暗号された状態）のハッシュ値を受信する．ハッシュ値で来歴情報記録を検索し，表示側 PA クライアントの真性を確認した上で，来歴情報から固定長の暗号鍵を生成する．暗号鍵の生成は「暗号鍵生成処理」と同様に CMAC を利用する．同一の来歴情報から同じ暗号鍵が生成されるため，共通鍵暗号の場合，この鍵で復号することができる．本処理で生成された復号鍵を PA クライアントに送信する．

- 削除確認処理

PA クライアントから受信された来歴情報を解析し，来歴記録用 DB に保存する．保存した来歴情報の状態フラグを「有効」に設定する．本処理の完了後，削除側 PA クライアントに削除確認の指示を送信する．

3.4 既知の制約

前述のように，各システムに導入される PA クライアントは，パソコンなどのデバイス上で実行するアプリケーションである．そのアプリケーションの耐タンパ性が要求される．特に，来歴情報の改ざん，暗号鍵の解読，データの不正保存，クライアント ID の偽造などの対策が必要である．今後，既存の技術の調査と共に，PA クライアントの耐タンパ性を検討する．

4. ケーススタディ

本章では，我々が想定するデータ共有のシナリオにおける具体例を挙げて，提案システムの効果および問題点を考察する．具体例として，HEMS（Home Energy Management System）で収集された電力使用データの活用事例を用いる．

4.1 事例の概要

電力全面自由化の背景に，一般家庭においてもスマートメータや HEMS の導入が加速している．HEMS は，電力供給側と使用側の協調，例えば，省エネの促進やピークカットなどを実現する重要な役割を担う．また，複数の HEMS を集約して効率的にエネルギーを管理するアグリゲータ事業者への期待が高まっている．アグリゲータの収益性を改善するために，HEMS で蓄積された電力使用データを企業間で活用して，新たなサービスを実現するための取り組みが行われている[6].

4.2 データ活用の問題点

電力使用データは，それを分析することで，個人や家庭の生活リズムまで明らかになり，活用価値が高い一方，プライバシー侵害のリスクが生じる．例えば，就寝時間や留守情報が把握できて，空き巣などの犯罪に悪用される可能性がある．2 章で述べたように，こうしたデータを，複数の企業のシステム間で共有する場合，データの追跡が複雑になり，データ提供者の信頼を得られない問題がある．

4.3 提案システムの考察

4.3.1 対象シナリオ

図 1 に相当する電力使用データ活用のシナリオを説明する．

- 企業 A に相当するアグリゲータは，複数の HEMS から各家庭の電力使用データ（生データ）を収集し，各家庭に対して省エネなどのサービスを提供する．
- アグリゲータは，一部の家庭の電力使用データ（データ α）を，企業 B に相当するデータ加工事業者に提供する．データ加工事業者は，電力使用データを各家庭の留守情報（データ β）に加工する，
- データ加工事業は，留守情報を企業 C に相当する宅配事業者と，企業 D に相当する警備事業者に提供し，配達やパトロールのルート最適化に利用される．

4.3.2 導入の効果

3.3 節で定められた動作によって，電力使用データの送信及び加工に関する来歴情報を強制的に記録することができる．上記のシナリオに関わる操作における来歴記録用 DB に記録される来歴情報（サンプル）を図 8 に示す．

管理ID	org_pa	mod_pa	org_hash	mod_hash	mod_time	op_type
1	PA_A	PA_B	null	HASH(データα)	(略)	SEND
2	PA_B	PA_B	HASH(データα)	HASH(データβ)	(略)	MODIFY
3	PA_B	PA_C	HASH(データβ)	HASH(データβ)_C	(略)	SEND
4	PA_B	PA_D	HASH(データβ)	HASH(データβ)_D	(略)	SEND

図 8：来歴情報サンプル

各来歴情報には，データ操作前後のハッシュ値（HASH(データ α), HASH(データ β), $\text{HASH(データ}\beta)_C$, $\text{HASH(データ}\beta)_D$）が記録されているため，これらの情報を用いて，2 章で述べた課題 1 の「データ配布における派生経路の追跡」と課題 2 の「データ流出における流出経路の遡及」を解決できる．

また，同じデータ β に対して，企業 C と企業 D に渡すデータの来歴情報が異なるため，$\text{HASH(データ}\beta)_C$ と $\text{HASH(データ}\beta)_D$ が異なる．万一，企業 C や企業 D からデータが不正流出した場合，課題 2 の「データ流出における流出元の特定」を解決できる．

従って，提案システムの導入によって，2 章で定義した課題を解決できると考える．

4.3.3 今後の課題

提案システムに関連するすべての操作は，PA クライアントを通じて行うことを想定する．しかし，ユーザが独自に実装したプログラムによるデータ加工などのニーズが存在すると考える．上記のシナリオにおいて，留守情報の推測やパトロールのルートの最適化を行うアプリケーションと，PA クライアントの連係が要求される．PA クライアントが

データ操作の API を公開することで，第三者アプリケーションとの連係が可能となる．その状況で，PA クライアントの耐タンパ性を確保することが今後の課題である．

5. 関連研究

既存の研究では，システム間のデータ追跡に関する様々な手法が提案されている．

ログ分析技術を用いてデータのトレーサビリティを実現する技術がある[7][8]. 各システムが収集した多量かつ多様なログをつなぎ合わせ，その中にあるトレース情報を解析することで,データの操作や移動などの動きを追跡する．しかし，異なるログ様式の連結や，不足情報の補完，ログ改ざんの検知などの課題が残されている．特に，運用者が異なる複数のシステムに跨る場合において，ログの収集は簡単にできないと考えられる．なぜなら，ログには技術ノウハウなどが含まれる可能性があり，他社に渡したくないためである．また，システムによって，ログの詳細度や可読性もバラバラである．こうしたログを収集しても，解析できない可能性があると考えられる．本論文で提案する手法は，専用のクライアントを用いて，データの来歴を特化したログ（来歴情報）を収集する．来歴情報からトレース情報を容易に解析できると考えられる．また，来歴情報のみ収集するため，技術ノウハウの流出リスクが少ないというメリットもある．

ファイルの操作ログを収集可能なプログラム（Viewer）及び同梱した専用の配信パッケージを用いて，データのトレーサビリティを実現する技術がある[9][10]．しかし，監視可能な対象は，元のファイルに限定されるため，加工後のファイルまたは再配布後のファイルの追跡は困難となる問題がある．本論文で提案する手法は，来歴情報を収集可能なクライアントを，データを利用するすべてのシステムに導入することによって，データを複数のシステムに跨っても，追跡が可能だと考えられる．また，来歴情報を解析することで，操作前後のデータの関連性が分かるため，加工されたデータの追跡も可能である．

匿名化したデータの漏えいを追跡する技術がある[11]. k-Anonymity アルゴリズムで匿名化したデータセットが流出される場合に，流出元を特定できるようになる．しかし，こうした手法も，匿名化したデータを集中管理する必要があるため，運用者が異なる複数のシステムに跨る場合において，各システムが自分でデータを管理したいため，十分に適用できない可能性がある．本論文で提案する手法は，データの集中管理を必要とせず，データの来歴情報のみを一元的に管理する．データを暗号化するための鍵を来歴情報に関連付けることで，上記の技術と同様に，複数のシステムに配布されるデータセットの流出における流出元の追跡ができる．

6. まとめ

本論文では，複数の企業のシステム間のデータ共有に着目して，データ提供者を安心させるための，来歴情報を用いたデータ追跡可能なシステムを提案した．提案システムは，データの暗号化鍵が来歴情報から生成されることを特徴とする．これによって，データの送信，表示，編集，削除等の操作に対する来歴情報の交換および記録を強制的に行うことができた．また，操作前後のデータのハッシュ値を記録することで，「データ配布における派生経路の追跡」と「データ流出における流出元の特定」を可能にした．

また，電力使用データ活用の事例を用いて，提案システムの導入による効果を確認した．本提案は，複数システム間でデータ追跡を実現するための初期検討の段階である．今後は，実用化に向けた課題として，来歴情報を生成する PA クライアントの耐タンパ性の保証の実現に向けた検討を進めていく．

参考文献

[1] IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, EMC DIGITAL UNIVERSE (online), available from <https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf> (accessed 2016-04-26)

[2] 経産省，分野・組織の壁を超えたデータ駆動型(ドリブン)イノベーションへの挑戦，データ駆動型イノベーション創出戦略協議会（オンライン），入手先 < http://www.meti.go.jp/press/2014/11/20141105002/20141105002c.pdf >（参照 2016-04-26）

[3] 総務省， パーソナルデータの利用・流通に関する研究会報告書，パーソナルデータの利用・流通に関する研究会（オンライン），入手先 <http://www.soumu.go.jp/main_content/000231357.pdf>（参照 2016-04-26）

[4] 佐藤一郎，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，情報管理，Vol. 58，No. 11，pp. 828-835（2015）

[5] 経産省，データ利活用の推進による新産業の創造，（オンライン），入手先 <http://ogc.or.jp/pdf/131202T_Mamiya.pdf>（参照 2016-04-26）

[6] 経産省，大規模 HEMS 情報基盤整備事業活動概要，（オンライン），入手先 < http://www.ienecons.jp/#prResult> （参照 2016-04-26）

[7] Shinichi, N. and Hidetaka, I., A study on the requirements of accountable cloud services and log management, APSITT 2010, pp.1-6 (2010)

[8] 中原慎一，張一凡，クラウドサービスの説明能力とトレーサビリティ技術，信学技報，Vol. 112，No. 22，ICM2012-8，pp. 81-85（2012）

[9] Yu Shyang, T., Ryan K L, K., et al., Tracking of Data Leaving the Cloud, 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), IEEE Computer Society, pp.137-144 (2012)

[10] Lokendra, V., Pallavi, G. and Awadheshwari, P., Optimized Method for Tracking of Data Leaving the Cloud Environment , International Journal of Computer Science and Information Technologie, Vol.5, pp.6389-6394 (2014)

[11] Shinsaku, K., Toru, N., Yutaka, M., Towards Tracing of k-Anonymized Datasets, Prof of IEEE Trustcom 2015 Workshops, IEEE Computer Society, pp.1237-1242 (2015)