個人情報の流通状況可視化方式の提案

菅友梨香[1] 吉村康彦[1] 山下高生[1] 大森芳彦[1]

概要： ユーザがネットワークを通じて提供されるサービスを利用する際，氏名，住所などの情報，閲覧履歴や購買履歴に関する情報を事業者に対して提供している．これらの情報は，事業者が管理し，流通や活用を行う権限を保持している．事業者に権限があることで，ユーザの意図しない流通や活用が行われる可能性があり，プライバシーの観点で問題がある．一方で，この権限をユーザに持たせた場合，ユーザの操作が増えることがあり，利便性の観点で問題がある．本検討では個人情報の流通状況の可視化を行うことで，ユーザが自身に関する情報の流通状況を把握し，制御できる状況を実現する．提案方式について，プライバシー保護のための機能，流通情報を制御する際のユーザの処理について評価を行い，プライバシー保護に関しては関連研究と比較して，履歴情報や二次流通まで含めるとより高い効果があり，利便性に関しては関連研究よりもユーザの処理を減らすことができる場合があることが分かった．

A Proposal of Visualization Method for Distribution Status of Personal Information

YURIKA SUGA[1] YASUHIKO YOSHIMURA[1] TAKAO YAMASHITA[1]
YOSHIHIKO OMORI[1]

1. はじめに

ユーザがネットワークを通じて提供されるオンラインサービスを使う機会が増えている．多くのオンラインサービスでは，ユーザはアカウントを作成する際に，メールアドレスやパスワード(登録情報)を登録することで，オンラインサービスを提供する企業(事業者)へ登録情報を提供する．登録情報は，氏名，住所，メールアドレスなどの個人を特定できる情報である．また，ユーザは作成したアカウントに紐づいて，サービスを利用する際に様々な履歴情報を提供する．履歴情報はメールサービスであればメールの内容，ショッピングサービスであれば注文内容など，登録情報の一部に紐づくことで個人を特定できる情報である．

登録情報に関して，事業者間で大量にやり取りされる場合があることや，それぞれの事業者がユーザからの登録情報を管理，分析しやすい登録情報を収集するため，ユーザはサービスごとに登録情報を使い分ける必要があり，ユーザが許可した覚えのない事業者が登録情報を保持しているといった，ユーザの意図に反していた場合ユーザから削除の要求を出す場合の手続きの手間があることなど，プライバシーや利便性の観点での問題がある．履歴情報は，オンラインサービス利用時のユーザの行動に関する増大し続ける情報である．履歴情報は，事業者にとってはマーケティングのために重要な情報である一方，ユーザにとっては日々の行動パターンなどが明らかになる情報であることから，プライバシーの観点での問題がある．

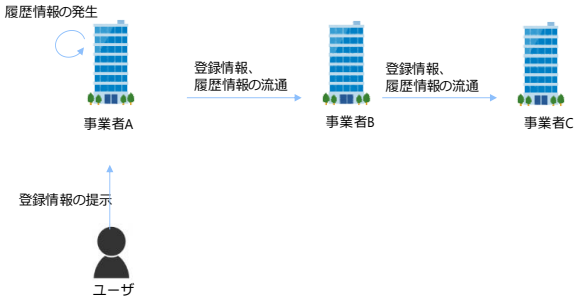

図 1 検討の範囲

Figure 1 Scope of study.

本稿では，多様なオンラインサービスに対して，前述のユーザのプライバシーや利便性の観点での問題を改善することを目的とする．

図 1 で今回の検討の範囲について説明する．事業者 A とユーザは，直接登録情報をやり取りするため，ユーザが，どの情報を提示するかを制御できる場合がある．事業者 A はこれらの登録情報と，実際にサービス利用時に発生する購入履歴や閲覧履歴等の履歴情報を関連づけて収集，管理する．これらの大量の情報(個人情報)はマーケティング等付加価値の高い情報であり，様々な事業者に流通し，二次利用されている．一方で図 1 の事業者 A から事業者 B，事

1 日本電信電話株式会社 NTT ネットワークサービスシステム研究所,〒180-8585 東京都武蔵野市緑町 3-9-11 NTT Network Service Systems Laboratories, NTT Corporation,3-9-11 Midori-cho,Musashino-shi,Tokyo 180-8585 Japan

業者 B から事業者 C への矢印で示される個人情報の二次利用に関しては，アカウント作成時に提示される利用規約への記載による周知のみであることも多く，ユーザはどこにどの情報が流通しているか把握することは困難である．

ユーザのプライバシーや利便性の観点での問題を考慮して登録情報をユーザから制御する取り組みがある．Microsoft が提案している Identity Overlay Network (ION)[1]では，登録情報をユーザが主体的に作成するユーザ用 ID である Decentralized Identifiers(DIDs)[2]に紐づけて管理することでユーザが登録情報をどの事業者に対して提供するか制御できる．DIDs と登録情報から個人を特定される場合があること，ION のシステムではユーザの行動によって発生する履歴情報について考慮されておらず，ユーザの行動に関する情報がユーザの把握できない部分で流出する恐れがあり，プライバシー保護の観点で問題がある．一度 DIDs を作成するとすべてのサービスで利用可能であるが，流通先がユーザの意図に反していた場合ユーザから削除の要求を出す場合の手続きが事業者毎に必要であるため，利便性の観点でも問題がある．Riverbed と名付けられている個人情報流通制御方式[3]では，登録情報に情報の流通に関する制約を定めたポリシーをユーザが付与できるシステムにより，ユーザが登録情報をどの事業者に対して提供するか制御できる．Riverbed のシステムはポリシーのみを管理するため，登録情報には関与しないが，ユーザの履歴情報，二次流通について考慮されていないためプライバシーの問題が解決されていない．ユーザは複数の事業者向けに一括して登録情報と，それの流通制約であるポリシーをルールとして管理しておくことができるが，ポリシーの設定の手間があり，利便性の観点でも問題がある．ユーザの登録情報を集中管理し流通状況をユーザへ知らせることを特徴とするシステム[4](以降，登録情報集中管理システムと呼ぶ)では，ユーザの登録情報をサーバに集中管理する．この集中管理サーバに事業者がアクセスし，ユーザからの許可があった場合のみ情報を受け取ることができる．このシステムでは履歴情報，二次流通について考慮されていないので，プライバシーの問題がある．また，ユーザは事業者毎に許可を行うので利便性の問題もある．

以上議論してきたように，関連研究において，登録情報のユーザと事業者間の流通については，プライバシーや利便性が一定レベルで考えられているが，履歴情報や二次流通時について考慮されていない．登録情報のユーザと事業者間の流通に加えて，履歴情報や二次流通時のプライバシーや利便性を高めることを本検討の目的とする．提案方式では，登録情報のユーザと事業者間の流通に加えて，履歴情報や二次流通の状況の可視化を行い，プライバシーや利便性の問題の改善を実現する．

本論文の構成について説明する．2 章では関連研究について述べる．3 章，および，4 章で，それぞれ，提案方式の機能，および，提案方式の実現方法について述べる．5 章で提案方式の機能を利用する場合のプライバシーや，履歴情報や二次流通を考慮した際の利便性について評価を行う．6 章で，本論文のまとめについて述べる．

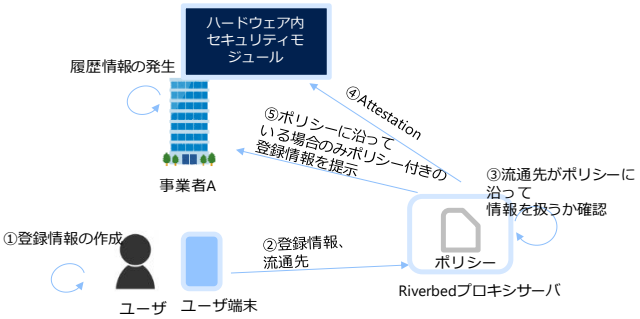

図 2 Riverbed での登録情報の流通

Figure 2 Distribution of registration information when using Riverbed, a related study.

2. 関連研究

ユーザのプライバシーや利便性を考慮して登録情報をユーザから制御する関連研究について以下に説明する．

2.1 Identity Overlay Network (ION)

Microsoft が提案している ION[1]では，ユーザは事業者へすべてのオンラインサービスに対してユーザがユーザであることの証明に使える DIDs を提供する．これにより，ユーザが登録情報をどの事業者に対して提供するか制御できる．

ION のシステムはユーザの登録情報等を暗号化して保存する Identity Hub，ユーザの端末で使用するアプリである User Agents，アプリで作成した ID に紐づく登録情報を参照する Universal Resolver，ハッシュ値などに変換した登録情報を記録するブロックチェーンノードからなる．

プライバシー保護に関して，ION のブロックチェーンノードではユーザの行動によって発生する履歴情報や二次流通について考慮されておらず，ユーザの行動に関する情報がユーザの把握できない部分で流出する恐れがあることなどの問題がある．利便性に関して，ユーザは User Agents で DIDs を発行し，登録情報を作成し，Identity Hub に保存する．1 つの DIDs で複数のサービスを利用することも可能であるが，流通先がユーザの意図に反していた場合ユーザから削除の要求を出す場合の手続きが事業者毎に必要であるため，問題がある．

2.2 Riverbed

MIT CSAIL の Frank Wang らに提案されている，Riverbed[3]では，ユーザ自身が登録情報の流通に関する制約をポリシーとして作成し，そのポリシーに従って登録情報が処理されることを担保する．図 2 に具体的なシステム

```
USER-ID: ALICE
AGGREGATION: False
PERSISTENT-STORAGE: True
ALLOW-TO-NETWORK: x.com
ALLOW-TO-NETWORK: y.com
TRUSTED-SERVER-STACK: {
   83145c082bbf608989f05e85c3c211f83,
   c8cd7ac93cab2b94f65a5b2de5709767f,
      ...
   590f01d8d18b1141988ee1975b3ce3b30
}
```

図 3 ポリシーの記述例

Figure 3 An example of policy statements in Riverbed.

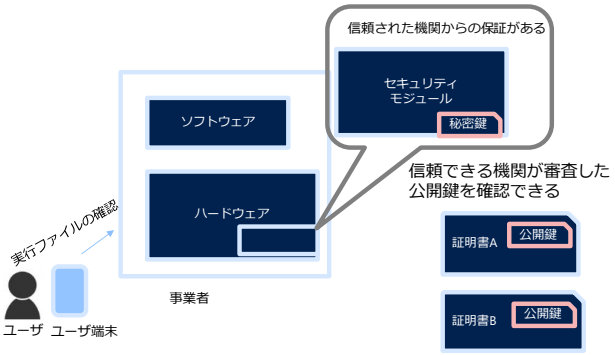

図 4 Attestation 機能

Figure 4 Attestation function in Riverbed.

の動作を示す．図 2 のように Riverbed プロキシサーバが Web プロキシとして動作し，ユーザは事前に Riverbed プロキシサーバに自身の登録情報の流通方針をポリシーとして設定する．ユーザが事業者に対して登録情報を提示する際，Riverbed プロキシサーバがこのポリシーを参照し，登録情報の流通可否を判断，制御する．ここで，ポリシーの具体的な記述例を参考文献[3]から引用し，図 3 に示す．図 3 のように，設定できる項目としては，User ID とともに，他のユーザの登録情報と集約可能であるか(AGGREGATION)，永続的に情報が保存される領域にユーザの登録情報を書き込むことができるかどうか(PERSISTENT-STORAGE)，どのサイトへのアクセスを許可するか(ALLOW-TO-NETWORK)といったことを定めることができる．また，Riverbed は登録情報の安全なやりとりを支援するために，Attestation の機能[5]も有する．Attestation 機能を用いると，図 4 のようにユーザが利用しようとしている遠隔地のハードウェア／ソフトウェアが信頼できるものであるか確認できる．Riverbed では，登録情報の流通先の事業者がもつ機器のハードウェア／ソフトウェアで動作している実行ファイルの組み合わせから計算されるハッシュ値が TRUSTED-SERVER-STACK の項目に記されている値と同じであることを検証することで，機器の信頼性を確認する．

Riverbed は，既存のアプリケーションを改造せずに使用できるようにするためプロキシとして実装されており，実

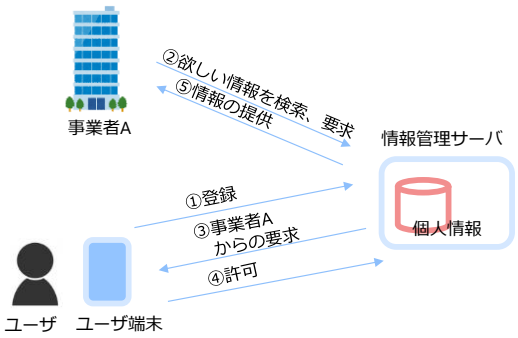

図 5 登録情報集中管理システムでの登録情報の流通

Figure 5 Distribution of registered information in a centralized personal information management system.

際に流通する登録情報に関しては直接関与しない．そのため，既存のアプリケーションの改造を伴わず実装でき，ユーザと事業者の間で直接やりとりされる登録情報に関しては制御することができる．しかし，履歴情報や二次流通を考慮する場合には，実現方法に工夫が必要となる．

プライバシー保護に関して，Riverbed プロキシサーバはポリシーのみを確認するため，登録情報に関与しない．そのため，利便性に関して，ユーザは登録情報の作成に加え，ポリシーの作成を行う必要があり，設定する手間が課題となる．

2.3 登録情報集中管理システム

流通する登録情報を集中管理する方式も様々な検討が進められている．一例として登録情報集中管理システム[4]について説明する．個人の登録情報に相当する情報であるプロファイルを外部のサービスで活用できるシステムであり，図 5 にその概要を示す．図 5 のように，まずユーザが登録情報を情報管理サーバへ保存する．他のユーザ(図 5 では事業者)がサーバ内でユーザに関する情報を検索する場合，検索結果を受け取る際に，情報を提示しているユーザへ通知が送られる．ユーザが許可をすることで，検索された情報が他のユーザへ通知される．この登録情報集中管理システムでは，検索によって得られるユーザに関する情報が情報管理サーバ内に集中管理されている．

管理サーバ（第三者）が登録情報を管理していることから，事業者が何らかの登録情報を取得したい場合は，必ず管理サーバへのアクセスやユーザへの確認が必要となる．登録情報集中管理システムでは，プライバシー保護に関して，ユーザの履歴情報，二次流通が考慮されておらず，利便性に関して，許可などのユーザへの負担が課題となる．

2.4 関連研究の課題

以上述べたように関連研究は，プライバシー保護に関して，ION，登録情報集中管理システム，Riverbed のいずれもユーザと事業者間の登録情報の流通をユーザから確認でき，登録情報を守ることができるが，その後の履歴情報，二次流通に関しては考慮されていない．また，利便性に関して，登録情報集中管理システムのような情報流通時の許可，

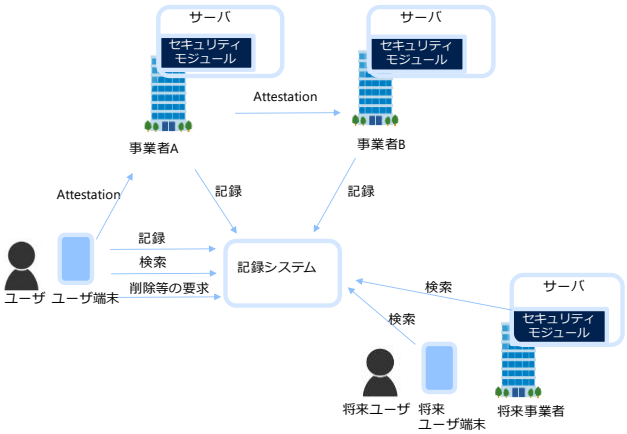

図 6 提案方式概要

Figure 6 Outline of the proposed method.

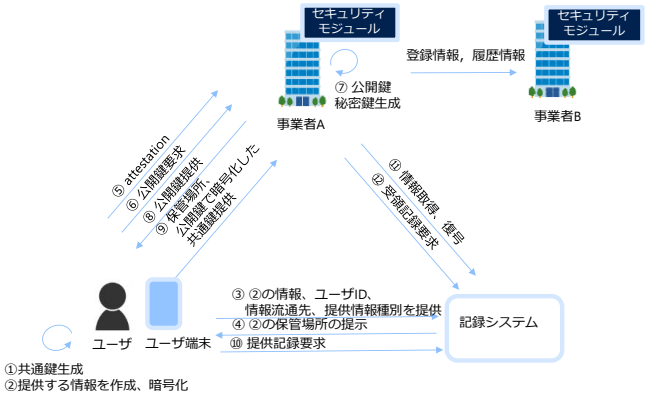

図 7 提案方式での記録作成処理

Figure 7 Processes to record the history of personal information distribution in the proposed method.

Riverbed のようなポリシーの作成などのユーザへの負担が課題となる．

3. 提案方式

以上をふまえ，関連研究で実現できているユーザと事業者間の登録情報の流通状況のユーザからの把握に加え，関連研究の課題を解決できる方式を実現するために以下の要件を満たすことが重要である．

- ユーザのプライバシーの問題改善のため，二次流通先による登録情報，履歴情報の取り扱いをユーザから把握できること
- ユーザの利便性改善のため，システム利用時の手数を少なくできること

以上の要件を満たすために，ユーザと事業者間，および，二次流通の個人情報の取り扱い状況をユーザから確認・制御可能とするために流通履歴可視化方式を提案する．本方式では，ユーザからの流通状況の可視化を行うことにより，ユーザから把握できない部分で情報が流通するなどのプライバシーの問題を改善するとともに，ユーザから削除等の要求をしやすくするなどの利便性向上を実現する．

まず，図 6 に本提案方式の概要を示す．登場人物として，情報流通に関わっているユーザ，事業者(以降，既存ユーザ，既存事業者)，将来情報流通に関わるユーザ，事業者(以降，将来ユーザ，将来事業者)がいる．ユーザは端末，事業者はサーバから記録システムを使用する．

提案方式が提供する機能として，情報流通先への Attestation，記録システムへの流通履歴記録，流通履歴検索，流通情報削除機能がある．事業者は，セキュリティモジュールを用いて登録情報・履歴情報を処理することを前提とし，Attestation は，既存ユーザから既存事業者間，二次流通時に提供元から流通先のセキュリティモジュールのハードウェア／ソフトウェアを確認し，流通先の信頼性を確認する機能である．流通履歴記録機能は，記録システムへ，既存ユーザ，既存事業者が登録情報，履歴情報を提供した記録，受領した記録を残す機能である．この記録機能では，記録システムは流通情報の内容には関与せず流通履歴のみを管理し，情報の流通時に記録システムが暗号化された内容を保持し，提供元と流通先双方からの記録を残す機能である．流通履歴検索機能は，全ての登場人物から，現在の情報の流通状況を把握するための機能である．流通情報削除機能は，既存ユーザから登録情報・履歴情報について既存事業者のセキュリティモジュールに削除要求を行うとともに，削除要求をおこなったこと，および，事業者が要求を受けたユーザに関する情報を削除したことを記録する機能である．

3.1 記録

流通履歴記録機能について図 7 を用いて説明する．まず，既存ユーザ，既存事業者 A，既存事業者 B は，記録システム内での識別のために，記録システムに対してアカウント登録を行う．

次に，既存ユーザは，記録システムに「ユーザから既存事業者 A へ登録情報を提供した事実」を記録する(図 7 ③)．登録情報を受け取った既存事業者 A は，記録システムに「既存ユーザが提供した情報を受領した事実」を記録する(図 7 ⑫)．既存事業者 A から既存事業者 B への登録情報・履歴情報の二次流通時も同様に双方が記録を残す．この記録によって，情報の流通時に提供元と流通先双方からの記録を残すことができる．この双方からの記録を，双方が信頼できる記録システムが提供することによって，実際に流通している事実と記録が一致していることを双方が納得できる状況を提供する．

3.2 流通する情報の内容

記録システムでは流通情報の内容は，記録システムが知ることがないよう，暗号化された状態で受け取ったものを保持し，流通先の事業者がこれを取得する．記録システムは，暗号化されていることにより，登録情報，履歴情報の中身には関与せず，流通情報のみを管理する．既存ユーザから既存事業者 A へ登録情報が流通する場合，既存ユーザ

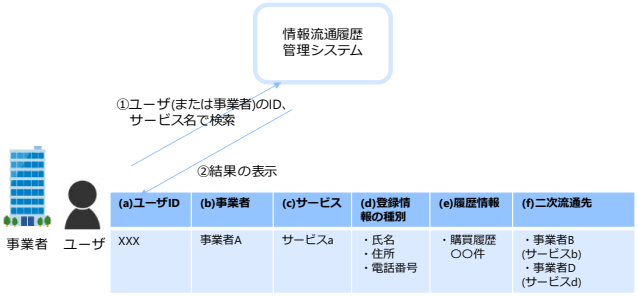

図 8 流通履歴の公開

Figure 8 Disclosure of distribution history in the proposed method.

の登録情報が「氏名：佐藤，住所：東京」であったとすると，記録システム内で「佐藤，東京」の部分は暗号化され，「既存ユーザから既存事業者 A へ氏名，住所が渡った」という内容が記録される．氏名，住所の部分を提供情報の種別と呼ぶ．

3.3 Attestation を用いた流通先の確認

Attestation を活用して事前に提供元から流通先のハードウェア／ソフトウェアを確認する．Attestation は，提供元から流通先のセキュリティモジュールのハードウェア／ソフトウェアの機能を確認する機能である[5]．提案方法では，この Attestation 技術を用いて，流通先のセキュリティモジュールのハードウェア／ソフトウェアが流通された登録情報，履歴情報に対してどのような処理を行うことができるか確認する(図 7 ⑤)．この確認により，ユーザ，または，事業者は，記録システム上の暗号化された個人情報を流通先の事業者が受け取ることがプライバシー上許容できるかを判断できる．

3.4 流通履歴の公開

提案方式では，流通履歴検索機能を用いて，記録システム内の流通履歴を公開し，既存事業者や既存ユーザ，将来ユーザや将来事業者に対して流通情報を検索可能とすることで可視化する．

流通履歴検索機能は，既存ユーザ，既存事業者，将来ユーザ，および，将来事業者が使用し，(i) 既存ユーザが自分自身について検索する場合，(ii) 既存事業者が特定の既存ユーザについて検索する場合，(iii) 既存ユーザ，既存事業者，将来ユーザ，将来事業者が特定の既存事業者の流通履歴について検索する場合の 2 つの場合がある．それぞれの機能を，以下に順に説明する．

(i)の検索では，既存ユーザ端末から記録システムに対して検索項目を入力する(図 8 ①)．既存ユーザは検索項目に既存ユーザのアカウントを含めて，記録システムに送信する．記録システムは，流通履歴記録機能の中で，管理している情報をまとめ，検索結果として既存ユーザへ提示する(図 8 ②)．検索結果の内容は，(a)ユーザ ID，(b)既存ユーザが直接登録情報を提示した既存事業者，(c)既存事業者のサービス名(d)登録情報の種別，(e)履歴情報の種別，(f)二次流通先である．(ii)の検索では，既存事業者は検索項目に特定の既存ユーザのアカウントを含めることで，(i)と同様の結果が得られる．(iii)の検索では，将来ユーザ，将来事業者はアカウントを作成していなくても，特定の既存事業者を検索項目にすることで，(b)，(c)，(d)，(e)，(f)を得られる．アカウントを保持している既存事業者も同様の検索結果が得られる．

提案方式では，上記検索結果を得られることで，既存ユーザは自身の情報が実際にどこに流通しているのか把握できる．既存事業者は記録システムへ記録を行うことで，将来ユーザや将来事業者に対して登録情報や履歴情報を適切に扱っているというアピールとなる．将来ユーザや将来事業者は，利用したいオンラインサービスに関して提示した情報が実際にどのように流通するのか事前に把握してからサービスを利用できる．

3.5 既存ユーザからの削除機能

流通情報削除機能は，既存ユーザが既存事業者へ登録情報・履歴情報について削除要求を行った時に実行される．本機能では，既存事業者が要求に基づいた登録情報，履歴情報の削除を行い，記録システムが削除要求や削除済みであることを記録する．本機能の使用例としては，まず最初に，既存ユーザが検索によって流通状況を確認する．確認後，記録システムを介して，既存ユーザの意図しない既存事業者に流通した情報を削除する要求ができる．本機能を用いることによって，ユーザは流通に関する要求のためにそれぞれの既存事業者ごとに，その連絡先に対してメールや電話でのコミュニケーションを行う必要がなくなり，既存事業者は受け取った要求に応じた記録を残すことで既存ユーザからの信頼を得られる．

これらの削除に関する要求や記録を行う機能を用いた場合，実際に事業者が既存ユーザからの要求に応じて情報を削除したかどうか，セキュリティモジュールだけに情報が格納されている場合，セキュリティモジュールからの実行結果の通知と，その通知に対する署名により確認できる．セキュリティモジュール外に情報が格納されていた場合であっても，実際に事業者が削除していない場合，事後に削除していなかったことが露呈した際に事業者の信頼が失墜すること，要求に応じていないという違法行為に問われるという圧力によって，事業者に正しい行動をとろうという姿勢を促すことにつながると考える．

更に，上記のユーザによる削除要求，および，事業者による情報の削除を記録する機能に加えて，既存事業者のセキュリティモジュール内での処理制限により，既存ユーザの個人情報をセキュリティモジュール内で保持し，他のストレージでコピーできない場合，セキュリティモジュールに対して削除機能が実際に使用され，情報が削除されたか確認することもできる．この場合，セキュリティモジュー

ルは，既存ユーザを認証した上で，削除要求の対象データの削除を行う機能を保持しているものとする．この機能により，より確実に既存ユーザの登録情報・履歴情報の取り扱いに対する意思を事業者に強制することができる．

4. 提案方式の実現方法

提案方式の実現方法に関して，図 7 を用いて，既存ユーザから既存事業者 A へ登録情報が流通する場合について説明する．本機能の処理の前に事前に，既存ユーザはアプリを介して記録システムでアカウントを作成することで ID を登録しているものとする．最初に，既存ユーザは「氏名：佐藤，住所：東京」のような登録情報をアプリ内で作成する．そして，図 7 ②で，登録情報を暗号化するために必要な共通鍵を使用して登録情報を暗号化する．この暗号化した情報，記録システムの ID，情報流通先(事業者 A)，提供情報種別(「氏名」,「住所」等)を，図 7 ③で，アプリから記録システムに提供する．記録システムは，その応答として図 7 ④で，保管場所の確保を行うとともに，受信した情報を保管した後，確保された保管場所の情報が，記録システムからユーザに提示される．既存ユーザは，図 7 ⑤で，既存事業者 A に対して Attestation を行い，既存事業者 A の情報の保管場所の安全性を確認する．確認後，既存ユーザは図 7 ⑥⑦⑧で，既存事業者 A が生成した公開鍵を受け取り，登録情報の暗号化に使用した共通鍵を受け取った公開鍵で暗号化する．既存ユーザは，図 7 ⑨で，この暗号化した共通鍵と保管場所を事業者 A に提示する．これらを受け取った既存事業者 A は暗号化された共通鍵を復号する．そして，図 7 ⑩で，既存ユーザは記録システムへ提供記録要求を行い，記録システムが要求に基づいて記録を行う．記録済みである通知を既存ユーザのアプリから受け取った既存事業者 A は，図 7 ⑪で，保管場所の情報を記録システムに提示し，記録システムから暗号化された既存ユーザの登録情報を転送するとともに，既存事業者 A は，暗号化された既存ユーザの登録情報を，既存ユーザからの共通鍵で復号する．最後に，既存ユーザは記録システムへの記録が完了したことを既存事業者 A から通知される．

以上は，ユーザから事業者 A に対して登録情報が流通する場合である．本研究では事業者間の情報流通の記録についても実現することを目指している．また，事業者に記録される履歴情報についても流通の記録を実現する．本提案方式では，事業者間の登録情報・履歴情報は，前の段落で説明したユーザから事業者 A への情報流通と同様に行われるものとする．

記録された情報は，記録システムへの検索によって参照される．既存ユーザや既存事業者が検索を行う場合，最初に，記録システムへログインする．既存ユーザや既存事業者は，ログイン後に，3.4 章で説明したように検索条件を指定して検索要求を行う．記録システムは流通記録から該当する情報を検索し，結果を通知する．将来ユーザ，将来事業者が検索を行う場合には ID に関する情報は結果に含まれない．

5. 評価

本稿では，プライバシー保護の観点，および，ユーザ利便性についての評価を行うことで提案方式の有効性を示す．

最初に，プライバシー保護観点での評価について述べる．

プライバシー保護に対する脅威は主に事業者の行動によって発生する．事業者の脅威に対する提案方式の効果は，2 つあり，記録が公開されていることによる抑止効果，および，セキュリティモジュールによる事業者に強制できる行動があることである．より確実にプライバシー保護をするためには，セキュリティモジュールの機能によって何を強制できるかを変える必要がある．また，事業者の行動による想定脅威によって必要となる「確認すべきセキュリティモジュールの機能」も異なる．以上から，評価のために，

- 事業者の脅威レベルの分類
- セキュリティモジュールの機能のレベルの分類

を行い，効果を考察する．

表 1 は，事業者の脅威レベルとセキュリティモジュールの機能のレベルの組み合わせで発生する脅威について分析した結果を示している．表 1 の横軸は，セキュリティモジュール内での処理制限という Attestation で確認するセキュリティモジュールの機能のレベルを示す．特定の事業者のみに流通先が制限されているのが「流通先の制限」，この流通先の制限に加え，流通先での個人情報の保管場所がセキュアな領域に限られるというのが「流通先の制限＋個人情報のセキュリティモジュール外への漏洩禁止」としている．縦軸は事業者の行動のレベルを示し，事業者がどの程度法律を守る前提であるかによってレベル分けしている．表 1 の中で，現状において多数を占めると思われる「不正にならない範囲で最大限情報を活用」を考える事業者に対する効果を中心に説明する．このような事業者の場合，ユーザの個人情報に関して，できる限り自由な扱いを求める傾向があると考えられる．一方，必要なセキュリティモジュールの機能を考えると，記録が公開されるという，周囲から不正をしているとわかる状況である場合，事業者は不正をしにくくなる．更に，「流通先の制限」レベルをセキュリティモジュールで管理しているにも関わらず制限外の事業者に流通するなどした場合には，過失ではなく意図的に不正をしていると思われる可能性が高いと考えられる．そのため，「流通先の制限」レベルでも，「不正にならない範囲で最大限情報を活用」するという事業者のレベルに対して大きな抑止力になると考えられる．また仮に，ユーザの意図に反した行動をとれば，削除要求が増えて公開されることで将来ユーザの獲得にマイナスに働くことや，セキュリティモジュールによる制限としてより厳しいものとしなけれ

ばユーザを獲得できないといった事業上のデメリットを被ると考えられる．以上の考えから，「流通先の制限」レベルで，プライバシーの保護を実現できる可能性は高いと考える．

提案方式では，Attestation 機能を活用することで，セキュリティモジュールでの処理制限を「個人情報のセキュリティモジュール外への漏洩禁止」等に更に厳しくすることもできる．そのため，関連研究で述べた ION や集中管理システムでできなかった流通先の処理制限についての確認や，Riverbed でできなかった二次流通先の確認が，より確実にできるようになる．

次に，ユーザ利便性の評価について議論する．ユーザの求められる操作について，関連研究で述べた ION では，ユーザはアプリで DIDs を発行し，登録情報を作成する．利用規約等に二次流通に関する情報に曖昧な部分がある場合，ユーザは同意し，DIDs を提示できるが，実際の流通状況を把握する場合，直接問い合わせる必要がある．登録情報集中管理システムではそれぞれの流通先ごとにユーザからの許可が必要である．Riverbed では，ユーザは登録情報の作成とポリシーの作成を行うが，ポリシーを設定する手間がある．提案方式では，ユーザは事業者から，登録情報，履歴情報の流通先のリストを受け取り，流通を許可するか選択する．その後，記録システムを利用して実際の流通状況をユーザが把握し，意図しない流通を発見した場合，削除等の要求を送ることができる．このことから，関連研究では事業者ごとに行っていた流通先の許可やポリシー作成を，本方式では事業者からの流通先リストでの許可によって一括にできる．更に，関連研究では一度流通を許可した事業者に関してユーザの意図しない流通が起きた場合，ユーザから直接事業者へ問い合わせをする必要があることに対し，本方式では記録システムでの検索によりユーザから意図しない流通の把握，流通情報削除機能により記録システムを介した事業者への削除要求ができる．

仮に，平均的に，一次流通先の二次流通先がN件あったとし，M件について流通がユーザの意にそぐわないとする．この一次流通先が一定程度信頼できる事業者であったとすると，おおむね二次流通結果についても信頼できる可能性が高い．つまり，$M \ll N$である．そのため，既存技術の場合，N件の二次利用先に対して，N件すべてで流通可否の操作やポリシーの記載の操作を行う必要がある．そのため，提案方式の場合，$1+M$回の操作となることから，NとMの差に応じたユーザ操作数の削減が可能である．

6. まとめ

本稿では，ユーザの個人情報の事業者での流通に関して，ユーザと事業者間の登録情報の流通に加え，登録情報と履歴情報の二次流通も考慮し，プライバシーと利便性の問題の改善を実現する方式を提案した．

表 1 セキュリティモジュールでの処理制限と事業者のレベルでの評価

Table 1 Assessment of threats against user's privacy depending on service-provider's behavior and security-module's functionality.

セキュリティモジュール内での処理制限 ＼ 事業者による脅威のレベル	なし	流通先の制限	流通先の制限＋個人情報のセキュリティモジュール外への漏洩禁止
	公開	公開	公開
法律を守らない	× 抑止力による効果がない	△ コピーによる不正流通の可能性あり	○ コピーも含めて不正流通を制限可能
不正にならない範囲で最大限情報を活用	△ 流通先、利用目的の修正	△～○ 不正流通はないが、利用目的の修正	○ モジュール内で定められた処理のみ可能
社会的な監視による抑止力があれば法律を遵守する	○ 公開による抑止力が法律の遵守につながる	○ 左と同じ	○ 左と同じ
法律を遵守する	○ 法律による抑止力	○ 記録、漏洩対策、法律による抑止力	○ 記録、漏洩対策、法律による抑止力

提案方式は，プライバシー問題を改善するために，個人情報の流通を可視化・公開することで，不正な流通に対する抑止力を働かせることを特徴とする．また，より確実に不正な流通を防止するために，Attestation 可能なセキュリティモジュールで事業者が個人情報を取り扱うことを前提とし，情報の流通元であるユーザ，事業者が流通先の信頼性を確認した上で個人情報を流通させる仕組みを導入した．さらに，利便性については，流通状況をユーザが検索によって確認し，意図しない流通先であった場合のみ削除機能を利用するという状況を実現する仕組みを導入した．本提案方式について，プライバシー保護に関する機能，利便性に関するユーザの処理について評価を行い，プライバシー保護に関しては関連研究と比較して，履歴情報や二次流通まで含めるとより高い効果があり，利便性に関しては関連研究よりもユーザの処理を減らすことができる場合があることが分かった．

参考文献

[1] Simons, A.: Toward scalable decentralized identifier systems (online), available from <https://techcommunity.microsoft.com/t5/azure-active-directory-identity/toward-scalable-decentralized-identifier-systems/ba-p/560168#> (accessed 2020-4-20).

[2] Decentralized Identifiers (DIDs) v1.0, W3C (online), available from < https://www.w3.org/TR/did-core/> (accessed 2019-12 9).

[3] Wang, F., Ko, R., and Mickens, J.: Riverbed: Enforcing User-defined Privacy Constraints in Distributed Web Services, *Proc. 16th USENIX Conference on Networked Systems Design and Implementation*, pp.615–629 (2019).

[4] 橋場基樹: プロファイル管理システム，情報管理方法，プログラム，情報処理装置，データ送信方法，特開 2019-159970 (2019).

[5] Coker, G., Guttman, J., Loscocco, P., Herzog, A., Millen, J., Hanlon, B.O., Ramsdell, J., Segall, A., Sheehy, J., and Sniffen, B.: Principles of Remote Attestation, *International Journal of Information Security*, Vol.10, No.2, pp. 63–81 (2011).