自己主権型アイデンティティ情報利活用基盤に関する考察

才所 敏明[*1]　　辻井 重男[*2]　　櫻井 幸一[*3]

概要：世界が，日常の生活活動や社会に向けた活動もサイバースペースで展開されるインターネット依存社会へ移行する中，活動に必要な個人のアイデンティティ情報（属性情報）のネット経由の提供も増加するのは必至であり，個人のサイバースペースでの活動を支援するアイデンティティ情報利活用基盤の早期の実現が期待される．一方，多くのアイデンティティ情報は個人情報・プライバシー情報であり，効率的な利活用のみならず，安心・安全な利活用の支援が求められる．本論文では，自己主権型アイデンティティ情報利活用基盤のあり方，要件，検討課題等を考察する．更に，アイデンティティ情報利活用基盤の中で個人のアイデンティティ情報の登録・保護・提供を支援する自己主権型アイデンティティ情報管理システムに期待される機能について考察し，自己主権型アイデンティティ情報管理システムを目指し提案・開発中の代表的なシステム uPort．Sovrin の機能を整理・評価する．

キーワード：アイデンティティ情報管理，自己主権，自己主権型アイデンティティ情報利活用基盤，SSIUF，自己主権型アイデンティティ情報管理システム，SSIMS，uPort，Sovrin

Consideration on Self-Sovereign Identity-information Utilization Framework (SSIUF)

Toshiaki Saisho[*1]　　Shigeo Tsujii[*2]　　Kouichi Sakurai[*3]

Abstract: As the world shifts to an Internet-dependent society where daily life activities and social activities are also developed in cyberspace, the provision of personal identity information necessary for activities via the Internet will increase. It is inevitable, and it is expected that the Identity-Information Utilization Framework that supports individual activities in cyberspace will be realized at an early stage. In this paper, we consider the ideal way, requirements, and issues to be examined for the Self-Sovereign Identity-information Utilization Framework. Furthermore, we will consider the functions expected for the Self-Sovereign Identity-information Management System that supports the registration, protection, and provision of individual identity information within the Self-Sovereign Identity-information Utilization Framework. And organize and evaluate the functions that have been implemented or are expected to be implemented for the typical Self-Sovereign Identity-information Management System that is being proposed and developed.

Keywords: identity information management，Self-Sovereign，Self-Sovereign Identity-information Utilization Framework，SSIUF，Self-Sovereign Identity-information Management System，SSIMS，uPort，Sovrin

1. はじめに

我が国をはじめ世界では，行政・民間を問わず多くの組織は個人へ提供する様々のサービスをインターネット経由のサービスへ，またコミュニケーションを含む個人間の多くの活動もインターネット経由へ移行しつつある．個人の活動がインターネット上で展開されるサイバー社会へ移行する中，活動遂行上求められる個人の様々の属性を示すアイデンティティ情報のインターネット上でのやり取りも必要となり，実際にその授受も行われている．今後もインターネット経由での個人の活動が増加し，その活動に必要な様々の個人のアイデンティティ情報の流通が活発になるものと考えられる．

本稿では，個人がインターネット経由の活動を円滑に効率的に実施できるために必要な，個人のアイデンティティ情報のインターネット上での安全な管理，提供，活用を可能とし，アイデンティティ情報保有者による自身の情報への自己制御を可能とする自己主権型アイデンティティ情報利活用基盤（SSIUF：Self-Sovereign Identity-information Utilization Framework）についての考察結果を報告する．

2 章にて自己主権型アイデンティティ情報利活用基盤のあり方，要件，検討課題等を考察し，3 章にて利活用基盤の中で個人のアイデンティティ情報の登録・保護・提供を支援する自己主権型アイデンティティ情報管理システム（SSIMS：Self-Sovereign Identity-information Management System）に期待される機能について考察し，4 章にて実用化を目指し提案されている二つのシステム uPort および Sovrin の機能を整理・評価する．

*1　（株）IT 企画　http://advanced-it.co.jp/
mail：toshiaki.saisho@advanced-it.co.jp
中央大学研究開発機構
(株)ZenmuTech
*2　中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp
*3　九州大学大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所
mail：sakurai@inf.kyushu-u.ac.jp
【 論文原稿：上記*の文字書式「隠し文字」 】

2. 自己主権型アイデンティティ情報利活用基盤（SSIUF）

アイデンティティ情報保有者の情報利活用を支えるアイデンティティ情報利活用基盤は，アイデンティティ情報の発行，アイデンティティ情報の管理，アイデンティティ情報の利用，の三つのフェーズをサポートする必要がある（図１）．

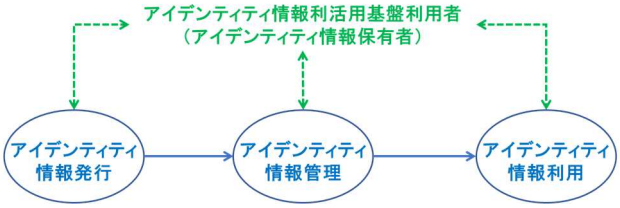

図１　アイデンティティ情報利活用のフェーズ

アイデンティティ情報利活用における自己主権性とは，アイデンティティ情報利活用基盤を構成する各フェーズにおけるアイデンティティ情報保有者の自己制御性である．

本章では，インターネット上の個人の活動を効率的に安全に支える社会基盤として活用されることが期待される自己主権型アイデンティティ情報利活用基盤を構成する各フェーズのあり方，要件，検討課題等について考察する．

2.1 アイデンティティ情報発行フェーズ

①情報保有者の意思に基づくアイデンティティ情報発行制御

自己主権性を重視するアイデンティティ情報発行のフェーズでは，一般にアイデンティティ情報は個人情報・プライバシー情報を含むため，情報発行事業者/システム運用者あるいは第三者ではなく，情報保有者の意思に基づいてのみ行われる必要がある．そのためには，情報発行要求者が情報保有者本人であることを確実に確認する必要がある．

②アイデンティティ情報の一定の標準化

アイデンティティ情報は，情報保有者の属性情報であり．名前，性別，生年月日，住所等の基本的な属性，所属・役職．健康状態等の現有属性，学歴，職歴，病歴等の履歴属性等，多様であるが，属性情報のグループ化と同一グループ内での属性名と属性値に関する一定の標準化，およびグループに依存しないアイデンティティ情報の構成・形式上の標準化が，アイデンティティ情報の利活用促進に必要であろう．

③アイデンティティ情報発行主体の信頼性確認可能性

アイデンティティ情報の発行主体は，TTP（Trusted Third Party：信頼できる第三者），必ずしも信頼できる第三者としての共通の認識を得られていない第三者，あるいは情報保有者自身が想定される．いずれにせよ，当該アイデンティティ情報の信頼性を保証する発行主体の特定を可能とし，その発行主体の信頼性の確認が可能な情報も，発行されるアイデンティティ情報に含めておくことが必要であろう．

2.2 アイデンティティ情報管理フェーズ

アイデンティティ情報管理フェーズは，情報登録，情報保護，情報提供の三つの機能から構成されている．

2.2.1 情報登録

①情報保有者の意思に基づくアイデンティティ情報登録

アイデンティティ情報は，情報保有者の指示によってのみ，登録を可能とすることが必要である．そのためには，情報登録要求者が情報保有者本人であることを確実に確認する必要がある．

②不正な情報登録への対応

情報保有者の登録要求アイデンティティ情報が，信頼できる第三者の保証のない情報には様々の悪意が含まれている危険性もある．不正な情報の登録回避，登録された不正な情報への対応の仕組みが必要である．

③登録情報の整合性

登録要求アイデンティティ情報の既登録アイデンティティ情報との整合性の検証，不整合の場合の対応の仕組みが必要である．

2.2.2 情報保護

①情報保有者の意思に基づくアイデンティティ情報保護

登録アイデンティティ情報の保護や開示の判断・指示は情報保有者のみが可能な仕組みが必要である．そのためには，情報保護要求者が情報保有者本人であることを確実に確認する必要がある．

②登録情報の多様な保護ニーズへの対応

登録アイデンティティ情報の保護方式としては，アクセス制御による保護，暗号化等による情報秘匿等が考えられる．登録情報の内奥に応じた適切な保護方式の選択が可能なことが望ましい．

③登録情報へのアクセス検証・監査可能性

登録アイデンティティ情報へのアクセスについて，アクセス者，アクセス日時等の検証・監査が可能なことが望ましい．

2.2.3 情報提供

①情報保有者の意思に基づくアイデンティティ情報提供

情報保有者自身の登録アイデンティティ情報を情報保有者のみが提供できる仕組みが必要である．そのためには，情報提供要求者が情報保有者本人であることを確実に確認する必要がある．

②提供先・提供依頼情報の妥当性

情報保有者による提供先・提供依頼情報の妥当性の確認が必要である．そのためには，情報保有者が提供先の真正性・信頼性を確認できる仕組みが必要であろう．

③提供情報の最小化機能

登録されているアイデンティティ情報から，妥当性を確認した提供依頼に対応する情報のみからなる提供情報を生成する仕組みが望ましい．

④提供情報の一定の標準化

アイデンティティ情報の場合と同様，情報保有者が提供する提供情報についても一定の標準化，共通仕様に基づく提供情報の提供が望ましい．具体的には，提供情報の形式，提供内容の形式・表現方法，提供内容の根拠となる登録アイデンティティ情報，情報保有者による提供先への提供情報であることの証明情報の内容・形式等の標準化が望ましい．

⑤提供先への安全な情報提供

提供情報の提供先への安全・確実な提供の仕組みが必要である．

⑥提供先・提供情報の検証・監査可能性

提供先，提供日時，提供情報，提供依頼情報等の，提供の検証・監査が可能なことが望ましい．

2.3 アイデンティティ情報利用フェーズ

①情報保有者の意思に基づく提供情報の利用制御

提供情報の，提供先による提供目的のための利用，に限定する仕組みが望ましい．

利用制御方式としては，提供情報と利用制御の仕組みを一体化し提供する方式や，提供後の情報の利用の都度，情報保有者の承認を得る方法などが想定される．

しかし，一般には契約等による利用制限にとどめることが多いと思われ，提供情報が提供先から不正に流出した場合の流出ルートの特定の仕組みも望まれる．

②提供情報の利用記録の検証・監査可能性

利用目的，利用日時，利用情報等の，提供先における提供情報の利用の検証・監査が可能なことが望ましい．

③提供情報の抹消/抹消確認

提供情報の内容により，提供先に提供した情報の抹消の仕組みあるいは抹消されたことを確認できる仕組みが望ましい．

3. 自己主権型アイデンティティ情報管理システム（SSIMS）

本章では，自己主権型アイデンティティ情報利活用基盤の中核を構成する，アイデンティティ情報管理フェーズで情報保有者の利活用を支援する，自己主権型アイデンティティ情報管理システム（SSIMS）の機能について考察する．

SSIMS の構成概要を図 2 に示す．2 章に既述の通り，SSIMS の主たる機能は，情報管理フェーズで期待される情報登録，情報保護，情報提供の三つの機能の他，本人確認のための身元確認，当人確認の二つの機能である．管理対象情報は，本人確認情報およびアイデンティティ情報の二つに分類される．

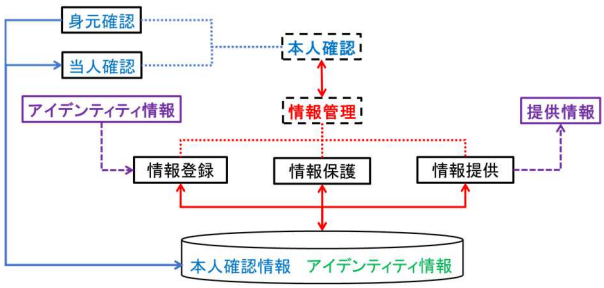

図２　SSIMS を構成する機能・情報

3.1 本人確認

自己主権性を目指すアイデンティティ情報管理システムでは，情報管理要求者がアイデンティティ情報保有者であることの確実な確認が不可欠である．

本人確認は，身元確認と当人確認から構成される．インターネット上での本人確認は，フィジカルスペースの本人の身元を確認の上に定義されたサイバースペース（インターネット上）の身元確認済エンティティの，登録されている当人確認情報を利用した当人確認により，実施される（図３）．

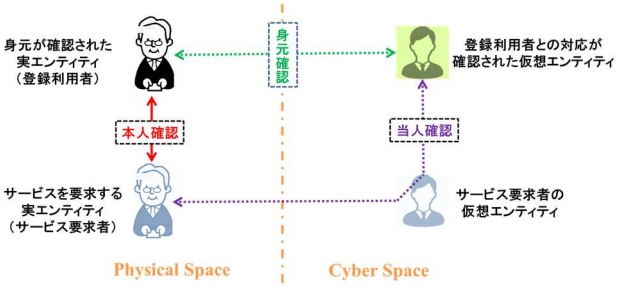

図３　本人確認＝身元確認＋当人確認

本人確認の保証レベルは，身元確認の保証レベルおよび当人確認の保証レベルに依存する．確実な本人確認のためには，高い保証レベルの身元確認および当人確認が必要である．

なお，身元確認の保証レベルについては NIST SP 800-63A にて IAL（Identification Assurance Level）規定されており，当人確認の保証レベルについては NIST SP 800-63B にて AAL（Authentication assurance Level）として規定されている（図４）．我が国をはじめ多くの国のネット経由の本人確認の保証レベルは，これらの NIST のドキュメントを参考に規定されている．個人情報，プライバシー情報を管理する SSIMS における本人確認では，NIST の規定における，身元確認の保証レベル（IAL）は３，当人確認の保証レベル（AAL）は３，の保証レベルが望ましい．

保証レベル	身元確認方法の要件・特徴（IAL）	当人確認方法の要件・特徴（AAL）
1	Applicant を現実世界の特定の Identity と紐づける必要はない。提供される Self-asserted Attribute は確認も検証もされない。	Subscriberのアカウントに対して結び付けられている単一要素または多要素の AuthenticatorをClaimantが所有・制御の証明が必要。
2	Applicant が現実世界の Claimed Identity と、適切に関連づけられていることをエビデンスにより証明が必要（リモートないしは対面での Identity Proofing が必要）。	Subscriberのアカウントに対して結び付けられている二つの異なるAuthentication要素をClaimantが所有・制御の証明が必要（Approved Cryptographic技術がAAL2及びそれ以上では必要）。
3	対面での Identity Proofing が必要。識別に用いる Attribute は Authorized かつ訓練を受けたCSP の代理人によって検証されることが必要。	Subscriberのアカウントに対して結び付けられている一つのハードウェアベースの Authenticatorと一つのVerifierなりすまし耐性を備えるAuthenticatorをClaimantが所有・制御の証明が必要。

図４　NIST Special Publication 800-63A,B における身元確認・当人確認の保証レベル

なお，身元確認は SSIMS 外部の信頼できる組織による身元確認済の ID を利用するケースも多い．信頼できる組織が身元確認を行って発行する DID（Decentralized Identifier）の利用，各国で整備が進んでいる NAF（National Authentication Framework）による身元確認後に発行される NAF-ID の利用等が考えられる（[3]～[5]）．

3.2 情報管理

情報管理は情報登録，情報保護，情報提供の三つの機能から構成される．SSIMS を構成するのもこの三つの機能であり，各機能において期待される機能について考察する．

3.2.1 情報登録

①情報保有者以外の情報登録の排除

情報登録要求者が情報保有者本人であることを確実に確認する必要がある．また，代行者による情報登録の場合は，情報保有者の代行者への委任の確実な確認も必要である．新規登録に限らず，登録情報の修正・削除においても同様の仕組みが必要である．

②不正な情報の登録回避/登録情報の不正確認後の対応

登録対象情報の検査等により，不正な情報の登録を回避/排除する仕組みが必要である．このような登録対象情報の内容により登録を回避/排除することは，情報保有者の意思に反することになるが，社会の安心・安全の維持の観点から必要な機能であろう．なお，登録対象情報が暗号化等により保護されている場合もあり，登録時の検査による不正な情報の登録の完全な回避/排除は難しく，登録後に不正な情報であると判明した場合の対応，不正な情報の登録者の特定・追跡等を可能とする仕組みも必要となろう．

③既登録情報との整合性

情報保有者の既登録アイデンティティ情報との整合性の検証，不整合の場合の情報保有者への通知等の対応が必要である．なお，登録対象情報・既登録情報が暗号化等により保護されている場合，整合性の検証は困難であり，整合性の確保は情報保有者の責任での対応となろう．

3.2.2 情報保護

①情報保有者以外の情報保護制御の排除

情報保護要求者が情報保有者本人であることを確実に確認する必要がある．また，代行者による情報保護要求の場合は，情報保有者の代行者への委任の確実な確認も必要である．

②登録情報の多様な保護方式

アイデンティティ情報のデータへの情報保有者以外のアクセスを防止することによる保護，暗号化等による情報秘匿により情報保有者以外のアイデンティティ情報内容へのアクセスを防止することによる保護等が考えられる．アイデンティティ情報の内容や開示条件等により，適切な保護方式の選択が可能なことが望ましい．

③登録情報へのアクセス記録

事後の監査に対応できるよう，誰が，いつ，どのアイデンティティ情報にアクセスしたか等の，アクセス情報の記録が望ましい．なお，アクセス者の特定・追跡を可能とするには．アクセス者の身元確認，利用時の当人確認が必要となろう．

3.2.3 情報提供

①情報保有者以外の情報提供制御の排除

情報提供は，提供先・提供依頼情報の妥当性の確認も含め，情報保有者のみが提供できる仕組みが必要である．そのためには，情報提供要求者が情報保有者本人であることを確実に確認する必要がある．

また，情報保有者が提供先の真正性・信頼性を確認できる仕組みが必要であろう．

②提供情報の多様な最小化機能

提供情報は，妥当性が確認された提供依頼情報の範囲に限定するのが望ましい．

提供情報の最小化の例としては，登録アイデンティティ情報の中で，提供不要な情報のマスキング，提供範囲の情報の抽出等が考えられる．また，提供依頼情報が登録アイデンティティ情報そのものと異なる場合は，意味的に等価な条件あるいは計算方式等の評価により，提供情報を生成する方法も考えられる．このような登録アイデンティティ情報の変形による提供の場合，TTP により発行されたアイデンティティ情報の適切な変形であることを保証する仕組みが必要である．

③提供先・提供情報の記録

事後の監査に対応できるよう，提供記録，提供先，提供日時，提供情報，提供依頼情報等を記録しておくことが望ましい．

フェーズ		検討課題
情報発行		①情報保有者の意思に基づくアイデンティティ情報発行制御 ②アイデンティティ情報の一定の標準化（形式、表現方法等） ③アイデンティティ情報発行主体の信頼性確認可能性
情報管理	（情報登録）	①情報保有者の意思に基づくアイデンティティ情報登録 ②不正な情報の登録への対応 ③登録情報の整合性
	（情報保護）	①情報保有者の意思に基づくアイデンティティ情報保護 ②登録情報の多様な保護ニーズへの対応 ③登録情報へのアクセス検証・監査可能性
	（情報提供）	①情報保有者の意思に基づくアイデンティティ情報提供 ②提供先・提供依頼情報の妥当性 ③提供情報の最小化機能 ④提供情報の標準化（形式、表現方法等） ⑤提供先への安全な情報提供 ⑥提供先・提供情報の検証・監査可能性
情報使用		①情報保有者の意思に基づく提供情報の使用制御 ②提供情報の利用記録の検証・監査可能性 ③提供情報の抹消/抹消確認

図５　SSIUF の主要な要件，検討課題一覧

4. 具体的 SSIMS（uPort，Sovrin）の評価

本章では，自己主権型アイデンティティ情報利活用基盤を構成する自己主権型アイデンティティ情報管理システム（SSIMS）に期待される機能の観点から，開発あるいは提案されている代表的な SSIMS である uPort および Sovrin を比較・評価する．

4.1 uPort 概要

uPort はイーサリアム･ブロックチェーンのスマートコントラクトを利用し実現されている SSIMS である．

利用者はモバイルデバイス上の uPort app からイーサリアム・ブロックチェーン上の Controller コントラクトを起動する．Controller コントラクトは利用者認証後，Proxy コントラクトを起動し，uPort app から送信されたアイデンティティ情報を Registry コントラクト経由で IPFS へ登録する．

uPort app は，第三者からの提供依頼をイーサリアム・ブロックチェーン経由あるいは別チャネル経由で受信し，uPort app からの利用者の判断・指示の元，提供情報そのものあるいは IPFS 上の情報へのアクセス情報が提供される（図６）．

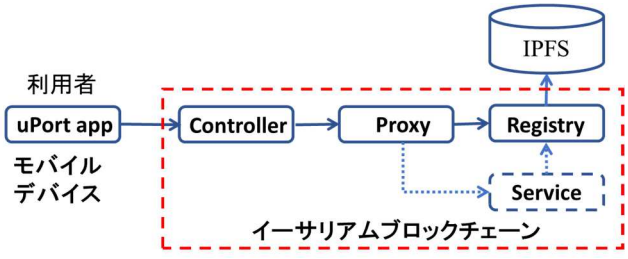

図６　uPort 構成概要

4.2 Sovrin 概要

Sovrin は Hyperledger Indy ベースの Sovrin Ledger（ブロックチェーン）を利用し実現を目指している SSIMS である．

利用者は，モバイルデバイス上の User Client App 経由，User Agent をアクセスし，User Agent 経由，アイデンティティ情報の Sovrin Ledger への登録を情報登録の承認プロセスに参加する Stewards（ノード）へ申請する．なお，Sovrin では個人情報を含むアイデンティティ情報は Sovrin Ledger ではなく，User Agent で管理するのが原則である．

Sovrin は，第三者からの提供依頼を User Agent の End Point 経由あるいは別チャネル経由で受信し，User Client App からの利用者の指示・判断の元，User Client App または User Agent で提供情報を作成し，情報の提供には User Agent 間の Direct Communication チャネルを使用する．Sovrin Ledger に登録されているアイデンティティ情報は，提供された情報の検証に使用される（図７）．

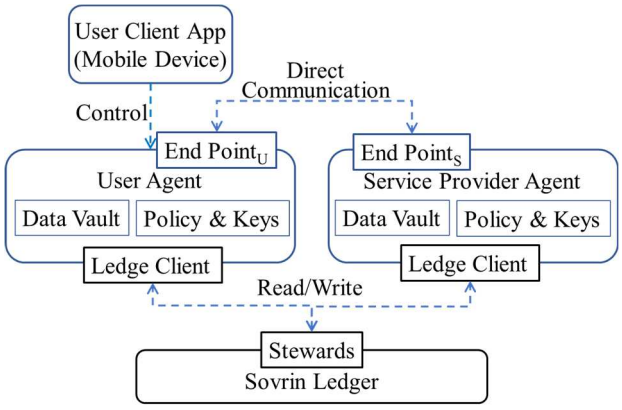

図７　Sovrin 構成概要

4.3 本人確認

4.3.1 身元確認

uPort および Sovrin 共に身元確認機能は用意されていない．

SSIMS では確実な本人確認が必要であり，両システムをベースにした SSIMS 構築時には，NIST SP 800-63A にて定義されている高い保証レベル（IAL 3）の身元確認方法の独自実装，あるいは信頼できる組織が身元確認を行って発行される DID，各国で整備が進んでいる NAF による身元確認後に発行される NAF-ID との連携等の検討が必要となろう．

4.3.2 当人確認

uPort および Sovrin 共に，公開鍵暗号の鍵ペアを使用した署名付与・検証により当人確認を行っている．NIST SP800-63B による当人確認結果の保証レベルは，利用者のモバイルデバイスがパスワード等によるロックが施されている場合は AAL3，そのようなロックが施されていない場合は AAL2 と考えられる．

SSIMS が管理するアイデンティティ情報は，一般には個人情報・プライバシー情報であるため，他人のアクセスを防ぐよう，結果に対する高い保証レベルの当人確認方法が望ましい．

4.4 情報管理

4.4.1 情報登録

①情報保有者以外の情報登録の排除

uPort，Sovrin 共に，当人確認に成功した情報保有者のみが登録可能な仕組みである．なお，Sovrin の場合，Ledger に登録されたアイデンティティ情報の修正・削除は不可能である．

SSIMS ではブロックチェーンの利用が期待されているが，修正・削除を必要とするようなアイデンティティ情報を対象とする場合は注意が必要である．修正・削除が必要となるアイデンティティ情報は，Sovrin のように，Ledger ではなく User Agent 内で登録・管理する，あるいは uPort のように，スマートコントラクトと IPFS の組み合わせで登録・管理する，などの配慮が必要であろう．

②不正な情報の登録回避/登録情報の不正確認後の対応

uPort および Sovrin 共に，不正な情報の登録を回避する機能は提供されていない．そもそも，登録情報は暗号化されている場合もあり，SSIMS での確実な検査は難しい．なお，Sovrin では，不正な情報登録をしないという誓約書への署名を求めることにより，一定の抑止効果を狙っている．

一方，情報の登録・流通を支援するシステムとしては，万一，不正な情報の登録・流通により個人や社会へ被害が発生した場合は，不正な情報の登録（発信）者のみならず，その不正な情報の登録・流通を支援したシステム運営事業者も一定の責任を負う必要があり，SSIMS 事業者もまたその責任を負う必要があろう．

万一，SSIMS が登録・流通を支援した情報による被害が発生した場合は，SSIMS 事業者は保有する登録者の身元情報あるいは身元確認が可能な情報（身元情報保有機関と登録 ID 等）の提供により捜査・調査機関による登録者の特定・追跡・責任追及，被害者救済のための活動を支援する必要があろう．

なお，登録情報の形式・表現の標準化の進展と，暗号技術を利用した仕組みの研究により，SSIMS 事業者が情報内容を知ることなく，一定の範囲の不正な登録情報の検知が可能になることも期待される．

③既登録情報との整合性確認

uPort および Sovrin 共に，登録情報の既登録情報との整合性確認機能は提供されていない．

利用者（情報保有者）にとっては，このような登録情報の一貫性の確認は望ましい機能であるが，暗号化情報間の内容の整合性確認は一般には困難であろう．将来的には，登録情報の形式・表現の標準化の進展と，暗号技術を利用した仕組みの研究により，暗号化された情報間の一定の範囲の整合性確認が可能になることが期待される．

4.4.2 情報保護

①情報保有者以外の情報保護制御の排除

情報の保護は，uPort および Sovrin 共に，SSIMS 事業者が関与することなく，情報保有者の判断で保護の範囲，保護方式等が決定されている．

②登録情報の多様な保護方式

uPort では，情報保有者は，公開領域のスマートコントラクト経由 IPFS 上でアイデンティティ情報を管理する．公開を制限する情報の場合は，適切な暗号化・鍵管理により，公開範囲を限定している．

Sovrin では，情報保有者は，非公開領域の User Agent 内あるいは公開領域の Sovrin Ledger 上でアイデンティティ情報を管理する．個人情報・プライバシー情報を含むアイデンティティ情報は，暗号化されていたとしても Ledger には登録せず，User Agent で管理するのを原則としている．Ledger には，提供情報の検証に使用される TTP の公開鍵証明書等が登録される．

Sovrin のように，非公開領域，公開領域の使い分けが可能なことは，管理対象情報の特質に応じた保護方式の選択を可能とし望ましい．

③登録情報へのアクセスの記録

uPort および Sovrin 共に，登録情報へのアクセスを記録・管理する機能は無い．

事後の監査に対応できるよう，アクセス情報の記録・管理が望ましい．また，アクセス者の特定・追跡を可能とするよう．アクセス者の身元確認，利用時の当人確認が必要となろう．

4.4.3 情報提供

①情報保有者以外の情報提供制御の排除

uPort および Sovrin 共に，提供依頼情報の妥当性，提供情報の作成，提供先への情報提供の判断は，モバイルデバイス上での情報保有者の指示のみに基づき実施される．

②提供情報の多様な最小化対応

uPort では，暗号化されているフィールドの復号のための公開鍵の提供などを含め，IPFS 上の登録情報をそのまま提供，あるいは登録情報をモバイルデバイス上で加工し提供，等が想定されている．モバイルデバイス上でのマスキングや一部抽出・削除等の加工の機能は提供されておらず，別途実装が必要である．

Sovrin では，User Agent にて提供情報の作成が想定されている．User Agent に登録・管理されているアイデンティティ情報をそのまま提供，あるいは登録情報を User Agent 内で加工し提供，等が想定されている．User Agent では，ZKP（ゼロ知識証明）を利用した提供情報の最小化機能が提供されている．具体的には，属性値が指定された値と一致するかどうか，属性値が指定された範囲に入っているかどうか，当該要素が指定された集合の要素かどうか，の 3 種の情報を，属性値や要素が記載されている TTP が発行する証明書の内容を開示せず，その情報が証明書の内容に合致していることを提供者へ示すことができる機能が用意されている．

一般に，提供する情報は，必要最小限に留めることが望ましい．同時に，提供先が提供情報の信頼性を確認できるよう，信頼できる第三者による提供情報への保証を付与することが望ましい．

必要最小限の提供情報の作成には，何らかの登録情報の加工，一部のフィールドの抽出，不要なフィールドのマスキング，フィールドの属性値の変形，質問への回答創出等の機能が期待される．

一方，このような加工された提供情報に信頼できる第三者による保証を付与するには，提供情報がもともとの登録情報（TTP により発行され一定の保証の裏付けのある登録情報）の内容に合致することを，もともとの登録情報を開示せずに証明できる仕組みが必要となる．

今後，アイデンティティ情報の標準化と提供情報の標準化が進展するにつれ，さまざまの提供情報創出の仕組み，もともとの登録情報に対する第三者の保証を利用した提供情報の保証の仕組み，の研究開発が展開されるものと期待される．

③提供先・提供情報の記録

uPort の場合は，モバイルデバイス上の uPort app 経由，Sovrin の場合はモバイルデバイス上の User Client App 経由または User Agent の Direct Communication による提供が想定されるが，uPort および Sovrin 共に，情報提供時の提供先・提供情報を記録・管理する機能は無い．

事後の監査に対応できるよう，提供先・提供情報の記録・管理が望ましい．

機能分類		期待される機能および検討が必要な課題
本人確認	（身元確認）	利用登録時の情報保有者の確実な身元確認
	（当人確認）	利用時の情報保有者の確実な当人確認
情報管理	（情報登録）	①情報保有者以外の情報登録の排除 ②不正な情報の登録回避/登録情報の不正確認後の対応 ③既登録情報との整合性確認
	（情報保護）	①情報保有者以外の情報保護制御の排除 ②登録情報の多様な保護方式 ③登録情報へのアクセスの記録
	（情報提供）	①情報保有者以外の情報提供制御の排除 ②提供情報の多様な最小化対応 ③提供先・提供情報の記録

図８　SSIMS に期待される主要な機能一覧

5. おわりに

個人の活動がインターネット上で展開されるサイバー社会へ移行する中，活動を支える様々の個人のアイデンティティ情報もインターネット経由でのタイムリーな提供が求められることになろう．本稿では，個人がインターネット上でのアイデンティティ情報の安心・安全な利活用を可能とする自己主権型アイデンティティ情報利活用基盤（SSIUF）の早期の社会実装が必要との認識から，SSIUF のあり方，要件，検討課題等の考察，および SSIUF の中核を担うであろう自己主権型アイデンティティ情報管理システム（SSIMS）に期待される機能について考察した．

SSIUF の実現に向けては，まず TTP が発行するアイデンティティ情報の一定のレベルの標準化が望まれる．分野ごとのアイデンティティ情報あるいは構成する情報単位（属性）の整理・体系化，および分野には依存しないであろうアイデンティティ情報や発行者の署名等の表現形式（Verifiable Credential（VC）の表現形式）などの標準化が望まれる．なお, VC の表現形式については, JSON-JWT, JSON-LD，JSON-LD ZKP with BBS+，JSON-ZKP-CL 等が定義されている．複数の表現形式が共存するあるいは概ね一つの方式に集約されるかは，今後，いろいろ応用分野への適用研究により結論が出るものと考えらえる．

情報保有者が依頼者へ提供する提供情報，提供情報が TTP 発行のアイデンティティ情報の変形であることを確認できる情報を含め，表現形式（Verifiable Presentation（VP）の表現形式）の一定の標準化も望ましい. VP の表現形式は，VC の表現形式の研究の中で並行し検討されるものと考えられる．

SSIMS には，VC から VP への写像（生成する機能）が期待されている．現状の uPort，Sovrin では，一部 ZKP を利用した高度な機能も一部用意されているが，実用には程遠い. VC および VP の表現形式等に関する研究から一定の標準化の進展により, VC から VP への高度な変換機能の実現も容易になるものと考えられる．

TTP 発行ではないアイデンティティ情報の登録は，不適切な情報，不正な情報の登録の危険性もあり，第三者や組織・社会へ被害も考えられる．SSIMS にて登録情報の妥当性に関する可能な検査は行うのが望ましいが，完全な検査は不可能なため，SSIMS の社会的責任として，事後のすみやかな対応の仕組みを整備しておく必要があろう．

SSIUF，SSIMS に関する議論・研究が進み，安心・安全で，効率的に簡便に活用できる，自己主権型のアイデンティティ情報利活用基盤の早期の社会実装を期待したい．

謝辞　本研究の一部は，一般財団法人テレコム先端技術研究支援センターの研究助成，および JSPS 科研費 基盤(B) JP18H03240 の支援を受けている．

参考文献

[1] 才所敏明, 辻井重雄, 櫻井幸一. “自己主権型アイデンティティ情報管理システム（uPort,Sovrin）考察”. 電子情報通信学会ソサイエティ大会. 2021. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20210916IEICE_soc2021Paper.pdf.

[2] 才所敏明, 辻井重雄, 櫻井幸一. “自己主権型アイデンティティ情報管理システムに関する一考察“. 電子情報通信学会総合大会. 2021. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20210312IEICE_gen2021Paper.pdf

[3] 才所敏明, 辻井重男. “インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立”. 電子情報通信学会暗号と情報セキュリティシンポジューム. 2021. http://advanced-it.co.jp/2016_wp/wp-

content/pdf/20210120SCIS2021Paper.pdf
[4] 才所敏明，辻井重男.”インターネット時代の本人確認基盤に関する考察－ NAF から GAF へ －”. 情報処理学会コンピュータセキュリティシンポジューム. 2020. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20201026CSS2020Paper.pdf
[5] 才所敏明. “NAFJP における本人確認方法に関する考察（National Authentication Framework in Japan）”. 情報処理学会コンピュータセキュリティシンポジューム. 2019. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20191021CSS-NAFJP_paper.pdf
[6] 才所敏明，辻井重男. “日本における本人確認基盤（NAFJA：National Authentication Framework in Japan）の考察”. 情報処理学会第 85 回コンピュータセキュリティ研究会. 2019. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20190524CSEC85_paper.pdf
[7] Christian Lundkvist, Rouven Heck, et al. “UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY”. 2016. https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf
[8] “Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust”. Sovrin Foundation. 2018. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf
[9] Paul Dunphy, Fabien A. P. Petitcolas. “A First Look at Identity Management Schemes on the Blockchain”. IEEE Security & Privacy, 2018. https://ieeexplore.ieee.org/document/8425607
[10] Yang Liua, Debiao He, et al. “Blockchain-based identity management systems: A review”. 2020. https://profsandhu.com/cspecc_publications/2020/Blockchain-Based_IMS_A_Review.pdf
[11] Komal Gilani, Emmanuel Bertin, et al. “A survey on blockchain-based identity management and decentralized privacy for personal data”. 2020. https://hal.archives-ouvertes.fr/hal-02650705/document
[12] Christopher Allen. “The Path to Self-Sovereign Identity”. 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[13] Kim Cameron. “The Laws of Identity”.2005. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

【 この位置に改ページを入れ, 以降のページを印刷対象外とする 】