

## 分散型 ID (DID)/検証可能属性証明 (VC) 技術を利用した 自己主権型アイデンティティ情報利活用基盤 (SSIUF) に関する考察

### Self-Sovereign Identity-information Utilization Framework using Decentralized Identifier/Verifiable Credential technologies

才所 敏明\*<sup>1</sup>                      辻井 重男\*<sup>2</sup>                      櫻井 幸一\*<sup>3</sup>  
Toshiaki Saisho                      Shigeo Tsujii                      Sakurai Kouichi

あらまし 個人の様々の活動がインターネット上で展開される時代へと移行する中、活動の過程で求められるアイデンティティ情報もネット経由の提供へ移行することが想定される。筆者らが提案する自己主権型アイデンティティ情報利活用基盤 (SSIUF) は、構成するエンティティ間での安全なアイデンティティ情報の流通およびアイデンティティ情報の検証を可能とする情報流通基盤である。本稿では、W3C で議論・標準化が進められている分散型 ID (DID) 技術、検証可能属性証明 (VC) 技術を活用した利用者の匿名性と特定・追跡性の両立を可能とする SSIUF の構成を提案し、匿名性および特定・追跡性の観点からの実装時および運用時の要件を考察する。

**キーワード** 自己主権型アイデンティティ, SSI, 自己主権型アイデンティティ情報利活用基盤, SSIUF, W3C, 分散型 ID, DID, 検証可能属性証明, VC, 匿名性, 特定性, 追跡性

**Abstract** As various individual activities shift to an era in which they are developed on the Internet, it is expected that the identity information required in the activities will also shift to the provision via the Internet. The Self-Sovereign Identity-information Utilization Framework (SSIUF) proposed by the authors is an information distribution platform that enables secure distribution of identity information and verification of identity information between constituent entities. In this paper, we are proposing SSIUF which enables both anonymity and identifiability / trackability of users by utilizing Decentralized Identifiers (DID) technology and Verifiable Credentials (VC) technology, which are being discussed and standardized by W3C. Also, we are proposing the configuration of SSIUF and consider the requirements at the time of implementation and operation from the viewpoint of anonymity and identifiability / trackability.

**Keyword** SSI, Self-Sovereign Identity-information Utilization Framework, SSIUF, W3C, Decentralized Identifier, DID, Verifiable Credential, VC, Anonymity, Identifiability, Trackability

## 1 はじめに\*

1974 年の TCP/IP 発表に始まるインターネットの歴史は高々半世紀ではあるが、今やインターネット無しでは産業界の経済活動や国民の生活活動も成り立たない、まさにインターネット (依存) 社会である。個人の活動もインターネット上の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、アイデンティティ情報の信頼性と個人情報・プライバシー保護を個別に工夫しつつ、実際に授受も行われ始めている。今後、インターネット経由での個人の活動が増加

\*1 (株) IT 企画 <http://advanced-it.co.jp/>  
(株) ZenmuTech <https://www.zenmutech.com/>  
mail: toshiaki.saisho@advanced-it.co.jp  
\*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所  
& サイバーセキュリティセンター  
(株) 国際電気通信基盤技術研究所  
mail: sakurai@INF.kyushu-u.ac.jp

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ことが想定される中、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管理、提供、活用を可能とする基盤は、個人の様々の社会活動のDX推進に必要な基盤の一つとして、早期の構築が期待される。

## 2 自己主権型アイデンティティ情報活用基盤 (SSIUF) 概要

SSIUF (Self-Sovereign Identity-information Utilization Framework) とは、筆者らが提案しているアイデンティティ情報保有者による自身の情報への確実な制御を可能とする自己主権型アイデンティティ情報活用基盤である ([1]~[3])。

SSIUF を構成する主要エンティティは、アイデンティティ情報保有者である利用者 (個人)、アイデンティティ情報の発行組織、アイデンティティ情報の使用組織の3種を想定している (図1)。また、利用者は様々のアイデンティティ情報の安全・確実な管理が必要となり、保有する情報の管理を支援するシステムが必要になるものと想定している。

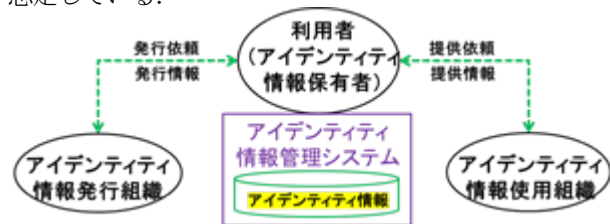


図1 SSIUFの主要構成エンティティ

## 3 分散型 ID (DID) / 検証可能属性証明 (VC) 技術概要

デジタル・アイデンティティ情報の使用に関する自己主権性およびデジタル・アイデンティティ情報の検証可能性を目指し、分散型 ID (DID : Decentralized Identifier) および検証可能属性証明 (VC : Verifiable Credential) の技術が W3C (World Wide Web Consortium) で標準化が進められている ([7]~[8])。

本章では、SSIUF の構成に利用する分散型 ID (DID) 技術、検証可能属性証明 (VC) 技術の特徴をまとめている。

### 3.1 分散型 ID (DID) 技術

分散型 ID (DID) 技術は、分散する多数の DID 発行組織がグローバルでユニークな ID である DID の発行を可能とする技術であり、また発行された DID の正当な所有者であることの検証が可能である ([7])。

DID 発行組織は、アイデンティティ情報発行組織、情報保有者、情報使用組織等の SSIUF を構成するエンティ

ティに、DID および秘密鍵を発行すると同時に、その DID に関する情報を DID Document としてまとめ、DID と DID Document の対を、一定の範囲の公開を前提とした、改ざんのリスクを回避可能な、Blockchain 等の Verifiable Data Registry (VDR) へ登録する (図2)。

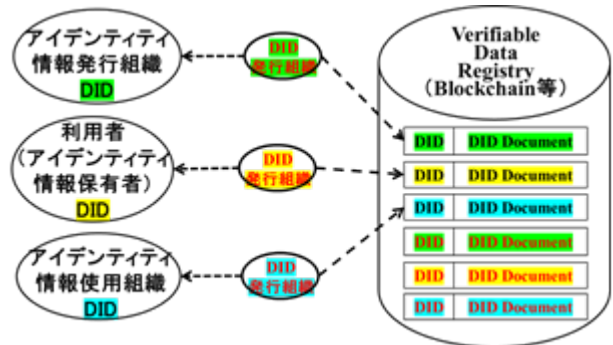


図2 DIDおよびDID Documentの発行

DID 発行組織が発行する DID は、発行組織ごとに異なる情報を含み、グローバルにユニークな ID であることが保証されている。また、DID Document には DID に紐づけられた秘密鍵に対応する公開鍵が格納され、秘密鍵・公開鍵のペアを利用した署名付与・検証により、DID 保有エンティティの真正性が確認できる (図3)。

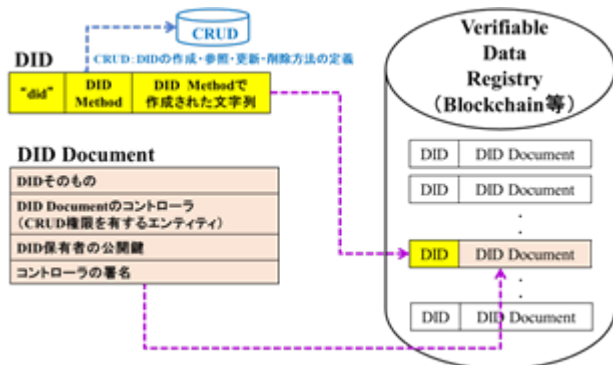


図3 DIDおよびDID Documentの内容概要

### 3.2 検証可能属性証明 (VC) 技術

検証可能属性証明 (VC) 技術は、アイデンティティ情報発行組織が情報保有者のアイデンティティ情報の保有を証明する VC (Verifiable Credential) を発行する技術、およびアイデンティティ情報保有者が VC を利用しアイデンティティ情報を情報使用組織へ提供・証明する VP (Verifiable Presentation) を発行する技術である。

VC (Verifiable Credential) は、VC 発行組織 (アイデンティティ情報発行組織) の DID、アイデンティティ情報本体、発行組織の署名等、から構成されている。VDR (Verifiable Data Registry) に格納されている VC 発行組織の DID に対応する DID Document から紐づけられている公開鍵を入手し署名を検証することにより、VC 発行組織の DID の真正性を確認できる (図4)。

VP (Verifiable Presentation) は、VP 発行者 (アイデンティティ情報保有者) の DID, 内蔵する VC, VP 発行者の署名等, から構成されている。VC と同様, VP 発行者の DID に対応する公開鍵を VDR から入手し署名を検証することにより, VP 発行者の DID の真正性を確認できる (図4)。

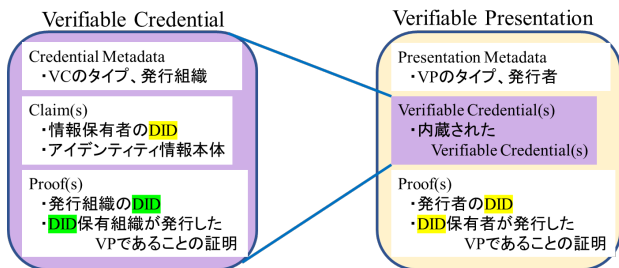


図4 VCおよびVCを内蔵するVPの構成例

このような DID および VC/VP によるアイデンティティ情報の基本的な利用 (流通) 形態を図5に示す。エンティティ間で授受される VC/VP 等には, 一般に送信先・送信元を示す DID が含まれており, 送信元 DID の署名の検証により送信 DID の真正性確認が可能である。

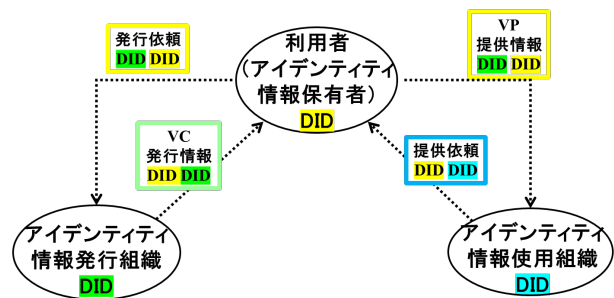


図5 DIDおよびVC/VPによるアイデンティティ情報の基本的な利用 (流通) 形態

#### 4 DID/VC 技術による SSIUF の構成

自己主権性を目指す SSIUF では, 利用者がアイデンティティ情報保有者であることの確認 (本人確認) が重要である。一方, 利用者の個人情報・プライバシー情報を使用した確実な本人確認を行う SSIUF においても, 利用者の一定の匿名性の確保が必要である。更に, 万一, 安心・安全な社会維持のための合法的捜査・調査が必要な場合は, 利用者の確実な特定・追跡も必要となろう。

筆者らは SSIUF の構成検討にあたって, 確実な利用者の本人確認および利用者の匿名性と特定・追跡性の両立の実現, 個人情報・プライバシー情報を保護しつつも社会的責任を果たせる, 安心・安全な社会情報基盤の一つとなりうる SSIUF, を目指した。

本章では, まず利用者の匿名性のみを確保しつつアイデンティティ情報の授受を可能とする SSIUF の構成を示す。次に, 利用者の特定・追跡性を匿名性と両立させる形で導入した利用者の匿名性と特定・追跡性を両立する

SSIUF の構成を提案する。最後に, 利用者の匿名性と特定・追跡性を両立する SSIUF 提案構成についての考察をまとめている。

#### 4.1 利用者の匿名性を確保可能な SSIUF の構成

W3C で標準化が進められている分散型 ID (DID) 技術および検証可能属性証明 (VC) 技術を利用したアイデンティティ情報の授受の仕組みを利用した, 匿名性のみを確保可能な SSIUF の構成を図6に示している。

利用者 (アイデンティティ情報保有者) は Cyber World ではそれぞれに発行された DID という仮名の Cyber Entity として識別され, VDR に登録されている DID に対応する DID Document 内に実名や住所等の個人情報を登録しない限り, DID によるアイデンティティ情報等の授受における利用者の一定の匿名性を確保できる。

また, それぞれの Cyber Entity が受信する情報および送信元 DID として指定される送信元の Cyber Entity の真正性は, 送信元 DID に対応する秘密鍵による署名の, VDR に登録されている送信元 DID に対応する DID Document 内の公開鍵による署名検証により確認できる。

DID/VC 技術の応用により, DID という仮名の仕組みを利用した一定の匿名性を確保可能な SSIUF の構成が可能である。

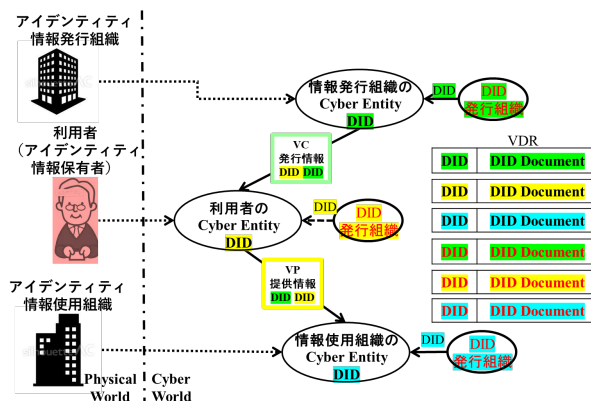


図6 匿名性を確保可能な SSIUF 構成

#### 4.2 利用者の匿名性と特定・追跡性の両立が可能な SSIUF 構成

前節で示した利用者の匿名性のみを確保可能な SSIUF 構成では, 利用者 (アイデンティティ情報保有者) の Cyber Entity の DID の真正性の確認は実施するが, その Cyber Entity に対応する Physical Entity そのものである利用者を確認する機能は無い。

本節では, 利用者の匿名性を確保しつつも利用者の特定・追跡を可能とする SSIUF の構成を提案する (図7)。匿名性のみを確保可能な SSIUF 構成 (図6) へ次の機能を追加した構成である。

①身元確認実施 DID 発行組織における

- a : 身元の確認
  - b : 身元情報 DB の管理
  - c : DID Document へ身元確認済情報の付加
- ②身元確認省略 DID 発行組織における
- a : 身元確認済 DID の確認
  - b : DID 対応 DB の管理
  - c : DID Document へ身元確認済情報の付加

具体的には、利用者（アイデンティティ情報保有者）の Cyber Entity へ DID を発行する DID 発行組織は、利用者の身元を確認の上、DID を発行するものとする。また、発行した DID と利用者の身元情報の対応（身元情報 DB）を安全に管理するものとする。万一、合法的捜査上、DID を保有する Cyber Entity に対応する利用者の特定・追跡が必要な場合は、その DID の発行組織の協力により利用者の身元情報を入手でき、特定・追跡を可能とする仕組みである。

ところが、一般に利用者は複数の DID を用途に応じて利用することが想定され、更に複数の異なる DID 発行組織の利用も想定される。それぞれの DID 発行組織にて身元確認を実施することは、利用者は身元情報を複数の DID 発行組織へ開示することが必要となり、またすべての DID 発行組織では利用者の身元情報の安全な管理が不可欠となり、利用者にとっても DID 発行組織においても大きなリスクを負うことになり好ましくない。

そこで、図7に示すように、利用者の身元確認を実施する DID 発行組織を少数に限定できるような仕組み、身元確認済であることが確認されている DID に基づく新たな DID の発行依頼時には、身元確認を省略できる仕組みを想定している。

具体的には、DID 発行組織が利用者の身元確認の上、新たな DID を発行した場合、DID 発行組織が DID Document 内に、身元確認済であることを示す情報を付加するものとする。利用者が新たに DID の発行を DID 発行組織へ依頼する時に身元確認済の DID を提示した場合、新たな DID を発行する DID 発行組織は身元確認を省略し、新たに発行する DID Document 内に身元確認済であることを示す情報を含めるものとする。なお、DID 発行組織は新たに発行する DID と利用者が提示した身元確認済 DID の対応（DID 対応 DB）を安全に管理するものとする。

このような仕組みにより、身元確認を省略した DID についても、万一、合法的捜査上、DID を保有する Cyber Entity の利用者（Physical Entity）の特定・追跡が必要な場合は、DID 発行組織が管理する DID 対応 DB を次々とたどることにより身元確認を実施した DID の発行組織を特定し、その発行組織の協力により利用者の身元情報を入手でき、特定・追跡が可能となる。

一方、以上のような仕組みの追加にもかかわらず、利用者（アイデンティティ情報保有者）、アイデンティティ情報発行組織、アイデンティティ情報使用組織間の情報

の授受は、発行された DID という仮名で行われ、一定の匿名性は維持されている。

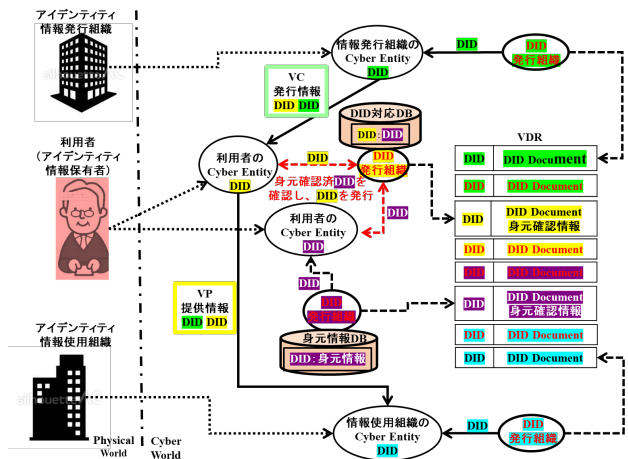


図7 匿名性と特定・追跡性を両立可能な SSIUF 構成

### 4.3 匿名性と特定・追跡性を両立可能な SSIUF 構成の考察

本節では、匿名性と特定・追跡性の両立を目指し提案した自己主権型アイデンティティ情報利活用基盤 SSIUF の構成（図7）について考察する。

#### (1)構成方式に関する考察

##### ①DID 発行組織にて確実な身元確認を実施する方式

SSIUF 利用者の確実な身元確認は必須の要件ではあるが、SSIUF に限らずインターネット上のサービスでも確実な身元確認が必要である。インターネット上の多くのサービスでは身元確認が不十分なため、様々の社会課題を引き起こしているのが現状である。社会のインターネット依存が進む中、安心・安全な社会の維持・発展には確実な身元確認を含め本人確認がますます重要となるとの認識から、筆者らはインターネット上の共通の本人確認基盤 (NAF: National Authentication Framework) を提案中である ([4]~[6])。SSIUF においても、このような各国で構築が期待される本人確認基盤 (NAF) の利用が望ましいが、NAF 整備が進むまでは SSIUF 独自に確実な身元確認機能を内蔵する必要がある。

##### ②身元確認を実施する DID 発行組織を限定する方式

利用者は、匿名性維持のため、複数の DID 発行組織の利用も想定されるが、それぞれの DID 発行組織では確実な身元確認の実施のための運用負担が求められ、一方、利用者は個人情報である身元情報を複数の DID 発行組織へ開示するというリスクを負うことになる。

そこで、すべての DID 発行組織への身元確認のための運用負担・利用者への個人情報開示のリスクを課す方式ではなく、身元確認を実施する DID 発行組織が発行する DID の提示により、身元確認を省略し新たな DID の発行を行う DID 発行組織を導入した。



### ③利用者の特定・追跡のための情報の管理方式

身元確認を実施する DID 発行組織では、発行した DID と身元情報の対応（身元情報 DB）を管理するものとする。また、身元確認を省略する DID 発行組織では、利用者が提示する身元確認済 DID と新たに発行する DID の対応（DID 対応 DB）を管理する。

身元情報は、個人情報のため利用者の匿名性維持のためには安全に管理する必要がある。また、利用者の特定・追跡のためには確実に管理する必要がある。

DID 対応 DB の情報は個人情報ではないが、DID 間の連結情報の漏洩は利用者の匿名性を脅かすため、安全に管理する必要がある。また利用者の特定・追跡のためには確実な管理が必要である。

このような、DID 発行組織が安全・確実に管理する必要がある身元情報 DB および DID 対応 DB は、通常の DID 発行には使用しないため、必ずしも DID 発行組織が管理する必要はない。利用者の特定・追跡のための情報として、別途の組織あるいは少数の DID 発行組織に安全・確実な管理を託する方式も考えられる。

### ④DID Document へ身元確認済情報を付加する方式

身元確認済情報の具体的な検討は今後であるが、身元確認の信頼性のレベルを付加する予定であり、NIST のドキュメントで定義されている身元確認方式の信頼性レベルを採用する方式を想定している ([9])。

### (2)利用者の匿名性に関する考察

匿名性のみを確保可能な SSIUF (図 6) は DID/VC 技術により構成され、利用者は仮名 DID として識別され、一定の匿名性の確保が可能である。

匿名性と特定・追跡性の両立を目指した SSIUF 構成 (図 7) で追加された機能に対する、利用者の確実な匿名性の観点からの考察結果を以下にまとめている。考察結果に留意した SSIUF の設計・実装・運用により、利用者の匿名性の確保が可能である。

#### ①身元確認実施 DID 発行組織における追加機能

##### a : 身元の確認

DID 発行組織の身元確認プロセスでの、個人情報・プライバシー情報の確実な保護が必要

##### b : 身元情報 DB の管理

DID 発行組織では、個人情報である身元情報が漏洩しないよう、身元情報 DB の安全な管理が必要

##### c : DID Document へ身元確認済情報の付加

公開情報である VDR 内の DID Document へ付加する身元確認済情報には、利用者を推測できるような情報を含めないことが必要

#### ②身元確認省略 DID 発行組織における追加機能

##### a : 身元確認済 DID の確認

DID Document 内の身元確認済情報の確認のみでよい (特に留意すべき事項は無い)

##### b : DID 対応 DB の管理

身元確認済 DID と新たに発行する DID の対応情報の漏洩は、DID に対応する利用者の特定不能性の大

きなりリスクとなるため、DID 対応 DB の安全な管理が必要

##### c : DID Document へ身元確認済情報の付加

公開情報である VDR 内の DID Document へ付加する身元確認済情報には、DID 間の連結を推測できるような情報を含めないことが必要

### (3)利用者の特定・追跡性の観点からの要件

匿名性のみを確保可能な SSIUF (図 6) では、そもそも DID 発行組織では利用者の身元確認を一切行わないので、合法的捜査が必要になっても、利用者の特定・追跡は不可能であるが、利用者の匿名性と特定・追跡性の両立を目指した SSIUF 構成 (図 7) では、利用者の特定・追跡が可能である。

匿名性と特定・追跡性の両立を目指した SSIUF 構成 (図 7) で追加された機能に対する、利用者の確実な特定・追跡性確保の観点からの考察結果を以下にまとめている。考察結果に留意した SSIUF の設計・実装・運用により、利用者の特定・追跡性の確保が可能である

#### ①身元確認実施 DID 発行組織における

##### a : 身元の確認

DID 発行組織が実施する身元確認および入手する身元情報の高い信頼性が必要

##### b : 身元情報 DB の管理

DID 発行組織では、身元情報 DB の確実な維持が必要

##### c : DID Document へ身元確認済情報の付加

身元確認済であることが確認できる情報の付加であれば良い (特に留意すべき事項は無い)

#### ②身元確認省略 DID 発行組織における

##### a : 身元確認済 DID の確認

身元確認済情報が付加されていることの確認、および身元確認済情報を付加した DID 発行組織の信頼性確認が必要

##### b : DID 対応 DB の管理

身元確認済 DID と新たに発行する DID の対応情報の消失は、利用者の特定・追跡を不可能とするため、DID 対応 DB の確実な維持が必要

##### c : DID Document へ身元確認済情報の付加

身元確認済であることが確認できる情報の付加であれば良い (特に留意すべき事項は無い)

## 5 おわりに.

個人の活動もインターネット上へ大きく移行し個人の活動の DX の進展が期待される中、ネット上でのアイデンティティ情報のやり取りが活発になることは必至で、アイデンティティ情報の利活用基盤が重要となろう。

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るため、利活用基盤においては情報保有者の自己制御性、自己主権性と共に、利用者 (情報保有者) の匿名性の確保も必要となろう。更に、安心・安全な社会の維持のために必要な様々の事故・事件等の発生時の対応が可能なるように、

利用者の特定・追跡性の確保も重要であろう。

本稿では、利用者の匿名性と特定・追跡性の両立が可能な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）の、分散型 ID (DID) 技術および検証可能属性証明 (VC) 技術による構成および各構成要素が果たすべき役割等を提案した。また、構成方式、匿名性、特定・追跡性の観点から SSIUF の考察結果を報告した。

SSIUF の実装イメージの具体化には、未だ多くの検討課題がある。その一つが、利用者が自身のアイデンティティ情報等を管理する仕組みである。多くのアイデンティティ情報の安全な管理、利用者の意思に基づくアイデンティティ情報の利活用制御を支援する、アイデンティティ情報管理システム (Identity Wallet 等) の機能、に関する検討である。今後、アイデンティティ情報管理システムを含め、SSIUF の具体的実装イメージの検討を実施する予定である。

さて、SSIUF は現状、各国国内での整備・運用を想定し検討を進めている。当然、インターネット上の個人の活動もグローバル化が進み、利用者と他国のアイデンティティ発行組織やアイデンティティ使用組織との連携、あるいは他国の利用者によるアイデンティティ情報の発行組織や使用組織との連携、も増加することが想定され、個人の活動のグローバル化に対応できる SSIUF の検討も今後の検討課題である。

EU では、EC (European Commission) と EBP (European Blockchain Partnership) の共同で、EBSI (European blockchain service infrastructure) の実現を目指しており、その活動の一環として ESSIF (European self-sovereign identity framework) の構築を目指している。ESSIF は、EU メンバーである 27 개국で国境を越えてアイデンティティ情報のやり取りを可能とすることを目指し、2022 年には ESSIF と各国の eID システムとの連携作業も開始される見込みであり、今後、ESSIF の詳細仕様・実装動向を把握しつつ、SSIUF のグローバル化対応の検討を進める予定である。

**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利活用基盤に関する考察”. 情報処理学会・コンピュータセキュリティシンポジウム. 2021. [http://advanced-it.co.jp/2016\\_wp/wp-content/pdf/20211028CSS2021Paper.pdf](http://advanced-it.co.jp/2016_wp/wp-content/pdf/20211028CSS2021Paper.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 (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](http://advanced-it.co.jp/2016_wp/wp-content/pdf/20210916IEICE_soc2021Paper.pdf)
- [3] 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](http://advanced-it.co.jp/2016_wp/wp-content/pdf/20210312IEICE_gen2021Paper.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 —」. コンピュータセキュリティシンポジウム. 2020. [http://advanced-it.co.jp/2016\\_wp/wp-content/pdf/20201026CSS2020Paper.pdf](http://advanced-it.co.jp/2016_wp/wp-content/pdf/20201026CSS2020Paper.pdf)
- [5] 才所敏明. 「NAFJA における本人確認方法に関する考察 — National Authentication Framework in Japan —」. コンピュータセキュリティシンポジウム. 2019. [http://advanced-it.co.jp/2016\\_wp/wp-content/pdf/20191021CSS-NAFJP\\_paper.pdf](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) の考察 — National Authentication Framework in Japan —」. 情報処理学会・第 85 回コンピュータセキュリティ研究発表会. 2019. [http://advanced-it.co.jp/2016\\_wp/wp-content/pdf/20190524CSEC85\\_paper.pdf](http://advanced-it.co.jp/2016_wp/wp-content/pdf/20190524CSEC85_paper.pdf)
- [7] 「Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations」. World Wide Web Consortium. 2021. <https://www.w3.org/TR/did-core/>
- [8] 「Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web」. World Wide Web Consortium. 2021. <https://www.w3.org/TR/vc-data-model/>
- [9] 「Digital Identity Guidelines: Enrollment and Identity Proofing Requirements」, NIST Special Publication 800-63A, 2017. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>
- [10] Peter Altmann, Erik Rissanen. “Self-Sovereign Digital Identity on the European Blockchain Services Infrastructure”. RISE Research Institutes of Sweden. 2020. [https://www.researchgate.net/publication/344295848\\_Self-Sovereign\\_Digital\\_Identity\\_on\\_the\\_European\\_Blockchain\\_Services\\_Infrastructure](https://www.researchgate.net/publication/344295848_Self-Sovereign_Digital_Identity_on_the_European_Blockchain_Services_Infrastructure)
- [11] “blockchain\_and\_diplomas\_use\_case\_-\_llus\_alfons\_ario\_martin\_201103”. European Commission. 2020. <https://eidproject.eu/download/v7DA4ZVxdKWFJKaVA2JiIcNgJRGSIbZmh6ZUxMUIECHBdEdIlgQA1FWZ0ZuBINtdw44FEAEKQUhe3RwTUxSUQIcF0QOWBAAARkt7Sm4XLj4xSnBZHUEpBSF7dGNAMQEXRk9ZEI8oHQZTVWJCaS4jW2ZfZ0QAaSRabW50e0d9e1BDRVRZSQEQXwFfZE9oUDYmcUBtVRhWY0hqZ>

Up2RndkUUIWWRhBFUEsVkpofG4Tf2FMAV1aH0B  
4dmJnc3hGYGRUUk9aKEEVQAdNZj8TPeM8N0wC  
clIVFycLb2p7cAopGVBOBEg/blockchain\_and\_diplom  
as\_use\_case\_-\_llus\_alfons\_ario\_martn\_201103\_.pdf

- [12] Dabiel DU Seuil. “European Self Sovereign Identity Framework – interoperability”. EBSI. 2021.  
<https://www.itu.int/en/ITU-T/webinars/20211013/Documents/Daniel%20Du%20Seuil.pdf>