SCIS 2024 2024 Symposium on
Cryptography and Information Security
Fukuoka, Japan, Jan. 23 – 26, 2024
The Institute of Electronics,
Information and Communication Engineers

安心・安全な学修歴利活用基盤（SSARUF）の考察
Considerations on Secure and Safe Academic Record Utilization Framework

才所敏明*1 Toshiaki Saisho　辻井重男*2 Shigeo Tsujii　櫻井幸一*3 Kouichi Sakurai

あらまし 1990 年代に始まった学修歴証明書のデジタル化は，インターネットの発展，普及に伴い，また人材の流動化傾向により，インターネット上でのデジタルの学修歴証明書の発行・利用システムが各国の大学等で開発・運用が進められている．我が国でも複数の大学で学修歴証明書の開発・運用が始まっており，またインターネット上での学修歴証明書の発行・利用の将来像を目指した研究開発プロジェクトも進行中である．本稿では，筆者らが提案中のブロックチェーンサービス基盤（BSI）上で動作する，検証可能な学修歴証明書の発行から検証までをサポートする安心・安全な学修歴利活用基盤（SSARUF），の構成案を提案する．SSARUF は，W3C で標準化が進められている DID/VC/VP を利用した仕組みにより，検証可能な学修歴証明書の利活用における自己制御性の実現を目指し，また，学修歴証明書の利活用にかかわる個人・法人の確実な認証の仕組み，個人（教育受講者）の匿名性および特定・追跡性の両立の仕組みにより，関係する個人・法人および社会の安心・安全の確保を目指した，学修歴証明書の利活用が可能な基盤である．

キーワード 学修歴利活用基盤，SSARUF，学修歴証明書，Academic Record，卒業証明書，学位証明書，ブロックチェーンサービス基盤，BSI，認証基盤，NAF，自己主権型アイデンティティ基盤，SSIF，アプリケーションサービス基盤，ASF，分散型 ID，DID，検証可能クレデンシャル，VC，VP，W3C

1. はじめに

教育機関が発行する学修歴証明書（卒業証明書や学位証明書）は，企業への就職や転職などの際に，教育受講者の学修歴を信頼できる形で提出するために利用されている．学修歴証明書は，正当な学修歴保有者が就職・転職等にて正当に評価されるための，採用する企業側にとっても，正当な学修歴保有者を採用するための，重要な情報である．

コンピュータ，ネットワークの利用が普及し，様々の活動がネット上へ移行する中，学修歴証明書も 1990 年代からオランダ等でデジタル化が始まり，学修歴の電子証明書発行システムの開発が進められてきた．また，インターネットの発展，普及は学修歴証明書の新たな利用パターンも可能となり，更に最近の人材の流動化傾向も相まって，インターネット上でのデジタルの学修歴証明書の発行・利用システムが各国の大学等で開発・運用が進められている（[15]，[16]）．

我が国でも，複数の大学で様々の最新技術を利用した学修歴証明書の開発・運用が始まっており，またインターネット上での学修歴証明書の発行・利用の将来像を目指した研究開発プロジェクトも進行中である（[17]，[18]）．

本稿では，筆者らが提案中のブロックチェーンサービス基盤（BSI：Blockchain Service Infrastructure）（詳細は次章）上で動作する，検証可能な学修歴情報の発行から検証までをサポートする安心・安全な学修歴利活用基盤（SSARUF：Secure and Safe Academic Record Utilization Framework），の構成案を検討し，機能面，セキュリティ面等について考察する．

*1 (株)IT 企画，(株)ZenmuTech
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

2. ブロックチェーンサービス基盤（BSI）概要

BSI は，様々のネット上のサービスに求められる，利用者の確実な本人確認，利用時の利用者の一定の匿名性の確保，不正・不法や悪意のある利用の場合の利用者の特定・追跡の確保，等の社会の安心・安全の維持に必要な機能の実装・運用を容易に実現可能とすることを目指した，提案中の構想である（[1]～[10]）.

BSI は，認証基盤（NAF : National Authentication Framework），自己主権型アイデンティティ基盤（SSIF : Self-Sovereign Identity Framework），および様々のアプリケーションサービス基盤（AS : Application Service Framework）により構成されることを想定している.

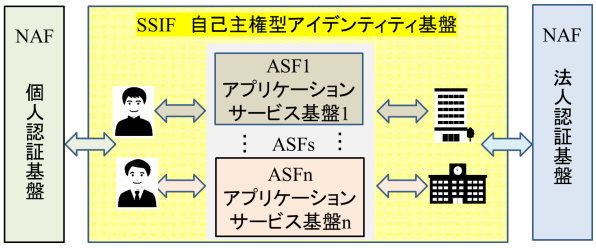

図１　BSI 構成概要

BSI を構成する認証基盤 NAF では，NAF 登録機関がサービス提供者・利用者（個人・法人）の確実な身元確認を実施し，NAF の新たなエンティティとして識別コード NAF-ID を付与すると共に，NAF-ID と身元情報の対応を管理する.

自己主権型アイデンティティ基盤 SSIF では，SSIF 登録機関が，サービスの利用を希望する個人・法人のエンティティが提示する NAF-ID の所有者であることの確認により，そのエンティティが身元確認済であることを確認し，SSIF の新たなエンティティとして識別コード SSIF-DID，W3C の DID（Decentralized Identifier）仕様（[20]）に準じた識別コード，を付与する．SSIF 登録機関はまた，NAF-ID と SSIF-DID の対応を管理する.

アプリケーションサービス基盤 ASF では，ASF 登録機関（またはサービス提供者）である SSIF 登録済みの法人がサービスの利用を希望する個人・法人のエンティティが提示する SSIF-DID の所有者であることの確認により，そのエンティティが身元確認済であることを確認し，その上でサービス提供の可否を判断する．サービス提供対象となったエンティティに対しては DID 仕様に準じた新たな識別コード ASF-DID が付与され，更に SSIF-DID と ASF-DID の対応を管理する.

SSIF や ASF で付与される DID には個人・法人を特定する情報は含まないことを前提としており，自らが身元に関する情報を開示しない限り，一定の匿名性が確保されることを想定している.

一方，一定の匿名性を維持している ASF の利用者（個人・法人）に対応するエンティティの活動において，何らかの事故・事件の発生あるいは不正・不法が疑われる活動が発見された場合には，そのエンティティの識別コード ASF-ID から合法的手続きにより，ASF 登録機関が管理する ASF-DID と SSIF-DID から利用者の SSIF-DID を特定し，SSIF 登録機関が管理する SSIF-DID と NAF-ID の対応情報から NAF-ID を特定し，NAF 登録機関が管理する NAF-ID と身元情報の対応情報から，ASF-ID に対応する利用者の特定・追跡が可能となることを想定している

以上のように，BSI では個人・法人の一定の匿名性および合法的手続きの元の特定・追跡性の確保を想定しており，BSI は，個人・法人の安心・安全な活動基盤であると共に，社会の安心・安全の維持の仕組みを備えた活動基盤となることを目指している.

BSI ではまた，W3C で標準化が進められている DID の多段/複数の利用により利用者の匿名性を確保すると共に，VC（Verifiable Credential）/VP（Verifiable Presentation）([21]）の利用によりエンティティ間の検証可能な情報の安心・安全な送受信を確保することを想定している.

3. 学修歴利活用基盤 SSARUF 概要

学修歴利活用基盤（SSARUF : Secure and Safe Academic Record Utilization Framework）は，BSI のアプリケーションサービス基盤の一つとしての実装・運用を想定している．SSARUF は，教育機関，教育受講者，学修歴評価事業者の他に，そのような SSARUF に参加する利用者(法人, 個人)の登録を担当する SSARUF 登録機関から構成される（図２）.

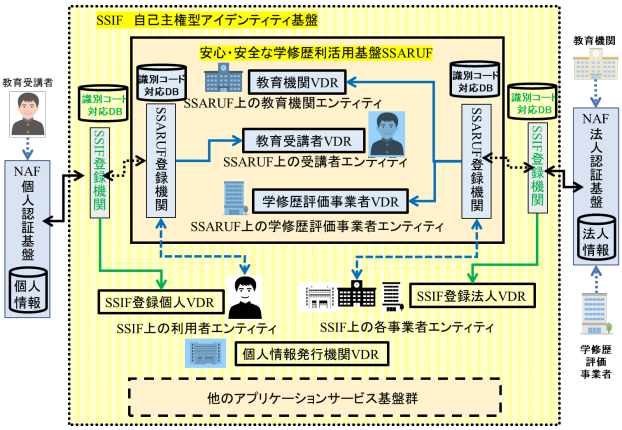

図２　BSI 上の SSARUF 構成概要

3.1 SSARUF における確実な本人確認

SSARUF を構成する教育機関，教育受講者，学修歴評価事業者の確実な身元確認は，BSI を構成する各国の認証基盤 NAF の役割とし，SSARUF 登録機関は，利用を希望する法人・個人のエンティティが，BSI 側で身元確認済であることを SSIF-DID を付与されたエンティティからの利用申請であること，およびそのエンティティ

との当人確認が成功することにより，本人確認を行うことを想定している．

各登録機関における法人・個人の当人確認は，ARUF-DID に対応する秘密鍵による署名の検証により行うことを，また署名検証に使用する ARUF-DID に対応する公開鍵は，複数存在する登録機関で管理される VDR（ブロックチェーン）に登録され公開されていることを想定している．

3.2 SSARUF 上のエンティティの識別コード ARUF-DID

SSARUF を構成するエンティティは，SSARUF 登録機関により登録される際に識別コード ARUF-DID および公開鍵ペアが付与され，ARUF-DID および対応する公開鍵を含む DID Document が VDR へ登録される．SSARUF 登録機関は複数存在することを想定しており，VDR は複数の登録機関によるコンソーシアムタイプのブロックチェーンとして実装・運用され，SSARUF 上のすべてのエンティティからの参照は可能とする．また，SSARUF 登録機関は，登録したエンティティの，登録申請時に提示された SSIF-DID と新たに付与した ARUF-DID の対応を DB に登録し，安全・確実に管理することを想定している．

3.3 SSARUF 利用者の匿名性と特定・追跡性

SSARUF 利用者は，登録時に個人を特定する情報を含まない識別コード ARUF-DID を SSARUF 登録機関より付与され，その ARUF-DID を使用し，SSARUF 上で活動を行うため，利用者の一定の匿名性が確保される．

また，SSARUF 上で匿名性が確保された ARUF-DID を使用し不正・不法あるいは悪意のある行為を行った場合は，それぞれの特定・追跡のための情報を管理している各機関に対し所定の手続きによる合法的情報開示請求により，利用者の特定・追跡性の確保を想定している．具体的には，SSARUF 登録機関が管理する ARUF-DID に対応する SSIF-DID を開示請求により確認し，更に SSIF 登録機関が管理する SSIF-DID に対応する認証基盤から付与された NAF-ID を開示請求により確認し，最後に NAF が管理する NAF-ID に対応する個人を特定するために必要な氏名・住所等を開示請求により入手することにより，不正・不法あるいは悪意のある行為を行った利用者の特定・追跡性を確保している．

3.4 SSARUF 上のエンティティ間の相互認証・通信情報保護

各エンティティは SSARUF 登録時に識別コード ARUF-DID および公開鍵ペアが付与されており，ARUF-DID および対応する公開鍵を含む DID Document が VDR に登録されている．

相互認証は，通信相手から提供される ARUF-DID および署名の，VDR より入手した ARUF-DID に対応する公開鍵による署名の検証により行うことを想定している．

通信情報は，DH 鍵共有等により安全に共有する共通鍵による暗号化等により保護することを想定している．

4. 学修歴情報の内容・形式に応じた SSARUF 構成案（６方式）と処理概要

教育機関が教育受講者へ発行する学修歴情報には様々の内容・形式が想定されるが，本章では代表的な学修歴情報の内容・形式のそれぞれに対する安心・安全な学修歴利活用基盤 SSARUF の構成案を示し，機能実現のための仕組み・手順等を説明する．

なお，本章では，利用者（教育機関，教育事業者，学修歴評価事業者）に対応するエンティティの識別コードはそれぞれ，教育機関 ARUF-DID，受講者 ARUF-DID，評価事業者 ARUF-DID と表記している．

A：学修歴情報は，学修歴を一括検証可能な単一のデータから構成

教育機関は，教育受講者の要請に応じ，学修歴証明書（VC）を含むＶＰを発行し，VC には受講者 ARUF-DID，受講者氏名を含む学修歴が記載されているケースを想定，教育受講者はその VC を含む VP にて学修歴評価事業者へ提供する（図４）．

学修歴評価事業者は，VP の発行者である受講者 ARUF-DID に対応する公開鍵を受講者 VDR より入手し VP を検証する．次に，VP に内蔵されている VC の発行者である教育機関 ARUF-DID に対応する公開鍵を教育機関 VDR より入手し VC を検証する．VC 内に記載された受講者 ARUF-DID と VP の発行者である受講者 ARUF-DID が同一であれば，VC・VP の検証は終了するが，もし異なれば，VP が VP の発行者である受講者 ARUF-DID の署名だけでなく，VC 内に記載された受講者 ARUF-DID の署名も付与されていることを確認し，VC・VP の検証は終了する．このように SSARUF では，受講者が異なる ARUF-DID を使用している場合は，それぞれの ARUF-DID の署名を付与することにより，それぞれの秘密鍵所有を確認でき，それぞれの ARUF-DID が同一の受講者に紐づけられていることを確認，という方法を想定している．

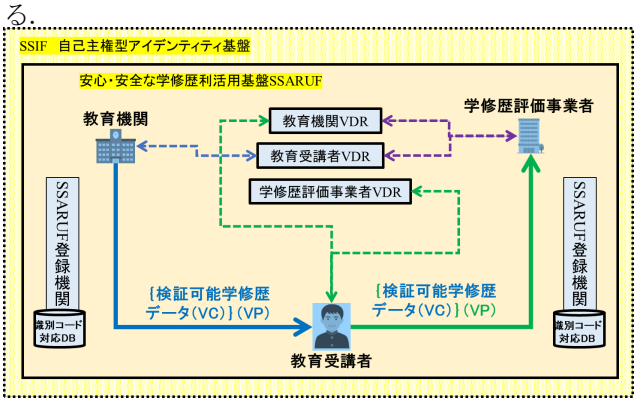

図３　SSARUF-A の情報の流れおよび各エンティティの参照情報

VC・VP の検証後に，学修歴評価事業者は学修歴の妥当性を評価する．学修歴の内容・表現形式は現時点では標準化されていないが，国内あるいはグローバルなレベルでも，一定の標準化・ガイドライン等が策定されることを期待したい．

B：学修歴情報は，項目の列で表現された学修歴データの選択的開示・検証が可能な単一のデータから構成

教育機関は学修歴情報を，“項目名：項目データ”の形式の項目の列で表現される学修歴データおよび一部の項目が削除されても検証が可能な BBS+署名による署名を付与した学修歴データを VC として発行する．教育受講者は学修歴評価事業者へ，学修歴データの中で開示しない項目の“項目名：項目データ”の列を削除し署名を変更し新たな検証可能な VC を作成の上，その VC を含む VP にて提供する．

学修歴評価事業者は，VP の発行者である受講者 ARUF-DID から対応する公開鍵を受講者 VDR より入手し VP を検証する．次に，VP に内蔵されている VC の発行者である教育機関 ARUF-DID から対応する公開鍵を教育機関 VDR から対応する公開鍵を教育機関 VDR より入手し VC を検証する．

なお，VC 内に記載された受講者 ARUF-DID と VP の発行者である受講者 ARUF-DID が異なる場合の対応は，方式 A と同一である．

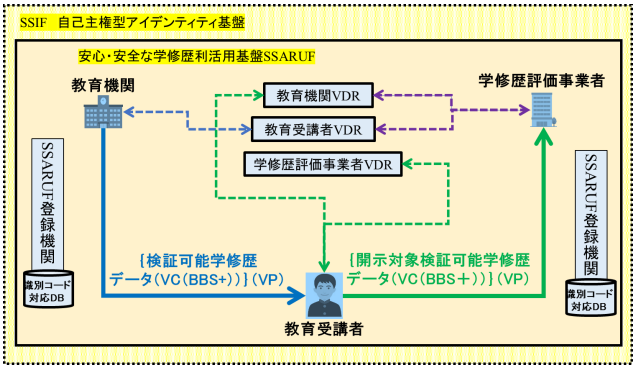

図４　SSARUF-B の情報の流れおよび各エンティティの参照情報

C：学修歴情報は，学修歴データおよびその一括検証用のデータから構成

学修歴情報が，受講者 ARUF-DID，受講者氏名が記載された学修歴データそのものと，VC として発行される学修歴検証用データ（学修歴データのハッシュ値に教育機関の署名を付与）から構成されるケースを想定している．

方式 C1 としては，教育受講者は学修歴データと学修歴検証用データ（VC）を教育機関より受領し，受領した学修歴データと学修歴検証用データ（VC）を含む VP を学修歴評価事業者へ提供することを想定している．学修歴評価事業者にとっては，学修歴データのハッシュ値の算出が必要となるが，VC・VP の検証方法は方式 A と同一である．

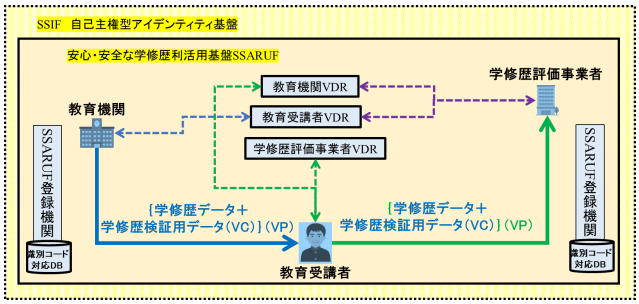

図５　SSARUF-C1 の情報の流れおよび各エンティティの参照情報

方式 C2 では，教育機関が教育受講者へ学修歴データを送信し，一方，学修歴検証用データを複数の SSARUF 登録事業者が管理する学修歴検証用データの VDR へ登録する．受講者は，学修歴検証用データの VDR より対応する学修歴検証用データを入手し，教育機関より入手した学修歴データを検証する．

教育受講者は，必要に応じ学修歴評価事業者へ学修歴データを提供する．提供を受けた学修歴評価事業者は，対応する学修歴検証用データを学修歴検証用データの VDR より入手し，教育受講者から提供を受けた学修歴データを検証する．

なお，方式 C2 は，MIT（マサチューセッツ工科大学）の研究機関 Media Lab と Learning Machine 社が共同開発した，Web 技術の標準化を行う非営利団体 W3C（World Wide Web Consortium）の標準規格 VC に準拠したブロックチェーン証明書の Blockcerts（[22]）と同等の方式となっている．

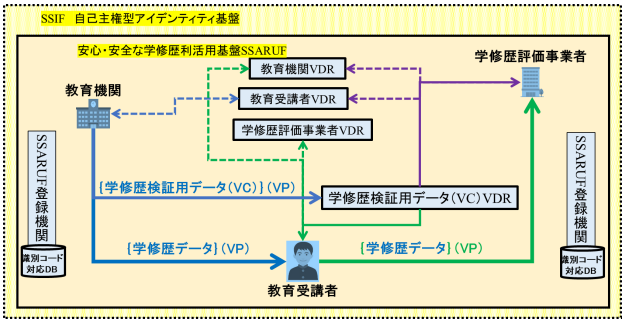

図６　SSARUF-C2 の情報の流れおよび各エンティティの参照情報

D：学修歴情報は，項目の列で表現された学修歴データおよびその選択的開示検証用のデータから構成

学修歴情報は，学修歴データは“項目名：項目データ”で表現される項目の列で表現され，VC として発行される学修歴検証用データも“項目名：項目データのハッシュ値”の列に教育機関の署名から構成されることを想定している．

方式 D1 としては，教育受講者は学修歴データの中で学修歴評価事業者に開示する項目の“項目名：項目データ”の列と，学修歴検証用データ（VC）を含む VP にて提供することを想定している．特徴は，学修

歴データの内，開示すべき項目の項目データについてのみ開示が可能，選択開示が可能なことである．

学修歴評価事業者にとっては，学修歴データのハッシュ値の算出が必要となるが，VC・VP の検証方法は方式 A と同一である．

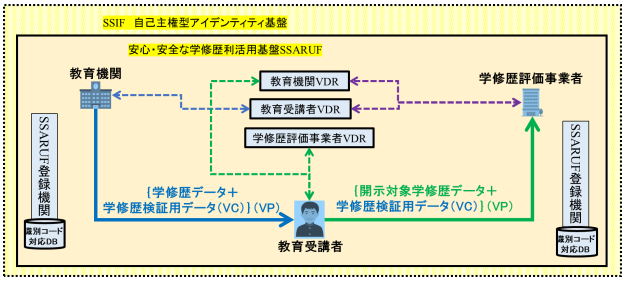

図 7　SSARUF-D1 の情報の流れおよび各エンティティの参照情報

方式 D2 では，教育機関が教育受講者へ学修歴データを送信し，また学修歴検証用データを複数の SSARUF 登録事業者が管理する学修歴検証用データの VDR へ登録する．受講者は，学修歴検証用データの VDR より対応する学修歴検証用データを入手し，教育機関より入手した学修歴データを検証する．

教育受講者は，必要に応じ学修歴評価事業者へ開示する項目のみから構成される学修歴データを提供する．提供を受けた学修歴評価事業者は，対応する学修歴検証用データを学修歴検証用データの VDR より入手し，教育受講者から提供を受けた開示学修歴データを検証する．

方式 D2 は，Web 技術の標準化を行う非営利団体 W3C（World Wide Web Consortium）の標準規格 VC に準拠したブロックチェーン証明書 Blockcerts へ選択開示機能を付加した拡張方式となっている．

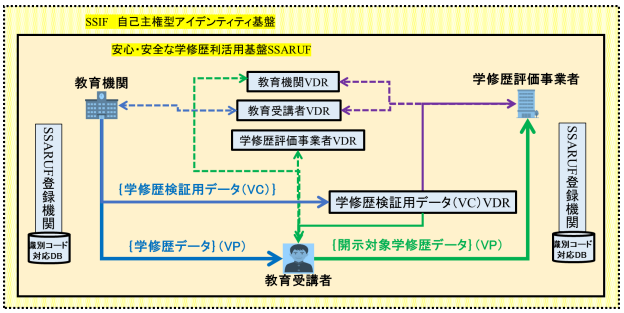

図 8　SSARUF-D2 の情報の流れおよび各エンティティの参照情報

5.　SSARUF のリスクと対応状況

SSARUF は，BSI のアプリケーションサービス基盤の一つとしての稼働を想定しており，3 章に記載した基本機能を W3C で標準化されている DID/VC/VP の活用により実現・提供することを想定している．

具体的には 4 章において，複数の学修歴情報の内容・形式に対応する SSARUF 構成案を提示し，学修歴情報の発行・提供・検証の仕組みを記載した．

本章では，提案した SSARUF 構成案・仕組みの，学修歴情報の利活用基盤としての主要なリスクへの対応について考察する．

5.1　教育機関のリスクへの対応

教育受講者へ学修歴情報を発行する教育機関の主要なリスクおよび SSARUF の対応は次の通り．

①保有する教育受講者の学修歴情報の漏えい・改ざん

学修歴情報については安全・確実に管理できる対策を教育機関が講じていることが前提．SSARUF では検討対象外としている．

②なりすまし教育受講者への学修歴情報の発行（漏えい）

教育受講者の ARUF-DID に対応する公開鍵による署名検証により，なりすましに対応可能．

5.2　教育受講者のリスクへの対応

教育機関から発行される学修歴情報を受信し管理，必要に応じ学修歴評価事業者へ提供する教育受講者の主要なリスクは以下の通り．

①教育機関から送信される学修歴情報の漏えい・改ざん

暗号技術を利用した通信情報の保護，DID/VC/VP を利用した学修歴情報の改ざん検知により対応可能．

②なりすまし教育機関による虚偽の学修歴情報

教育機関の ARUF-DID に対応する公開鍵による署名検証により，なりすましに対応可能．

③保有する学修歴情報の漏えい・改ざん

受講者が管理する情報については安全・確実に管理できるウォレットの利用が前提．本稿では検討対象外としている．

④学修歴評価事業者への必要な学修歴情報のみの提供

学修歴データの選択開示は，方式 C2，D2 にて対応可能である．

⑤なりすまし学修歴評価事業者への学修歴情報の提供（漏えい）

学修歴評価事業者の ARUF-DID に対応する公開鍵による署名検証により，なりすましに対応可能．

5.3　学修歴評価事業者のリスクへの対応

教育受講者から提供される学修歴情報を検証する学修歴評価事業者の主要なリスクおよび SSARUF の対応は次の通り．

①教育受講者から提供される学修歴情報の漏えい・改ざん

暗号技術を利用した通信情報の保護，DID/VC/VP を利用した学修歴情報の改ざん検知により対応可能．

②なりすまし教育機関による虚偽の学修歴情報

教育機関の ARUF-DID に対応する公開鍵による署名検証により，なりすましに対応可能．

③保有する教育受講者の学修歴情報の漏えい・改ざん

管理する情報については安全・確実に管理できる対

策を学修歴評価事業者が講じていることが前提．SSARUF では検討対象外としている．

④学修歴情報内の個人情報の不足への対応

一般に教育機関が発行する学修歴データ内には一般に学修歴評価事業者が必要とする個人情報は含まれず，教育受講者は別途，詳細な個人情報を求められることが多く，学修歴利活用基盤においても対応する機能が不可欠であろう．

そこで，SSARUF では教育受講者の検証可能な身元情報の，教育受講者から学修歴評価事業者への提供の仕組み，具体的には，教育受講者は SSIF 上の信頼できる検証可能な個人情報を VC として発行する機関より検証可能個人情報データ（VC）を入手し，学修歴評価機関へ提供することを想定している．

方式 A を例に，学修歴情報と共に検証可能個人情報データ（VC）を学修歴評価機関へ提供する方式への拡張方法を図 9 に示している．

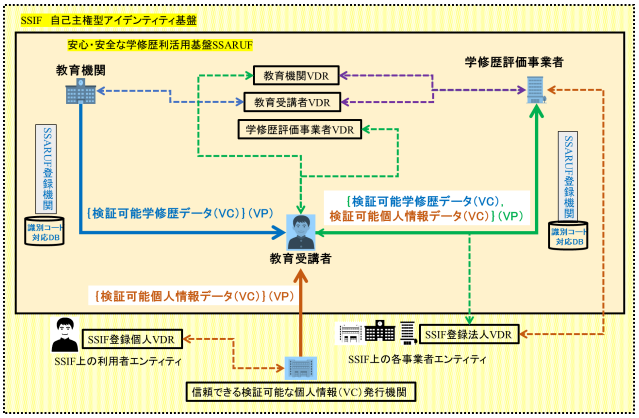

図 9　検証可能身元情報も提供する方式 A の拡張版

5.4　SSARUF 登録事業者のリスクと対応状況

方式 C2 および方式 D2 における，教育機関の要請に基づく学修歴検証用データ（VC）の登録，学修歴評価事業者の要請に基づく学修歴検証用データ（VC）の提供を担当する SSARUF 登録事業者の，主要なリスクおよび SSARUF の対応は次の通り．

①教育機関から送信され登録される学修歴検証用データの漏えい・改ざん

暗号技術を利用した通信情報の保護，DID/VC/VP を利用した学修歴情報の改ざん検知により対応可能．

②なりすまし教育機関による虚偽の学修歴検証用データの登録

教育機関の ARUF-DID に対応する公開鍵による署名検証により，なりすましに対応可能．

③管理する教育受講者の学修歴検証用データの改ざん

学修歴検証用データは VDR（ブロックチェーン）による管理であり，適切な技術の採用・運用により改ざん検知・復旧策は，SSARUF 登録事業者が講じていることが前提．本稿では検討対象外としている．

表 1　SSARUF が提供するセキュリティ機能一覧

SSARUFが提供するセキュリティ機能			特記事項
教育機関	①	保有・管理情報の保護	SSARUF外で対応
	②	なりすまし受講者の排除	
教育受講者	①	教育機関から送信される学修歴情報の保護	
	②	なりすまし教育機関の排除	
	③	保有・管理情報の保護	SSARUF外で対応
	④	不必要な学修歴データの開示の回避	C2、D2で選択開示可能
	⑤	なりすまし学修歴評価事業者の排除	
学修歴評価事業者	①	教育受講者から送信される提供学修歴情報の保護	
	②	なりすまし教育機関の排除	
	③	保有・管理情報の保護	SSARUF外で対応
	④	教育受講者の個人情報の精査	各方式共、拡張可能
SSARUF登録機関	①	教育機関から送信される学修歴検証用データの保護	
	②	なりすまし教育機関の排除	
	③	保有・管理情報の保護	SSARUF外で対応

6.　その他の学修歴利活用基盤として考慮すべき機能と，SSARUF の対応可能性

⑴学修歴証明書の失効時の対応

教育機関は，一度発行した学修歴証明書を，何らかの理由で失効させることが必要となる場合も想定される．

失効された学修歴証明書が誤用・悪用されないよう，学修歴評価事業者は学修歴証明書の検証過程で失効が検知できる仕組みが必要である．

SSARUF では，SSARUF 登録事業者が別途の失効情報 VDR を運用する方法と，構成案の C2，D2 については，登録事業者群が管理する検証用データ（VC）の VDR へ失効情報を登録する方法，いずれかの方法で対応可能である．

⑵教育機関の廃止時の対応

教育機関は統廃合される可能性がある．

卒業あるいは学位を得た教育機関が統廃合されても，教育受講者には適切な学修歴証明書の入手を可能とする仕組みが必要である．

統廃合された教育機関の学修歴情報は，統合の場合は統合後の教育機関が代理発行することが想定され，廃止の場合は他の教育機関あるいは関連機関が引き継ぎ代理発行することが想定される．

代理発行の仕組みへの対応は，学修歴証明書（学修歴データ，学修歴検証データ）の項目の追加，付与署名および使用する署名鍵についての検討は必要だが，現在の SSARUF 構成案で対応可能と考えている．

⑶ 教育受講者の学修歴情報に対する自己制御上の課題

学修歴情報は個人情報であり，教育受講者の制御の元での利活用が望ましい．

SSARUF では，教育受講者の要請に基づき学修歴情報が発行され，教育受講者の判断で学修歴評価事業者へ提供され，学修歴情報の発行・提供については教育受講者の自己制御性が確保されている．

しかし，学修歴評価事業者による学修歴情報の再配布のリスクが存在し，教育受講者による学修歴情報の流通（再配布）の制御は困難な状況である．

学修歴情報を構成する学修歴データそのものは，一般に学修歴評価事業者の担当者自らが確認する情報であり，学修歴データそのものの再配布についてはセキュアなウォレット等の利用により制御は可能と考えられるが，学修歴データの内容の担当者経由の再配布を技術的に制御することは困難である．現状では，学修歴情報の再配布の制御は，技術的対応ではなく学修歴情報提供時の契約における守秘義務により行われている．将来的に現方式での対応で問題ないかどうかは，学修歴情報の保護に関する社会の意識の変化を注視しつつの判断が必要となろう．

なお，SSARUF の方式 C2，D2 の拡張により実現可能な，SSARUF 登録事業者のような信頼できる第三者またはスマートコントラクトによる学修歴データの検証サービス方式の採用により，学修歴検証用データについては正当な学修歴評価事業者以外への開示を回避することができる．学修歴情報の意図しない流通の制御は困難だが，検証できないことによって，意図しない学修歴情報の流通によるリスクを一定程度軽減できるものと考えている．

7. おわりに

本稿では，筆者らが別途提案している，W3C で標準化が進められている DID/VC/VP をベースに構成したブロックチェーンサービス基盤 BSI，その BSI 上で稼働する安心・安全な学修歴利活用基盤 SSARUF を提案した．

SSARUF は，学修歴利活用基盤としての機能を提供すると共に，学修歴証明書の利活用にかかわる個人・法人の確実な認証の仕組み，個人（教育受講者）の匿名性および特定・追跡性の両立の仕組みによる，関係する個人・法人および社会の安心・安全確保を目指した，学修歴証明書の利活用が可能な基盤の構想である．

SSARUF の動作基盤として採用を想定している BSI は，筆者らが 2018 年頃より研究開発を進めてきた，各国の認証基盤 NAF やそのグローバルな相互運用性を目指した構想 GAF（[8]～[10]），その後の自己主権型アイデンティティ情報利活用基盤 SSIUF（[2]～[7]），をさらに発展させ，アプリケーションサービス基盤を含めた構想である．

EU では，European Blockchain Partnership (EBP) が，ブロックチェーンに関する EU 戦略を策定し，公共サービス用のブロックチェーン インフラストラクチャを構築するために創設された EU 加盟国 27 カ国とノルウェーおよびリヒテンシュタインから構成されるパートナーシップで，欧州委員会（EC）と EBP は，2019 年に欧州ブロックチェーンサービス基盤（The European Blockchain Services Infrastructure＝EBSI）の構築に着手した．EBSI ではまた，学修歴証明書の教育受講者主導の利活用が応用の一つとして検討されている．

安心・安全な学修歴利活用基盤 SSARUF およびその動作環境として採用したブロックチェーンサービス基盤 BSI は，グローバルな連携が不可欠である．現在はβ版である EBSI の構築状況，EBSI 上での学修歴利活用を含む様々の応用 PJ の構築状況を今後も注視，EBSI との相互運用の可能性も念頭に置きながら SSARUF の改良・拡張を検討する予定である．

謝辞

武市正人大学改革支援・学位授与機構名誉教授には，教育機関の統廃合時の課題の指摘等，有益な助言をいただいた．

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, 辻井重男. “ブロックチェーンサービス基盤に関する考察”. SCIS2023. https://advanced-it.co.jp/2016_wp/wp-content/pdf/20230124SCIS2023BSIpaper.pdf

[2] 才所敏明, 辻井重男, 櫻井幸一. “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）― 利用者の匿名性と特定・追跡性の両立 ―”. 情報処理学会・第 84 回全国大会. 2022. https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220305IPSJ84SSIUFPaper.pdf

[3] 才所敏明, 辻井重男, 櫻井幸一. “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”. SCIS2022. https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220119SCISPaper.pdf

[4] 才所敏明, 辻井重男, 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”. CSS2021. https://advanced-it.co.jp/2016_wp/wp-content/pdf/20211028CSS2021Paper.pdf

[5] 才所敏明, 辻井重男, 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. https://advanced-it.co.jp/2016_wp/wp-content/pdf/20210916IEICE_soc2021Paper.pdf

[6] 才所敏明, 辻井重男, 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. https://advanced-it.co.jp/2016_wp/wp-content/pdf/2

0210312IEICE_gen2021Paper.pdf
[7] 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”. SCIS2021.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20210120SCIS2021Paper.pdf
[8] 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 －“. CSS2020）.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20201026CSS2020Paper.pdf
[9] 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 －”. CSS2019.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20191021CSS-NAFJP_paper.pdf
[10] 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.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20190524CSEC85_paper.pdf
[11] 才所敏明, 辻井重男, 櫻井幸一. “安心・安全な暗号資産取引基盤の提案－SSVATF：Secure and Safe Virtual Asset Transfer Framework－”. CSS2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20221027CSS2022SSVATFPaper.pdf
[12] 才所敏明, 辻井重男. “メタバースにおける利用者の匿名性と特定・追跡性の実現方式の提案およびその安心・安全な社会維持効果についての考察”. CSS2023.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20231031CSS2023MVpaper.pdf
[13] 才所敏明, 櫻井幸一, 辻井重男. “メタバース利用者の匿名性と特定・追跡性の両立に関する考察―安心・安全なメタバースを目指して―”. 情報処理学会・DICOMO202 シンポジューム. 2023.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/2023DICOMO2023MVpaper.pdf
[14] 山下純一, 荒木俊輔, 砲崎賢一, “ブロックチェーンを用いた情報管理における個人データ保護に関する考察”, SCIS2023.
[15] “高等教育機関における電子証明書に関する調査報告書”, 独立行政法人大学改革支援・学位授与機構, 2022 年 3 月・
https://www.nicjp.niad.ac.jp/en/site/2023/02/20220426114241.pdf
[16] “諸外国における学修歴証明のデジタル化に向けた導入事例・導入方法に関する調査研究”, 未来工学研究所, 2022 年 4 月.
https://www.ifeng.or.jp/wordpress/wp-content/uploads/2022/06/JP-Digital-Credentialing-20220401.pdf
[17] “学修歴等の本人管理による人材流動の促進”, SSI/FIDO コンソーシアム, 2023 年 3 月.
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/11_The_University_of_Tokyo_report_agenda.pdf
[18] “人材育成のための Trusted な学修情報流通システム”, 人材育成のための Trusted な学修情報流通システム開発コンソーシアム, 2023 年 3 月.
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/15_Fujitsu_Japan_report_agenda.pdf
[19] “Trusted Web に係る国際標準化動向調査報告資料”, NTT データ経営研究所, 2023 年 3 月.
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/003_report_intenational_standard.pdf
[20] “Decentralized Identifiers (DIDs) v1.0”, World Wide Web Consortium, July, 2022.
https://www.w3.org/TR/vc-di-bbs/
[21] “Verifiable Credentials Data Model v2.0”, World Wide Web Consortium, September, 2023.
https://www.w3.org/TR/vc-data-model-2.0/
[22] “ The Open Standard for Blockchain Credentials”.
https://www.blockcerts.org/