第12部

Delight WG: 非中央集権的なデータセキュリティとトラスト

阿部 涼介、竹村 太希

第１章　はじめに

Deight WGでは，ブロックチェーンをはじめとしたデータセキュリティ技術と，トラストに関する研究に取り組んでいる．本年度は，9月合宿においてメンバの活動を紹介し議論した．本報告書では，9月合宿において議論した以下の2点の取り組みについて概説する．

- プロセスの履歴の記録と結果の検証可能性
- デジタルアイデンティティウォレットアプリの開発

第２章　プロセスの履歴の記録と結果の検証可能性

本取り組みは特定のプロセスの履歴を記録することによって，当該プロセスの結果の検証可能性を確保する試みである．ここでは，3Dプリントされた製造物の情報と，商取引の結果の検証可能性を確保する試みを紹介する．

2.1　3Dプリント物の情報の検証可能性

3Dプリントは，3Dモデルデータから物理的な物品を造形する仕組みである．3Dプリントの普及によって，個人が物品の製造が可能になり，様々な活用が模索されている．一方，3Dプリントされた製造物の製造責任追求のためには，“いつどこでだれが，特定の3Dモデルから物品を製造したか”を特定する必要がある．

そこで，本取り組みでは3Dプリントプロセスの一部である，3Dプリント命令を出すクライアントと3Dプリンタを制御するプリントサーバ間のやり取りに着目した．特定の3Dプリントサーバへのプリント命令と当該プリント完了のやり取りをブロックチェーン上で実施することで，製造物の情報がブロックチェーン上に記録される．

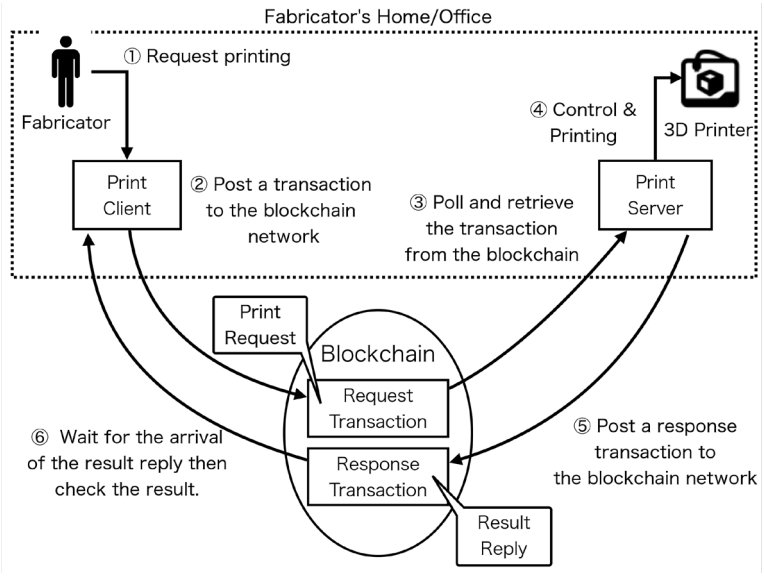

Figure 1：ブロックチェーンを通じた3Dプリントリクエストレスポンス

また，記録された情報は，ブロックチェーンの特性によって改ざん困難な形式で記録される．Fig.1に取り組みの概要を示す．

本取り組みの詳細は，IEEE ICBC 2022で発表され，ArXivにてそのフルペーパが公開されている[36, 37]．

2.2 商取引結果の検証可能性

インターネット上で，デジタルデータの売買といった様々な商取引が行われている．商取引には，販売者(Seller)からの商品の受け渡し，購入者(Buyer)からの代金の支払いが含まれる．例えば，イラストなどのデジタルデータの制作依頼の取引においては，当該商品に関する要件の合意のためのコミュニケーションが取引中に実施されることが考えられる．このような商取引において，販売者および購入者にとって双方に相手が誠実に振る舞わないことによる経済的リスクがある．具体的には，先払いのケースでは購入者が代金を支払ったにもかかわらず，販売者が商品を受け渡さないケースが考えられる．後払いのケースにおいても，販売者が商品を受け渡したにもかかわらず，購入者が代金を支払わないケースが同様に考えられる．この問題は“seller and buyer’s dilemma”として知られている[38]．

典型的には，この問題は第三者による仲介によって対処される．エスクロー（Escrow）と呼ばれる仕組みでは，取引開始時に購入者が仲介者に代金を預け，商品の受け渡しを当該仲介者が確認した上で，販売者へ代金を払い出す．仲介者を介して取引を成立させるには，仲介者が誠実に代金を預かり，商品の受け渡しを確認した上で払い出すことを販売者と購入者の双方が仮定しなければならない．従って，そのような仮定を置ける仲介者が存在しない場合，仲介者を用いた取引は実施できない．特定の仲介者に依存せず取引を実施するために，特定の管理者なくシステムを動作させることが可能なブロックチェーン技術を用いて仲介者の(一部の)機能を実現する試みがある[38, 39, 40, 41, 42, 43, 44]．これらの試みでは，特定のデータの送受信を保証する暗号プロトコルである“Fair Exchange”と，ブロックチェーン上で動作するプログラムである“スマートコントラクト”を活用する．

しかし，データの送受信の確認のみでは，先述のseller and buyer’s dilemmaへの対処としては不十分である．例えば，制作依頼の取引において，販売者が商品をFair Exchangeを用いて受け渡しはしたが，当該商品が購入者の期待する質を満たさないケースが考えられる．このケースに対処するためには，商品が期待したものであると購入者が承認した際に報酬を払い出す仕組みが考えられる．一方，購入者の承認基準はスマートコントラクトで実装可能な基準であるとは限らない．従って，seller

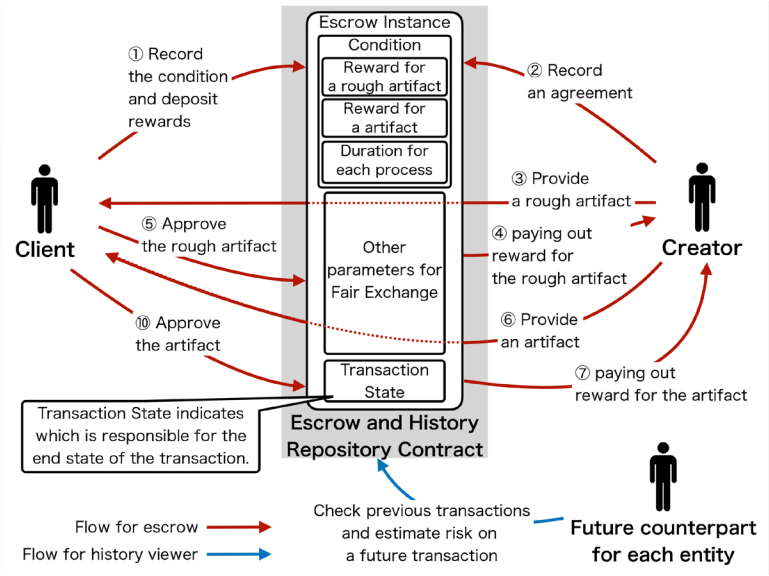

Figure 2：ブロックチェーンを通じたデジタルデータ制作依頼取引の記録と結果の検証

and buyer's dilemmaはスマートコントラクトのみでは解決できない.

購入者が商品を承認しない場合，紛争状態となり，購入者と販売者は紛争解決をする必要がある．通常，紛争解決はコストのかかる作業であるため，紛争に陥る傾向のあるエンティティを両者は取引開始前に取引相手として避けるモチベーションがある．したがって，取引開始前に対象エンティティが過去の取引を異常終了する傾向があることを確認できれば，紛争リスクを見積もり，取引相手として選択しない，あるいは代金を調節するなどの対処が可能であり，seller and buyer's dilemmaが緩和できると考えられる．

そこで，本取り組みでは，デジタルデータの制作依頼の取引を対象に取引プロセスの定義と，その実施の履歴を記録することで，取引結果を検証可能にする手法を提案する．Fig.2に提案の概要を示す．取引プロセスの定義では，各取引の終了状態が以上終了であった場合，購入者あるいは販売者どちらの責任であるかを明確化する．これによって，将来の取引相手は，当該購入者あるいは販売者が過去の取引において，その責任の下取引を異常終了する傾向があることを検証可能となる．

本取り組みの詳細はAINTEC2023にて発表され，論文はオープンアクセスにて公開されている[45]．なお，当該論文はAINTEC2023にてBest Paper Awardを受賞した．

2.3　両取り組みに共通するモデルの抽出と今後の展望

両取り組みでは，それぞれ特定のプロセスの履歴を改ざん困難な形式で記録し，当該プロセスの結果の検証可能性を確保するものであると整理できる．この時，特定のプロセスの定義とそれに沿った履歴フォーマットを形式化が必要である．また，結果を検証する検証者が，当該履歴を以てプロセスの結果を確認するというエコシステムをデザインすることが重要である．例えば，本稿で紹介した両取り組みでは，履歴を改ざん困難な形式で記録するためにブロックチェーンを活用した．この時，検証者視点ではブロックチェーン自体に対する攻撃等は取り組みの検討範囲外としている．すなわち，検証者はブロックチェーンの正常動作および記録される履歴が改ざん困難であることは仮定していると整理できる．

今後の検討として，ブロックチェーンに依存しない形で議論を汎化させることが考えられる．例えば，履歴の改ざん困難性を担保することが要件であれば，記録者のデジタルアイデンティティが明らかな状態でデジタル署名を活用すれば、ブロックチェーンに依存せずとも実現できるのではないかと考えられる．本稿で議論した3Dプリントおよび商取引以外のユースケースも検討しながら，より議論を汎化することで様々なプロセスの結果を検証可能にすることが期待される．

第３章　ウォレットアプリの開発

Delight WGでは，検証可能なデジタル証明書のデータモデル標準であるVerifiable Credentials（以下，VC）の活用に関して活発に議論している．特に，ユーザーが受け取ったVCを保存・管理・提示するアプリケーションであるウォレットのあり方について議論が進められている．また，2024年度に開始された伊藤忠テクノソリューションズ株式会社と慶應義塾大学SFC研究所データアーキテクチャラボによる共同研究プロジェクト「Trust Knots」において，ウォレットアプリの開発が進められており，ここにDelightWGメンバーが複数人参加している．

9月合宿では，まずVerifiable Credentials技術について紹介した上で，開発中のウォレットの概要を共有し，議論した．

3.1　Verifiable Credentialsの概要

従来のデジタルアイデンティティのモデルは，アイデンティティマネジメントサービスが，同意の下でユーザーのデジタルアイデンティティを管理していた．当該サービス以外にアイデンティティを提示する際には，当該サービス上で認証の上，ユーザの許諾のもとでサードパーティに提供する．一方，ユーザがアイデンティティを提示した先を当該サービスに知られてしまうなどのプライバシーや，当該サービスに依存することによる可用性の課題が指摘されている．

こうした課題に対処するため，自己主権型アイデンティティと呼ばれる，新たなデジタルアイデンティティモデルおよび関連する技術の議論が始まっている．自己主権型のデジタルアイデンティティとは，特定の第三者に管理されることなく，ユーザー自らの手でデジタルアイデンティティをコントロールできるようにしようとするコンセプトである．

自己主権型デジタルアイデンティティの特徴は，Issuer-Holder-Verifierという3つの主体から構成されるモデル（以下，IHVモデル）である．主な役割分担をFig.3に示す．デジタルアイデンティティ技術は，対象となる主体に紐づけられた属性情報の正当性を検証する認証，および認証された主体に対して様々な資源へのアクセス権限を付与する認可に用いられる．ここで，属性情報と主体の紐づけは，何らかの事実を確認した主体によって発行された，属性証明書として表現できる．この発行者をIHVモデルでは，Issuerと呼ぶ．そして，この属性証明書を管理する主体をHolderと呼ぶ．Holderは属性証明書の指す主体（Subject）と同一の場合が多いが，異なるケースもありうる．提示された属性証明書を検証し，認証および認可する主体をVerifierと呼ぶ．

従来のデジタルアイデンティティのモデルとの違いとして，IHVモデルでは，Holderによるアイデンティティを含む属性証明書の提示時に，Issuerへの問い合わせが発生しない．したがって，IssuerはHolderがどのVerifierに対してアイデンティティを提示したかを知ることはなく，プライバシ側面での有用性があるとされている．

3.1.1 Verifiable Credentialsデータモデル

Verifiable Credentialsは，IHVモデルにおいて用いられる属性証明書のデータモデルの標準仕様であり，W3Cによって標準化されている[46]．また，同じくW3Cによるグローバルに一意な識別子の標準仕様であるDecentralized Identifiers（以下，DID）と併せ，自己主権型アイデンティティを実現する中核技術の1つとして期待されている[47]．

VCのデータモデルをFig.4に示す．Credential Metadataには，VCの識別子・種別・Issuerの情報・発行日等の情報が格納される．Claim（s）には，Issuerの主張するSubjectの属性情報が1つ以上格納される．Proofは，Issuerによる証明書に対するデジタル署名が格納される．これにより，VerifierはVCを検証できる．

HolderはVCをVerifierに提示する際は，VCを内包するVerifiable Presentation（以下VP）の形式で提示する．VPのデータモデルをFig.5に示す．Presentation Metadataには，VPの識別子・種別・Holderの情報等の情報が格納される．Verifiable Credential（s）には，提示するVCが1つ以

Figure 3：Issuer-Holder-Verifierモデル

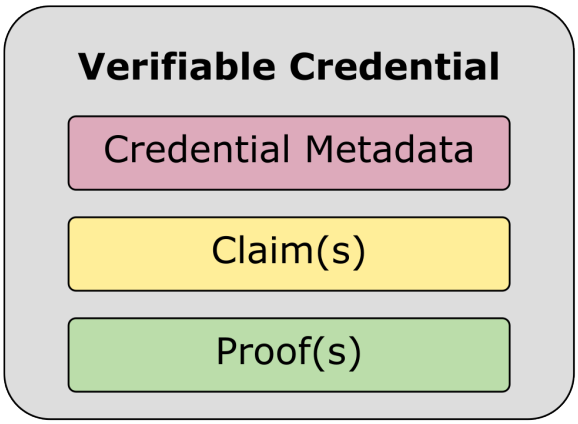

Figure 4：Verifiable Credentialのデータモデル[46]より引用

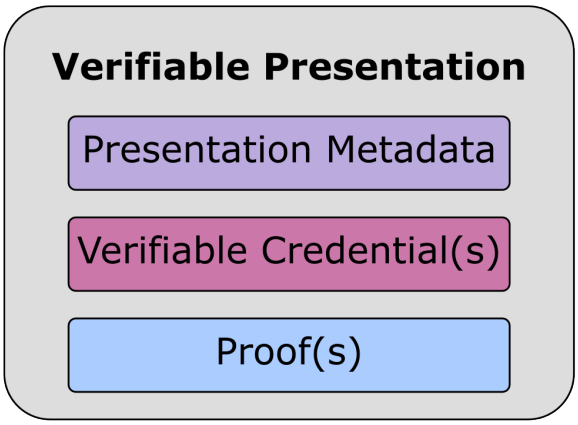

Figure 5：Verifiable Presentationのデータモデル[46]より引用

上格納される．Proofsには，HolderによるVPに対するデジタル署名が格納される．これにより，Verifierは確かにHolderから提示されたVPであると検証できる．

ここまでVCについて概要を説明してきたが，より詳細な解説については仕様およびDelightメンバーが執筆に携わった解説論文を参照されたい[48]．

3.2　ウォレットアプリ開発の取り組み

Verifiable Credentialsの応用を検討する上で，Issuer・Holder・Verifier用にそれぞれVCの発行ツール・保管ツール・検証ツールが必要となる．発行ツールや検証ツールは，MicrosoftのEntra IDなどSoftware as a Serviceの形で提供されているものが存在する．IssuerやVerifierは多くのケースでは企業・大学・小売店などの団体が担うと想定され，マネタイズが可能であることから，開発および導入のモチベーションがある．

一方，Holder用のVC保管ツールであるウォレットには，現状洗練された製品が存在しない．開発が進まない理由の1つとして，ウォレットには多様なIssuerによって発行されたVCが複数格納されることから，一企業にとってはマネタイズが難しく，積極的に開発する動機に欠けることが挙げられる．また，VCの応用研究などの検討に際し，特定の製品に依存した形で検討するのは好ましくない．したがって，業界全体での応用検討を進めるためには，汎用的に活用できるオープンなウォレットが好ましい．

2024年度から，伊藤忠テクノソリューションズ株式会社と慶應義塾大学SFC研究所データアーキテクチャラボによる共同研究プロジェクト「Trust Knots」が開始された[49]．同プロジェクトの枠組みの中で，Verifiable Credentials技術を活用したメダルアプリである「MedalBook」および，汎用ウォレットライブラリである「DelightWallet Core（以下:DeliWaC）」の開発が進んでいる．この開発に，Delight WGのメンバーが複数人携わっている．

単にウォレットを開発するだけでなく，実装を進める中で相互運用性などにまつわる課題を洗い出し，解決手法の研究および標準化へのフィードバックを進めていくことを目指している．以降の記載は，2024年12月現在の設計であり，今後公開予定のソフトウェアとは異なる可能性がある．

3.2.1　MedalBook

MedalBookは，様々な実績だけでなく，所謂“推し活”の表明などのカジュアルなユースケースも想定した，VCに準拠する“メダル”を発行・保管・提示・検証するアプリケーションである．誰かからもらったメダルを保管し提示できるだけでなく，自らメダルを発行・検証できる．モバイル端末での利用を想定しており，iOSおよびAndroid向けに実装を進めている．

MedalBook内のメダルのデータモデルはVCの標準に沿っているため，メダルの発行者および提示者が検証可能である．また，メダルを発行・検証するAPIはOpenIDをベースにしたVCのトランスポートプロトコルであるOpenID for Verifiable Credentials Issuance（以下，OID4VCI）・OpenID for Verifiable Presentation（以下，OID4VP）に準拠している[50, 51]．

3.2.2　Delight Wallet Core

MedalBookの中でもVCの受け取りおよび提示するためのウォレット機能の部分は，汎用ウォレットライブラリ「Delight Wallet Core（略称:DeliWaC）」として切り出して開発を進めている．

DeliWaCのアーキテクチャをFig.6に示す．Deli-WaCは，ウォレットに必要な各機能をコンポーネントとして分割し，実装している．多様な拡張を可能とするため，各コンポーネントのインターフェースをそれぞれ定義している．したがって，当該インターフェースに対応したプラグインを開発することで，現状実装を進めているプロトコル以外へ対応，あるいは拡張が可能である．

以下に，各コンポーネントの概要を説明する．

- DID Component:Holderの識別子を管理するコンポーネント．現在did:key，did:pkhなどのプラグインを実装している[52, 53]．
- Receiving Component:Issuerと通信し，VCの受け取る

コンポーネント．現在OID4VCIプラグインを実装している．

- Presentation Component:Verifierと通信し，VPを提示するコンポーネント．現在OID4VPプラグインを実装している．
- Credential Storage Component:VCを保管するコンポーネント．現在，モバイル端末のローカルストレージに保管するプラグインを実装している．
- Verification Component:署名検証およびVPへ署名するコンポーネント．現在，ES256プラグインを実装している[54]．
- Serialization Component:VCのデシリアライズおよびVPのシリアライズを行うコンポーネント．現在，VC-JWTプラグインを実装している．

また，ウォレット側で以下のコンポーネントを実装し，Controllerに注入する必要がある．

- KeyStorage:Holderの鍵を管理する．現在，秘密鍵を端末のSecure Elementで管理するプラグインと，OSのキーチェーンで管理するプラグインを実装している．

DeliWaCは現状MedalBookのサブセットとして開発が進んでいるが，MedalBook固有の機能とは明確に分離されている．したがって，設計上は，汎用的にウォレットの開発で利用可能なライブラリとなる．

今後はDeliWaCをオープンソースとして公開するだけでなく，他の様々な実証実験プロジェクト等で活用することを予定している．実証実験でのフィードバックを受けながら機能を拡充し，多様なニーズに答えられるライブラリとして洗練させ，最終的な目標である汎用ウォレットの実装・提供へと進めていく予定である．

3.3 議論

9月研究会では，参加者からVCおよびMedalBook・DeliWaCについていくつかの質問が投げかけられ，活発な議論が行われた．

特に，VCおよびDIDの相互運用性の課題が注目された．VCはあくまでデータモデルを規定するのみであり，現状多様なシリアライゼーションや署名フォーマットが乱立している状況にある．DeliWaCはプラグインで多様な形式に対応できる形でデザインしているが，Verifierも同様に多様な形式に準拠していく必要がある．これは開発者にとって負担であり，今後の標準化の動向を見守る必要があるだろう．

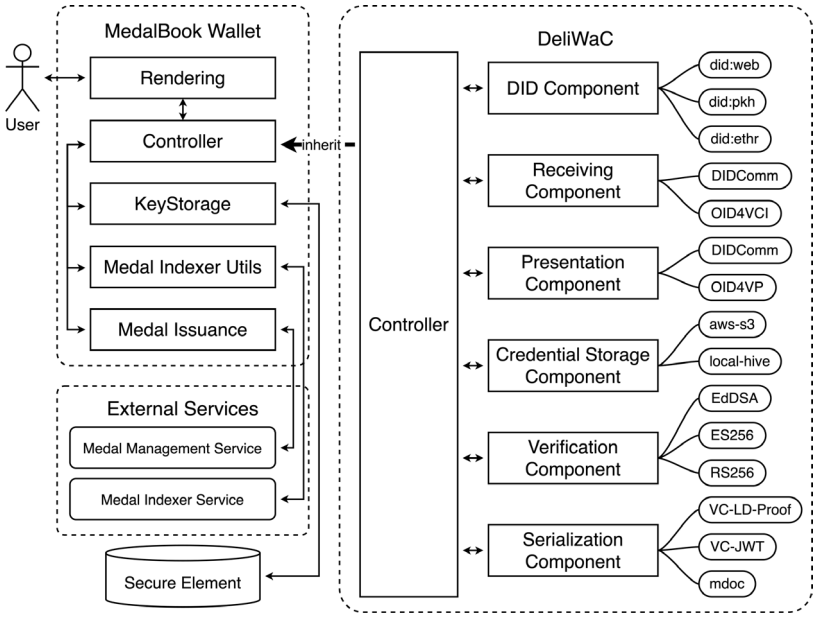

Figure 6：DeliWaCのアーキテクチャ図

また，Issuerがサービスを終了した際の持続可能性についても疑問が投げかけられた．VCは署名付きのポータブルなデータであり，なんらかの方法でVerifierはIssuerの検証鍵さえ入手できればよく，必ずしも検証時にIssuerへ問い合わせる必要はない．したがって，HolderはIssuerの可用性に左右されない形で自らの属性情報を提示できると期待されている．しかしながら，特定のユースケースではIssuerの検証鍵が保管されているレジストリの可用性に依存してしまうことや，VCの失効管理を行う場合には失効情報が格納されるレジストリの可用性に依存することとなり，自己主権性が十分保証されないケースへの対応は今後の議論が必要である．

今後はMedalBookおよびDeliWaCの開発を進めながら，今回の議論の中で見えてきた研究課題に取り組んでいく予定である．

第４章　終わりに

本稿では，Delight WGの今年度の活動報告として9月合宿で議論した取り組みについて概説した．インターネット上でさまざまな活動が行われる現代において，それぞれの取り組みで検討したような情報の検証可能性は大きな課題である．来年度以降も，Walletアプリの開発とともに，そのユースケースを開拓しながら，インターネット上で安心･安全なやり取りを実現するための研究開発を行なっていく予定である．