ブロックチェーン技術をベースとした アイデンティティ管理・流通の動向

2.1 はじめに

ブロックチェーン技術をベースにした様々なサービスが毎日のように報道されています。その中には単なる分散データベースとしてブロックチェーンを用いる残念な提案も多く、本当にそこにブロックチェーンは必要なのかを自己確認できるフローチャートが複数発表されるほどです[*1]。ブロックチェーンにはいくつかの分類方法があり、大きく分けてプライベートで用いられるものと、いわゆる暗号資産の安全性の裏付けとなるパブリックなものがあります。後者のパブリックブロックチェーンではマイニングしてチェーンを繋げ続けることにインセンティブを持たせる必要があり、Bitcoinなどの暗号資産では、定められたルールに基づきチェーンを伸ばしていく必要があります。暗号資産で用いられるブロックチェーンはあるアドレスからあるアドレスへの資産の移動に用いられることが大きな目的ですが、このブロックチェーンにおける価値移動の基盤を用いてその用途以外に使おうとする動きが見られ、セカンドレイヤーまたはレイヤー２といった用語で呼ばれています。

本稿は、Ethereumブロックチェーン[*2]におけるセカンドレイヤーにあたるサービスのうちクレデンシャル(アイデンティティ情報)に用いられるERC(Ethereum Improvement Proposals)[*3]提案の動きを取り上げます。更にこうしたクレデンシャルがブロックチェーンに格納され、在籍証明などの公的な証明書をデジタル空間で確認できるユースケースについて触れます。最後に、ここ数ヵ月で複数のベンダーやコンソーシアムが非中央集権型の識別子であるDIDs(Decentralized Identifiers)やアイデンティティ管理をユーザ自らがコントロールするSSI(Self Sovereign Identity)などの概念を提示している背景とブロックチェーンをベースとしたクレデンシャル管理技術が注目されていることを示します。

2.2 識別子としてのIDとクレデンシャルの整理

2015年発行のフォーカスリサーチにおいて、当時のID管理技術の動向について報告しています[*4][*5][*6]。本稿ではIDを識別子(Identifier)という狭義の意味と捉えて説明を行います。

現実世界の実体はデジタル世界のエンティティと結び付けられ、デジタル世界のエンティティを識別(identify)するために、ユニークな識別子(Identifier＝ID)が割り当てられます。識別子としてのIDと、そのIDに紐付けられるあらゆるアイデンティティ情報は別に考える必要があります。更にID空間はそれぞれのレルム(IDが有効で識別可能な範囲)が別途定められていることから、リアルワールドに唯一存在するエンティティに対して同じレルムでも複数のIDを持つこともあります。

次にデジタル空間においてなぜIDが付与されるのかを考えると、そのエンティティであることをネットワーク上の第三者に認識してもらう必要があるためです。デジタル世界におけるあらゆるアクティビティには認証という行為が伴います。認証行為によりリソースにアクセスできるようになったり、各種サービスを受けられたりするようになります。

この認証行為では、秘密情報であるトークンと公開情報であるクレデンシャルの組を用いる、という整理を行うことができます。NIST SP800-63の定義に従うと、トークンは当該IDが割り当てられたユーザが持つ秘密にすべき情報を指し、クレデンシャルはIDと紐付けられるあらゆる種類の属性情報を意味します。クレデンシャルは暗号技術を用いて内容の完全性が保証されます。当該IDを持つエンティティがデジタル世界で自分の属性情報を第三者に確認してもらう際に、秘密情報であるトークンで当該IDを持つエンティティが割り当てられたエンティティであることを確認してもらうことができます。

＊1　NISTIR 8202、"Blockchain Technology Overview"(https://doi.org/10.6028/NIST.IR.8202) Figure 6 - DHS Science & Technology Directorate Flowchartにフローチャートが記載されている。
＊2　Ethereum Project、Developer Resources(https://www.ethereum.org/developers/)。Ethereumの大きな特徴であるスマートコントラクトに関連する関連技術については本稿では取り上げません。
＊3　Ethereum Improvement Proposals(http://eips.ethereum.org/)。
＊4　Internet Infrastructure Review Vol.26「1.4.3 ID管理技術」(https://www.iij.ad.jp/dev/report/iir/026/01_04.html)。
＊5　Internet Infrastructure Review Vol.27「1.4.2 ID管理技術～利便性と安全性の観点から～」(https://www.iij.ad.jp/dev/report/iir/027/01_04.html)。
＊6　Internet Infrastructure Review Vol.28「1.4.3 ID管理技術～オンライン認証にパスワードを使わない方法へ～」(https://www.iij.ad.jp/dev/report/iir/028/01_04.html)。

認証行為と共にクレデンシャルが提示されたときに、それを受け取った第三者は、当該IDがどのようなエンティティであるのかをクレデンシャルに書かれている属性情報で確認することができます。このようにして認証に加えて認可(Authorization)のためにクレデンシャルが利用されるケースもあります。X.509証明書は単一もしくは複数のIDに公開鍵を紐付けることからクレデンシャルの1例です。実際にSSL/TLSクライアント認証がそれにあたります。ブラウザ側に個人のX.509証明書を配備した上でサーバにログインすることができ、法人向けのオンラインバンキングなどで利用されています。よりクレデンシャルとしての利用形態に近い方法として、X.509属性証明書(Attribute certificate)[*7]と呼ばれる仕様が存在しています。属性証明書は通常のX.509証明書と異なり公開鍵を内包していません。*holder*と呼ばれる識別子を格納するエリアに証明書を同定するためのシリアル番号を入れ、当該X.509証明書を指定した上で証明書のホルダー(subject)と紐付ける属性情報を格納するという形式を持っています。これは、レルムがCAの発行する証明書群、IDはシリアル番号、クレデンシャルが属性証明書、という関係を持っていると理解できます。X.509属性証明書はクレデンシャルを書くことができる一方で、実際にブラウザなどの一般ユーザが触れるアプリケーションにおいて実装されることはなく、現在利用されている事例はほとんど見られません。

2.3 ERC-725の概要

ERC-725[*8]はERC-20トークン標準の策定やweb3.jsの開発者として知られるエンジニアであるFabian Vogelsteller氏[*9]が2017年10月に提案しました。ERC(Ethereum Improvement Proposals)はIETFのRFCのように、誰でも提案できる改善型のドキュメントでERC-1に書式や書くにあたっての指針などが掲載されています。大きな特徴としては、とにかくコンパクトに書くことが求められていることが挙げられます。同様の文書群としてはBitcoinのコミュニティにおいてもBIP(Bitcoin Improvement Proposals)[*10]として知られているドキュメント群があり、例えばSegWitとして知られるトランザクションデータの削減方式はBIP-141で規定されています。

電子契約の締結とサービスの実行を自動的に行う方式として知られるスマートコントラクトは、1997年にNick Szaboによって提案された新しい概念であり、Bitcoinが登場する前から存在していました。スマートコントラクトの例として、自動販売機の例がよく取り上げられています。「ユーザが購入したいジュースの代金を自販機に投入する」と「その後購入したいジュースのボタンを押す」という2つのプロセスが、両者ともある一定の条件を満たすと自動的に販売が開始されるという例です。Ethereumは暗号資産としての側面だけでなく、スマートコントラクトを作成し実行することができるため分散アプリケーションのプラットフォームであるとされています[*11]。ERC-725はプロキシアカウントのふるまいに関して分散アプリケーションを記述する言語の1つであるSolidityのインターフェースを定義しています。ERC-725からはERC-735[*12]とERC-780[*13]が参照されており、これらの仕様に基づきEthereumブロックチェーン上でクレデンシャルを流通させる仕組みを提供します。ERC-725の文脈においては、クレデンシャルはClaimと呼ばれます。ERC-735はClaimのフォーマットが、ERC-780はCliamのレジストリであるEthereum Claims Registry(ECR)に関する仕様が記載されています。Ethereumブロックチェーンというレルムにおいて ID(識別子)はEthereumアドレス(コントラクトアドレスではない点に注意)でありClaimと呼ば

*7 RFC 5755、"An Internet Attribute Certificate Profile for Authorization"(https://datatracker.ietf.org/doc/rfc5755/)。
*8 ERC-725 version2:Proxy Account(https://github.com/ethereum/EIPs/issues/725)(http://eips.ethereum.org/EIPS/eip-725)。
*9 Fabian Vogelsteller(http://frozeman.de/blog/)。
*10 BIP(Bitcoin Improvement Proposals)(https://github.com/bitcoin/bips)。
*11 Ethereum Project、White paper(https://github.com/ethereum/wiki/wiki/White-Paper)。
*12 ERC-735、Claim Holder(https://github.com/ethereum/EIPs/issues/735)。
*13 ERC-780、Ethereum Claims Registry(https://github.com/ethereum/EIPs/issues/780)。

れるクレデンシャルによって、あるアドレスに紐付けられるIdentity Holder（ホルダー）のアイデンティティ情報が保証されるという仕組みが規定されています。Claimを発行するClaim Issuer（認定者）は自身の持つ秘密鍵を用いて任意のEthereumブロックチェーン上のエンティティに対してClaimを発行することができます。Identity Holderは検証対象となるClaimを何らかの方法でClaim Checker（価値判断者）に受け渡し、価値判断者はデジタル署名を確認することでClaimの確からしさを確認することができます。これらの一連の検証作業はオンライン・オフラインの両方で実行できることが想定されています[*14]。

ERC-735で規定されるClaimの形式は以下のようにシンプルなデータ構造をしています。

```
struct Claim {
    uint256 topic;
    uint256 scheme;
    address issuer;
    bytes signature;
    bytes data;
    string uri;
}
```

表-1 ERC-735 Claimの各構成要素

topic	現在未定義。形式は256ビット空間でClaimの種別に関する情報が入る見込み。例としてバイオメトリクス情報や住居情報が記載されています。
scheme	現在未定義。形式は256ビット空間で、別途定義されるであろうスキーマに基づいた処理方法や署名アルゴリズムを格納します。
issuer	コントラクトアドレスもしくは署名に用いられた鍵に呼応したEthereumアドレス。
signature	署名データ。被署名対象エリアは{アイデンティティ情報の保持者であるIdentity HolderのEthereumアドレス、topic、data}のみという点に注意です。
data	アイデンティティ情報のハッシュ値。アイデンティティ情報そのものを記載しないため機微情報をそのままブロックチェーンに載せるわけではありません。
uri	アイデンティティ情報を指し示すURI。HTTPリンクやIPFSのURIが想定されています。

ERC-735 ClaimはIdentity Holder自身で価値判断者に提示することができるように実装されるべきであり、データとして可搬性を持つ点が大きな特徴となります。ERC-735ではToBeSigned（改ざん防止対象）ではないエリアにURIを記載するゾーンが設けられており、ここにアイデンティティ情報を指し示すデータを分散ファイルシステムであるIPFS[*15]などで共有します。ERC725 Alliance[*16]ではERC-725に関連するオープンソースプロジェクトが存在しています[*17]。また、この参照実装を使って構築されたサイト[*18]ではいくつかのサンプルが参照でき、ブラウザ上でClaimの確からしさを検証できるようになっています。また、自分で自分のアイデンティティ情報に署名してオレオレClaimを発行可能な仕様は特筆すべき点です。

このようにERC-725フレームワークではClaimを誰でも発行できる、つまりClaim Issuerは誰でもなれるためEthereumアドレスさえ分かれば誰にでもClaimを発行することができます。そのためClaim Issuerをどのように信頼して、そのIssuerから発行されたClaimを価値判断するかについては大きな課題

＊14 Fabian Vogelsteller、ERC Identity（https://www.slideshare.net/FabianVogelsteller/erc-725-identity）。
＊15 IPFS（InterPlanetary File System）（https://ipfs-book.decentralized-web.jp/what_is_ipfs/）。
＊16 ERC725 Alliance（https://erc725alliance.org/）。
＊17 ERC725 Alliance、"Repository for code and discussion around ERC725 and related standards"（https://github.com/ERC725Alliance/erc725/tree/master/contracts/contracts）。
＊18 ERC 725 Demo implementation by Origin Protocol, Inc.（https://erc725.originprotocol.com/）。Origin Protocol, Inc.,（https://www.originprotocol.com/）。

です。またCliamの失効やEthereumアドレスの付け替えなどの機能もあるとされていますが、まだ仕様としては不完全な状況です。Issuerの評価(レピュテーション)の仕組みについても議論が始まったばかりという状況のように見受けられます。

このように現在はレピュテーションの問題をはらんでおり、最終的にうまくClaimを流通させていくためにはいくつかの段階を踏むことになるでしょう。筆者は以下の3ステップで徐々に「Claimの考え方」が浸透していくと予想しています。第1段階はSNSなどの閉じたネットワークで知り合い同士で投げ銭として気軽にClaimを発行し、スケーラビリティを確認するフェーズです。次の段階では既存のユーザ評価・通報システムを活用して誤ったClaimを発行したIssuerかどうかをランク付けする仕組みが整い、最終的には完全に分散・自動化されたレピュテーションシステムへと昇華していくと考えられます(図-1)。

ERC-725と同様に可搬性を持つClaimの例としてはBlockcerts[*19]によるプロジェクトがあり、オープンソース[*20]や検証デモ[*21]を参照することができます。BlockcertsはMIT Media LabとLearning Machine社で作製されたプロトタイプがベースとなっています。BlockcertsではBitcoinやEthereumを含む複数の種類のブロックチェーンでも実装可能なように拡張が続けられています。スマートフォンアプリであるBlockcerts Walletも実装・公開されており、MITでは学位証明書がBlockcertsの仕組みを利用してブロックチェーンに書き込まれています[*22]。この他にもスペインの大学においては学位証明書を発行する際にSmartDegreesプラットフォームを利用してEthereumブロックチェーン上で管理することが発表されています[*23]。このようにセカンドレイヤーのプラットフォームは複数存在するなど現在はまだ混沌とした状況のため、プラットフォームの選択においては事業継続性を鑑みて選択する必要があるでしょう。

ここまで説明したように、Claimは単純な仕組みながら、Issuerが信頼でき、かつセカンドレイヤーの仕様が正しく運営されていれば、Ethereumブロックチェーンの信頼性が崩れない限りは半永久的に利用することができると認識されてい

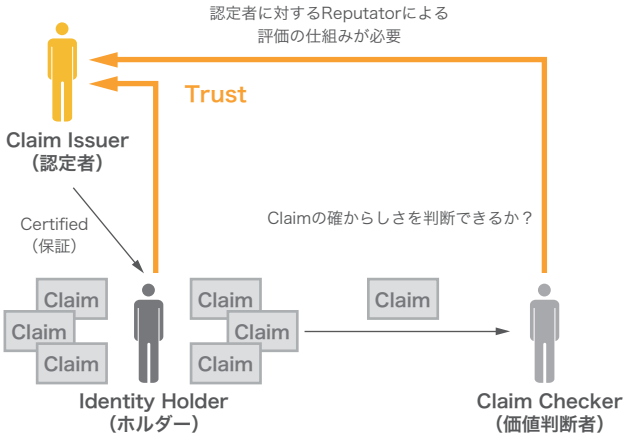

図-1 Claim発行とClaim価値判断の仕組み

＊19 Blockcerts(https://www.blockcerts.org/)。
＊20 Repositories of Blockcerts project(https://github.com/blockchain-certificates)。
＊21 Example Blockcerts(https://www.learningmachine.com/new-product/examples/)。
＊22 MIT News、Digital Diploma debuts at MIT(http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017)。
＊23 Universidad Carlos III de Madrid is issuing degree certificates with blockchain(https://www.uc3m.es/ss/Satellite/UC3MInstitucional/en/Detalle/Comunicacion_C/1371252827656/1371215537949/Universidad_Carlos_III_de_Madrid_is_issuing_degree_certificates_with_blockchain)。

ます。そのためブロックチェーン技術をうまく活用する事例として学位証明書のデジタル発行は適しているアプリケーションの1つであると考えられ、実際に国内でサービスインした事例もあります。昨今の地方私大の閉校や地方自治体による検定試験の終了など、かつて信頼できた組織であっても未来永劫運営されているとは限りません。そしてそこから発行された物理的な証書が保証できなくなってしまった事例もあります。現物の証書を代替する手段として今回紹介したオープンな仕組みでClaimが流通する時代が来ることが望まれます。

2.4 非中央集権型識別子DIDs

識別子としてのIDはある特定のレルムの中でアサインされます。レルムを超えて認証する際にはID Federation（ID連携）という概念があり、シングルサインオンの文脈でしばしば登場します。先に挙げたX.509属性証明書やERC-735 Claimのようなクレデンシャルは、発行された特定のレルムでしか流通されません。IDを振り出す役目でもあるアイデンティティプロバイダは現実的には単独で存在せず、SNSなどのサービスプロバイダのログイン機能が外部サービスと連携できるようにするために機能分離してアイデンティティプロバイダとしての役割を担っているのが現状です。このとき、ID連携機能を用いて別のサービスにログインするようなケースにおいて、特定の企業や組織により運営されているがために当該IDが急遽使えなくなるリスクが存在します。これは1つのIDが利用停止されることにより、他の複数のサービスが利用できないことになりかねません。実際、あるSNSにおいて運営側が不適当な書き込みと判断されたケースで当該IDが利用停止、最悪のケースでは削除されることにより起きる弊害が散見されます。

このような背景から、非中央集権型識別子Decentralized Identifiers（DIDs）という概念が登場しています。ある特定のレルムだけで有効なIDではない点、そしてIDを一括管理する中央集権的な存在を持たないという特徴を持ちます。これは非営利団体であるSovrin Foundation[*24]で提唱された自己主権型アイデンティティSSI（Self Sovereign Identity）[*25]との親和性が高いと認識されています。SSIは自己情報コントロール権の考えとよく似ていて、管理当局を介さずに自分自身でアイデンティティ情報の所有と管理を行う必要があることを認識するために使用される用語です。先に挙げたERC-735 Claimなどのクレデンシャルは意図せずひとりでに流通してしまう可能性があります。そうではなく

＊24 The Sovrin Alliance（https://sovrin.org/library/rise-of-self-sovereign-identity/）。
＊25 The Sovrin Alliance、"A White Paper from the Sovrin Foundation: A Protocol and Token for SelfSovereign Identity and Decentralized Trust(Version 1.0 January 2018)"（https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf）。

自身のクレデンシャルの流通の主権をIdentity Holderが持とうという考え方です。

プライバシーを保護しポータブルでユーザ中心のアイデンティティ管理を実現しようとしている組織に非営利団体であるID2020 Alliance[*26]があります。また、国の発行する通貨の信頼が落ちているようなケースにおいて法定通貨ではなく暗号資産が利用されようとするのと同じく、パスポートの代替技術としてブロックチェーン上のClaimが活用できないかというプロジェクトが存在します[*27]。この考え方は皆が認め、そして信頼できる機関によって発行されたClaimに相当するデータがパスポートライクな本人確認手段を提供することと解釈できます。2015年に国連でまとめられた持続可能な開発目標(SDGs)[*28]の16.9節に記載のゴール目標には「2030年までに出生登録情報を含めすべての人に合法的なアイデンティティを提供する」と記載されています。10億を超えるとも言われるID難民を救うべくID2020技術的な機能要件[*29]がまとめられています。この要件書では、社会適用性、個人識別、認証、プライバシ管理、信頼性、相互運用性、リカバリの7カテゴリでまとめられており、この類いの設計指針としては非常に有用なドキュメントとなっています。

一方DIDはW3C[*30][*31]で策定された文書群からその意図を読み取ることができます。W3CではDIDを分散元帳技術(DLT;Distributed Ledger Technology)やその他の分散ネットワークに登録されており、中央集権的なオーソリティを必要としないグローバルに一意な識別子[*32]と定義しています。ERC-735 ClaimはEthereumアドレスをID空間として利用していましたが、そのままDIDとして利用せずにW3C DID形式でEthereumアドレスをWrapして記載する方法も提案されています[*33]。このようにW3C DIDは様々なIDを表記可能なグローバルIDとしての利用を推進していることが分かります。DIDの存在だけでは重複しないナンバリングしか解決しませんが、Claimのユースケース[*34]やVerifiable Credentials(当初Claimと表現されていましたがクレデンシャルという用語に変更されました)のデータフォーマット[*35]と連動して世の中を解決していくことになるでしょう。

2019年3月に開催されたWeb of Trust VIII(RWOT8)[*36]でのグループワーク、そして同年4月に開催されたthe 28th Internet Identity Workshop[*37]ではDIDやSSIを軸にしたトピックが多く取り上げられています。またIGF(Internet Governance Forum)でも今年のAnnual Meeting[*38]でDID

＊26 ID2020 Alliance、The Alliance Manifesto(https://id2020.org/manifesto)。
＊27 Taqanu(https://www.taqanu.com/impact)。
＊28 Transforming our world: the 2030 Agenda for Sustainable Development(https://sustainabledevelopment.un.org/post2015/transformingourworld)(https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E)。
＊29 ID2020 Technical Requirements: V1.0 (https://docs.google.com/document/d/1L0RhDq98xj4ieh5CuN-P3XerK6umKRTPWMS8Ckz6_J8/edit)。
＊30 W3C Credentials Community Group(https://www.w3.org/community/credentials/)。
＊31 W3C Verifiable Claims Working Group(https://www.w3.org/2017/vc/WG/)(https://github.com/w3c/verifiable-claims)。
＊32 Decentralized Identifiers (DIDs) (https://w3c-ccg.github.io/did-spec/#decentralized-identifiers-dids)。執筆時の最新版は2019年6月3日発行のv0.13。
＊33 eth DID Resolver(https://github.com/uport-project/eth-did-resolver)。
＊34 Verifiable Claims Use Cases(https://www.w3.org/TR/verifiable-claims-use-cases/)。
＊35 Verifiable Credentials Data Model 1.0(https://www.w3.org/TR/verifiable-claims-data-model/)。2019年3月が最終版。執筆時はW3C勧告候補。
＊36 Rebooting the Web of Trust VIII: Barcelona(March 2019)(https://github.com/WebOfTrustInfo/rwot8-barcelona)(https://www.weboftrust.info/pastevents.html)。
＊37 IIW(The Internet Identity Workshop)Workshop Proceedings(https://internetidentityworkshop.com/past-workshops/)。
＊38 IGF 2019 Workshop Selection Results(https://www.intgovforum.org/multilingual/content/igf-2019-workshop-selection-results)。

関連技術が取り上げられており、ガバナンスに関しても議論されていくことになります。今後も多くの人を巻き込んで議論が進んでいくものと考えられます。

2.5 関連したその他の動向

2019年5月にマイクロソフトはBitcoinブロックチェーンを基盤としたDIDを扱うプラットフォームを発表しました。5月15日、2つのブログ記事で今後の取り組みなどが示されています[*39][*40]。またDIDに関するホワイトペーパーも公開されました[*41]。これらの情報によると、ID空間としてはW3C DIDを利用しDecentralized Identity Foundation（DIF）[*42]で策定されているSidetree protocolが採用されていることが窺えます。このDIDシステムはBitcoinブロックチェーンのセカンドレイヤーでの実装であり、ION（Identity Overlay Network）[*43]と名付けられて既にソースコードも公開されています。

最後に信用スコアや情報銀行についても触れておきます。インターネット上でのアクティビティから信用スコアとして算出するサービスが国内でもサービスインされるとの報道もありました。GAFAやFAANGなどのビッグブラザーによる中央集権的な管理下での評価のみが正しいと判断され、自らのスコアが意図せず世の中に流通してしまうことが懸念されます。ここには昨今頻繁に議論されているAI技術などと同様に、評価制度だけでなく評価アルゴリズムの透明性を確保する必要があります。よく分からないロジックで、ある特定の地域に在住する方々や人種、宗教などに拠って不当な評価がなされることも理論的には起こり得ます。そのため倫理的な側面での配慮が必要となります。それは、ERC-735 Claimでの懸念点として述べたように現実世界のエンティティが行うレピュテーションの仕組みにも同じことが言えます。

このように現実世界のエンティティが、様々な手段で評価される時代になってしまいました。管理する側からすると安全保障のためにこれらの措置は必要であるかもしれませんが、やはりSSIの考え方に基づき自分で自分の機微情報を管理できることが求められています。特に、初めてDIDやClaimが発行されたIdentity Holderに様々な自衛を求めることは容易ではないかもしれませんが、デジタル時代に生きる我々には当然のリテラシーとして持っておくべき素養ではないかと考えます。

＊39 Microsoft Security Blog、"Decentralized identity and the path to digital privacy"（https://www.microsoft.com/security/blog/2019/05/15/decentralized-identity-digital-privacy/）。
＊40 Azure Active Directory Identity Blog、"Toward scalable decentralized identifier systems"（https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Toward-scalable-decentralized-identifier-systems/ba-p/560168）。
＊41 Microsoft Whitepaper、Decentralized Identity - Own and control your identity（https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY）。
＊42 Decentralized Identity Foundation（DIF）（https://identity.foundation/）（https://github.com/decentralized-identity/）。
＊43 ION（Identity Overlay Network）（https://github.com/decentralized-identity/ion/）。

自分が他界した後は、SNSのアカウントを子供や孫に受け渡そうと考える方もいらっしゃいますが、事業継続性の観点からはあまりお勧めできない状況になりつつあります。やはりここでもAI技術の発展により、書き込み内容の検閲によりアカウント自体を一時的もしくは永久的に無効にする措置が大きく影響します。これらの身近な事例も、DIDとその周辺技術のサービス提供が早急に実現するよう望まれている要因であると筆者は考えます。

大規模な統計情報を扱う際の仮名IDの取り扱いに関してや、クレデンシャルそのものを暗号化してアクセスコントロールするケースなどに関してはまだ議論が十分になされていない段階にあるように思います。バックグラウンドとなる技術が整合性を持っており、うまくディプロイできれば社会的適合性を持つ、という理由だけで、その技術が実際に世の中に浸透できなかった事例はこれまでにも多く目にしてきました。今回紹介した技術群がユーザに身近なアプリケーションにディプロイされ世の中の役に立つのかどうかは、現時点では分かりません。

情報銀行などのリアルなユースケースが出てくることによって、実社会におけるエンティティに結びつく各種情報(機微情報も含む)を、インターネットを介して流通させる仕組みの利便性が認識されるようになりました。しかしここには大きな問題があります。EUが定めるGDPRなどのプライバシー情報管理を定める規制はEU諸国に限ったことではなく、日本を含む世界各国においてもその規制を受けることになりました。そのため今回紹介する技術はブロックチェーンを用いることから、クレデンシャルが流通する範囲は特定のリージョンに留まらず、各国の各種規制によって利用が制限される可能性があります。これはBitcoinやEthereumのような暗号資産の考え方とは大きくかけ離れており、技術の浸透を阻害する大きな要因になる可能性があります。ERC 725 AllianceやID2020は、このような国を越えた流通の仕組みに対する阻害要因を払拭するアクティビティが必要となるでしょう。しかし今のところそれらに関するアクティビティは見受けられません。そもそもこれらのコンソーシアムで扱うべき問題なのかどうかも含め、広い見識と視野を持った有識者がこの問題に取り組む必要があるでしょう。

執筆者:
須賀 祐治(すが ゆうじ)
IIJ セキュリティ本部 セキュリティ情報統括室 シニアエンジニア。2008年7月より現職。暗号と情報セキュリティ全般に関わる調査・研究活動に従事。CRYPTREC TLS暗号設定ガイドラインWG 主査。CRYPTREC暗号技術活用委員会 委員。暗号プロトコル評価技術コンソーシアム 幹事。情報処理学会 CSEC研究会 幹事。電子情報通信学会 ISEC研究会 幹事補佐。CyberSciTech2019 Program co-chair。IWSEC2019 Organizing committee member。Cryptoassets Governance Task Force(CGTF) Security WG member。