Vol.2019-CSEC-86 No.45
Vol.2019-SPT-34 No.45
2019/7/24

Ethereumブロックチェーンで綿菓子を巻く方法 ～ERC725フレームワークを用いてe-KYC-eを実現する～

須賀 祐治[1,a)]

概要：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る．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ある．こうした中でブロックチェーン技術をうまく活用する事例として，学位証明書等の物理的な証書に対応するClaimのデジタル発行は適しているアプリケーションのひと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る．本稿はIDにEthereumブロックチェーンにおけるERC735 Claim形式のクレデンシャルを付与することを想定したモデルを考える．タイトルにある「綿菓子」は，このように複数のClaimがあるIDにまとわりついていく様を表現したメタファーである．さらに，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を紹介しe-KYC-eという新しい概念を提案する．e-KYC-eは，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から見ても社会的に受け入れられやすいと考えられる．

How to make cotton candy under the Ethereum blockchain (To realize the e-KYC-e method by using ERC725 framework)

Yuji Suga[1,a)]

1. 識別子としてのIDとクレデンシャルの整理

本稿ではIDを識別子（Identifier）という狭義の意味と捉えて説明する．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）が割り当てられる．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る．さらに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を持つこともあると想定する．

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ある．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う．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．．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る．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する．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ており，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

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan
[a)] suga@iij.ad.jp

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るようになる．

認証行為ととも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 3 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る．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る．

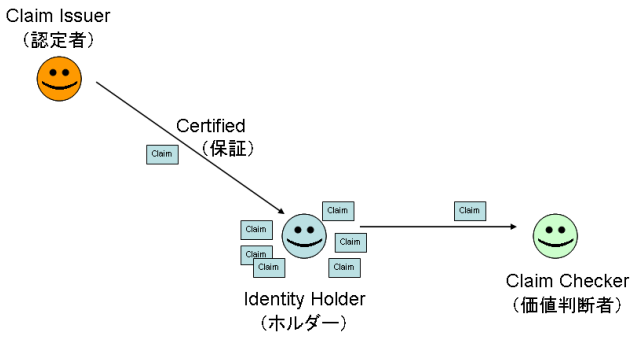

図 1　Claim の流通に関わる IHC3 者モデル

2. 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 FabianVogelsteller[9] により 2017 年 10 月に提案された．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る．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る．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る．「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ある．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る [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る．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ている．ERC-725 の文脈においては，クレデンシャルは Claim と呼ばれる．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る．

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（コンセンサスアドレスではない点に注意）であり Claim と呼ば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る．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る．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る．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る [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る．

ERC-735 Claim のデータ構造

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

2.1 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る．

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．

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．

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ない点に留意．

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 が想定されている．

2.2 可搬性を持つ Claim の重要性

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る．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] などで共有することが想定されている．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 [17] があり，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る．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ある．

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る．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である．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るが，まだ仕様としては不完全な状況である．そして 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である．

2.3 Reputator の必要性

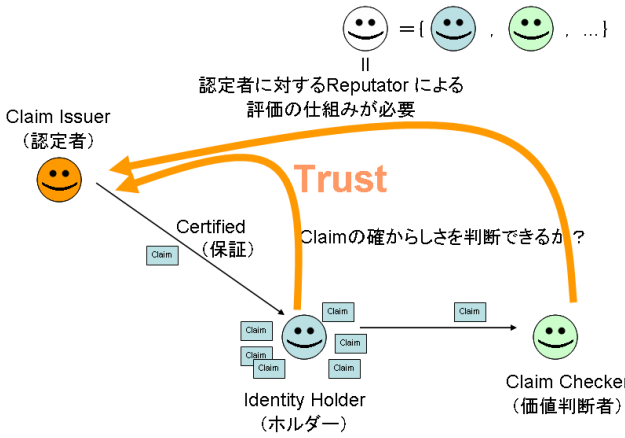

図 2 IHC3 者モデルにおけるレピュテーションの仕組み

3. 犯罪収益移転防止法改正と e-KYC

日本では KYC （Know Your Customer）に関わる各種法律が 改正され 2020 年 4 月から施行されようとしている [39] ．本来ならば対面もしくは郵送などによって免許証などの本人確認書類を送付する必要があったプロセスがスマートフォン等で本人確認書類を撮影をすることで従来の確認方法を代替することを容認するように法律改正が行われた．その結果 e-KYC という新しい概念が登場している．これは，仮想通貨交換業などが自前で KYC のための確認作業をする必要がなく，アウトソースすることにより顧客の実在性確認を行うことができることを意味する．実際いくつかの企業がこの e-KYC サービスを行うことを表明しており，今後利用が拡大されると考えられる．

3.1 提案:e-KYC-e

e-KYC で顧客確認がなされた後，Ethereum アドレスを生成し ERC-735 Claim で e-KYC マークをつけるなどの操作を行うことを想定する．このとき，e-KYC された暗号資産アドレスという概念ができ，匿名性を確保する必要のない用途においては Claim を確認することで安全な資産移動を行うことができるようになる．e-KYC-e は「さらに次の -e」を意味しており，連鎖的にそのアドレスが安全であることを第 3 者が利用できるメリットがある．

しかし，これは元々の暗号資産の原理・原則からは反しているため，特に海外での社会受容性は低いと考えられる．しかし日本での暗号資産運用は，すでに匿名性を排除するような規制がなされており十分に実用的であるとも考えられる．

一方で，汚染されたアドレスから勝手にエアドロップされてあらぬ疑いをかけられてしまうなどの行為により Claim だけを確認しても汚染されたかどうかを確認することができないというジレンマを引き起こすことも想定される．

4. まとめ

本稿は e-KYC-e の概念を提示したが，第 1 段階では 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が進み，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うことになるであろう．さらに，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る．これらをどの暗号資産で行うかはあまり関係なく，今回は Etherem で行ったが DIDs を定義する W3C などの団体により標準的なフォーマットやプロトコルが整えば，十分普及していくものと考えられる．

参考文献

[1] NISTIR 8202, ”Blockchain Technology Overview”, https://doi.org/10.6028/NIST.IR.8202
[2] Ethereum Project, Developer Resources, https://www.ethereum.org/developers/
[3] Ethereum Improvement Proposals, http://eips.ethereum.org/
[4] IIR Vol.26「1.4.3 ID 管理技術」, https://www.iij.ad.

jp/dev/report/iir/026/01_04.html
[5] IIR 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] IIR 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
[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
[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/, https://www.originprotocol.com/
[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
[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
[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
[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/
[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
[39] 警察庁，犯罪収益移転防止法の解説, https://www.npa.go.jp/sosikihanzai/jafic/hourei/law_com.htm
[40] Microsoft Security Blog, ”Decentralized identity and the path to digital privacy”, https://www.microsoft.com/security/blog/2019/05/15/decentralized-identity-digital-privacy/
[41] 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
[42] Microsoft Whitepaper, Decentralized Identity - Own and control your identity, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY
[43] Decentralized Identity Foundation (DIF), https://identity.foundation/, https://github.com/decentralized-identity/
[44] ION (Identity Overlay Network), https://github.com/decentralized-identity/ion/