ブロックチェーン技術における分散型鍵管理の研究

研究年度　令和　5年度

研究代表者名
松崎なつめ

１．はじめに **3**

２．研究内容 **3**

３．研究成果 **4**

3.1 PKI とその課題 4

3.2 SSI について 5

3.3 分散鍵管理について 6

3.4 分散鍵管理の課題 7

４．おわりに **7**

参考文献 **8**

1. はじめに

認証や署名などセキュリティシステム／サービスにおいて、鍵の役割は重要である。特に、ポイント 1：秘密鍵の管理と、ポイント 2：対応する公開鍵の信頼性をどのように確保するのかは運用上、セキュリティシステムの根幹に関係する課題である。

本研究においては、最近検討が進んでいるブロックチェーン技術を用いた分散型鍵管理を考察する。まずは、今年度は分散型鍵管理に関して調査する。

2. 研究内容

本研究では、以下について調査し、3 章に整理する。

１） PKI とその課題

２） 分散型鍵管理とその利点

３） 分散鍵管理の課題

なお、以下では本稿の準備として鍵管理について概説する。

【鍵の役割とポイント】

暗号方式（ここでは、公開鍵暗号を扱う）は、主に守秘と認証に用いる情報セキュリティの要素技術である。暗号方式は主に、入力データのかく乱手順を示す公開の暗号アルゴリズムと、特定の ID（Identity：識別子）だけが有する秘密鍵からなる。暗号アルゴリズムは、例えば、守秘目的の場合は、復号する権利のある ID だけが鍵を有す。認証目的の場合は、秘密鍵はその本人であることを示す情報である。そのため、秘密鍵は漏洩しないよう、また紛失しないよう、安全に管理することが必要である（ポイント 1)。また対応する公開鍵は一般的にランダムな数値であるため、これが誰のものであるか(つまり、特定の ID との紐づけ）を保証することも必要である（ポイント 2)。

なお、認証目的のために、ID/PW で認証する場合もある。鍵を用いる場合と達成できる機能は同じであるが、鍵を用いるほうが PW を直接提示するよりも安全性が向上する。

【鍵と ID、属性】

認証サービスの場合、ある ID が所定の属性を有することを示すことでサービスを使うことができる。例えば、大学の学生サービスを使う場合には、ある ID が「その大学の学生である」との属性を示す。ある ID において所定の属性を有することは、その ID が対応する秘密鍵を有することで確認する。

なお、従来の PKI を用いる場合、ID はサービスや組織ごとに発行されるものであり、1 つのユーザに複数存在する。

以上を整理して例で示すと、ユーザと ID、属性、秘密鍵と公開鍵の対応は例えば次のような対応である。

ユーザＡ

ID1、属性 1：対応する秘密鍵 1、公開鍵 1

ID2、属性 2：対応する秘密鍵 2、公開鍵 2

ユーザB

ID3、属性１：対応する秘密鍵 1、公開鍵 1

ID4、属性 3：対応する秘密鍵 3、公開鍵 3

【ユーザとプライバシ】

ユーザには複数の属性があり、これらを一部開示しないことで、ユーザを特定することが難しくプライバシを確保することが可能となる。例えば上記の例では、属性 1 の認証により、対応するサービスはユーザ A、ユーザ B 双方に提供可能であり、一方どちらであるかは特定できない。

【鍵の漏洩と、鍵の無効化、鍵の紛失】

前述したとおり、秘密鍵は守秘目的の場合は、暗号文を復号する権利を持つものだけが有する。また認証目的の場合は、秘密鍵はその本人であることを示す。このため、前述したとおりもし鍵が第三者に漏洩して悪用されると、本来権利を持たない第 3 者が暗号文を復号できるようになる。また、認証目的の場合は第三者が本人になりすましできるようになる。また、秘密鍵を紛失すると、その権利を有する本人であっても、暗号文を復号できなくなる。また認証ができずに対応するサービスを利用できなくなる。このため、秘密鍵は漏洩しないよう、また紛失しないよう、安全に管理することが必要である（ポイント 1)。

もし鍵が漏洩した場合は、対応する鍵を無効化し別の鍵に更新することが有用となる。

また、秘密鍵を紛失した場合に備え、あらかじめマスター鍵を信頼できるところに預けるなどのあらかじめの施策が必要となる。

なお、一般的な鍵管理については、NIST SP800-130[1]、および CRYPTREC 暗号運用ガイドライン[2]が参考となる。

3. 研究成果

3.1 PKI とその課題

鍵の管理において、その公開鍵が誰のものであるか（つまり、特定の ID との紐づけ）を保証することが必要である（ポイント 2)。

従来使われている PKI（Public Key Infrastructure：公開暗号基盤）は、当該公開鍵を「正当なエンティティ（ID)」が所有していることを、「信頼できる第 3 者（TTP：Trusted Third Party)」が、公開鍵と ID を紐づけて署名した証明書より保証する方法である。より具体的には、いわば、TTP をシステム全体が信頼することで成立する中央集権的なセキュリティシステムである。システム／サービスごとに TTP を設定することで、柔軟な運用が可能となる一方、以下３つの課題があると考察される。

A)　鍵を発行管理する TTP が万が一攻撃されると、システムの信頼性が崩壊する。

2011 年には、英 Comodo、オランダ DigiNotar という SSL/TLS の CA 局（SSL/TLS システムにおける TTP)において、ハッキングにより偽造証明書が発行されるといった事件が起こった。英 Comodo 事件[3]では、Comodo が委託するイタリアの登録局（RA）がハッキングされ、証明書

発行を自動化していたこともあり、Gmail、Skype、Mozilla、Microsoft アップデートなどの偽造証明書が発行された。幸いなことに実害は報告されていないという。一方、オランダ DigiNotar 事件[4][5]では、システムへのパスを不正に入手し侵入した攻撃者が証明書を発行するための情報を盗み出し、偽造証明書が発行された。そして、この対処のためにルート証明書を無効化したことも１原因として、事業破綻となった。

B)　サービスごとに ID や鍵が発行されると、ユーザは複数の ID を管理する必要がある。

利便性の問題を解消する方法としては、例えば「Google アカウントでログイン」のようなシングルサインオン（SSO）の仕組みがある。OpenID Connect[6]は SSO の代表的な方法であり、米 OpenID Foundation において標準化され Google などがサービスに実装している。確かに便利ではあるが、認証システムへの依存が大きく、万が一 Google システムが停止した場合、すべてのシステム、サービスが利用できなくなる。また、認証サーバが不正アクセス等された場合の被害範囲が拡大する。

C)　サービスごとに ID や鍵が発行されると、例えばサービス利用などの個人の情報が分散する。

所謂 GAFA（Google, Amazon, Meta, Apple）と呼ばれる米国巨大 IT 企業は、プラットフォーマとして、ユーザの ID 管理とサービスに伴う個人情報を確保することで、ユーザを囲い込んで成長している。[7]には、ID こそがサイバービジネスの核心であると記載されている。

本来その本人の情報である情報が、サービス企業に囲い込まれているだけでなく、同一人物に関する情報が、サービスごとに分散しているため、サービスを横断したユーザに適した新たなサービスが生まれにくい点が課題である。

3.2 SSI について

前節で述べた３つの課題 A)B)C)を踏まえ、検討された概念が「自己主導型アイデンティティ（SSI：Self-Sovereign Identity)」である。以下では、SSI およびこの概念を具現化する技術である DID と関連する鍵管理（ここでは、分散型鍵管理と称する）について、インターネット上の解説記事等を参考にして著者の理解した内容を述べる。

【SSI とは】

SSI は、2016 年に SSL/TLS の専門家である Christopher Allen 氏が記事[8]において述べた概念である。この中、Allen 氏は ID の進化（集中型から連合 ID、ユーザ中心の ID、そして SSI）と SSI の 10 原則を次（各項目を一部のみ引用）のように述べている。

1. Existence. Users must have an independent existence.
2. Control. Users must control their identities.
3. Access. Users must have access to their own data.
4. Transparency. Systems and algorithms must be transparent.
5. Persistence. Identities must be long-lived.
6. Portability. Information and services about identity must be transportable.
7. Interoperability. Identities should be as widely usable as possible.
8. Consent. Users must agree to the use of their identity.
9. Minimalization. Disclosure of claims must be minimized.

10. Protection. The rights of users must be protected.

なお、この概念の背景としては、前節で述べた３つの課題 A)B)C)の解決に加え、EU 一般データ保護規則 GDPR（General Data Protection Regulation）の思想とも共通したものがある[9]。つまり、GAFA プラットフォーマに牛耳られている個人の情報を、本来の所有者である本人に帰属すべきとの思想である。

この概念の具現化のためには、[10]では以下の４つの要素を挙げている。

i) Verifiable Credentials（VC）：証明書、本稿の分散型鍵管理の一部であるため、3.3 節にて整理する
ii) DID（Decentralized Identifiers）：各エンティティを区別する ID
iii) Agent：各エンティティでの処理、プロセスやソフトウェア
iv) Blockchain：もともとはビットコインなどの暗号資産を支える技術であり、検証可能で変更不可な分散型データベースと考えてよい。

このうち、特に VC と DID は、Web 技術の標準化団体 W3C（World Wide Web Consortium）において議論されている。

以下の図は、W3C の資料[11]から抜粋した図である。この図では、４つの要素の関係を示す。

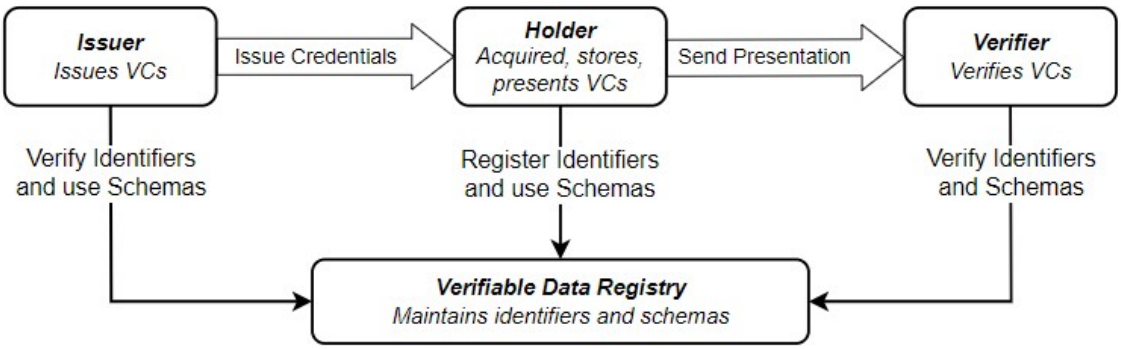

Figure 1 The roles and information flows forming the basis for this specification.

・エンティティは、Issuer、Holder、Verifier の３つ。それぞれ個別の DID を有する。
・Issuer は Holder の属性に対して署名して VC を発行。Holder から Verifier に対しては、VC すべて、あるいはその一部を開示する。一部の属性を選んで開示することにより、匿名認証が可能となる。
・Agent はそれぞれのエンティティ内での処理である。
・各エンティティの動作や VC などは、Blockchain に記録される。

3.3 分散鍵管理について

【分散鍵管理とは】

本稿では、分散鍵管理は、前節における SSI を実現する鍵管理のことを示すものとする。以下はその

１つの具現化方法である。W3C での定義はより広い具現化方法も含む記述となっている

・秘密鍵：Holder が有する。ポイント 1 に示す通り、漏洩しないよう、また紛失しないよう、安全に管理することが必要である（ポイント 1)。

・公開鍵：秘密鍵に対応して定まる。公開鍵は、Blockchain に記録される。Verifier が公開鍵を用いて Holder を認証する。

・VC：証明書：Blockchain に記録されていることで、公開鍵の正しさを検証する（ポイント 2)。

【分散型鍵管理の利点】

分散鍵管理の着目点は、VC が、従来の PKI が発行者である TTP の信頼に基づいていたのに対応し、SSI では、Blockchain に記録していることで確実に確認できることである。このことにより、公開鍵が誰のものであるか（つまり、特定の ID との紐づけ）（ポイント 2）を、特定の TTP を設けずに実現できることが利点である。

SSI においては、Issuer はシステムで信頼する TTP である必要はなく、どのようなエンティティであってもよい。この点より、Issuer が「分散」されていると言える。[10]には、このことを「分散型の PKI」と称している。

3.4 分散鍵管理の課題

鍵管理の２つの課題のうち、ポイント 2 はブロックチェーン技術で解決される一方、分散鍵管理においては、秘密鍵、公開鍵がすべて本人管理となるため、鍵漏洩や鍵紛失の検知、鍵更新、鍵無効化、鍵紛失時の対応などの処理を本人が行う必要がある。従来の PKI に比べ、より安全性が高く、本人が使いやすい方法が必要となる。

これらのうち、鍵紛失に関連しては、科研：20K11815 の研究（タイトル：ブロックチェーンに適した分散管理システム用鍵管理方法の設計と評価の研究:2020 年～2023 年）が活用できる可能性がある。この研究は、具体的には、鍵の紛失時に，対応する暗号資産を救済する方法[12][13][14][15]である。2020 年に関連研究を調査し、2021 年に基本となる非常ボタン式資金退避手法を考案した。この方法は，暗号資産を別アカウントに避難するスマートコントラクト（ブロックチェーン上のプログラム）を用いる方法である。2022 年度には，イーサリウム上で実装評価した。2023 年度には、論文にとりまとめ国際会議に投稿・発表[16]した。

4. おわりに

本稿では、集中 TTP を用いた従来の PKI ベースの鍵管理の課題を確認し、これら課題解決に向けて提案された、SSI およびこの鍵管理である分散型鍵管理に関して調査し、課題を抽出した。鍵管理については、以下２つのポイントを考慮しなければならない。

ポイント 1：秘密鍵は漏洩しないよう、また紛失しないよう、安全に管理しなければならない

ポイント 2：公開鍵が誰のものであるか（つまり、特定の ID との紐づけ）を保証する

このうち、ポイント 2 は、Blockchain を活用した SSI 概念の具現化により解決可能と考える。一方、ポイント 1 については従来の PKI に比べても、さらに重要性が高まっており解決策の検討が必要である。

参考文献

[1] NIST SP800-130 A Framework for Designing Cryptographic Key Management Systems, https://csrc.nist.gov/pubs/sp/800/130/final

[2] CRYPTREC 暗号運用ガイドライン, 2022, https://www.cryptrec.go.jp/report/cryptrec-gl-3004-1.0.pdf

[3] SSL 認証局が偽の証明書を発行、大手サイトに影響の恐れ、 ITmedia, 2011.3.24, https://www.itmedia.co.jp/enterprise/articles/1103/24/news020.html.

[4] 2011 年デジノター事件、Wikipedia, https://ja.wikipedia.org/wiki/2011%E5%B9%B4%E3%83%87%E3%82%B8%E3%83%8E%E3%82%BF%E3%83%BC%E4%BA%8B%E4%BB%B6.

[5] ブラウザだけでなく一部クラウドでもアップデートを DigiNotarの不正証明書問題､その影響は､ ITmedia, 2011.9.8, https://atmarkit.itmedia.co.jp/news/201109/08/diginotar.html.

[6] OpenID 公開資料、https://www.openid.or.jp/document/

[7] 崎村夏彦、デジタルアイデンティティー、日経 BP、2021.

[8] Christopher Allen, The Path to Self-Sovereign Identity, 2016.4.26, https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

[9] Galia Kondova, Jörn Erbguth, Self-Sovereign Identity on Public Blockchains and the GDPR, Proceedings of ACM SAC Conference, Brno, Czech Republic, March 30- April 3, 2020 (SAC'20), 342 - 345. DOI: 10.1145/3341105.337406

[10] @pirodate in TIS 株式会社自己主権型アイデンティティ（Self-Sovereign Identity）の概要、2020.10.5, https://qiita.com/pirodate/items/afc8c239345cfd9fb3a

[11] Verifiable Credentials Data Model v2.0, 2024.3.23, https://www.w3.org/TR/vc-data-model-2.0/

[12] 松崎、喜多、鍵紛失時における非常ボタン式資産退避手法の考察、暗号と情報セキュリティシンポジウム 2021.

[13] 松崎、喜多、鍵紛失時における非常ボタン式資産退避手法の実用化に関する考察、電子情報通信学会 ISEC 研究会、ISEC2021-28, 2021.7.12.

[14] 松崎、喜多、鍵紛失時における非常ボタン式資金退避手法の実装と評価、暗号と情報セキュリティシンポジウム 2022.

[15] 松崎、喜多、福光、鍵紛失時における非常ボタン式資金退避手法の再実装、暗号と情報セキュリティシンポジウム 2023.

[16] Natsume Matsuzaki, Masayuki Fukumitsu, Yoshihiro Kita, Emergency Button: Evacuation of Crypto Asset When Key Loss, 2012 Eleventh International Symposium on Computing and Networking Workshops (CANDARW), 2023. https://www.cs.hiroshima-u.ac.jp/Proceedings23/CANDAR%202023/pdfs/CANDARW2023-dDGdIIHvWRXlB0gY3qHj3/069400a246/069400a246.pdf