様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 １８ 日現在

機関番号：１３９０３
研究種目：研究活動スタート支援
研究期間：2019～2020
課題番号：１９Ｋ２４３４２

研究課題名（和文）分散台帳技術によるメタPKIの構築

研究課題名（英文）Construction of Meta-PKI by Distributed Ledger Technology

研究代表者
掛井　将平（Shohei, Kakei）

名古屋工業大学・工学（系）研究科（研究院）・助教

研究者番号：７０８４６３０２

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：様々なデバイス・サービスを相互接続するデータ流通基盤を中心として，異分野データの連携による付加価値の創出が期待されている．インターネットにおけるデバイスの身元の保証に公開鍵基盤は広く利用されているが，その仕組みの根幹となる認証局への絶対的な信頼を前提とする必要がある．多様なデバイスの相互接続を支える基盤を目指して，本研究では認証局の信頼点を分散する分散型の認証基盤であるメタPKIの開発を行った．

研究成果の学術的意義や社会的意義
多様なデバイス・サービスの信頼性を保証しながら相互接続を支える基盤を目指して，本研究では認証局の信頼点を分散する分散型の認証基盤であるメタPKIの開発を行った．認証局を相互に接続する仕組みとして横断認証技術が利用できるが，その実施判断は各認証局で統一できる必要がある．本研究では，横断認証の枠組みをスマートコントラクトで実現することで，全体で統一された基準のもとで横断認証することが可能となる．

研究成果の概要（英文）：In the data distribution infrastructures that interconnect various devices, it is expected to be created added value through the collaboration of data from different fields. Public key infrastructures (PKIs) are widely used to guaranetee the identity of devices on the Internet, but it is necessary to assume absolute trust in a certification authority, which is the foundation of PKI. Aiming for an infrastructure that supports the interconnection of various devices, we have developed a meta-PKI, which is a decentralized authentication infrastructure that decentralizes the trust points of a certification authority.

研究分野：情報セキュリティ

キーワード：公開鍵基盤　認証局　横断認証　スマートコントラクト　分散型台帳技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

IoT（Internet of Things）や CPS（Cyber Physical System）により，物理世界と仮想世界から得られるデータを分野横断的に活用し，社会課題の解決やイノベーションの創造を計るデータ駆動型社会の実現を目指した取り組みが進められている．データ駆動型社会の実現を目指すうえで，データは価値を持つ資源として活用されることが期待されており，多くのデータを収集しうるサービス提供者は，そこから得られた新たな知見をサービスに還元することで，より多くのデータを集めることができると考えられる．これはデータの寡占に繋がることから，複数のサービス提供者がデータ共有する基盤を構築できれば，データの寡占を自然な形で防ぎ，データ駆動型社会を支えるサービスの創出を促すと期待できる．これには，データを受け渡しする主体の本人性を保証し，なりすましや否認を防ぐ仕組みが安全に機能していることが求められる．

主体と公開鍵を結びつける公開鍵基盤（Public Key Infrastructure，PKI）が本人性を確認する技術として使われている．データ共有基盤に参加する全ての主体が公開鍵証明書を発行する認証局を信頼することで，各主体間の信頼関係が間接的に構築される．データ共有基盤上の認証局が単一の場合，データの価値が高まるほど，認証局への中央集権化が強まる．その結果，公正なデータ共有が阻害されるので，特定の認証局に依存しない認証基盤の構築が必要不可欠である．

２．研究の目的

単一の認証局でなく，サービス提供の範囲にあわせて認証局を配置する形で分散することが，認証局の中央集権化の問題の解消に有効であるが，人手による認証局の運用ポリシーの確認が必要である．インターネット上のサーバ証明書の発行と検証では機能しているが，データ駆動型社会を支える膨大なデバイス群に対してそのサービス提供範囲ごとに設置される認証局を従来通りに横断認証することは事実上不可能である．そこで，本研究では，サービス提供者が自サービス用の認証基盤を個別に運用し，それらを連携したものをデータ共有基盤における仮想的に単一の認証基盤として運用することを目標とする．そのために，まず，認証局間の信頼関係を構築する（課題１）．さらに，データを広く有効活用するために，不特定のサービス提供者との連携ができるように，対向する認証局の信頼性を確認できること（課題２）と確認した認証局の信頼性が正当であるか確認できること（課題３）の三つの課題を設定する．

異なる認証局の信頼関係を構築する手法に横断認証がある．しかし，その実施の判断は当事者に委ねられる．そこで，認証局間で自律的に信頼関係を構築可能な横断認証の機能を含む分散型認証基盤の枠組みを確立する（課題１に対応）．そして，横断認証するための対向する認証局の信頼性を検証できる手法を確立することと（課題２に対応），検証した信頼性が正当であることを確認可能とするセキュリティチップ TPM を信頼点とした認証局の構成方法を確立する（課題３に対応）．

３．研究の方法

本研究では，三つの研究項目を設定して，分散型台帳技術によるメタ PKI の構築を目指す．

研究項目１：スマートコントラクトによる分散型認証基盤の枠組みの設計
研究項目２：横断認証のための認証局の信頼性を検証する手法の設計
研究項目３：信頼性確認の正当性を検証できる TPM を信頼点とした認証局の設計

分散型認証基盤に向けて，横断認証を行うための基盤と，これを統一的な信頼性確認の基準のもとで実施するための枠組みをスマートコントラクトで開発する．加えて，その信頼性確認を TPM のようなハードウェアに由来させることで第三者による正当性の検証可能とする．

４．研究成果

研究項目１では，コンソーシアム型の分散型台帳技術（Distributed Ledger Technology）の Hyperledger Fabric[1]を用いて，メタ PKI を設計・構築した．図 1 に示すように，認証局（Certificate Authority，CA）が Trustee の本人性を保証するとき，CA を信頼する Trustor は Trustee の本人性を信頼する．これは，Trustor と Trustee 間の信頼関係を CA が仲介している構造となっている．CA は自身の秘密鍵を使って，Trustee が安全に保管する公開鍵に対して

Trustee の本人性を埋め込んだ公開鍵証明書を発行する．公開鍵暗号方式により，CA の秘密鍵の対となる CA の公開鍵を使えば，CA が Trustee に公開鍵証明書を発行したことを検証できる．秘密鍵はその管理者が安全に保管している一方で，公開鍵は誰でも利用可能なように公開されている．この非対称性により，公開鍵証明書を発行できるのは CA のみであるが，その検証は誰でも実施できる．

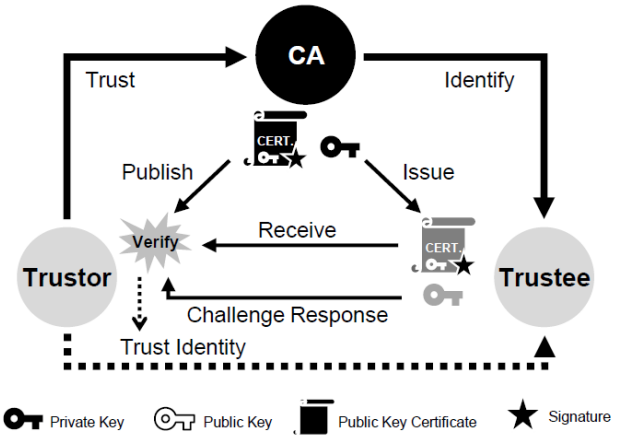

図 1　CA により構築される信頼関係．Trustor が Trustee の本人性を CA を介して信頼している様子．

単体の CA が，多数の主体の信頼関係を仲介することから，CA は単一信頼点となる．CA が Trustee の本人性を保証し，公開鍵証明書の発行を担うことで，効率的に Trustee の本人性を検証できるが，これは CA の秘密鍵は安全に保管されていることが前提である．CA の秘密鍵が漏洩すれば CA になりすまして任意の公開鍵証明書を発行できる．つまり，偽の証明書所有者になりすますことができる．これは，実世界における免許証の偽造のような行為にあたる．CA の運用は安全対策が施されているものの，一部の CA で不正な公開鍵証明書が発行された事例がある．

CA の秘密鍵が漏洩すれば，Trustor は Trustee が本人かどうか判断できない．CA が仲介する信頼関係が増えるほど，この影響は大きくなる．つまり，単体の CA で全ての信頼関係を仲介するのではなく，分散配置された複数の CA が分担して信頼関係を仲介する仕組みがあれば，単一信頼点のリスクを軽減できる．CA を分散する仕組みに，CA が別の CA に公開鍵証明書を発行し，相手の本人性を保証する横断認証（Cross-Certification）がある．しかし，横断認証の実施判断の基準は各 CA に委ねられており，全体として整合のとれた信頼関係の構築はできない．

本研究では，複数の CA が横断認証を実行する基盤として図 2 に示す**メタ PKI** を提案した．メタ PKI は，図 1 に示す従来の PKI（EE Layer と CA Layer）の上位に配置された Meta-CA Layer が対向の mCA（メタ CA）と横断認証を実行する．横断認証の実施は，mCA_X と mCA_Y が直接実施するわけではなく，図 2 の Distributed Ledger Network が仲介する．

Distributed Ledger Network は，複数のノードが各自所有する台帳を同期させて，分散型台帳を構築するネットワークである．ネットワーク上には一つの台帳があるように見えるものの，その台帳のコピーが複数のノードで管理されている．その台帳への操作はスマートコントラクトで定義される．スマートコントラクトはプログラミング可能な台帳へのインタフェースであり，入力と処理を定義して，その処理結果

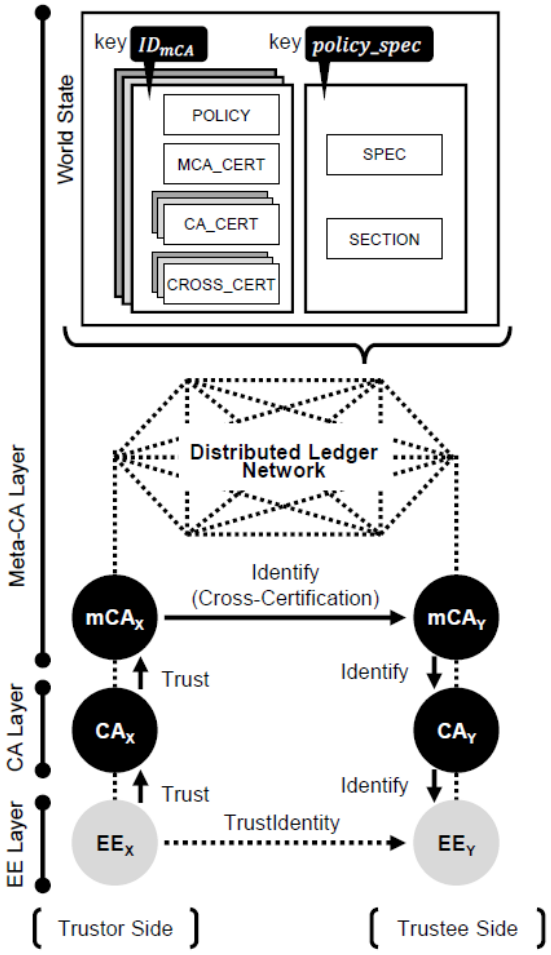

図 2　本研究課題で開発したメタ PKI．EEX が EEY の本人性を CA_X，mCA_X，mCA_Y，CA_Y を介して信頼している様子．

を台帳へと保存する．反対に，台帳から取り出したデータを処理に応じて加工してスマートコントラクトのユーザに提示することもできる．本提案では，Distributed Ledger Network として Hyperledger Fabric を用いた．

分散型台帳で管理されるデータは図 2 上部の World State である．World State 内には，「policy_spec」として定義された領域に，mCA を評価するためのポリシーが使用する「鍵アルゴリズム」と「署名アルゴリズム」,「公開鍵証明書の有効期限」の三つのセクションに分かれて定義されている．各セクションが取る値に応じて信頼度スコアが事前に定義されている．使用するアルゴリズムはセキュリティが高いものほど信頼度のスコアは高く，有効期限は短いほど信頼度のスコアが高くなるように事前に設定されている．policy_spec とは別に，mCA ごとに，mCA 自身の公開鍵証明書（MCA_CERT）・mCA が対向する mCA に発行した公開鍵証明書（CROSS_CERT）・mCA の配下の CA が発行した公開鍵証明書（CA_CERT）と mCA のポリシー（POLICY）が管理されている．

従来の横断認証では，横断認証の実施判断の基準は各 CA に委ねられており，全体として整合のとれた信頼関係の構築はできなかった．本研究課題で提案したメタ PKI は，Distributed Ledger Network とスマートコントラクトにより，横断認証を実施する枠組みを定義している．つまり，各 mCA の横断認証はこの枠組み内に強制されることで，全体として整合のとれた信頼関係を構築するアプローチをとっている．

複数の台帳を同期させることから台帳へのデータの書き込みには時間がかかる．一方で，台帳は各ノードが持っていることから，台帳からのデータの読み込みは書き込みに比べて高速に実行できる．提案システムを実装し，汎用的な PC を用いて Docker 上に Distributed Ledger Network を構築し，横断認証の処理時間と横断認証の検証時間の評価を行った．前者は書き込み処理が発生するが，後者は台帳に格納されたデータを使って検証するので読み込み処理だけが発生する．検証の結果，横断認証は平均 2463.3ms，横断認証の検証は平均 65.7ms となった．横断認証よりも検証の方が実行頻度が高くなることが想定されることから，このような処理時間の傾向はメタ PKI にとって望ましい．

研究項目２に関して，CA の信頼性の判定には「CA の構成」と「CA の運用」の二つの側面からのアプローチが考えられる．前者は CA がどのようなポリシーに基づいて構成されているかに着目しており，後者は実際に CA がどのような運用を行っているかの側面に着目している．CA を設置するには，「証明書ポリシー」と「認証局運用規定」の二種類の文書の公開が求められており，これらの文書の品質を測るのが前者のアプローチであり，これらの文書通りに運用できているかを測るのが後者のアプローチである．これらの文書は各 CA が用意するものではあるが，業界標準（Baseline Requirements[2]，RFC5280）が存在する．その標準にあわせて CA が運用されているかどうかを CA が実際に発行した公開鍵証明書から測る技術を開発中である．

研究項目３に関して，CA は秘密鍵の安全な管理が必要であるが，この管理を Trusted Platform Module（TPM）を用い，かつ，TPM で管理されていることをリモートから検証できる仕組みを関連研究や技術面での調査をもとに検討中である．

[1] The Linux Foundation, ″Hyperledger Fabric,″ https://www.hyperledger.org/use/fabric.
[2] CA/Browser Forum, ″Baseline Requirements Documents (SSL/TLS Server Certificates) | CAB Forum,″ https://cabforum.org/baseline-requirements-documents.

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Shohei Kakei, Yoshiaki Shiraishi, Masami Mohri, Toru Nakamura, Masayuki Hashimoto and Shoichi Saito	４．巻 8
２．論文標題 Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 135742～135757
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.3011137	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 掛井将平，白石善明，毛利公美，中村徹，橋本真幸，齋藤彰一	４．巻 2019
２．論文標題 分散型認証基盤に向けたスマートコントラクトを用いた相互認証方式の提案	５．発行年 2019年
３．雑誌名 コンピュータセキュリティシンポジウム2019 論文集	６．最初と最後の頁 539-546
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 江澤友基，掛井将平，白石善明，瀧田愼，毛利公美，森井昌克	４．巻 119
２．論文標題 ブロックチェーンを用いたユーザ中心の認可プロトコルの一実装～User-Managed AccessのHyperledger Fabricによる実装～	５．発行年 2020年
３．雑誌名 信学技報	６．最初と最後の頁 307-312
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 江澤友基，掛井将平，白石善明，瀧田愼，毛利公美，森井昌克
２．発表標題 ブロックチェーンを用いたユーザ中心の認可プロトコルの一実装～User-Managed AccessのHyperledger Fabricによる実装～
３．学会等名 情報通信システムセキュリティ研究会（ICSS）
４．発表年 2020年

１．発表者名
Shohei Kakei, Yoshiaki Shiraishi, Masami Mohri, Toru Nakamura, Masayuki Hashimoto, Hiroyuki Yokoyama, Shoichi Saito

２．発表標題
The Concept of Meta-PKI: A Decentralized Trust Model Using Smart Contract for Internet of Things

３．学会等名
The 14th Asia Joint Conference on Information Security (AsiaJCIS2019)（国際学会）

４．発表年
2019年

１．発表者名
掛井将平，白石善明，毛利公美，中村徹，橋本真幸，齋藤彰一

２．発表標題
分散型認証基盤に向けたスマートコントラクトを用いた相互認証方式の提案

３．学会等名
コンピュータセキュリティシンポジウム 2019 (CSS2019)

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
研究者詳細 - 掛井　将平
http://researcher.nitech.ac.jp/html/100000784_ja.html

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関