indicio

初心者のための分散型IDと検証可能なデータのガイド

Trevor Butterworth
VP Communications & Governance

インターネットはその設計当初、コンピュータ同士の通信に重点を置いており、人間、組織、そして物理的なオブジェクトを識別する仕組みが備わっていませんでした。

現在、世界には50億人を超える人々、200億台以上の機器がネットワークに接続されています。さらに、数千万の企業や組織もネットワークで繋がっており、人工知能（AI）もますます普及しています。

あなたがオンラインにいる1億8,000万人のうちの1人であるならば、デジタル「アイデンティティ」、つまりデジタルIDを持っている可能性が高いでしょう。このデジタルIDには、電子メールアドレスやソーシャルメディアのアカウント、商品を購入したりサービスにアクセスするための多数のユーザーアカウントやプロフィール等が含まれます。また、FacebookプロフィールのようなID識別子を使って、複数のサイトやサービスに簡単にアクセスすることもできます。

私たちは、このようなデジタルIDを「集中型」と呼びます。これらのIDは、利用者が提供した個人データが中央データベースに保存されるという特徴を持っています。たとえば、電子メールアドレスやユーザーアカウントを作成する際に入力した情報は、特定の企業やサービス提供者によって管理されます。これにより、利用者の身元確認やアクセス権の管理・検証が、その単一の環境内で行われます。

集中型IDのシステムでは、ID管理が利用者自身の手にないことが特徴の一つです。これはIDプロバイダー（電子メールサービス、企業、その他のオンラインサービス等）が、利用者が提供した情報を中央データベースに保存し、その情報を管理する責任を負うからです。一例として、アカウントを作成する際に電話番号を提供し、その番号に送られてきたコードを入力して本人確認を行う手順が挙げられます。このプロセスではIDプロバイダーが利用者の情報を確認・検証しIDを一元的に管理します。結果として、あなたのID情報は、提供した情報を基にIDプロバイダーが管理し、維持することになります。

このようにして、デジタルID とデジタル ID の認証がオンラインで管理されるようになりました。Federated identity (連合アイデンティティ)では、1 つのアイデンティティ アカウントを使用して複数のサイトやサービスにアクセスできますが、アイデンティティアカウントとそれに関連付けられた個人データは依然として元のアイデンティティプロバイダーによって保持、管理されているため、依然として一元化されています。

私たちがこのような手法をとっているのは、インターネットが人間や組織のアイデンティティを管理するように設計されていないからです。ネットワークは接続するために構築されており、コンピューターを認識するように設計されています(そして長年、接続されているコンピューターの数は非常に少なかったため、誰が使用しているかを誰もが知ることができました。インターネットが World Wide Web に進化し、世界人口の65 パーセント (今後も増加中) と数十億台以上の機器が接続されるとは誰も予想していませんでした。

一元化されたID により、インターネットを利用している全ての人々と組織がオンラインで参加する方法を可能にしました。これは驚くべき成果です。しかし、このシステムは、信頼できるID層が構造的に欠如している問題に対する不完全な解決策でもあります。その結果、詐欺、摩擦、プライバシーの損失、データ保護規制の順守の複雑さなどの問題が発生しています。

データを信頼できるようにするには、根本的な検証問題を解決する必要があります。

ユーザー名、パスワード、電子メールなどの一元的なID の構造により、単純なパスワード(1、2、3、4、5...)を推測したり、フィッシングメールやロボコールを使用したりすることで、デジタルID や識別子が簡単に偽造、盗用されます。

たとえあなたがオンラインで詐欺に対して聡明で、本人が何も悪いことをしていなくても、大量の個人データを保持するデータベースは個人情報盗難の魅力的な標的となります。集中型モデルでは、これらのデータベースが一元的に管理されているため、単一の脆弱性がセキュリティを崩壊させ、データベース全体の情報が危険にさらされる可能性があります。このようなシステムの弱点により、詐欺やデータ侵害が発生した場合の損失は莫大です。被害を受ける個人や企業の損失だけでなく、その防御のためのコストも膨大です。

同様に、一元化されたID システムに障害が発生した場合、自分のアカウント、または障害がederated identity に関係する場合は複数のアカウントから締め出されます。そして、これらの外部の脅威に加え、内部の問題もあります。誰があなたのデータにアクセスできるのか、また、アカウントを開設したときに「同意」ボックスにチェックを入れて、そのデータをどのように扱うことに同意したかなどです。

かつては、全てをオンラインで行うことが便利であるため、データのプライバシーを気にする人は誰もいないと考えられ、問題視されていませんでした。しかし、現実は変わりました。データ収集と監視の拡大により、国民と政治の両方の懸念が高まり、その結果、GDPR (欧州連合の一般データ保護規則) やその他の世界的な類似の規制等、広範なデータプライバシー法が制定され、これらはすべて人々の個人情報の保護とデータが悪用されないことを目的としています。今日個人データの保存は、企業や組織にとってコンプライアンスの悩みの種であり、コストがかかります。

パスワードの煩わしさは誰も好みません。パスワードが解読しにくいと覚えにくくなり、覚えやすいと解読しやすくなります。多要素認証は保護を強化しますが、煩わしさも増します。デジタル世界の全体的な流れは、物事を可能な限り合理化してシンプルにすることですが、多要素認証はハッキングに対して、無防備というわけではありません。

デジタル世界におけるパスワードへの依存度は膨大です。ある調査では、平均的な人は100個のパスワードを持っていると推定されています。これらのパスワードはすべて頻繁に変更する必要があり、簡単に推測されない程度に複雑で、アカウントごとに固有で、再利用されないものでなければなりません。2022年には240億個のパスワードが盗まれました。

これらの問題が重なり、企業、消費者、公共部門がデジタル化を推進し、受け入れているにもかかわらず、デジタル インタラクションはより複雑でコストがかかり、信頼性が低くなっています。しかし、人々や組織がオンライン セキュリティに失敗し続けるのであれば、オンライン セキュリティは、私たちが望むような行動や機能ではなく、人々の行動や組織の機能に対処するように設計する必要があるのではないでしょうか。

数十億台の接続された機器に識別子を付与する必要性により、問題の規模が拡大する一方、人工知能の進化により、偽造や詐欺がより巧妙になり、その範囲が拡大しています。今日、私たちはアイデンティティシステムで画像や音声のディープフェイクを考慮する必要があります。データの信頼性を確保するために、根本的な検証問題を解決する必要があるのです。このような状況下では、分散型アイデンティティが役立ちます。

分散型アイデンティティとは何か?

分散型 ID では、次の質問に答えることで、ID を集中管理する必要がなくなります。

1. 誰があなたのデジタルID 識別子を管理すべきか?
2. 個人データはどこに保存する必要があるか?
3. 個人データはどのように共有されるべきか?
4. デジタル ID とそれに関連付けられたデータが信頼できるものであることを検証できる方法で、これら全てをどのように行うことができるか?

ビジネス、組織の実装とユーザーエクスペリエンスの観点から、これを実現するテクノロジーは、既存のインフラストラクチャーに簡単に統合でき、誰もが簡単に使用でき、プライバシーが保護され、摩擦がなく、拡張可能で、低コストである必要があります。

更に掘り下げ、先に進みたい場合は、Google Marketplace 、そして間もなくAWS Marketplace で、これら全てをバーチャルボックスから入手することができます。またこの分野に興味を持たれたら、まずこれから述べる以下の質問に答えることから始めてみてください。

1. デジタル ID 識別子を管理するのは誰か ?

回答:あなたです!これを可能にする重要な技術開発は、分散型識別子、別名「DID」です。 電話番号、電子メール、Web サイトについて考えてみましょう。ある意味、これらはすべて、誰かまたは何らかの組織に連絡したり、リソースやサービスにアクセスしたりするためのアドレスです。

DID は一種のアドレスでもあり、自分自身、組織、または自分の管理下にあるものを表すために作成できるものです。ただし、電話番号、電子メール、Web サイトのアドレスとは異なり、DID は完全に管理できます。ID プロバイダー、認証局、中央レジストリが存在する必要はありません。

まずこれを頭に留めておいてください。

2. 個人データはどこに保管する必要があるか?

回答: あなたが保管してください! ID 用のデジタルアドレスを作成する際、デジタルパスポートや運転免許証などの ID 資格情報など、そのアドレスに送信される情報を受け入れることができます。これらの認証情報は、モバイル デバイス上の特別なソフトウェア(デジタル ウォレット) またはクラウドに保存できます。

これも頭に留めておいてください。

3. 個人データはどのように共有されるべきか?

回答: 誰と共有したいかを選択することです。個人データを保持できる場合は、共有に同意できます。もちろん、データを共有したり、身元を証明したりする法的義務がある状況は数多くあります。しかし、そうではない状況も多くあるのです。

DID と検証可能な資格情報

おそらく、これがどのように機能するかについて多くの質問があると思いますが、それらについてお答えします。まず、要約しましょう

- **自分のアイデンティティのためのアドレスを作成できる。**
- **自分の個人データ(または組織や物に関するその他の重要な情報) を保存できる。**
- **そのデータを共有する相手をコントロールできる。**

私たちが行ったのは、デジタルID と識別子を作成管理するために個人データが詰まった集中型データベースの必要性をなくしたことです。代わりに、私たちは自分のデータを保有し、つまり自分のデータをコントロールします。これはプライバシーとセキュリティに重大な影響を及ぼします。広告がインターネット上で私たちを追跡できるように(そして他の未知の目的で) 個人データにチェックを入れる小さなチェックボックスは、もはやかつてのような重要性がありません。

4. デジタル ID とそれに関連付けられたデータが信頼できるものであることを確認するには、どうすればよいか?

回答: 検証可能な資格情報を使うことです。ここで、物事はさらにエキサイティングになり、また複雑になります。まず、高度40,000 フィート (役12,000メートル) から眺めていても、DID の所有者は、自分がDID を管理していることを暗号的に証明できます。

どうやってそれが可能なのでしょうか？可能な限りの簡潔な説明: DID を作成する際、DID の宛先がどこであるかを定義します。個人、運転免許証を交付する都道府県公安委員会、企業、銀行などです。あなたが自身がコントロールするのです。企業や政府機関は、複数の管理者がいる場合があります。

ここまでご理解いただけましたでしょうか。

各 DID には、秘密暗号キーとペアになった公開暗号キーがあります。(暗号キーとは何か?データを暗号化および復号化するアルゴリズム(関数) を備えた文字列です。)

銀行の DID に連絡すると、銀行の公開キーを使用してメッセージが暗号化されます。メッセージを復号化するための秘密キーを持っているのは銀行だけです。銀行がメッセージに応答した際、その銀行が銀行DID を管理していることがわかります。また、あなたが銀行に接続するためにDID を使用しているため、銀行はあなたがあなたの名前でDID を管理していること、つまり口座所有者であることを確認することもできます。

これらはすべて、DIDComm と呼ばれる DID 間に作成された直接的で安全な通信チャネルを通じて瞬時に行われます。

これが、DID がアイデンティティのアドレスであると言うだけでは、DID が何であるかを完全に捉えていない理由です。DID は、他の DID と安全に通信できるようにする通信エンドポイントが組み込まれたアドレスなのです。

これは、DID が接続すると、暗号化されたピアツーピア通信チャネルを介し、相互に認証されることを意味します。

これが何を意味するか ?あらゆる情報の出所を確認する方法ができるようになったということです。

セキュリティ上の利点 DID はいくつでも作成できるため、別の DID との各々のインタラクションを一意に暗号化することができ、デジタルインタラクションが相関するのを防ぐことができます。

DID から検証可能なデータの共有まで

これで、私たちはデジタルID をコントロールし、相互にデータを共有する前に相互認証できるようになりました。しかし、1) DID を取得し、2) DID を捜すにはどうすればよいのでしょうか?

1)。デジタル ウォレット内のソフトウェアがDID を作成します。2)。資格情報の発行者は、パブリックDID を検証可能なデータレジストリ、または分散台帳に送信し、その DID を DID 通信チャネルに接続して作成できるようにリンクを送信します。

検証可能なデータレジストリは ID 用のブロックチェーンであり、パブリックDID、つまり資格情報発行者の DID (個人の DID ではありません) の書き込みと検証に使用されます。資格情報の発行者は分散台帳ネットワークを使用し、アドレスと公開キーを書き込み、そうすることで発行した資格情報を検証できます。

情報はブロックチェーンベースの台帳に特別にリンクされた方法で書き込まれ、保存されるため、その情報を変更しようとする試みはタイムスタンプ付きのブロックチェーンを破壊し、検出することが可能になります。

さらに、ネットワーク上には台帳のコピーが複数あるため、台帳の各コピーは、いずれか1 つの台帳に書き込まれた内容を記録し、配布します。ネットワーク内の台帳のコピーは全て、台帳に書き込まれる内容に関して一致している必要があります「コンセンサス」。

.

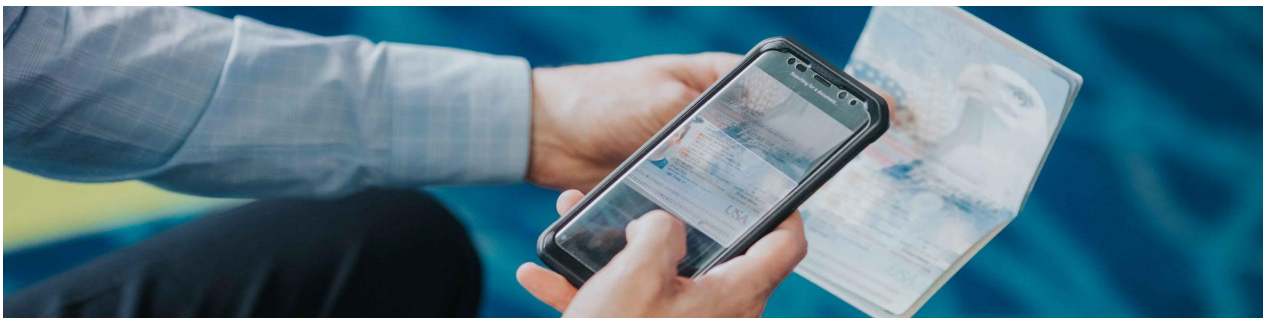
これが意味すること 分散型台帳ネットワークは、情報源のアドレスを検索して認証し、情報が改ざんされていないことを証明する方法を提供します。

信頼関係を構築するためのこのアーキテクチャーは完成しましたが、実際のデータはどのように共有されるのでしょうか?このセクションは「検証可能な資格情報」という答えから始まりました。

検証可能な資格情報を理解する1 つの方法は、資格情報を ID とデータの輸送コンテナとして考えることです。コンテナを開け、改ざんすることなく、コンテナの起源を偽ったり、コンテナ内のデータ変更を行うことはできません。もしそのような事態が発生すれば、即座に判明します。これらのコンテナは、モバイルデバイス上のデジタルウォレット アプリケーションで保持するのです。

技術的には、資格情報は情報を組み立てるためのスキーマ (デジタル概略図) です。パスポートの検証可能な資格情報には、パスポートの構造と特定の情報領域の説明が含まれています。パスポート資格証明書を発行する政府は、このスキーマをパスポート局にリンクする情報とともに、このスキーマを分散台帳ネットワークに書き込みます。

パスポート発行者はパスポート申請者にQR コードを送信します。このプロセスにより、潜在的な所有者は DIDComm 経由で接続できるようになります(これを有効にするためのデジタルウォレット アプリを持っていない場合は、ダウンロードするよう求められます。



DID から検証可能なデータの共有まで

DIDComm 接続が確立されると、その人には検証可能な資格情報としてパスポートが提供されます。受け入れると、特定のデータが入力された資格情報を受け取ります。データは暗号スタンプでデジタル署名されており、情報が発行者からのものであり、変更されていないことを確認します。

実際のパスポートデータを保持しているのは、パスポートオフィス(発行者) と、検証可能な証明書を受け取ったあなただけです。このデータは分散型台帳ネットワークに書き込まれず、検証を機能させるために書き込まれる必要もありません。分散型ID ネットワークの鉄則があるとすれば、それは個人データを台帳に書き込んではならないということです。

我々は、ネットワーク上のDID と DIDComm、スキーマ、およびその他の資格情報メタデータを使用して、全ての検証作業を実行します。これは、データソースにチェックインしたり、第三者とデータをクロスチェックしたりすることなく、いつでもどこでも(適切なソフトウェアがある限り) 検証可能な資格情報を検証できることを意味します。

重要事項 ブロックチェーン ベースのネットワークは、エネルギー消費に関して精査されています。この懸念は、検証に「マイニング」が必要ないため、ブロックチェーンベースの ID ネットワークには当てはまりません。台帳にスキーマを書き込むことや DID を検索することは、Web 検索と同じだけのエネルギーしか消費しません。

例えば...

私が銀行だとしましょう。あなたが本人であることを証明するために必要な従来の保証手順を全て終え、新しい口座を承認しました。ここで、これまで説明したテクノロジーを使用して口座の検証可能な資格情報を発行することで、あなたが口座所有者であることを証明する方法を紹介します。

第一段階 私 (銀行) が口座資格情報を記載したQR コードを電子メールまたはテキストメッセージで送信します。顧客はこのQR コードをモバイルデバイスでスキャンします。これにより、DIDComm 経由で安全な直接接続が確立され、検証可能な資格情報の送受信が可能になります。

第二段階 この資格情報の提供を受け入れます(または拒否します)。同意すると、認証情報を受け取り、モバイル デバイス上の特別なソフトウェア(デジタル ウォレット アプリ) に保存されます。資格情報には、アカウントに関する関連詳細が含まれています。

最終的には、ユーザ名やパスワード、多要素認証の代わりに、このクレデンシャルを使用して口座にログインし、口座取引を行ったり承認したりします。

銀行は、あなたがDID を管理していることを確認できるため、口座にログインしているのがあなたであることを知ることができます。また重要なことは、ソフトウェアが銀行の DID を自動的に検証するため、銀行の偽装をしている相手ではなく、銀行とやりとりしていることを確認できるという点です。

検証可能な資格情報が作成されると、銀行は口座の詳細を直接送信します。それらは検証可能な資格情報に含まれています。

また、銀行は暗号デジタル署名と、スキーマと呼ばれる資格情報の構造に関するメタデータを分散台帳ネットワークに書き込みます。

この情報は、資格情報の信頼性と、資格情報に含まれる情報の完全性、つまり情報が改ざんされていないことを検証できることを意味します。

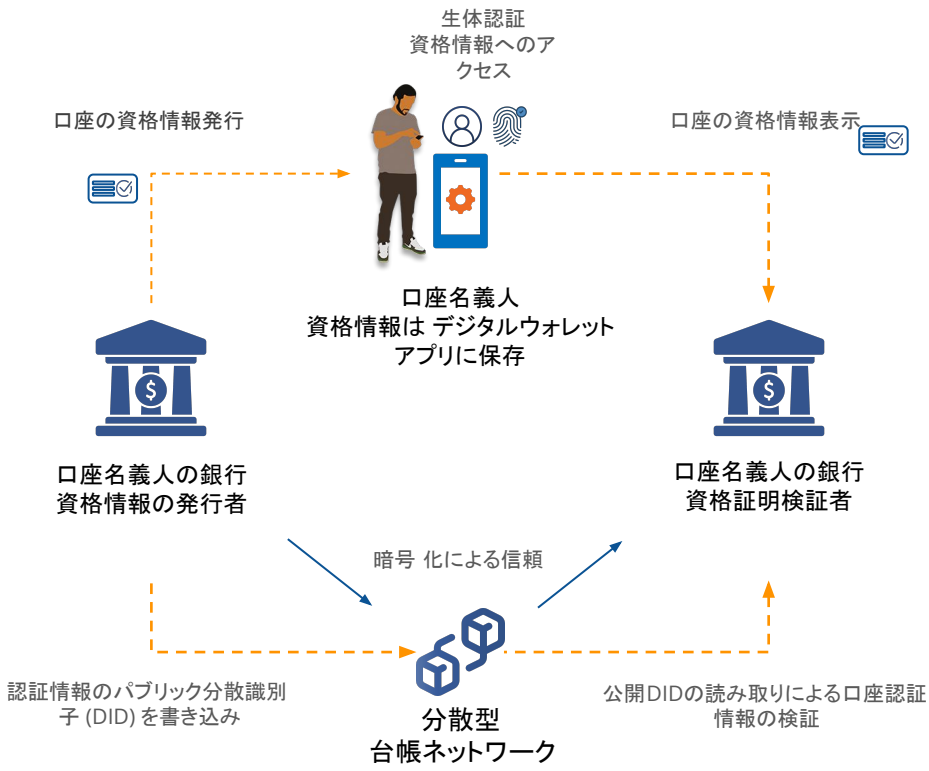
分散台帳には個人情報は書き込まれません。もしあなたの個人データが台帳に書き込まれると、誰でもそれを見ることができます。

検証ソフトウェアは、他の組織が使用して、あなたが銀行口座の所有者であることを確認するために使用することができ、不正行為を減少させ、住宅ローンの承認などのプロセスを合理化するさまざまな方法を可能にします。

これは、銀行や決済サービスが顧客を確認し、顧客が銀行とやり取りしていることを確認するための強力な方法です。

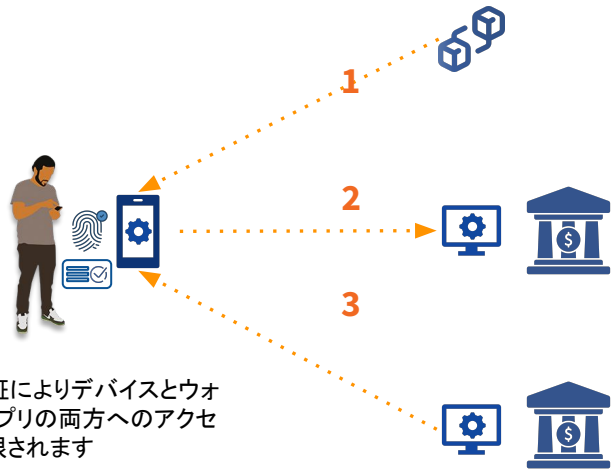
*資格情報の発行、保存、提示、検証を管理するソフトウェアを「エージェント」と呼びます。

口座資格情報の発行、保持、検証



分散型台帳には個人情報は保存されません。

情報を共有する前に本人確認



生体認証によりデバイスとウォレット アプリの両方へのアクセスが制限されます

顧客は、ウォレット アプリと銀行口座の検証可能な資格情報を使用して、分散台帳上の銀行の公開 DID とキーを読み取ります。

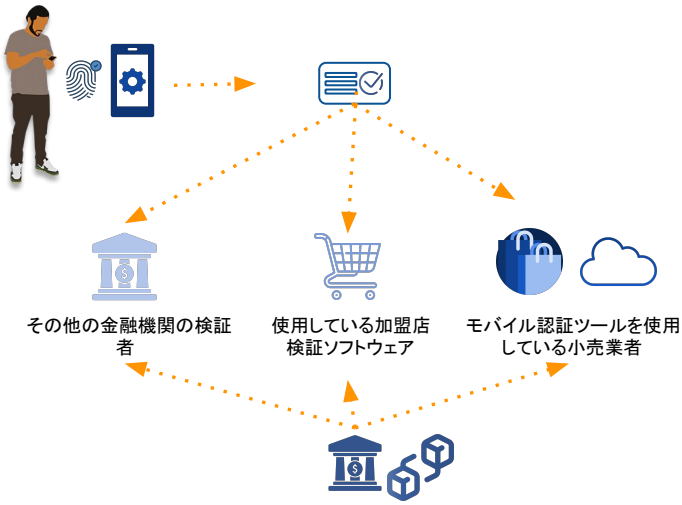
顧客は銀行の公開キーを使用して暗号化されたメッセージを銀行に送信します。

銀行は、検証可能な資格情報内の顧客の公開キーを使用してメッセージを復号化し、顧客に応答します。

この検証は自動で即時に行われます。

これらの作業は全て、個人データや取引データが通信される前に行われます。

検証ソフトウェアは、検証可能な ID とデータのエコシステムを作成します



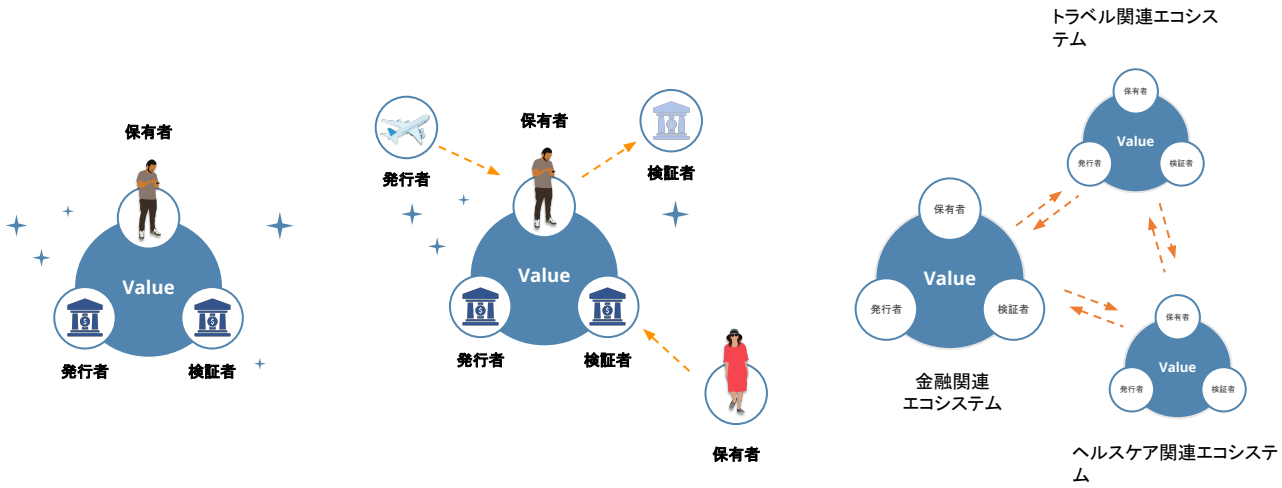
アカウント認証情報を提示します

検証者は、発行者の公開暗号キー、資格情報スキーマ、および資格情報定義を含む公開発行者 DID を読み取ります。台帳レコードのデジタル署名により、その完全性 (つまり、資格情報が変更されていないこと) が確立されます。

失効がある場合、検証者は失効レジストリの状態をダウンロードします。

分散型台帳には個人情報は保存されません。

オープンスタンダードと相互運用性により、データとアイデンティティを異なるエコシステム間で共有し、認証することができます。



発行者、保有者、検証者からなる単一のクローズド エコシステム。資格情報を発行するエンティティは、資格情報を検証するエンティティです。

相互運用性により、認証情報を検証できる他の関係者にエコシステムが開かれ、さらに他の認証情報の発行者や所有者にもエコシステムが開かれます。

価値を示す検証可能な認証エコシステムは、他のエコシステムとのリンクを推進し、すべての人に価値をもたらします。

検証可能な ID とデータによりシームレスなプロセスが可能になります

各当事者は情報を共有する前に相互に認証し、共有される情報のソースと完全性を信頼できるため、情報に基づいて即座に対処できます。データを信頼する必要がある対話において、瞬時の意思決定が可能になります。検証ソフトウェアを持っている人は誰でも、資格情報とその中のデータを検証できます。これにより、信頼を拡大してエコシステムを構築し、他のネットワークを統合することができます。

例として、検証可能な資格情報が住宅ローンの申請のようなものをどのように管理するかを考えてみましょう。多数の紙の文書を集めて手渡ししたり、スキャンして電子メールで送信したりする代わりに、

多くの場合、繰り返しになりますが、様々なな検証可能な資格情報(銀行取引明細書、給与明細、個人ID など) を通じ、全ての情報を保持し、それらをまとめて住宅ローンブローカーに送信することができます。

クレデンシャル・スキーマを通じて伝達可能な情報は全て、その情報源とともに検証可能になりました。発行者のトラスト・リスト、複雑な情報の流れと承認は、クレデンシャル・エコシステムの各参加者のエージェント・ソフトウェアに直接送信される、機械可読のガバナンス・ファイル によって管理されます。

indicio

セキュリティとプライバシー

分散型 ID の主な特徴は、サードパーティの集中型データベースが不要になることです。ID を検証し、アカウント、リソース、サービスへのアクセスを管理するために個人データを保存する必要がありません。保管庫が不要で保管庫内に個人データがない場合は、企業や組織のセキュリティが大幅に向上します。

また、検証がシームレスであるため、企業や組織は「ゼロトラスト」セキュリティをより簡単に導入できます。ゼロトラストとは、従業員またはユーザーにシステム内のリソースへのアクセスを提供することに関して「決して信頼せず、常に検証する」ことを意味します。

個人データの保存はセキュリティだけでなく、プライバシーとデータ保護規制の遵守にも関係します。これは、分散化によって企業や組織が欧州の一般データ保護規則（General Data Protection Regulation）のような規制などに準拠できるよう支援するためです。

企業やサービスとして、個人情報を保管せずに本人確認やリクエスト処理、販売処理ができれば、データ処理や保管に関するルールの遵守が簡素化されます。

ただし、一部の認証情報形式には、さらに優れたプライバシー機能を提供する機能が組み込まれています。スキーマの属性領域に基づいて、特定のデータを選択的に共有することを選択できます。

また、特定のデータを共有する必要のない方法で、自分自身に関するデータを証明することもできます。これは「ゼロ知識証明」と呼ばれ、例えば"あなたは18歳以上ですか？"という質問に対し、"はい "か "いいえ "で答えることができます。

派生的な認証情報は、詳細を共有せずに何かを証明するもう一つの方法です。たとえば、ある国に入国する際に健康診断に合格する必要があるとします。このデータは、まず医療提供者によって検証可能な認証情報の形で発行されます。しかし、この認証情報はその後、政府機関によって検証され、今度は検査結果が検証されたことのみを証明する2 番目の認証情報が発行されます。その後、この認証情報を使用して、本人の健康やその他の個人データを一切共有せずに健康を証明できます。

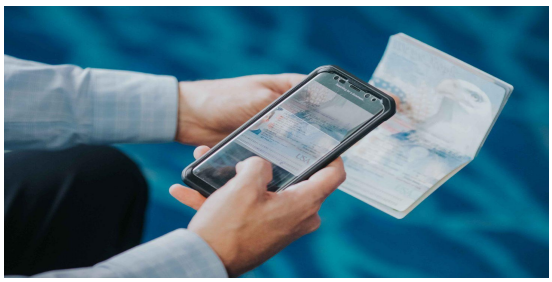
これは、以前の証明のデータからデータのない証明を作成する機能と考えてください。

最後に、一番気になる質問です。携帯電話を紛失したらどうなりますか？

携帯電話を紛失したり、誰かに盗まれたりしたらどうしますか? 生体認証バインディングと生体認証チェックにより、携帯電話とデジタルウォレットアプリを使用しているのが本人であることが確認できます。バックアップはクラウドに保存できます。また、検証可能な資格情報は取り消してすぐに再発行できます。

分散型アイデンティティの実践

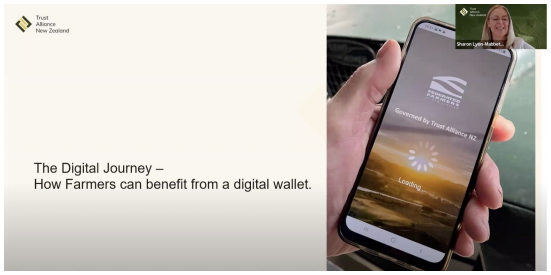
検証可能な資格情報
旅行と観光において



アルバ島 は AHOP (Aruba Happy One Pass) で旅行業界の分散型ID 革命をリードしています。こちらの**ビデオ**をご覧ください。

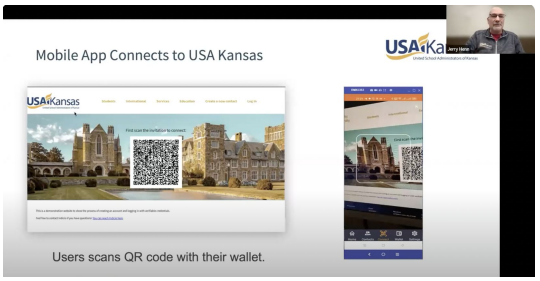
検証可能な資格情報が旅行をどのように変えるか — Indicio Meetup **ディスカッション**

検証可能な資格情報を
農業で



Trust Alliance New Zealandは、検証可能な認証情報によって農家がコンプライアンスと持続可能性の要件を満たすためにデータを管理できる仕組みを説明しています — Indicio Meetup **ディスカッション**

教育における検証可能な資格情報



United School Administrators (USA) Kansas は、検証可能な資格情報がカンザス州全体の学校管理者向けのリーダーシップトレーニングの認定にどのように役立っているか、またマイクロ資格情報と成績証明書を受信者に直接発行して検証できることの利点について説明しています— Indicio Meetup **ディスカッション**

詳細については
そしてどこから始めればよいのか...

この初心者向けガイドが、このテクノロジーが何をするのか、どのように機能するのか、そしてそれがいかに強力で便利なのかを皆さんに理解していただければ幸いです。このガイドでは、その機能と意味を「イメージ」しやすくするために、多くの用語や事柄を省略しています。以下に挙げたリソースや、Hyperledger Foundation、Trust over IP Foundation など、さらに深く掘り下げるためのリソースは数多くあります。結局のところ、このテクノロジーで何ができるのかを知るには、実際に手に取って使ってみるのが一番です。

Indicioの検証可能な ID 、製品により、企業や組織は迅速な意思決定を行い、シームレスなプロセスを実装できるようになります。

アカウント、機器、施設へのアクセスから、ID オーケストレーション、KYC、認証、資格、機器の監視、監査まで、ユースケースは無限大です。

どのように始めるか？

Indicio Proven®: 検証可能な ID とデータが 1 つのすぐに使えるパッケージにまとめられており、迅速に実装して、用途を拡大可能にするために必要な全てのコンポーネントが含まれています。

Holdr+: iOS および Android で利用可能な検証可能な資格情報を保存するためのカスタマイズ可能なデジタル ウォレット。

Indicio Proven Mobile SDK: iOS と Android の両方の既存のアプリ上で検証可能な ID を実現するカスタマイズされたアプリを簡単に開発できるようになりました。

Indicio Network: 開発用の無料の TestNet を備えた、専門的に管理された、グローバルに分散された分散型台帳ネットワーク。

Indicio Academy: 業界に特化した唯一のトレーニングおよび認定プログラム。検証可能なアイデンティティとデータのあらゆる側面に関する包括的な実践コース。

Digital Travel Credential (DTC): ICAO標準に基づく世界初の完全なDTC (デジタル・トラベル・クレデンシャル)。データプライバシーとセキュリティで数々の賞を受賞したDTCは、事前承認チェックインとシームレスな国境通過を数秒で可能にします。どの航空会社や空港システムにも対応できます。

Indicio Open Badges 教育の成果、スキル、承認をデジタルで証明するための世界的に認められた標準を簡単に使用できるようになります。さらに、バッジホルダーがバッジをデジタルウォレットに保管したり、バッジを直接共有したり、バッジ発行者とコミュニケーションしたりできる強力な新機能を追加しました。

こらからお問い合わせください:

Sales@Indicio.tech

メーリングリストに参加してください

無料のデモを入手する

私達と繋がりましょう:

- ニュースレター
- ブログ
- YouTube
- LinkedIn