Hyperledger
FOUNDATION

HYPERLEDGER について

Hyperledger Foundation は、オープンソースのブロックチェーン ソフトウェア技術を中心としたエコシステムを育成することにより、エンタープライズ市場に透明性と効率性をもたらすことを目的として、2015 年に設立されました。Linux Foundation のプロジェクトとして、Hyperledger Foundation は、ブロックチェーン、分散型台帳、および関連テクノロジーを使用したマルチパーティ システム向けのエンタープライズ グレードのプラットフォーム、ライブラリ、ツール、およびソリューションを構築するメンバー組織、非メンバー組織、個人コントリビューター、およびソフトウェア開発者のコミュニティを調整しています。詳細については、**www.hyperledger.org** を参照してください。

TDIDN: 通信業界における パラダイムシフト

このソリューション概要の目的

このソリューション概要では、Telecom Decentralized Identity Network (TDIDN) という画期的な概念を紹介します。これは、分散 ID (DID) とブロックチェーン テクノロジーを使用して ID 管理を改善する新しい方法です。この概要では、TDIDN の革新的なアプローチが通信事業のセキュリティ、効率、プライバシーを向上させる方法について説明します。

対象読者

このソリューション概要の主な対象者は、セキュリティの向上、オーバーヘッドの削減、プライバシーの強化、パートナーや顧客との紛争の軽減に関心のある通信事業者です。

コラボレーション

このソリューション概要は、**Hyperledger Telecom Special Interest Group** によって推進されました。これは、LF Networking とのコラボレーションであり、通信業界におけるブロックチェーン テクノロジーのユースケースを調査する関連プロジェクトです。

V1.0 published April 2024.

本訳文について

この日本語文書は、TDIDN: A Paradigm Shift in Telecom の参考訳として、The Linux Foundation Japan が便宜上提供するものです。英語版と翻訳版の間で齟齬または矛盾がある場合（翻訳版の提供の遅滞による場合を含むがこれに限らない）、英語版が優先されます。この日本語文書を引用する際には、下記の一文を記載してください。
引用：TDIDN: A Paradigm Shift in Telecom 参考訳（The Linux Foundation Japan 提供）

翻訳協力：木下 兼一

概要

TDIDN (Telecom Decentralized Identity Network) は、分散型識別子 (DID) とブロックチェーン技術を活用して通信業界の ID 管理に革命を起こす画期的なソリューションです。このソリューション概要では、TDIDN の可能性と、通信業務におけるセキュリティ、効率、プライバシーを向上させる革新的なアプローチについて説明します。

1. はじめに

通信業界は、現代の世界をつなぎ、デジタル革命を推進する上で極めて重要な役割を果たしています。ただし、この役割には、セキュリティ、オーバーヘッド、プライバシーなど、多くの課題が伴います。

このデジタル変革の時代において、業界はこれらの課題に対応できる革新的なソリューションを緊急に必要としています。

このソリューション概要では、ID 管理を再考することで通信業界に革命をもたらすことが期待される、画期的な概念である Telecom Decentralized Identity Network (TDIDN) について紹介します。

TDIDN は、分散型識別子 (DID) とブロックチェーン テクノロジーを基盤として構築されています。これにより、ユーザーの権限を強化し、運用を合理化しながら、通信分野で ID を管理するための安全で透明性の高い効率的な方法が提供されます。

この概要では、通信業界の現在の ID 管理状況の概要を示し、TDIDN の使用例、コンポーネント、およびユーザーの操作について説明します。これらすべては、TDIDN が通信 ID 管理にパラダイムシフトをもたらす可能性を示しています。

2. 通信業界は多くの課題に直面

通信業界は、革新的なソリューションを必要とする多くの差し迫った課題に直面しています。これらには、次のような重要な問題が含まれます。

2.1 セキュリティに関する懸念

通信ネットワークは、膨大な量の機密データを処理するため、サイバー攻撃やデータ侵害の魅力的なターゲットとなっています。ユーザー名やパスワードなどの従来の認証方法は、ID 窃盗や資格情報ベースの攻撃に対して脆弱です。

実際、Verizon は最近、サイバー犯罪者が組織を攻撃する 2 つの主な方法は、盗まれた資格情報とフィッシングであると報告しています [1]。

2.2 管理オーバーヘッド

個々の通信事業者が、許可されたデバイスとブロックされたデバイスの独自のレジストリを管理すると、各企業の管理負担が大きくなります。このようなサイロ化された取り組みは、非効率性を生み出し、運用の機敏性を妨げ、不要なコストを課します。

2.3 プライバシーの問題

プライバシーに関する懸念が高まっている時代にあって、すべての通信事業者は、ユーザー データを保護し、個人情報を選択的にのみ開示するように努めなければなりません。通信ユーザーは、自分のデータとそれにアクセスできるユーザーをより細かく管理する必要があります。

2.4 課金の透明性

透明性の高い請求プロセスと正確な請求計算は、通信サービス プロバイダーと顧客の間で信頼を構築するために不可欠です。今日の不透明な請求システムは、顧客満足度を損なう紛争につながることがよくあります。

2.5 OTP による脆弱な認証

SMS または電子メールで送信される一時コードに依存する One Time Password (OTP) 認証は、面倒な場合があります。また、OTP はスパムやフィッシングで攻撃される可能性があります。通信業界は、ユーザーを認証するためのより簡単で堅牢な方法を作成する必要があります。

2.6 サービス レベル アグリーメント (SLA) の難しさ

サービス レベル アグリーメント (SLA) は通信サービス プロバイダーの生命線ですが、その管理は煩雑で、紛争が起こりやすい場合があります。

要求されるサービス レベルとそれに伴う違反に対する罰則は、必ずしも明確に定義されていません。実際のサービス レベルの監視は複雑です。サービスのギャップは、発生してからかなり経ってから見落とされたり、特定されたりする可能性があります。

多くの場合、SLA に基づく紛争の解決には数か月かかり、スタッフは膨大な時間を費やし、すべての人に不快感を与えます。

通信業界が直面している多くの課題には、ID 管理の実施方法を再考する革新的で包括的なソリューションが必要です。

3. TDIDN がこれらの課題に対応する方法

TDIDN は、最新で安全な分散型ネットワークを提供することで、これらの課題すべてに対応できます。この革新的なアプローチでは、分散型識別子 (DID) とブロックチェーン テクノロジーを使用して、通信セクターの id 管理に革命を起こします。

ここでは、TDIDN アプローチが上記の通信業界の課題を解決できる 6 つのユースケースを示します。

3.1 分散型 ID によるセキュリティの強化

セキュリティの脅威が増大するにつれて、ユーザー名、パスワード、電話番号などの従来の認証方法では十分ではなくなりました。TDIDN では、安全で分散型の ID ソリューションとして DID を導入しています。

ユーザーは、独自の分散型 ID を提示することで認証を行うことができ、ログイン情報を覚える必要がなくなります。これは、より便利であり、より安全です。また、DID を使用することで、

アイデンティティ盗難や資格情報に基づく攻撃のリスクが大幅に減少します。

3.2 スマート コントラクトによるオーバーヘッドの削減

従来の通信システムは、多数の個別のレジストリに依存しており、その維持には膨大な時間と労力がかかります。TDIDN では、デバイスの International Mobile Equipment Identity (IMEI) 番号と、そのデバイスの所有者と状態 (許可またはブロック) を格納できる分散型台帳またはブロックチェーンが導入されています。

これにより、各通信会社が独自の一意のレジストリを維持する必要がなくなり、オーバーヘッドが削減され、効率が向上します。

TDIDN を使用すると、購入者、法執行機関、保険会社などのユーザーは、デバイスの所有権をすばやく確認し、状態を確認できます。

3.3 プライバシーの保護

データ プライバシーの要求が高まっている時代に、ユーザーは自分の個人情報を管理したいと考えています。TDIDN は、ユーザーが選択的な開示を行うことを可能にします。つまり、ユーザーは、ID の確認や新しいサービスへのサインアップなど、特定の目的のために電話番号や ID をサードパーティと共有できます。

しかし、ユーザーは日常的な取引のたびに自分の身元をすべて開示する必要はなくなりました。この選択的な開示により、プライバシーが促進され、個人データへの不正アクセスのリスクが最小限に抑えられます。

3.4 課金の透明性の強化

通信課金は、競合や顧客の不満の原因になることがよくあります。TDIDN を使用すると、通信事業者は、分散識別子 (DID) を使用して、ブロックチェーン ネットワークに通話詳細レコード (CDR) を安全に格納できます。

スマート コントラクトは、関連するサービス レベル アグリーメント (SLA) の条件に対して各 CDR を自動的に検証します。これにより、安全でコスト効率の高い方法で自動化された、正確で透明性の高い課金が保証されます。これにより、紛争が減少し、実際の使用量に基づいて公正な請求が保証され、サービス プロバイダーと顧客の間の信頼が構築されます。

3.5 認証の強化

OTP 認証は不便で、スパムやフィッシングに対して脆弱な場合があります。TDIDN は、OTP を DID に置き換え、より安全でユーザー フレンドリーな代替手段を提供します。

ユーザーは、DID の所有権を証明することで、自分自身を認証するだけで済みます。これにより、認証プロセスが合理化され、ユーザー エクスペリエンスが向上し、スパム電話や SMS の普及率が低下します。

3.6 スマート コントラクトを使用した SLA の管理

サービス レベル アグリーメント (SLA) の使用は、通信業界では一般的な方法です。しかし、信頼性の高い自動化なしでこれらの契約を管理することは、標準化されたものではありません。

より現代的なアプローチは、スマート コントラクトを使用することです。スマート コントラクトは、

すべての条件がコードで表現された自己実行型のコントラクトです。TDIDN は、スマート コントラクトを使用して、プロバイダーと顧客の間の SLA を管理します。

これらの SLA は、プロバイダーと顧客の両方がいつでもアクセスできる分散型ネットワークに格納され、実行されます。これにより、透明性、不変性、および自動適用が保証されます。

TDIDN によって提供されるコスト効率の高い自動化により、SLA コンプライアンスのリアルタイム監視、違反の自動通知、および合理化された紛争解決のすべてが可能になります。

これらのすべてのユースケースは、提案された TDIDN アーキテクチャが通信業界の差し迫ったニーズを解決できる多くの方法を示しています。

4. TDIDN の 2 つの新しいコンポーネント

TDIDN アーキテクチャには、通信業界の誰もが使い慣れていない 2 つのコンポーネントが含まれています。分散識別子 (DID) とスマート コントラクトです。このセクションでは、各コンポーネントの背景について詳しく説明します。

4.1 Decentralized Identifiers Specifications (DIDs)

分散型 ID 管理システムに対して提案されているアプローチは、Decentralized Identifiers (DID) の概念に基づいています。

DID は、W3C DID 仕様に従ってユーザーごとに生成される一意の識別子です[※2]。W3C Credentials Community Group は、分散型識別子のデータ モデルと構文に関する業界標準を定義するこれらの仕様を管理および監督しています。

DID は、さまざまな分散型台帳およびネットワークと互換性があるように設計されています。これにより、分散型 ID エコシステム内での柔軟性と相互運用性が保証されます。

TDIDN は、Hyperledger Foundation の 2 つの関連プロジェクトを通じて、ブロックチェーンに DID を実装するための包括的なアーキテクチャを提供します。

- **Hyperledger Aries** は、分散型 ID ソリューションを構築するための完全なツールキットを提供します。Aries は、検証可能な資格情報を最大限のプライバシーで発行、保存、提示し、豊富な対話のための機密性の高い継続的な通信チャネルを確立できます。Aries は、基になるブロックチェーン インフラストラクチャにプラグインできるように、ブロックチェーンに依存しないことを目的としています[3]。
- **Hyperledger Indy** は、管理ドメイン、アプリケーション、およびその他のサイロ間で相互運用可能なブロックチェーンに根ざしたデジタル ID をサポートしています[4]。

TDIDN は、これらの両方のオープンソース フレームワークを使用しています。簡単に言うと、Aries はシステムのクライアント側を構築するためのツールであり、Indy はデータベースをサポートするサーバー側と考えることができます。

つまり、Aries は、Indy によって提供される基になる DID ブロックチェーンに対して読み取りと書き込みを行う、分散型 ID アプリケーションのエージェント側を提供します。

DID は、DID ドキュメントをアドレス指定し、DID リゾルバーによる解決を可能にする汎用 URL 形式によって特徴づけられます。この汎用形式は、仕様 RFC3986 で定義されている URI スキームの一般的な原則に準拠しています [5]。

すべての有効な DID には、次の 3 つの必須フィールドが含まれています。

1. urn スキーム (この例では「*did*」)
2. 名前空間またはメソッド名 (選択した DID メソッドに応じて「*ethr*」、「*sov*」など)
3. メソッド固有の ID。DID を一意に識別する文字と数字の組み合わせにすることができます。

フィールドはコロン (:) で区切られます。たとえば、TDIDN システムの完全な DID は、「*did:example:12345AbCDEfgh*」のようになります。

4.2 スマート コントラクト

スマート コントラクトは、買い手と売り手の間の契約条件がすべてコードに直接書き込まれているため、人間の介入なしに実行できます。

Ethereum やその他の一般的なブロックチェーン ネットワークのような公開台帳は、スマート コントラクトをデプロイするための安全で透過的な環境を提供します。これらのブロックチェーンは、コントラクトのコードと実行履歴をすべての参加者が確認できるようにします。これにより、買い手と売り手の間の信頼と説明責任が強化されます。

また、公開台帳は分散型のコンセンサスメカニズムを提供し、スマート コントラクトの実行が改ざんされにくく、信頼性が高いことを保証します。

TDIDN アーキテクチャでは、DID または Ethereum アドレスによるアクセス制限によってプライバシーを維持しながら、透明性とアクセシビリティのために公開台帳を使用します。

5. TDIDN システムの概要

このセクションでは、TDIDN アーキテクチャの主要部分の概要について説明します。図 1 は、TDIDN システムの簡単なブロック図を示しています。図 2 は、モバイル ユーザーとスマートフォンのブロック図を示しています。

5.1 TDIDN ネットワーク

図 1 に示すように、ネットワークの基盤は 3 つのブロックチェーン (分散型台帳とも呼ばれます) にあります。各ブロックチェーンの目的は異なります。

- モバイルデバイスの IMEI 番号の管理
- 課金のためのコール詳細レコード (CDR) の録音
- Hyperledger Indy を使用した DID の追跡

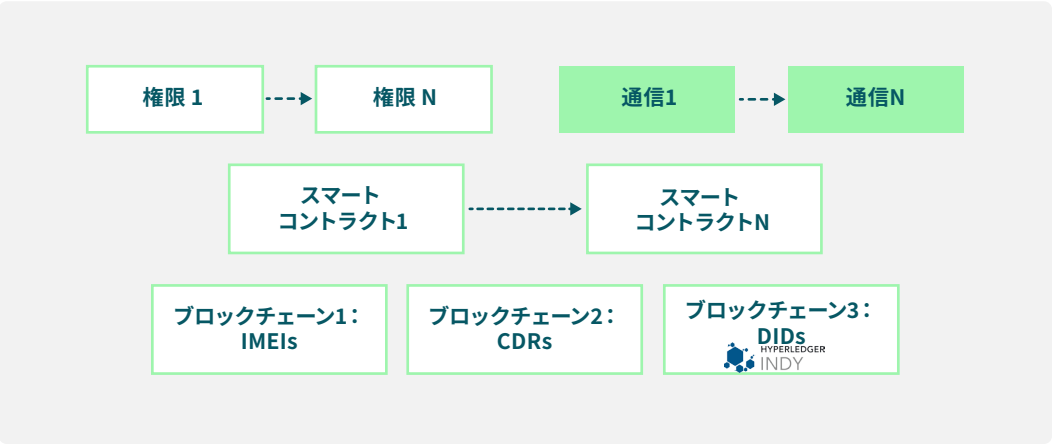


図1：TDIDN ブロック図

TDIDN の参照インスタンスでは、IMEI と CDR の両方のブロックチェーンで sepolia テストネットが使用されます。Sepolia は、開発者がスマート コントラクトをデプロイおよびテストするための安定したインフラストラクチャを提供する Ethereum テストネットです。

DID ブロックチェーンでは、Linux Foundation のオープンソース プロジェクトである Hyperledger Indy を使用します。これにより、ID 管理に最適なパブリックで許可されたブロックチェーンが提供されます。

TDIDN のこのインスタンスの 3 つのブロックチェーンはすべて無料で利用できます。

これらのブロックチェーンは、これら 3 つの台帳を更新する分散型の方法を提供します。つまり、各通信事業者は、独自のサイロ化されたデータベースの管理に費やしていた時間と労力を節約できます。

必要に応じて、有効な機関はブロックチェーンにデータを書き込むことができます。ネットワークは、それぞれが検証されている限り、無制限の数 (N) の機関をサポートできます。機関は、ネットワークの他のすべてのメンバーによって信頼されている任意の通信事業者またはサードパーティです。

5.2 通信事業者

図 1 の紫色に示すように、通信事業者はネットワークの主要なユーザーです。ネットワークは、無制限の数 (N) の通信会社をサポートできます。

ある通信事業者と別の通信事業者との間のビジネス契約は、SLA や通信事業者間の請求などの詳細を説明するスマート コントラクトによって管理されます。各スマート コントラクトは、必要に応じてブロックチェーン データにアクセスして更新できます。また、ネットワークは無制限の数 (N) のスマート コントラクトをサポートできます。

前に説明したように、ブロックチェーンは、通信事業者が IMEI と CDR のために独自のデータベースを維持するための大きなコストを節約します。また、スマート コントラクトは、インテリジェントな自動化の新しい時代の到来を告げるものです。

これらの 2 つの革新により、通信事業者は、これまで以上に安全でコスト効率の高い方法でデバイスを管理できます。

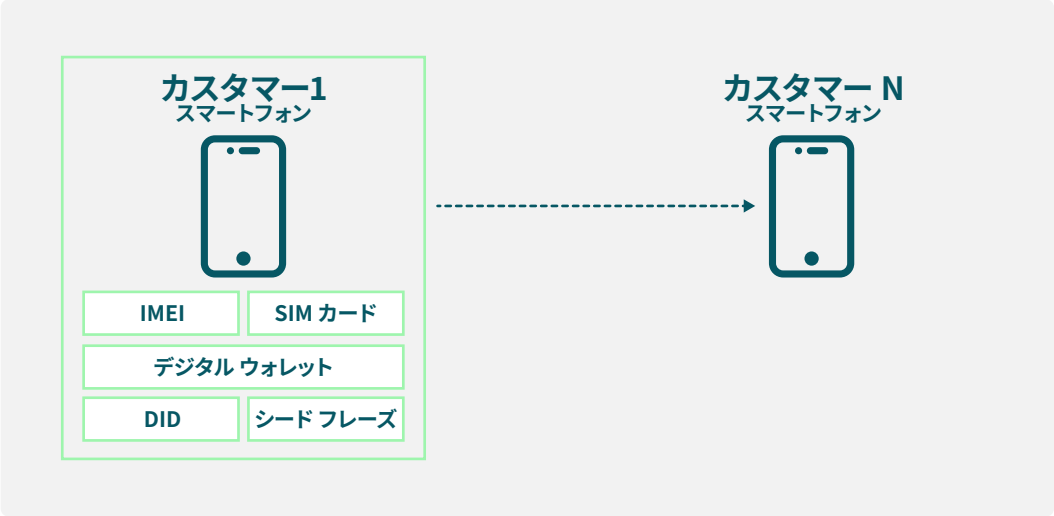


図2：モバイルカスタマー ブロック図

5.3 モバイル カスタマー

図 2 に示すように、モバイル デバイスを所有する各ユーザーは、そのデバイスの一意の IMEI 番号と SIM カードを通信サービス プロバイダーから受け取ります。

これは現在のプラクティスに似ています。唯一の違いは、これらのアイテムが 2 つの分散型ブロックチェーンによって管理されるようになったことです。このブロックチェーンは、ネットワークの任意のメンバが表示できます。

各ユーザーは、一意の DID と一意のシード フレーズを含むデジタル ウォレットも所有します。DID は、電話番号とデバイスのステータスを検証するために使用できます。シード フレーズは、デバイスが紛失、譲渡、または盗難された場合にデバイスのステータスを更新するために使用できます。

ネットワークは、無制限の数 (N) のモバイル カスタマーをサポートできます。

6. TDIDN アーキテクチャの主な機能

図 3 は、ネットワークの多くの機能のプロセス フローを示しています。このセクションでは、TDIDN アーキテクチャの 4 つの主要な機能について説明します。

- システムにアクセスする準備をしているユーザー
- IMEI 番号の管理
- SIM カードの管理
- CDR の処理

ご覧のように、TDIDN アプローチは、通信事業者の IMEIs と Sim の割り当て、検証、管理を大幅に効率化します。

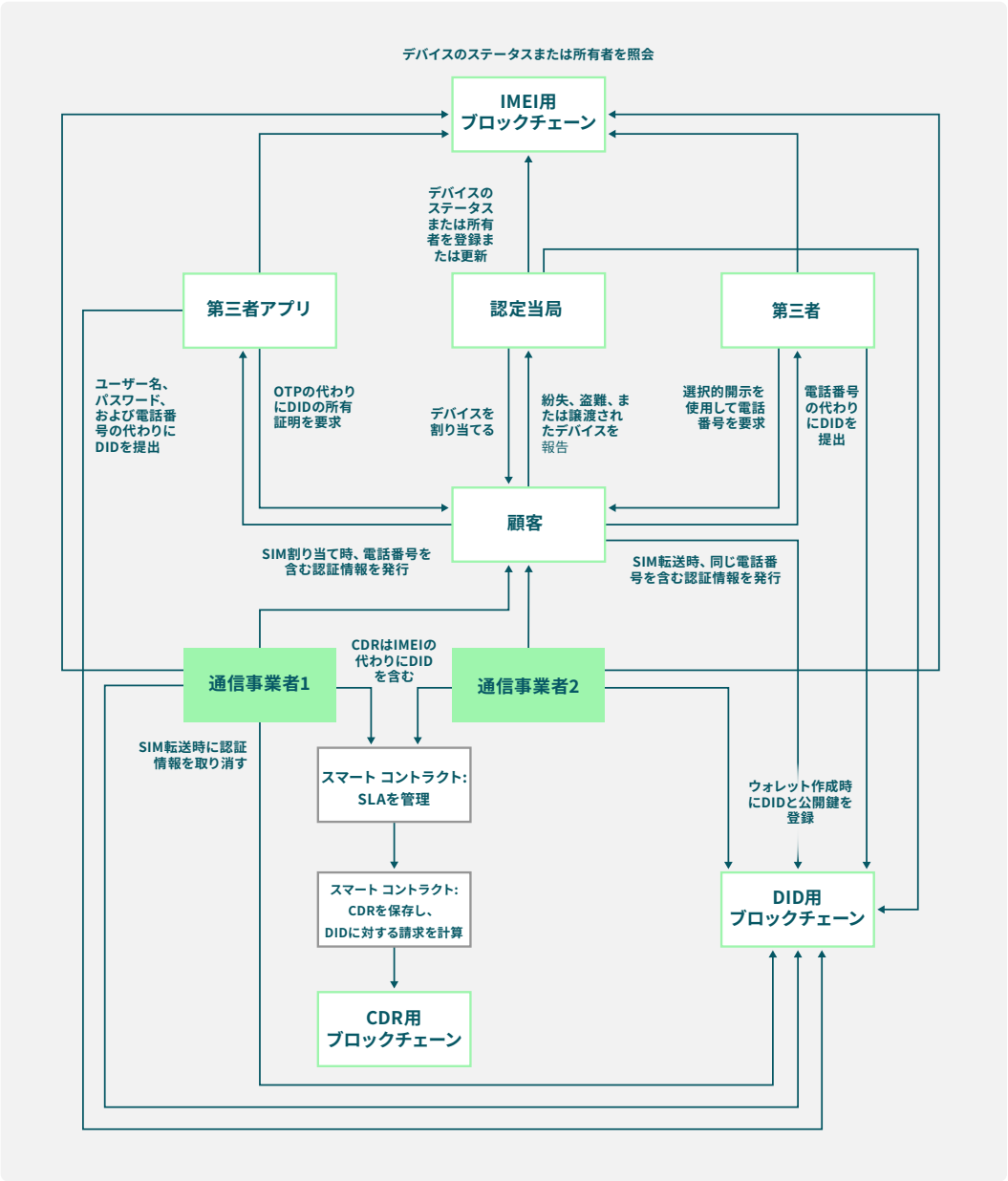


図3:TDIDN プロトコル フロー

6.1 準備

ユーザーは、TDIDN にアクセスする前に、次の 3 つの基本タスクを実行する必要があります。

ウォレット アプリのダウンロード

ユーザーは、推奨されるデジタル ウォレット アプリをデバイスにダウンロードしてインストールする必要があります 。

ユーザー アカウントの作成

ユーザーはウォレット アプリでアカウントを作成する必要があります。これには、ユーザーの ID と場所を検証するための個人情報の入力が含まれます。

シード フレーズの安全な保管

新しいアカウントが作成されると、ユーザーにシード フレーズが提供されます。ユーザーは、このシード フレーズを安全に保存する必要があります。暗号化キーを生成し、DID の制御を維持するために必要になります。

6.2 IMEI 番号の管理

ご存知のように、IMEI は世界中のすべての携帯電話に割り当てられた一意の 15 桁のシリアル番号です。TDIDN は、新しい IMEI を割り当て、ユーザーの DID にマップし、要求に応じてデバイスの状態 (許可またはブロック) を変更できます。

ユーザーによる IMEI 番号の要求

ユーザーは、DID を指定し、機関に IMEI 番号を要求することで、プロセスを開始します。

機関による IMEI の DID へのマッピング

承認された機関は、ランダムな IMEI 番号を生成し、ユーザーの DID にマッピングします。このマッピングは、デバイスの状態 (割り当てられた IMEI が許可されているかブロックされているか) を含む IMEI 分散台帳 (ブロックチェーン) に公開されます。

ユーザーからのステータス変更要求

ユーザーが携帯電話を紛失、譲渡、または盗難にあった場合、そのユーザーは通常、そのデバイスのネットワーク アクセスを停止し支払いを中止することを望むでしょう。 この場合、ユーザーは特定の IMEI 番号のステータス (許可またはブロック) を変更するように機関に要求できます。ユーザーは、シード フレーズを使用して別のデバイスでウォレット アプリを開くことによって、その IMEI に関連付けられている DID を所有していることを証明する必要があります。

機関による IMEI のステータスの更新

機関は、ユーザーの要求と DID の所有権を確認します。要求が適切に確認されると、機関は IMEI ブロックチェーン内の IMEI 番号のステータスを更新し、ブロックまたは許可のマークを付けます。

6.3 SIM カードの管理

ご存知のように、SIM カードはモバイル デバイスを特定の通信サービス プロバイダーにリンクする小さなスマートカードです。TDIDN は、新しい SIM カードの割り当て、SIM カードの更新または更新、およびサードパーティによるユーザーの電話番号の検証をサポートできます。

ユーザーからの SIM カード要求

ユーザーは、DID と承認された政府 ID 資格情報を入力して、通信当局に SIM カードを要求することによってプロセスを開始します。

当局が資格情報を検証し、SIM を発行します

通信当局は、ユーザーのデジタル ウォレットに格納されている政府 ID 資格情報の有効性を確認します。

資格情報が適切に検証されると、通信当局は SIM カードを発行し、ユーザーの新しいデジタル資格情報を生成します。この資格情報には、電話番号、オペレーター名、その他の詳細などの情報が含まれています。

当局による SIM の再発行または更新

通信当局は、TDIDN システムを使用して SIM を再発行または更新することもできます。これにより、ユーザーの ID が検証され、セキュリティで保護されます。

たとえば、ユーザーが電話を他のユーザーに売却したり、下取りに出したりした場合、通信当局は元の所有者の資格情報を取り消し、同じデバイス IMEI にリンクされた新しい所有者の新しい資格情報を発行できます。

ユーザーが電話を紛失したり盗まれたりした場合、当局はそのデバイスの状態を変更して、ブロックしたデバイスとして登録することができます。

ユーザー自身の電話番号であることの証明

ユーザーは、銀行、政府機関、サービス プロバイダーなどの第三者、またはサービス プロバイダーのサードパーティ アプリケーションに対して、自分の電話番号を所有していることを証明する必要がある場合があります。この場合、ユーザーはデジタル認証情報を提示できます。

サードパーティまたはアプリケーションは、実際の電話番号を知らなくても、認証情報の信頼性を確認できます。この選択的開示により、ユーザーのプライバシーが保護され、トランザクションのセキュリティが強化されます。

6.4 CDR の処理

コール詳細記録（CDR）は、すべてのモバイル デバイスによって行われた通話ごとに作成されることはよく知られています。CDR は、通話の時間、通話の長さ、発信元の名前と番号、発信先の名前と番号、および通話の完了ステータスや通話終了の理由などの品質および診断データを含む、各通話に関するすべての関連データを記録します。

現在、各 CDR はデータベースに記録され、通話を発信した通信事業者によって管理されます。その後、CDR は、元の通信事業者と関連する他の通信事業者との間の関連コストを、それらの通信事業者間で設定されている SLA に従って決済するために使用されます。

CDR を処理し、不一致や紛争を解決するための自動化と高度化のレベルは、通信事業者によって異なります。しかし、どの通信事業者も、CDR データベースの維持、請求書の計算、他の通信事業者との紛争の解決に多大なリソースを費やしています。

TDIDN は、紛争を減らすために、より透明で正確な方法で CDR を処理できます。TDIDN は、CDR の記録、通信事業者間の SLA の管理、CDR からの請求書の計算を行うことができます。

CDR の記録

顧客が電話をかけると、現地のオペレーターによって CDR が作成されます。通話は IMEI ではなく DID によって識別されます。各 CDR は不変のブロックチェーンに記録され、有効な機関はそのレコードを表示できますが、変更することはできません。これにより、CDR の精度と透明性が向上します。

SLA の管理

オペレーターが別のオペレーターと SLA に合意すると、すべての条件が CDR 台帳にアクセスできるスマート コントラクトにコード化されます。SLA を表示するために、オペレーターは関連するオペレーターとの関連するスマート コントラクトを表示できます。SLA を再交渉するために、関連するオペレーターは契約を再交渉し、関連するスマート コントラクトを更新できます。

請求書の計算

顧客契約のすべての契約条件も、スマート コントラクトにコード化されます。

顧客の請求書を作成するために、スマート コントラクトは DID を使用して関連するすべての CDR を検索し、関連する契約条件に従って各通話の請求書を計算します。次に、顧客への請求に必要なすべての情報をまとめ、そのデータをオペレーターの請求システムにエクスポートします。

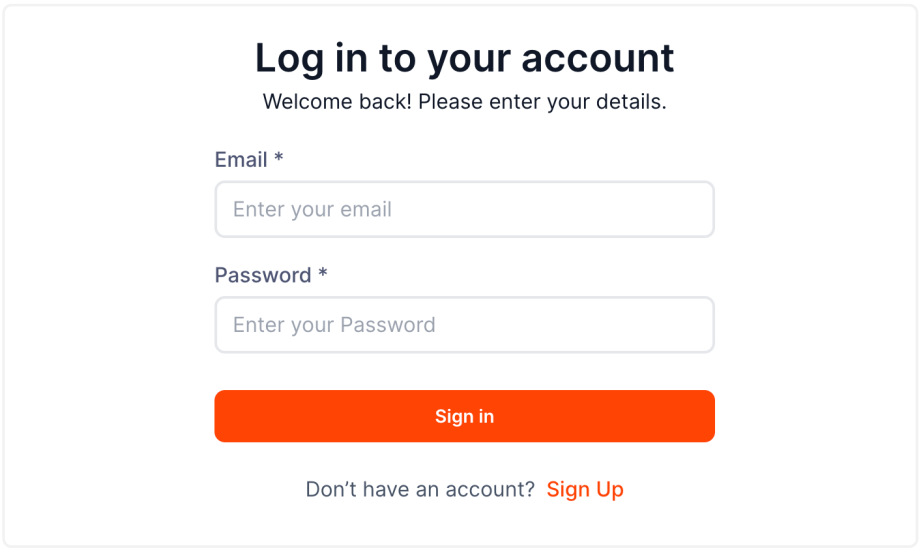
別のオペレーターの請求書を計算するために、スマート コントラクトは関連するすべての CDR を検索し、関連する契約条件に従って未払い額を計算します。関連するオペレーターのスマート コントラクトは、必要に応じて請求書を自動的に支払うように設定できます。各トランザクションはブロックチェーンに記録されます。

7. 提案されたユーザー インターフェイス

このセクションでは、現在存在する TDIDN のリファレンス インスタンスのユーザー インターフェイスについて説明します。このコードは、Hyperledger Telecom SIG を通じてオープンソースとして入手できます。このシステムでは MetaMask Web ウォレットを使用しますが、Ethereum ネットワーク経由でトランザクションに署名して送信できる他のデジタル ウォレットをサポートできます。

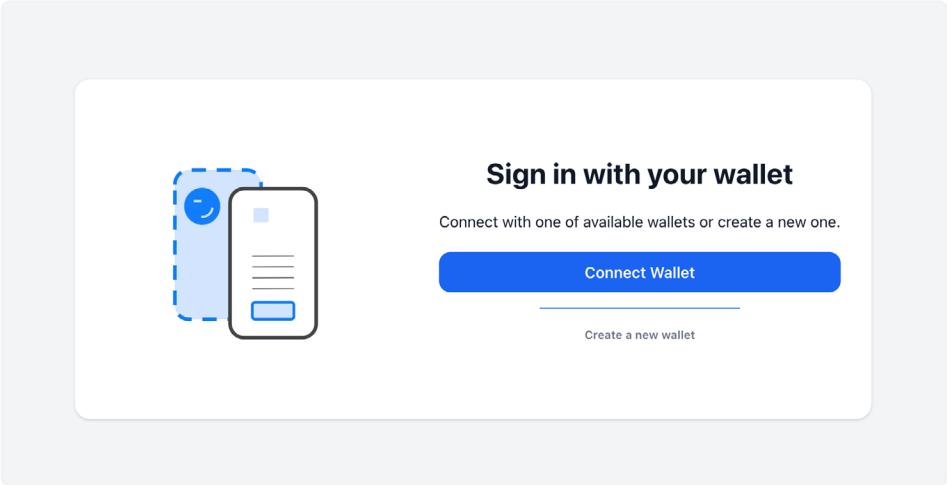
7.1 ウォレット アカウントの作成

ユーザーは、Web ウォレットを登録して作成できます。この Web ウォレットを使用すると、クレデンシャルを安全に保存および確認し、DID を管理できます。



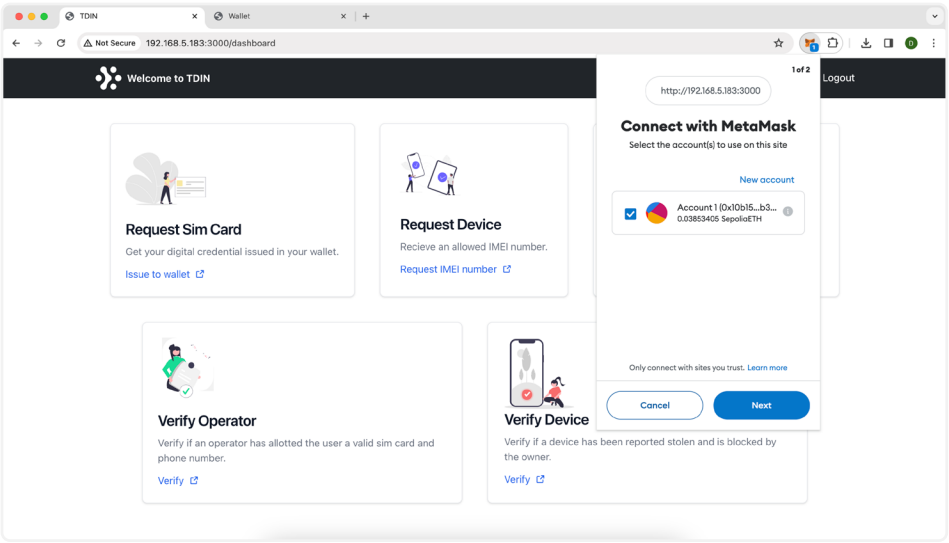
7.2 アプリケーションへのログイン

ログイン時に、ユーザーは TDIDN への認証にユーザー名とパスワードの代わりに DID を使用できます。



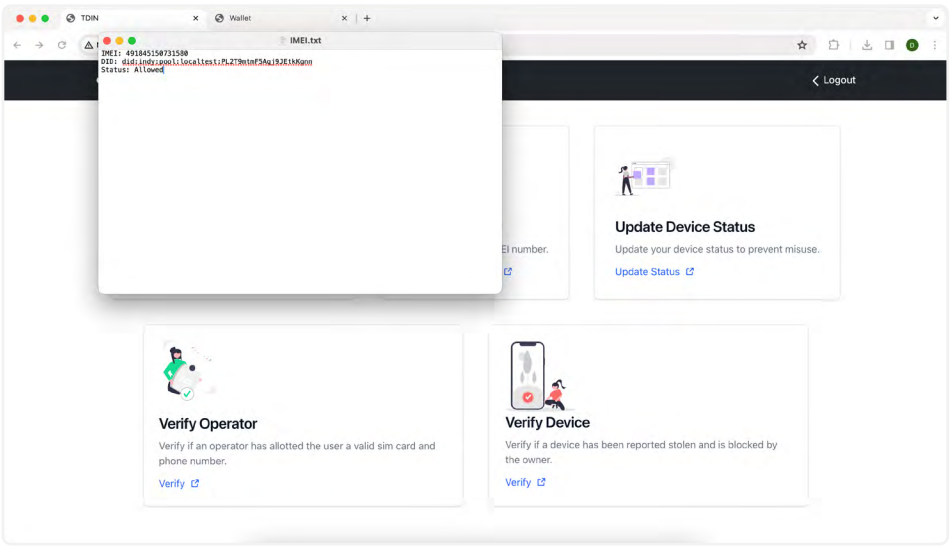
7.3 ウォレットを接続してトランザクションを有効にします

TDIDN サービスにログインすると、ユーザーは Metamask ウォレットを接続して Ethereum testnet ブロックチェーン (具体的には Sophia ネットワーク) でのトランザクションを有効にするように求められます。



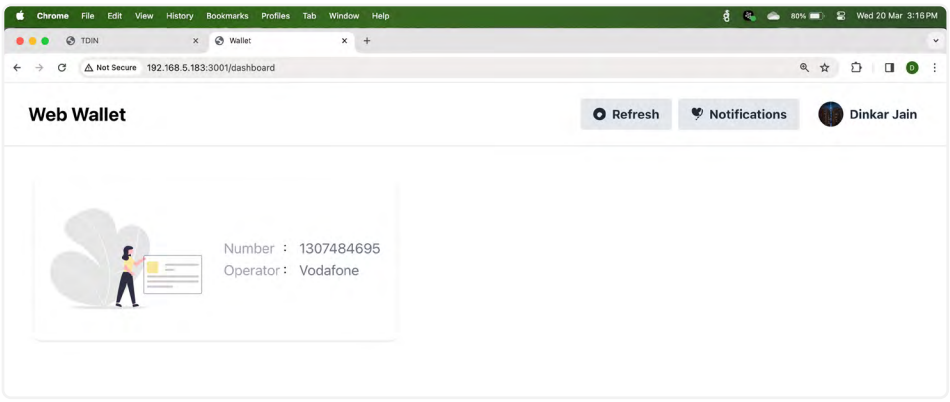
7.4 IMEI 番号の要求

ユーザーは、[Request IMEI Number] ボタンをクリックして IMEI 番号を生成できます。生成された IMEI 番号はそのユーザーに関連付けられ、IMEI ブロックチェーンに保存されます。



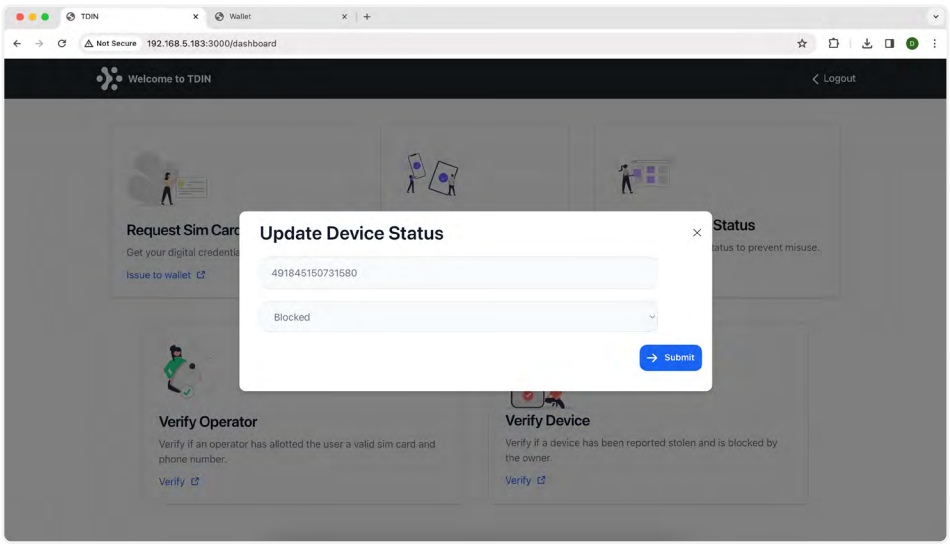
7.5 SIM カードの要求

ユーザーは、「Issue to Wallet」ボタンをクリックすることで、SIM カードを要求し、検証可能な資格情報をウォレットで受け取ることができます。



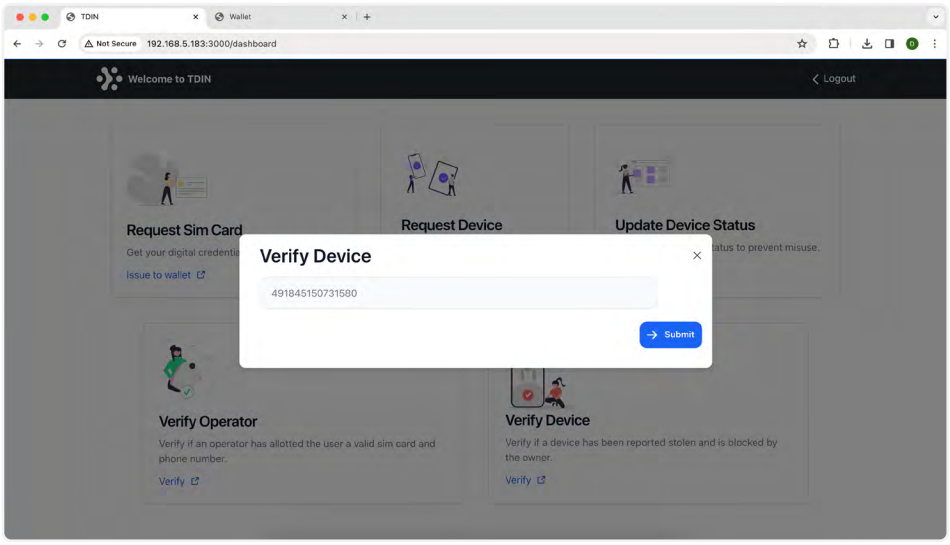
7.6 デバイスのステータスの更新

ユーザーのデバイスが紛失または盗難された場合、ユーザーは「デバイス ステータスの更新」機能を使用して、台帳上のデバイスのステータスを変更できます。



7.7 第三者によるデバイスのステータスの確認

第三者は、「デバイスの確認」機能を使用して IMEI ブロックチェーン上の IMEI 番号を表示することで、モバイル デバイスのステータスを確認できます。第三者は、「オペレーターの確認」機能を使用して、検証可能な資格情報を検証することもできます。



8. 結論

このソリューション概要では、通信事業者による ID 管理の重要な一歩として TDIDN アーキテクチャを紹介します。TDIDN は、分散型識別子 (DID) とブロックチェーン テクノロジーを使用して ID 管理を合理化します。

このソリューション概要では、通信事業者による ID 管理の重要な一歩として TDIDN アーキテクチャを紹介します。TDIDN は、分散型識別子 (DID) とブロックチェーン テクノロジーを使用して ID 管理を合理化します。

謝辞

Hyperledger Telecom Special Interest Group は、このソリューションの概要に貢献した次の方々に感謝します。
David Boswell, Dinkar Jain, Vipin Rathi

参加方法

Hyperledger Telecom Special Interest Group は、通信業界におけるブロックチェーン テクノロジーの適切なユースケースに関する技術レベルおよびビジネス レベルの会話に重点を置いています。SIG は世界中のすべてのユーザーに開かれています。

詳細については、**wiki.hyperledger.org/TCSIG** を参照してください *。

* 訳注　2023 年秋より以下の Web サイト：
https://lf-hyperledger.atlassian.net/wiki/spaces/TCSIG/overview

TDIDN リファレンス アプリケーションのリポジトリとドキュメントをダウンロードするには、**https://github.com/hyperledger-labs/TDIDN** を参照してください。

出典

1 C. David Hylender, Philippe Langlois, Alex Pinto, and Suzanne Widup, “Verizon 2023 Data Breach Investigation Report,” May 2023, page 8. **https://www.verizon.com/business/resources/reports/dbir/**

2 “Decentralized Identifiers (DIDs) v1.0,” 19 July 2022, World Wide Web Consortium (W3C). **https://www.w3.org/TR/did-core/**

3 Hyperledger Aries, Hyperledger Foundation. **https://www.hyperledger.org/projects/aries**

4 Hyperledger Indy, Hyperledger Foundation. **https://wiki.hyperledger.org/display/indy/Hyperledger+Indy**

5 Tim Berners-Lee et al, “Uniform Resource Identifier (URI): Generic Syntax,” The Internet Society, 2005. **https://datatracker.ietf.org/doc/html/rfc3986**