WORLDCOIN

プライバシー
を考慮した設計

目次

エコシステム 3

AI時代のプライバシー 4

Worldcoinプライバシー原則 5

原則 1 セキュリティ: 数学的に保護された安全性 7

原則 2 匿名性: オンラインで自由に活動できる 8

セキュア・マルチパーティ・コンピュテーション（SMPC） 8

ゼロ知識証明 (ZKP) 10

原則 3 選択とコントロール: 自分のデータは自分で管理 12

データの最小化 12

パーソナルカストディ(個人情報の自己管理機能) 13

顔認証 13

原則 4 透明性: 開かれた環境での設計 15

監査 15

オープンソースとパーミッションレス 15

エコシステム

Worldcoinプロジェクトは、様々な参加者やツールによって構成されており、オンラインでの取引やコミュニケーションにおいて信頼性を最重視した、人間を第一に考えたIDのネットワークを構築しています。

Worldcoinは、匿名のデジタルパスポートであるWorld IDとデジタル資産の利用を可能にするネットワークで構成されたプロジェクトであり、世界中の何十億もの人々に対して、グローバルのデジタル経済へのアクセスを提供します。

World IDは、自分が唯一無二の人間であることを証明するための分散型アイデンティティプロトコルです。動画を認証してディープフェイクの防止するなど、さまざまなオンライン活動において、World IDを使用して自分が人間であることを証明できます。また、「Google でログイン」に似た形で、名前やメールアドレス、電話番号などの個人データを共有せずに、ウェブサイトやアプリへのログインにも利用できます。

World Chainは、イーサリアムネットワーク上にまもなくローンチされるレイヤー2ロールアップであり、World IDを活用して、ボットよりも人間のためのトランザクションを優先させます。

WLDは、Worldcoinトークンであり、Worldcoinネットワークに参加している人間に無償で提供されます。[1]

Worldcoin財団は、Worldcoinプロトコルの管理者として機能する非営利団体です。また、Orbの知的財産やプロトコルのオープンソース技術など、Worldcoinブランドに関連するほとんどの資産を所有または管理しています。

Tools for Humanity (TFH)は、WorldcoinのためにOrbやWorld Appなどのツールを開発するテクノロジー企業です。

Orbは、ユーザーが唯一無二の人間であることを認証するための特別なカメラで、World IDを使用して自分が人間であること証明するためのデータを提供します。

World Appは、World IDの基盤となる、Worldcoinの自己管理型のウォレットです。このアプリを使用して、Worldcoinトークンやその他のデジタル資産の送受信も可能です。

詳細はこちらをご覧ください: Worldcoinとは何か、どのように機能するのか?

[1] 利用可能な法域において

AI時代のプライバシー

欧州連合（EU）の法執行機関であるユーロポールが2022年に発表した報告書では、2026年までにインターネット上のコンテンツの最大90%が人工的に生成される可能性が示唆されています。

なりすまし、スパムボット、ディープフェイク、個人情報の盗難、偽情報の拡散など、インターネットは危険な場所になり得る可能性があります。AIの進歩により、インターネットはこれまで以上に便利になる一方で、既存の問題がさらに深刻化するリスクについても慎重に考える必要があります。私たちは、人間同士でのなりすましが引き起こす問題を見てきましたが、もし相手がAIによるなりすましだったらどうなるでしょうか?

私たちには、オンライン上で話したり、送金したり、コンテンツを見たりしている相手が、実際に人間であることを確認できる手段が必要です。Worldcoinは、AI時代において、人々がこれらの確認を自らの手で行えるようにすることを目指しています。

AIがインターネット上で偽の人間（ボット）を大量に作り出してしまうことを防ぐためには、高度なセキュリティが不可欠です。しかし、多くの対策はプライバシーを犠牲にする傾向があります。企業や政府による監視に利用される可能性のある従来の身分証明書や認証技術に頼らざるを得ない現状も、その一例です。果たして、プライバシーを犠牲にして得られるものは何なのでしょうか。

私たちは、より良い方法があると信じています。Worldcoinプロジェクトは、人間を最優先に考えた安全な技術を提供し、プライバシーを守りながら、オンライン体験をより信頼できるものにすることを目指しています。

Worldcoinは、**プライバシーを重視した**設計で運営されています。

AIがプライバシーに与えるリスク

すでに、政治家や有名人のディープフェイクが多く流通しています。これは、インターネット上に彼らの膨大なコンテンツが存在することが原因です。

しかし、AIの進化により、今後は一般の人々を模倣した非常にリアルな映像や音声によるディープフェイクの使用が懸念されています。インターネットやその利用者が、AIがもたらす課題に対して十分な準備ができていない現状は特に懸念すべき事態です。たとえば、実際には同僚や家族ではない相手とZoomで通話していたらどうでしょうか。人々は簡単に騙されて送金したり、秘密を漏らしたり、さらには予測もつかない事態に巻き込まれる可能性があります。

AIの悪用を防ぐためには、プラットフォーム側が、利用者が実在する人間であることを確認できる仕組みが必要です。従来の「CAPTCHA」のようなツールはもはや効果的ではなく、インターネット上の行動履歴に紐づくデータに依存しています。World IDは、CAPTCHAに代わるプライバシー保護型のソリューションであり、個人情報を公開することなく、デジタルIDシステムや本人確認手続き(KYC)の代替として機能します。

Worldcoinプライバシー原則

Worldcoinコミュニティは、これまでに例のないものを構築しています。それは、グローバルに信頼され、最大限にインクルーシブで、プライバシーを守りながら「人間であること」を証明できるネットワークです。特に、このプロジェクトのプライバシーに対するアプローチは、従来のものとは異なり、どの企業、組織、政府も採用していない、全く新しい革新的な方法を提示しています。

Worldcoinは、あなたが誰であるかを知りたいのではなく、ただあなたが唯一無二の人間であることを確認したいのです。

AIを活用したボットがさらに広がり、その精度が高まる中、オンラインでの信頼性が低下し、人間を装うケースが増えています。そのため、相手が人間かボットかを見分けることが、ますます重要になっています。もし、オンラインでの身分証明が唯一の課題であれば、解決策は比較的単純に思えるかもしれません。つまり、政府発行のIDを使って私たちの身元を認証し、それをオンライン上でも活用することです。実際、銀行では度々IDの提示が求められます。オンライン上での取引全般も、AI時代においては銀行の取引と同じくらい機密性が高くあるべきではないでしょうか?

しかし、世界で約8億5千万人が公的な身分証明書を持っていないことや、政府自体がオンラインで偽情報キャンペーンを展開している事例を考慮すると、政府発行のIDによるオンライン認証が万能な解決策とは言えません。政府発行のIDは、自分の住所などの必要以上の情報を公開することで、個人情報が盗まれるリスクや、AIに悪用されるリスクに晒される可能性があります。

私たちは、できるだけ多くの人が使いやすく、かつプライバシーを保護した「人間である証明」が必要です。

「これまで、オンラインで人間性を証明する手段として、政府発行のIDなどが使用されてきましたが、これにはユーザーの特定や、不要な個人情報の公開といったデメリットが伴っていました。それに対して、World IDは匿名で『唯一無二の人間であることの証明』を提供し、『監視資本主義』モデルに対抗しながら、データ保護を促進する新たなモデルを提案しています。これにより、World IDはデータ保護を重視したオンライン活動の機会を促進します。」

ー ステファン・ブリンク博士（2017年1月から2022年12月まで、ドイツ・バーデン＝ヴュルテンベルク州のデータ保護および情報の自由に関する前州委員）

これがWorldcoinが解決しようとしている課題であり、World IDを通じて実現しています。World IDは、個人のスマートフォンに保存されるグローバルなデジタルパスポートで、個人情報を共有せずに唯一無二の存在であることを証明できます。

World IDは、インターネット上で「人間であること」を認証するシステムであり、利用者はどこにいても匿名性を保つことができます。認証されたWorld IDは、名前やメールアドレス、ウォレットの取引データなどの個人情報と関連付けられることはなく、誰がそのIDを使用しているのかも明らかにしません。Worldcoinはデータ最小化の理念に基づいて設計されており、個人情報は保存されません。

さらに、World IDは各アプリでの利用情報がトラッキングされることなく、複数の異なるアプリ間で使用することができます。利用履歴を収集する中央のデータベースも存在しないため、どれだけ多くのアプリでWorld IDを使用しても、アプリ同士が連携することもなく、World ID自体もアプリについて知ることはありません。

Worldcoinは、プライバシーを重視して設計されており、4つの相互に作用するプライバシー原則に基づいています。

原則 1

セキュリティ: 数学的に保護された安全性

原則 2

匿名性: オンラインで自由に活動できる

原則 3

選択とコントロール: 自分のデータは自分で管

原則 4

透明性: 開かれた環境での設計

原則 1

セキュリティ: 数学的に保護された安全性

セキュリティなしにプライバシーは成立しません。

Worldcoinは、人々がオンラインで個人情報を開示することなく利用でき、ボットと人間を区別できることを目指しています。セキュリティは、そのプライバシーを確実に守るために不可欠な要素です。

World IDは、利用者のデータセキュリティを強固にするため、さまざまなセキュリティ技術を採用しています。

まず、オープンソース化や監査（透明性を参照）などの人為的な手段により、Worldcoinプロジェクトにおけるセキュリティ対策が検証され、ストレステストが実施されています。

次に、ゼロ知識証明（ZKP）やセキュア・マルチパーティ・コンピュテーション（SMPC）といった暗号技術を使用し、高度な数学に基づいてデータを保護し、暗号化、プライバシーの確保、そして匿名化を実現しています。

SMPCは完全な秘密保持を提供する数少ない暗号技術の一つです。また、ZKPはアプリケーションごとに固有のヌリファイアハッシュを使用することで、ユーザーの利用履歴を追跡されるリスクを防ぎます。

まさに、これこそが**数学的に保護されたセキュリティ**なのです。

原則 2

?

しかし、ウェブサイトやアプリを利用する際に、料理をする時以上に個人データを提供する必要はないはずです。人々はインターネット上で自由に活動できるべきです。

匿名性: オンラインで自由に活動できる

多くの場合、私たちは日常生活において身元を証明する必要はありません。例えば、夕食を作ったり、本を読んだり、眠ったりする際に、自分が誰であるかを証明することはほとんど求められません。私たちの行動は、通常、気づかれることも、観察されることも、記録されることもないため、匿名でいることができるのです。

しかし、オンラインでは匿名性を保つことが難しくなります。ウェブサイトは私たちの活動を監視し、ブラウザは私たちのオンラインの行動を追跡することができます。この監視は、IPアドレスのモニタリングから、政府発行のID認証を求められるような場合まで、個人のプライバシーに大きな影響を与える可能性があります。

とはいえ、ウェブサイトやアプリを利用する際に、私たちのデータを提供する必要は必ずしもありません。人々は、**誰にも追跡されずにオンラインで自由に活動**できるべきです。World IDを使ってサイトにログインすることで、それが可能になります。

Worldcoinは、オンラインでの匿名性を維持するために、秘密分散計算（SMPC）やゼロ知識証明（ZKP）など、さまざまなプライバシー保護技術を採用しています。

セキュア・マルチパーティ・コンピュテーション（SMPC）

World IDの作成にはスマートフォンがあれば十分ですが、利用者が複数のWorld IDを作成していないことを確認しつつ、その人物のプライバシーを守ることは、複雑な課題です。

適切に匿名化された生体認証データが、この課題に対する解決策を提供します。しかし、生体認証データの有用性が高いからこそ、最小限の収集と利用に留める必要があります。そして、これが唯一の実行可能な方法である場合には、慎重な取り扱いが求められます。

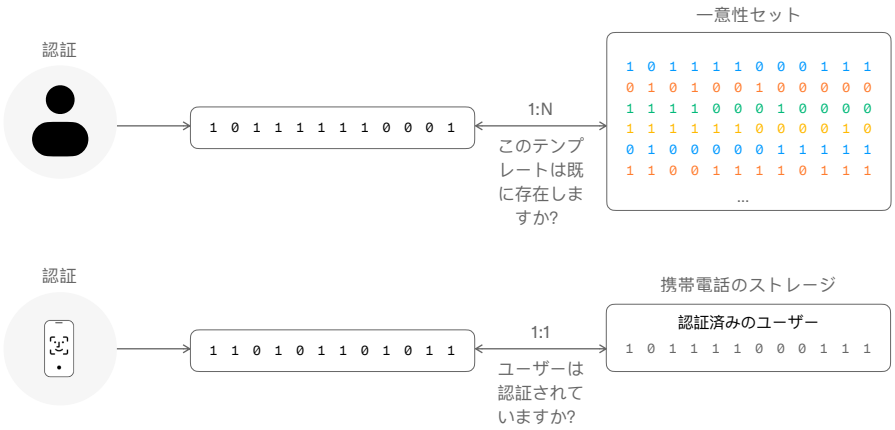
Worldcoinは、この課題をSMPC（セキュア・マルチパーティ・コンピュテーション）技術で解決しています。

Orbを通じてWorld IDを認証する際、Orbは虹彩と顔の写真を撮影し、それを基に虹彩コードを生成します。この虹彩コードは1と0の組み合わせであり、2つとして同じものは存在しません。また、名前や性別、年齢などの直接的な個人情報は一切含まれません。

生成された虹彩コードは複数に分割され、SMPCを使用して永久に暗号化されます。SMPCは、データを複数の抽象化された値（SMPCシェア）に分割し、それぞれを法的に異なる2つの団体が管理する別々の場所に保存することで、データの匿名性を確保します。近い将来、大学や非営利団体などの追加のストレージパートナーが参加し、さらに多くの抽象化された値が、より多くの独立した団体によって管理される予定です。どの団体も虹彩コードの一部にはアクセスできず、それぞれが管理するSMPCシェアにしかアクセスできないため、全体像にアクセスすることはできません。

データを複数の場所に保存することは、一見するとデータが盗まれるリスクが高まるように思えるかもしれませんが、実際にはその逆です。SMPCシェアは、悪意のある者が1つにアクセスしただけでは解読できないように設計されています。すべてのシェアが揃って初めて、意味を持つのです。

では、なぜ暗号化されたSMPCシェアを保存する必要があるのでしょうか? それは、Worldcoinプロトコルがその人が引き続きユニークな存在であることを証明できるようにするためです。これがなければ、アプリが認証を要求するたびに、ユーザーは毎回World IDを再度認証しなければならなくなります。



さらに、撮影された写真はOrbには残りません。Orbは、ユーザーのスマートフォンが提供する公開鍵を使用してデータを完全に暗号化します（プライベートキーを持っているのはユーザーだけで、データを復号できるのもユーザーのみです）。暗号化された写真はユーザーのデバイスに送信され、Orbからは即座に削除されます。これらの処理は、認証プロセス中の数秒の間にすべて行われます。

なぜ虹彩なのか?

Orbは、高度なカメラ機能を備えた、Worldcoinプロトコルをサポートする初のハードウェアデバイスです。現時点では、World IDがユニークな人間に属することを認証する唯一の方法は、Orbを訪れ、虹彩の写真を撮影することです。

TFHは、World IDの認証に使用できるさまざまな生体認証技術を研究しました。それぞれに長所と短所がありますが、AIが進化する世界で、すべての人々が唯一無二で人間であることを証明するためには、次の条件を満たす方法が必要です。1) 正確であること、2) プライバシーを保護できること、3) 非常に偽造が難しいこと、4) スケーラブルであること、5) とても使いやすいこと。

指紋は非常に使いやすい反面、偽造が容易です。一方、虹彩は正確でありながら使いやすく、スケーラブルで、多様な人々に対応でき、さらに偽造が極めて難しい特徴を持っています。また、虹彩はプライバシー保護にも優れています。顔のようにソーシャルメディアで広く公開されることがなく、他人に気づかれずに虹彩のクローズアップ写真を撮影することはできません。加えて、虹彩を撮影するには特殊なカメラ機器が必要です。

Worldcoinプロトコルはオープンかつ分散型であり、認証メカニズムを追加することでプロジェクトとしての魅力と安全性がさらに強化されます。

ゼロ知識証明 (ZKP)

World IDを認証すると、そのIDを使って、World IDプロトコルと連携するサードパーティアプリにログインして利用することが可能になります。

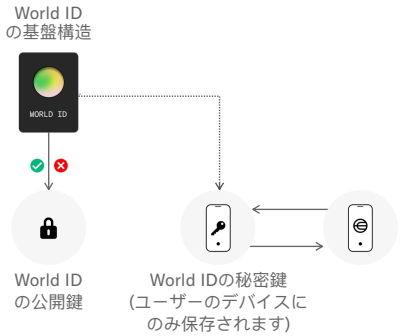
ただし、これはユーザーが自分のWorld IDをサードパーティアプリに直接共有するわけではありません。

代わりに、Appleの「メールを非公開」機能やバーチャルクレジットカードに似た仕組みの、World IDの使い切り版が生成されます。例えば、会社のクレジットカードが1回の購入にしか使えないと想像してみてください。他のベンダーで支払いをするには、別のカードを生成する必要があります。煩わしく聞こえるかもしれませんが、このプロセスはバックグラウンドで素早くシームレスに行われ、アプリにも安全であり、ユーザーの保護にもつながります。

この方法により、Worldcoinやアプリが利用履歴や他のアプリとの連携を追跡したり、特定の取引に関わる当事者を知ることができなくなります。このために使用される暗号技術がゼロ知識証明（ZKP）です。ZKPは、何かが正しいことを証明する際、その結論に至るまでの情報を一切開示せずに証明を行う技術です。

サードパーティアプリを使用するたびに、そのアプリはユーザーのデバイスに証明を要求します。これは、デバイスに対して「このデバイスがこのWorld IDを管理しているか」を尋ねるようなものです。ユーザーのデバイスにインストールされたWorld Appは、World IDが認証されていることを示すZKPを返送します。

ZKPは、どの国の規制要件も超える高度な技術です。WorldcoinがZKPを採用した理由は、これがユーザーの匿名性を保つための最も効果的な方法であるからです（ユーザーがサードパーティサービスに追加情報を提供しない限り）。この仕組みにより、サードパーティやWorldcoin財団自身がユーザーのWorld IDや、どのサービスを利用しているかを知ることができなくなります。



ゼロ知識証明（ZKP）の実践的な例え

ゼロ知識証明（ZKP）は高度な暗号技術であるため、完璧に例え話で説明するのは難しいですが、基本的な考え方を理解するために、ある場面で特定の物や人物を見つけるパズルを想像してみてください。[2]

数分探した後、一人が「どこにあるか分かった」と言います。もう一人は、本当に正しいかどうか確信が持てません。

そこで、最初の人が「場所を教えずに証明できる」と言います。

彼女はパズル全体をコピーし、目的の物を切り抜いてもう一人に見せます。これで、もう一人はその物が確かにパズルの中に存在し、彼女がそれを見つけたことを確認できます。

[2] 例：「ウォーリーを探せ」

このシナリオでは、もう一人がユーザーが人間かどうかを確認しようとしているアプリ、そして切り抜かれたものがZKPです。最初の人は、ユーザーの身元を明かすことなく、その人が人間であることを証明するWorldcoinプロトコルに相当します。

事例:
Xにおけるボットか人間か?

イーロン・マスクがX（旧Twitter）を買収した際、ボットの排除を約束しました。しかし、それが容易ではないことはすぐに明らかになりました。マスクは2023年12月に「現実には、実際のユーザーに影響を与えずにボットを止めるのは極めて難しい。」と述べています。「高度なAIが誰でも使えるようになれば、これはほとんど不可能になるだろう。」

Elon Musk
@elonmusk

現実には、実際のユーザーに影響を与えずにボットを止めるのは極めて難しい。

高度なAIが誰でも利用できるようになれば、これはほとんど不可能になるだろう。

マスクは、ソーシャルプラットフォームにおけるボットの課題について正しかったのです。しかし今では、ユーザーに影響を与えずにボットを排除する実現可能な方法が存在します。

Xでは、「Google でログイン」「Appleのアカウントでログイン」「ユーザー名とパスワード」の3つのサインイン方法があります。アカウント作成時には、名前、電話番号またはメールアドレス、生年月日を提供するよう求められます。しかし、複数のメールアドレスを簡単に作成できるため、Xアカウントを複数作成するのも比較的容易です。その結果、ボットが容易にオンラインにアクセスし、人間のユーザー体験を損なう可能性があります。

一方、World IDは設定が簡単なメールアドレスや、偽装が容易な電話番号には依存していません。人間だけがWorld IDを取得でき、しかも1人1つに制限されています。したがって、もしXがWorld IDを人間認証メカニズムとして導入すれば、認証された人間であることを示すバッジを追加することが可能です。ボットはログインしても認証されることはありません。

重要な点は、これによりXユーザーの匿名性がさらに強化されることです。ユーザーはXに既に提供した情報以外の追加情報を提供する必要がありません。

これは単なる理論ではありません。TFHは、World IDのTelegram連携機能を構築し、ネットワーク上のスパムボットを排除しました。公開チャットの管理者は、グループ内で投稿する前に、各アカウントに対してWorld IDでの認証を義務付けることができます。

原則 3

選択とコントロール:
自分のデータは自分で管理

私たちはこれまで、巨大IT企業のサービスを利用する代わりに、個人情報を提供し、それが高値で取引されるという状況に慣れてきました。[3]

しかし、Worldcoinはこうした従来の考え方とは一線を画します。これは単なる約束ではなく、そもそもそのようなことができないように意図的に設計されています。

Worldcoinのアプローチ: **自分のデータは自分で管理する**

データの最小化

人々が自分のデータをコントロールできるようにするための出発点は、そもそも多くのデータを要求しないことです。認証されたWorld IDは匿名であり、人々は名前、電話番号、住所など、一般的にテクノロジー企業によって収集される情報を提供する必要がありません。たとえば、図書カードを取得するには住所の証明が必要ですが、グローバルなデジタルパスポートであるWorld IDを取得するには、スマートフォンとOrbを訪れるだけで十分です。

事例:
Shopifyの割引コード

Shopifyは、売上拡大やオンライン決済の管理を目指す事業者向けのイーコマースプラットフォームです。プラットフォーム上の販売者は、新規顧客を獲得するために、時折、一度限りの割引を提供することがあります。

しかし、ユーザーが複数の偽のメールアドレスを作成して何度も割引を利用したり、ボットを使って不正に割引を取得することが問題となっています。その結果、新規顧客を引きつけるどころか、販売者は詐欺にお金を払ってしまう状況に陥っています。

そこで、店舗がWorld IDと連携することで、販売者は実際の顧客にQRコードをスキャンしてもらい、World IDを認証して割引コードを適用できるようになります。この方法により、ユーザーから追加の個人情報を取得せずに、一人につき一回の割引を確実に提供することができるようになります。（ただし、購入時にはクレジットカード情報や配送先の詳細を入力する必要があります。）

[3] 詳細は https://en.wikipedia.org/wiki/Real-time_bidding をご覧ください

パーソナルカストディ(個人情報の自己管理機能)

World IDを認証する過程では、生体画像や虹彩コードなどの一部のデータが必要です。虹彩コードはSMPCを経て、完全に匿名化された形式でサーバーに保存されます。しかし、Orbを通じてユーザーが提供した個人認証のためのデータは保持されず、第三者に提供されることもありません。そのデータはユーザーのスマートフォン内にのみ存在し、個々の公開鍵で暗号化されます。

Worldcoinのパーソナルカストディでは、ユーザーは認証時に収集・生成されたデータ(World IDや画像）を自分で管理し、誰と共有するかを決めることができます。

顔認証

World IDを導入することで、プラットフォームはユーザーのプライバシーを侵害することなく、ボットから保護することができます。認証されたWorld IDは、ユーザーが人間であることを高い確証をもってプラットフォームに証明します。

しかし、金融取引などの重要な場面では、相手がただの人間であるだけでなく、特定の個人であることを確認しなければならない場合もあります。つまり、World IDを利用している人が、そのデバイスでWorld IDを認証した同一の人物であるかどうかを確認したい場合です。

これを実現するために、Worldcoinのアプリでは顔認証を使用できます。

顔認証は、Orbでの認証時に撮影された画像と、World IDを使用しようとしている人物の画像を比較する方法であり、デバイスに依存しない技術です。

最初の画像は、ユーザーがOrbでWorld IDを認証した際に生成されます。初期設定では、このデータはユーザーのスマートフォンのみに保存されます。この高解像度の写真は暗号化され、安全にユーザーのスマートフォンへ送信され、個人管理の一環としてOrbから完全に削除されます。

2枚目の画像は、ユーザーがWorld IDにアクセスまたは使用する際に、World App上で撮影される自撮り画像です。顔認証は、この自撮り画像と、Orbで認証時に撮影された最初の画像を比較します。この2つの画像が一致した場合にのみ、ユーザーはログインや取引を続けることができます。

これにより、悪意のある第三者がスマートフォンを盗んだり購入したりして、他人のWorld IDを不正に使用するのを防ぎます。顔認証を使用することで、データとWorld IDの管理は常に本人が行い、**比較は個々のデバイス上でローカルに行われます。**その結果、自撮り画像やOrbで撮影された写真、その他の個人データは、Tools for HumanityやWorldcoin財団を含む第三者と共有されることはありません。[4]

[4] 将来的に、このプロジェクトでは、安全性やAIの学習のために、ユーザーが自分の情報をWorldcoinと共有することを選択できるようになります。これは完全に任意であり、いつでも許可を取り消すことが可能です。

顔認証とFace IDの比較

ユーザーにとって、顔認証はAppleのFace IDと同じように親しみやすいものに感じられるでしょう。

しかし、なぜFace IDをそのまま使わないのでしょうか?

顔認証は、World Appを使用している人が、OrbでWorld IDを作成した本人であることを確認する機能を持っていますが、Face IDにはその能力がありません。

Face IDはハードウェアとソフトウェアの組み合わせであり、最終的にはiPhoneに紐づけられています。そのため、Face IDでは、World IDを認証した顔と異なる顔がデバイスに登録される可能性があり、不正利用のリスクが高まります。一方、顔認証はデバイスレベルではなくアプリレベルでWorld IDを保護しており、認証時にWorld IDを作成した本人以外がアクセスできないようにします。

原則 4

透明性: 開かれた環境での設計

セキュリティの専門家たちは常に警戒を怠らず、ソースコードの一行一行に潜むリスクを探し出しています。これが私たちの安全を守る上で重要な役割を果たしています。

TFHや一部のWorldcoin開発者が、プロトコルに潜むすべての問題を予測できるとは考えにくいことです。だからこそ、Worldcoinは**開かれた環境で設計**されています。

監査

Worldcoinは、可能な限り多くの外部の意見や専門知識を取り入れています。暗号学者やバイオメトリクスの専門家が継続的にソースコードを評価し、セキュリティ監査の専門家やコンサルタントがわずかな脆弱性の可能性を探っています。Worldcoinはその結果を公表し、たとえ小さな問題でもそれに対処するために取った措置を公開しています。

潜在的なセキュリティ侵害を特定するには、プロトコルが現実世界でどのように使用されているか、そして今後どのように利用されるかを理解することが必要です。そのためには、世界中のさまざまな文化的要素を考慮し、まだ存在しない可能性のある悪用に対しても対応できるセキュリティモデルを構築することが求められます。

2023年4月から、監査会社であるNethermindとLeast Authorityは、Worldcoinプロトコルに対して2つの別々のセキュリティ監査を実施しました。 これらの監査は、特に以下の領域をカバーしています:

- 暗号化構成と原始技術、スマートコントラクト構造の適切な使用を含む実装の正確性。
- 一般的または特定の実装エラー。
- コードに対する悪意のある行為やその他の攻撃。
- 安全な鍵の保管と暗号化および署名鍵の適切な管理。
- ユーザーインタラクション中の重要な情報の漏洩。
- 分散型サービス拒否（DDoS）攻撃および同様の攻撃に対する耐性。
- 悪意のある行動やその他の攻撃を可能にするコードの脆弱性。
- 悪意のある攻撃やその他の悪用方法に対する保護。
- パフォーマンスの問題またはその他の潜在的なパフォーマンスへの影響。
- 個人情報保護、データ漏洩、情報の整合性。
- 不適切な権限、権限の昇格、過度の権限。

オープンソースとパーミッションレス

Worldcoinのコードをオープンソースにし、パーミッションレスなシステムとすることで、以下の3つの目的を達成できるようになります。まず第一に、ネットワークを改善するための批判や提案を受け入れることができるようになります。

第二に、開発者がWorldcoinプロトコル上で安心して開発できるようになります。他のチームがWorld IDを活用した個人認証アプリケーションを作成したり、Orbよりも使いやすい認証方法を見つけてくれるかもしれません。

最後に、オープンソースとパーミッションレスであることは、分散型プロジェクトに不可欠です。誰でも、いつでも、どんな理由でも、プロトコルの独自のバージョン（または「フォーク」）を作成でき、それがプロジェクトにとって良い影響をもたらします。

詳細はこちら: よくある質問

最終更新日2024年9月18日