# ゼロ知識証明のお本

tiz

## Contents

**この本のゴール** **1**

**ゼロ知識証明の背景** **1**
分類 . . . . . 2

**具体例** **2**
1. ブロックチェーン（公開台帳） . . . . . 2
2. 範囲の証明 . . . . . 2

## この本のゴール

ゼロ知識証明という言葉を知っていますか？

多分、知らなかったらこの本をいま読んではいないですよね。

では、ゼロ知識証明がどのように行われて、どんなときに使われているか、知っていますか？そう聞かれたとき

- なんとなくでなら答えられるかも知れませんが、うまく言葉にして表せない。
- これから自分のやりたいことの中に取り入れられそう・・・なんて思っても本当にゼロ知識証明を用いるのが適切なのか、いまいちわからない。

以上のような方に向けて

ゼロ知識証明がどのように行われているかの言語化、応用方法を思いつく手助けをするためにこの本は存在します。

筆者自身も、ゼロ知識証明という言葉を聞いて、なんとなく自分のやりたいこと（後述します）と合ってそうだな～と考え、手を出してみました。しかし、インターネットにも書籍にも限られた情報しか見つかりません(2022年現在)。

この本がその足しになれば良いと考えています。

## ゼロ知識証明の背景

なぜゼロ知識証明という手法が生まれたかについて触れます。一体、この手法は「どのような問題」を解決するために生まれたのか、「どのように解決するのか」ということです。最初はまだゼロ知識証明の説明をしていないので、問題提起だけしておきます。読者の皆さんがどのような分野に詳しいか、というのは私には知りかねます。なので、以下に複数の例を列挙します。ピンときた内容が一つでも見つかれば、ほかは読み飛ばして大丈夫です！ただいろんなことに使われるのだ、ということは頭の片隅に入れておいてください。

### 分類

ゼロ知識証明はPETs(Privacy Enhancing Technologies：プライバシー強化技術)の一つです。

1. ブロックチェーンのプライバシー確保

ブロックチェーンではトランザクションを全部公開して検証してるけど、誰が誰にお金渡したとかバレちゃわない？

2. 範囲の証明：ZKRP(Zero-Knowledge Range Proof)
3. オンライン選挙
4. ユーザー認証
5. 機械学習

## 具体例

### 1. ブロックチェーン（公開台帳）

Bitcoin, Ethereum などのブロックチェーンではトランザクションを公（要するに参加したい人誰でも）に検証することができる。

本来は、「隠さない」ことで成立している仕組み。

#### 問題

でも、これだとちょっと頑張れば、誰が誰にお金を渡したかなどの情報も公開されるものとなってしまう。プライバシーの懸念として挙げられるだろう。

#### 解決

ゼロ知識証明を用いることで、この公開台帳の内容をプライバシーを確保ができる。

例はZcashなどがある。具体的には

- 送金側・受取側両方のウォレットのアドレス
- トランザクションの量（送金の額）
- 暗号化されたメモの内容　←　Zcash特有のもの

を隠すことができる。

### 2. 範囲の証明

住宅ローンの契約を結ぶときなど、源泉徴収票を提出させ、契約者が対象の所得の範囲にいるかを確認する、という作業がある。

#### 問題

でも源泉徴収票には正確な収入といった、プライベートな情報・個人を特定できる可能性のある情報が含まれる。これを不動産業者が保持することは情報漏えいのリスクが増加するとともに個人情報管理のコストが上がる

#### 解決

ヨーロッパを中心とした国際的な銀行であるINGは「(明かしたくない）ある数字」が「特定の範囲」内にあるという命題をゼロ知識証明するZKRPをオープンソースソフトウェアとして開発した。これを用いることで、収入の値が対象の範囲内にあるかを、その値を明かすことなく証明できる。