日本総研
The Japan Research Institute, Limited

ゼロ知識証明の現在地
～ブロックチェーンを超えた活用可能性～

2024年8月6日

株式会社日本総合研究所
先端技術ラボ

＜本件に関するお問い合わせ＞ 渡邊　大喜（watanabe.hiroki@jri.co.jp）

エグゼクティブサマリ

ゼロ知識証明技術とは？	• 「ゼロ知識証明（Zero-Knowledge Proof, ZKP）」とは、「特定の情報を知っていること」を、何ら具体的な事実を明らかにせず（このことを「ゼロ知識」と呼ぶ）他者に数学的に証明することができる技術である。 • 1980年代の半ばに考案。当初は、デジタル署名やユーザ認証などの分野で活用。
汎用ZKPとは？	• 直近10年で、ブロックチェーン領域での実用をきっかけとして、様々な事柄をより効率的に証明できるゼロ知識証明技術が、進展してきている。 • 特定の用途に限らず、幅広い応用分野に利用できることから「汎用ZKP（General-purpose Zero-Knowledge Proof）」とも呼ばれている。
どのようなユースケースがある？	• 汎用ZKPは、プライバシーの保護やデータの秘匿性の強化が必要な幅広いアプリケーションに応用可能であり、プライバシー強化技術（※）の一つとして活用できる。 （※）プライバシー保護規制の基となるプライバシー原則を実現・強化する技術。詳細は「プライバシー強化技術の概説と動向」参照 • ブロックチェーン領域以外でも活用が見込めるユースケースとして、「デジタルアイデンティティの検証」「プライバシーとコンプライアンスの両立」「計算のアウトソーシング」などがある。
今後の見通しは？	• 技術面では、技術の汎用化や標準化が進み、暗号学に精通していない一般のエンジニアでも容易に扱えるようになる。 • 企業ニーズとして、ESG経営の観点でもサイバーセキュリティへの注力は必須の時代となっており、プライバシー強化技術の積極的な採用が進むと思われる。これらの技術が顧客/自社情報をどのように守り得るかの検討を推奨する。

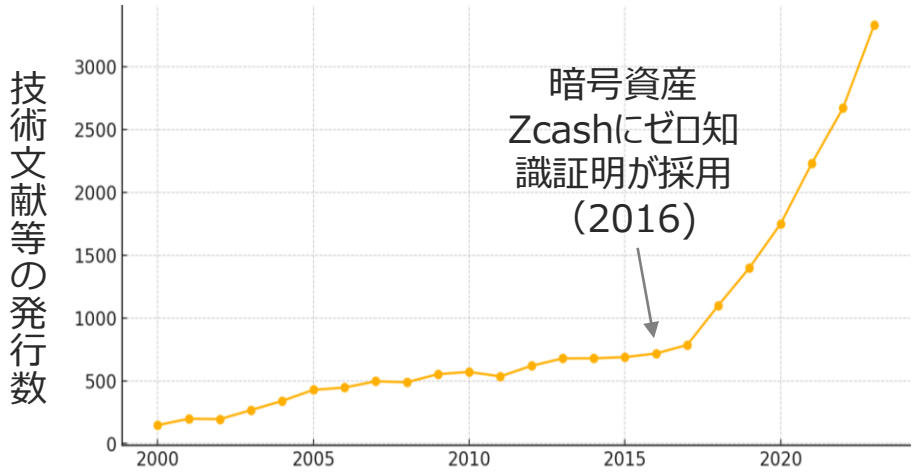
目次

日本総研 The Japan Research Institute, Limited

ゼロ知識証明技術の需要の高まり

- ゼロ知識証明技術が暗号資産・ブロックチェーン領域での実用を起点に、プライバシー強化技術としても注目が高まる。

加速するゼロ知識証明の技術開発



出所）Google Scholarでの文献検索数を基に日本総研作成

- 2015年以前は、ユースケースに乏しかったものの暗号資産やブロックチェーン技術での匿名取引の需要を受けて、技術開発が急速に進む。
- 2019年発行の世界経済フォーラム白書では、金融分野に新たな価値をもたらす技術の一つに位置付け*1。

*1: World Economic Forum. “The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value.” 2019.

プライバシー強化技術（PETs）として注目

- プライバシー強化技術（Privacy Enhancing Technologies, PETs）は、プライバシー保護の原則を実現・強化する技術の総称。
  ※詳細は別レポート「プライバシー強化技術の概説と動向」を参照
- 国連やOECD（経済協力開発機構）が発行するプライバシー強化技術（PETs）関連のレポート*2では、ゼロ知識証明も主要なPETs技術の一つとして位置づけ。

*2: UN, “The pet guide: The United Nations Guide on privacy-enhancing technologies for official statistics”, UN Big Data, 2023.
OECD, “Emerging privacy-enhancing technologies: Current regulatory and policy approaches”, OECD Digital Economy Papers, No. 351, 2023.

プライバシー強化技術に分類され得る要素技術	
認証・アクセス制御	連合学習
デジタル署名	ゼロ知識証明
ブロックチェーン	匿名化
秘密計算	暗号化
差分プライバシー	合成データ

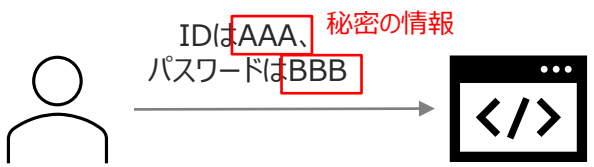
日本総研 The Japan Research Institute, Limited

ゼロ知識証明とは：基本の概念

- ゼロ知識証明技術とは、「特定の情報を知っていること」を、何ら具体的な事実を明らかにせず（このことを「ゼロ知識」と呼ぶ）他者に数学的に証明することができる技術。
- 基本的な概念としては、1980年代に証明系の一種として定式化されている*1。当初は、ユーザ認証やデジタル署名などを応用先として研究されてきた。

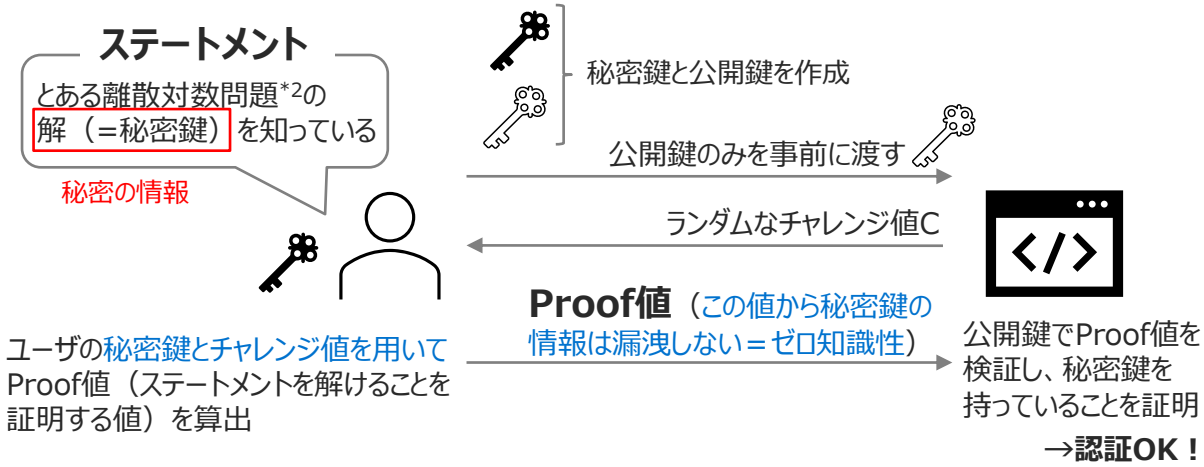
ゼロ知識ではないユーザ認証の例

（秘密の情報そのものを渡す）



Webサービス側は
秘密の情報（ID、パスワード）
を知り得るためゼロ知識ではない

ゼロ知識証明を用いたユーザ認証の例



ユーザの秘密鍵とチャレンジ値を用いて
Proof値（ステートメントを解けることを
証明する値）を算出

公開鍵でProof値を
検証し、秘密鍵を
持っていることを証明

→認証OK！

基礎用語（本レポート内でも使用）

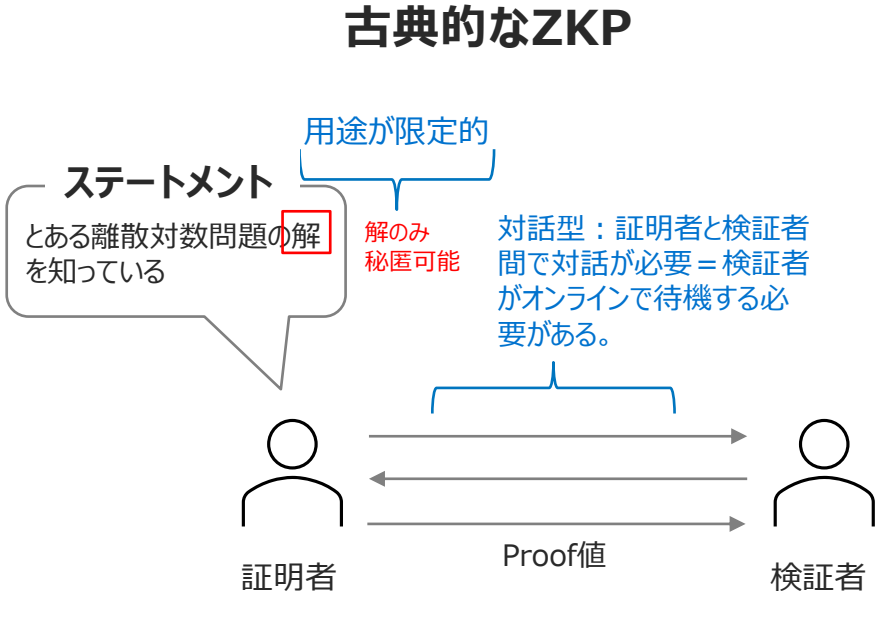
ステートメント：証明者が、検証者に示そうとしている事実・情報（命題）
Proof値：証明者が秘密としたい値を公開せずに、ステートメントが正しいことを証明する数学的な値

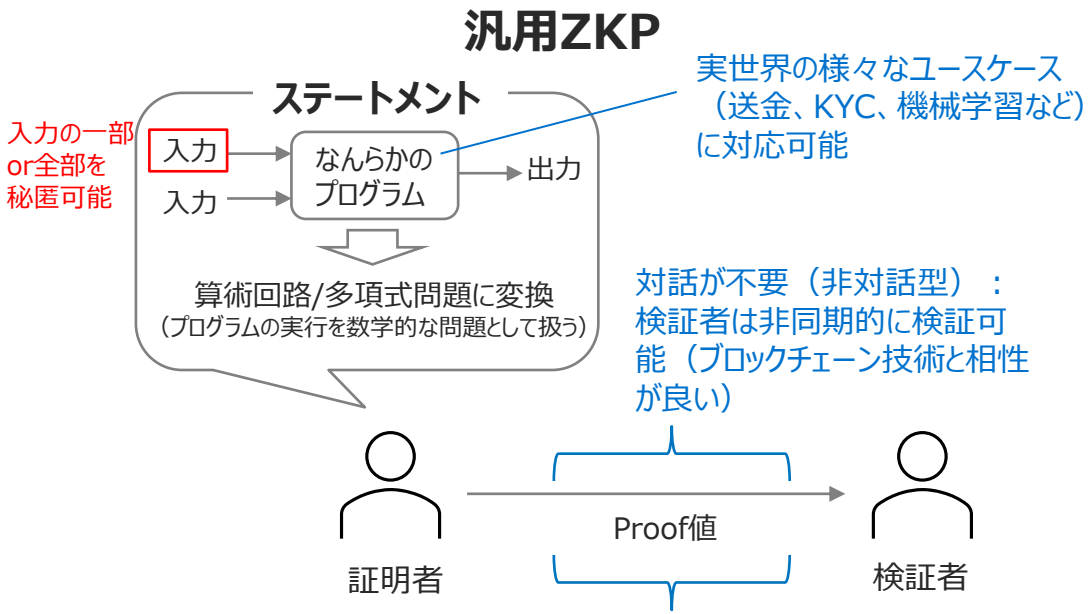
*1: S. Goldwasser, S. Micali, and C. Rackoff. “The knowledge complexity of interactive proof-systems.” STOC ’85, 1985.
*2: 簡単に言えば、ある数を何乗したら別の特定の数になるかを見つける問題。大きな数では、計算機で効率的に解くことは難しいが、解が合っていることを確かめることは容易。

日本総研 The Japan Research Institute, Limited

ゼロ知識証明とは：汎用ZKP

- ゼロ知識証明は、離散対数問題などの特定の問題のみならず、どのような任意のNP問題（≒コンピュータプログラムで判定できるような問題）でも実現できることが知られている*
- 近年のゼロ知識証明は、効率性や柔軟性を向上させて、任意のプログラムに適用可能なように発展してきた。（例えば、非対話型、証明サイズの簡潔化、算術回路への変換など）
- これらは汎用（General-Purpose）なゼロ知識証明（ZKP：Zero-Knowledge-Proof）とも呼ばれ、古典的なゼロ知識証明と比べて、様々な用途への適用が期待される。





* O. Goldreich, S. Micali, and A. Wigderson. “Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems.” Journal of the ACM 38(3), 1991

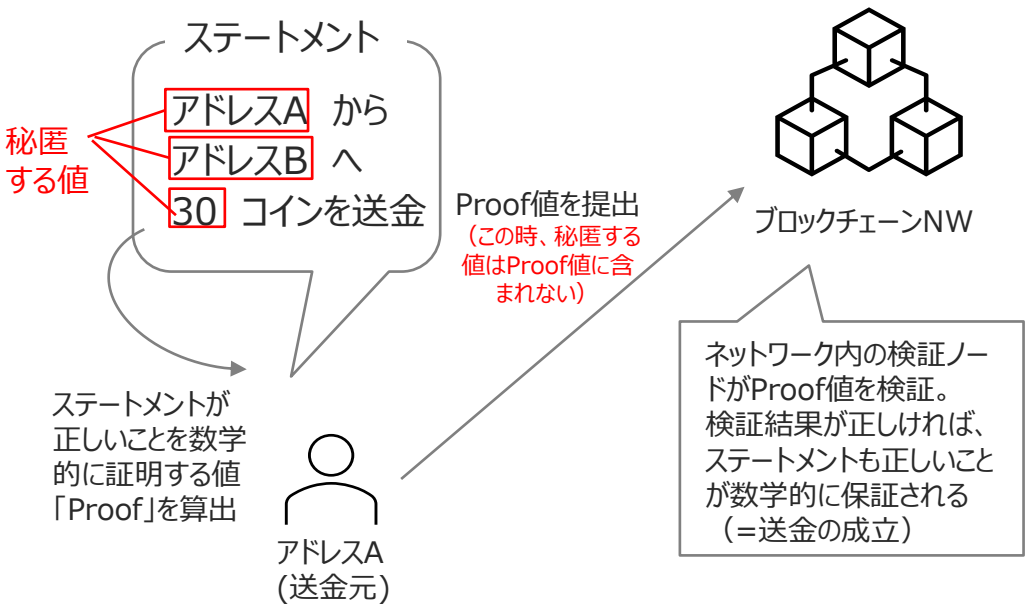
日本総研 The Japan Research Institute, Limited

暗号資産（ブロックチェーン）と汎用ZKP

- 秘匿性の高い暗号資産「Zcash」にて汎用ZKP（汎用的なゼロ知識証明）が採用されたことを発端に、ブロックチェーン技術への適用の研究が進み、急速な発展を遂げている。
- 主な用途はプライバシー保護のための「取引の秘匿化」と、スケーラビリティ向上のための「取引の圧縮」

用途①：取引の秘匿化

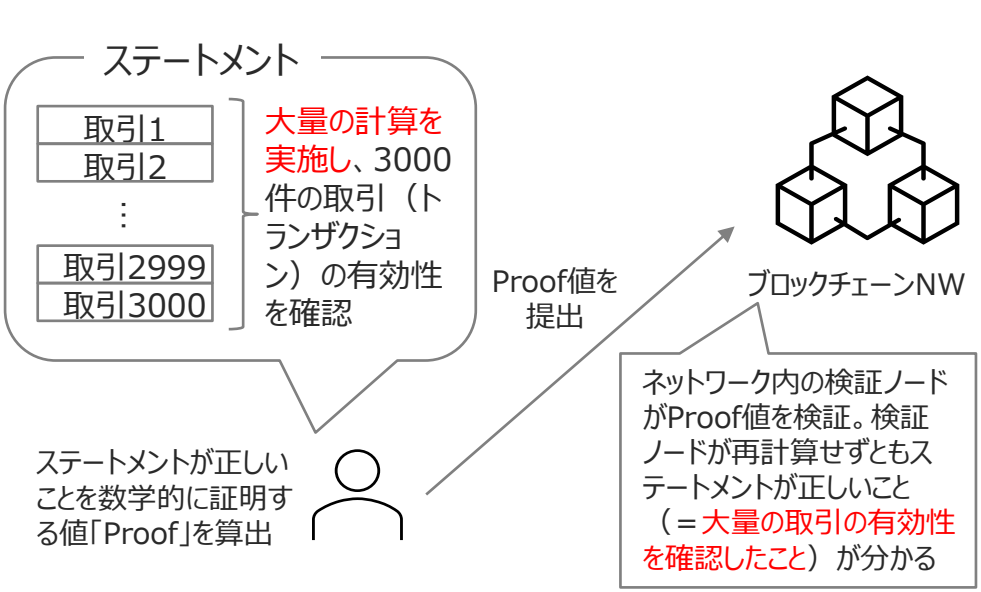
例：**プライバシーコイン**（送金額・送金元/先を隠して取引する暗号資産）



- プライバシーコイン自体はマネロン・テロ資金供与の観点で、世界的には規制傾向にあることには留意。

用途②：取引の圧縮

例：**ZKロールアップ**（取引を低コスト・高速に行う技術）



- ZKロールアップでは、ゼロ知識性（情報の秘匿化）の効用を用いていないケースが多いことには留意。（従って、単に「有効性証明」と呼ばれることもある）

日本総研 The Japan Research Institute, Limited

汎用ZKPの基本プロトコル

汎用ZKPには、それぞれ特徴の異なる複数の基本プロトコルがあり、ユースケースの要件に応じて使い分ける必要がある。
（どのユースケース（P.13）にどのプロトコルが適するかは研究途上。）

	zk-SNARK（**Z**ero-**K**nowledge **S**uccinct **N**on-interactive **Ar**gument of **K**nowledge）	**zk-STARK**（**Z**ero-**K**nowledge **S**calable **T**ransparent **Ar**gument of **K**nowledge）	**BulletProof**
Trusted Setup*（信頼されたセットアップ）	必要	不要	不要
Proof値のサイズ	・かなり小さい ・0.3～数キロバイト程度	・大きい ・50～数百キロバイト程度	・小さい ・数キロバイト程度
証明者がProof値を生成する時間	・早い ・数ミリ～数秒程度	・早い ・数ミリ～数秒程度	・かなり遅い ・数十秒程度
検証者がProof値を検証する時間	・早い ・数ミリ秒程度	・早い ・数ミリ秒程度	・遅い ・数秒程度
量子耐性	無	有	無
特徴	・Proof値が小さくブロックチェーンに格納が容易で、証明/検証の実行時間も効率的であるため幅広いユースケースに適する。 ・アプリケーション構築/運用時に「誰が」「いつ」「どのように」、”信頼されたセットアップ”を行うのか設計が必要である。	・量子耐性があり、依拠する暗号の仮定も少ないため、より安全性が高い。 ・”信頼されたセットアップ”が不要のため、構築/運用は、よりシンプルになる。 ・大規模なデータセットでは証明/検証時間が長くなる。 ・Proof値のサイズが大きくなるため、ブロックチェーンへの格納が難しく、スマートコントラクト上での検証などが高コストになる。	・Proof値が小さくブロックチェーンへの格納が容易。 ・”信頼されたセットアップ”が不要のため、構築/運用は、よりシンプルになる。 ・証明/検証の実行時間が長くなる。複雑なアプリケーションには向かず、現状は、範囲証明（送金額などがある値の範囲以下に収まっているかの証明）のユースケースが主。

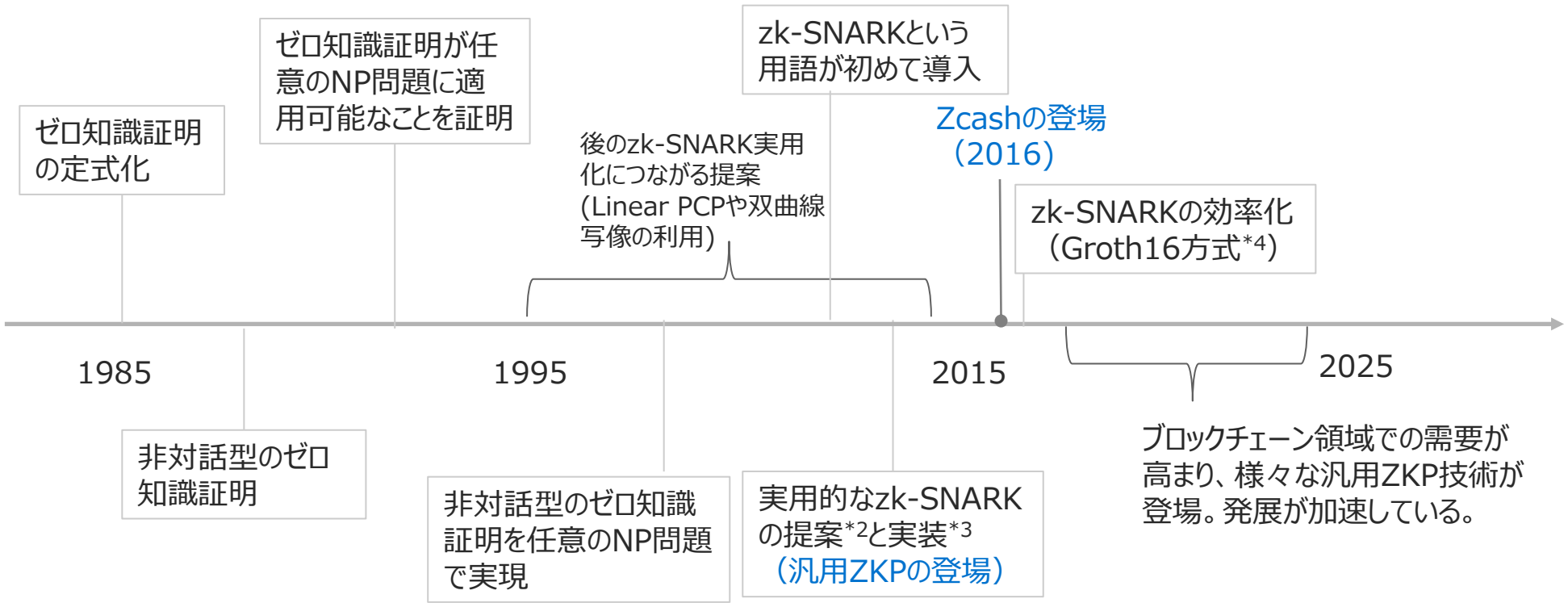
表内のProof値サイズや時間については、証明したい知識の内容（アプリケーション）の複雑性や入力データセットのサイズによって大きく変動することに留意。
表の数値記載は、各種ベンチマーク資料を基に、認証などで用いられるような「あるハッシュ値の原像を知っていること」を証明するアプリケーションを想定し作成。
*:Trusted Setup（信頼されたセットアップ）とは、プロトコルが正しく機能するために必要な共通パラメータの生成プロセス。通常、複数の異なる利害関係者間で実施する。利用者は、これら共通パラメータを基に証明鍵や検証鍵を生成し、管理する必要がある。このためZKPシステムは複雑になる。

日本総研 The Japan Research Institute, Limited

参考：汎用ZKP（zk-SNARK）登場の歴史

- 汎用ZKPの研究領域は、直近10年で目覚ましい発展を遂げてきた。
- zk-SNARK（**Z**ero-**K**nowledge **S**uccinct **N**on-interactive **Ar**gument of **K**nowledge）は、Proofのサイズが「簡潔（Succinct）」な「非対話型」のゼロ知識証明のプロトコル*1である。
- zk-SNARKが匿名性の高い暗号資産「Zcash」で実用化され、汎用ZKP発展のきっかけとなった。

*1 より厳密には計算量的健全性を持つ証明系である「知識のアーギュメント」に分類される



*2: R. Gennaro, C. Gentry, B. Parno and M. Raykova. “Quadratic Span Programs and Succinct NIZKs without PCPs.” EUROCRYPT 2013, 626-645, 2013
*3: B. Parno, J. Howell, C. Gentry, M. Raykova. “Pinocchio: Nearly Practical Verifiable Computation.” 2013 IEEE Symposium on Security and Privacy, 238-252, 2013
*4: J. Groth. “On the Size of Pairing-Based Non-interactive Arguments.” EUROCRYPT 2016, 305-326, 2016

日本総研 The Japan Research Institute, Limited

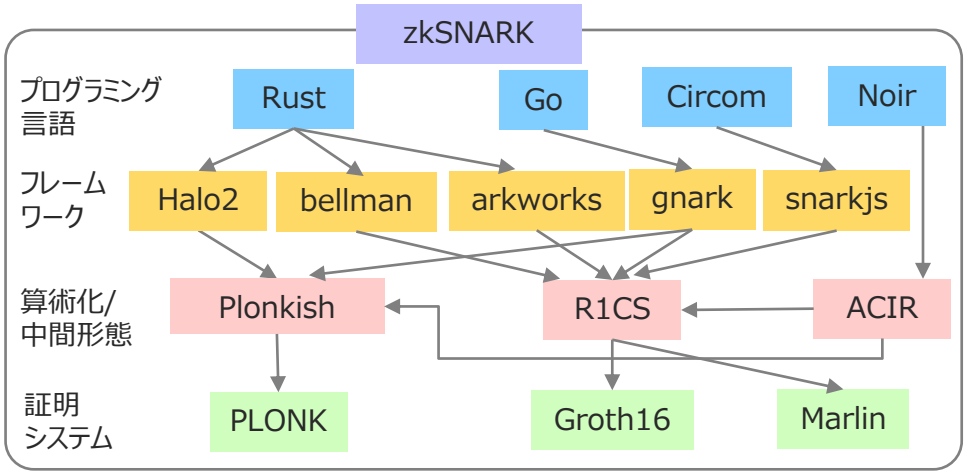
汎用ZKPの多様なツール群

- 汎用ZKPを扱うためのライブラリ・フレームワーク・プラットフォーム等が、急成長をしており、現存する全てのツール群を把握することが、難しくなってきている。
- 基本のプロトコルをベースとしながらも、暗号学的スキームや実装言語も異なるためパフォーマンスや表現力も様々である。

多様な実装/組み合わせ

- 一口にzk-SNARK（P.8）と呼ばれるプロトコルも、技術要素や実装の組み合わせ方によって（下図）、パフォーマンスや適用範囲に差がでることが知られている*1。

*1: J. Ernstberger et al. “zk-Bench: A Toolset for Comparative Evaluation and Performance Benchmarking of SNARKs”, International Conference on Security and Cryptography for Networks (SCN 2024)



- このような、多種多様な技術方式に対して、産業界と学術界が集まり、暗号学的な利用方式の標準化を行おうとする動き*もある。*: ZKProof Standards, https://zkproof.org/ (参照日:2024.7.12)

汎用ZKPの専用言語

- 汎用ZKP用のドメイン固有言語 (Domain Specific Language, DSL)が登場している。
  例：Circom、Noir、Leoなど
- DSLはZKPプロトコルで扱うためのロジック（算術回路と呼ばれる）を構築するための言語。「入力信号」と「出力信号」、それらの「入出力に作用する制約」の観点で記述する。

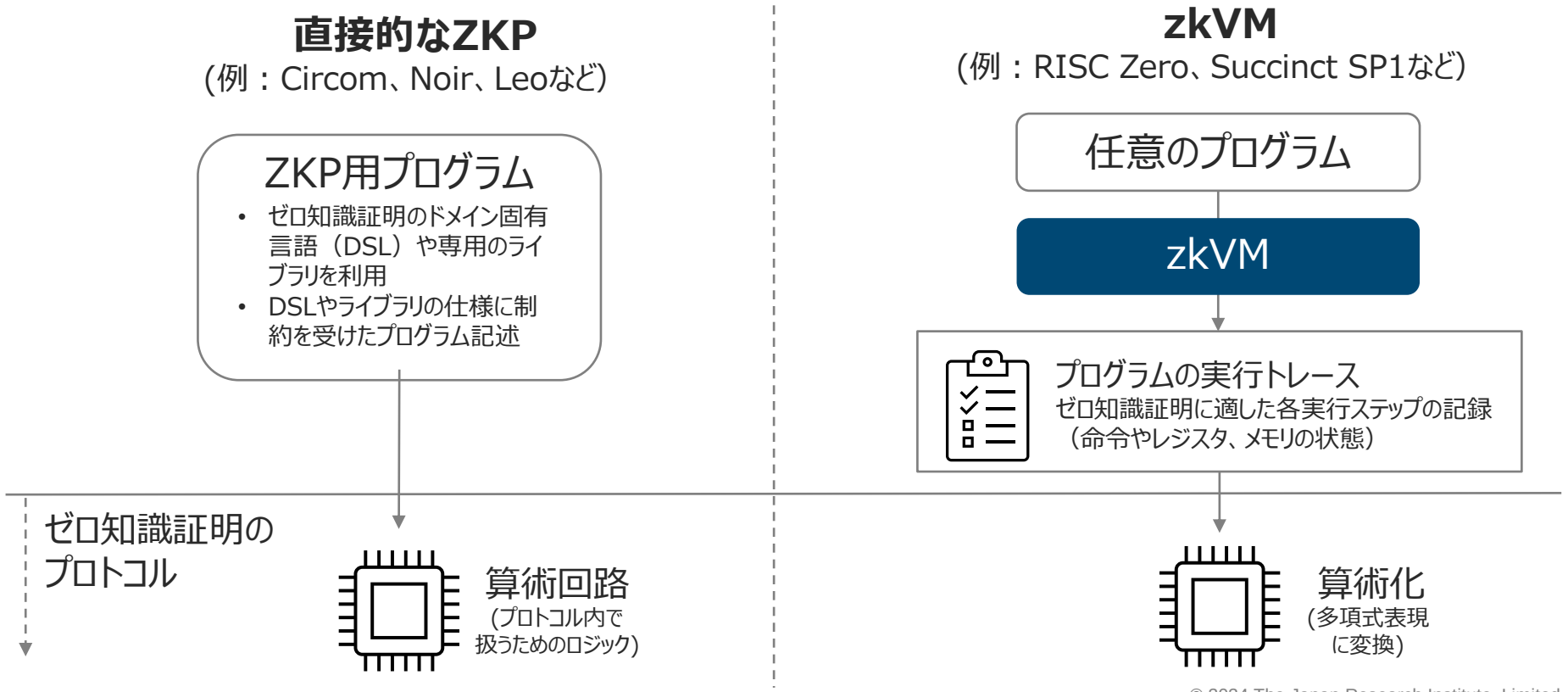
```
pragma circom 2.0.0;

/*This circuit template checks that c is the multiplication of a and b.*/

template Multiplier2 () {

   // Declaration of signals.
   signal input a;
   signal input b;
   signal output c;

   // Constraints.
   c <== a * b;
}
```

画像出所）https://docs.circom.io/getting-started/writing-circuits/
Circomのプログラム例。必ず「AxB+C=0」の線形結合の制約となるように記述しなければならない。

日本総研 The Japan Research Institute, Limited

zkVM：ゼロ知識仮想マシン

- zkVMは、ゼロ知識証明に適したVM（仮想マシン）を通じて、プログラムを実行することで、その実行トレースに対してゼロ知識証明を行うことができる、より発展的な汎用ZKP技術である。
- 既存の高級言語（Rustなど）を用いて、任意のプログラムを構築し、zkVM上で実行するだけでゼロ知識証明を構築できるため、ZKPの背景となる数学やプロトコル詳細の理解が不要。
- ZKP導入の敷居を下げ、広域な用途に期待できる。また、zkML（ゼロ知識機械学習、P.20）の基盤としても期待されており、より高いパフォーマンスでの実用化に向けた競争が過熱している。

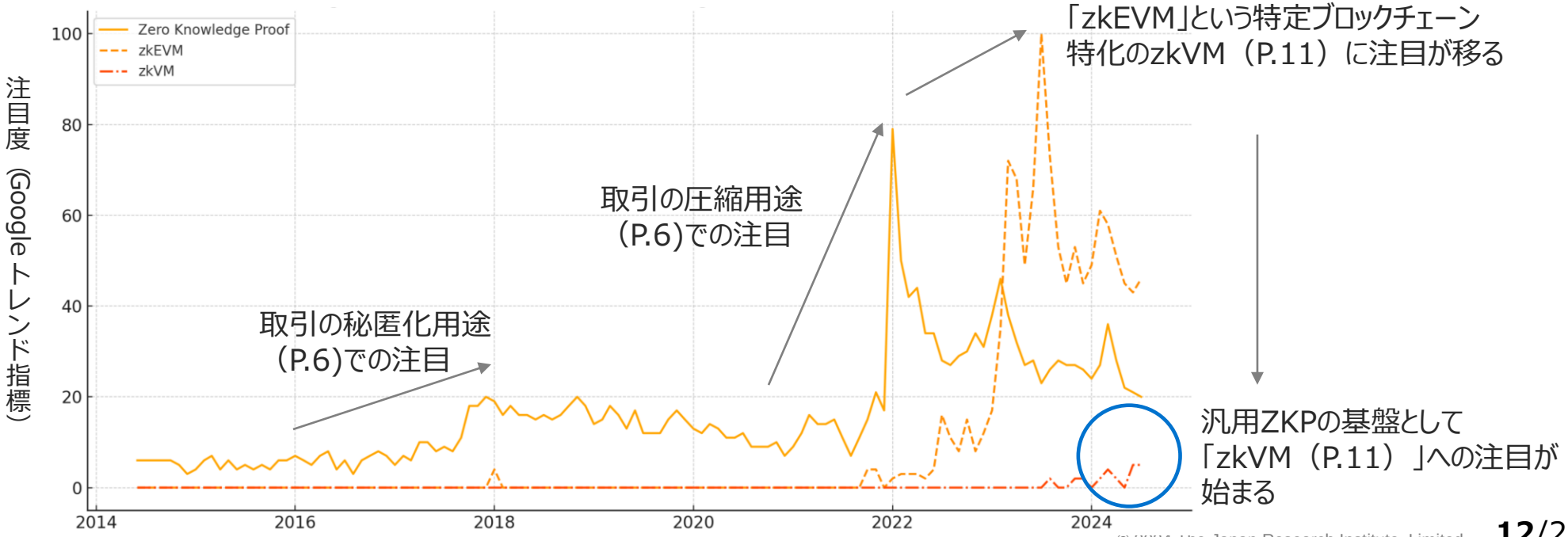


日本総研 The Japan Research Institute, Limited

技術の現在地、今後の展望

- 現在、暗号資産（ブロックチェーン）領域のインフラ技術として、汎用ZKP技術への需要が高まり、急速な技術開発が行われている。
- 技術要素レベルでは、基本プロトコル（P.8）上のパフォーマンスの課題（検証スピード等）を解消する方向。ツールレベルでは、専門言語（P.10） やzkVM（P.11）の開発も行われており、一般の技術者がゼロ知識証明の理論を深く理解せずとも利用できる環境が整いつつある。
- 今後のゼロ知識証明技術の開発動向として、様々なプログラムで活用できるよう、より汎用性を求めて発展を続ける可能性がある。ブロックチェーン領域を超えて、プライバシー強化が必要とされる様々なユースケースにおいて、ゼロ知識証明技術が適用されてくると予想する。

ZKP技術の注目度の変化（Googleトレンドを基に日本総研作成）



日本総研
The Japan Research Institute, Limited

ゼロ知識証明のユースケース

- ゼロ知識証明技術は、ブロックチェーンを用いた暗号資産の取引で最も用いられており成熟度が高い。
- 本レポートでは、金融領域への活用にも関連する「デジタルアイデンティティの検証」「プライバシーとコンプライアンスの両立」「計算のアウトソーシング」の中心的に３つを取り上げる。

成熟度	主なユースケース	具体的な取り組み事例
実用	暗号資産の取引	• プライバシーコイン（P.7） • ZKロールアップ（P.7）
一部実用	デジタルアイデンティティの検証	• 範囲証明（Range Proof）によって、住宅ローンの借り手が一定の年収の範囲にあるか、年収の値を明かさずに検証（P.14） • 生体認証とゼロ知識証明を組合わせて「本物の人間である」ことをプライバシーを保護しながら証明（P.14）
実験的	プライバシーとコンプライアンスの両立	• リテール型CBDCにおいて、プライバシーを保護しながらAML/CFTのコンプライアンスに準拠（P.16） • 画像の操作や通信のポリシー適用をプライバシーを保護しながら検証（P.17）
実験的	計算のアウトソーシング	• 機械学習のモデルパラメータや入力データを隠したまま、アウトソーシング先が行った推論結果の正当性を示す（P.18）

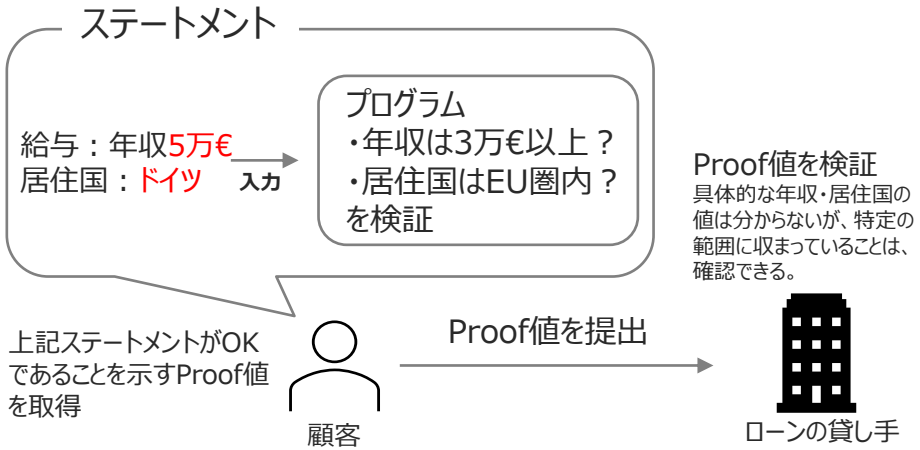
日本総研 The Japan Research Institute, Limited

デジタルアイデンティティの検証

- デジタルアイデンティティへの応用は、最もよく例示されるケースであり、詳細な身元情報を明かさずともアイデンティティが必要最低限の要件を満たしていることを証明する。

ING銀行による範囲証明

- 2017～2019年頃、オランダ最大手のING銀行では、ゼロ知識証明技術を用いたプロダクトを発表*1 。
- 主に、「範囲証明（Range Proof）」と呼ばれる種類のゼロ知識証明技術を扱い、主なユースケースとして「住宅ローンの申請者は、正確な数値を明らかにすることなく、給与が特定の範囲内にあることを証明」「新しい顧客がEUに属する国に住んでいることを、国を明かさずに検証できる」としている*2。

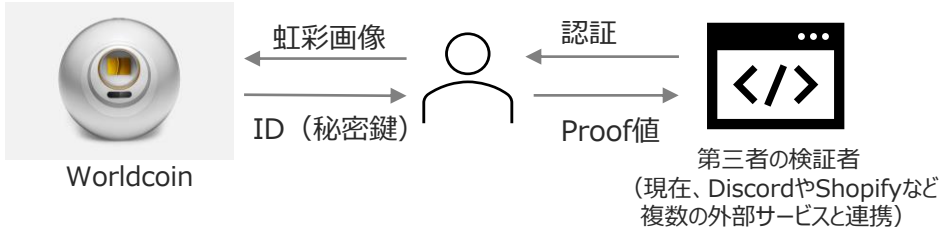


*1: 現在は当該リポジトリが削除されており、プロジェクトは停止している様子である。

*2: ING Bank N.V. “ING launches Zero-Knowledge Range Proof solution, a major addition to blockchain technology.” https://www.ingwb.com/en/insights/distributed-ledger-technology/ing-launches-major-addition-to-blockchain-technology (参照日:2024.7.11)

Worldcoin：「人間であること」の証明

- OpenAIのサム・アルトマン氏が2019年に立ち上げた、世界中の人々に唯一固有のIDを付与するプロジェクト。
- Worldcoinでは、虹彩データを利用した生体認証のプロセスを通じて*3 World IDが付与されると、「身元を明かさなくとも」本物の人間であることを証明できる。
- 人間であることの証明には、「ゼロ知識証明」が用いられており、申告したユーザが本物の人間であること以外の情報を明かさず証明できる。



*3 Worldcoinでは、Orbと呼ばれる生体認証デバイスが必要である。生体認証デバイスは、目の虹彩画像を取得し、暗号化された虹彩コードを生成、ユーザの公開IDと紐づけて保管する。

World IDのユースケース	
助成金や社会福祉などの平等な給付	先行事例として、インドでは生体認証を元にした国民ID（アーダール）により、助成金の給付を行っている。Worldcoinでも同様のユースケースを、よりプライバシーに配慮した形で実行可能としている。
SNS上でのAIボットの排除	AIモデルによる精巧なスパム投稿が社会問題化。本物の人間であることを証明することで防止する。

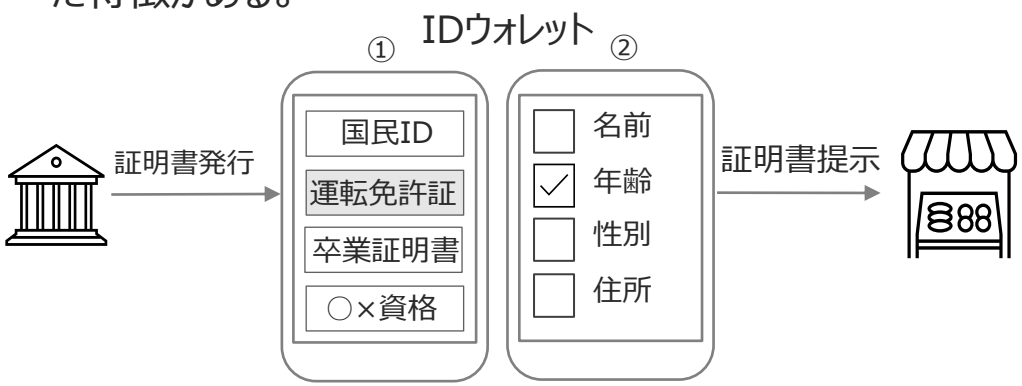
日本総研 The Japan Research Institute, Limited

[参考] IDウォレットとゼロ知識証明

- ゼロ知識証明を用いたKYCでは、身元情報の全てを明かさずとも、一定の要件を満たすか（例えば、年齢が一定以上であるか）を検証できる。
- 上記は、ゼロ知識証明の利点として強調されることが多く、自己主権型・プライバシー保護を重視している「欧州デジタルウォレット」でも、採用が検討されていた。

欧州デジタルIDウォレット：選択的開示

- 2024年5月に施行されたEUの新たなデジタルID規則（eIDAS2.0）では「欧州デジタルIDウォレット」の導入を加盟国に義務付け。
- 本IDウォレットの特徴は、デジタルIDの開示先を市民が自己主権的に選択できること、開示先に身元情報の全てを明かさず限定して開示できる（選択的開示）といった特徴がある。



デジタルIDウォレットでは、異なる発行者/認証局から、それぞれ証明書が発行され、これをスマートフォン等のウォレットアプリに格納できる。証明書を提示する際には、どの証明書を見せるか（図の①：例えば運転免許証）どの項目を開示するか（図の②：例えば年齢）をユーザが選択できる。

ゼロ知識証明技術の採用は見送り

- 欧州デジタルIDウォレットでは、選択的開示を実現する技術として「BBS+署名*1」を用いたゼロ知識証明の採用が検討された（JSON-LD ZKP with BBS+署名）。
- 一方で、2024年時点では、eIDAS2.0の参照フレームワークにおいて、標準化の不足などの理由により、ゼロ知識証明は含まれず「SD-JWT」と呼ばれるデータフォーマット仕様を採択。
- 本決定に関しては、プライバシー保護の観点を懸念する声が多く上がったため、仕様の検討チームは、ゼロ知識証明の適用に関するフィードバックを暗号の専門家に求めている*3。

仕様	選択的開示	リンク不能性*2	技術的成熟度
JSON-LD ZKP with BBS+署名	可能	可能（ゼロ知識証明により）	中
SD-JWT	可能	不完全	高

*1 BBS+署名を用いると、データの一部を隠しつつ(選択的開示)、かつ署名者の情報を一切開示することなく（ゼロ知識）、署名検証が可能。
*2 リンク不能性(Unlinkability）とは、認証技術の専門用語で、同じユーザの行動を名寄せしたり、追跡したりできないことを意味する。
*3 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/211 (参照日:2024.7.11)

プライバシーとコンプライアンスの両立：CBDC

- リテール型CBDC（Central Bank Digital Currency：中央銀行デジタル通貨）の検討において消費者プライバシー保護は重要な考慮事項の一つ。
- プライバシーを重視する一方で、マネロン・テロ資金供与の規制においては、トランザクションの秘匿は不正利用の追跡を困難にすると考えられており、プライバシーとコンプライアンスの両立が課題。
- 匿名化など他のプライバシー強化技術と共に、ゼロ知識証明技術の適用検討が進められている。

	近年のCBDCとゼロ知識証明に関する調査・研究例
2020年	カナダ銀行の調査*1では、ゼロ知識証明を用いたプライバシー保護は、技術的に複雑で、**オーバヘッドが大きいと指摘。また、技術分野として未熟であり、**導入と保守に必要なスキルセットを持つ人材も不足と指摘。
2022年	グロスらの研究*2では、CBDCでAML/CFT規制に遵守しながら、ゼロ知識証明技術を用いてプライバシーを確保できることを実証。さらに、**近年の技術進化により、処理速度面での大幅な改善が見込める**と述べている。
2024年	BIS（国際決済銀行）イノベーションセンタは、**各国の検討において、リテール型CBDCのプライバシー保護は重要な考慮事項となっているとし、**香港金融管理局（HKMA）と進めているCBDCの実証のフェーズ2では、ゼロ知識証明を含むプライバシー強化の手段をテストすることを発表*3。

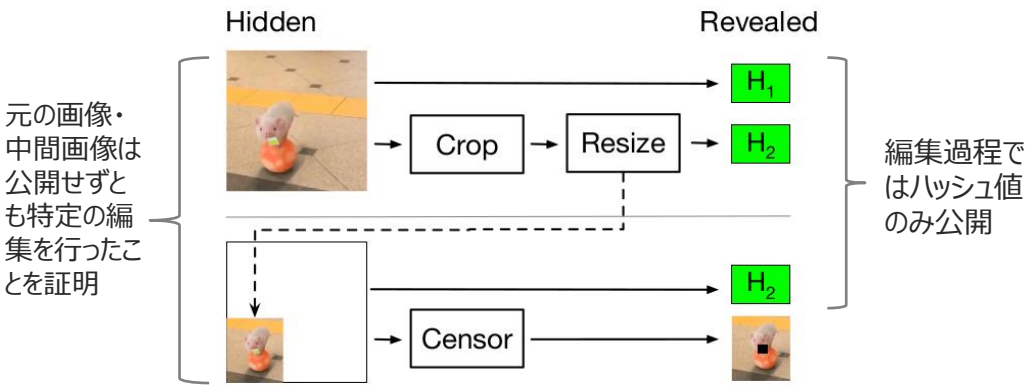
*1: Bank of Canada. “Privacy in CBDC technology.” https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/ (参照日: 2024.7.11)
*2: J. Gross et al. “Designing a Central Bank Digital Currency with Support for Cash-Like Privacy.” Available at SSRN 3891121, 2022(revised version)
*3: BIS. “Project Aurum 2.0: Improving privacy for retail CBDC payment.” https://www.bis.org/about/bisih/topics/cbdc/aurum2_0.htm（参照日：2024.7.11）

プライバシーとコンプライアンスの両立：“正しさ”を主張する

- CBDCのケース以外にも、「プライバシーの保護」と「コンプライアンス（ポリシー）の準拠」のジレンマは日常の様々なところにある。
- 近年のZKP技術の発展に伴い、アカデミアの研究では様々な適用シーンが提案されている。

ZK-IMG: 編集画像の真正性を検証

- AIによる動画像のディープフェイク（偽情報）が爆発的に増加したことを背景に、真正性カメラ*（撮影時にハードウェア内で画像に電子署名を付与）などによる対策が広まっている。
- ZK-IMGでは、ゼロ知識証明を用いて、元の画像からリサイズや編集を行ったことを証明する技術。
- この際に**元の画像を公開することなく、特定の編集作業を行ったことを証明できる。**

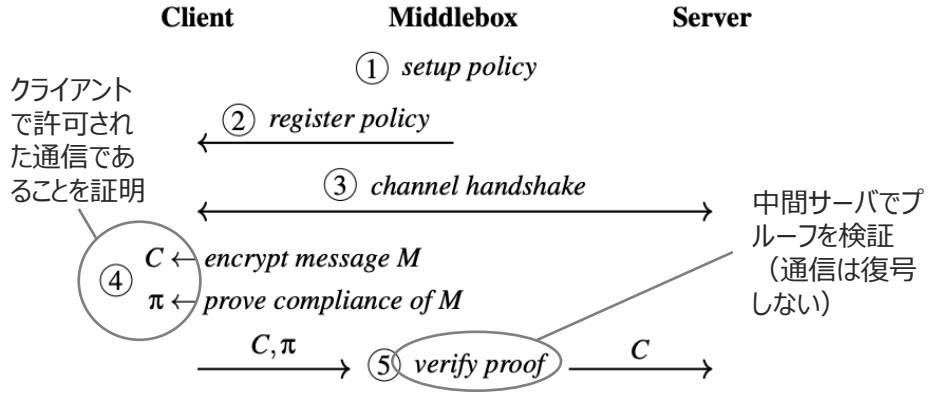


出所）Daniel Kang et al. “ZK-IMG: Attested Images via Zero-Knowledge Proofs to Fight Disinformation.” arXiv preprint arXiv:2211.04775

*: ソニー株式会社, ニュースリリース, ” C2PA規格対応を含む真正性カメラソリューションを報道機関向けに提供” https://www.sony.co.jp/corporate/information/news/202403/24-008/（参照日：2024.7.9）

ZKMBs: 暗号化された通信を検証

- DNS over HTTPSなどDNS通信の暗号化は、ネットワーク運用者がマルウェアスキャンなどのポリシー適用を困難にするという課題がある。
- ZKMBs（Zero-Knowledge MiddleBoxes)は、暗号化された**トラフィックを復号せずにポリシーに準拠しているか（組織に許可された通信か）をゼロ知識証明で判断する**技術。
- クライアント側で許可された通信であることを示すゼロ知識証明を生成し提示する。



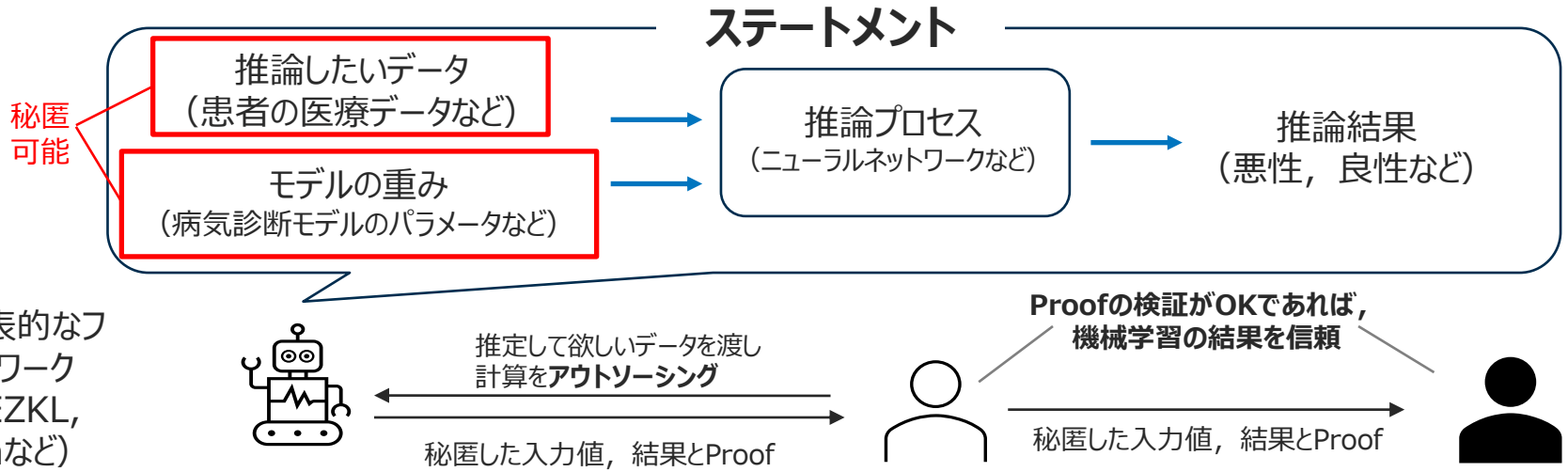
出所）Paul Grubbs et al. “Zero-Knowledge Middleboxes. In USENIX Security.” 2022

日本総研 The Japan Research Institute, Limited

計算のアウトソーシング：機械学習（zkML）

- ゼロ知識証明を機械学習の推論結果の正当性を検証するために利用する技術が注目されている。
- zkML（Zero-Knowledge Machine Learning）と呼ばれる研究領域*では、機械学習のモデルや入力データを開示せずとも、推論結果の正当性を示すことができる。
- MLaaS（Machine Learning as a Service）などのように、機械学習の計算タスクのアウトソーシングが普及しているが、その結果を数学的に証明し、第三者に納得させることができるようになる。

＊ zkMLの定義は明確には存在していないが、ここでは機械学習の推論プロセスを証明するものとする。



考えられるユースケース

医療	医療データから機械学習により推論された結果を、機械学習のモデルの詳細（例えば、モデル・パラメータが機密事項）を開示せずとも、その正しさを第三者（例えば製薬会社）に証明できる。
金融	ある財務データから機械学習により推論された顧客の信用ランクを、実際の財務データを開示せずに、その正しさを第三者（例えばローンの貸し手）に証明することができる。

日本総研
The Japan Research Institute, Limited

企業活用への課題

- ゼロ知識証明が企業で活用される際の課題として「活用事例」「技術人材」「標準化」「社会的土壌」の4つの不足が挙げられる。

	課題	予測
（ブロックチェーン以外の）活用事例の不足	技術的に未成熟であることを理由に、ゼロ知識証明の導入に至らないケースがある（P.10）	汎用ZKPの性能（P.8表に示す項目）は、年々向上しており、適用可能なユースケースが増加すると思われる。
技術人材の不足	ゼロ知識証明を扱うためには、一定の技術理解が必要。保守・運用人材の確保が課題（P.16）	• 任意のプログラムの実行を、そのままゼロ知識証明に適用できるzkVMが進展（P.11）。 • 技術発展により、学習ハードルは下がると予測する。
標準化の不足	国際的に標準化された仕様は未だない。	• 標準化の取り組みが進行。 • ゼロ知識証明の標準化を目指す学術イニシアチブZKProof[*1]では、企業やNIST（米国立標準技術研究所）とも協力し標準化プロセスを進めている。
社会的土壌の不足	ゼロ知識証明が活きる世界観（次頁解説）が、国内では浸透しているとは言い難く、企業やユーザが価値を感じにくい。	• ESG（環境・社会・ガバナンス）経営にサイバーセキュリティを注力領域に定める流れがあり[*2]。 • データ最小化や自己主権型アイデンティティ(P.20)などプライバシーを優先する概念の広まりと共に浸透。

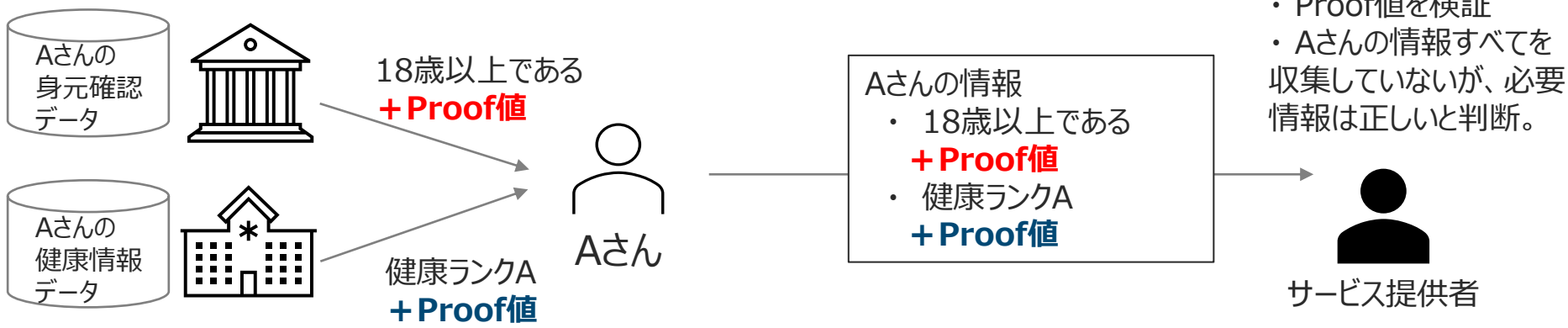
*1: ZKProof Standards, https://zkproof.org/ (参照日:2024.7.12)

*2: 別レポート「ESG経営発展の鍵となるCybersecurity Strategy －欧米のESG・先進デジタル動向から考察する日本企業の課題と対策－」を参照のこと

ゼロ知識証明が活きる世界観

- ゼロ知識証明技術は、情報が一極集中で管理される世界観よりも、情報が分散的に管理され、それぞれが必要な時に、必要な情報のみ取り扱う世界観で活きる。
- このような世界観を持つ概念としては「自己主権型アイデンティティ」「プライバシー・バイ・デザイン」などがあり、日本政府からも「Trusted Web」構想が提唱され、取り組みが進んでいる。

ゼロ知識証明を用いて必要な情報のみを取り扱う世界観



関連する概念・取り組み	
自己主権型アイデンティティ（Self-Sovereign Identity, SSI）	個人が行政当局の介入なしに、自分のアイデンティティを所有および管理する必要があると認識するデジタルムーブメント。個人が自己のアイデンティティ情報を完全に制御し、必要な時のみ必要な情報を提供できる。 詳細は別レポート「自己主権型アイデンティティの動向と考察 ～企業のデジタルアイデンティティ戦略へ向け～」参照
プライバシー・バイ・デザイン	「データの最小化」「収集制限」等のプライバシー原則や技術を、システム設計段階から取り込むことで、プライバシーを保護していく考え方。1990年代に提唱されたものであるが、欧州GDPR（一般データ保護規則）の法的要求事項になるなど、企業やユーザに広く認知されつつある。
Trusted Web	特定のサービスに過度に依存せずに、データ自体とデータのやり取りを検証できる領域を拡大し、トラスト（信頼性）を向上させる仕組み。日本政府は「Trusted Web推進協議会」を設置し、議論を進めている。 参考) Trusted Webホームページ, https://trustedweb.go.jp/ (参照日：2024.7.19)

日本総研
The Japan Research Institute, Limited

今後の見通し、企業への推奨事項

見通し

技術のシーズ面

技術の汎用品化や標準化が進み、企業が安定して扱えるZKPプロダクトが普及。

兆候：汎用ZKPの技術発展スピードは加速、zkVM（P.11）などの技術が活用の敷居を下げる。

社会のニーズ面

情報の一極集中リスク（情報を持ちすぎること）回避のための技術需要が高まる。

兆候：

- ランサムウェア等のサイバー攻撃の猛威により、「抱えすぎる」情報資産はリスクに。
- 諸外国ではサイバーセキュリティをESG経営の注力領域として定める傾向。

詳細は「ESG経営発展の鍵となるCybersecurity Strategy　－欧米のESG・先進デジタル動向から考察する日本企業の課題と対策－」を参照のこと

推奨事項

- 「プライバシー・バイ・デザイン（P.20）」の考え方に則り、ゼロ知識証明を含むプライバシー強化技術（P.4）が、顧客/自社情報をどのように守り得るか検討する。
- 現時点の汎用ZKP技術は、実績が少なく未熟な領域にあるとの見解（P.19）ではあるが、技術の発達スピードは早く、2-3年後にはブロックチェーン領域以外でも扱いやすく実用的なプロダクトが広まると予測。リサーチやプロダクトの評価を通じて、まずは正しく技術を知る人材を育てる。