データ活用社会における
プライバシーと中立性

川口 将司 / Cho Jang Sa
as Enigma Collective

もくじ

- プライバシーと中立性の問題
- 秘匿計算基盤”Enigma”の提案
- Enigmaの未来と課題

もくじ

- **プライバシーと中立性の問題**
- 秘匿計算基盤”Enigma”の提案
- Enigmaの未来と課題

＜プライバシーの問題＞

ひとびとは自らが提供するデータに対するコントロールを失っている

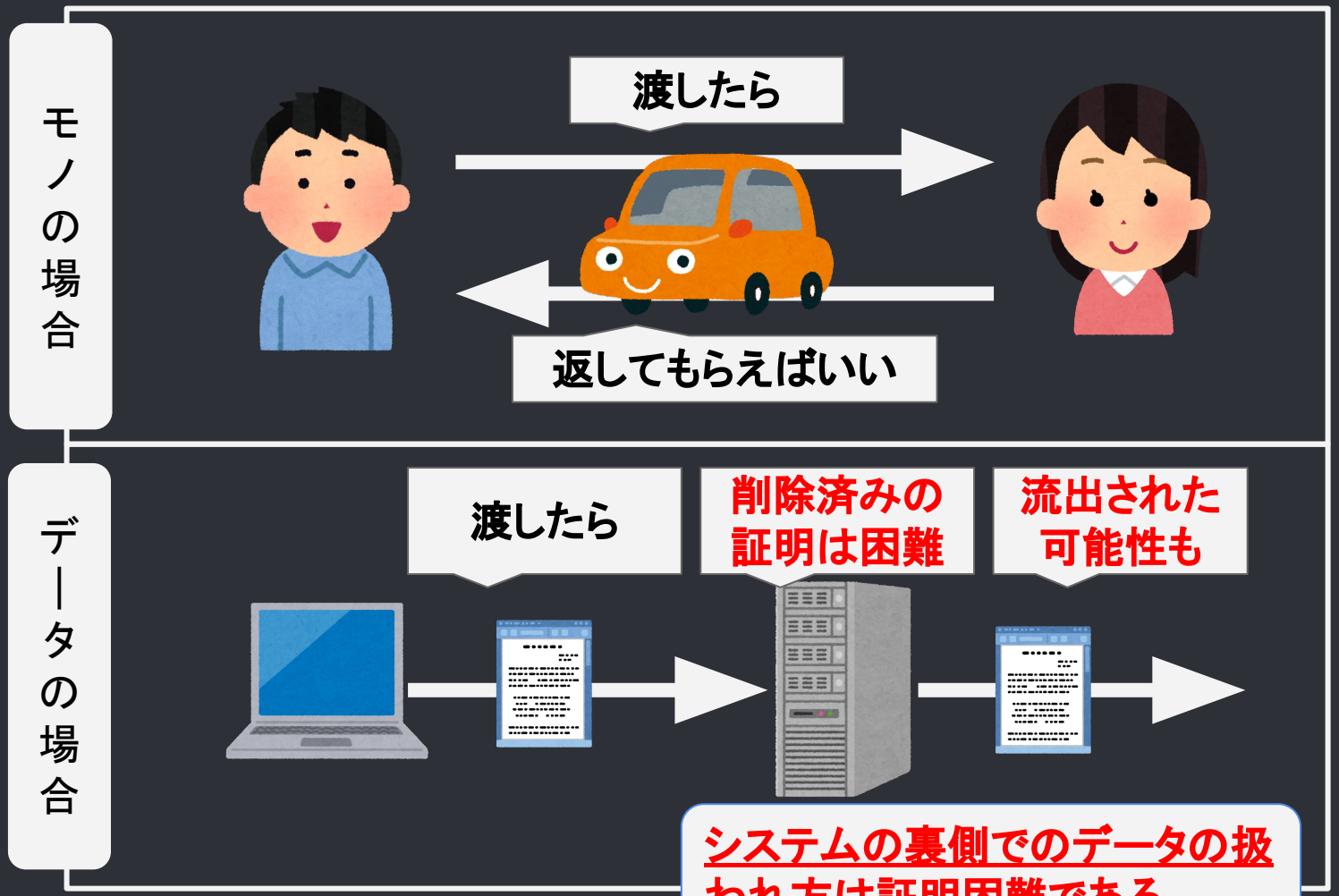
適法・公正・透明なデータ処理を受けられているか？ 	データは取り決めた目的に限定して使われているか？ 	収集されているデータの範囲は必要最小限に抑えられているか？ 
最新かつ正確なデータが適切に扱われているか？ 	必要な期間を超えてデータが保管されていないか？ 	データは完全性・秘匿性を損なわない環境下に保護されているか？ 

GDPRデータ保護7原則の1～6より

＜プライバシーの問題の本質＞

モノと異なり、**データの受け渡しは不可逆な行為**である

- 受け渡し対象のコントロールを持ち主が取り戻すには……



＜中立性の問題＞

ひとびとはサービスの由来成分・制作工程を知らない
結果的に**バイアスに晒される**

- 商業的・政治的利害のために、**不都合なデータは取り除かれた上で、**そのサービスは提供されているかもしれない

- 以下に挙げるような情報を操作することで利害が生まれる
  - 製品の評価、レコメンド
  - 歴史・経緯・定義の説明
  - 価格情報・シグナル
  - ほか

- ひとびとがAIに依存することで、

この影響は今後さらに強まっていく

個人であれ、組織であれ、
あらゆる情報を好き嫌いせず、
公正公平に取り扱うことは難しい

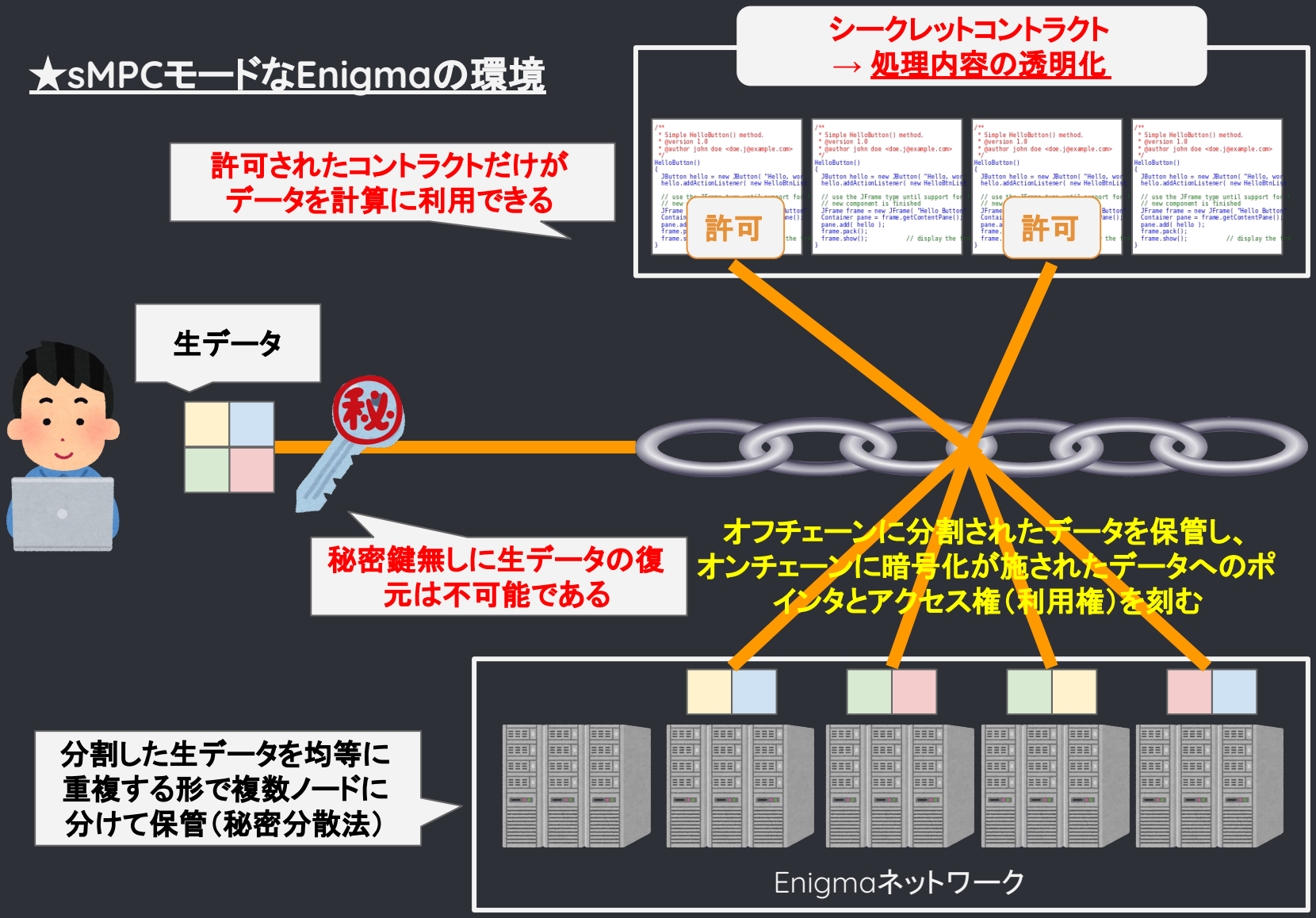
もくじ

- プライバシーと中立性の問題
- **秘匿計算基盤”Enigma”の提案**
- Enigmaの未来と課題

＜Enigmaの本質的な価値＞

Enigmaとは、**データの被処理を許しながらもプライバシーは失われない**計算基盤である

★sMPCモードなEnigmaの環境

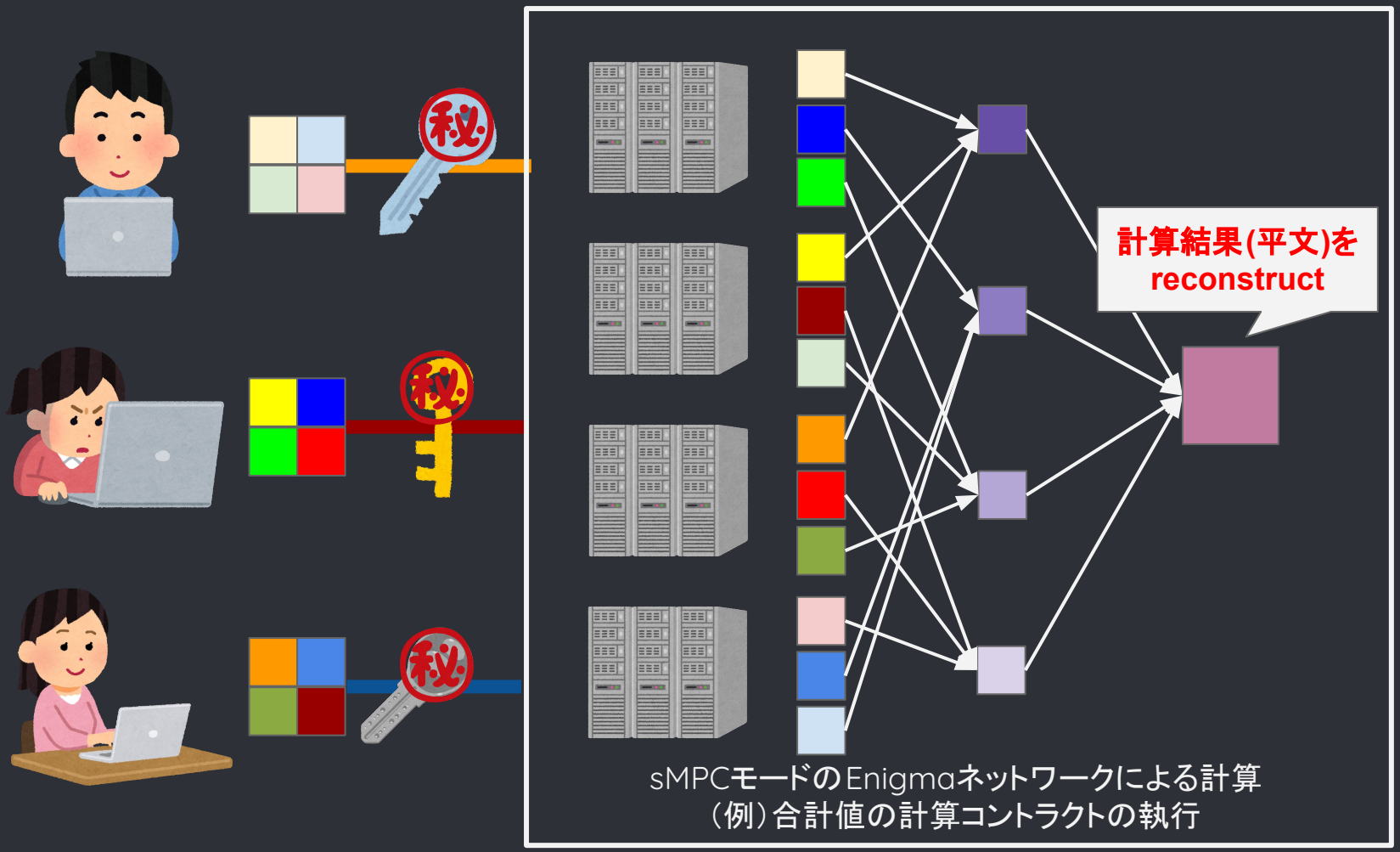


＜Enigmaの特徴＞

Enigma上での計算過程において**生データが復元されることは一度もない**

秘密分散法と制限付き準同型暗号を応用した計算法で秘匿性は守られる

★平文を公開せずに加法/乗法準同型な計算が可能 = 機能的完全性を満たす

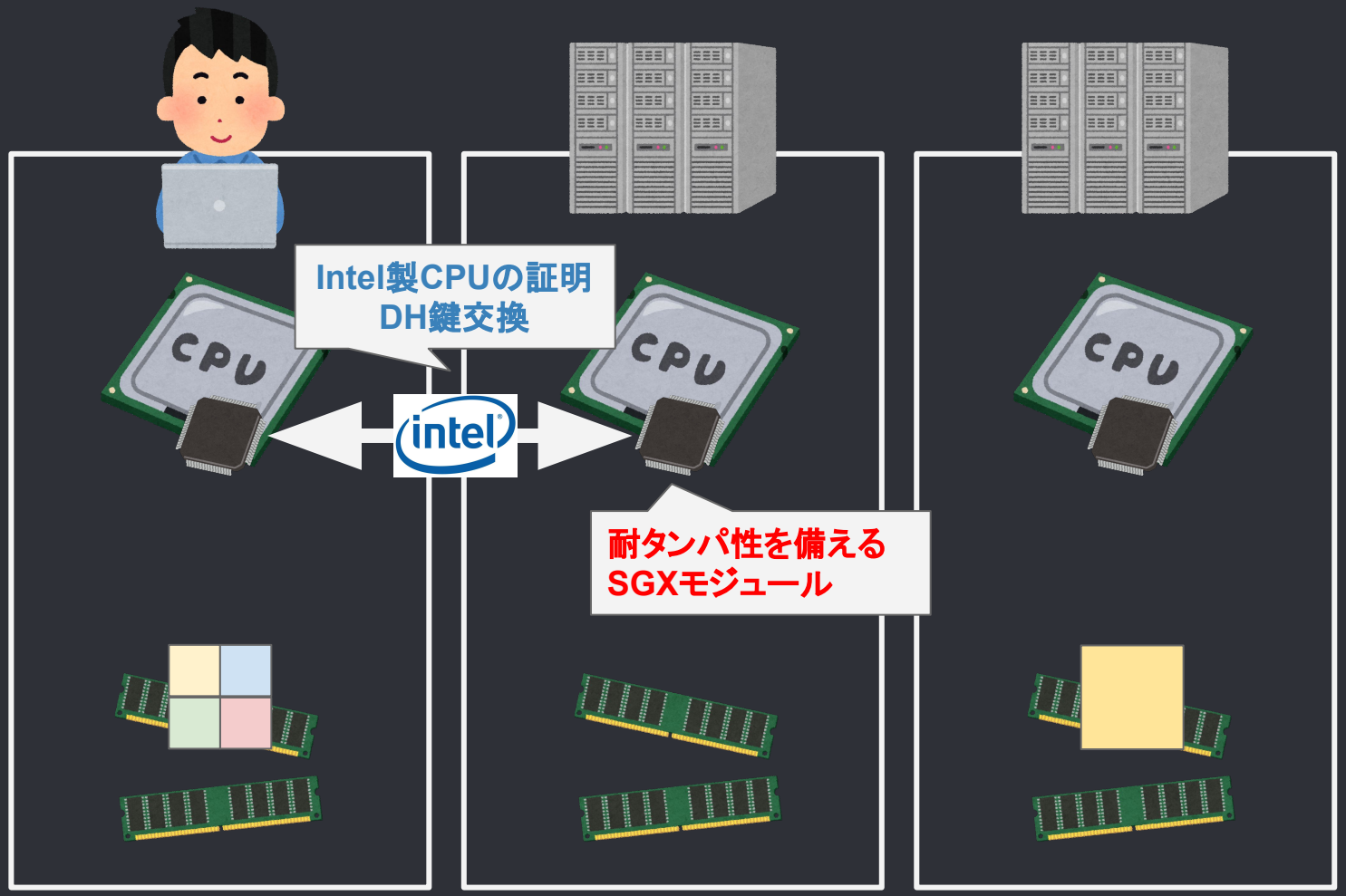


sMPCモードのEnigmaネットワークによる計算
（例）合計値の計算コントラクトの執行

＜補足資料：Enigmaのもうひとつの秘匿計算アプローチ＞

Enigmaはハードウェアに依拠する秘匿計算モードも持つ（TEE）
分権性／秘匿性とパフォーマンスのトレードオフといえる

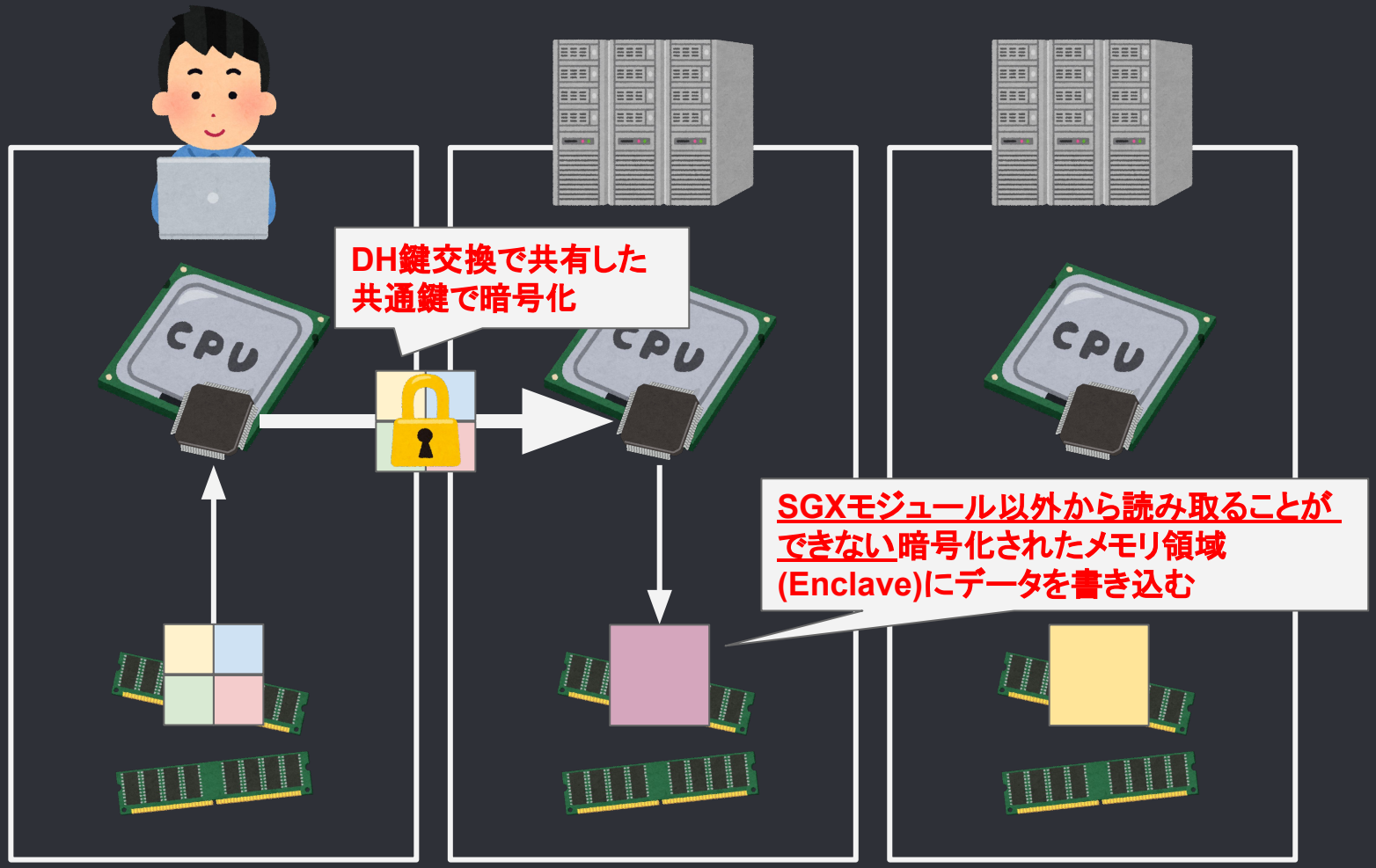
Trusted Execution Environment(TEE)は、CPUベンダーを信頼する前提と引き換えに、sMPCに比べて優れた計算速度を手に入れることができる



＜補足資料：Enigmaのもうひとつの秘匿計算アプローチ＞

Enigmaはハードウェアに依拠する秘匿計算モードも持つ（TEE）
分権性／秘匿性とパフォーマンスのトレードオフといえる

Trusted Execution Environment(TEE)は、CPUベンダーを信頼する前提と引き換えに、sMPCに比べて優れた計算速度を手に入れることができる

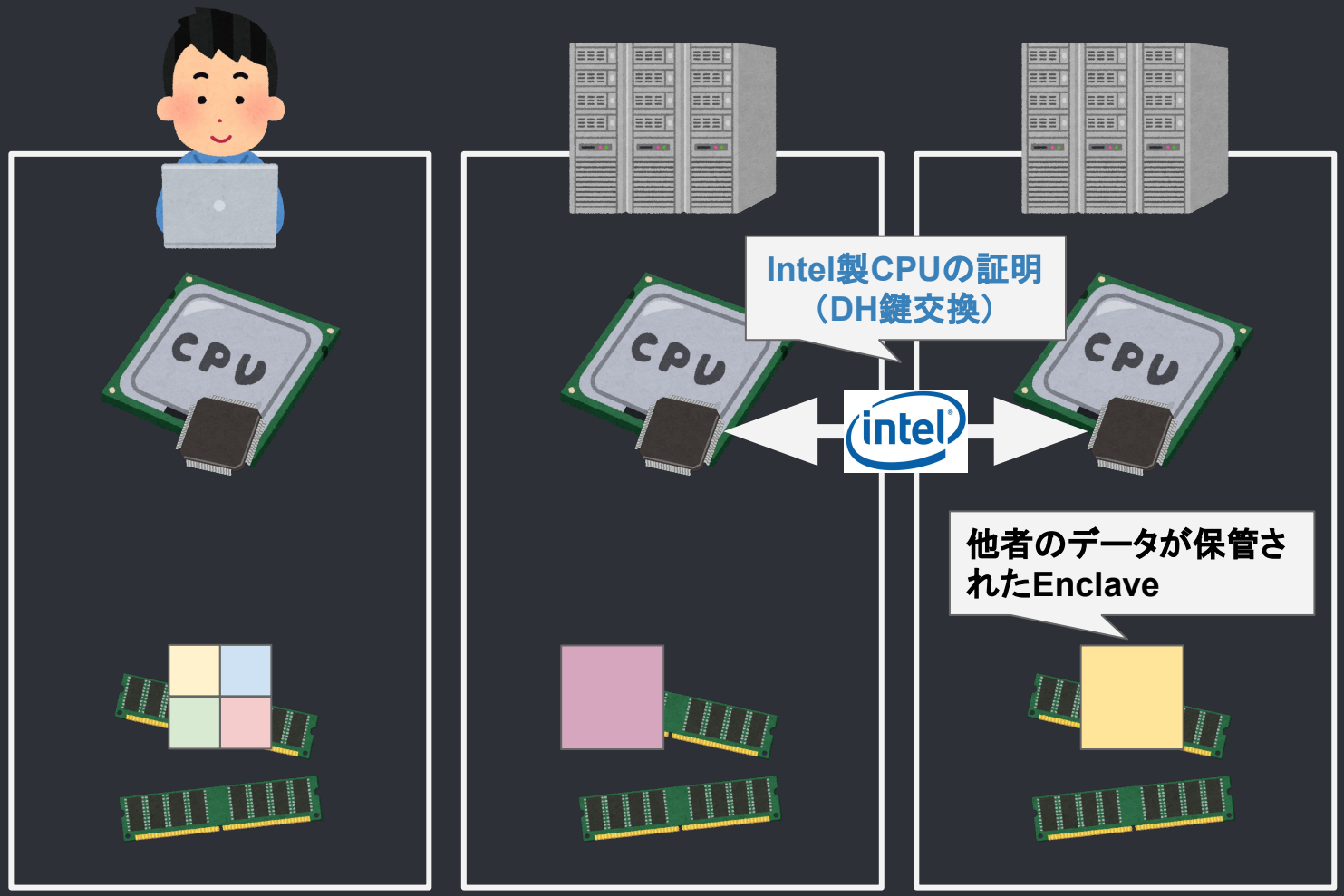


＜補足資料：Enigmaのもうひとつの秘匿計算アプローチ＞

Enigmaはハードウェアに依拠する秘匿計算モードも持つ（TEE）

分権性／秘匿性とパフォーマンスのトレードオフといえる

★ ■ と ■ を引数としたシークレットコントラクトを執行する時

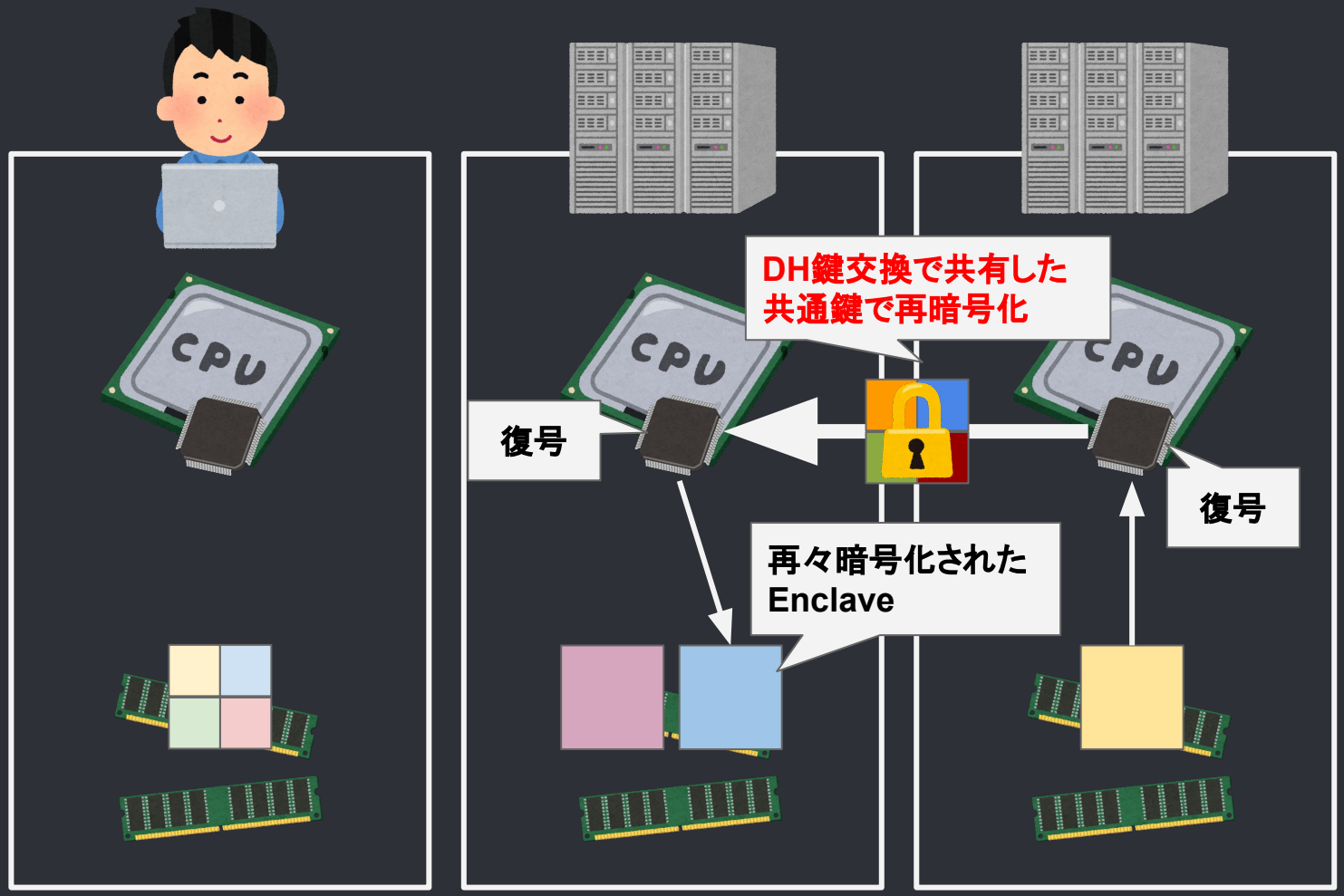


＜補足資料：Enigmaのもうひとつの秘匿計算アプローチ＞

Enigmaはハードウェアに依拠する秘匿計算モードも持つ（TEE）

分権性／秘匿性とパフォーマンスのトレードオフといえる

★  と  を引数としたシークレットコントラクトを執行する時

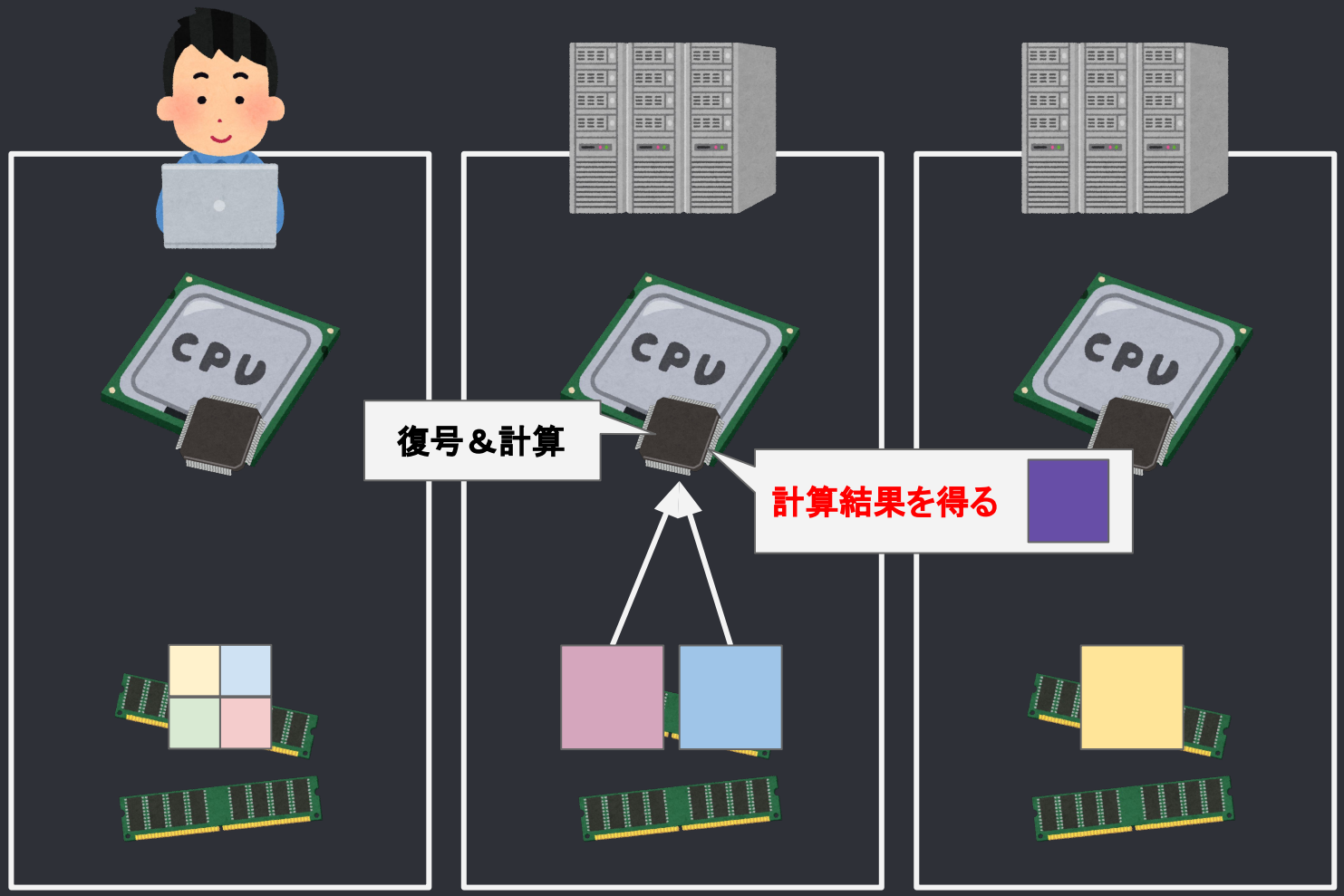


＜補足資料：Enigmaのもうひとつの秘匿計算アプローチ＞

Enigmaはハードウェアに依拠する秘匿計算モードも持つ（TEE）

分権性／秘匿性とパフォーマンスのトレードオフといえる

★ ■ と ■ を引数としたシークレットコントラクトを執行する時



もくじ

- プライバシーと中立性の問題
- 秘匿計算基盤”Enigma”の提案
- **Enigmaの未来と課題**

＜Enigmaで実現できる仕組み＞

Enigmaによる【 1 to 10 】と【 0 to 1 】

既存の仕組みを改善する【 1 to 10 】	まったく新しい価値を提供する【 0 to 1 】
既存のしくみを置き換え、プライバシーと中立性の問題を解決する手段を提供する	Enigmaの到来以前は実現が困難だったしくみを提供する
 投票、オークション  クレジットスコア、ID  ヘッジファンド、価格情報、シグナル CATALYST	次スライド参照 enigma data marketplace 情報銀行基盤 ※従来のパーソナルデータ取引所やデーターブローカーのための基盤と、インセンティブを提供する基盤を併せた環境

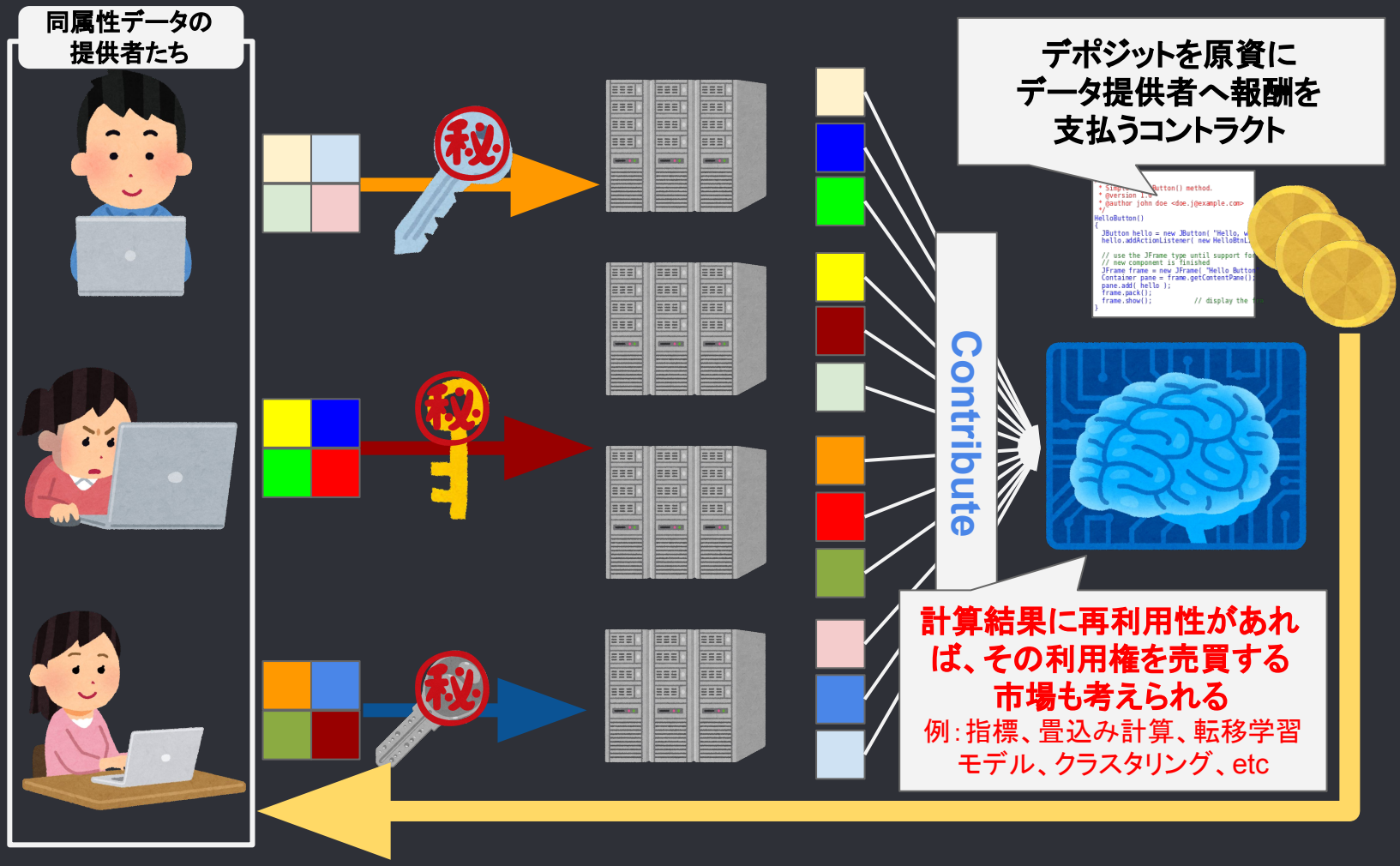
＜Enigmaによるデータマーケットプレイス（情報銀行基盤）＞

”秘匿性を保ったデータ提供”という行為がひとびとの新たな収入源となる

インセンティブにより多種多様なデータが提供されることが期待できる

単価や報酬の支払い条件はコントラクト毎に定義できる

例）データ利用毎、計算結果が利用されて売上が立つ毎、など



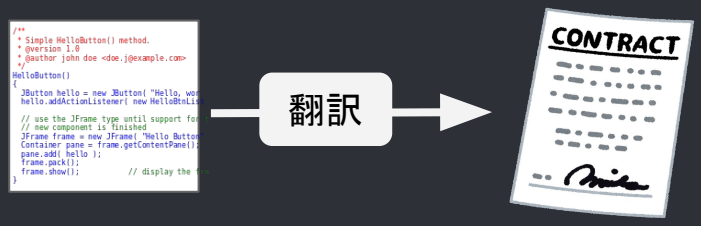
＜Enigmaの課題＞

Enigmaの本格活用に向けて、技術的・政治的な課題が存在する その解決に向けたいくつかの研究開発の必要性を提言する

技術的課題

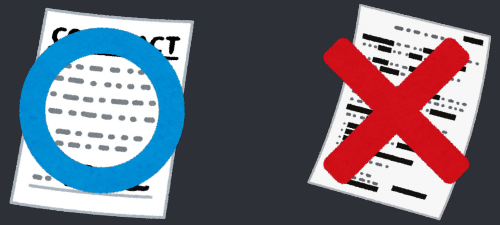
1. **シークレットコントラクトを読める人は少数派である**

データ提供者のリテラシ格差を埋める手段の研究（例:コントラクトの自然言語化）が必要



2. **コントラクトの表現制約が必須である**

秘匿されたデータを絞り込めてしまう表現を排除する手段の研究が必要



3. **sMPCの計算速度が遅い** ※特に非定数の乗算

4. **アプリケーション層の信頼性**

政治的課題

1. **反社会勢力への対処法を喪失する恐れ**

従来は省庁の求めに応じ、サービスの管理者がデータ提供を可能としていたが、中央管理者が不在な秘匿計算基盤では不可能である。
対策例として、データを暴露すべきかの判断をERC792的なアプローチで、全ノード間で投票し合う仕組みが有効と個人的に考える。

2. **デジタルマーケティング技 術の後退は許容されづらい**

プライバシーを犠牲にした現在のマーケティング技術の利便性に、Enigma上の仕組みが追いつくには時間がかかる。
既得権団体からのロビー活動がある限り、法規制などの追い風は期待しにくい。

＜まとめ＞

ひとびとが自身のデータに対して望むコントロールと、分析対象への需要を両立しながら、公正公平な計算基盤を提供できるのが”Enigma”

- ***『他人が管理するサーバに自身の情報を送った。けれど、その管理人に自身の情報を明け渡したつもりはないし、覗き見されたくもない』***
- ***『だれかに私のことを知って欲しい。けれど、私のことを知って欲しくない人たちもいる』***
- ***『あの人のことには興味ないけれど、あの人のデータが稼いでくれるおカネには興味がある』***

- このような複雑かつ困難な要求に応えられる仕組みが実現したとき、健全なデータ活用社会の発展を目指すことができる
- また提供されるサービスの構築プロセスを正しく明かすことで、権力の局所化を未然に防ぐことは、必然的になされるべき努力であると私は考える

Enigmaは
乙女心のように複雑で矛盾した
ひとびとの気持ちに応えてくれる

Enigma meets privacy.
Enigma meets neutrality.